OBSAH

Kapitola 1
Jak rychle začít

1.1 Úvod

Průvodce rychlým startem vám umožní rychle nastavit širokopásmový přístup k internetu. Tohoto průvodce také najdete na internetových stránkách pro nastavení zařízení řady Vigor2500V. Můžete ho tedy využít pro online nastavení zařízení prostřednictvím Internetu.

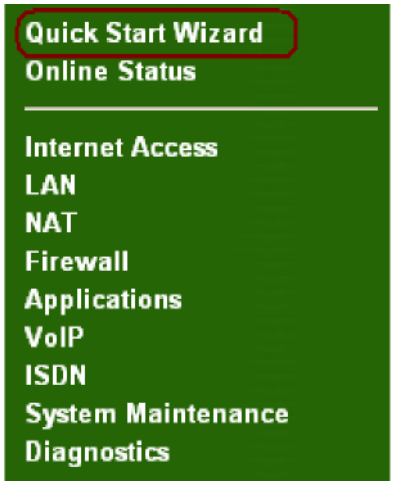
Průvodce rychlým startem můžete také vyvolat z nástroje směrovač (router), který najdete na CD, které je součástí balení. Pro bezproblémové nastavení vám doporučujeme využít možnosti on-line nastavení zařízení přes internet, prostřednictvím on-line průvodce rychlým startem.

Nastavení směrovače pomocí webovského konfiguračního programu (Web Configurator)

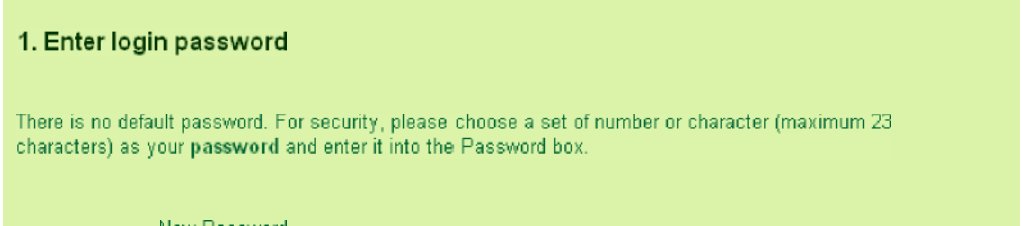
Krok 1 Spusťte internetový prohlížeč na vašem počítači, ke kterému je směrovač připojen a připojete se na IP adresu směrovače (standardní IP adresa **192.168.1.1).** Po úspěšném navázání připojení **(**http://192.168.1.1**)** se zobrazí vyskakovací okno pro zadání uživatelského jména (username) a hesla (password). Ponechte zde přednastavené hodnoty (prázdné pole) a klikněte na **OK.**

Pokud se vám nedaří připojit se k serveru pro online nastavení, podívejte se do průvodce "Problémy a jejich řešení (Trouble Shooting)".

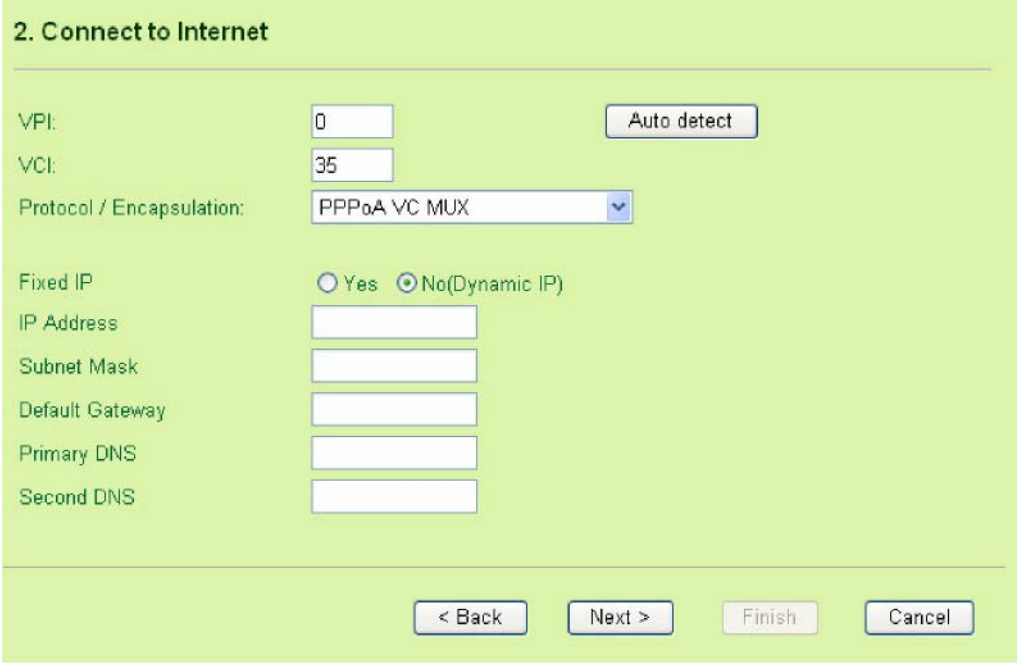
Krok 2 Po úspěšném dokončení předchozího kroku se zobrazí okno **Hlavní nabídka** (Main Menu).



Krok 3. Nyní je průvodce rychlým nastavením spuštěn. Zadejte přihlašovací heslo. Klikněte na tlačítko **Další** (Next).

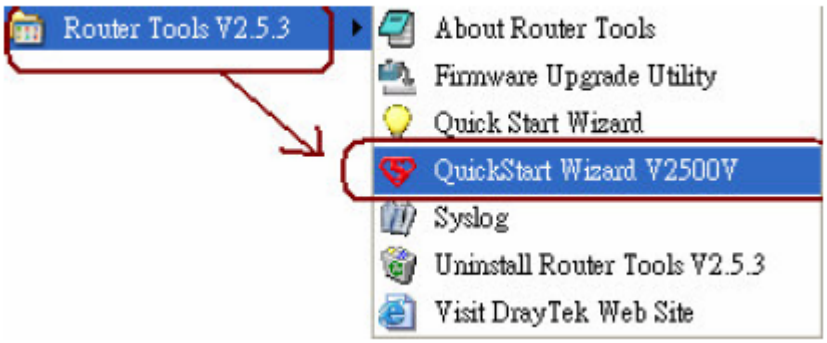


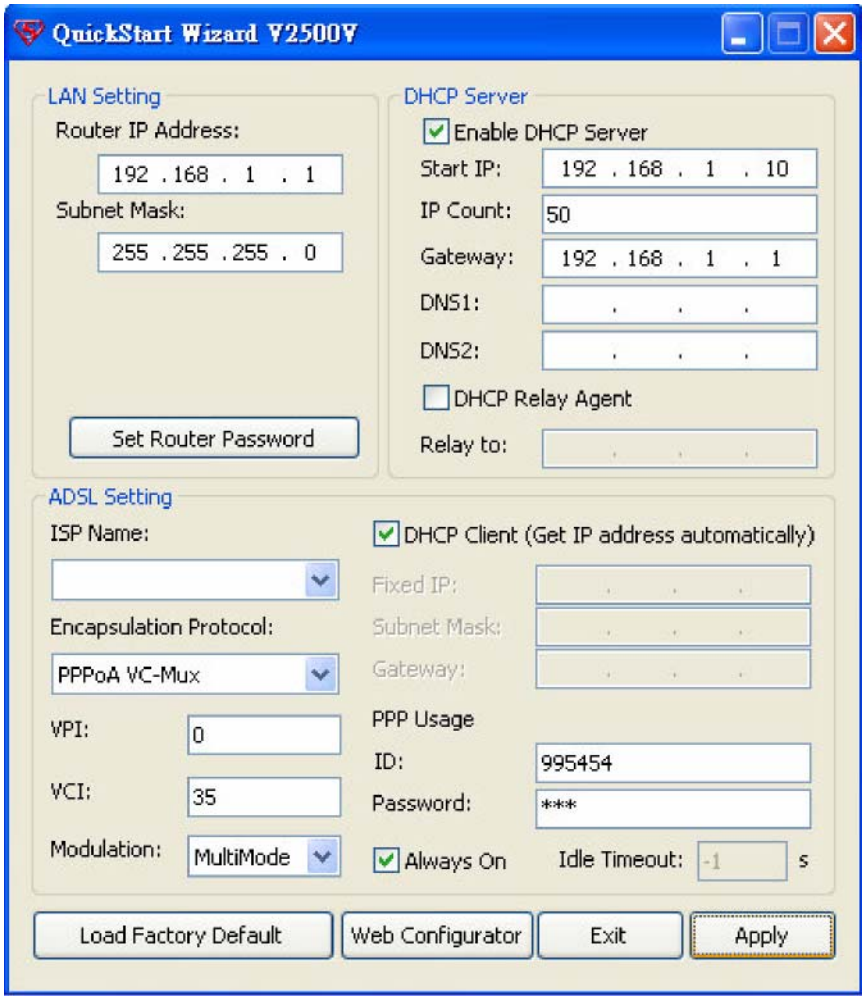
Krok 4 Nastavte parametry připojení podle údajů vašeho poskytovatele.
Poznámka: Pokud jste směrovač zakoupili od vašeho poskytovatele mohou být změny nastavení údajů pro jiné poskytovatele zakázány. Předtím než začnete měnit standardní nastavení nebo měnit poskytovatele připojení, pročtěte si podrobně smluvní podmínky, kterými jste vázáni vůči vašemu stávajícímu poskytovateli.



Pokud jste obdrželi pevnou IP adresu od vašeho poskytovatele připojení, zadejte údaje od vašeho poskytovatele.
Krok 5 Směrovač se "v případě potřeby" připojí k vašemu poskytovateli připojení. "V případě potřeby" znamená situaci, kdy se kterýkoli uživatel sítě LAN pokouší poslat data na Internet. Pokud nejsou přenášena žádná data, směrovač automaticky ukončí připojení k internetu, protože není "žádný požadavek" na datové přenosy. **"Odpojení v případě nečinnosti"** je odpojení po určité době nečinnosti internetového připojení, například po 10 minutách. Můžete zvolit 0 (nula) pokud chcete, aby po navázání připojení směrovač vždy zůstal připojen. Pokud zadáte parametr -1 (mínus jedna) bude směrovač usilovat o trvalé udržení připojení - "**Vždy online**". Nastavení 0 a -1 doporučujeme pouze pro pevná připojení (trvale online), jako je například ADSL. Nastavení lze také provést kliknutím na "**Vždy online (Always On)**".

I když je Průvodce rychlým startem k dispozici také na CD dodávaném se směrovačem, nebudete jej po dokončení předchozích nastavení připojení prostřednictvím internetu potřebovat.
Pokud nechcete postupovat výše uvedeným postupem, můžete použít Průvodce z CD. V takovém případě musíte průvodce nejprve nainstalovat z nabídky Nástroje směrovače (Router Tools):





Po nastavení parametrů ADSL, vám Průvodce rychlým startem pomůže automaticky nastavit zapouzdření protokolu (Encapsulation Protocol), VPI/VCI a modulaci (Modulation). Po nastavení nezbytných parametrů, klikněte na tlačítko **Použít** (Apply) a získáte připojení k internetu velmi snadno. Zobrazí se hláška "**Směrovač je nyní nastaven** (Router is now configured)"**!**
Zařízení Vigor2500V nejprve použije potřebné kodeky pro co nejlepší využití dostupné šířky pásma. Ovšem zařízení Vigor2500V je také vybaveno **automatickým zajištěním QoS!!** Funkce automatického zajištění QoS přidělí přenosu hlasu přes internet vysokou prioritu. Budete tak mít vždy k dispozici potřebné šířku pásma pro příchozí a odchozí hlasové informace, což je nutné pro přenos hlasu přes internet. Navíc zaznamenáte pouze malé zpomalení datových přenosů.

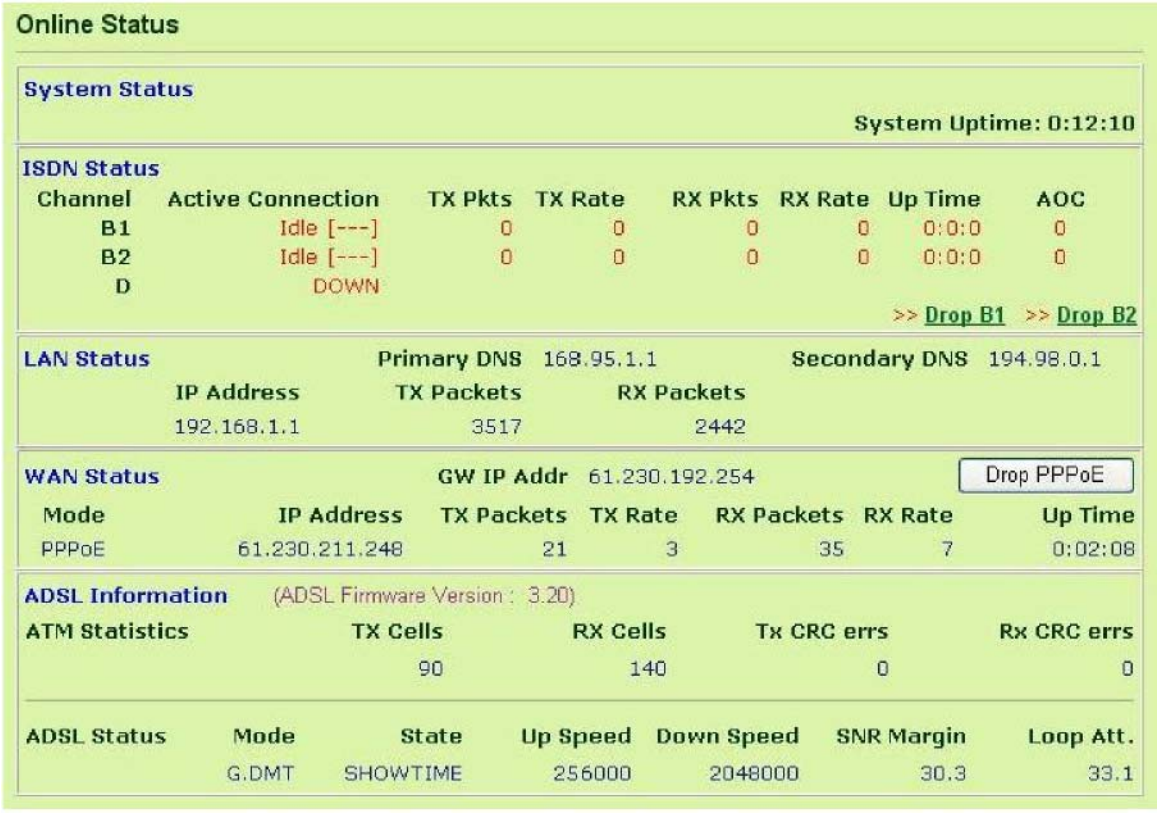
Kapitola 2
Stav připojení

2.1 Úvod

Stav připojení (**Online Status**) poskytuje užitečné informace o směrovači Vigor a o rozhraních ISDN, LAN a WAN. Tuto stránku můžete také využít ke sledování stavu připojení k internetu.

2.2 Popis obrazovky Stav připojení

Kliknutím na položku **Stav připojení** (Online Status) otevřete příslušnou stránku. K vysvětlení funkcí stránky **Stav připojení** použijeme následující příklad. V našem příkladě používá směrovač pro připojení k internetu režim dynamicky generovaného IP - viz. obrázek níže.



Stránka Stav připojení obsahuje tři základní podskupiny. Jedná se o podskupiny **Stav systému, Stav LAN, Stav WAN a informace o ADSL**. V případě modelu s podporou ISDN se na stránce Stav připojení zobrazují také údaje o ISDN připojení.

2.2.1 Stav systému (System Status)

Doba provozu systému (System Uptime): Doba provozu směrovače. Zobrazí se čas ve formátu HH:MM:SS, kde HH, MM, a SS představuji hodiny, minuty a sekundy.

2.2.2 Stav LAN (LAN Status)

IP Adresa: IP adresa připojení LAN.
TX Pakety: Celkový počet přenesených IP paketů od spuštění směrovače.
RX Pakety: Celkový počet přijatých IP paketů od spuštění směrovače.

2.2.3 Stav WAN (WAN Status)

Režim (Mode): Zobrazuje právě aktivní režim ADSL připojení. V závislosti na způsobu přístupu k ADSL se zobrazí **PPPoE, PPPoA nebo MPoA.**
IP adresa přenosové brány (GW IP Addr): IP adresa přenosové brány.
IP Adresa: IP adresa připojení WAN.
TX Pakety: Celkový počet přenesených IP paketů během aktuálního připojení.
Přenosová rychlost pro odesílání (TX Rate): Přenosová rachlost ve znacích za sekundu (cps) pro odesílání dat.
RX Pakety: Celkový počet přijatých IP paketů během aktuálního připojení.
Přenosová rychlost pro přijímání (RX Rate): Přenosová rachlost ve znacích za sekundu (cps) pro příchozí data.
Doba připojení (Up Time): Doba připojení. Zobrazí se čas ve formátu HH:MM:SS, kde HH, MM, a SS představuji hodiny, minuty a sekundy.

Odpojit PPPoE nebo PPPoA (Drop PPPoE or PPPoA): Klikněte na odkaz pro odpojení připojení PPPoE nebo PPPoA.

2.2.4 Stav ISDN (pouze pro model s podporou ISDN)

Aktivní připojení (Active Connection): Poskytovatel (ISP), aktivní vzdálený uživatel ISDN, nebo název připojení LAN-LAN a také IP adresa každého kanálu B.
Pakety TX (TX Pkts): Celkový počet přenesených IP paketů během aktuálního připojení.
Přenosová rychlost pro odesílání (TX Rate): Přenosová rachlost ve znacích za sekundu (cps) pro odesílání dat.
Pakety RX (RX Pkts): Celkový počet přijatých IP paketů během aktuálního připojení.
Přenosová rychlost pro přijímání (RX Rate): Přenosová rychlost ve znacích za sekundu (cps) pro příchozí data.
Doba připojení (Up Time): Doba připojení. Zobrazí se čas ve formátu HH:MM:SS, kde HH, MM, a SS představuji hodiny, minuty a sekundy. **Odpojit B1 (Drop B1):** Klikněte pro odpojení kanálu B1.
Odpojit B2 (Drop B1): Klikněte pro odpojení kanálu B2.

2.2.5 Informace o ADSL (ADSL Information)

Na obrazovce s aktuálním stavem směrovače (včetně logovacích souborů telnet) se zobrazují dvě čísla, která vyjadřují kvalitu a úroveň signálu ADSL.
Dobrý signál ADSL je spolehlivější a generuje méně chyb. Pokud si objednáte připojení ADSL zajistí vám váš poskytovatel připojení nebo Telecom jeho správné fungování.
Verze firmware ADSL (ADSL Firmware Version): Tento údaj představuje verzi čipové sady ve vašem ADSL modemu (je jiná než verze čipové sady směrovače).
Statistika ATM (ATM Statistics):
Odeslané bloky (TX Blocks): Celkový počet přenesených ATM bloků.
Přijaté bloky (RX Blocks): Celkový počet přijatých ATM bloků.
Opravené bloky (Corrected Blocks): Celkový počet přijatých ATM bloků, které byly porušeny, ale podařilo se je opravit.
Neopravené bloky (Uncorrected Blocks): Celkový počet přijatých ATM bloků, které byly porušeny a které se nepodařilo opravit.
Stav ADSL (ADSL Status):
Režim (Mode): Zobrazuje používaný způsob modulace: G.DMT, G.Lite, nebo T1.413.
Stav (State): Zobrazuje stav linky DSL.
Rychlost pro odesílání (Up Speed): Zobrazuje rychlost pro odesílání (bity/sekundu).
Rychlost pro stahování (Down Speed): Zobrazuje rychlost stahování (bity/sekundu).
Odstup signálu a šumu (SNR Margin): Zobrazuje odstup signálu a šumu (dB). Čím vyšší hodnota, tím lepší kvalita připojení.
Útlum smyčky (Loop Att.) : Zobrazuje útlum smyčky.

Kapitola 3
Přístup k internetu

3.1 Úvod

Pro většinu uživatelů je přístup k internetu primární aplikací. Směrovače řady Vigor2500V podporují pro připojení k internetu rozhraní ADSL, WAN a vzdálený přístup. V následujících odstavcích se dozvíte více o nastavení ADSL. Pokud kliknete na **Nastavení přístupu k internetu** (Internet Access Setup), můžete si pro váš směrovač nastavit různé režimy přístupu k internetu (tedy PPPoE, PPPoA a MPoA)
Jednotlivé možnosti nastavte výběrem následujících položek:

Internet Access Setup> **PPPoE / PPPoA**
> **MPoA (RFC 1483 / 2684)**
> **Multi-PVCs**

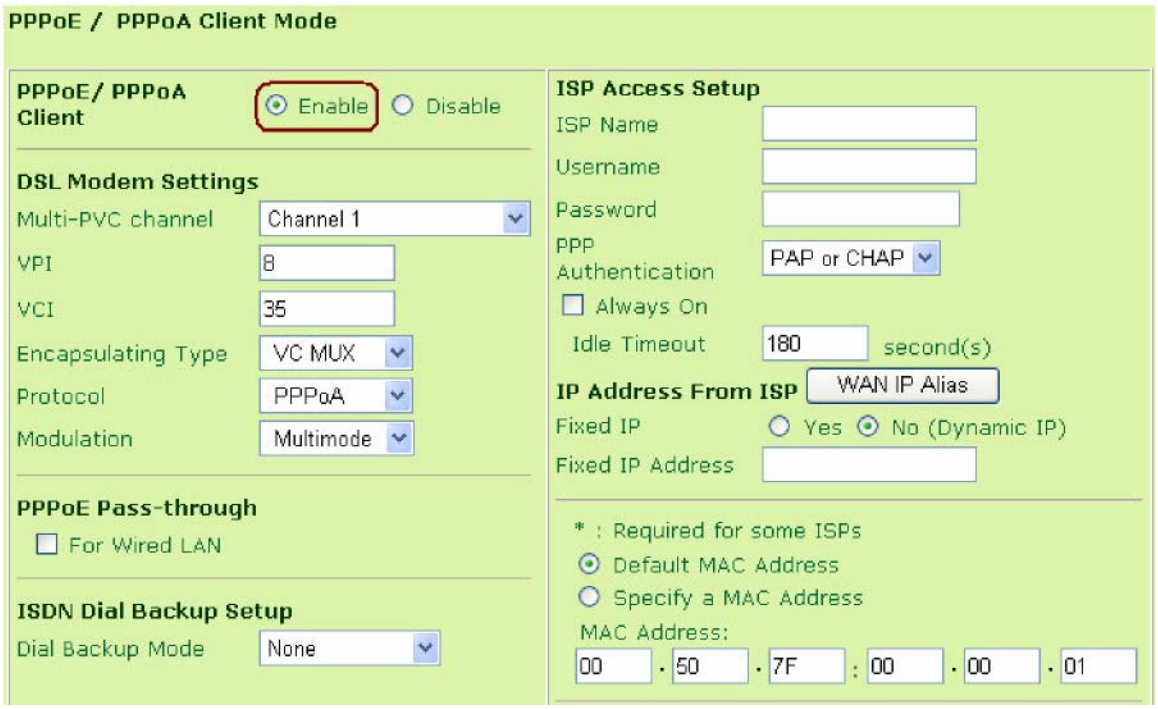
Pokud používáte připojení ADSL, musíte si od vašeho poskytovatele připojení zjistit jaký režim přístupu využívá. Režimy PPPoE / PPPoA a MPoA (RFC 1483 / 2684) nelze využívat současně.

Poznámka: Pokud chcete využívat více režimu současně (Multi-PVC), poraďte se nejprve s vaším poskytovatelem připojení. Ve většině případů nebudete v nabídce multi-PVC muset upravovat žádná nastavení pro režim MultiPVC, protože naše nastavení je již podporováno vaším poskytovatelem připojení nebo Telecomem.

3.2 Nastavení

3.2.1 Uživatelé PPPoE/PPPoA

Zadejte přidělené uživatelské jméno, heslo a parametry DSL, které vám poskytne váš poskytovatel připojení. Pokud chcete být k internetu připojeni trvale, zaškrtněte "**Vždy připojen**" (Always On).



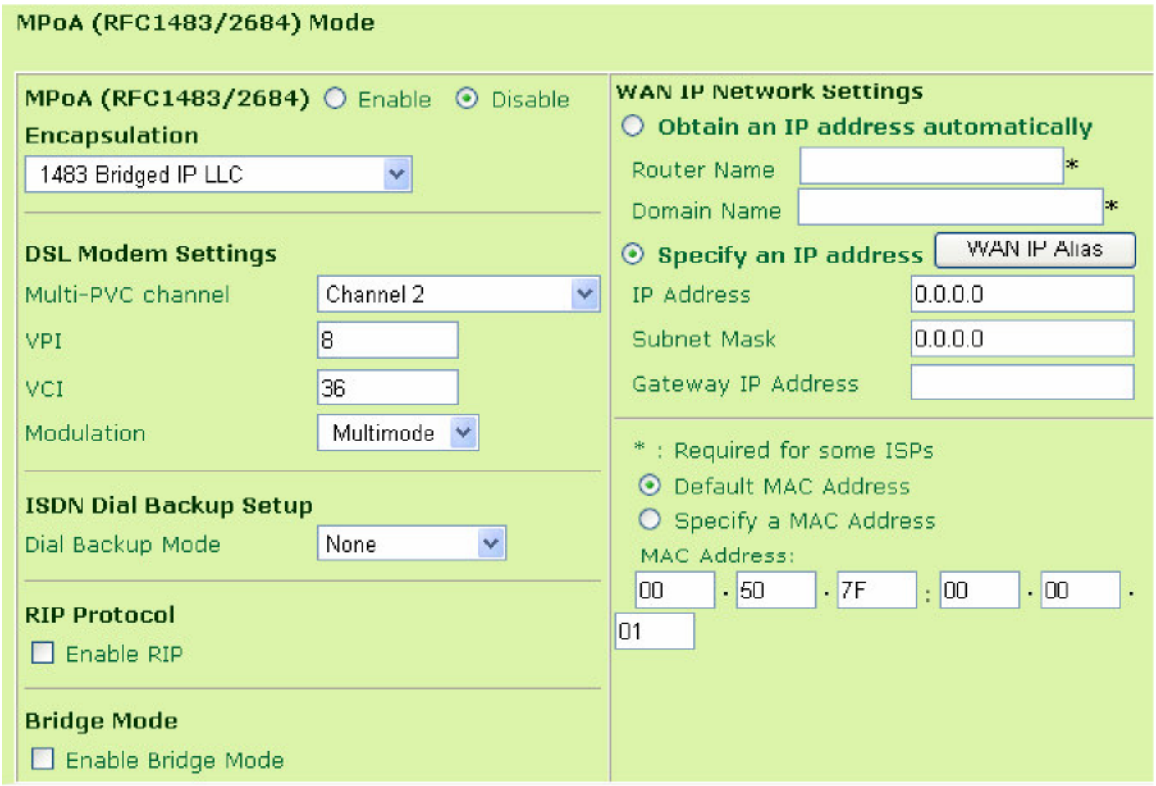
PPPoE připojení

Směrovač Vigor podporuje vytáčené připojení PPPoE. Kromě toho se prostřednictvím směrovače Vigor můžete připojit k vašemu poskytovateli připojení přímo z vašich místních počítačů.

Pro drátové sítě LAN: Zaškrtněte toto zaškrtávací pole. PPPoE připojení místních počítačů k vašemu poskytovateli připojení probíhá přímo přes síť LAN.

3.2.2 Uživatelé MPoA (RFC 1483/2684)

Zadejte přidělenou adresu WAN IP (nebo povolte automatické stahování IP adresy od svého poskytovatele připojení) a nastavení DSL, na základě informací získaných od vašeho poskytovatele připojení.

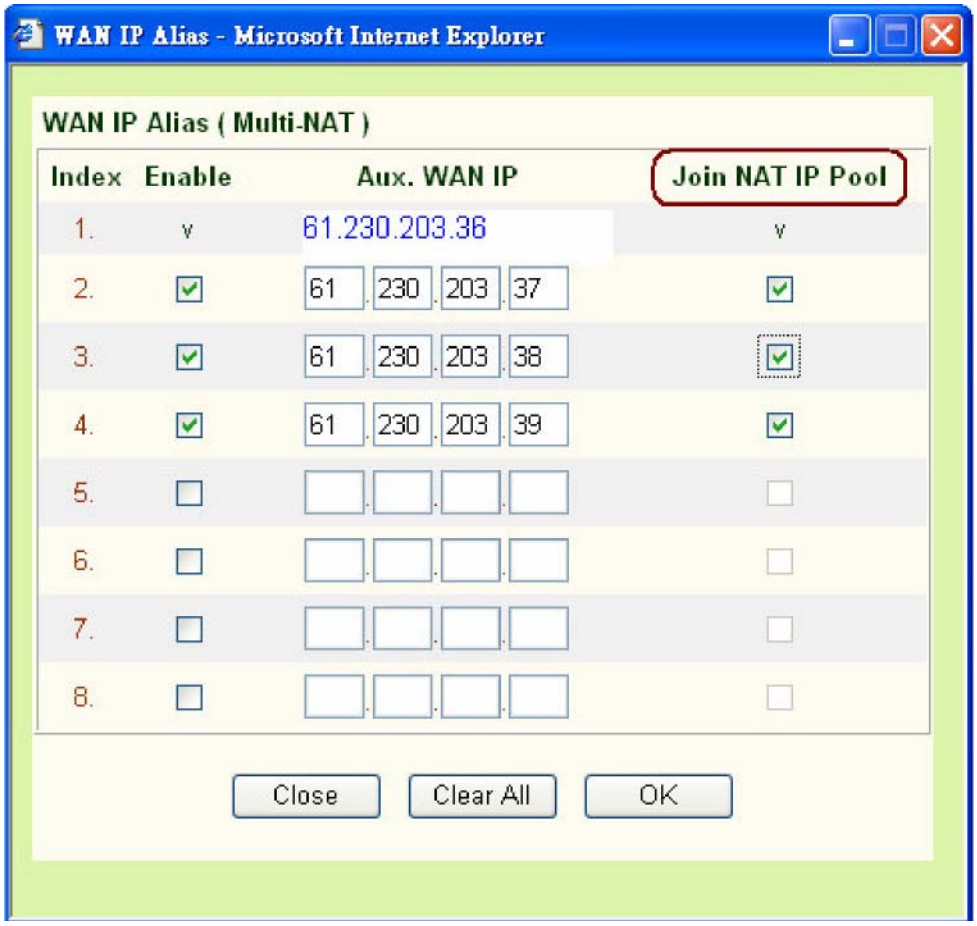


Protokol RIP (RIP Protocol)

Protokol pro směrování informací je označován zkratkou RIP

Zapnout RIP - Zaškrtněte toto zaškrtávací pole. Směrovač periodicky mění celou směrovací tabulku.

Pokud máte několik veřejných IP adres, přidělují se z rozhraní WAN. Po kliknutí na alias WAN IP se zobrazí následující vyskakovací okna. Zde můžete zadat další IP adresy a poté vše potvrdit stisknutím tlačítka OK.

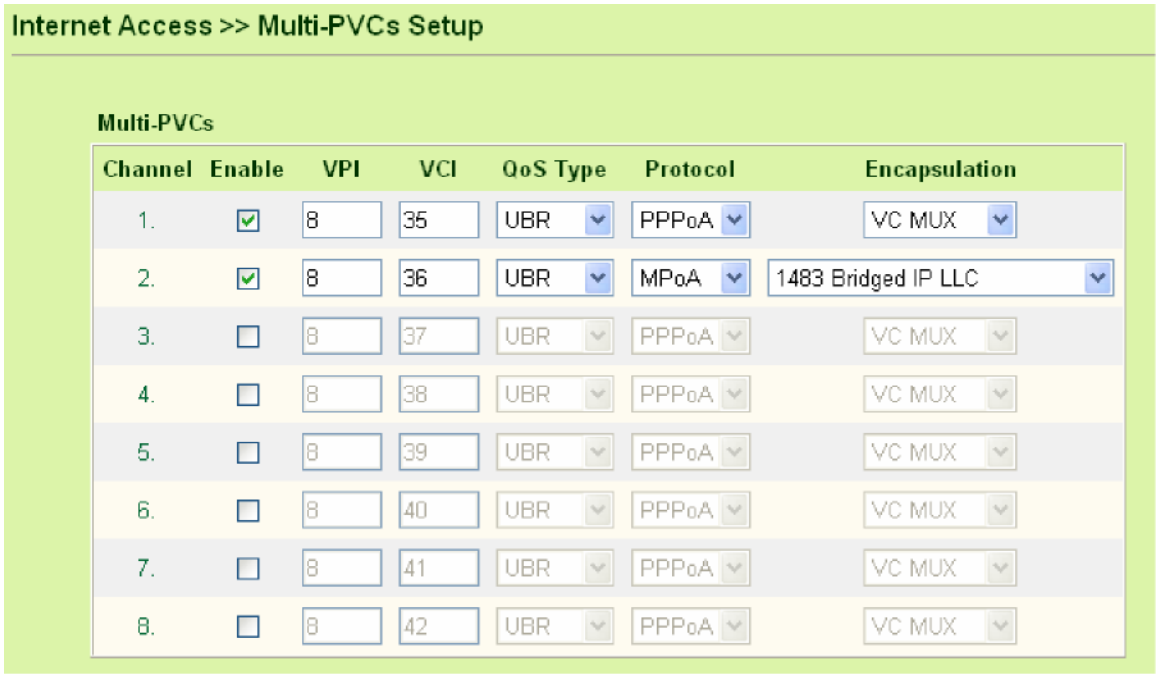

WAN IP Alias - Microsoft Internet Explorer
WAN IP Alias (Multi-NAT)
Index
Enable
Aux. WAN IP
Join NAT IP Pool
1.
v
61.230.203.36
v
2.
61 . 230 . 203 . 37
3.
61 . 230 . 203 . 38
4.
61 . 230 . 203 . 39
5.
6.
7.
8.
Close
Clear All
OK

3.2.3 Více protokolů (Multi-PVCs)

Tato funkce je určena pro správcovské funkce vašeho internetového poskytovatele nebo Telecomu. Ve většině zemí je funkce **MultiPVC určena ke vzdálené správě systému pro usnadnění technické podpory vašeho poskytovatele nebo Telecomu.**

Zadejte přidělené parametry DSL, které vám poskytne váš poskytovatel připojení. Typ QoS (QoS Type) je QoS nabízená ATM. Doporučujeme ponechat standardní nastavení (UBR).

Pokud chcete využívat více režimu současně (Multi-PVC), poraďte se nejprve s vaším poskytovatelem připojení. Ve většině případů nebudete v nabídce multi-PVC muset upravovat žádná nastavení pro režim MultiPVC, protože naše nastavení je již podporováno vaším poskytovatelem připojení nebo Telecomem.



Načtení nastavení ATM/ DSL z Průvodce rychlým startem

Nastavení ATM/DSL lze také načíst pomocí **Průvodce rychlým startem**. Postupujte podle pokynů na obrazovce. Pokud nenajdete vaši zemi v seznamu, může automatické načtení parametrů trvat delší dobu.

Internetové statistiky

Stav DSL lze také zjistit z okna stavu připojení.

Online Status

System Status

System Uptime: 0:12:10

ISDN Status

Channel	Active Connection	TX Pkts	TX Rate	RX Pkts	RX Rate	Up Time	AOC
B1	Idle [---]	0	0	0	0	0:0:0	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	DOWN						

>> Drop B1 >> Drop B2

LAN Status

Primary DNS 168.95.1.1 Secondary DNS 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	3517	2442

WAN Status

GW IP Addr 61.230.192.254 [Drop PPPoE]

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
PPPoE	61.230.211.248	21	3	35	7	0:02:08

ADSL Information

(ADSL Firmware Version : 3.20)

ATM Statistics	TX Cells	RX Cells	Tx CRC errs	Rx CRC errs
	90	140	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	30.3	33.1

Kapitola 4
LAN TCP/IP a DHCP

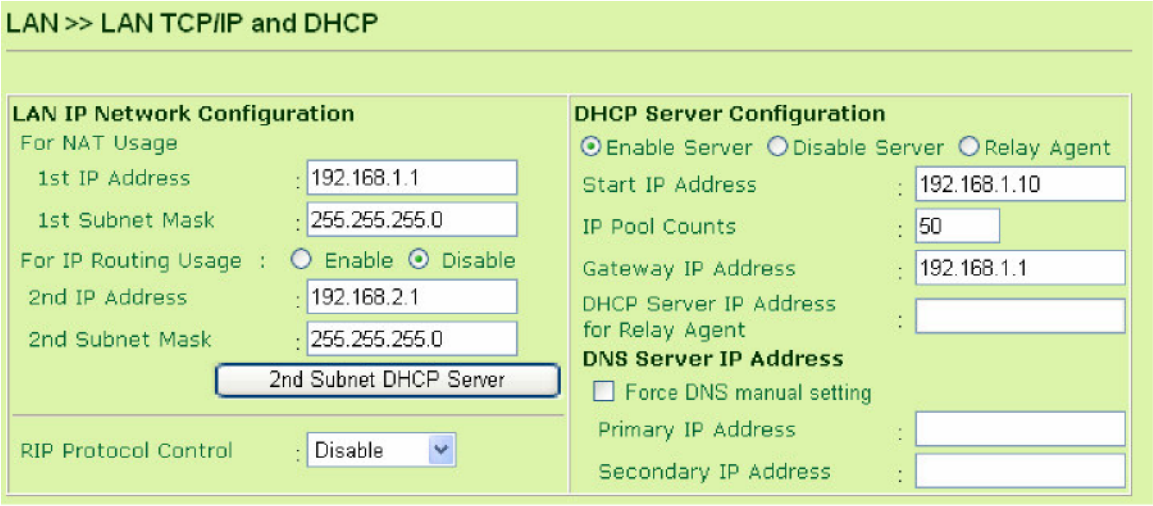
4.1 Nastavení IP sítě LAN

Směrovač Vigor nabízí dvě nastavení IP adres pro připojení LAN, tak jak je uvedeno dále. První nastavení IP adresy/masky podsítě je určeno pro privátní uživatele nebo uživatele NAT (překlad síťové adresy) a druhé nastavení IP adresy/masky podsítě slouží pro veřejné uživatele. Pro povolení přístupu veřejným uživatelům je nutné požádat vašeho poskytovatele služeb o přihlášení ke globálně přístupné podsíti.

Váš poskytovatel vám například k některým DSL účtům přidělí několik veřejných IP adres pro vaši místní síť. Jednu z těchto IP adres můžete použít pro váš směrovač a do druhého pole pro nastavení IP adresy/masky podsítě nastavte veřejnou IP adresu. Při nastavování ostatních lokálních počítačů nastavte IP adresu směrovače jako standardní přenosovou bránu. Po navázání DSL spojení s poskytovatelem služeb bude každý místní počítač přímo směrován na internet. První IP adresu/masku podsítě můžete využít také k připojení dalších privátních uživatelů (počítačů). IP adresy uživatelů budou směrovačem přeloženy na druhou IP adresu a odeslány přes DSL připojení.

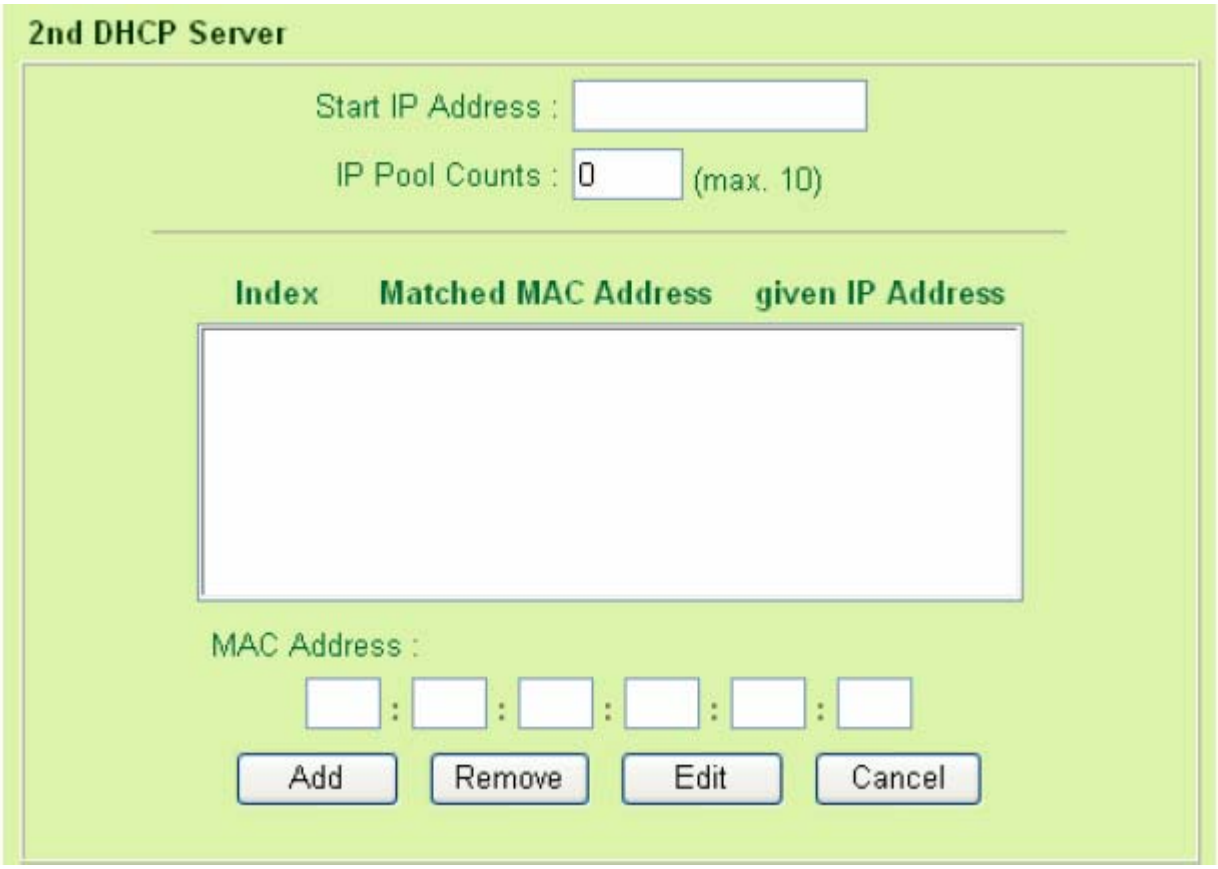
Nastavení můžete provést kliknutím na následující položky:

Internet Access Setup > **LAN TCP/IP a DHCP**



Používání překladu síťové adresy (NAT): (Standardní nastavení: Vždy zapnuto)
1. IP Adresa: Privátní IP adresa pro připojení k místní privátní síti (Standardně: 192.168.1.1).
1. maska podsítě (1st Subnet Mask): Maska podsítě pro místní privátní síť (Standardní nastavení: 255.255.255.0/24).
Používání směrování IP: (Standardní nastavení: Vypnuto)
Zapnutí: Zapne druhou IP adresu.
Zakázání: Vypne druhou IP adresu.
2. IP Adresa: Zadejte veřejnou IP adresu.
2. maska podsítě (2nd Subnet Mask): Nastavte masku podsítě pro veřejnou IP adresu.

2. DHCP server podsítě: Obrázek níže ukazuje 2 DHCP server podsítě směrovače Vigor.



Počáteční IP Adresa: Nastavte počáteční IP adresu z koše IP adres.
Počet IP adres v koši (IP Pool Counts): Nastavte počet IP adres v koši.
MAC adresy: Zadejte specifické MAC adresy, které lze přidávat, odebírat nebo upravovat ze seznamu přístupů.
PŘIDAT (ADD): Přidá MAC adresu do seznamu.
Smazat: Smaže MAC adresu ze seznamu.
Upravit: Úprava MAC adresy ze seznamu.
Zrušit: Zrušit nastavování kontroly přístupu přes MAC adresu.
Zavřít: Zavře toto okno.
Vymazat vše: Vymaže všechny MAC adresy ze seznamu.
OK: Uloží seznam řízení přístupů.

Nastavení RIP protokolu (RIP Protocol Control):
Zakázat: Zakáže výměnu RIP paketů přes síť LAN.
1. podsíť: Nastavte první podsíť pro výměnu RIP paketů s okolními směrovači připojenými do sítě LAN.
2. podsíť: Nastavte druhou podsíť pro výměnu RIP paketů s okolními směrovači připojenými k síti LAN.

4.2 Nastavení serveru DHCP

DHCP je aplikační protokol pro dynamickou konfiguraci koncových stanic sítě. Umožňuje automatické doručení příslušných nastavení IP na každou koncovou stanici, která je nastavena jako

Počáteční IP adresa*:* Nastavte počáteční IP adresu z koše IP adres.
Počet IP adres v koši*:* Nastavte počet IP adres v koši.
MAC adresa*:* Zadejte příslušnou MAC adresu, kterou můžete přidat do seznamu, smazat ze seznamu nebo upravovat.

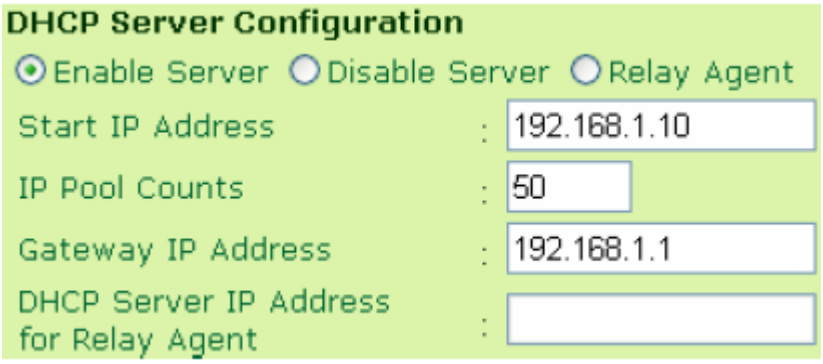
Přidat (ADD)*:* Přidá MAC adresu do seznamu.
Smazat (Remove)*:* Smaže vybranou MAC adresu ze seznamu.
Upravit (Edit)*:* Upraví vybranou adresu ze seznamu.
Zrušit (Cancel)*:* Zruší nastavování MAC adresy.

Zavřít (Close)*:* Zavře toto okno.
Smazat vše (Clear All)*:* Smaže všechny MAC adresy ze seznamu.
OK*:* Uloží seznam kontroly přístupu.

Ovládání RIP protokolu:
Zakázat (Disable): Zakázat výměnu RIP paketů přes síť LAN.
***1. podsíť*:** Nastavte první podsíť pro výměnu RIP paketů se sousedními směrovači *LAN TCP/IP a DHCP* připojenými k síti LAN.
***2. podsíť*:** Nastavte druhou podsíť pro výměnu RIP paketů se sousedními směrovači připojenými k síti LAN.

4.2 Nastavení serveru DHCP

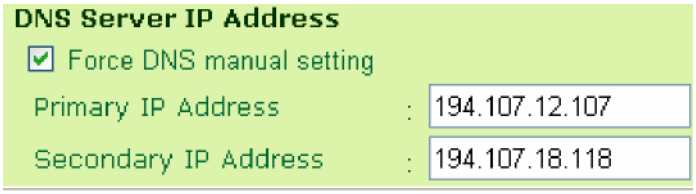
DHCP znamená protokol řízení dynamické konfigurace síťových počítačů. Umí automaticky zasílat nastavení IP kterémukoli místnímu uživateli, jehož konfigurace je DHCP klient. Pro nastavení DHCP serveru využijte níže uvedený obrázek.



Zapnout server: Automatické přidělení IP adresy pro PC připojené k síti LAN.
Zakázat server: Ruční nastavení IP adresy pro PC připojené k síti LAN.
Přenos (Relay Agent): Umožňuje počítačům připojeným k síti LAN vyžádat si IP adresu z jiného DHCP serveru.
Počáteční IP Adresa: Nastavte počáteční IP adresu z koše IP adres.
Počet IP adres v koši (IP Pool Counts): Nastavte počet IP adres v koši.
IP Adresa propojovací brány: Zadejte IP adresu DHCP serveru. Pokud směrovač funguje jako standardně nastavená propojovací brána, bude obvyklé nastavení stejné jako nastavení první IP adresy.

4.3 Jak pracovat s DNS na směrovači Vigor?

Dva body připojené do internetu jsou charakterizovány číselnou IP adresou. Pro usnadnění jsme si zvykli používat jména, spíše než čísla (například www.draytek.com), ovšem pokud chceme posílat data, musí být tyto názvy převedeny zpět na svoji skutečnou číselnou adresu. Tomu se říká tzv. "rozpoznávání jmen". DNS server zajišťuje tento převod, takže všichni uživatelé sítě LAN musí znát adresu jejich DNS serveru.
Pokud váš počítač získává IP adresu automaticky ze směrovače (použitím protokolu **DHCP**), bude mu automaticky sdělena i adresa příslušného DNS serveru**.** Na počátku nastaví adresu DNS serveru směrovač, ale poté co je navázáno spojení s vaším poskytovatelem připojení, je adresa DNS serveru přidělována poskytovatelem. Následkem toho máte možnost zrušit všechny nastavení DNS serverů a vynutit si používání vlastního nastavení, které zadáte do příslušných polí při nastavování sítě LAN (viz. níže).¨



Primární IP Adresa: Primární IP adresa DNS serveru.
Sekundární IP Adresa: Sekundární IP adresa DNS serveru.

Po připojení směrovače k vašemu poskytovateli internetu, přidělí nastaví poskytovatel připojení adresu svých DNS serverů. Toto nastavení potom přepíše vaše ruční nastavení DNS serverů. Pokud si i přesto chcete vynutit používání ručně nastavených DNS serverů, můžete použít příkaz telnetu " **srv dhcp frcdnsmanl on"** (parametrem "**off**" zrušíte používání manuální nastavení). Použití tohoto příkazu ale vyžaduje verzi čipové sady 2.5.6 nebo vyšší.

Pokud necháte obě pole pro primární a sekundární IP adresy prázdná, směrovač automaticky přidělí svoji vlastní IP adresu lokálním uživatelům, jako DNS proxy server a uloží ji do DNS cache.
Pokud je IP adresa vašeho doménového jména již uložena v DNS cache, zjistí směrovač doménové jméno okamžitě. V opačném případě pošle směrovač paket s dotazem na jméno DNS serveru na externí DNS server pomocí WAN (tedy DSL/kabelového) připojení.

Kapitola 5
NAT (Překlad síťové adresy)

5.1 Úvod

NAT (Network Address Translation) umožňuje namapování jedné nebo více IP adres a/nebo obslužných portů pro různé aplikace. Směrovač Vigor vezme jednu veřejnou IP adresu, přidělenou vaším poskytovatelem a automaticky odešle data probíhající mezi směrovačem a lokální stanicí (nebo přenosným počítačem) do vaší místní sítě. Externí uživatelé mimo síť mohou vidět veřejnou IP adresu směrovače. Nicméně externí uživatelé se nemohou dostat k IP adrese každého počítače / přenosného počítače. Všechny "nevyžádané" TCP/IP pakety směřující na vaši IP adresu dojdou k vašemu směrovači, ale směrovač nemůže tento paket poslat na žádný počítač nebo notebook v síti LAN. NAT tedy hraje důležitou úlohu při ochraně vašich síťových uživatelů, protože privátní IP adresy uživatelů připojených k vaší síti jsou skryty před okolním světem, dokud porty nebo protokoly neotevřete pro navázání spojení.
Prostřednictvím jediné veřejné IP adresy tak může několik počítačů připojených k vaší síti sdílet širokopásmové připojení poskytované ADSL linkou. To má význam z hlediska úspory nákladů, protože pro každý počítač či notebook nemusíte kupovat veřejnou IP adresu, ale díky funkci NAT směrovače Vigor můžete využít jednu veřejnou IP adresu pro generování několika privátních IP adres pro počítače ve vaší síti.

5.2 Nastavení NAT

Funkci NAT vašeho směrovače budete využívat pro většinu aplikací. Směrovač s funkcí NAT získá jednu (v režimech Single ISP, PPPoE, PPPoA, MPoA) globální směrovatelnou IP adresu od poskytovatele připojení a přiděluje privátní síťové IP adresy definované protokolem RFC-1918 lokálním počítačům. Směrovač vybavený funkcí NAT překládá privátní síťové adresy na globálně směrovatelnou IP adresu tak, aby koncoví uživatelé sítě mohli vzájemně komunikovat se směrovačem a připojovat se k internetu. Směrovač Vigor nabízí 3 následující možnosti mapování portů:
Přesměrování portu
Vzdálený počítač DMZ
Otevření portů
Co se týče definice RFC1918 pro privátní IP adresy, mohou uživatelé pro místní síťové klienty použít adresu 192.168.1.0/24 - máte-li například 3 počítače v různých místnostech, můžete jim přidělit 3 privátní adresy. Z těchto počítačů se můžete připojovat k internetu, protože směrovač Vigor tyto privátní IP adresy přeloží na jedinou veřejnou IP adresu, kterou vám přidělil poskytovatel připojení.
Nastavení můžete provést kliknutím na následující položky: **NAT> Port Redirection (Přesměrování portů)**
> DMZ Host
> Open Ports (Otevřené porty)
> Well-Known Ports List (Seznam známých portů)

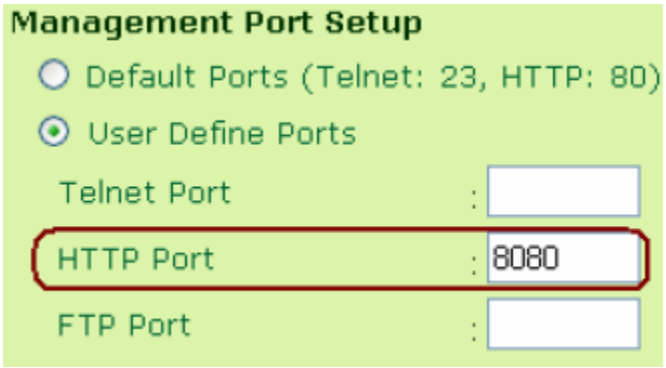
5.3 Nastavení tabulky přesměrování portů

Funkce Port Redirection vám umožní zpřístupnit vaše interní servery přes veřejnou doménu. Například provozujete internetový server a ostatní uživatelé chtějí mít k tomuto serveru přístup. Můžete také provozovat interní poštovní SMTP server pro vaši domácí kancelář a chcete, aby váš poskytovatel posílal všechny emaily na váš poštovní SMTP server. V **Tabulce přesměrování portů** nastavíte přidělíte různým službám jednotlivá čísla portů, jako například http, smtp, ftp, apod. Externí uživatelé, tedy lidé připojení k síti internet, pak získají přístup k vaší internetové prezentaci přes vaši veřejnou IP adresu. Dokonce i v případě, že je vaše veřejná IP adresa dynamicky přidělována, můžete použít službu Dynamic DNS k získání WAN IP adresy online (například hostnmae.dyndns.org), kterou je možno namapovat k vaší stávající dynamické IP adrese. V tomto případě může kterýkoli externí uživatel navštívit vaše internetové stránky jednoduše přes online WAN IP adresu.
Níže uvedený příklad ukazuje zpřístupnění FTP serveru přes veřejnou doménu. Interní FTP server běží na místí hostitelské adrese 192.168.1.10.

Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	FTP	TCP	21	192.168.1.10	21	☑
2		---	0		0	☐
3		---	0		0	☐
4		---	0		0	☐
5		---	0		0	☐
6		---	0		0	☐
7		---	0		0	☐
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

Z výše uvedeného obrázku vyplývá, že **Tabulka přesměrování portů** nabízí 10 volných polí pro namapování jednotlivých interních serverů.
Název služby (Service Name): Uveďte název příslušné služby sítě.
Protokol (Protocol): Vyberte vrstvu přenosového protokolu (TCP nebo UDP).
Veřejný port (Public Port): Uveďte číslo portu, který chcete přesměrovat na interní server.
Privátní IP adresa (Private IP): Zadejte privátní IP adresu interního serveru, na kterém služba běží.
Privátní port (Private Port): Uveďte číslo privátního portu serveru, na kterém běží příslušná služba.
Aktivace (Active): Zaškrtněte pro aktivaci přesměrování. Klikněte na **OK**
POZNÁMKA!
Protože směrovač má v sobě zabudovaný vlastní internetový server musíte, pokud chcete měnit jeho nastavení pomocí vzdáleného přístupu, změnit http "port" směrovače na jinou než **standardně** nastavenou hodnotu **80.** Změnu nastavení administrátorského portu provedete z menu **Nastavení řídícího portu** (**Management Setup**) a poté se připojíte k administrátorské obrazovce tak, že standardní IP adresy směrovače Vigor přepíšete na 8080 - tedy **http://192.168.1.1:8080.**



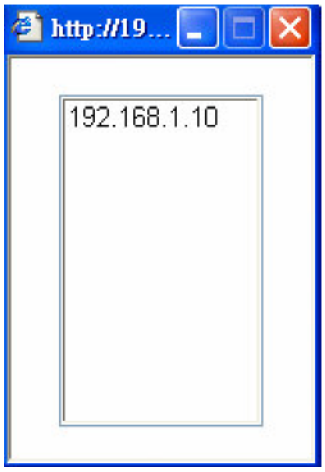
POZNÁMKA!
Přesměrování portu lze použít pouze vůči externím uživatelům - tedy pro příchozí data. Uživatelé internetu mimo vaší LAN nemohou přistupovat k vaší externí veřejné IP adrese a dostat se dovnitř; interní uživatelé se připojují k serveru pomocí jejich místní privátní IP adresy, nebo jim můžete nastavit alias v hostitelském souboru Windows. Funkci přesměrování portů používejte pouze u těch portů, u kterých je to nezbytné. Nepřesměrovávejte všechny porty. Mohli byste porušit zabezpečení systému přes bránu Firewall.

5.4 Nastavení DMZ Host

Funkce **Přesměrování portů** umožňuje přesměrovat všechna data na protokolem UDP/TCP na porty interních klientů vaší sítě LAN. Nicméně ostatní IP protokoly, jako například Protocols 50 (ESP) a 51 (AH) nemají čísla portů a proto nemáte možnost určit na který lokální klientský počítač se data budou přesměrovávat. Směrovač Vigor disponuje funkcí DMZ, která vám umožní nastavit jednoho lokálního klienta (pomocí privátní IP adresy), na kterého budou přesměrovávána VŠECHNA nevyžádaná data ze všech protokolů. Normální přístup k internetu a další internetové činnosti prováděné ostatními klienty budou normálně fungovat bez přerušení.

POZNÁMKA!
Interní zabezpečení funkce NAT je v případě používání funkce DMZ poněkud obcházeno. Proto zvažte možnost přidání dalších pravidel filtrování dat, či instalaci druhé brány Firewall.
I když přes DMZ budou všechny data přesměrována, existují protokoly, které se s funkcí překladu adres (NAT) nesnáší. Například přípona "AH" funguje tímto způsobem. Znemožňuje překlad adresy – v záhlaví paketu je uvedena zdrojová IP adresa, kterou je v tomto případě vaše privátní IP adresa. Ovšem přijímací strana zjistí, že paket přichází z vaší veřejné IP adresy a proto jej odmítne přijmout. AH protokol tedy nebude fungovat. Naproti tomu ESP protokol je tolerantnější.
Klikněte na položku **DMZ Host Setup** pro otevření níže uvedené nastavovací stránky. Nastavení DMZ Host umožní, aby vybranému internímu uživateli byl umožněn přístup na internet za účelem používání speciálních IP-protokolů, které jsou využívány aplikacemi, jako například Netmeeting, Internet Games, apod. Postup nastavení je uveden dále.

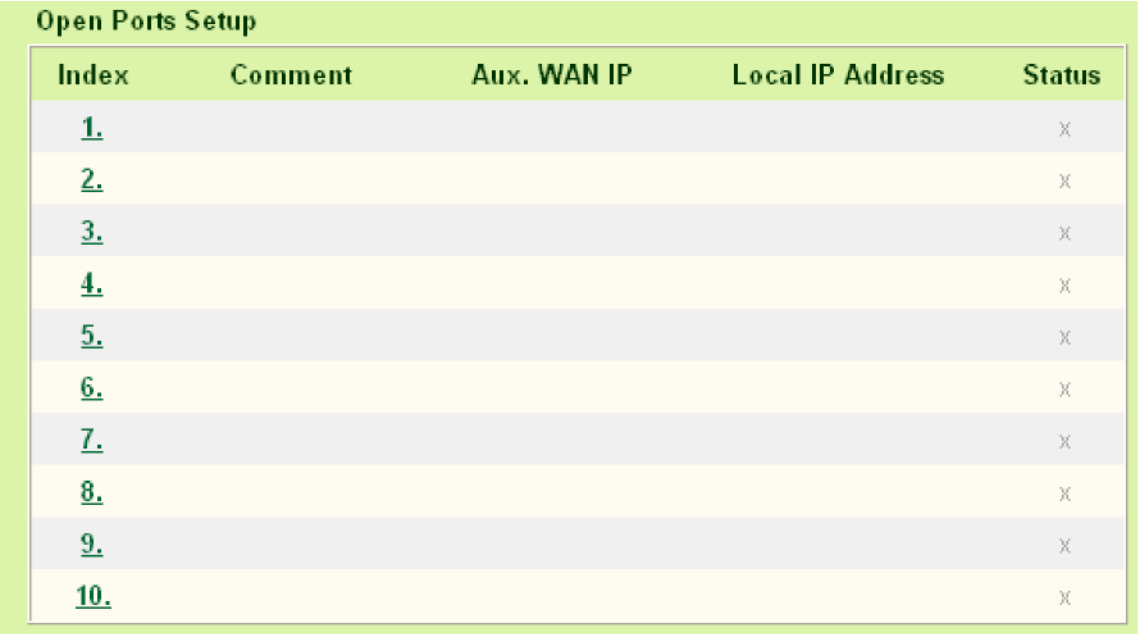
Zapnout (Enable): Zaškrtněte pro zapnutí funkce DMZ Host.
Privátní IP adresa (Private IP): Zadejte privátní IP adresu hostitelského počítače DMZ.
Vybrat PC (Choose PC): Po kliknutí na toto tlačítko se automaticky zobrazí okno se všemi privátními IP adresami všech hostitelských počítačů ve vaší síti LAN. Zvolte jednu privátní IP adresu ze seznamu, která bude fungovat jako hostitelský počítač DMZ.



5.5 Nastavení otevřených portů (Open Port Setup)

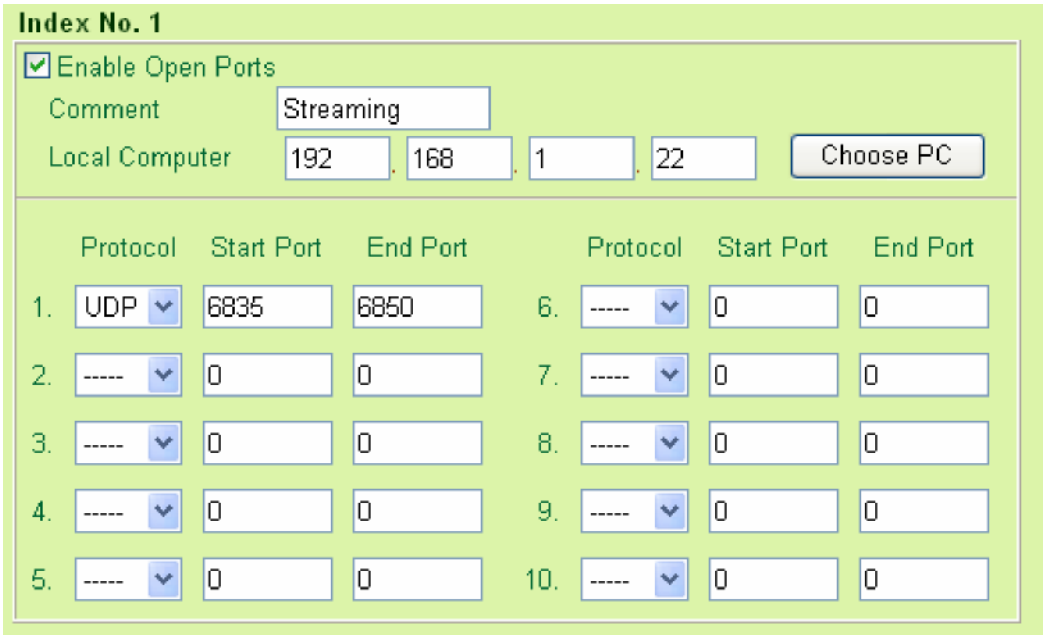
Funguje stejně jako přesměrování portů (viz. výše), ale umožňuje vám definovat **rozsah** portů.

Obrázek níže ukazuje obrazovku **Open Ports Setup.** Směrovač Vigo umožňuje nastavení funkce **Open Ports** až pro deset interních hostitelských počítačů.



Index: Pořadové číslo nastavené služby. Pro úpravu nebo vymazání dané služby, klikněte na danou položku.
Název (Comment): Zobrazuje název příslušné služby sítě.
Místní IP Adresa (Local IP Address): Zobrazuje privátní IP adresu interního serveru, na kterém služba běží.
Stav (Status): Zobrazuje stav příslušné služby. Písmena X a V znamenají *Aktivní* nebo *Neaktivní* stav.

Jak je uvedeno výše, po kliknutí na příslušné pořadové číslo (například Index 1) se zobrazí následující obrazovka, kde lze provést podrobné nastavení dané položku seznamu. Pro každou položku (místní hostitelský počítač) lze nastavit až deset rozsahů portů pro různé služby. Počítač s privátní IP adresou 192.168.1.22 bude hostitelským počítačem pro příchozí paket s názvem "streaming". Z obrázku vidíme, že nastavení rozmezí portů pro UDP protokol je mezi 6835 - 6850.



Zapnout funkci Open Ports: Zaškrtněte pro povolení funkce Open Port pro tuto položku.
Název (Comment): Uveďte název příslušné služby sítě.
Místní počítač (Local Computer): Zadejte privátní IP adresu místního hostitelského počítače.
Vybrat PC (Choose PC): Po kliknutí na toto tlačítko se automaticky zobrazí okno se seznam privátních IP adres místních hostitelských počítačů. IP adresu příslušného místního hostitelského počítače vyberte ze seznamu.
Protokol (Protocol): Zvolte přenosový protokol. Možná nastavení jsou TCP, UDP nebo ŽÁDNÝ (NONE).
Počáteční port (Start Port): Uveďte počátečního číslo portu místního hostitelského počítače, na kterém běží příslušná služba.
Koncový port (End Port): Uveďte koncové číslo portu místního hostitelského počítače, na kterém běží příslušná služba.

5.6 Priority jednotlivých nastavení mapování portů

Směrovač Vigor nabízí 3 možnosti mapování portů: Přesměrování portu (Port Redirection), Otevření portů (Open Ports) a DMZ.
Port Redirection – příchozí paket je přesměrován na zvolený místní počítač nebo notebook, pokud se číslo portu shoduje s číslem portu počítače. Přesměrování portu na jiný port můžete provést místně.
Open Ports -- Funguje stejně jako přesměrování portů (viz. výše), ale umožňuje vám definovat **rozsah** portů.
DMZ Host – Zcela otevře vybraný počítač nebo notebook. Všechny příchozí pakety budou přesměrovány na PC se zadanou místní IP adresou. Jedinou výjimkou jsou pakety obdržené jako odpověď na odchozí pakety z ostatních místních počítačů, nebo příchozí pakety, které vyhovují pravidlům dvou výše uvedených způsobů mapování.
Používání mapování se řídí určitými prioritami. **Priorita výše uvedených 3 možností mapování je následující: Port Redirection > Open Ports > DMZ**
Například: Pokud příchozí paket současně splňuje podmínky nastavené v **Port Redirection** a **Open Ports**, bude přesměrován na místní adresu uvedenou v **Port Redirection.**

5.7 Seznam obecně známých čísel portů (Well-known Port Number List)

Na této stránce najdete seznam nejpoužívanějších čísel portů.

NAT >> View Well-Known Ports List

Well-Known Ports List

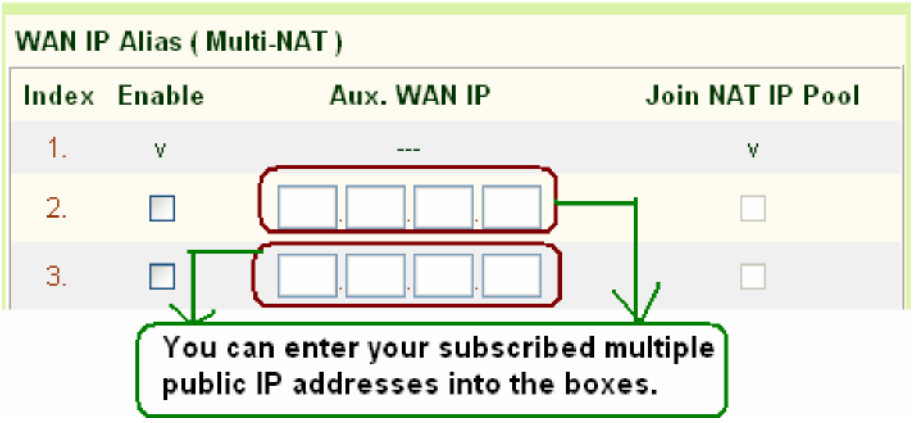
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

5.8 Nastavení funkce Multi-NAT

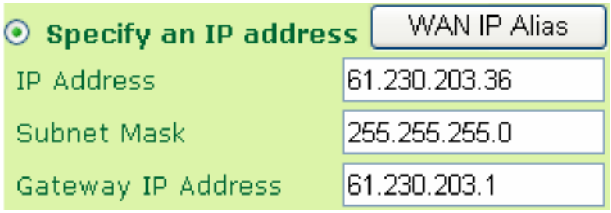
Systém překladu síťové adresy (NAT - Network Address Translation) zajišťuje převod mnoha vašich privátních IP adres na vaši jedinou veřejnou IP adresu. Ve většině případů budete funkci NAT směrovače používat pro širokopásmový přístup, tedy situaci kdy členové vaší rodiny mají každý svůj počítač, ale pouze jedno připojení k internetu (veřejnou IP adresu). Směrovač Vigor poté každému připojenému počítači nebo notebooku přiděluje privátní IP adresu. Funkce NAT zajišťuje důležitou bezpečnostní ochranu vašich síťových počítačů (klientů), protože jejich privátní IP adresa je skrytá před okolním světem a není přímo dosažitelná, pokud tuto funkci nepovolíte.

Funkci MultiNAT můžete použít v případě, kdy vám váš poskytovatel připojení přidělil více veřejných IP adres. Díky tomu může být mezi vaší privátní a veřejnou IP adresu vztah 1 - 1 (a nikoli Mnoho - 1, jako v případě 1 veřejné IP adresy) . To znamená, že jste stále chráněni systémem NAT, ale k jednotlivým počítačům vaší sítě se již lze připojit přímo zvenčí přes jejich veřejnou IP adresu (ovšem i zde je nutné otevřít pro toto připojení zvláštní porty - například Port 80 TCP pro http/web server).

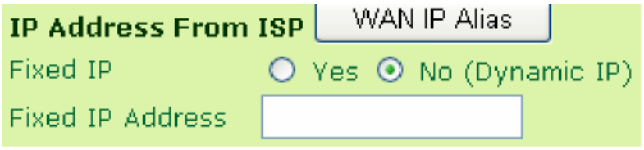
Pokud chcete využívat funkci MultiNAT, klikněte na tlačítko **WAN IP Alias**, které najdete na obrazovce **Nastavení přístupu k internetu (Internet Access Setup).**



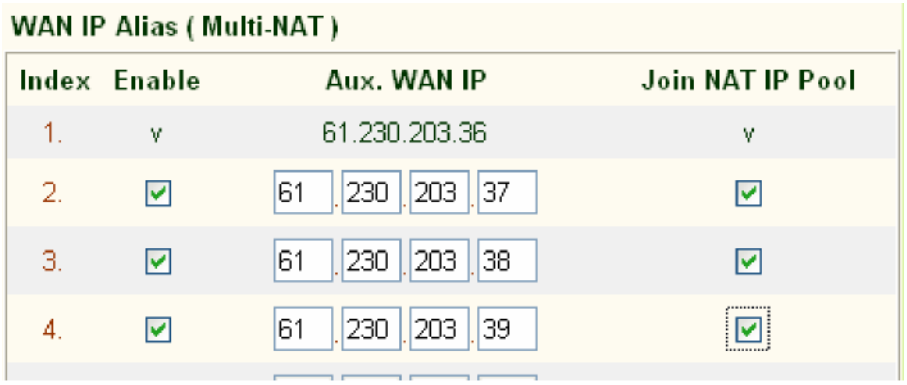
Pokud váš poskytovatel pracuje v režimu MPoA, proveďte nastavení v okně Internet Access>>MPoA:



Pokud váš poskytovatel pracuje v režimu PPPoE nebo PPPoA proveďte nastavení v okně **Internet Access>>PPPoE/PPPoA** :

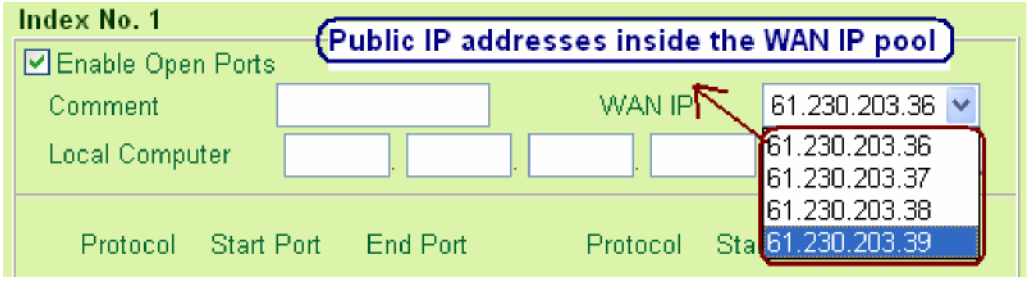


Po kliknutí na tlačítko **WAN IP Alias** se zobrazí okno pro nastavení veřejných IP adres, jak je ukázáno níže. Poté co do příslušných polí zadáte vaše veřejné IP adresy, zaškrtněte položku **Přidat do koše NAT IP adres** (**Join NAT IP Pool**), aby váš síťový klient mohl tyto veřejné adresy používat ke komunikaci s okolními počítači. Takto můžete například jeden počítač nadefinovat jako internetový server. Další veřejné IP adresy pak mohou používat například vaše děti pro online výuku přes internet.

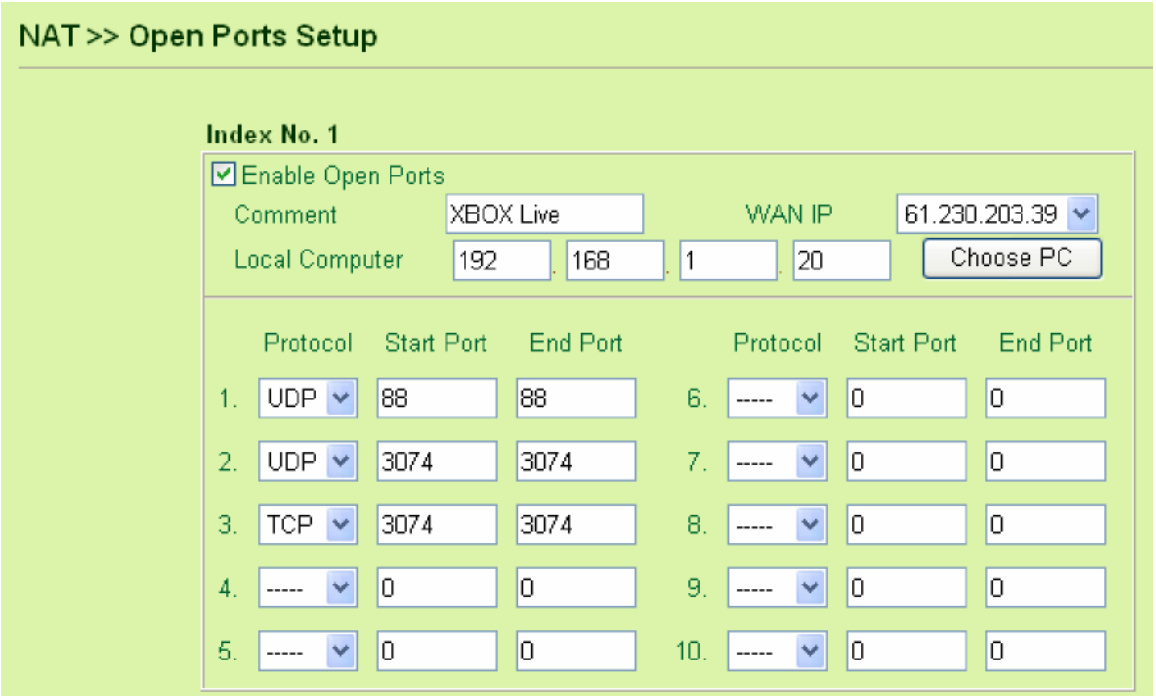


Po zadání vašich veřejných IP adres do oken **WAN IP Alias (Multi-NAT)**, bude možné pro tyto adresy specifikovat jednotlivá nastavení v oknech **NAT/Open ports** nebo **NAT/DMZ**.

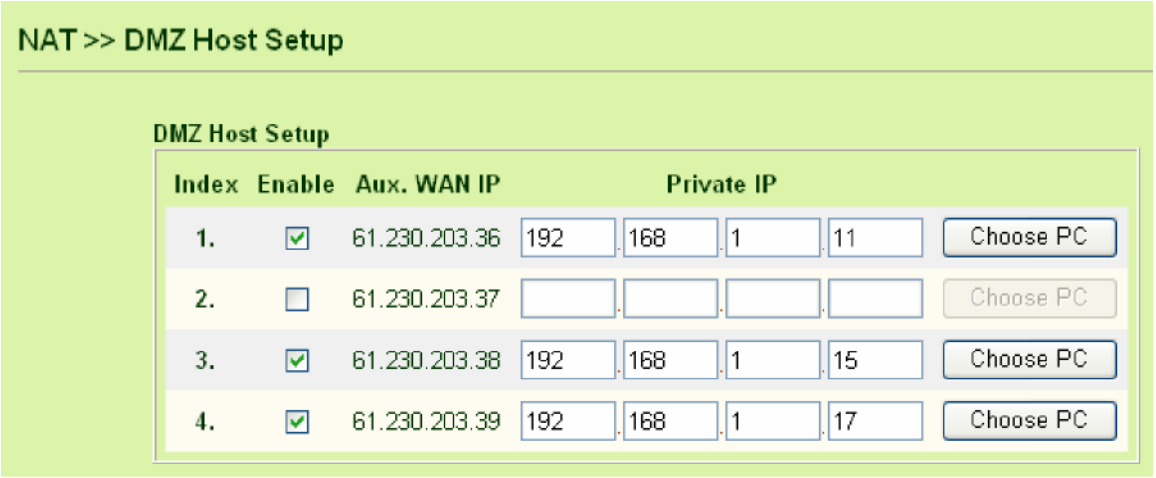
Poté co jsou vaše veřejné IP adresy uvedeny v koši NAT IP adres, můžete pro ně provádět jednotlivá nastavení v okně **NAT/Open Ports**. Můžete například určit jeden počítač pro připojení k XBox Live přes UDP a TCP porty:



Směrovače řady Vigor2500V by měli být kompatibilní s XBox Live. Pokud nebude standardní nastavení fungovat, můžete otevřít porty UDP 88 a 3074 a TCP 3074 pro přesměrování místní IP adresy Xboxu.
Na zvoleném počítači vaší sítě LAN zvolte jednu veřejnou IP (např. 61.230.203.39). Privátní IP adresa zvoleného počítače je 192.168.1.20. Po otevření portů UDP 88 a 3074 a TCP 3074 již směrovačem Vigor nebude zamezen přístup k aplikaci XBox Live.



Poté co jsou vaše veřejné IP adresy uvedeny v koši NAT IP adres, můžete pro ně provádět jednotlivá nastavení v okně **NAT/DMZ Ports**. Veřejnou IP adresu můžete přidělit počítači ve vaší síti LAN a nechat si všechny příchozí pakety přeposílat na počítač s místní IP adresu kterou jste nastavili. Například chcete, aby jste se s vaším počítač s privátní IP adresou IP 192.168.1.17 mohli připojovat ke službě Netmeeting. Tomuto počítači je také přidělena veřejná IP adresa 61.230.203.39. Po tomto nastavení již aplikace Netmeeting nebude blokována interním systémem zabezpečení NAT.



POZNÁMKA!
Interní zabezpečení funkce NAT je v případě používání funkce DMZ poněkud obcházeno. Proto zvažte možnost přidání dalších pravidel filtrování dat, či instalaci druhé brány firewall.
POZNÁMKA!
ADSL směrovače řady Vigor2500V je dodáván s již předinstalovanými bránami ALG (Application Level Gateways) pro lepší fungování multimediálních aplikací v rámci bezpečnostních systémů NAT. Brány ALG jsou již nastaveny od výrobce směrovače (DrayTek), takže na vašem směrovači Vigor již nemusíte provádět žádná další nastavení.

Kapitola 6
Firewall

6.1 Úvod

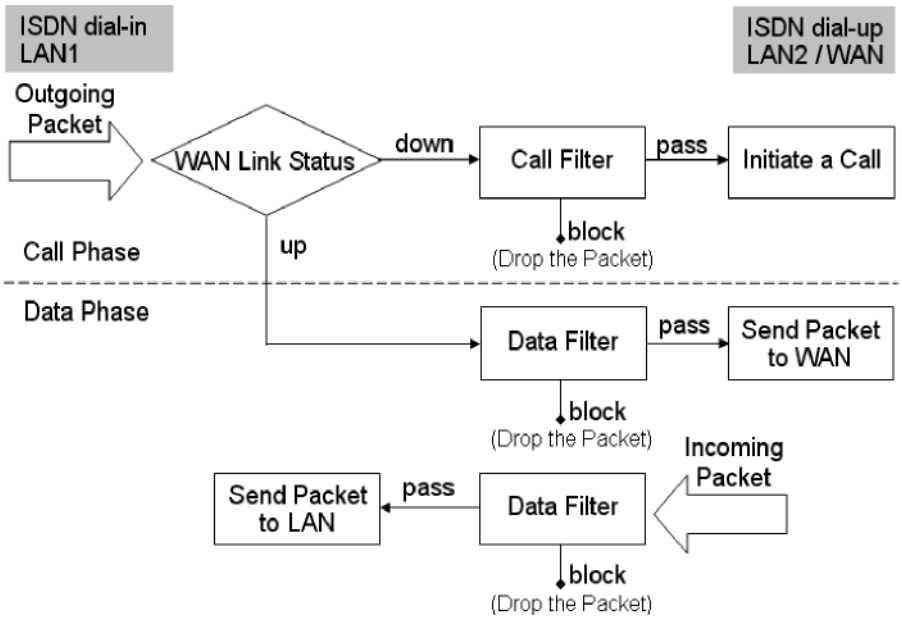
Bezpečnost je tou nejdůležitější prioritou, protože uživatelé širokopásmového připojení ADSL požadují větší přenosové kapacity pro multimédia, interaktivní aplikace a online výuku. Funkce Firewall umožňuje lépe chránit vaši místní síť před útoky zvenčí. Firewall také umožňuje omezit práva přístupu k internetu pro uživatele místní sítě.

Navíc tato funkce provádí analýzu paketů pro předcházení útokům na vaše sítě.
Uživatelé sítě LAN mohou využívat následující možnosti ochrany zajišťované bránou Firewall:
Analýza paketů: prohlížení paketů a zamezení přístupu pro nevyžádaná data
Volitelná ochrana proti útokům DoS/DDoS
Uživatelsky nastavitelný paketový filtr
Funkce NAT/PAT s funkcí přesměrování a DMZ
Podporuje ALGs (Application Layer Gateways)
Virtuální server pomocí funkce přesměrování portu nebo funkce otevření portu
Ochrana před nevyžádanou poštou

Poznámka: Pokud si chcete aktivovat funkci analýzy paketů (SPI - Stateful Packet Insepction), proveďte příslušná nastavení v nabídkách: Firewall>Edit Filter Rule.

6.2 Základní přehled funkcí brány Firewall

Pro bránu Firewall (**Firewall Setup**) vašeho směrovače Vigor můžete nastavit filtrování paketů, filtry pro ochranu před útoky DoS a filtry pro obsah internetových stránek (URL). V této kapitole se budeme zabývat představením funkce filtrování paketů. V **Přílohách A a B** se potom budeme podrobněji zabývat popisem ostatních filtrů, tedy ochranou proti útokům DoS a filtrováním obsahu internetových stránek.
IP filter / Firewall v sobě obsahuje dva typy filtrů: Call Filter (Filtr volání) a Data Filter (Filtr dat). Call Filter je navržen tak, aby blokoval, nebo přepouštěl IP pakety, na základě kterých směrovač spustí vnější spojení. Data Filter je navržen tak, aby blokoval, nebo přepouštěl definovaný druh IP paketů, které mají umožněn přechod přes směrovač, pokud je navázáno WAN spojení.
V zásadě, pokud je odcházející paket přesměrovaný do WAN, IP Filter rozhodne, zda má být přesměrován na Call Filter, nebo Data Filter. Pokud není navázáno WAN spojení, paket bude přesměrován na Call Filter. Jakmile daný paket nemá umožněno spustit směrovač, aby navázal vnější spojení, bude zrušen. V opačném případě bude inicializováno volání pro navázané WAN spojení. Jakmile WAN spojení je navázáno, bude paket v tomto případě přesměrován na Data Filter. Jakmile je paket v nastavení definován pro blokování, bude zrušen, případně současně přicházející paket přejde přes WAN rozhraní a prochází přímo Data Filtrem. Jakmile je paket v nastavení definován pro blokování, bude zrušen. V opačném případě bude poslán do vnitřní LAN. Schéma filtrů je zobrazeno níže.
.



Následující kapitoly popisují rozsáhlejší nastavení IP filtrů / Firewallu přes Web Configurátor. Je možné nastavit 12 skupin filtrů a pro každý jeden, 7 charakteristik. To je dohromady 84 filtrovacích předpisů pro IP Filtry / Firewall. V default nastavení je Call Filter definován ve Filtrovací skupině 1 a Data Filter ve filtrovací skupině 2. Nastavení můžete provést kliknutím na následující položky:

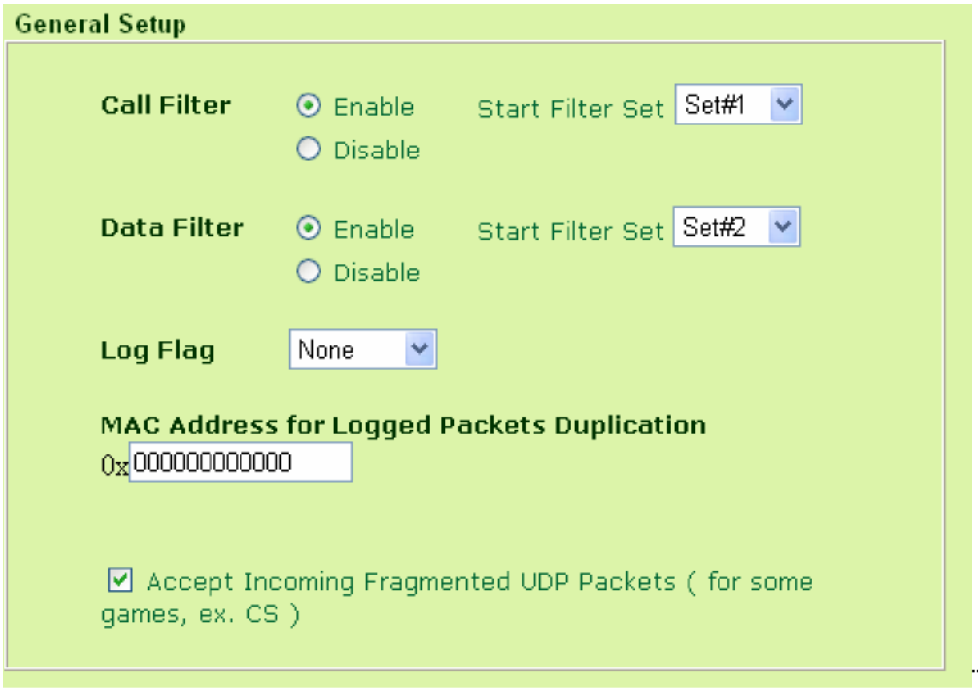
Firewall > **General Setup (Všeobecné nastavení)**
> **Filter Setup (Nastavení filtrů)**
> **DoS Defense (Ochrana proti DoS)**
> **URL Content Filter (Filtr obsahu webovských stránek - URL)**

Obecné nastavení: Zde můžete provést některá základní nastavení.
Nastavení filtru: Zde najdete 12 skupin IP filtrů.
Ochrana proti útokům DoS: Klikněte pro nastavení ochrany proti DoS (detekce a odrážení DoS útoků). Více podrobností najdete v Příloze A kapitoly 6.
Filtr obsahu webovských stránek - URL: Zde můžete zablokovat dětem přístup k nevhodným serverům. Více podrobností najdete v Příloze B kapitoly 6.

6.3 Všeobecné nastavení

Na stránce všeobecných nastavení můžete aktivovat / zablokovat Call Filter, nebo Data Filter a popsat startovací skupinu pro každou z nich. Můžete tu též konfigurovat přihlašovací nastavení a zadat MAC adresu pro duplikaci přihlašovaných paketů.

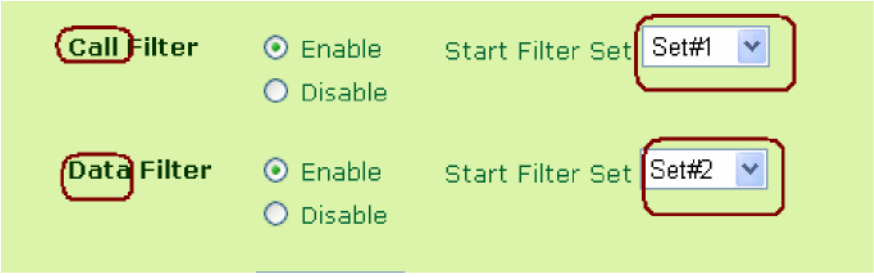
.



Call Filter (Filter volání): Volbu "**Enable**" (aktivovat) zvolíte možnost filtrování pro odeslané volby čísla, přičemž však musíte zvolit jeden počáteční filtr. Zaškrtnutím "**Disable**" (zablokovat) zakážete filtrování volání.
Data Filter (Filter dat): Volbu "**Enable**" (aktivovat) zvolíte možnost filtrování průtoku dat, přičemž musíte zvolit jeden počáteční filtr. Zaškrtnutím "**Disable**" (zablokovat) zakážete filtrování dat.
Log Flag (Indikace záznamu): Funkce vhodná pro servisní záznamy případných problémů.
• **None (žádné)**: Funkce zaznamenávání není aktivní.
• **Block (blokované)**: všechny blokované pakety budou zaznamenané.
• **Pass (propuštěné)**: všechny pakety, které projdou filtrem, budou zaznamenané.
• **No Match (bez pravidel)**: zaznamenají se všechny pakety, které neodpovídají pravidlům filtrování.
.
Poznámka : Filtrovací záznam se vám zobrazí v Telnetu, jakmile zadáte příkaz "log-f".
MAC Address for Packet Duplication (MAC adresa pro duplikaci paketů): Jestli chcete duplikovat některé zaznamenané pakety směrované ze směrovače na jiné vzdálené síťové zařízení, zapište do této položky MAC adresu zařízení v HEXa formátu. Pokud chcete zakázat "duplikaci paketů, pak do položky napište hodnotu "0"-nula (viz kapitola "Duplikace v LAN"). Funkce je velmi užitečná pro Ethernet zařízení.

6.4 Editing the Filter Sets (Nastavení skupin filtrů)

Comment: Zadejte název/popis skupiny filtrů. Maximální povolená délka je 23 znaků.
Filter Rule: Pravidlo filtru upravíte kliknutím na tlačítko **1 ~ 7**. **Aktivace (Active):** Zapnutí nebo vypnutí používání pravidla filtru.
Next Filter Set (následující sada filtrů): můžete přiřadit následující sadu filtrů do řetězce pravidel pro filtrování.
POZOR : Při řetězení filtrů nesmíte vytvořit uzavřenou smyčku.
Následující stránky uvádí standardní nastavení pro Call Filter a Data Filter, přičemž první je zadaný ve skupině filtrů (Filter Set) číslo 1 a druhý v skupině filtrů číslo 2.



6,5 Úprava pravidel filtrů (Editing the Filter Rules)

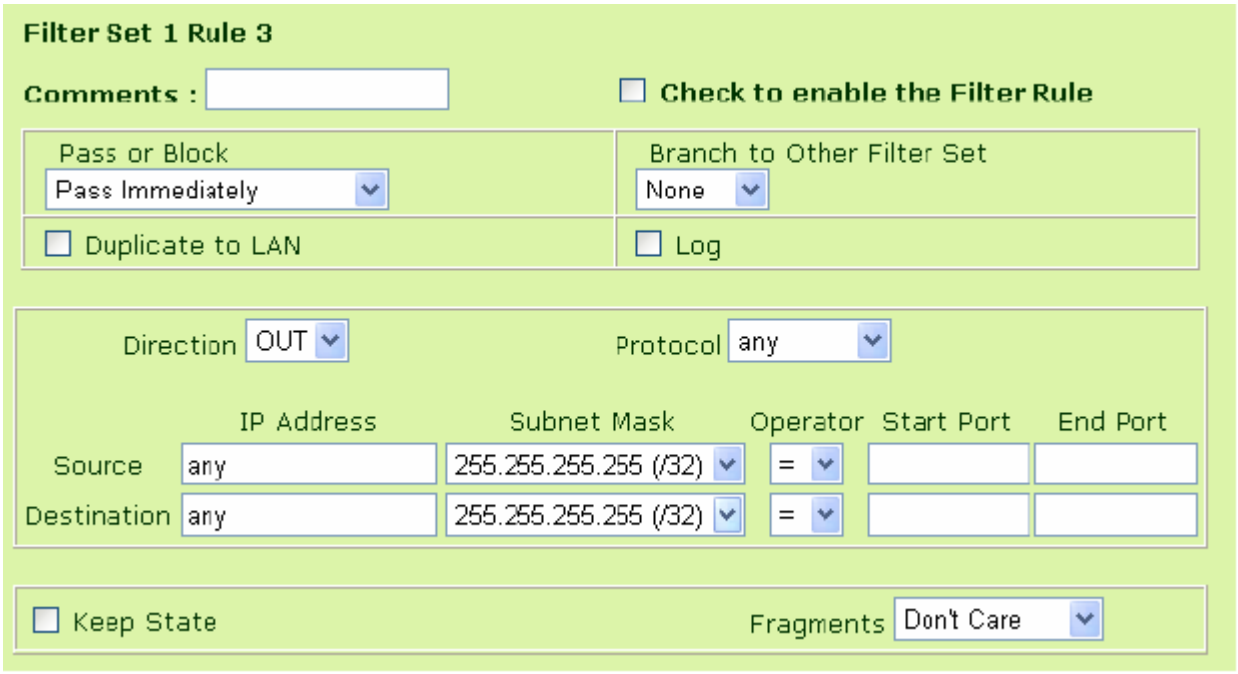
Klikněte na tlačítko Filter Rule a zobrazí se stránka nastavení příslušného filtru. Níže uvádíme podrobný přehled jednotlivých nastavitelných parametrů.

Comments (poznámky): tato kolonka je určená pro zápis poznámek, nebo popis pravidla. Maximální délka je 14 znaků.

Check to enable the Filter Rule (povolení pravidel filtrování): zaškrtnutím aktivujete pravidlo filtrování.

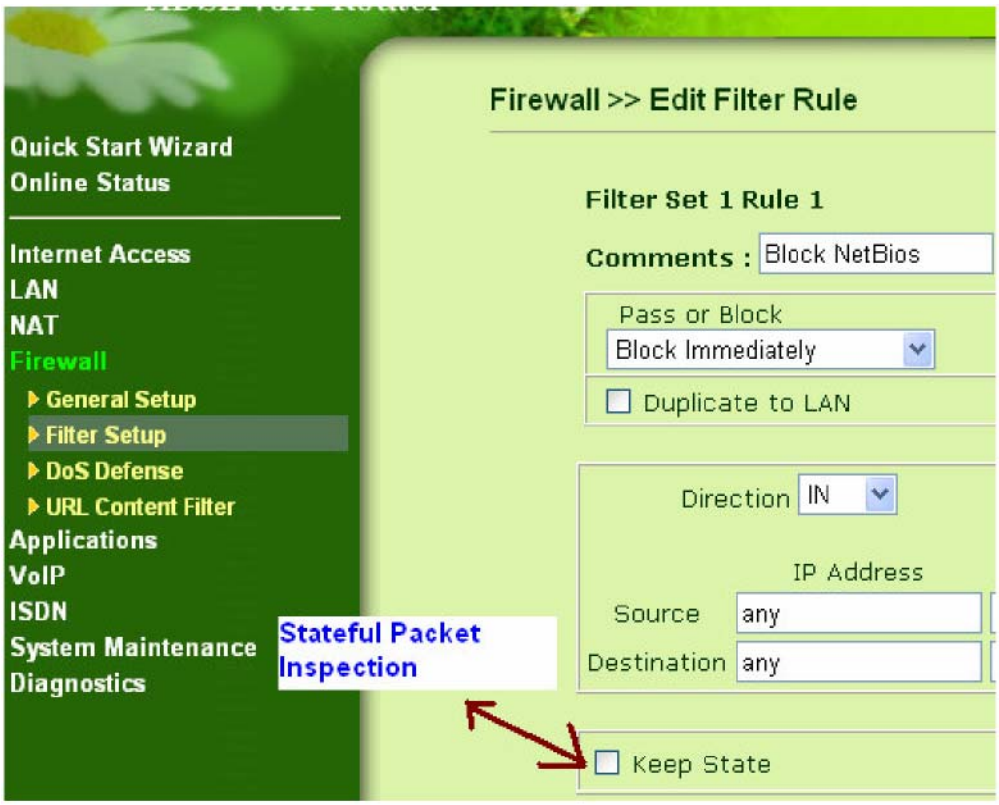
Pass or Block (propuštění nebo blokování): specifikujete následně vykonanou činnost v případě, že paket odpovídá pravidlu.

+ **Block Immediately** (blokuj okamžitě): paket odpovídající pravidlu bude okamžitě blokován.
+ **Pass Immediately** (propusť okamžitě): paket odpovídající pravidlu bude okamžitě propuštěn.
+ **Block if No Further Match** (blokuj, jakmile nevyhovuje dalším): paket, který sice vyhovuje danému pravidlu, ale nevyhovuje dalším, bude blokován.
+ **Pass If No Further Match** (propusť, jakmile nevyhovuje dalším): paket, který sice vyhovuje danému pravidlu, ale vyhovuje danému pravidlu, bude propuštěn.



Branch to Other Filter Set (nasměrování na další filtry): Pokud je paket propuštěn daným pravidlem filtrování, pak tato větev bude pokračovat na další sadu filtrů, definovanou v tomto poli. Tato filozofie konstrukce filtrů umožňuje definovat rozsáhlé a přitom velmi efektivní struktury podmínek pro filtrování.
Duplicate to LAN (duplikování do LAN): Pokud chcete propuštěné pakety duplikovat do některých dalších síťových zařízení (PC v LAN), zaškrtněte dané políčko. Fyzickou adresu síťového zařízení definujete v nabídce "**General Setup">>"MAC Address fot Logged Packets Duplication**". Tato funkce je užitečná pro tzv. off-host protokolizaci specifikovaných paketů využívající síťový sniffer.
Log (záznam): zaškrtnutím políčka zvolíte zaznamenávání do tzv. Log pole. Pro zobrazení záznamu v Telnetu zadejte příkaz "log-f". Příkazy pro Telnet najdete v kapitole 8.1 Používání terminálových příkazů pro Telnet.
Direction (směrování): pole pro výběr směrování paketů ve vztahu ke směrovači..
(Pro Call Filter je toto pravidlo irelevantní).

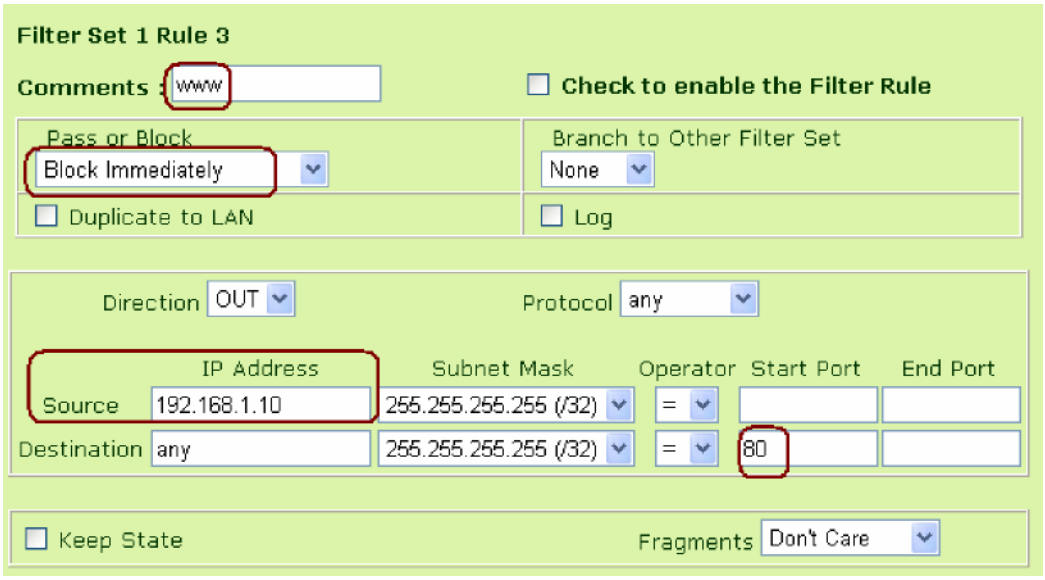
Pro Data Filter:
IN (příchozí): Značí pravidlo pro filtrování příchozích paketů.
OUT (odchozí): Značí pravidlo pro filtrování odchozích paketů.
Protokol (Protocol): Určuje protokoly, na které se toto filtrační pravidlo vztahuje.
IP Adresa: Určuje zdrojovou a cílovou IP adresu, na kterou se toto filtrační pravidlo vztahuje. Znak "!" před IP adresou znamená inverzi (NOT). V podstatě to znamená "ne z této adresy" nebo "ne na tuto adresu" podle směrování paketu.
Subnet Mask (Maska podsítě): Určuje masku podsítě pro danou IP adresu, na kterou se vztahuje dané filtrační pravidlo.
Operátor (logický operátor): položka specifikace čísla portu. Jakmile je položka "**Start Port**" (startovací port) prázdná, pak "**Start Port**" a "**End Port**" (cílový port) budou ignorovány. Pravidlo filtrování vyfiltruje každé číslo portu. V následující tabulce jsou popsány jednotlivé možnosti:
= Jakmile je pole "**End Port**" prázdné, potom je jeho hodnota shodná s hodnotou "**Start Port**". V ostatních případech jsou kontrolované hodnoty portů v rozsahu od "Start Port" do "End Port" vráceny.
! = Jakmile je pole "**End Port**" prázdné, pak je jeho hodnota shodná s hodnotou "**Start Port**". V ostatních případech jsou kontrolované hodnoty portů mimo rozsah definovaného v políčkách od "Start Port" po "End Port" vráceny.
> číslo portu je větší než hodnota v poli "**Start Port**" vrácena.
< číslo portu je menší než hodnota v poli "**Start Port**" vrácena.
Keep State (vezmi stav): zaškrtnutím políčka získáte informace o daném spojení v protokolu TCP/UDP/ICMP. V políčku "**Protocol**" musí být některý z protokolů zvolen. (TCP,UDP,TCP/UDP nebo ICMP)
.



Fragments (rozdělení): v nabídce specifikujte způsob rozdělení paketů na fragmenty.
+ **Do not Care** (nepodstatné): znamená žádné fragmentové podmínky v aplikaci pravidla.
+ **Unfragmented** (nerozdělené): použijte pravidlo filtrace na nefragmentované pakety.
+ **Fragmented** (rozdělené): použijte pravidlo filtrace na fragmentované pakety.
+ **Too Short** (velmi krátké): aplikuje pravidlo pouze na velmi krátké pakety, neobsahující hlavičku.

6.6 Ukázka nastavení pro omezení přístupu k Internetu

V tomto odstavci si ukážeme jednoduchý způsob jakým lze uživateli znemožnit přístup k Internetu. V tomto příkladu předpokládáme, že IP adresa uživatele, jemuž bude přístup k Internetu zakázán je 192.168.1.10 V rámci sady datových filtrů je vytvořeno pravidlo, kde Port 80 je číslo HTTP protokolu pro přístup ke službám www (viz. obrázek níže).


Filter Set 1 Rule 3
Comments : www
Check to enable the Filter Rule
Pass or Block
Block Immediately
Branch to Other Filter Set
None
Duplicate to LAN
Log
Direction OUT
Protocol any
IP Address
Subnet Mask
Operator
Start Port
End Port
Source 192.168.1.10 255.255.255.255 (/32) =
Destination any 255.255.255.255 (/32) = 80
Keep State
Fragments Don't Care

Příloha A
Ochrana před útokem "Denial of Service"

Útoky

A.1 Úvod

Funkce ochrany před útokem DoS umožňuje zachycení a odražení DoS útoků. Tyto útoky se dělí na tzv. zaplavující útoky a paralyzující útoky. Zaplavující útoky se snaží využít veškerou kapacitu vašeho systému, zatímco paralyzující útoky se snaží paralyzovat váš systém útokem na slabá místa vašeho protokolu nebo operačního systému.

A.2 Základní popis funkce ochrany před útokem DoS

Ochranný systém proti DoS útokům porovnává každý příchozí paket s databází podpisů útoků. Každý paket, který může paralyzovat bezpečnostní zónu je zablokován a klientovi je poslána systémová zpráva (syslog). Engine ochrany před útokem DoS také monitoruje provoz na síti. Při zjištění jakékoli abnormality, která porušuje administrátorské nastavení systému dojde k předání zprávy o problému a provede se příslušné obranné opatření pro odražení útoku.

A.3 Nastavení

Dále uvádíme podrobnější popis nastavení ochrany před útokem DoS pomocí webovského konfiguračního rozhraní (Web Configurator). Jedná se o doplňkovou ochranu k systému IP Filter/Firewall. Celkem je k dispozici 15 druhů obranných funkcí proti DoS. Standardně je funkce ochrany před útoky DoS vypnuta. Při zapnutí ochrany před útokem DoS budou prahové hodnoty počtu paketů a časový limit nastaveny na 300 paketů za vteřinu a 10 sekund. Níže uvádíme krátký popis jednotlivých položek funkce ochrany proti útokům DoS.

Enable DoS Defense - Zapnout ochranu před DoS útoky: Zaškrtnutím tohoto pole aktivujete ochranu před útoky DoS.

Enable SYN flood defense - Zapnout ochranu před zaplavovacím útokem SYN: Zaškrtnutím tohoto pole aktivujete ochranu před zaplavovacím útokem SYN. Pokud množství TCP SYN paketů z internetu překročí uživatelem nastavenou prahovou hodnotu nebo dobu, zablokuje směrovač Vigor další pakety TCP SYN. Hlavním smyslem je chránit směrovač Vigor proti TCP SYN paketům, které se pokouší plně využít jeho omezených kapacitních možností. Standardně jsou prahové hodnoty nastaveny na 300 paketů za sekundu a 10 sekund (časový limit).

Enable UDP flood defense - Zapnout ochranu před zaplavovacím útokem UDP: Zaškrtnutím tohoto pole aktivujete ochranu před zaplavovacím útokem UDP. Pokud množství UDP paketů z internetu překročí uživatelem nastavenou prahovou hodnotu nebo dobu, zablokuje směrovač za uživatelem nastavenou dobu další pakety UDP. Standardně jsou prahové hodnoty nastaveny na 300 paketů za sekundu a časový limit na 10 sekund.

Enable ICMP flood defense - Zapnout ochranu před zaplavovacím útokem ICMP: Zaškrtnutím tohoto pole aktivujete ochranu před zaplavovacím útokem ICMP. Stejně jako v případě ochrany před zaplavovacím útokem UDP, směrovač zablokuje všechny ICMP pakety z internetu při překročení nastavených prahových hodnot (standardně 300 paketů za sekundu) v nastaveném čase (standardně 10 sekund do odpojení).

Enable Port Scan - Zapnout detekci útoku typu Port Scan (skenování portu): Při útocích tohoto typu jsou pakety posílány na různá čísla portů s cílem zjistit, na které služby daný port bude odpovídat. Pokud chcete tyto útoky sledovat, zaškrtněte položku Enable Port Scan Detection. Směrovač Vigor bude monitorovat jednotlivé porty a rozešle varovnou hlášku v případě, že počet paketů přistupujících na port za sekundu překročí uživatelem nastavenou prahovou hodnotu. Standardně směrovač Vigor nastaví tuto prahovou hodnotu na 300 paketů za sekundu.

Enable Block IP options - Zapnout blokování volitelných IP polí : Tuto funkci aktivujete zaškrtnutím položky Block IP. Směrovač Vigor bude ignorovat IP pakety u nichž se volitelné IP pole objevilo v záhlaví datagramu. Volitelná IP pole umožňují hostitelskému počítači posílání důležitých informací, jako jsou bezpečnostní informace, kompartmentace, uživatelské skupiny TCC (uzavřená skupina uživatelů), internetové adresy, zprávy ze směrovače, apod., které mohou narušitelům poskytnout informace o vaší privátní síti.

Enable Block Land - Zapnout funkci Block Land: Pokud chcete blokovat tyto útoky, zaškrtněte příslušné pole. Směrovač eliminuje jakýkoliv nesprávný TCP paket, který obsahuje stejnou zdrojovou a cílovou IP adresu a zdrojové a cílové číslo portu jako ty, které byly vyslány ze SYN, zaznamenané v systému.

Enable Block Smurf - Zapnout ochranu proti útokům Block Smurf: Zaškrtnutím tohoto pole aktivujete funkci Block Smurf. Směrovač Vigor zablokuje všechny ICMP ozvěny určené vysílací adrese.

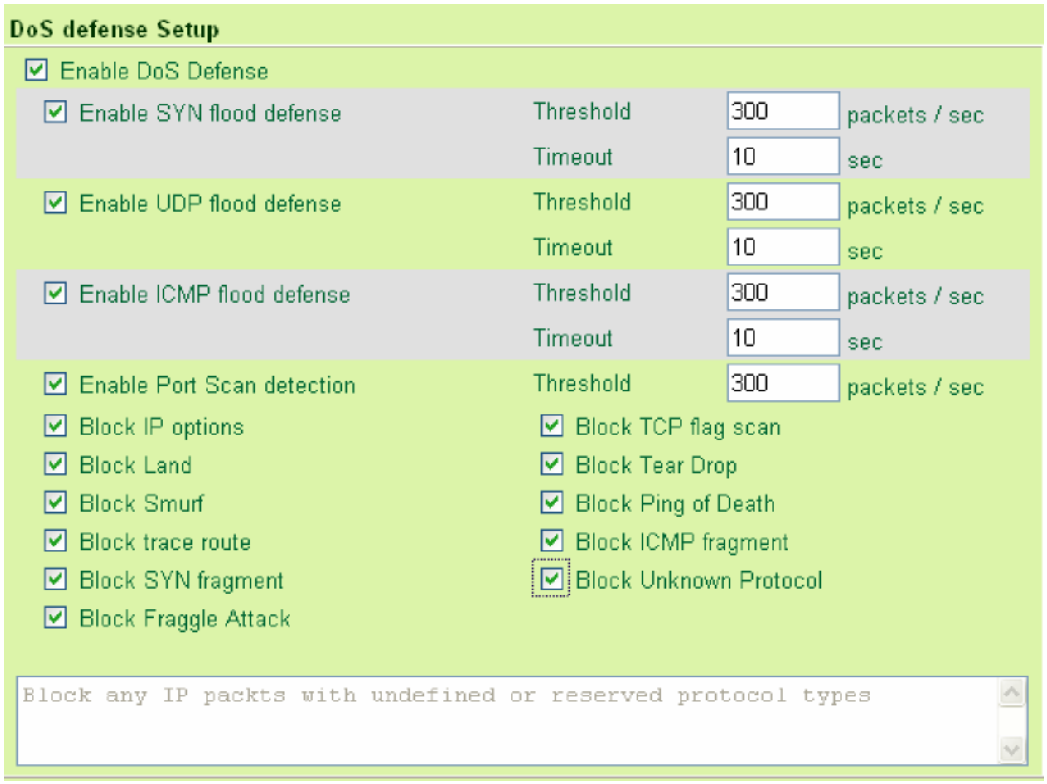
Enable Block trace route - Zapnout funkci blokování vyhledávací cesty: Tuto funkci aktivujte zaškrtnutím příslušného pole. Směrovač odmítne přeposlat jakýkoliv paket vyhledávající cestu.

.

Enable Block SYN fragment - Zapnout funkci blokování fragmentovaných SYN paketů: Zaškrtnutím tohoto pole aktivujete funkci Block SYN Fragment. Všechny fragmentované pakety s příznakem SYN budou zablokovány.

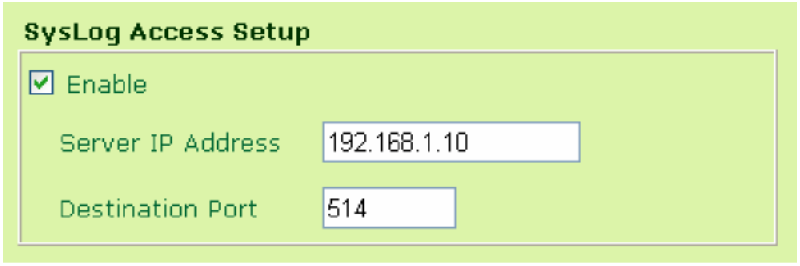
Enable Block fraggle Attack - Zapnout ochranu proti útokům fraggle: Zaškrtnutím tohoto pole aktivujete ochranu před útoky typu fraggle. Všechny UDP pakety přijaté z internetu budou zablokovány.

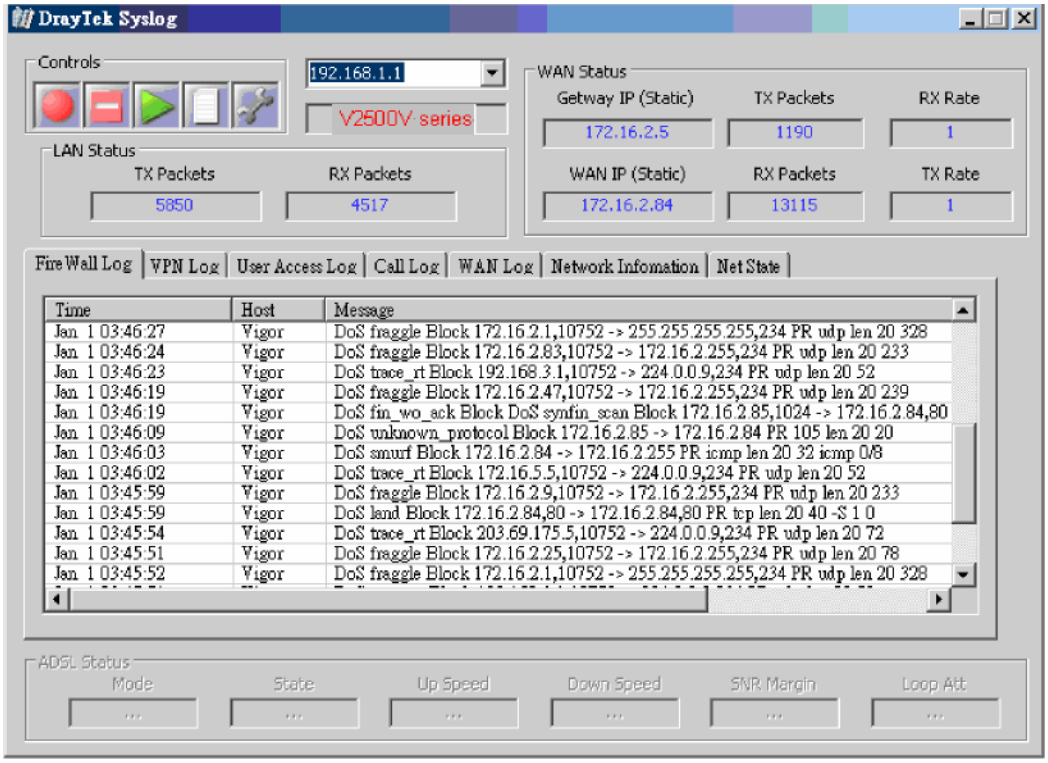
Enable TCP flag scan - Zapnout skenování příznaku TCP: Zaškrtnutím tohoto pole aktivujete funkci skenování příznaku TCP. Jakýkoli TCP paket s nepřiměřeným nastavením signálu bude zrušen. Tento přehled v sobě zahrnuje: žádné skenování signálu, FIN bez ACK skenu, SYN FIN sken, Xmas sken a plný Xmas sken.
Enable Tear Drop: Zaškrtněte příslušné pole pro aktivaci této funkce. Mnoho strojů se může zhroutit po vyslání IP paketu přesahující maximální povolenou délku. Jakýkoliv fragmentovaný paket delší než 1024 oktetů bude vyhozen.
Enable Ping of Death (aktivace smrtícího pingu): Zaškrtněte příslušné pole pro aktivaci této funkce. Tento útok se týká toho, že pachatel vysílá cíli přesahující pakety, stroj se je pokusí rekonstruovat a cílový stroj je vyřazen z provozu. Jakýkoliv paket s těmito znaky je zrušen.
Enable Block ICMP fragment (blokování fragmentovaných ICMP paketů): Zaškrtněte příslušní pole pro aktivaci této funkce. Jakýkoli ICMP paket s větším počtem sad fragmentovaných bitů bude zrušen.
Enable Block Unknown Protocol (blokování neznámého protokolu): Zaškrtněte příslušné pole pro aktivaci této funkce. IP paket má v hlavičce indikovanou vrchní protokolovou vrstvu. Hodnota protokolu vyšší než 100 není standardně definovaná, proto budou tyto pakety vyhozeny.
.



A.4 Varovací zprvány

Všechny varovací zprávy jsou zasílány syslog klientovi, pokud je funkce syslog aktivní. Administrátor může nastavit syslog klienta v položce **System Maintenance >> Syslog Setup / Mail Alert** (nastavení syslog). Též je možné sledovat varovací zprávy přicházející od DoS ochrany přes DrayTek Syslog daemona. Formát zprávy je velmi podobný zprávám o IP filtrech/Firewallu, až na začátek s klíčovým slůvkem "DoS" a následujícím názvem o jaký druh útoku jde.




DrayTek Syslog
Controls
192.168.1.1
V2500V series
LAN Status
TX Packets
RX Packets
5850
4517
WAN Status
Getway IP (Static)
TX Packets
RX Rate
172.16.2.5
1190
1
WAN IP (Static)
RX Packets
TX Rate
172.16.2.84
13115
1
Fire Wall Log
VPN Log
User Access Log
Call Log
WAN Log
Network Infomation
Net State
Time
Host
Message
Jan 1 03:46:27 Vigor DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328
Jan 1 03:46:24 Vigor DoS fraggle Block 172.16.2.83,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:46:23 Vigor DoS trace_rt Block 192.168.3.1,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:46:19 Vigor DoS fraggle Block 172.16.2.47,10752 -> 172.16.2.255,234 PR udp len 20 239
Jan 1 03:46:19 Vigor DoS fin_wo_ack Block DoS synfin_scan Block 172.16.2.85,1024 -> 172.16.2.84,80
Jan 1 03:46:09 Vigor DoS unknown_protocol Block 172.16.2.85 -> 172.16.2.84 PR 105 len 20 20
Jan 1 03:46:03 Vigor DoS smurf Block 172.16.2.84 -> 172.16.2.255 PR icmp len 20 32 icmp 0/8
Jan 1 03:46:02 Vigor DoS trace_rt Block 172.16.5.5,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:45:59 Vigor DoS fraggle Block 172.16.2.9,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:45:59 Vigor DoS land Block 172.16.2.84,80 -> 172.16.2.84,80 PR tcp len 20 40 -S 1 0
Jan 1 03:45:54 Vigor DoS trace_rt Block 203.69.175.5,10752 -> 224.0.0.9,234 PR udp len 20 72
Jan 1 03:45:51 Vigor DoS fraggle Block 172.16.2.25,10752 -> 172.16.2.255,234 PR udp len 20 78
Jan 1 03:45:52 Vigor DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328
ADSL Status
Mode
State
Up Speed
Down Speed
SNR Margin
Loop Att

Příloha B
Filtrování obsahu webovských stránek

B.1 Úvod

Na internetu je k dispozici celá řada materiálu, který v některých zemích může být považován za urážlivý, či dokonce přímo zakázán. Na rozdíl od tradičních médií nemá samotný internet žádný běžný nástroj pro dělení jednotlivých materiálů na základě URL adresy, či obsahu. Systémy pro filtrování obsahu webovských stránek představují nástroj, který plní funkci fyzického rozdělení obsahu stránek a umožňuje nastavení omezení přístupu k některým druhům materiálu. Pokud je obsah stránek vyhodnocen jako urážlivý nebo nevhodný, filtr zabrání zobrazení takové www stránky na obrazovce uživatele, což mohou využít například rodiče, pokud chtějí dětem zabránit v přístupu k pro ně nevhodnému obsahu. Blokování zobrazení nevhodných www stránek plní tedy stejnou funkci, jako prodejce časopisů, který odmítne prodat pornografický časopis žákům střední školy. Filtr obsahu www stránek také využívají firmy pro omezení přístupu svých zaměstnanců k obsahu, který nesouvisí s jejich pracovní náplní, nebo je pro ně jinak nevhodný.
URL filtr (filtr webovských stránek) kontroluje obsah znakového řetězce URL adresy. Běžná brána Firewall třídí pakety na základě informace uvedené v záhlaví protokolů TCP/IP, zatímco URL filtr kontroluje řetězce URL adresy nebo velikost TCP/IP paketů. Směrovače Vigor nabízí jednak funkci prohledávání řetězce URL adresy a jedak vyhledávají některá HTTP data, skrytá v TCP paketech.

B.2 Základní informace o filtrování obsahu

Obsahový filtr širokopásmového směrovače Vigor kontroluje každý řetězec URL a porovnává jej se seznamem klíčových slov. Pokud určitá část řetězce nebo celý řetězec URL adresy odpovídá aktivovanému klíčovému slovu (jako například http://www.draytek.com výše), zablokuje směrovač Vigor otevření příslušné www stránky a automaticky zašle syslog zprávu syslog klientovi. Rovněž všechny stránky, které se pokouší do počítače nasadit nebezpečný program, budou směrovačem Vigor zablokována. Stejně jako v předchozím případě bude otevření těchto stránek zablokováno a bude odeslána syslog zpráva klientovi.
Obsahový filtr URL brání uživatelům v přístupu k nebezpečeným či nevhodným stránkám, na základě porovnání řetězce URL se zakázanými klíčovými slovy.
Aby tato funkce fungovala správně, musíte nejprve odstranit všechny soubory cookie, vyprázdnit veškerý obsah off-line a smazat historii ve vašem prohlížeči.

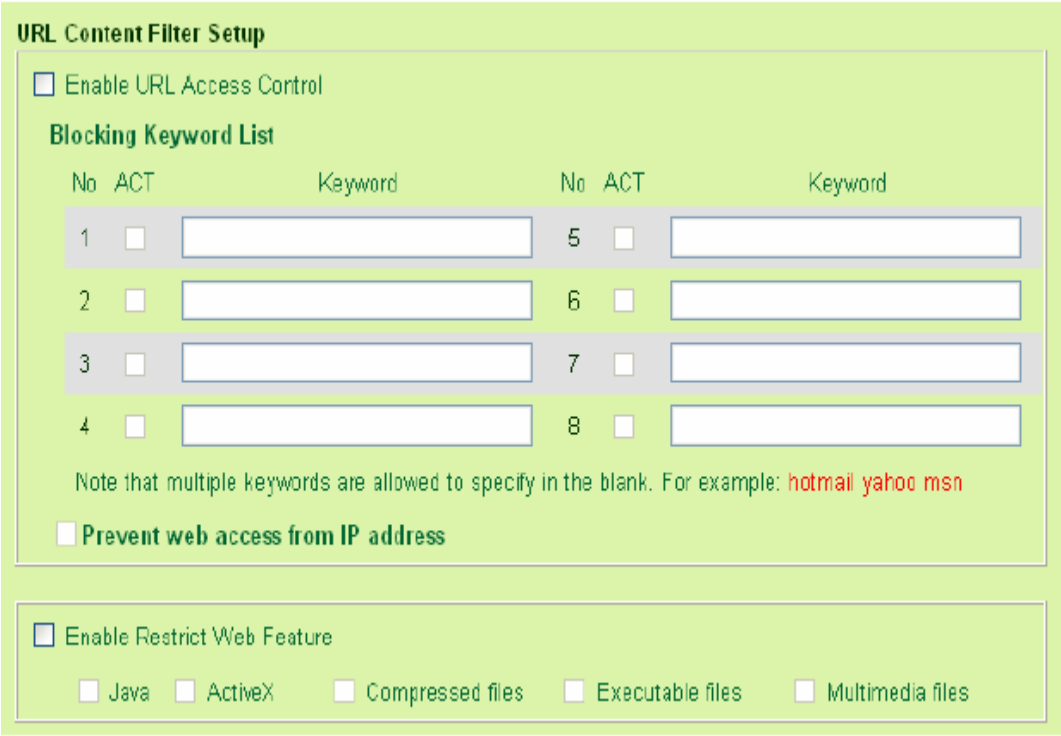
B.3 Nastavení

V následujících odstavcích popisujeme nastavení filtrování URL, včetně zvláštností a omezení této funkce. Nastavení URL filtru se provádí z hlavní nabídky kliknutím na položku **Firewall**.

Směrovač Vigor nabízí následující funkce pro filtrování obsahu: ***URL Access Control (řízení přístupu k www stránkám - URL), Prevent web access from IP address (zakázat IP adresu), Restrict Web Feature control (blokování nebezpečných kódů) , Exceptional Subnet handling (výjimky),*** a ***Time schedule (časové období)***. Funkce *URL Access Control* řídí přístup k webovským stránkám porovnáváním jejich řetězce se seznamem zakázaných klíčových slov. Funkce *Restrict Web Feature control* blokuje zlé kódy a programy schované v internetových stránkách, jako jsou aplety *Java,* prvky *Active X, Cookies, Proxy, komprimované* a *spustitelné* soubory. Filtry směrovače Vigor také umožňují blokování stahování *multimediálních* souborů z internetových stránek, aby nedocházelo k přetěžování připojení.

Funkce *Prevent web access from IP address* se používá pro blokování stránek, na které je možno se dostat zadáním URL adresy do okna prohlížeče, přestože obsahují uživatelem nadefinovaná klíčová slova v URL řetězci. Funkce *Exceptional Subnet handling* umožňuje správci sítě definovat skupinu uživatelů, na něž se nebude blokování nastavené v *URL Access Control* vztahovat. Skupinu těchto uživatelů můžete definovat pomocí skupiny

IP adres, nebo podsítí. A konečně směrovač Vigor umožňuje nastavení časového období, ve kterém se mají pravidla filtrování obsahu uplatňovat (funkce *Time schedule*). Nyní si popíšeme jednotlivé položky podrobněji.



Zapnout funkci URL Access Control: Tuto funkci zapněte zaškrtnutím pole *URL Access Control*. Zaškrtněte pole ACT a zadejte klíčové slovo do pole Keyword. Váš směrovač Vigor poté automaticky zablokuje přístup ke stránkám, jejichž URL adresa obsahuje řetězec některého z vybraných klíčových slov. Například při zadání blokování slova "sex" bude uživateli směrovačem Vigor znemožněn přístup ke stránce www.backdoor.net/images/sex_/p_386.html, protože adresa obsahuje zakázané slovo. Uživatel ovšem může navštívit stránky www.backdoor.net/firewall/forum/d_123.html. Do polí pro klíčová slova můžete zadat i celou URL adresu (např. "www.whitehouse.com" a "www.hotmail.com") nebo neúplnou URL adresu (např. "yahoo.com"). Tyto adresy poté budou blokovány. Směrovač Vigor automaticky identifikuje daný URL řetězec a zablokuje přístup k příslušným stránkám.

Prevent Web Access by IP Address: Zaškrtnutím tohoto pole bude blokován přístup pro položky, které využívají přímo IP adresy. Zaškrtněte příslušné pole a proveďte příslušná nastavení.
Pokud objekt Active X obsahuje nebezpečný kód, může způsobit otevření vašeho systému pro případné útoky.
Java: Zaškrtnutím tohoto pole aktivujete funkci Block Java (blokování objektů Java). Směrovač Vigor automaticky zablokuje Java objekty z internetu.
ActiveX: Zaškrtnutím tohoto pole aktivujete funkci Block Active X (blokování prvků Actie X). Všechny prvky Active X z internetu budou zablokovány.
Compressed file: Zaškrtnutím tohoto pole bude zablokováno stahování komprimovaných souborů. Směrovač Vigor podporuje blokování níže uvedených formátů komprimovaných souborů.

.zip .rar .arj .ace .cab .sit

Zaškrtněte příslušné pole.

Executable file: Stejně jako u výše uvedené funkce bude po zaškrtnutí této položky znemožněno stahování spustitelných souborů z internetu. Zaškrtněte příslušné pole. Směrovač Vigor bude blokovat soubory s následujícími příponami.

.exe .com .scr .pif .bas .bat .inf .reg

Tzv. *cookies* které vynalezla firma Netscape umožňují serverům podrobně sledovat pohyb uživatelů na stránkách. Mnoho serverů tuto funkci využívá

pro vytváření sledování pohybu uživatelů jejich webovských stránek, což může ohrozit soukromí uživatelů. Proto směrovače Vigor nabízí funkci pro filtrování *Cookies* , která tyto prográmky blokuje. Pro ještě vyšší úroveň zabezpečení vám směrovač Vigor umožňuje také zablokovat proxy přenosy.

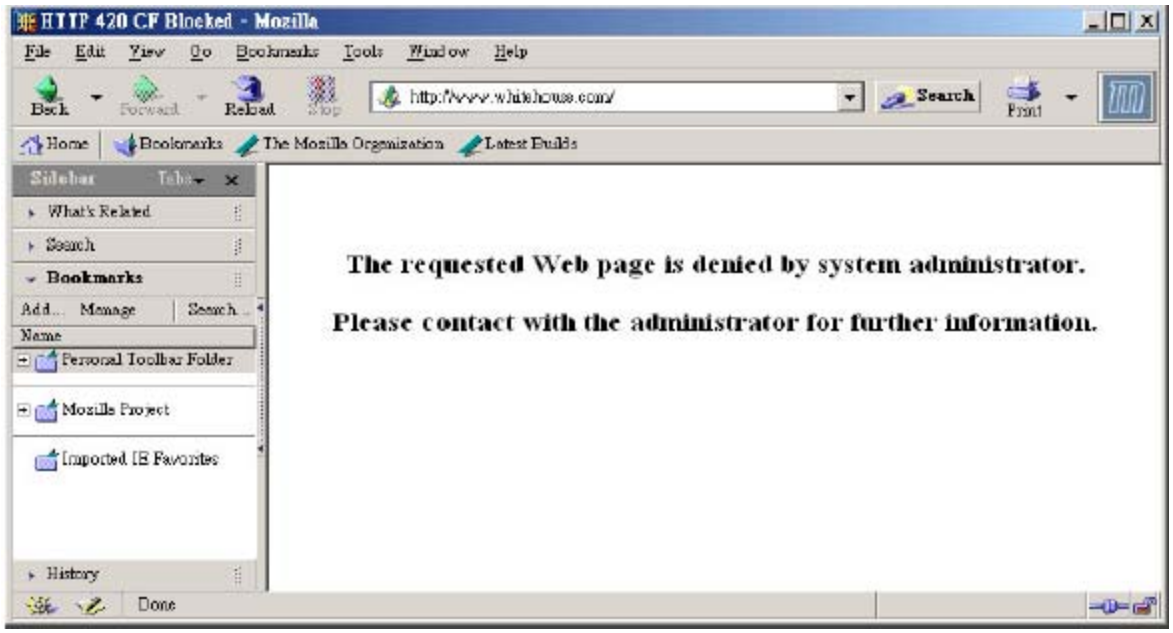
Cookie: Zaškrtnutím tohoto pole aktivujete funkci Block Cookie (blokování Cookie). Směrovače zablokuje všechny soubory Cookie přicházející ze sítě.
Proxy: Funkci aktivujete zaškrtnutím příslušné položky. Zaškrtněte příslušné pole.

Pro omezení přetěžování přípojky nabízí směrovač Vigor užitečnou funkci pro blokování stahování multimediálních souborů z internetu. Zaškrtněte příslušné pole. Směrovač Vigor bude blokovat soubory s následujícími příponami.

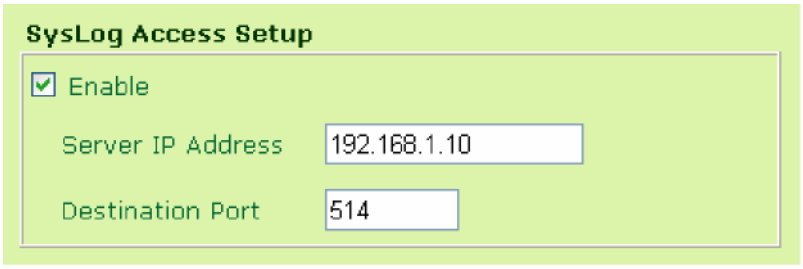
.mov .mp3 .rm .ra .au .wmv
.wav .asf .mpg .mpeg .avi .ram

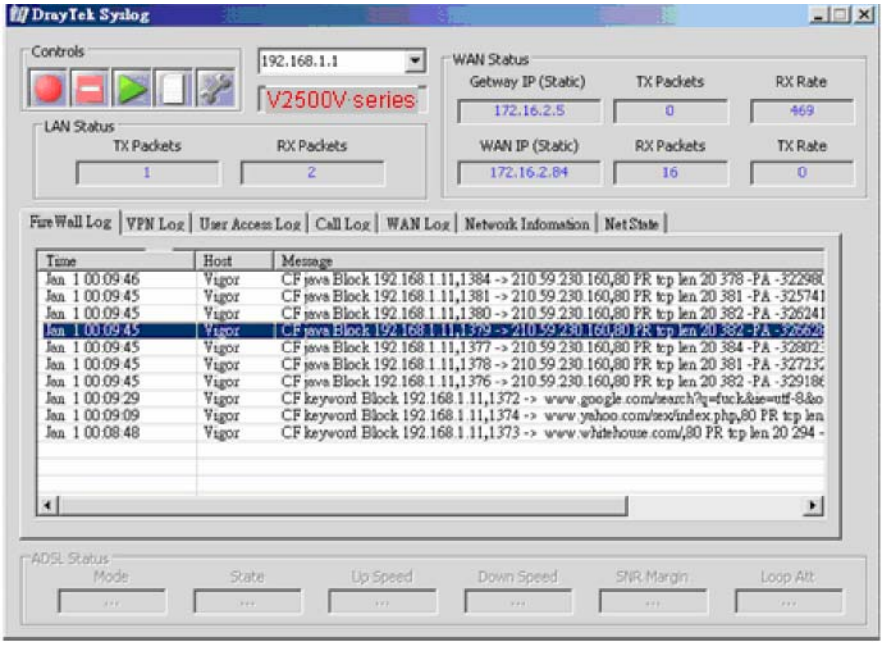
Time Schedule (časové období): Tato funkce umožňuje nastavit období, ve kterém budou filtry obsahu aktivní. (pouze u modelů firmware 2.5.6 a vyšších)
Always Block (vždy blokovat)*:* Zaškrtnutím tohoto pole budou nastavená pravidla blokování obsahu používána stále.
Block from H1:M1 To H2:M2 (blokovat od - do): Nastavte hodinu a minutu počátku a konce blokování v jednom dni. *H1* a *H2* představují hodiny. *M1* a *M2* představují minuty.
Days of Week (dnyv týdnu): Zadejte dny, ve kterých bude směrovač Vigor blokovat obsah, podle vašich nastavení. Směrovač Vigor nabízí dvě nastavení (buď blokování každý den, nebo ve vybraných dnech týdne). Pokud chcete, aby funkce blokování obsahu URL byla aktivní po celý týden, zaškrtněte pole "**Everyday - Každý den**". V opačném případě vyberte příslušné dny. Pokud například chcete, aby blokování obsahu bylo zapnuto od pondělí do středy, zaškrtněte příslušné dny (Monday - Tuesday - Wednesday (Po - Út - St)). V ostatních dnech nebude blokování obsahu aktivní.

B.4 Varovná zpráva



Pokud se uživatel pokusí přistoupit k zakázanému obsahu, zobrazí se mu níže uvedená obrazovka.
Rovněž bude zaslána varovná syslog zpráva syslog klientovi (pokud jste tuto možnost vybrali). Nastavení syslog klienta se provádí v nabídce **Syslog Setup** prostřednictvím webovského konfigurátoru (Web Configurator). Pokud je zasílání těchto zpráv nastaveno, může správce sítě sledovat varovné zprávy prostřednictvím syslog daemona firmy DrayTek. Formát těchto zpráv je stejný jako v případě zpráv v sekci **Firewall** s tím rozdílem, že se v záhlaví zprávy objevuje předpona **"CF"** s názvem blokované adresy.


SysLog Access Setup
Enable
Server IP Address
192.168.1.10
Destination Port
514


DrayTek Syslog
Controls
192.168.1.1
V2500V series
LAN Status
TX Packets
RX Packets
1
2
WAN Status
Getway IP (Static)
TX Packets
RX Rate
172.16.2.5
0
469
WAN IP (Static)
RX Packets
TX Rate
172.16.2.84
16
0
Fire Wall Log
VPN Log
User Access Log
Call Log
WAN Log
Network Infomation
Net State
Time
Host
Message
Jan 1 00:09:46 Vigor CF java Block 192.168.1.11,1384 -> 210.59.230.160,80 PR tcp len 20 378 -PA -322968
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1381 -> 210.59.230.160,80 PR tcp len 20 381 -PA -325741
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1380 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326241
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1379 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326628
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1377 -> 210.59.230.160,80 PR tcp len 20 384 -PA -328023
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1378 -> 210.59.230.160,80 PR tcp len 20 381 -PA -327232
Jan 1 00:09:45 Vigor CF java Block 192.168.1.11,1376 -> 210.59.230.160,80 PR tcp len 20 382 -PA -329186
Jan 1 00:09:29 Vigor CF keyword Block 192.168.1.11,1372 -> www.google.com/search?q=fuck&ie=utf-8&o
Jan 1 00:09:09 Vigor CF keyword Block 192.168.1.11,1374 -> www.yahoo.com/sex/index.php,80 PR tcp len
Jan 1 00:08:48 Vigor CF keyword Block 192.168.1.11,1373 -> www.whitehouse.com/,80 PR tcp len 20 294 -
ADSL Status
Mode
State
Up Speed
Down Speed
SNR Margin
Loop Att

Kapitola 7
Dynamické DNS

7.1 Úvod

Váš poskytovatel připojení vám často přidělí tzv. dynamickou generovanou IP adresu. To znamená, že váš směrvoač používá pro každé připojení k vašemu poskytovateli jinou veřejnou IP adresu (dynamicky generovanou z "volných" adres doménového koše). Vzdálení uživatelé tedy pro připojení k vaší internetové prezentaci nemohou zjistit IP adresu vašeho místního serveru.

Funkce dynamické DNS (Dynamic DNS) umožňuje vzdáleným uživatelům přístup do vaší sítě prostřednictvím tzv. registrované WAN IP adresy (například hostnmae.dyndns.org) kterou přidělují poskytovatelé dynamických DNS adres. Funkce Dynamic DNS tedy směrovači umožňuje aktualizovat svoji online WAN IP adresu, přidělenou poskytovatelem připojení uvedenému dynamickému DNS serveru. Po navázání spojení tak budete moci, pomocí této adresy, přistupovat k vašemu směrovači nebo interním virtuálním serverům přímo z internetu.

Použijeme-li příměru ze života, lze službu Dynamic DNS můžete nastavit jako **pošťáka** a registrovanou WAN IP adresu (např. **hostnmae.dyndns.org)** jako **číslo vaší poštovní schránky** vašeho pronajatého domu. Vaši přátelé vám pak budou moci kdykoli zasílat balíky (pakety) i tehdy, měníte-li často váš pronajatý dům.

Než začnete používat funkci Dynamic DNS, musíte si zaregistrovat nějaké volné doménové jméno u poskytovatelů DNS služeb. Na směrovači můžete nastavit až 3 účty pro 3 různé DNS služby. Směrovače Vigor jsou kompatibilní se systémy nejpopulárnějších poskytovatelům služeb Dynamic DNS, jako jsou například **www.dynsns.org**, **www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** Navštivte jejich internetové stránky a zaregistrujte si vlastní doménové jméno pro váš směrovač.

7.2 Nastavení

Enable the Function and Add a Dynamic DNS Account (Zapnout funkci Dynamic DNS a přidat účet dynamické DNS)

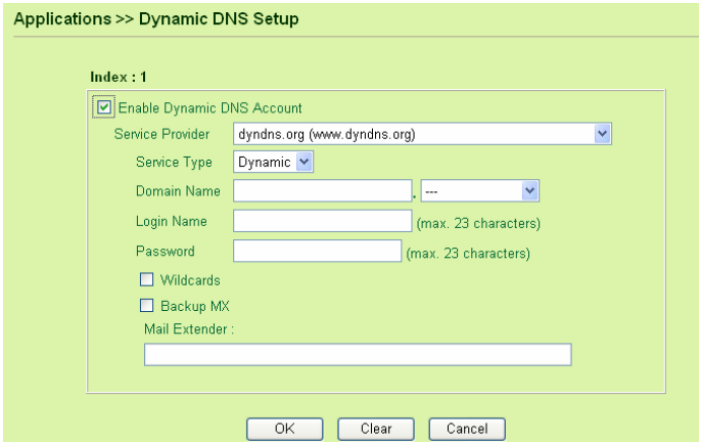
1. Předpokládejme, že jste si u vašeho poskytovatele služeb Dynamic DNS (DDNS) ***hostname.dyndns.org*** zaregistrovali účet s uživatelským jménem: ***test*** a heslem: ***test.***
2. Jděte do nabídky **Applications > Dynamic DNS**

   Zaškrtněte položku **Enable Dynamic DNS Account - Zapnout účet Dynamic DNS** a vyberte vašeho poskytovatele služby (**Service Provider**)**:** **dyndns.org** . Do pole **Domain name** (název domény) zadejte vaše registrované jméno: ***hostname*** a příponu doménového jména: **dyndns.org**. Do pole přihlašovací jméno (**Login Name**) zadejte ***test*** a do pole heslo (**Password**) zadejte ***test.***

   Klikněte na tlačítko **OK** pro aktivaci nastavení.

POZNÁMKA!

Funkce **Wildcard (divoká karta)** a **Backup MX** nejsou podporovány všemi poskytovateli služby Dynamic DNS. Přečtěte si pozorně pokyny vašeho poskytovatele služby Dynamic DNS.



Disable the Function and Clear all Dynamic DNS Accounts - Vypnutí funkce Dynamic DNS a vymazání všech účtů Dynamic DNS

1. Jděte do nabídky **Applications > Dynamic DNS**
2. Zrušte zaškrtnutí pole **Enable Dynamic DNS Setup,** a klikněte na tlačítko **Clear All** (Smazat vše).

Smazání účtu Dynamic DNS

1. Jděte do nabídky **Applications > Dynamic DNS**
2. Klikněte na číslo položky (**Index)**, kterou chcete smazat a klikněte na tlačítko **Clear All** (smazat vše).

7.3 Ověření a řešení problémů

Prozvonění registrovaného doménového jména

1. Po navázání spojení použijte utilitu **PING (Prozvonění)** pro prozvonění vašeho doménového jména a ověření jeho fungování.
2. Přejděte na obrazovku **Online Status (online stav)** a přesvědčte se, že IP adresa z dynamického DNS serveru je stejná jako WAN IP adresa směrovače.

Prohlížení log souborů poskytovatelem DDNS (Dynamic DNS)

Pomocí Telnet rozhraní vašeho směrovače si můžete prohlédnout aktuální stav vaší služby (ve Windows spusťte program telnet.exe). Příkazem ***ddns log*** vyvoláte informace o výsledku připojení. Níže uvádíme příklad pro poskytovatele dyndns.org:

1. Jděte do nabídky **Applications > Dynamic DNS**
2. Klikněte na tlačítko **View Log**. Zobrazí se následující informace z DDNS.

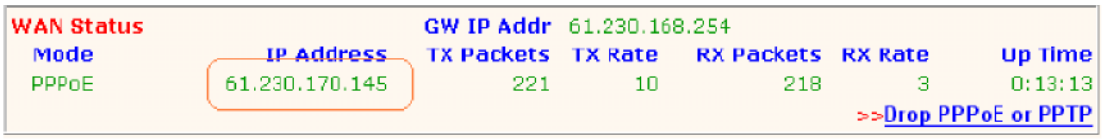
>ddns log
###1 DDNS is updating… (DDNS aktualizuje...)
>>>2 A=username H=hostname, U=1 (A=uživatelské jméno H=hostname)
>>>3 Connecting to the DDNS server (0x4225dad2) (připojuji se k DDNS serveru)
<<<4 Return Code= nochg 61.230.170.145 (hostname.dyndns.org) (Návratový kód = nochg...)

H: znamená doménové jméno bez přípony (ověřte zda jste zadali správné údaje pro uživatelské jméno a hostname - tyto údaje mohou být různé v závislosti na poskytovateli služby (někdy zde může být uvedena i přípona doménového jména).

Return Code= good 61.230.170.145 (Návratový kód = dobrý 61.230.170.145)

Budete-li mít problémy s nastavneím či používáním služby Dynamic DNS, pošlete výše uvedený log soubor a informace o nastavení vašemu poskytovateli služby DDNS, nebo přímo nám na email **support@draytek.com**.

3. Klikněte na položku **Online Status** a zjistíte vaši aktuální WAN IP adresu.



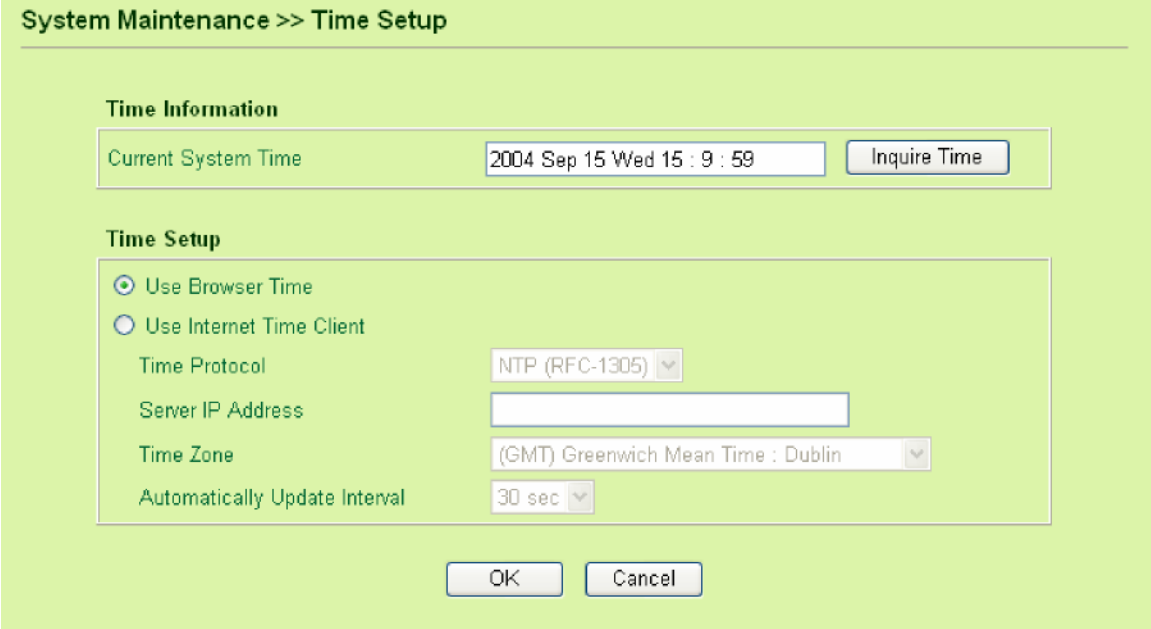
Pokud je IP adresa na výše uvedeném obrázku (viz. zakroužkovaná IP adresa) shodná s parametrem Return Code z DDNS log souboru, je nastavení správné. Tím je nastavování DDNS dokončeno.

Kapitola 8
Časový plán vytáčení

8,1 Úvod

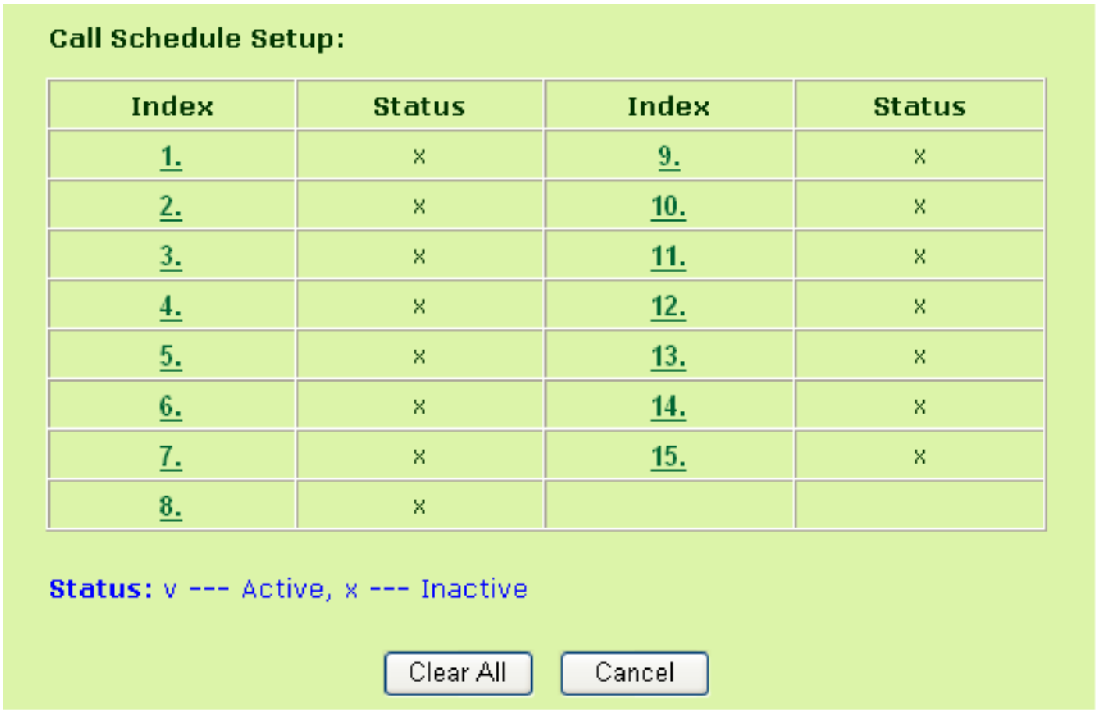
Ve směrovači Vigor jsou zabudované systémové hodiny, které lze nastavovat ručně prostřednictvím internetového prohlížeče, nebo automaticky pomocí serveru NTP (internetový server pro nastavování času). Tato funkce umožňuje nastavit čas, kdy se směrovač automaticky připojí k internetu, nebo ji lze naopak využít k omezení přístupu k internetu v určitých hodinách (takže směrovače umožní uživatelům sítě LAN přístup k internetu pouze v určitých hodinách - například v pracovní době). Totéž platí pro vytáčené připojení (při použití ISDN linky). Časové nastavení lze také použít pro připojení typu LAN - LAN.

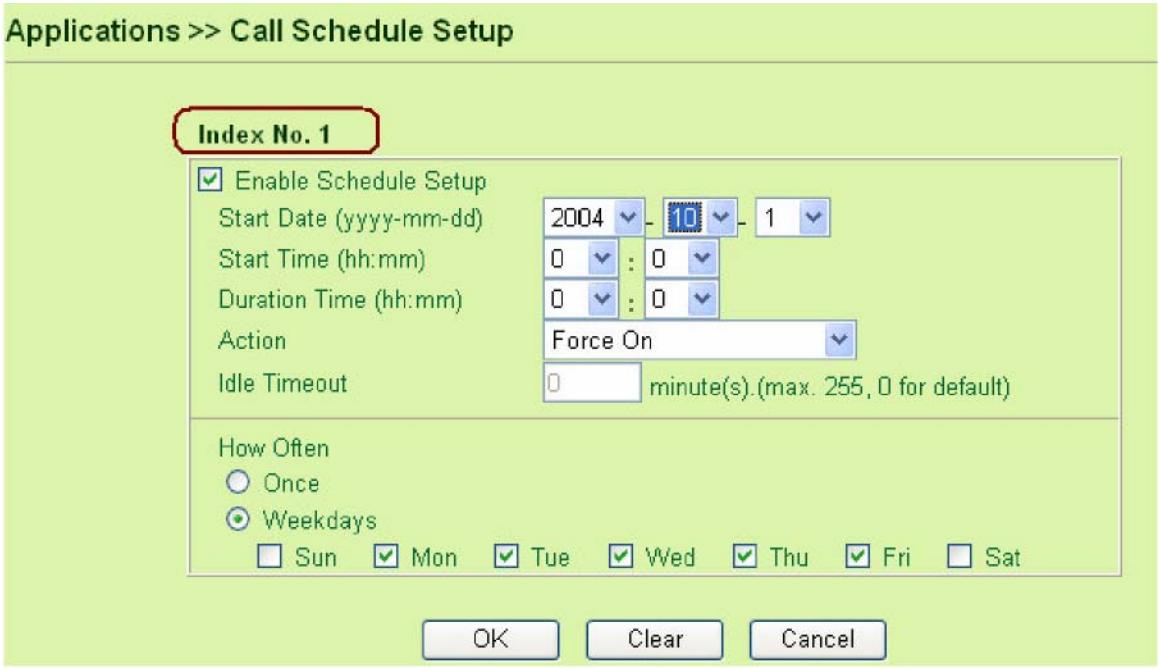
Než začnete využívat funkci **Call Scheduling (Časové plány)** je třeba ověřit nastavení správného času na vašem směrovači správný čas. To provedete v nabídce **Time Setup (Nastavení času).**



Pokud v nabídce **Time Setup** stiskněte tlačítko **Inquire Time (Dotázat se na čas)** nastaví se systémové hodiny směrovače na stejný čas, na který je nastaven systémový čas vašeho PC. Při výpadku napájení nebo resetu směrovače dojde rovněž k vymazání času vašeho směrovače. Proto také můžete využít funkci automatického nastavení času pomocí NTP serveru na internetu. Automatické nastavení času pomocí NTP serveru funguje pouze při připojení na internet (směrovače se automaticky nepřipojí k internetu za účelem automatického nastavení času).

Můžete nastavit až 15 různých časových plánů a poté aktivovat jednotlivé časové plány podle potřeby (viz. obrázek níže):





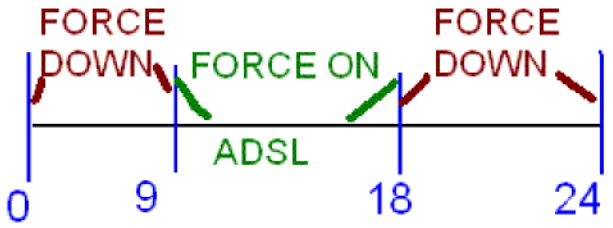
Podrobný popis nastavování časových plánů:
Enable Schedule Setup (Aktivovat používání časových plánů): Zaškrtněte toto pole pro zapnutí funkce používání časových plánů.
Start Date (yyyy-mm-dd) - Datum počátku (rok-měsíc-den): Uveďte počáteční datum spuštění plánu.
Start Time (hh:mm) - Počáteční čas (hodina - minuta): Uveďte počáteční čas spuštění plánu.
Duration Time (hh:mm) - Doba trvání (hodina - minuta): Uveďte dobu trvání (období) platnosti plánu.
Action - Akce: Uveďte co se má provést během zadaného období.
Force On - Připojit: Připojit se.
Force Down - Odpojit: Odpojit se.
Enable Dial-On-Demand - Aktivovat vytáčení na požádání: Uveďte druh připojení a do pole **Idle Timeout** (časový limit) zadejte dobu odpojení při nečinnosti.
Disable Dial-On-Demand - Deaktivovat vytáčení na požádání: Zadejte připojení, které se má provést, je-li linka obsazená. Pokud nedojde k obsazení linky během časového limitu (idle timeout) bude spojení přerušeno a již nikdy

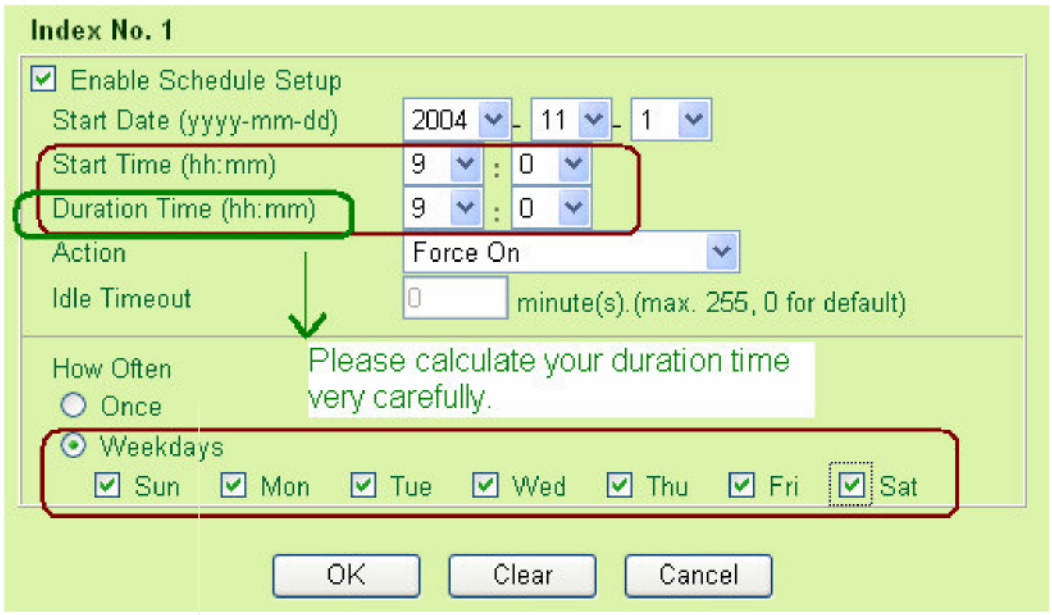
nebude v rámci daného časového plánu aktivováno.
How Often - Jak často: Uveďte jak často se bude daný plán používat.
Once - Jednou: Časový plán bude použit pouze jednou.
Weekdays - dny v týdnu: Zaškrtněte dny, ve kterých bude tento časový plán využíván.

Nastavte období trvání a akci, která se má provést a poté klikněte na tlačítko **OK**.
Uveďte časový plán pro vytáčení připojení k internetu nebo přístupu LAN - LAN.

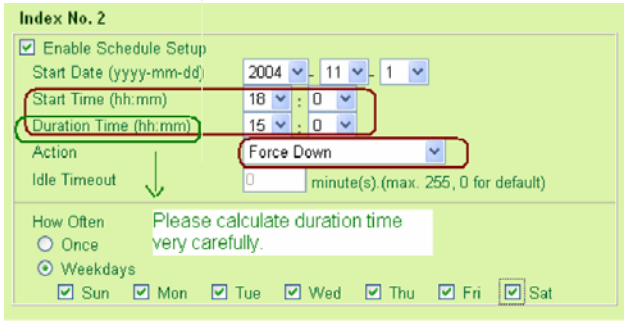
Delete a Call Schedule - Smazat časový plán vytáčení
1. Klikněte na nabídku **Call Schedule Setup** a zvolte číslo plánu (**Index**), který chcete smazat.
2. Klikněte na tlačítko **Clear (Smazat)** pro vymazání vybraného profilu.

8.2 Příklad pro uživatele připojující se pomocí služby ADSL
Prostřednictvím služby PPPoE (ADSL) můžete nastavit například trvalé připojení (Force On) směrovače k síti od 9:00 do 18:00 po celý týden. Mimo uvedené rozmezí bude připojení deaktivováno (Force Down).
1. Nejprve se přesvědčte zda máte nastavený správný čas (nabídka **Time Setup**) a zda připojení přes PPPoE funguje správně.
2. Nastavte připojení PPPoE tak, aby bylo vždy zapnuto v období od 9:00 do 18:00 hodin (doba trvání -Duration Time - 9 hodin) po celý týden.

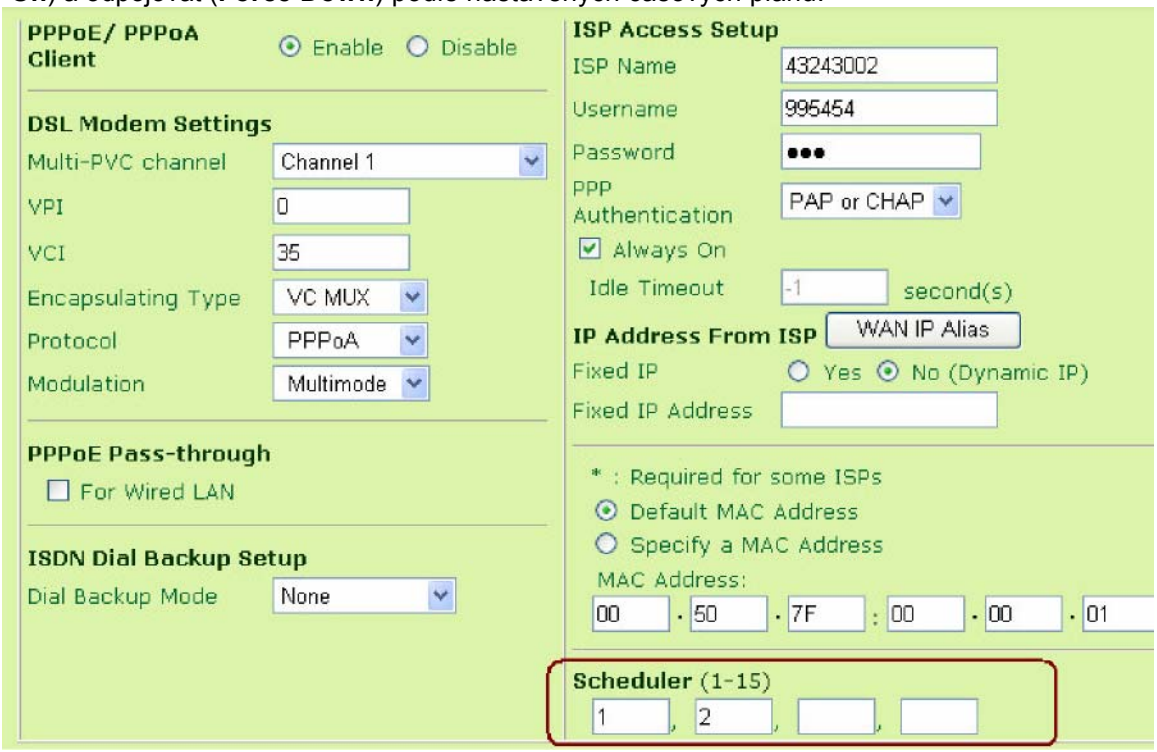




3. Pro období od 18:00 do 9:00 následujícího dne nastavte odpojení (**Force Down**) - doba trvání 15 hodin.

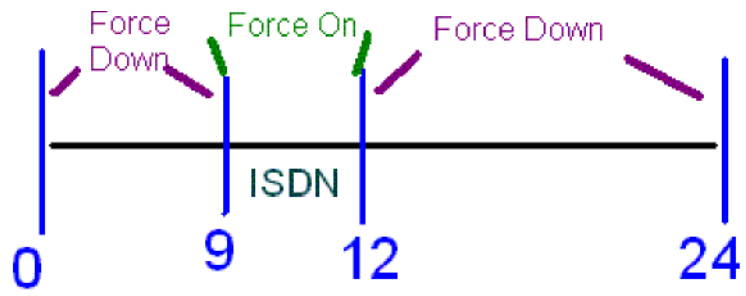


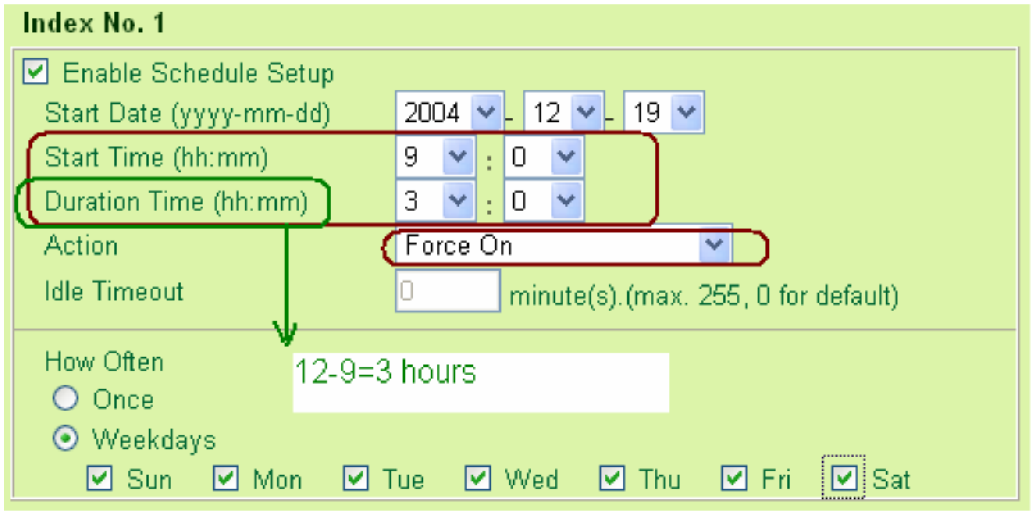
4. Tyto dva profily přiřaďte k internetovému připojení PPPoE. Nyní se připojení PPPoE bude automaticky připojovat (**Force On**) a odpojovat (**Force Down**) podle nastavených časových plánů.



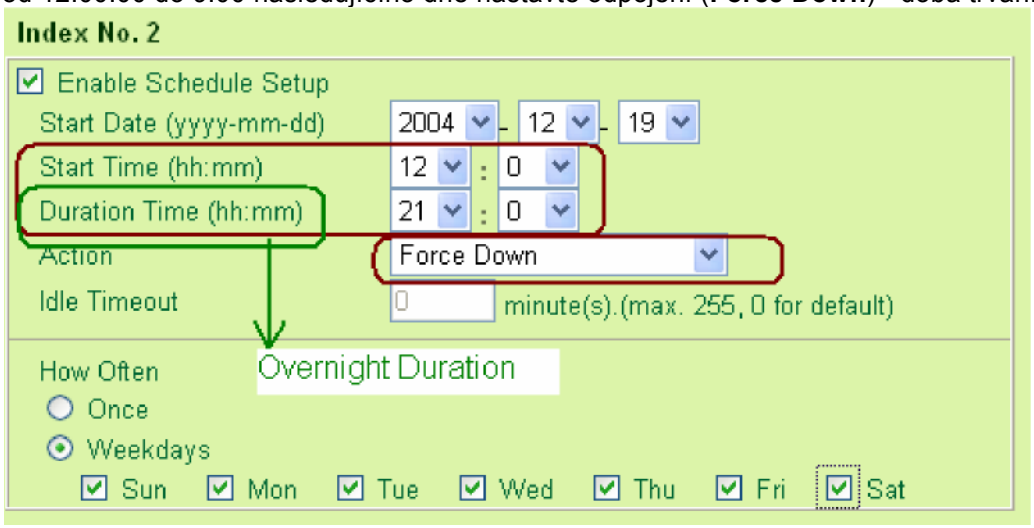
8,3 Příklad pro uživatele připojující se pomocí služby ISDN

Protože často potřebujete zasílat do práce důležité soubory z vašeho domácího ISDN připojení, můžete váš směrovač Vigor řady 2500Vi nastavit tak, aby každý den v týdnu od 9:00 do 12:00 dopoledne aktivoval své ISDN rozhraní. Po zbytek času bude ISDN nastaveno na odpojení (**Force Down**).



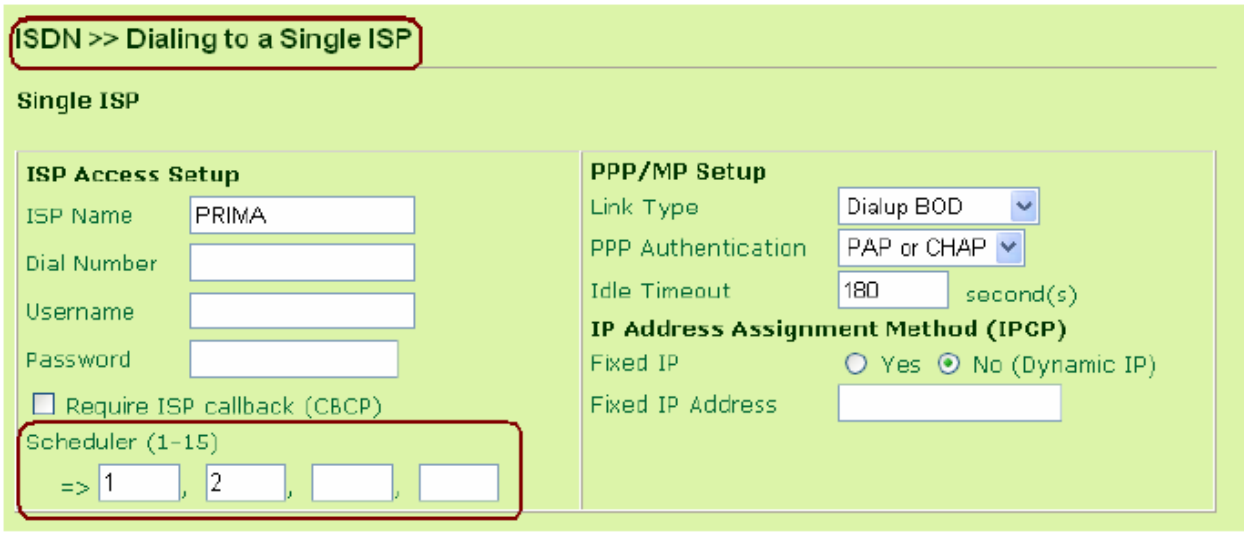


3. Pro období od 12:00:00 do 9:00 následujícího dne nastavte odpojení (**Force Down**) - doba trvání 21 hodin.



Pole "**Duration Time - Doba trvání**" slouží ke snadnému nastavení období obsahující dva dny (přes noc).

4. Tyto dva profily přiřaďte k internetovému profilu pro připojení přes ISDN.



Kapitola 9
Statická trasa

9,1 Úvod

Pokud máte přihlášeno několik veřejných IP adres (tedy kromě podsítě od vašeho poskytovatele, máte ještě další vedlejší veřejné IP adresy, můžete nastavit do pole pro druhou IP adresu směrovače vaší první přidělenou veřejnou IP adresu. V tomto případě bude zbytek podsítě vašeho poskytovatele přepuštěn do vaší sítě LAN.
Nastavení TCP/IP pro osobní počítač připojený k síti LAN je třeba provést ručně. Poté co vašemu osobnímu počítači přidělíte jednu z vašich veřejných IP adres, musíte pro tento počítač také nastavit výchozí bránu (tedy 2. IP adresu směrovače) a nějaké adresy DNS serveru, které vám poskytne váš poskytovatel připojení. Na vaší síti LAN můžete míchat přeložené IP adresy (NAT) s veřejnými IP adresami. K vaší síti tedy budou připojeny jako počítače s veřejnou IP adresou, tak počítače s privátní "přeloženou" podsítí.

Funkce statického směrování vašeho směrovače Vigor nabízí rychlý a účinný způsob směrování dat z jedné podsítě do druhé, bez nutnosti používání směrovacího informačního protokolu (RIP - Routing Information Protocol). Statické směrování je tedy jakási cesta, která směrovači říká jak se pomocí určité cesty dostat na určitou podsíť. Pokud máte za směrovačem připojeno mnoho privátních podsítí, nebo pokud chcete získat přístup k jiné veřejné podsíti pomocí vnitřního směrovače, můžete nastavit váš směrovač tak, aby směroval IP palety na pakety uvnitř IP sítí. Toto nastavení se provádí na konfiguračních stránkách protokolů **LAN TCP/IP a DHCP** v polích pro zadání 1. IP adresy a masky podsítě.
Směrovač má v sobě také standardně zabudovaný protokol RIP. Pokud používají sousední směrovače stejný protokol, bude protokol RIP používán pro výměnu informací mezi směrovači. V takovém případě slouží funkce statického směrování (**Static Route**) pouze pro nastavení statických cest pro určité IP pakety. V této kapitole popisujeme nastavení funkce statického směrování na vašem směrovači Vigor.

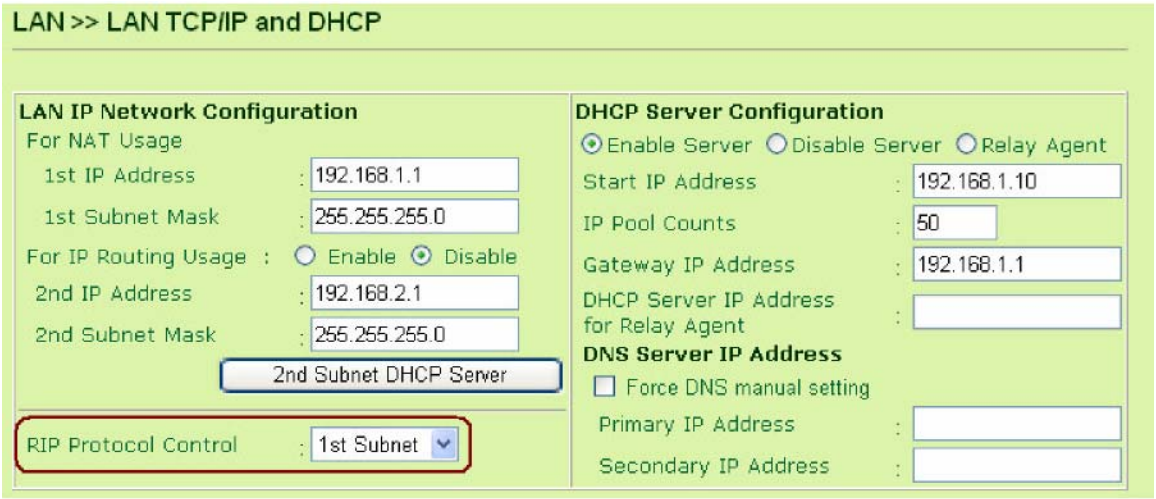
9.2 Nastavení

Přidání statických tras do vnitřních veřejných a privátních sítí (Add Static Routers to Inside Private and Public Networks)

Předpokládejme, že máte správně nastavený směrovač a fungující připojení k internetu. První adresu podsítě 192.168.1.0/24 používáte k brouzdání po internetu. Kromě toho provozujete také vnitřní privátní podsíť s adresou 192.168.10.0/24 přes interní směrovač (192.168.1.2/24) a vnitřní veřejnou podsíť 211.100.88.0/28 přes interní směrovač (192.168.1.3/24). Dále předpokládejme, že směrovač 192.168.1.1/24 je standardní bránou pro směrovač 192.168.1.2/24.

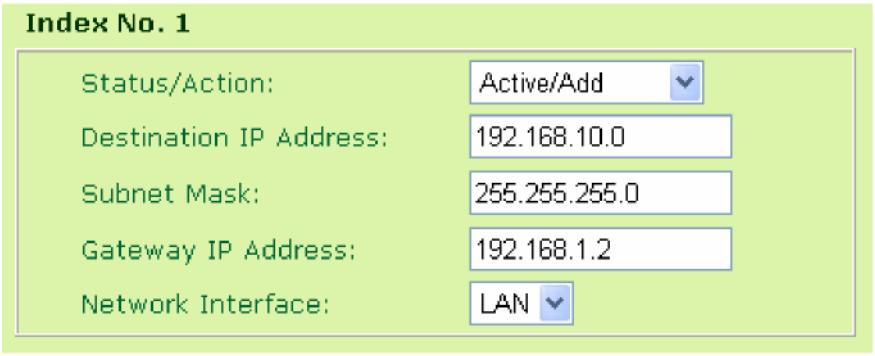
1. Klikněte na nabídku **LAN TCP/IP and DHCP Setup (nastavení LAN TCP/IP a DHCP)**, do pole **RIP Protocol Control (řízení RIP protokolu)** zadejte **1 st Subnet** (1. podsíť) a klikněte na tlačítko **OK**.

Nastavení řízení RIP protokolu první podsítí (**RIP Protocol Control - 1 st Subnet**) má dva různé cíle. Prvním důvodem je umožnění síti LAN výměnu RIP paketů se sousedními směrovači prostřednictvím první podsítě (192.168.1.0/24). Druhým důvodem je zajištění, aby vnitřní privátní podsítě (například 192.168.1.0/24) mohly být před přístupem na internet nejen směrovačem přeloženy, ale aby plnily také funkci směrování IP.

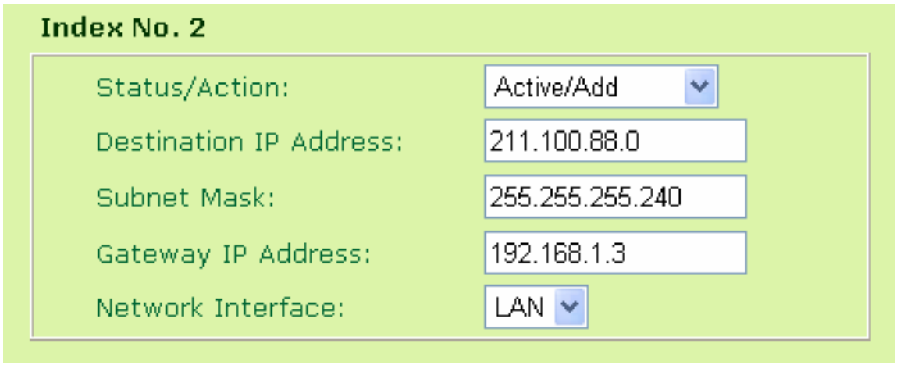


2. Přidejte statickou trasu do privátní podsítě 192.168.10.0/24 přes vnitřní směrovač 192.168.1.2/24. Nastavení

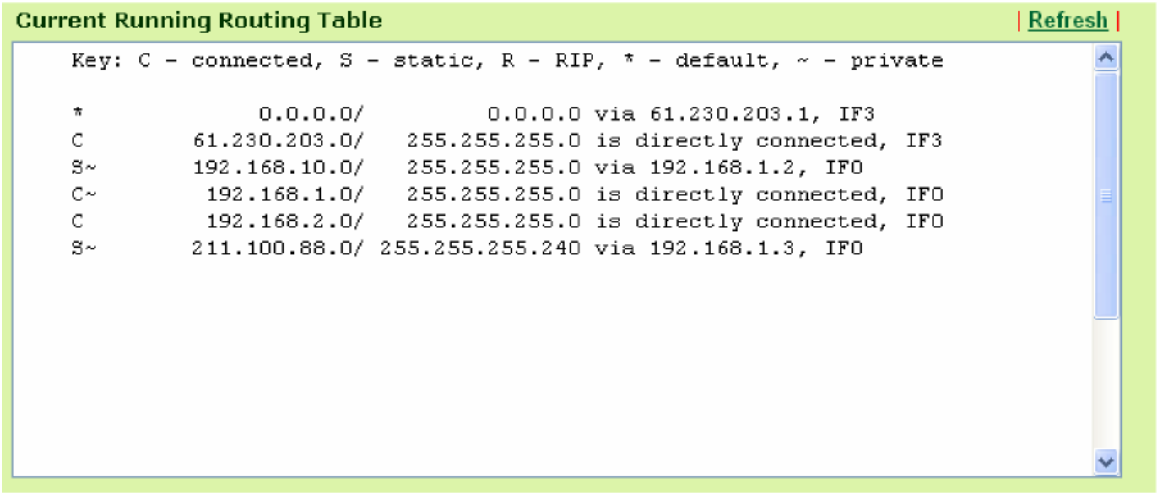
proveďte podle níže uvedeného obrázku na stránkách **Static Route > Index Number**.



3. Přidejte statickou trasu k vnitřní veřejné podsíti 211.100.88.0/28 přes vnitřní směrovač 192.168.1.3/24 jak je uvedeno níže:

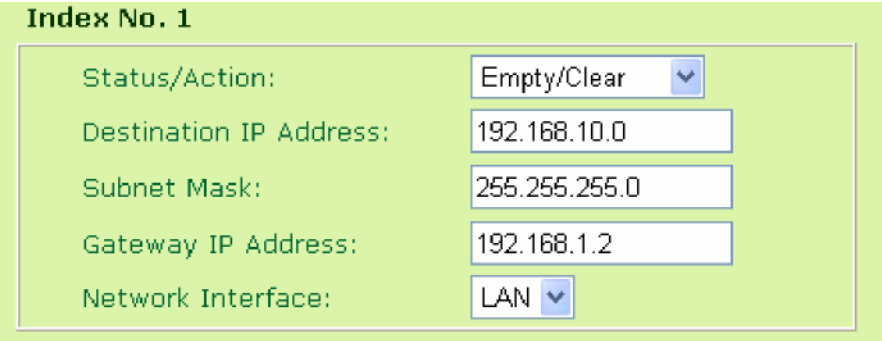


4. Klikněte na položky **Static Route > View Routing Table (statická trasa - ukaž směrovací tabulku)** a zkontrolujte správnost zadání.



Vymazání statické trasy

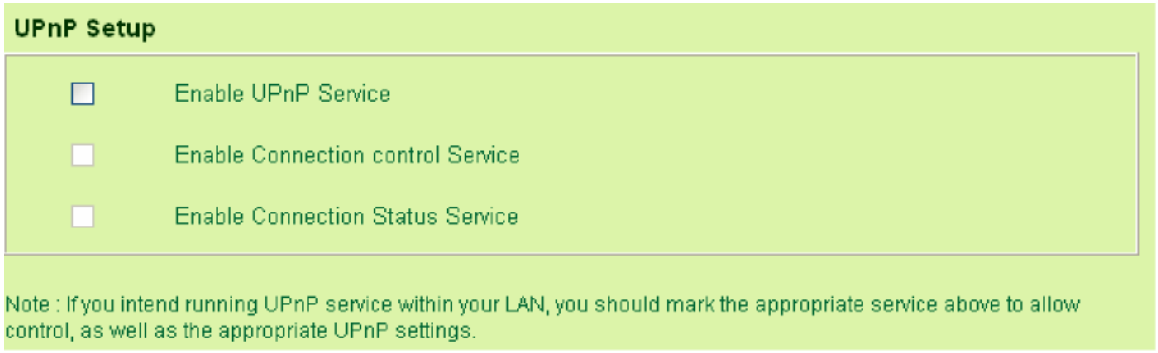
1. Klikněte na položku **Static Route Setup > Index Number** a na číslo trasy které chcete smazat (**Index Number**).
2. Do pole **Status/Action (Stav/ Akce)** zadejte **Empty/Clear (Vyprázdnit/Smazat)**. Klikněte na tlačítko **OK** pro smazání trasy.



Kapitola 10
Protokol UPnP (Universal Plug and Play)

10.1 Úvod

Protokol UPnP umožňuje zařízením připojeným k síti využívat inteligentní systém jejich instalace a nastavení (jedná se o stejný systém jako je Windows "Plug and Play" pro zařízení připojené k osobnímu počítači).
Pro směrovače využívající technologii NAT (překlad síťové adresy) je základní funkcí UPnP funkce "NAT Traversal - průchod NAT". Zapnutím této funkce zajistíme automatické otevření portů směrovače uvnitř brány firewall, potřebných pro instalaci síťového zařízení. Tato funkce je spolehlivější než ruční otevírání portů směrovače pomocí mapování portů a funkce DMZ.



Systém UPnP je součástí operačního systému Windows XP a směrovač Vigor podporuje službu MSN Messenger pro plnohodnotné využívání hlasových služeb, videoslužeb a služeb zpráv.

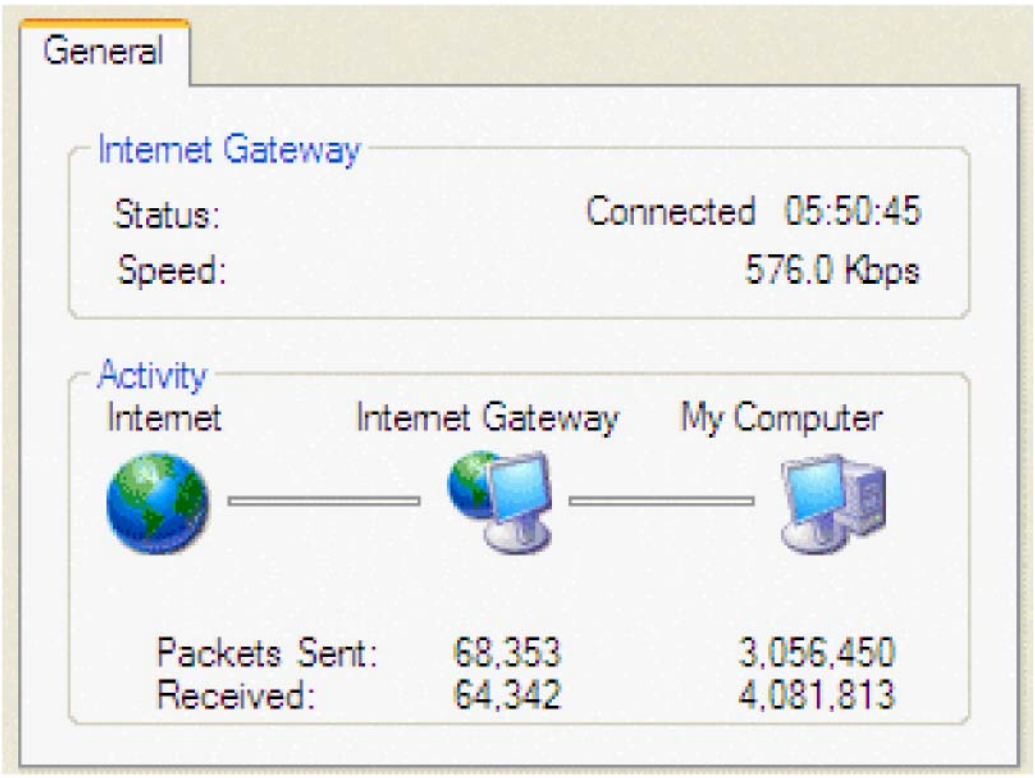
10,2 Nastavení

Nastavení služby UPnP provedete prostřednictvím webovského konfigurátoru **(Web Configurator)** vašeho směrovače,kliknutím na položky **UPNP Setup via Advanced Setup > UPNP Service Setup**.

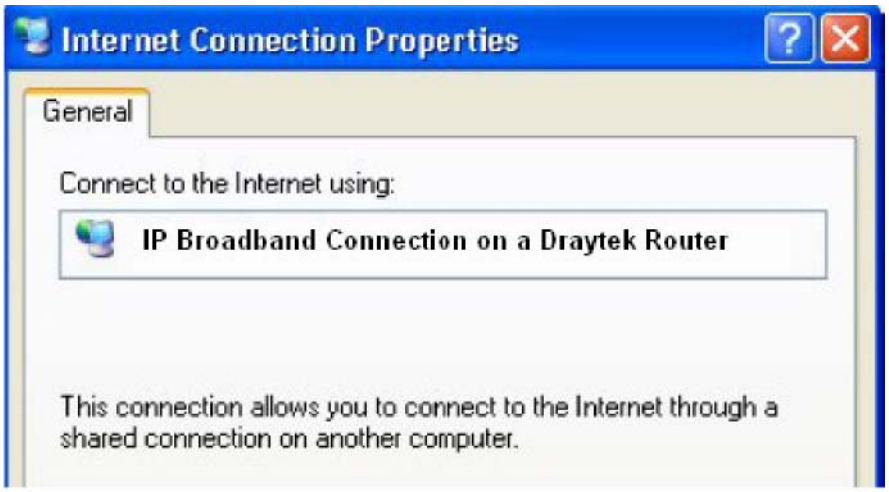
Zapněte službu UPNP.

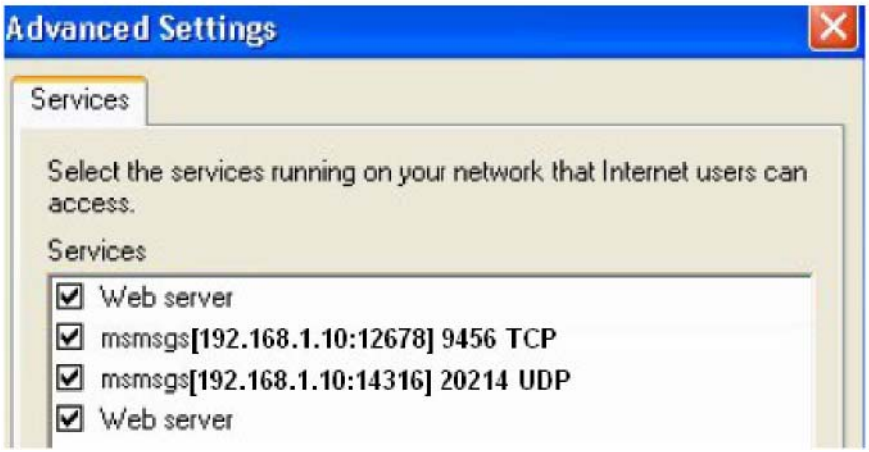
Stejným způsobem můžete aktivovat buď Connection Control Service (službu řízení připojení) nebo Connection Status Service (službu řízení stavu připojení).

V okně "Síťová připojení" se objeví ikona “Internet Gateway - internetová brána” . Pokud jste odpojeni, dvojím kliknutím na tuto ikonu (Internet Gateway) se připojíte k internetu přes vaší internetovou bránu.



V poli **Vlastnosti připojení** (v nabídce **Síťová připojení**) ve Windows XP, vyberte položku **IP Broadband Connection on Draytek Router** (širokopásmové připojení IP na směrovači Draytek). Funkce NAT Traversal zajistí přesné namapování a otevření jednotlivých portů, takže příslušné pakety z internetu budou moci být odeslány na správné místo. Níže uvedené obrázky ukazují příklad tohoto nastavení.





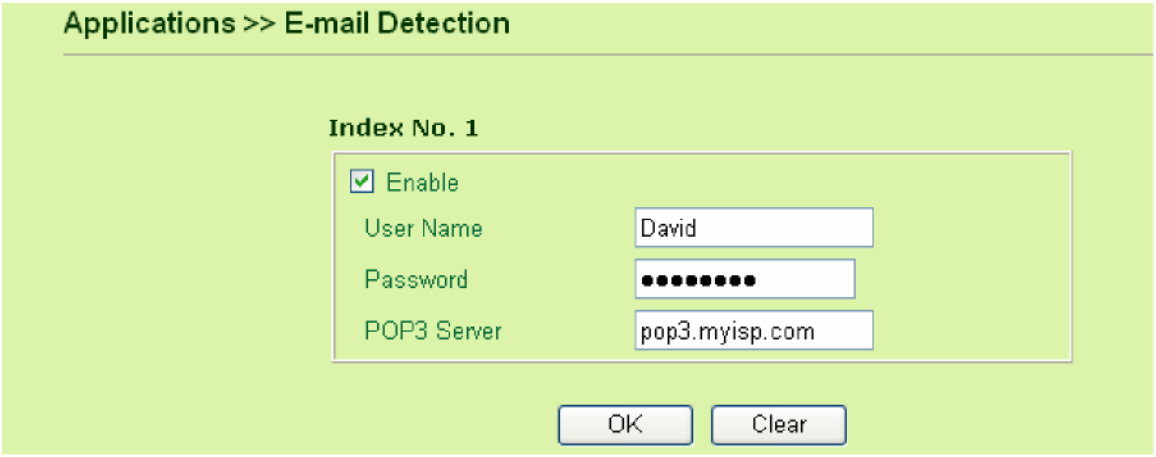
Funkce UPnP směrovače Vigor umožňuje zařízením a službám podporujícím UPnP (například MSN Messenger) zjistit, že se nachází za NAT směrovačem, zjistit externí IP adresu a namapovat všechny porty tak, aby se pakety z externích portů dostali na interní síťové porty, kde budou aplikací využity.
ADSL směrovače řady Vigor2500V je dodáván s již předinstalovanými bránami ALG (Application Level Gateways) pro lepší fungování multimediálních aplikací v rámci bezpečnostních systémů NAT. Brány ALG jsou již nastaveny od výrobce směrovače (DrayTek), takže na vašem směrovači Vigor již nemusíte provádět žádná další nastavení.

Kapitola 11
Detekce elektronické pošty

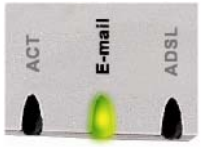
11.1 Úvod

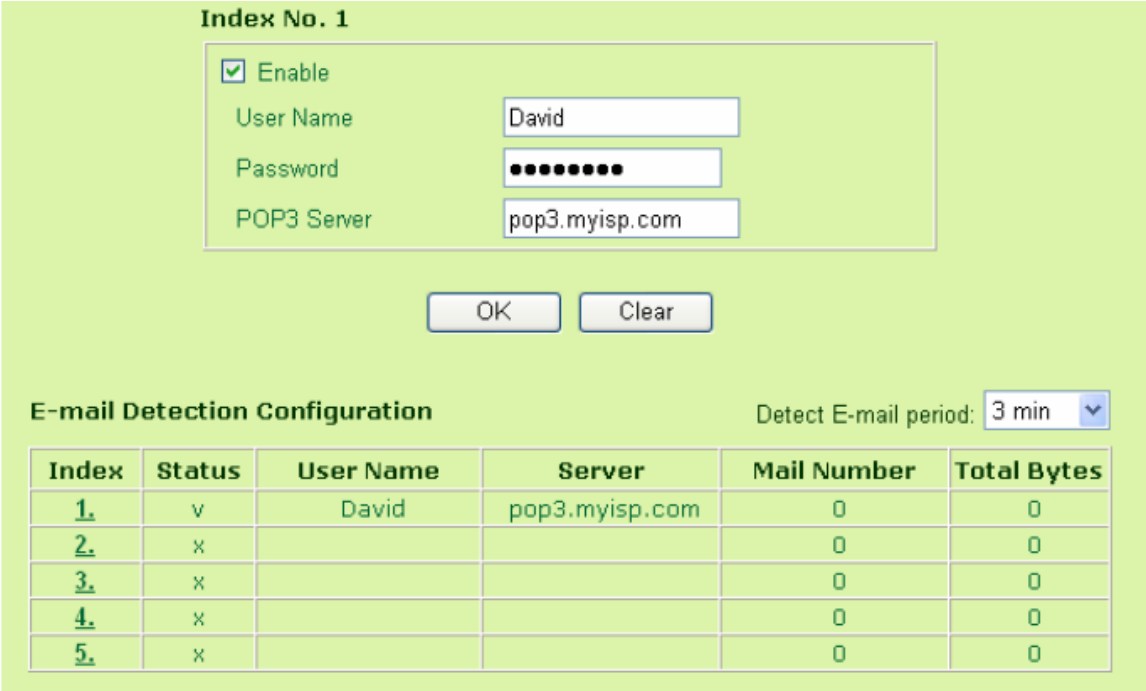
Snímače řady Vigor2500V jsou vybaveny systémem detekce elektronické pošty, který upozorňuje uživatele, že na poštovním serveru POP3 je nový e-mail. Na směrovači je LED dioda označená “e-mail”. Váš směrovač můžete nastavit tak, aby pravidelně kontrolovat zda na poštovním serveru POP3 vašeho poskytovatele připojení nejsou pro vás nějaké zprávy elektronické pošty. Pokud systém zjistí, že máte nevyzvednutou zprávu, rozsvítí se dioda "E-mail" na směrovači. Celkem si můžete směrovače nastavit až na sledování 5 poštovních účtů POP3. LED dioda na směrovači vás pak rozsvícením upozorní na příchod nové zprávy, aniž byste museli zapínat váš počítač či se k němu zalogovat.
Přesvědčte se , že váš e-mailový klient (aplikace pro správu elektronické pošty) přijímá zprávy pomocí protokolu POP3. Protokol POP3 je nejpoužívanějším serverem pro příjem e-mailu na světě. Takto nicméně nelze kontrolovat e-maily na internetových e-mailových službách (například Hotmail), pokud od nich nezískáte jméno a heslo pro vzdálený přístup k poštovnímu serveru. Funkci automatické detekce aktivujete zaškrtnutím položky **Enable** (viz. dole). Do pole POP3 Server napište adresu serveru pro přijatou poštu a do polí **User name** a **Password** vaše uživatelské jméno a heslo pro přístup k poštovnímu serveru. Postup nastavování je úplně stejný jako nastavování poštovních účtů v programu pro správu elektronické pošty (např. MS Outlook).

11-1



Celkem můžete funkci detekce příchozích zpráv elektronické pošty aktivovat až u 5 různých poštovních účtů. Pokud máte nějaké zprávy v poštovní schránce, zobrazí se jejich počet v poli ***Mail Number*** (viz. obrázek níže). V poli ***Total Bytes*** se zobrazí celková velikost přijatých zpráv.
Blikající dioda LED na směrovači signalizuje, že ve sledovaných schránkách jsou nové, nepřečtené zprávy.



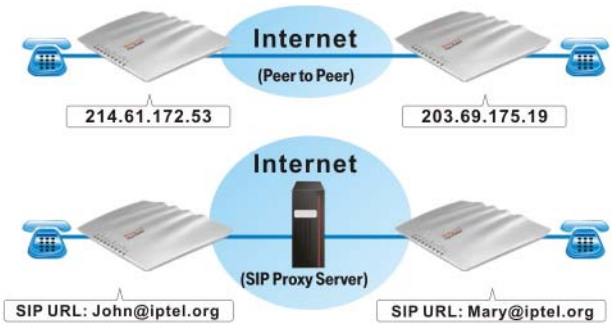


Standardně je kontrola nových zpráv nastavena na každé 3 minuty. Toto nastavení můžete samozřejmě změnit podle potřeby (viz. obrázek výše).

Kapitola 12
Vo I P

12.1 Úvod

Síť Voice over IP network (VoIP) umožňuje internetovou telefonii.
Existuje mnoho signalizačních protokolů pro zpracování hovorů, stejně jako způsobů komunikace VoIP zařízení mezi sebou. Nejčastěji používanými protokoly jsou SIP, MGCP, Megaco a starší protokol H.323. Tyto protokoly nejsou vzájemně kompatibilní (ledaže používáte softwarový přepínač).
Směrovače řady Vigor2500V podporují protokol SIP, protože představuje vhodné a ideální řešení pro poskytovatele internetové telefonie (ITSP - Internet Telephony Service Provider) a těší se široké podpoře. Protokol SIP podporuje přímé volání typu peer-to-peer, případně volání přes SIP proxy server (funguje na podobném principu jako hlídač (gatekeeper) u starších sítí H.323.). Protokl MGCP využívá architekturu klient - server a spojení hovorů probíhá na velmi podobném systému, jako spojení přes klasickou telefonní ústřednu.
Po sestavení hovoru, je hlas přenášen přes protokol RTP (Real-Time Transport Protocol). Do protokolu (paketů) RTP lze implementovat různé kodeky (CODECs). Kodeky nabízí různé způsoby komprimování a enkódování hlasu. Směrovač řady Vigor2500V nabízí různé druhy tzv. G kodeků, včetně G.711 A/ -law a G.729 A & B. Každá kodek používá jinou šířku pásma a nabízí tedy rozdílnou kvalitu přenosu hlasu. Čím větší šířku pásma kodek využívá, tím je kvalita přenášeného hlasu lepší. Nicméně musíte volit takové kodeky, které vyhovují vaší internetové šířce pásma.
Funkce VoIP směrovačů řady Vigor2500V tak představuje náklady šetřící alternativu ke klasické pevné telefonní lince. Rozhodnete-li se využívat služeb poskytovatelů internetové telefonie (např. DrayTEL, www.draytel.org) můžete také telefonovat na běžné telefonní linky, včetně mobilních telefonů a samozřejmě i přijímat hovory z libovolné telefonní i mobilní sítě. Protože je váš hovor přenášen přes vaše internetové připojení, zůstává vaše pevná telefonní linka volná pro další hovory.
Uživatelé směrovačů řady Vigor, mohou využívat funkci internetové telefonie dvěma způsoby: buď přímou volbou IP adresy, nebo čísla volit přímo na telefonu, prostřednictvím registrované služby SIP. SIP server umožňuje vašemu směrovači přenášet údaje o vaší aktuální pozici (IP adresa), takže vám uživatelé mohou volat přímo na vaši SIP adresu (například 98141@draytel.org

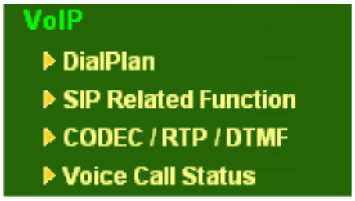


Než začnete používat protokol SIP, musíte si vytvořit SIP účet u příslušného správce (např. IPTEL, DrayTEL (www.draytel.org).)

Přestože Vigor2500V nejprve použije potřebné kodeky pro co nejlepší využití dostupné šířky pásma, je směrovač vybaven také **automatickým zajištěním QoS!!**
Funkce automatického zajištění QoS přidělí přenosu hlasu přes internet vysokou prioritu. Budete tak mít vždy k dispozici potřebné šířku pásma pro příchozí a odchozí hlasové informace, což je nutné pro přenos hlasu přes internet. Navíc zaznamenáte pouze malé zpomalení datových přenosů.

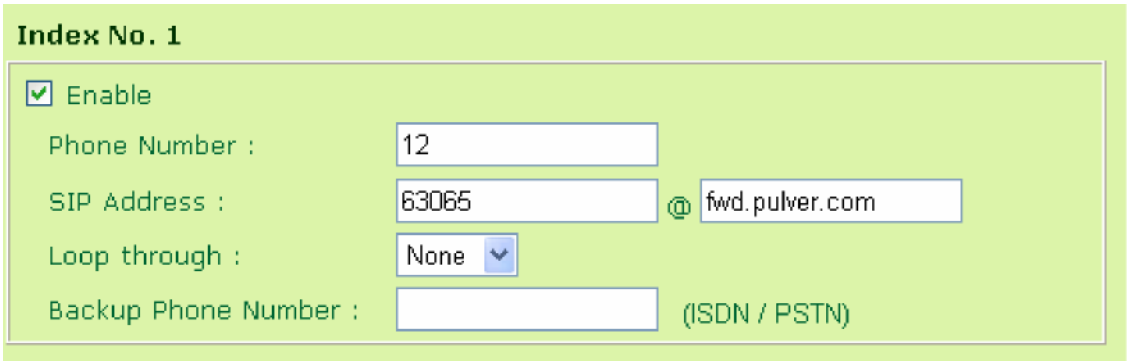
12.2 Nastavení VoIP

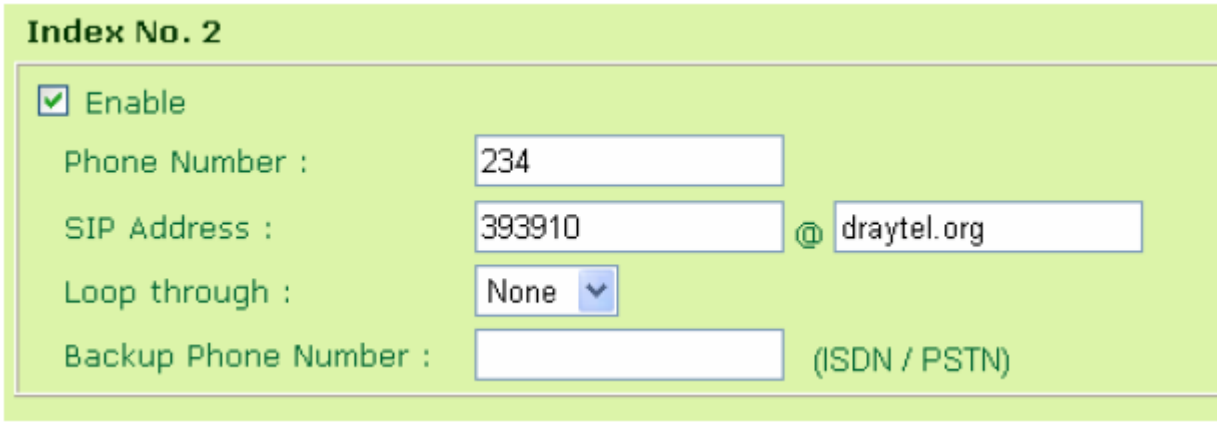
Nastavení můžete provést kliknutím na následující položky:



12.2.1 Sestavení hovoru(Dial Plan)

Směrovač Vigor2500V je vybaven jedním portem FXS (port “Phone - telefon” na zadní straně směrovače) který umožňuje připojit ke směrovači běžný (analogový) drátový či bezdrátový (DECT) telefon. Funkce Dial Plan vám umožní zadat do příslušných polí jednotlivé nejpoužívanější SIP adresy (telefonní čísla), která pak lze volit jednoduchým způsobem. Kapacita telefonního seznamu je 60 míst, což vám umožní zadat SIP adresy všech vašich přátel a rodinných příslušníků.

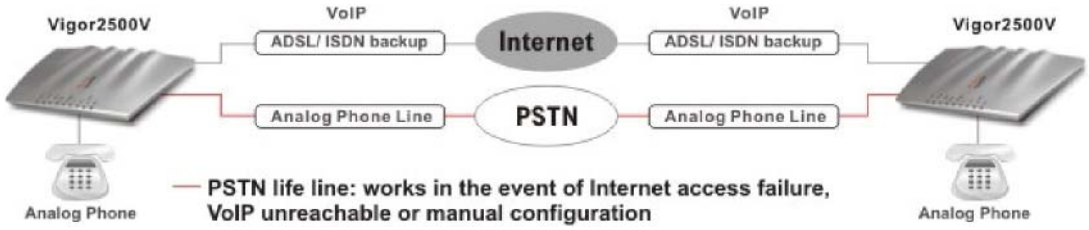




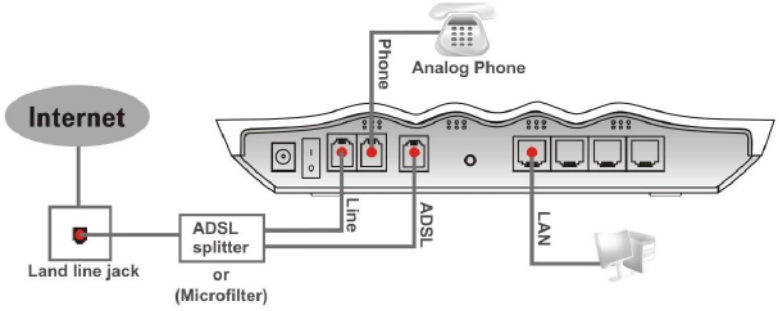
Index	Phone number	SIP Address
1.	12	63065 @ fwd.pulver.com
2.	234	393910 @ draytel.org

Zapnout (Enable): Zaškrtnutím tohoto pole funkci zapnete.
Phone Number (telefonní číslo): Číslo, které chcete volat z vašeho telefonního přístroje. Zadejte číselnou hodnotu pomocí tlačítek 0-9 a*
SIP Address (SIP adresa): Zadejte SIP adresu příslušné kontaktní osoby (například 98141@draytel.org)
Loop Through (propojení): Na zadní straně směrovače Vigor 2500V je port pro připojení standardní analogové telefonní linky (port "**Line**"). Funkci Loop Through lze použít pro nastavení alternativního telefonního

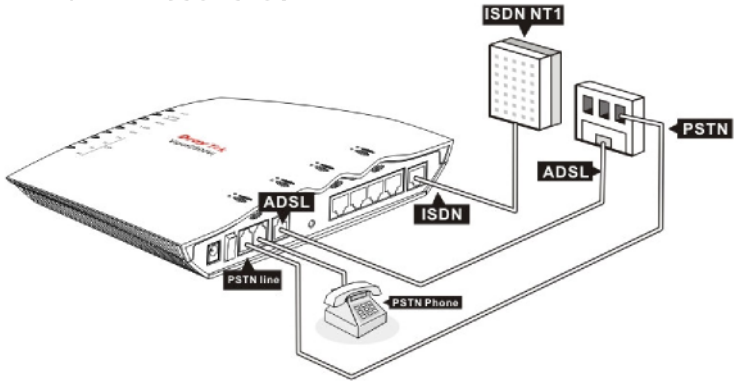
čísla, které směrovač Vigor2500V vytočí namísto SIP adresy vaší kontaktní osoby v případě ztráty spojení ADSL, nebo v případě výpadku napájení. Funkce analogové linky (PSTN) tedy funguje jako záložní mechanismus pro případ výpadku internetové telefonie (VoIP). Tento záložní mechanismus se aktivuje automaticky, ale jeho nastavení lze též ručně měnit.
Směrovač řady Vigor2500Vi je dokonce vybaven i ISDN rozhraním, které můžete rovněž využít jako běžnou telefonní linku. Při výpadku napájení směrovače nebo přo poruše internetové telefonie (VoIP) tak můžete stále telefonovat přes ISDN. ISDN linka tedy funguje jako záložní mechanismus pro případ výpadku internetové telefonie (VoIP).



Annex- A countries:



Annex – B countries



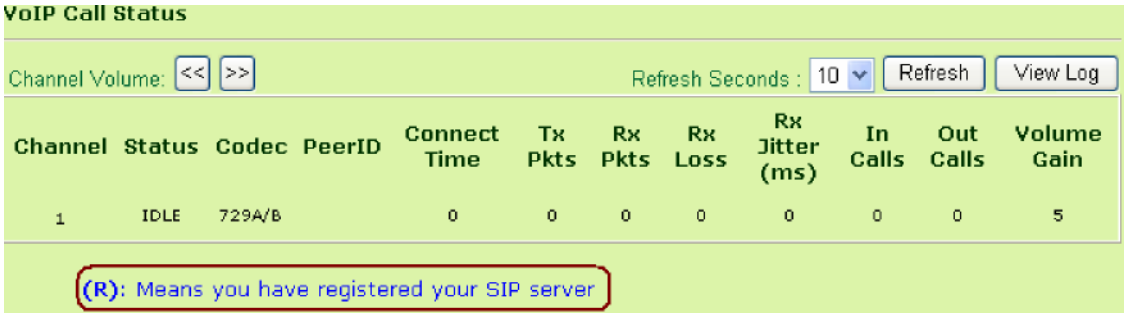
Backup Phone Number (náhradní telefonní číslo): Náhradní telefonní číslo (nastavené v poli **Backup Phone Number**) buď pro klasickou analogovou telefonní linku (PSTN), nebo pro ISDN linku (pouze u modelu Vigor2500Vi) se vytočí pouze tehdy, zadáte-li do pole **Loop Through** položku **PSTN phone number** nebo **ISDN phone number**.

only Vigor2500Vi model has ISDN and can let ISDN number be backup for VoIP

Pouze model Vigor2500Vi je vybaven ISDN rozhraním. Pokud doma používáte ISDN linku a ISDN telefonní číslo budete moci záložní funkci ISDN linky využívat pouze u tohoto modelu, který je vybaven ISDN portem pro připojení linky ISDN NT1, kterou získáte od vašeho poskytovatele nebo Telecomu. Pokud tedy chcete využívat ISDN linku jako zálohu pro případ výpadku internetové telefonie, musíte si koupit směrovač Vigor2500Vi, který je vybaven ISDN rozhraním.
Pokud chcete číslo vytočit ručně přes **ústřednu PSTN, zvolte na vašem telefonním přístroji "#0"** a teprve poté volte číslo volaného účastníka. Pokud máte strach, abyste neplatili příliš velké peníze v důsledku automatického přepojování (Loop Through), doporučujeme vám, abyste nezadávali číslo vaší analogové telefonní stanice do pole "Backup Phone Number - Záložní číslo". V tomto případě musíte pro přepojení vytočit telefonní číslo ručně na vašem telefonním přístroji. V případě sítě **ISDN, zadejte před volbou čísla účastníka "#1"** , protože máte model **Vigor2500Vi.**

12.2.2 Nastavení funkcí souvisejících se SIP

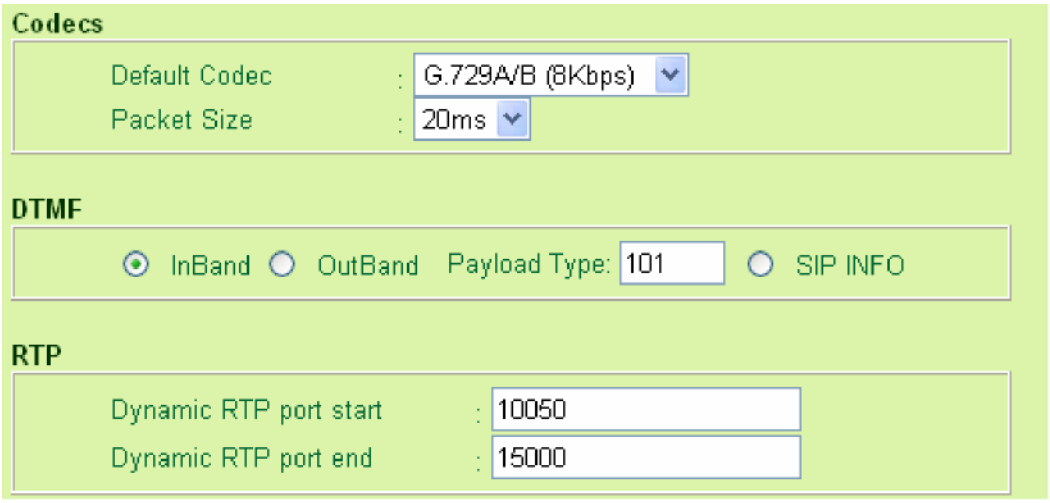
Poté co jste se zaregistrovali na SIP serveru (např. **DrayTEL**) zadejte do příslušných polí vaše uživatleské jméno a heslo pro SIP (podrobné vysvětlení uvádíme dále). Do pole **Registrar** (registrátor**)** zadejte název SIP serveru – celý text následující po znaku @ vaší SIP adresy. Klikněte na tlačítko **OK** a váš směrovač se připojí k SIP serveru. V okně "**VoIP Call Status - Stav volání VoIP**" se objeví znak "R" který ukazuje, že jste se připojil k vašemu SIP serveru.



SIP Port: Číslo portu užívané pro odesílání/přijímání SIP zpráv pro sestavení hovoru. Standardně nastavená hodnota je 5060 a tato hodnota musí odpovídat nastavení u vašeho registrátora (Registar) při sestavování VoIP hovorů.
Registrar (registrátor): Zadejte název domény (nebo IP adresu) vašeho registrovaného SIP serveru**.**
Use Registrar (použít registrátora): Zaškrtnutím tohoto pole sdělíte směrovači Vigor2500V, aby používal vámi zvoleného SIP registrátora.
Name (jméno): Zadejte vaše uživatelské jméno SIP (první část vaší SIP adresy před zavináčem @
Password (heslo): Zadejte vaši SIP adresu, kterou jste získali od SIP registrátora při registraci SIP služby**.**

Expire Time (čas vypršení): Doba po kterou server SIP registrátora uchovává údaje o vašem záznamu o registraci. Než tato doba vyprší, zašle směrovač Vigor ještě jednu registrační zprávu na registrační server.

12.2.3 Nastavení CODEC/RTP/DTMF



Default Codec (přednastavený kodek): Zvolte jeden z pěti kodeků, který bude prioritně používán pro internetovou telefonii. Kodek použitý pro dané volání je vybrán před sestavením hovoru na základě komunikace, takže se může stát, že bude pro komunikaci nakonec vybrán jiný než ten přednastavený. Přednastavený kodek je G.729A/B, protože zabírá malou šířku pásma při zachování dobré kvality přenosu hlasu.
Pokud je rychlost vašeho připojení pro odesílání dat pouze 64 Kb/s, nepoužívejte kodek G.711. Pro používání tohoto kodeku je doporučena rychlost alespoň 256 Kb/s.
Packet Size (velikost paketu): Objem dat obsažených v jednom paketu. Standardní nastavení je 20 ms což znamená, že každý paket ponese 20 ms hlasové informace.
DTMF InBand: Pokud zvolíte tuto funkci bude směrovač Vigor posílat DTMF tóny jako audiosoubory přímo po síti okamžitě po jejich stisknutí na klávesnici.
DTMF OutBand: Pokud zvolíte tuto možnost, směrovač Vigor nejprve zachytí stisknuté číslo, převede ho do digitální podoby a pošle jej na druhý konec komunikačního kanálu. Na straně příjemce se poté vygeneruje příslušný tón na základě přijatého digitálního signálu. Tato funkce je velmi užitečná v případech, kdy dochází k přetížení sítě, protože zaručuje přesnou reprodukovatelnost DTMF tónů.
DTMF Payload Type: Standardně nastavená hodnota je 101, ale může výt nastavena na jakoukoli hodnotu v rozmezí 96 - 127.
SIP INFO: Tuto možnost aktivujte pokud chcete, aby SIP proxy server posílal DTMF tóny volané straně.
RTP: Počáteční a koncový port RTP řetězce. Standardně nastavené hodnoty jsou 10050 - 15000.

12.3 Způsoby volání

12.3.1 Příklad volání typu Peer-to-Peer

Arnor a Paulin mají oba směrovač Vigor2500V. Níže uvádíme nastavení jejich směrovačů pro vzájemné internetové volání.

Arnorova IP adresa: **214.61.172.53**
Paulinova IP adresa: **203.69.175.19**

A. Arnorovo nastavení

A-1. Volací plán číslo 1 (DialPlan index 1)

Tel. číslo: **1234**
(číslo podle libosti)
- Jméno: **paulin**
IP Address / Domain: **203.69.175.19**

A-2. Funkce související se (SIP Related Function)
SIP Port: 5060 Registrar: **nechat prázdné**
Port 1:
Use Register: **nechat prázdné**
Name: **arnor**
Password: **nechat prázdné**
Expiry Time: **použijte přednastavenou hodnotu**
SIP Port: **5060**

A-3. CODEC/RTP/DTMF
(použijte přednastavenou hodnotu)

B. Paulinovo nastavení

B-1. DialPlan index 1

Tel. číslo: **123**
(číslo podle libosti)
Jméno: **arnor**
IP Address / Domain: **214.61.172.53**

B-2. SIP Related Function
Registrar: **nechat prázdné**
Port 1:
Use Register: **nechat prázdné**
Name: **paulin**
Password: **nechat prázdné**
Expiry Time: **použijte přednastavenou hodnotu**

B-3. CODEC/RTP/DTMF
(použijte přednastavenou hodnotu)

Nyní když chce Arnor volat Paulinovi, zvedne telefon a vytočí **1234#**.
Nyní když chce Paulin volat Arnorovi, zvedne telefon a vytočí **123#**

12.3.2 Volání přes SIP Server

Níže uvádíme nastavení pro Johna a Davida, kteří si volají přes registrované SIP účty (u firmy DeayTEL), protože žádný z jejich směrovačů nemá pevnou veřejnou IP adresu.
Johnova SIP URL adresa je : john@draytel.org Davidova SIP URL adresa je: david@draytel.org

A. Nastavení pro Johna

A-1. DialPlan index 1
Phone Number (telefonní číslo): **2536**
(libovolné telefonní číslo chcete)
Name (jméno): **david**
IP Address / Domain: draytel.org

A-2. Funkce související se SIP
SIP Port: 5060 Registrar:**draytel.org**
Port 1:
Use Register: **(zaškrtnuto)**
Name: **john**
Password: ********
(zadejte Johnovo registrační heslo)
Expiry Time: **(použijte přednastavenou hodnotu)**
A-3. CODEC/RTP/DTMF (použijte přednastavenou hodnotu)

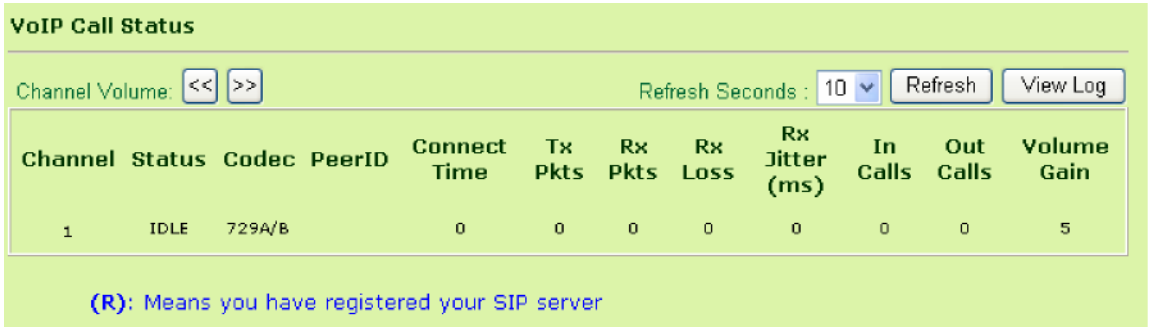
B. Nastavení pro Davida

B-1. DialPlan index 1
Phone Number (telefonní číslo): **8989**
(libovolné telefonní číslo)
Name (jméno): **john**
IP Address / Domain: draytel.org

B-2. Funkce související se SIP
SIP Port: 5060 Registrar: draytel.org
Port 1:
Use Register: **(zaškrtnuto)**
Name: **david**
Password: ********
(zadejte Davidovo registrační heslo)
Expiry Time: **(použijte přednastavenou hodnotu)**
B-3. CODEC/RTP/DTMF (použijte přednastavenou hodnotu)

Nyní když chce John volat Davidovi, zvedne telefon a vytočí 2536#.
Když chce David volat Johnovi, zvedne telefon a vytočí 8989#

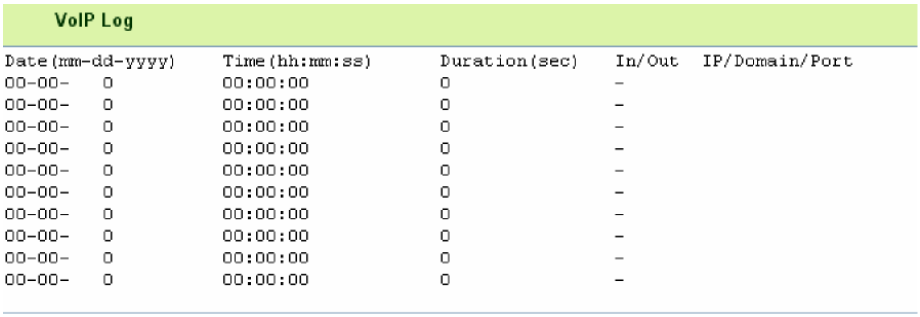
12.4 Stav hlasového volání (VoIP Call Status)



Channel Volume - Hlasitost: Hlasitost vašich VoIP volání nastavíte prostřednictvím těchto tlačítek (viz. obrázek výše). Nastavte příslušnou hlasitost (**Volume Gain)**.
Refresh Seconds (Doba obnovení v sekundách): Interval obnovy okna pro získání aktuálních informací o VoIP spojení. Pokud stisknete tlačítko **Refresh** zobrazí se aktuální údaje okamžitě.
Stav (Status): Zobrazuje stav připojení VoIP.

- **IDLE** : Není žádné VoIP spojení.
- **HANG_UP** : Spojení není navázáno (obsazovací tón).
- **COLLECTING** : Uživatel volá ven.
- **WAIT_ANS** : Spojení je navázáno, čeká se na odpověď druhé strany.
- **ALERTING** : Příchozí volání.
- **ACTIVE** : Spojení VoIP je navázáno a je aktivní.

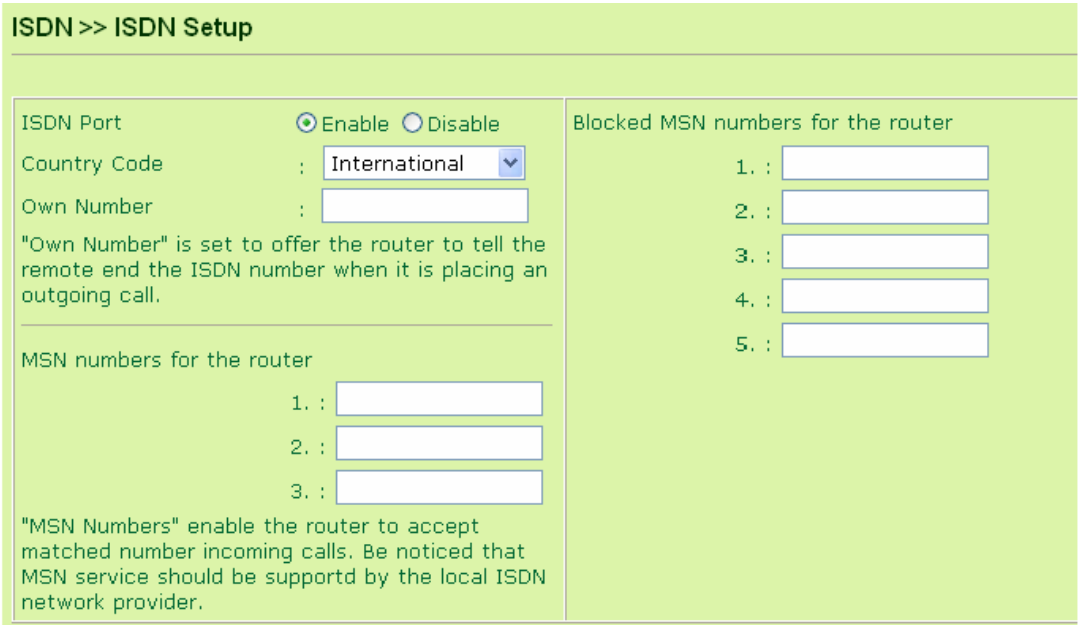
Codec: Hlasový kodek používaný příslušným kanálem.
PeerID: Aktuální identifikační číslo pro volání dovnitř a ven (číslo je buď ve formátu IP nebo jako doména).
Connect Time (doba připojení): Doba připojení v sekundách.
Tx Pkts: Celkový počet přenesených IP paketů během aktuálního telefonního volání.
Rx Pkts: Celkový počet obdržených IP paketů během aktuálního telefonního volání.
Rx Loss (ztracené pakety): Celkový počet ztracených IP paketů během aktuálního volání.
Rx Jitter (kolísání): Kolísání přijatých hlasových paketů.
In Calls (příchozí volání): Celkový čas příchozích volání.
Out Calls (odchozí volání): Celkový čas odchozích volání.
Volume Gain: Hlasitost aktuálního hovoru.
View Log (prohlížet log soubor): Zobrazí informace o hovorech v log souborech.



Kapitola 13
Nastavení ISDN

13,1 Úvod

V této kapitole se budeme zabývat vysvětlením nastavování ISDN (**ISDN Setup**). Níže uvedený text se vztahuje pouze pro model směrovače vybavený ISDN rozhraním.



13.2 Nastavení rozhraní ISDN

ISDN Port: ISDN port zapněte zaškrtnutím pole **Enable - Zapnout**. Vypnout používání ISDN portu můžete provést zaškrtnutím položky **Disable - Vypnout**. **Country Code (směrové číslo země):** Pro správné fungování vaší místní ISDN sítě musíte vložit správné směrové číslo země.

Own Number (vlastní číslo): Zadejte číslo vaší ISDN linky. Informace z tohoto pole bude při odchozích hovorech zasílána volanému účastníkovi.

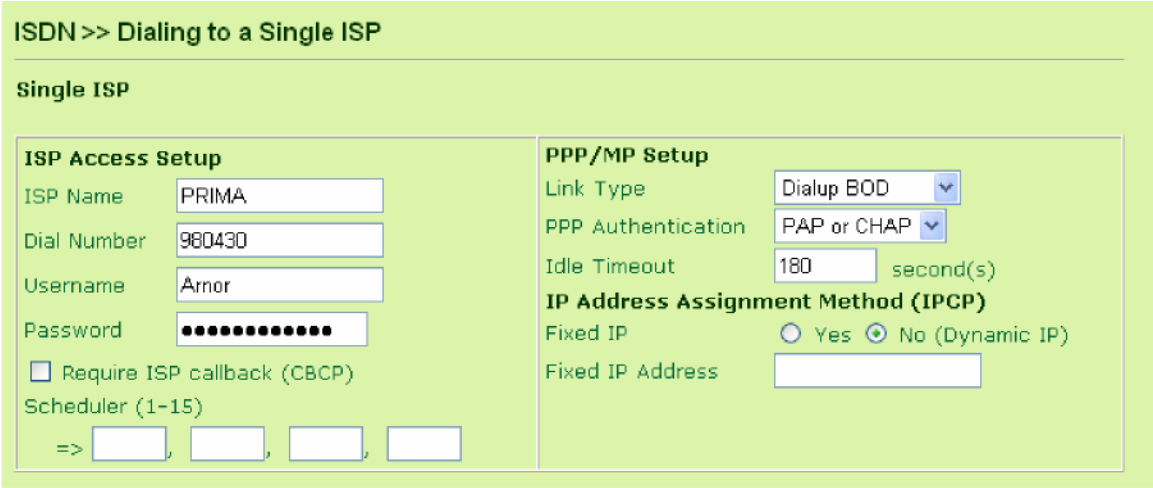
MSN Numbers for the Router (čísla služeb MSN pro směrovač): Čísla MSN (česky vícenásobná uživatelská čísla) umožňují směrovači směrovat příchozí hovory na jednotlivá čísla. Služba MSN musí být podporována vaším poskytovatelem ISDN. Ve směrovači jsou 3 pole pro zadání 3 různých MSN čísel. Službu MSN musíte mít objednanou u vašeho poskytovatele telekomunikačních služeb.

Ve standardním nastavení je tato funkce zakázána. Pokud pole pro zadání číslem MSN necháte prázdná, budou přijímány všechny příchozí hovory bez směrování na jednotlivá čísla.

Společnost DrayTek poskytuje předplatitelům ISDN internetu pracujícím z domova možnost **vzdáleného přístupu (Remote Activation)** k serveru v centrále jejich společnosti. Díky této funkci může uživatel z domova "požádat" směrovač v hlavní kanceláři o navázání spojení s poskytovatelem internetu. Pracovníci z domova se tak mohou přes ISDN bezpečně připojit k firemní síti LAN, což jim umožní pracovat efektivněji.

Rozhraní ISDN směrovače řady Vigor2500Vi podporuje také technologii **VTA (Virtual Terminal Adapter)**. VTA je vlastně rozhraní "CAPI", stejné jako je rozhraní CAPI na vašem počítači připojeném prostřednictvím ISDN. Díky CAPI rozhraní si můžete instalovat různé softwarové aplikace pro síťové, faxové či hlasové služby. Pokud chcete používat technologii VTA, stáhněte si příslušný ovladač (je k dispozici pouze pro Windows 98SE/2000/XP) ze serveru http://www.draytek.com/english/support/download.php .

13.3 Nastavení údajů pro vytáčené připojení k vašemu poskytovateli



Nastavení informací pro vytáčení (ISP Access Setup)
ISP Name (název poskytovatele): Zadejte název vašeho poskytovatele.
Dial Number (vytáčené číslo): Zadejte ISDN číslo pro připojení k internetu, které jste získali od vašeho poskytovatele.
Username (uživatelské jméno): Zadejte uživatelské jméno získané od vašeho poskytovatele.
Password (heslo): Zadejte heslo získané od vašeho poskytovatele.
Require ISP Calback (CBCP) - Před vytočením se dotázat na telefonní číslo: Pokud váš poskytovatel využívá funkci zpětného volání, zaškrtnete toto pole.
Scheduler (1-15) - Časový plán: Zadejte čísla jednotlivých časových programů pro přístup k internetu, tak jak jste si vaše časové plány nastavili.
PPP/MP Setup (Nastavení PPP/ MP)
Link Type (způsob připojení): Celkem jsou k dispozici 4 možnosti: Link Disable (zakázat vytáčení), Dialup 64 Kbps (vytáčení s rychlostí 64 kb/s - 1 kanál), Dialup 128 Kbps (vytáčení s rychlostí 128 kb/s - 2 kanály) a Dialup BOD (vytáčení BOD).
Link Disable: Připojovat se pomocí ISDN linky je zakázáno.
Dialup 64Kbps: Pro připojení k internetu bude použit jeden ISDN kanál (B). **Dialup 128Kbps:** Pro připojení k internetu budou použity oba ISDN kanály (B).
Dialup BOD: BOD znamená přidělování šířky pásma podle potřeby. V případě potřeby malé přenosové kapacity bude směrovače využívat pouze jeden B kanál. Po naplnění kapacity B kanálu směrovač automaticky vytočí druhý B kanál. Podrobnější informace o nastavení parametrů BOD najdete v nabídce **Advanced Setup** > **Call Control and PPP/MP Setup.**
PPP Authentication (ověření PPP):
PAP Only (pouze PAP): PPP session bude používat PAP protokol pro ověření hesla a uživatelského jména u poskytovatele připojení.
PAP or CHAP (PAP nebo CHAP): PPP session bude používat protokoly PAP nebo CHAP protokol pro ověření hesla a uživatelského jména u poskytovatele připojení.
Idle Timeout (odpojení při nečinnosti):
Nastavení doby nečinnosti, po jejímž uplynutí směrovač automaticky ukončí připojení. Přednastavená doba je 180 sekund. Pokud tento parametr nastavíte na 0, zůstane ISDN připojení trvale aktivní.
IP Address Assignment Method (IPCP) (způsob přidělování IP adres): pevná IP (Fixed IP), a pevná IP adresa (Fixed IP Address):
Ve většině případů nedoporučujeme měnit standardní nastavení,, protože většina poskytovatelů připojení přiděluje směrovači IP adresy dynamicky při každém připojení. Pokud vám váš poskytovatel přidělil pevnou IP adresu, zaškrtněte **Yes** (Ano) a příslušnou IP adresu zadejte do pole **Fixed IP Address**.

13.4 Připojovací informace alternativních poskytovatelů

Většinu parametrů nastavíte výše popsaným způsobem. Na nastavovací stránce najdete zaškrtávací pole **Enable Dual ISP** (povolit alternativní poskytovatele připojení). Pokud chcete využívat více poskytovatelů, zaškrtněte jej. Zadejte požadované údaje o vašem druhém poskytovateli. Nastavovací stránka je uvedena výše.

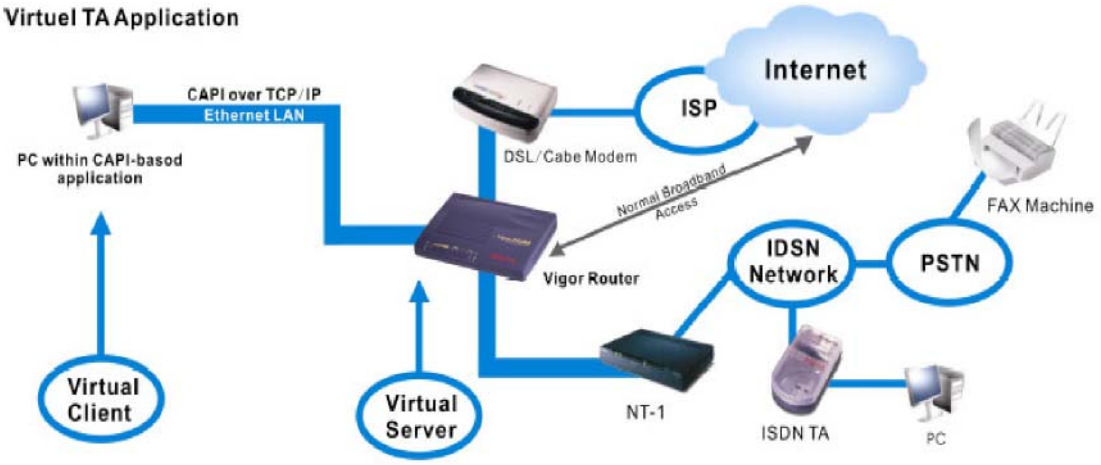
Kapitola 14
Virtuální TA (vzdálené CAPI)

14,1 Úvod

Tato kapitola se vztahuje pouze na směrovač Vigor2500Vi, který je vybaven ISDN rozhraním a funkcí **Virtual TA (virtuální TA)**. Aplikace **Virtual TA** jsou k dispozici na přiloženém firmware CD nebo na stránkách www.draytek.com/support .

Virtual TA je funkce, která umožňuje počítačům nebo ethernetovým síťovým zařízením využívat CAPI software (například RVS-COM nebo BVRP) pro přístup ke směrovači, pro zasílání či posílání faxů nebo pro přístup k internetu. V podstatě se jedná o síťovou architekturu typu klient/server. Server **Virtual TA** zabudovaný ve směrovači zajišťuje navázání spojení a jeho ukončení. Na druhou stranu klient **Virtual TA**, který je instalován na počítači nebo ethernetovém síťovém hostitelském zařízení vytváří CAPI rozhraní pro přenos zpráv mezi jednotlivými aplikacemi a CAPI portem směrovače. Než přistoupíme k podrobnému popisu systému **Virtual TA** instaloveném ve směrovačích Vigor, vezměte na vědomí níže uvedená omezení.

1. Klient **Virtual TA** je podporován pouze platformami Microsoft™ Windows 95 OSR2.1 /98/98SE/Me/2000.
2. Klient Virtual TA podporuje pouze protokol CAPI 2.0 a nemá zabudovaný žádný FAX engine.
3. Jedno rozhraní ISDN BRI má pouze 2 B kanály. Proto je maximální počet současně aktivních klientů omezen na 2.
4. Než začnete nastavovat systém Virtual TA, zadejte správní směrové číslo země. Pro zahájení nastavování klikněte na položku **ISDN Setup** v nabídce **ISDN**.



Jak je uvedeno ve výše uvedené tabulce může klient Virtual TA přijímat telefonní hovory, nebo realizovat odchozí volání, odesílat nebo přijímat faxové zprávy přes připojené faxové zařízení nebo ISDN TA, apod. Nastavení funkce Virtual TA (vzdálené CAPI) provedete na následujících obrazovkách.

ISDN > Virtual TA (Remote CAPI)

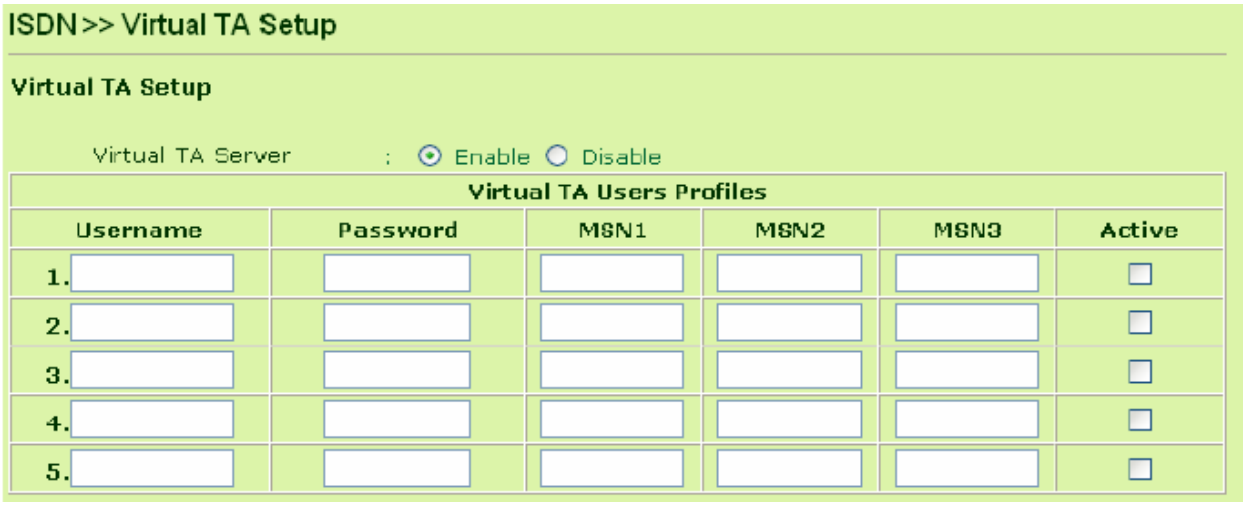
14.2 Instalace klienta Virtual TA

1. Vložte CD-ROM, které jste dostali s vaším směrovačem Vigor, do mechaniky a dvakrát klikněte na instalační soubor. Soubor Vsetup95.exe je určen pro prostředí Windows 95 OSR2.1 nebo vyšší, soubor Vsetup98.exe je určen pro prostředí Windows 98, 98SE a Me a soubor Vsetup2k.exe je určen pro prostředí Windows 2000.
2. Postupujte podle pokynů instalátoru na obrazovce. Po dokončení instalace budete vyzváni k restartování počítače. Kliknutím na tlačítko **OK** restartujte počítač.
3. Po restartování počítače se v navigační liště zobrazí ikona VT (obvykle v pravém dolní rohu obrazovky vedle hodin - viz. obrázek níže).

Pokud svítí text v ikoně ZELENĚ, znamená to, že klient Virtual TA je připojen k serveru Virtual TA a můžete spustit váš CAPI software pro přístup ke směrovači. Podrobnější informace najdete v uživatelské příručce k vašemu CAPI softwaru. Pokud svítí text uvnitř ikony ČERVENĚ znamená to, že klient ztratil spojení se serverem. Zkontrolujte správné zapojení jednotlivých koncových ethernetových zařízení.

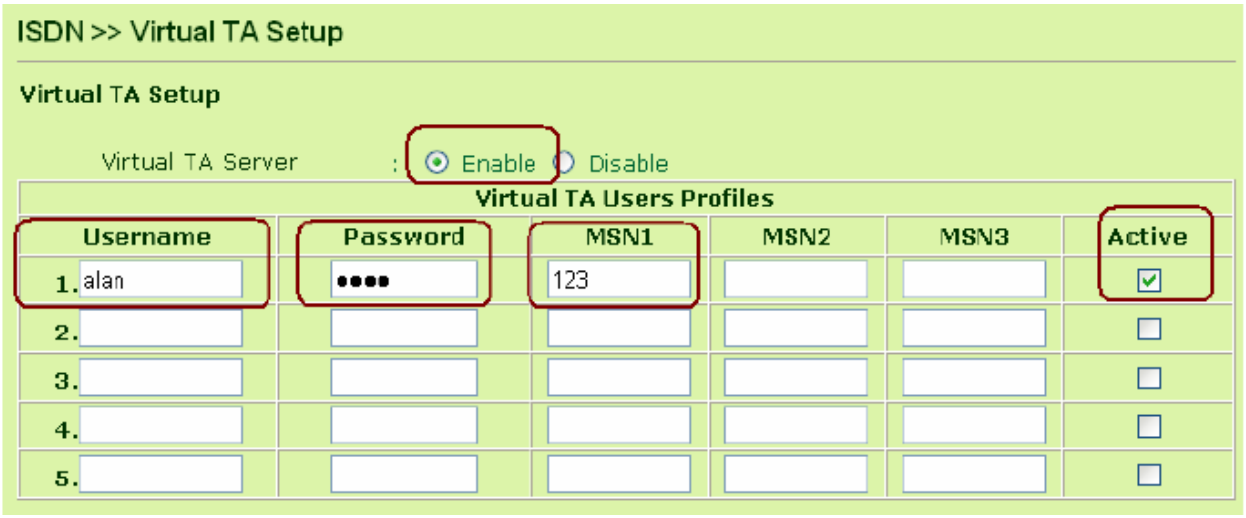
14.3 Nastavení klienta/serveru Virtual TA

Aplikace Virtual TA je založena na modelu klient/server. Proto její správné fungování musíte nastavit oba konce (klient a server).
Standardně je Virtual TA server povolen a pole pro zadání uživatelského jména a hesla (Username - Password) jsou prázdná. To znamená, že se k serveru může připojit jakýkoli klient Virtual TA. Pokud do polí Username/Password zadáte příslušná hesla, povolí server Virtual TA přístup pouze klientům s platným jménem a heslem. Nastavení aplikace Virtual TA je uvedeno níže.

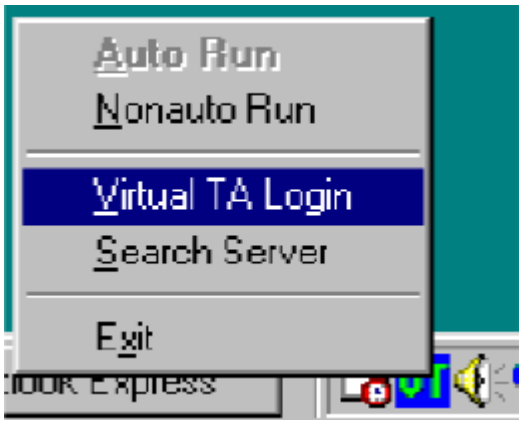


Virtual TA Server
Zapnout (Enable): Zaškrtněte pro aktivaci serveru.
Zakázat: Zaškrtněte pro deaktivaci serveru. Všechny aplikace Virtual TA budou zastaveny.
Virtual TA User Profiles (Uživatelské profily Virtual TA)
Username (uživatelské jméno): Zadejte uživatelské jméno daného klienta.
Password (heslo): Zadejte heslo daného klienta.
MSN1, MSN2, MSN3: MSN znamená Multiple Subscriber Number - Vícenásobné uživatelské číslo. To znamená, že můžete k jedné ISDN lince mít několik ISDN telefonních čísel. Tuto službu si musíte objednat u vašeho Telekomu. Zadejte uživatelské jméno daného klienta. Pokud službu MSN nevyužíváte, nechte toto pole prázdné.
Active (aktivní): Zaškrtněte toto pole pro povolení přístupu klienta k serveru.
Vytvoření uživatelského profilu
Pokud vytvoříte uživatelský účet, bude přístup k serverové straně Virtual TA omezen pouze na majitele příslušného uživatelského účtu.
V následujících odstavcích předpokládáme, že nemáte sjednanou MSN službu s vaším poskytovatelem služby ISDN.

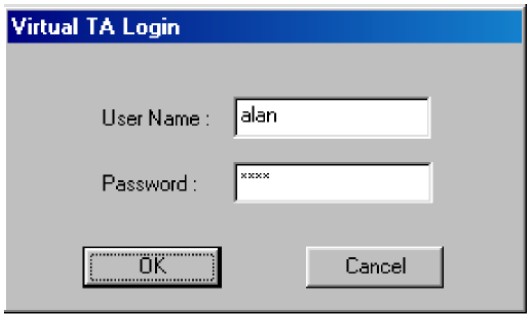
1. **Na straně serveru**: Klikněte na položku **Virtual TA (Remote CAPI) Setup** a vyplňte pole **Username** (uživatelské jméno) a Password (heslo). Zaškrtněte pole **Active** pro aktivaci účtu.



2. **Na straně klienta:** Klikněte pravým tlačítkem myši na ikonu VT. Zobrazí se následující rozbalovací nabídka.



3. Klikněte na položku **Virtual TA Login** (přihlásit se k Virtual TA) a otevře se toto okno pro přihlášení.



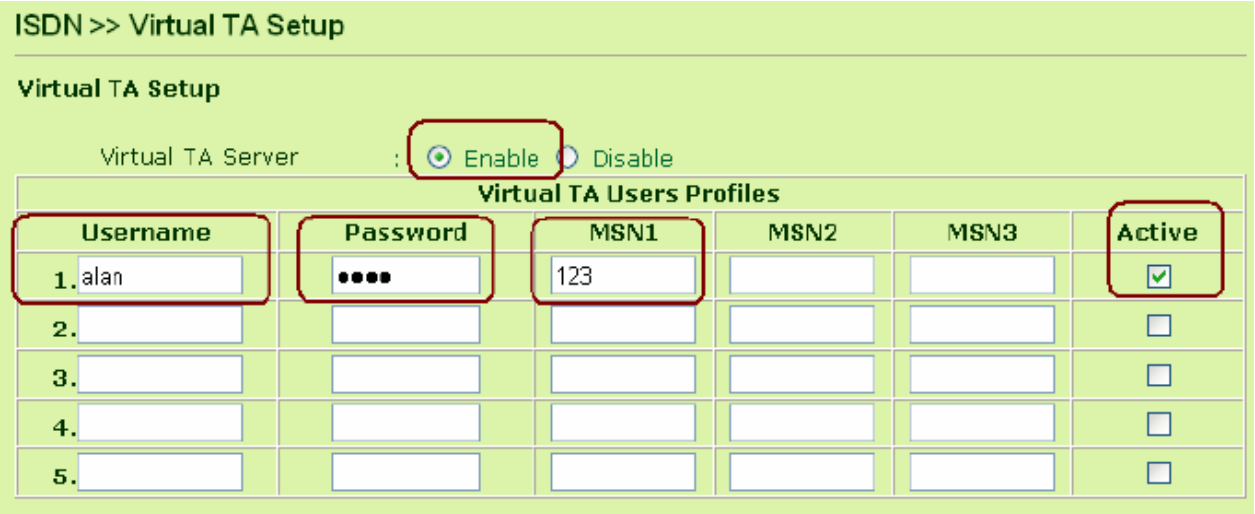
4. Zadejte Username/Password (uživatelské jméno/heslo) a klikněte na tlačítko **OK**. Po chvíli se text v ikoně VT zbarví dozelena.

Nastavení čísla MSN

Pokud využíváte službu MSN, můžete pro jednotlivým klientům přiřadit jednotlivá MSN čísla. V případě příchozího hovoru použije server uživatelské jméno a heslo klienta, kterému odpovídá příslušné MSN číslo. V

následujících odstavcích popíšeme nastavení MSN služby.

1. Předpokládejme, že chcete klientovi "alan" přidělit MSN číslo **123**.



2. Nastavte příslušné číslo v CAPI software. Až Virtual TA server pošle signál klientovi Virtual TA, zachytí tento signál také CAPI software. Bude-li zadáno nesprávné MSN číslo, software nepřijme příchozí volání.

Kapitola 15
Řízení volání a nastavení PPP/MP

15.1 Úvod

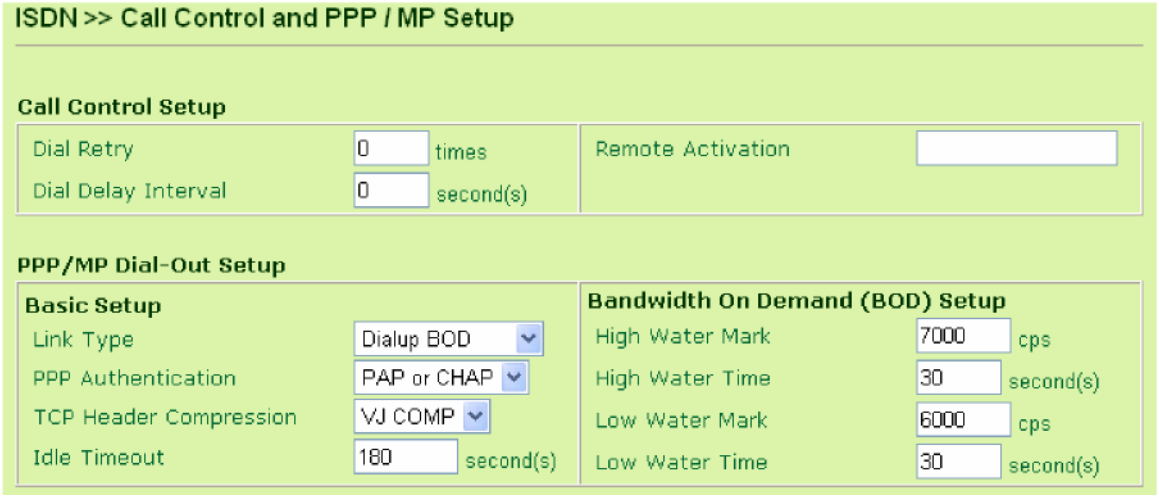
Pro správnou funkci některých aplikací je nutné, aby váš směrovač (týká se pouze směrovače s podporou ISDN) mohl být na dálku "požádán" o navázání spojení s vaším poskytovatelem přes rozhraní ISDN. Pokud se například potřebujete připojit z práce k domácímu počítači s vytáčeným ISDN přístupem k internetu, obvykle je vaše domácí připojení neaktivní, když jste v práci. Ovšem někdy si potřebujete do kanceláře poslat soubory z vašeho domácího počítače. Proto jsou směrovače Vigor vybaveny funkcí, která vám umožní "zavolat" směrovači a požádat jej o sestavení připojení k vašemu poskytovateli. Stejným způsobem se můžete připojit k vaší domácí síti a stáhnout si příslušné soubory. Je k tomu samozřejmě nutné, abyste měli pevnou IP adresu a sdíleli některé informace ze sítě s okolím (například FTP, www, apod.).

V následujících odstavcích si ukážeme jak nastavit řízení volání a nastavení protokolů PPP/MP. Pro nastavení použijte níže uvedenou cestu. **ISDN > Call Control and PPP/MP Setup**.

Funkce řízení volání a PPP/MP jsou k dispozici pouze u ISDN verze směrovače Vigor (tedy Vigor2500Vi). Pokud nemáte směrovač Vigor s ISDN rozhraním, nemusíte tuto kapitolu číst.

15.2 Nastavení

Po kliknutí na položku **Call Control and PPP/MP Setup**. se ve vašem prohlížeči objeví následující obrazovka.



Call Control Setup (nastavení řízení volání):

Na stránce nastavení **Call Control and PPP/MP Setup** jsou pole **Dial Retry (opakované vytáčení)** a **Dial Delay Interval (doba mezi opakovaným vytáčením)**. Tyto dva parametry představují globální nastavení vytáčeného přístupu ISDN.

Dial Retry: Určuje počet opakovaných vytáčení na odesílaný paket. Odesílaný paket je jakýkoli paket, směřující mimo místní síť. Standardní nastavení je neopakovat vytáčení. Pokud tento parametr nastavíte na 5, bude směrovač opakovat vytáčení 5x dokud se nepřipojí k vašemu poskytovateli nebo ke vzdálenému směrovači.

Dial Delay Interval: Zadejte interval mezi opakováním vytáčení. Standardně je tato hodnota nastavena na 0 sekund.

Remote Activation (vzdálená aktivace): Do pole Remote Activation zadejte telefonní číslo pro které bude aktivována funkce vzdálené aktivace. Pokud poté směrovač zachytí volání z čísla 12345678 okamžitě přeruší příchozí hovor a připojí se k vybranému poskytovateli připojení.

POZNÁMKA!
Ke správnému fungování této funkce je nutné **správné nastavení** v polích **Internet Access Setup > Dialing to a Single ISP.**

Nastavení PPP/MP

Základní nastavení :

Link Type (způsob připojení): Link Disable (zakázat vytáčení), Dialup 64 Kbps (vytáčení s rychlostí 64 kb/s - 1 kanál), Dialup 128 Kbps (vytáčení s rychlostí 128 kb/s - 2 kanály) a Dialup BOD (vytáčení BOD).

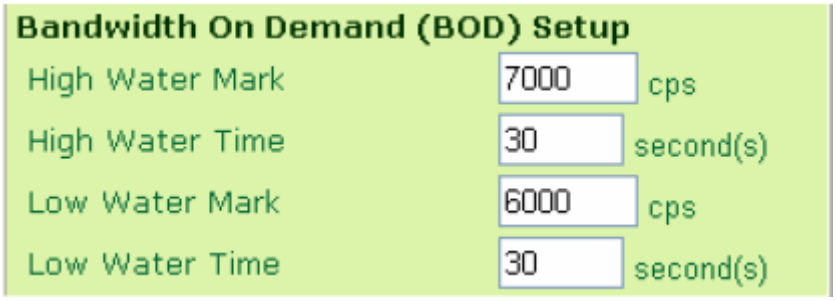
PPP Authentication (ověření PPP): Uveďte způsob ověření pro připojení PPP/MP. Doporučujeme nastavení PAP/CHAP pro pokrytí většiny možností.

Komprese záhlaví TCP: Pro záhlaví TCP/IP protokolu se používá VJ komprese. Aktivujte VJ kompresi pro zlepšení využití šířky pásma.

Idle Timeout (odpojení při nečinnosti): ISDN spojení bude ukočeno po nastavené době nečinnosti.

BOD Setup (nastavení BOD) :

BOD znamená šířka pásma na přání. Příslušné parametry jsou uvedeny níže.



Tyto parametry můžete nastavit pokud nastavíte **Link Type (typ připojení)** na **Dialup BOD (vytáčené BOD)**. Pokud nastavíte typ připojení na Dial BOD, bude ISDN linka obvykle při připojení na internet nebo do vzdálené sítě využívat jeden B kanál. Parametry nastavené ve výše uvedeném okně bude směrovač využívat k rozhodování o tom, kdy aktivovat/deaktivovat další B kanál. Parametr cps (znaků za sekundu - characters-per-second) měří celkové využití připojení.

High Water Mark a High Water Time: Do těchto polí se zapisují podmínky pro zapnutí dalšího kanálu. Pokud využití prvního kanálu přesáhne hodnotu uvedenou v poli **High Water Mark** a pokud je tento kanál používán po dobu delší než je hodnota uvedená v poli **High Water Time** bude druhý kanál aktivován. Celková rychlost připojení tedy bude 129 kb/s (dva B kanály).

Low Water Mark a Low Water Time: Do těchto polí se zapisují podmínky pro vypnutí druhého kanálu. Pokud využití dvou B kanálů klesne pod hodnotu uvedenou v poli **Low Water Mark** a pokud jsou tyto kanály současně využívány po dobu delší než **High Water Time** bude kanál vypnut. Rychlost připojení tedy klesne na 64 kb/s (jeden B kanál).

Pokud nevíte zda váš poskytovatel připojení podporuje službu BOD a/nebo používání protokolů ML-PPP, obraťte se nejprve na vašeho poskytovatele, prodejce či na naše centrum podpory support@draytek.com .

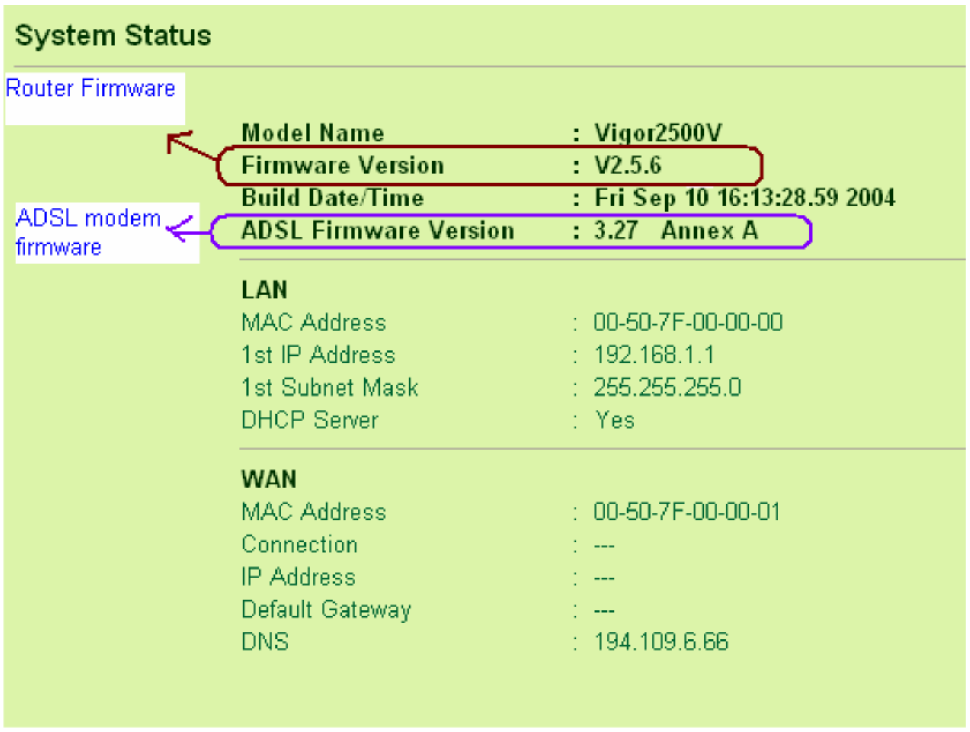
Kapitola 16
Stav systému

16.1 Úvod

Okno **System Status (stav systému)** poskytuje základní informace o nastavení směrovače Vigor, včetně informací o rozhraní LAN a WAN. Rovněž zde najdete informace o aktuální verzi firmware směrovače a aktuální verzi firmware ADSL modemu.

16,2 Popis obrazovky Stav připojení

Kliknutím na položky **System Maintenance > Online Status** se zobrazí níže uvedená obrazovka. Níže uvedneé hodnoty jsou ukázkové hornoty pro směrovač Vigor 2500V.



Kapitola 17
Zálohování nastavení

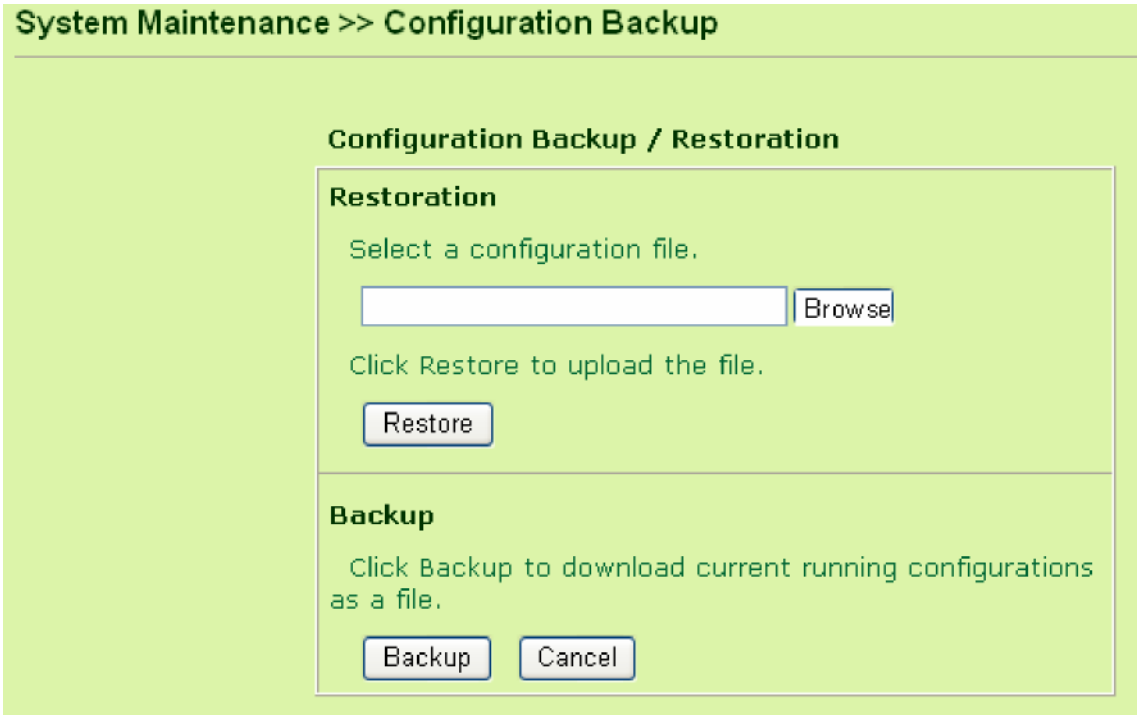
17.1 Úvod

Někdy je užitečné uložit si aktuální nastavení směrovače do souboru a ten uchovat pro pozdější potřebu. Směrovače Vigor nabízí jednoduchý a pohodlný způsob zálohování aktuálního nastavení a načítání nastavení prostřednictvím webového rozhraní.

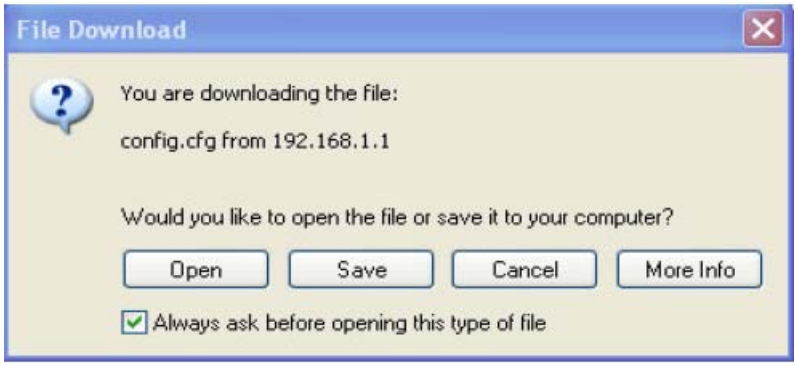
17.2 Použití

17.2.1 Zálohování stávajícího nastavení (Configuration Backup)

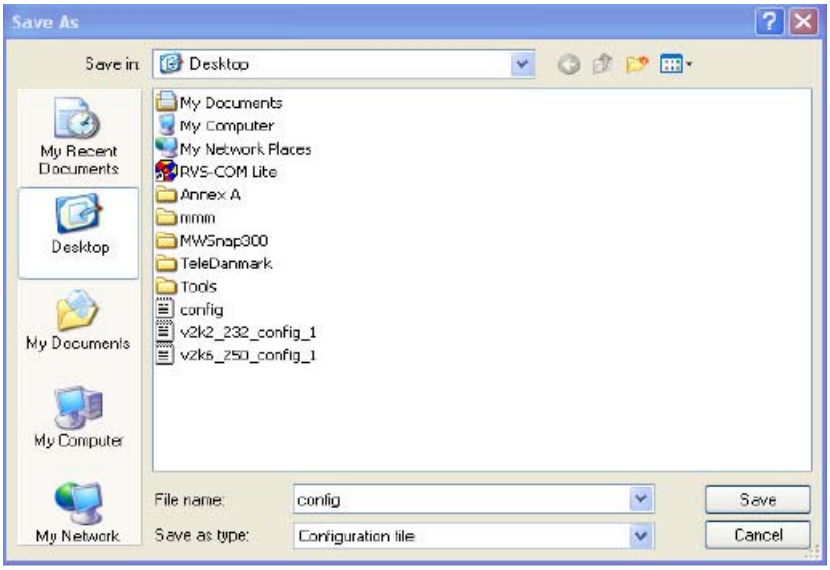
1. Klikněte na položky **System Maintenance > Configuration Backup**. Zobrazí se níže uvedená obrazovka.



2. Klikněte na tlačítko **Backup** pro stažení aktuálního nastavení.



3. Kliknutím na tlačítko **OK** uložíte aktuální nastavení jako soubor. Standardně je soubor pojmenován jako config.cfg. Název souboru si však můžete libovolně upravit.

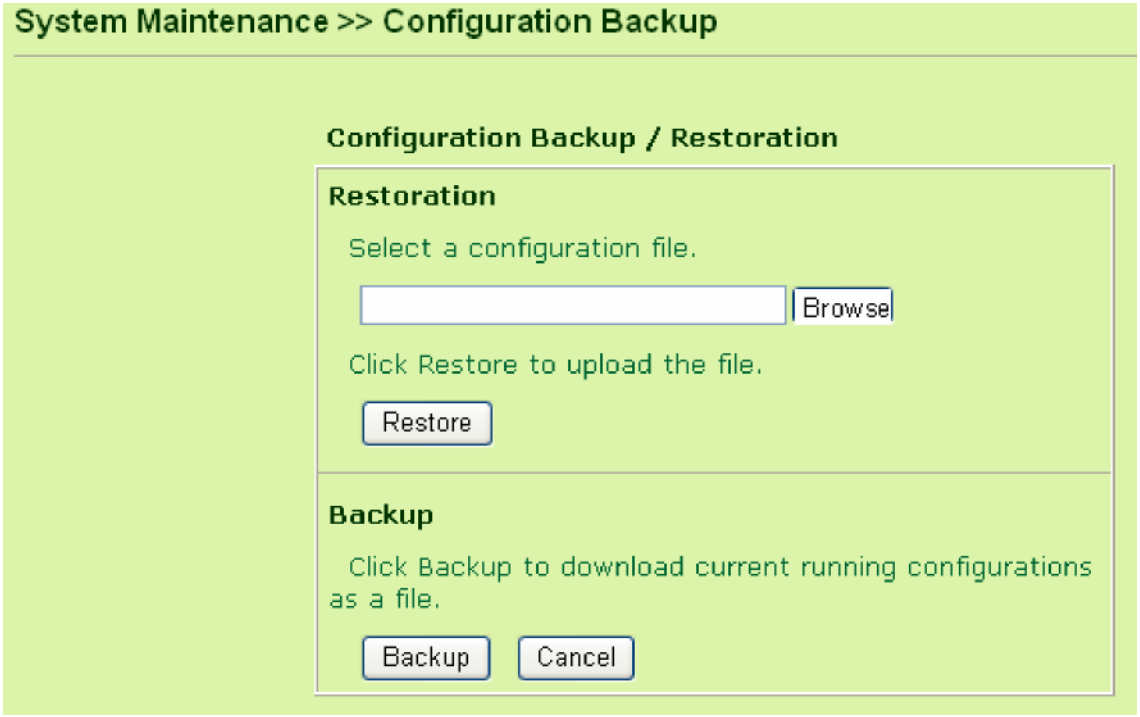


4. Klikněte na tlačítko **Save (uložit)**. Soubor s aktuálním nastavením (config.cfg) se automaticky stáhne a uloží na váš počítač.

POZNÁMKA!
Ve výše uvedeném příkladě jsme ukázali postup pro operační systém **Windows**. Nicméně uložení aktuálního nastavení je možné i na platformách **Mac** nebo **Linux**, pouze se zobrazí jiná okna.

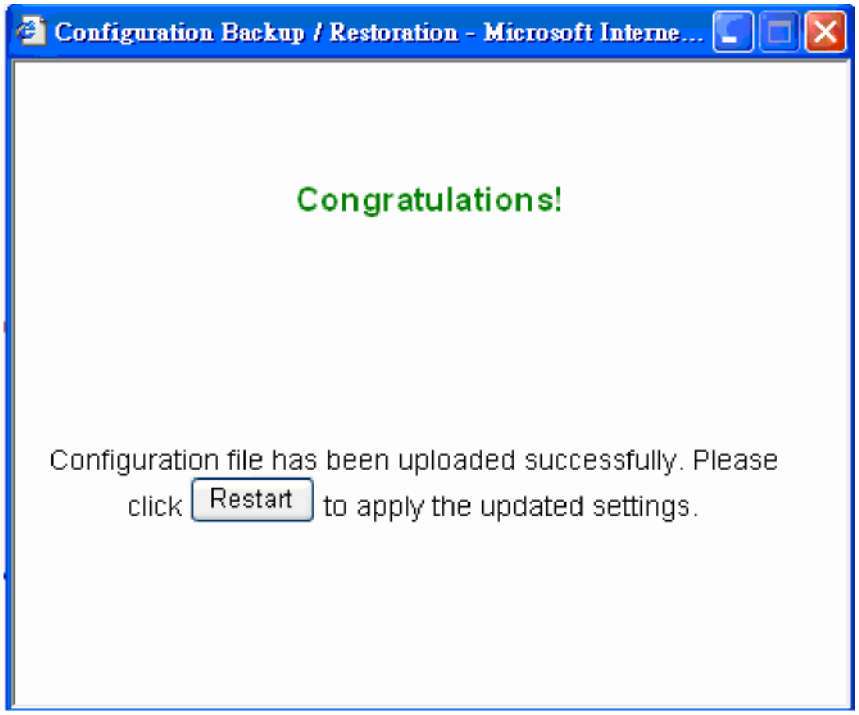
17.2.2 Obnovení nastavení pomocí staženého konfiguračního souboru

1. Klikněte na položky **System Maintenance >Configuration Backup**. Zobrazí se níže uvedená obrazovka.
2. Klikněte na tlačítko **Browse** (**Procházet**) a vyhledejte soubor s uloženým nastavením směrovače.



3. Klikněte na tlačítko **Restore (obnovit)**, počkejte několik sekund na zobrazení následující obrazovky o úspěšném obnovení nastavení.

4. Klikněte na tlačítko **Restart (restartovat)** a počkejte několik sekund na restartování směrovače s aktualizovaným nastavením.



Kapitola 18
SysLog / upozorňování e-mailem

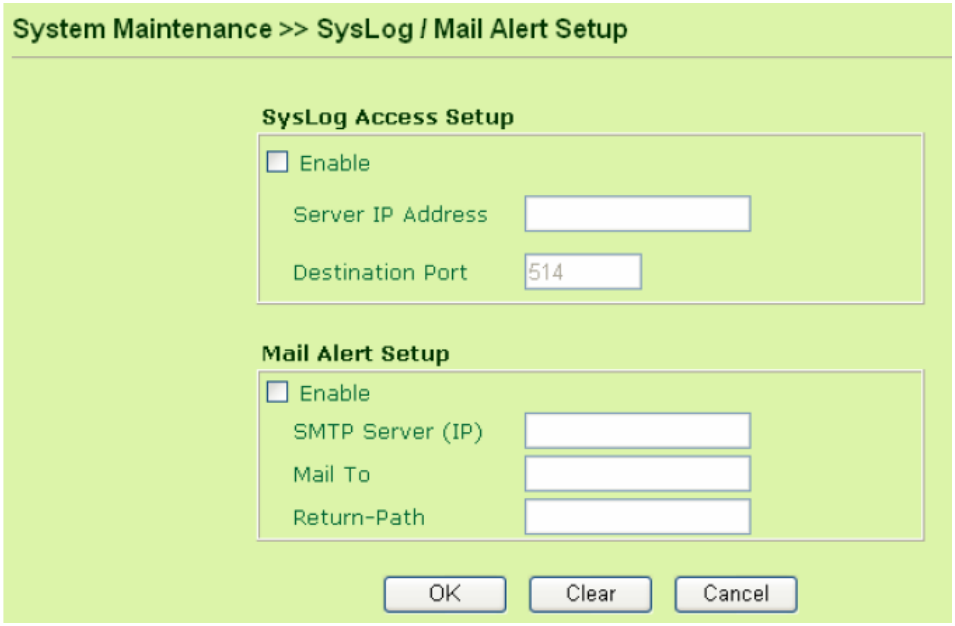
18.1 Úvod

Syslog je velmi populární utilita zejména v prostředí UNIXu. Pokud chcete sledovat činnost směrovače, můžete spustit program s názvem Syslog Daemon, který monitoruje a ukládá informace o všech činnostech směrovače. Daemona může běžet na místním nebo vzdáleném počítači či kdekoli na internetu. Směrovače Vigor navíc nabízí funkci upozorňování e-mailem (Mail Alert), která zabalí syslog soubory do zprávy elektronické pošty a odešle je na uživatelem nadefinované e-mailové adresy. V následujících odstavcích si ukážeme nastavení funkcí syslog a upozorňování e-mailem. Pro přístup k obrazovce nastavení použijte následující cestu:

System Maintenance > Syslog/Mail Alert

18.2 Nastavení

Poté co kliknete na položku **Syslog / Mail Alert Setup** zobrazí webovský konfigurátor níže uvedené okno. Jak vidíte, jsou zde k dispozici dvě funkce: jedna pro nastavení přístup k souborům syslog (**SysLog Access Setup**) a druhá pro nastavení upozorňování e-mailem (**Mail Alert Setup**).



Syslog Access Setup

1. Tuto službu aktivujete zaškrtnutím pole **Enable (Aktivovat)**.
2. **Server IP Address**: zadejte IP adresu, na kterou budou zasílány všechny syslog zprávy.
3. **Destination Port (cílový port)**: Zadejte číslo portu UDP daného syslog serveru. Přednastavená hodnota je 514.

Mail Alert Setup

1. Tuto službu aktivujete zaškrtnutím pole **Enable (Aktivovat)**.
2. **SMTP Server (IP)**: Zadejte IP adresu SMTP serveru, který je schopen rozesílat maily z vašeho směrovače přímo do schránek daných osob.
3. **Mail To (příjemce mailu)**: Zadejte e-mailovou adresu na kterou budou zasílány zprávy syslog. Můžete například zadat e-mailovou adresu správce sítě, který bude získané syslog zprávy prohlížet a analyzovat.
4. **Return-Path (návratová adresa)**: Zadejte e-mailovou adresu (jinou než v předchozím případě) na kterou budou zaílány syslog zprávy v případě, že mailbox výše uvedeného příjemce zprávy nebude fungovat.

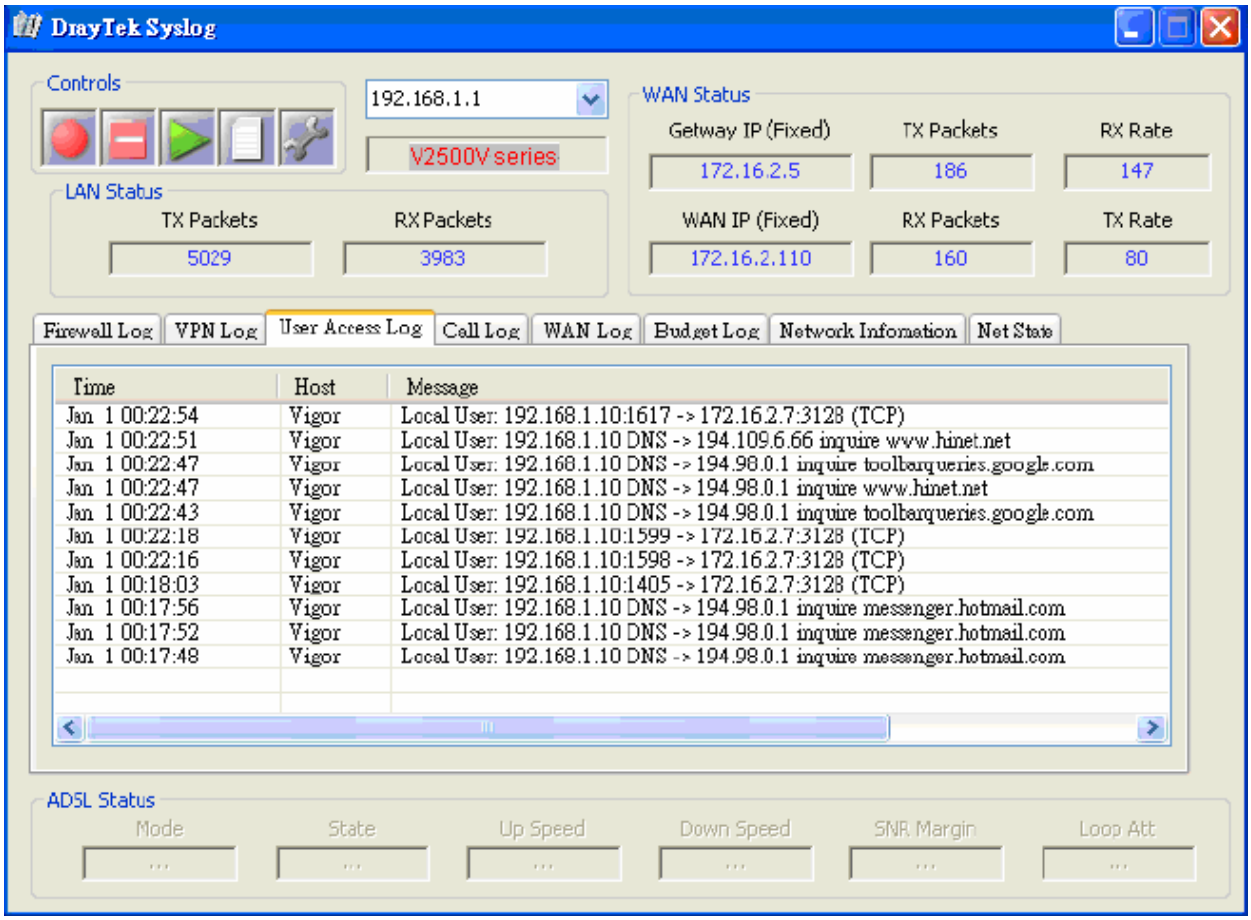
POZNÁMKA!

Funkce upozorňování e-mailem zatím umožňuje pouze zasílání syslog zpráv o obraně před útoky DoS (Denial of Service).

18.3 Příklad

Váš směrovač Vigor bude serveru zasílat velké množství syslog zpráv. Některé ukázky syslog zpráv a jejich formátů jsou uvedeny níže.

Příklad logu s informacemi o uživatelských přístupech:


DrayTek Syslog
Controls
192.168.1.1
V2500V series
LAN Status
TX Packets
RX Packets
5029
3983
WAN Status
Getway IP (Fixed)
TX Packets
RX Rate
172.16.2.5
186
147
WAN IP (Fixed)
RX Packets
TX Rate
172.16.2.110
160
80
Firewall Log
VPN Log
User Access Log
Call Log
WAN Log
Budget Log
Network Infomation
Net State
Time
Host
Message
Jan 1 00:22:54 Vigor Local User: 192.168.1.10:1617 -> 172.16.2.7:3128 (TCP)
Jan 1 00:22:51 Vigor Local User: 192.168.1.10 DNS -> 194.109.6.66 inquire www.hinet.net
Jan 1 00:22:47 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan 1 00:22:47 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire www.hinet.net
Jan 1 00:22:43 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan 1 00:22:18 Vigor Local User: 192.168.1.10:1599 -> 172.16.2.7:3128 (TCP)
Jan 1 00:22:16 Vigor Local User: 192.168.1.10:1598 -> 172.16.2.7:3128 (TCP)
Jan 1 00:18:03 Vigor Local User: 192.168.1.10:1405 -> 172.16.2.7:3128 (TCP)
Jan 1 00:17:56 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan 1 00:17:52 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan 1 00:17:48 Vigor Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
ADSL Status
Mode
State
Up Speed
Down Speed
SNR Margin
Loop Att

Kapitola 19
Nastavení času

19.1 Úvod

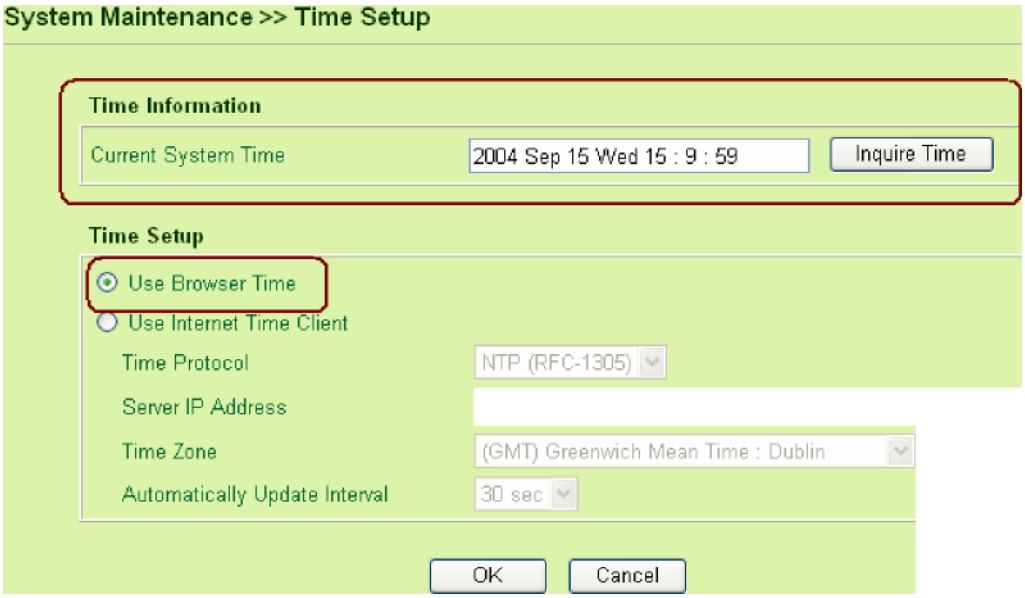
Chcete-li používat jakoukoli funkci směrovače závislou na čase (například časový plán vytáčení (**Call Schedule**) či filtrování obsahu URL adres (**URL Content filtering**)) musíte nejprve nastavit správný čas.
Směrovač nabízí dvě možnosti nastavení času. Jednou z možností je nastavení času na čas systémových hodin vyšeho počítače prostřednictvím HTTP protokolu. Druhou možností je potom nastavit čas směrovače automaticky pomocí protokolu NTP přes internet.
Pokud v nabídce **Time Setup** stiskněte tlačítko **Inquire Time (Dotázat se na čas)** nastaví se systémové hodiny směrovače na stejný čas, na který je nastaven systémový čas vašeho PC. Při výpadku napájení nebo resetu směrovače dojde rovněž k vymazání času vašeho směrovače. Proto také můžete využít funkci automatického nastavení času pomocí NTP serveru na internetu. Automatické nastavení času pomocí NTP serveru funguje pouze při připojení na internet (směrovače se automaticky nepřipojí k internetu za účelem automatického nastavení času).

19.2 Nastavení

19.2.1 Nastavení systémových hodin pomocí internetového prohlížeče

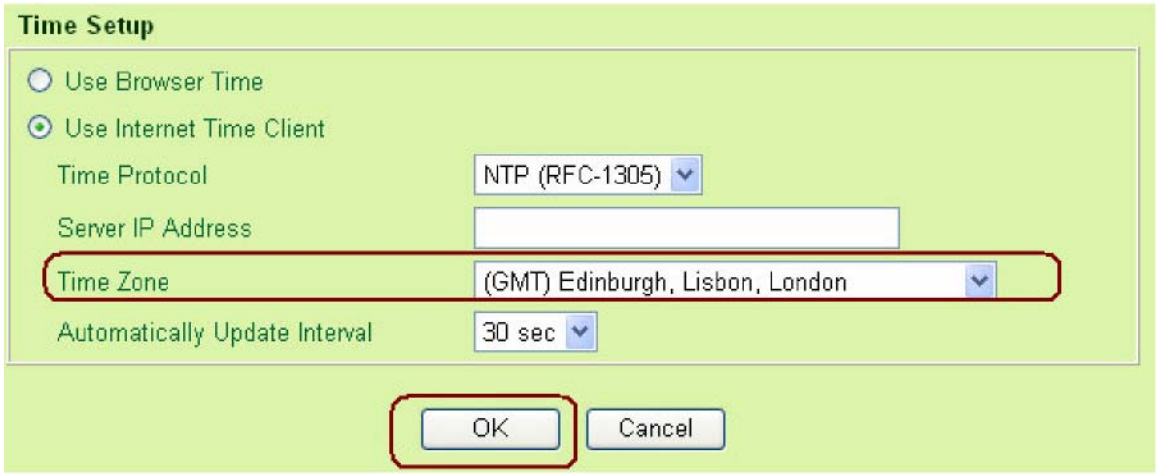
1. Než začnete nastavovat čas pomocí internetového prohlížeče, musíte se ujistit zda je čas na vašem počítači nastaven správně nebo ne. V nabídce **System Maintenance** klikněte na položku **Time Setup**.

Pokud v nabídce **Time Setup** stiskněte tlačítko **Inquire Time (Dotázat se na čas)** nastaví se systémové hodiny směrovače na stejný čas, na který je nastaven systémový čas vašeho PC.

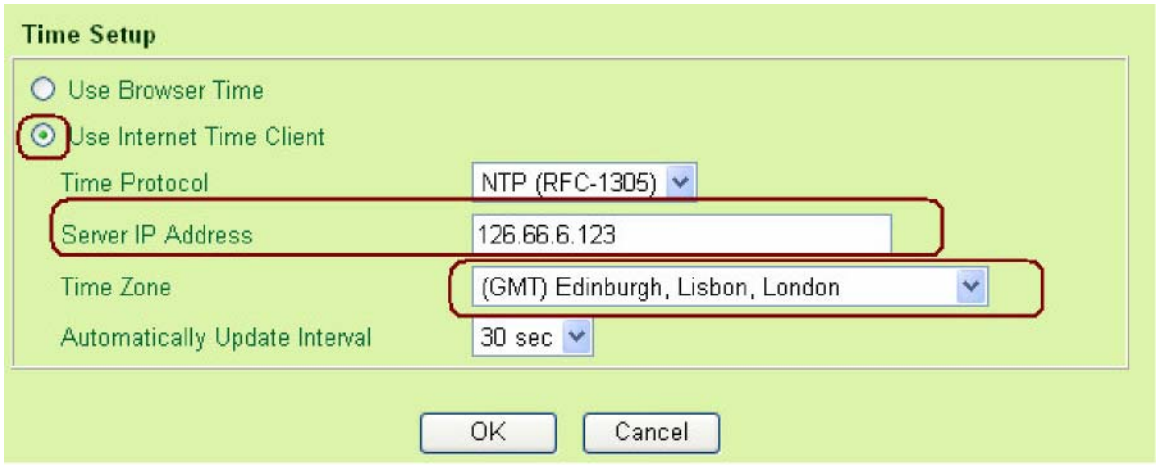


19.2.2 Použij NTP server na internetu (časový server) pro automatické nastavení času

1. Než přistoupíte k vlastnímu nastavení přesvědčte se, že časový server funguje správně. Pokud je časový server umístěn na internetu, ujistěte se, že váš směrovač má správné nastavené připojení k internetu. V nabídce **System Maintenance** klikněte na položku **Time Setup**.
2. Zaškrtněte položku **Use Internet Time Client (používat časový server na internetu)**, do pole časový protokol (**Time Protocol**) zadejte **NTP**, zadejte IP adresu časového serveru do pole **Server IP Address**, do pole časové pásmo (**Time Zone**) zvolte příslušné časové pásmo a nastavte periodicitu automatické aktualizace času v poli **Automatically Update Interval**. Příklad nastavení ukazuje následující obrazovka.



3. Klikněte na tlačítko **OK**, počkejte několik sekund, než klient stáhne správný čas ze serveru. Klikněte znovu na položku **Time Setup** a kliknutím na položku **Current System Time** (aktuální systémový čas) se přesvědčte o správnosti nastavení.



Kapitola 20
Vzdálená správa směrovače

20.1 Úvod

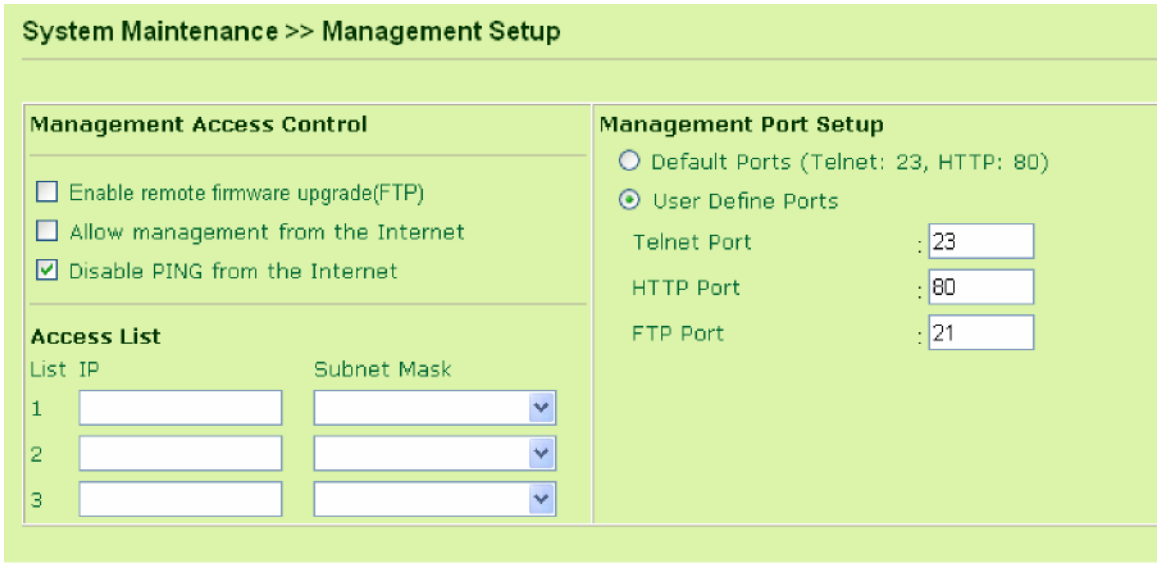
Standardně můžete funkce vašeho směrovače ovládat prostřednictvím libovolného Telnet klienta nebo internetového prohlížeče na libovolném operačním systému. Není k tomu třeba žádný další software ani utility. Nicméně za určitých okolností máte možnost se rozhodnout zda povolíte správu směrovače přes internet nebo ne (můžete například změnit čísla portů pro Telnet či HTTP server, vytvářet seznamy s přístupovými právy, apod.) Můžete například nastavit, aby technik nebo zaměstnanec technické podpory měli přístup ke vzdálené správě směrovače, mohli provádět změny nastavení a prohlížet si příslušné log soubory zobrazující aktuální stav směrovače.

Vzdálená správa může být prováděna buď přes web (internetový prohlížeč) nebo přes telnet. Je samozřejmě velmi důležité pro váš směrovač nastavit správcovské heslo. Jinak totiž může k vašemu směrovači přistupovat kdokoli ze kteréhokoli místa na světě. V menu můžete nastavit také směrovači zakázat, aby odpovídal na "prozvánění (pingování)" z internetu. Tím opět zvýšíte zabezpečení vaší sítě, protože někteří uživatelé se zkoušejí připojovat na veřejné IP adresy a pokud zakážete vašemu směrovači aby odpovídal na prozvánění, bude pro takové útoky "neviditelný".

Z bezpečnostního hlediska je také užitečné omezit počet uživatelů s administrátorskými právy ke směrovači. Pokud specifikujete interní či externí IP adresy mající právo přístupu ke správě směrovače, budou mít pouze uživatelé s těmito IP adresami přístup k nastavení směrovače. Abyste nepřišli o možnost správy směrovače (funkce směrování bude normálně fungovat), ***NESMÍTE ZAPOMENOUT*** nastavit do přístupových práv pro správu směrovače také vaši IP adresu/podsíť.

20.2 Nastavení

Klikněte na položku **Management Setup (Nastavení vzdálené správy směrovače).** Zébrazí se následující okno.

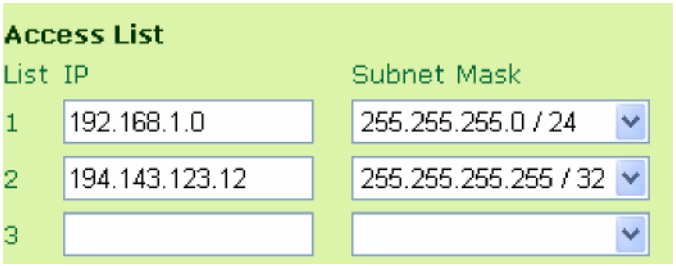


20.2.1 Management Access Control (Řízení přístupu ke správě)

Enable remote firmware update (FTP) - Povolit vzdálenou aktualizaci firmware přes FTP: Toto pole zaškrtněte pokud chcete povolit vzdálenou aktualizaci firmware přes FTP (File Transfer Protocol).
Allow management from the Internet - Povolit správu přes internet: Toto pole zaškrtněte pokud chcete správcům systému povolit vzdálenou správu vašeho směrovače přes internet. Standardně je zvolena možnost NEPOVOLOVAT.
Disable PING from the Internet (Odmítnout prozváněcí (ping) pakety z internetu): Pokud chcete odmítnout všechny prozváněcí pakety z internetu, zaškrtněte toto pole. Z bezpečnostních důvodů je tato funkce ve standardním nastavení aktivována.

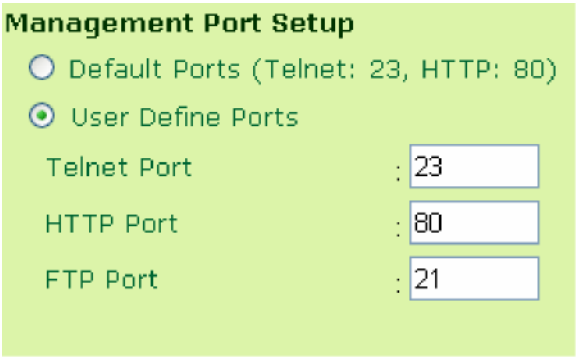
20.2.2 Access List - Seznam uživatelů s povolením přístupu

Zde můžete nastavit práva vzdáleného přístupu ke směrovači. Můžete zadat maximálně 3 IP adresy/masky podsítě).
IP: Zadejte IP adresy ze kterých bude umožněn vzdálený přístup ke směrovači.
Subnet Mask (Maska podsítě): Zadejte masku podsítě ze které bude povolen vzdálený přístup ke směrovači.



20.2.3 Nastavení portů pro správu

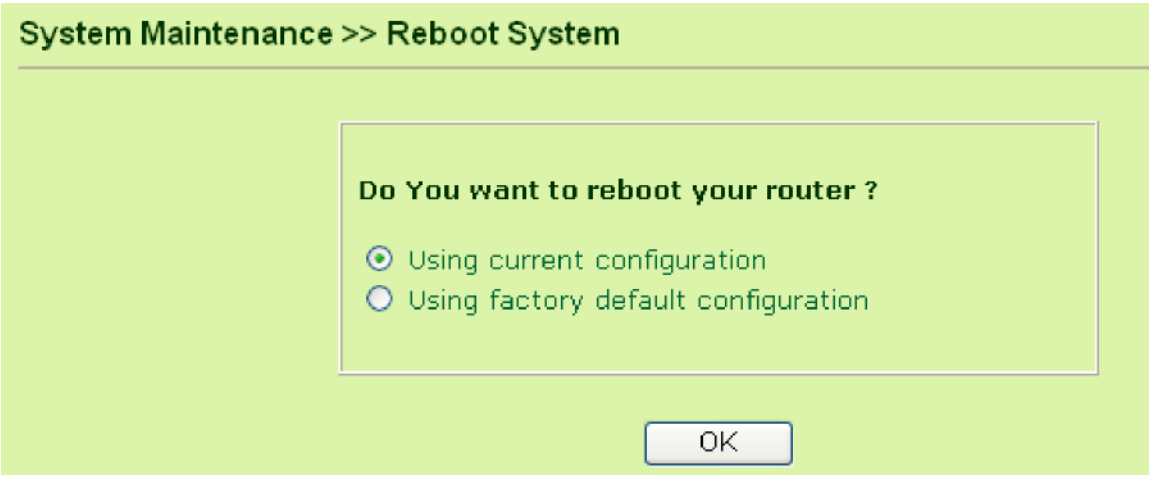
Default Ports (přednastavené porty): Zaškrtnutím této položky budou použity předdefinovaná čísla portů pro Telnet a HTTP servery.
User Defined Ports (uživatelem definované porty): Po zaškrtnutí této položky nastavte uživatelská čísla portů pro Telnet a HTTP servery.



Kapitola 21
Restart systému / aktualizace firmware

21.1 Restart systému

Pomocí webovského konfigurátoru můžete váš směrovač restartovat. V nabídce ***System Maintenance*** klikněte na položku ***Reboot System*** a zobrazí se vám následující stránka.



Máte dvě možnosti restartování:

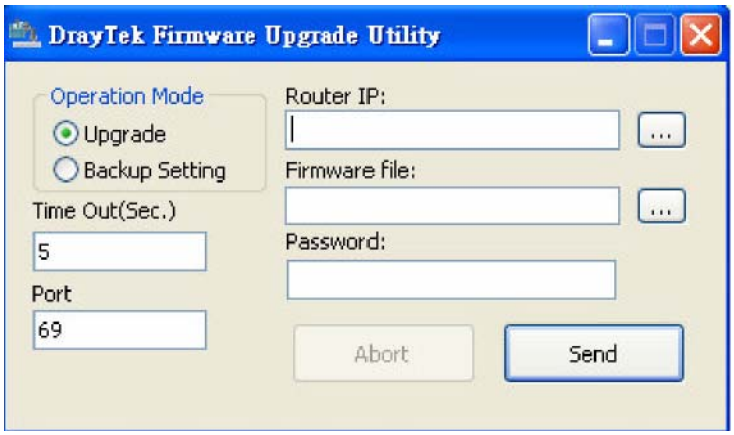
1. **Using current configuration - restart se zachováním aktuálního nastavení**: Pokud chcete po restartu zachovat aktuální nastavení vašeho směrovače, zaškrtněte pole **Using current configuration** a klikněte na tlačítko **OK**.
2. **Using factory default configuration - restart s nastavením na výrobcem přednastavené hodnoty**: Pokud chcete aktuální nastavení smazat a provést restart s nastavením na výrobcem přednastavené hodnoty, zaškrtněte pole **Using factory default configuration** a klikněte na tlačítko **OK**.

Během 3 - 5 sekund bude směrovač restartován.

21.2 Firmware Upgrade (TFTP Server) - Aktualizace Firmware (TFTP server)

Než přistoupíte k aktualizaci firmware,nainstalujte si balík nástrojů Router Tools z přiloženého CD. Nástroj pro aktualizaci firmware (Firmware Upgrade Utility) je součástí balíku Router Tools. Postupujte podle níže uvedených pokynů. V níže uvedeném postupu jsou použity ukázkové hodnoty jako názorný příklad. Níže uvedený příklad platí pro operační systém Windows.

1. Stáhněte si poslední verzi firmware z webovských stránek firmy DrayTek, nebo z firemního FTP serveru. Stránky firmy DrayTek najdete na ***www.draytek.com*** (nebo stránky vašeho místního distributora) a FTP server je ***ftp.draytek.com***.
2. Klikněte ve Windows na **Start > Programy > Router Tools > Router Firmware Upgrade Utility** a spusťte nástroj pro upgrade Firmware (**Router Firmware Upgrade Utility**).



Klikněte na tlačítko **Procházet** a vyhledejte soubor s novou verzí firmware. Program vyhledá všechny směrovače Vigor připojené k vaší síti LAN a zobrazí je podle IP adres. Vyberte IP adresu příslušného směrovače a klikněte na tlačítko

Upgrade (Aktualizovat). Do pole heslo (password) zadejte příslušné heslo (nebo klikněte na **OK**, pokud heslo nepoužíváte). Aktualizace bude zahájena a její průběh můžete sledovat na obrazovce vašeho počítače. Po dokončení aktualizace počkejte asi 30 sekund, než bude směrovač znovu připraven k provozu (dioda ACT na předním panelu směrovače Vigor bude opět normálně blikat).

Kapitola 22
Diagnostika

22,1 Úvod

Diagnostické nástroje směrovač nabízí užitečné funkce pro sledování funkce směrovače a diagnostiku problémů. Budete-li mít nějaké technické dotazy či problémy, můžete nám (nebo vašemu prodejci) zaslat obrazovku s údaji vygenerovanou diagnostickými nástroji směrovače.
Na obrázku níže je uveden přehled diagnostických nástrojů směrovače Vigor.

22.2 Pokud je váš směrovač řady Vigor2500V: PPPoE / PPPoA

Broadband Access Mode/Status	---
Internet Access	>> Dial PPPoE/PPPoA
WAN IP Address	---
Drop Connection	>> Drop PPPoE/PPPoA

Refresh - Obnovit: Kliknutím na toto tlačítko se stránka znovu načte s aktuálními informacemi.
Broadband Access Mode/Status - režim/stav širokopásmového přístupu: Zobrazí režim a stav širokopásmového přístupu. Je-li širokopásmové připojení aktivní, zobrazí se buď PPPoE, PPTP, Static IP, nebo DHCP Client, podle režimu širokopásmového přístupu. Pokud není navázáno připojení, zobrazí se "---".
WAN IP Address (WAN IP adresa): WAN IP adresa pro aktuální aktivní připojení.
Dial PPPoE or PPTP (připoj se k PPPoE nebo PPTP): Klikněte pokud chcete, aby se směrovač připojil k PPPoE nebo PPTP.
Drop PPPoE or PPTP (odpoj se od PPPoE nebo PPTP): Klikněte pokud chcete, aby se směrovač odpojil od právě aktivního připojení k PPPoE nebo PPTP.

22,3 Pokud je váš směrovač řady Vigor2500Vi:

Objeví se tyto údaje o ISDN:

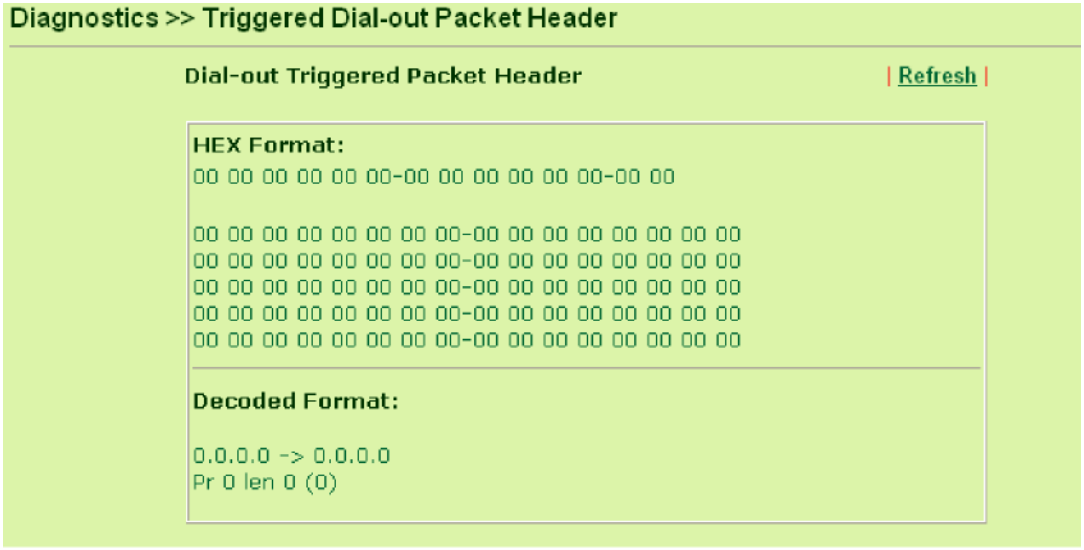
ISDN Link Status		DOWN
Internet Access	>> Dial ISDN	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	>> Drop B1	>> Drop B2

ISDN Link Status - stav připojení ISDN: Je-li připojení aktivní zobrazí se v tomto okně slovo UP. V opačném případě se zobrazí DOWN.
Dial ISDN (vytočit číslo ISDN): Kliknutím se směrovač připojí k právě vybranému poskytovateli připojení. Nastavení připojení provedete v menu **ISDN > Dial to a Single ISP**.

Activity (aktivita): Zobrazí se název připojení pro každý B kanál. Pokud B kanál není připojen, zobrazí se slovo **Idle**.
Drop B1 (Odpojit B1): Klikněte pro odpojení kanálu B1.
Drop B2 (Odpojit B1): Klikněte pro odpojení kanálu B2.

22.4 Triggered Dial-out Packet Header (Záhlaví posledního paketu, který "požádal" o sestavení připojení)

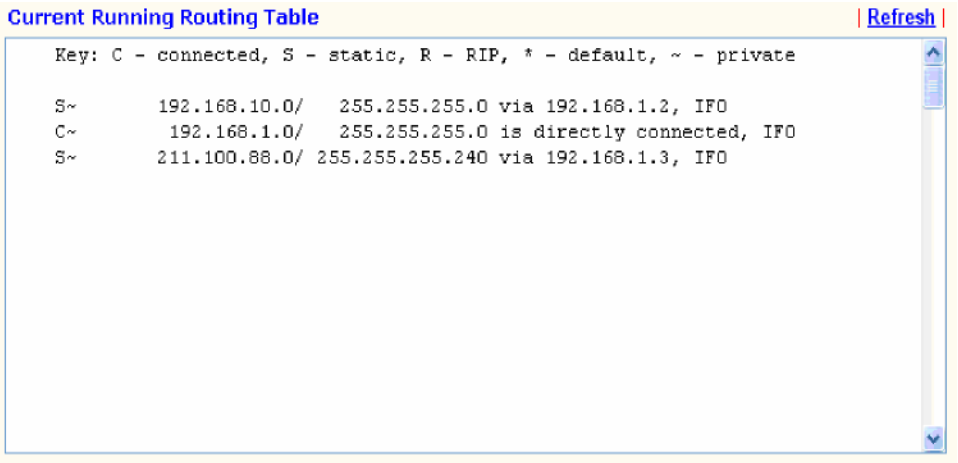
Tato obrazovka ukazuje záhlaví posledního IP paketu, který "požádal" směrovač o sestavení připojení (volání ven).



22.5 Routing Table - Směrovací tabulka

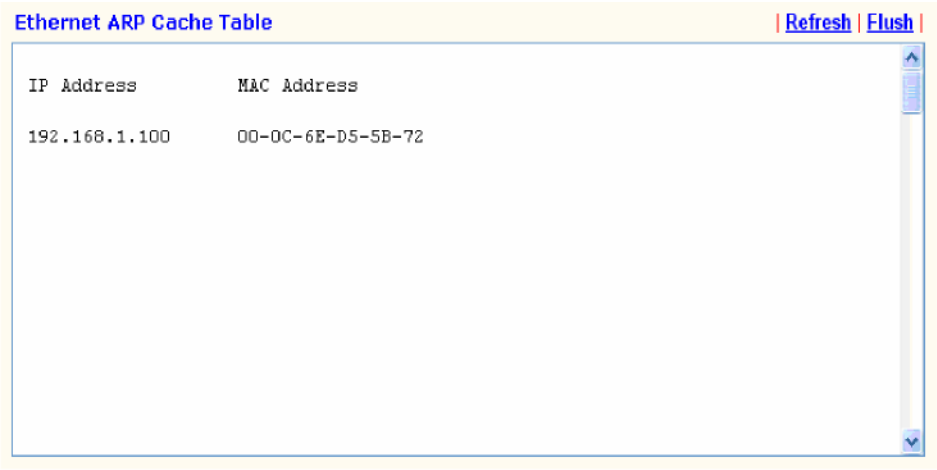
Kliknutím na položku **Routing Table** se zobrazí směrovací tabulky směrovače.
V této tabulce jsou aktuální informace o IP směrování uložené ve směrovači. Vlevo vedle každého pravidla najdete příznak. Význam těchto příznaků je následující:
C --- Přímo připojen.
S --- Statická trasa.
R --- RIP.
***** --- Defaultní trasa.
~ --- Směrování na privátní domény.

V pravé části každého pravidla najdete následující identifikační znaky.
IF0 --- místní síť LAN.
IF3 --- WAN rozhraní.



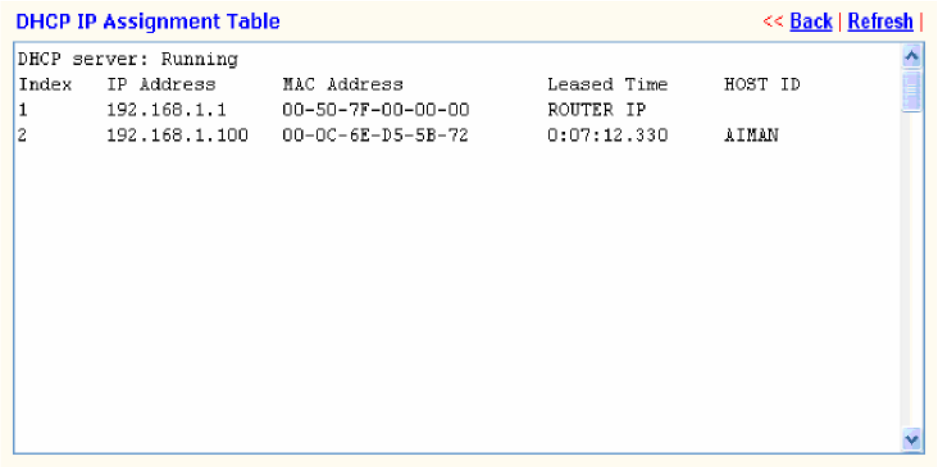
22.6 ARP Cache Table - Cache tabulka ARP

Kliknutím na položku ARP Cache Table se zobrazí obsah cache protokolu ARP (Address Resolution Protocol) tak jak je uložen v paměti směrovače. Tabulka níže zobrazuje mapování mezi MAC adresou (Ethernetovou hardwarovou adresou) a IP adresou.



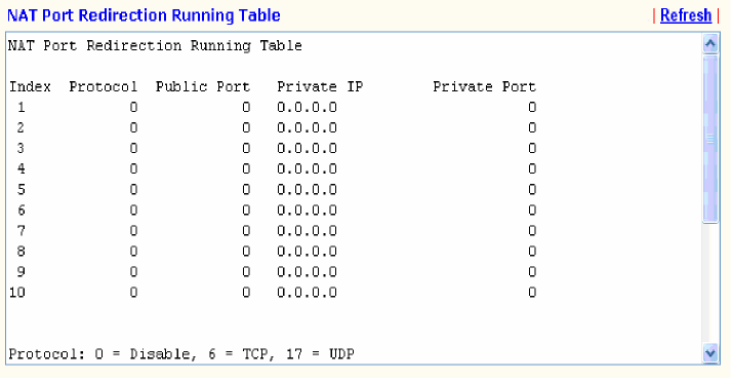
22.7 DHCP Table - Tabulka DHCP

Tato tabulka zobrazuje informace o přidělení IP adres. Tato informace je užitečná například pro diagnostiku síťových problémů, konfliktů mezi IP adresami, apod.



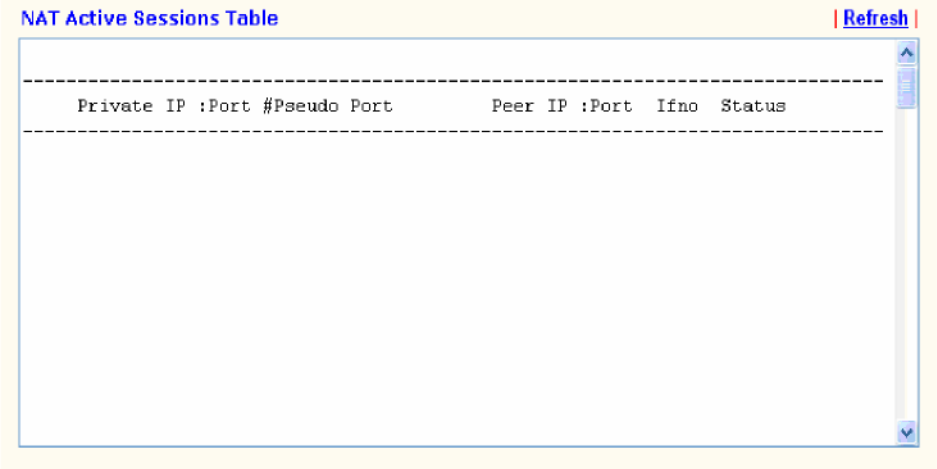
22.8 NAT Port Redirection Table - Tabulka přesměrování portů NAT

Pokud jste prováděli změny v nastavení přesměrování portů (Port Redirection) v menu **NAT Setup**, klikněte na tuto položku pro zobrazení níže uvedené tabulky, kde si můete ověřit správnost nastavení přesměrování jednotlivých čísel portů na jednotlivé uživatele.



22.9 NAT Active Sessions Table - Tabulka aktivních sessions (NAT)

Protože směrovač přistupuje k internetu přes engine překladu síťové adresy (**NAT engine**) zobrazuje níže uvedená tabulka informace o aktivních odchozích sessions.



Jednotlivé aktivní sessions jsou uvedeny v řádcích. Zobrazují se následující informace:
Private IP, Port (privátní IP, port): IP adresy a čísla portů interních uživatelů (počítačů).
#Pseudo Port: Číslo veřejného portu.
Peer IP, Port: IP adresy a čísla portů uživatelů (počítačů) protistrany.
Ifno: Znamená číslo rozhraní. Níže uvádíme jednotlivé možnosti pro tento parametr:
0 --- rozhraní LAN.
3 --- rozhraní WAN.
V případě technických dotazů ohledně používání diagnostických nástrojů (**Diagnostic Tools**) kontaktujte vašeho místního prodejce, nebo přímo nás na adrese support@draytek.com.

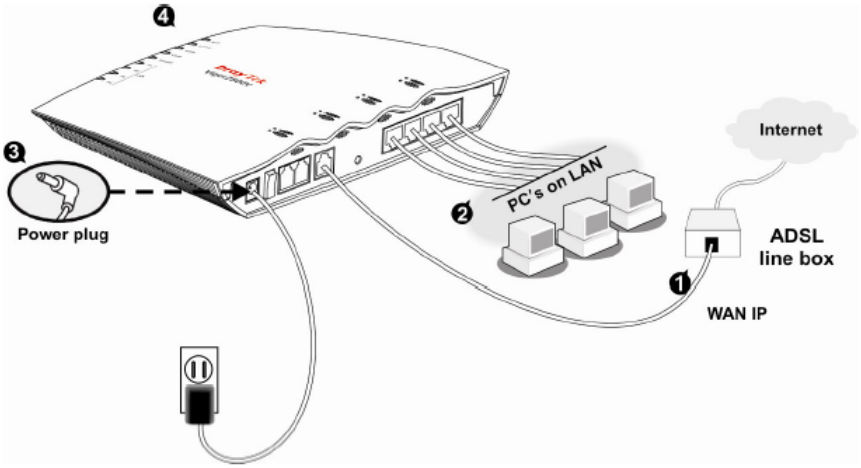
Problémy se směrovači řady Vigor2500V/Vi ADSL VoIP a jejich řešení

Nejprve zkontrolujte správné zapojení vašeho hardware!

Než začnete směrovač používat, zkontrolujte správnost zapojení všech zařízení.

1. **ADSL** box připojte k externímu rozbočovači (splitteru) pomocí kabelu RJ-11.
2. Jeden z portů 4 portového přepínače připojte k vašemu počítači pomocí kabelu RJ-45.
3. Přiložený síťový adaptér zapojte do příslušné zdířky na směrovači (viz. položka 3 - power plug (konektor napájení)).
4. Zkontrolujte zda všechny diody LED, indikující stavy **ACT, ADSL** a **LAN** svítí tak jak mají. (Informace o stavu LED najdete v části 1.3)

Modelové zapojení uvádíme níže:

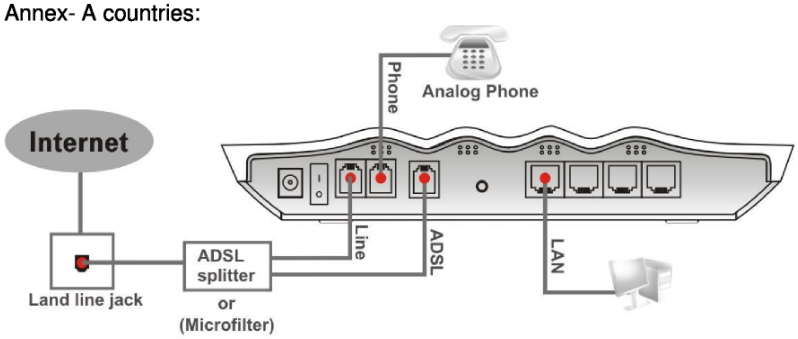


POZNÁMKA:

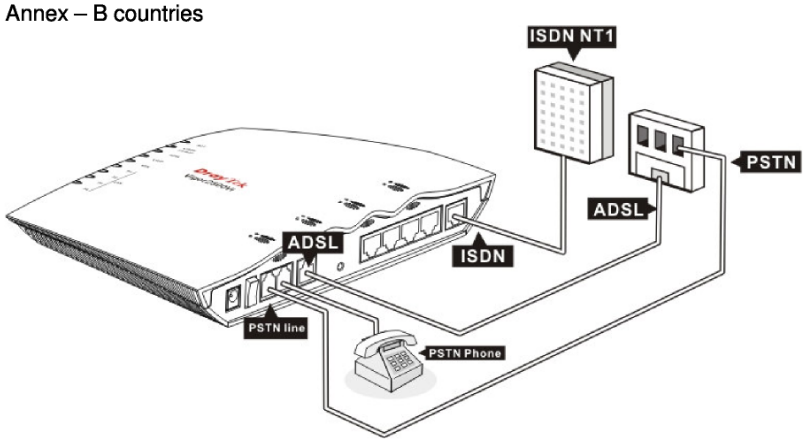
Rozbočovač (splitter) nebo mikrofiltr jsou doplňková zařízení, které nejsou součástí dodávky.

Existují různé způsoby zapojení pro země v příloze A (Annex A countries) a B (Annex B countries). Viz. níže uvedené obrázky:

Annex- A countries:

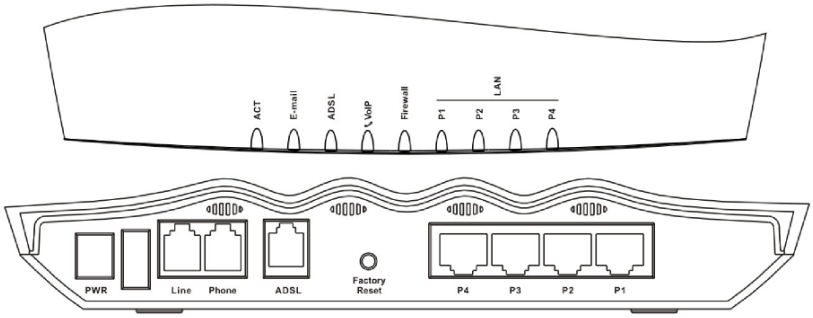


Annex – B countries



2. Základní popis stavu LED diod na přední straně směrovače a připojovacích rozhraní na zadní straně směrovače

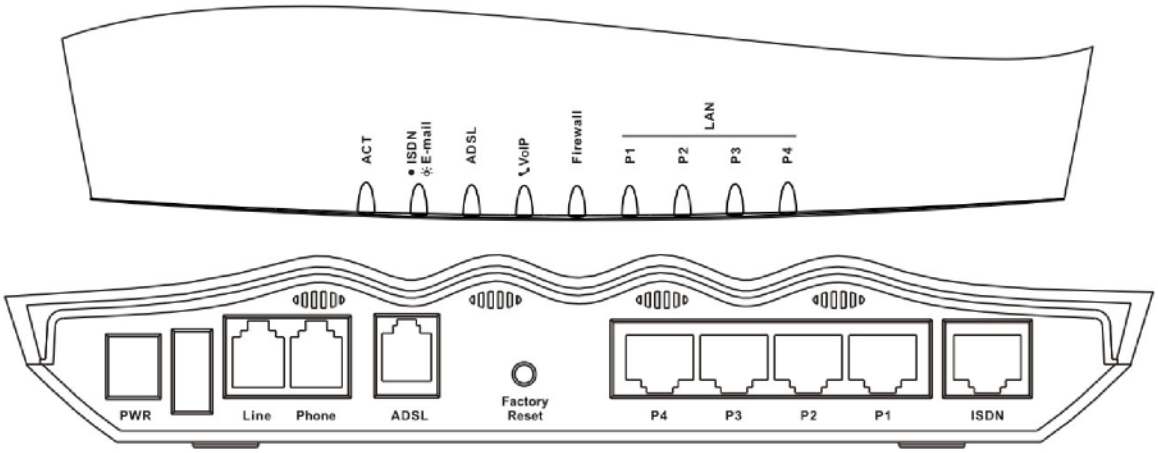
Vigor2500V



LED	Stav	Vysvětelní
ACT (Aktivita)	bliká	Napájení směrovače je v pořádku a směrovač funguje správně
E-mail	bliká	Na sledovaným mailserverech přibily nepřečtené e-maily
ADSL	svítí	ADSL je připojena
VoIP	zelená	Svítí při zvednutí sluchátka telefonu (vyvěšení)
		Bliká po dobu 0,3 s pokud jde přes smyčkové ISDN propojení
		Je-li telefon propojen přes VoIP bliká po dobu 2 sekund
	oranžová	Svítí pokud je hovor realizován přes telefonní linku ústředny
Firewall	svítí	Funkce firewall je zapnuta
	bliká	Odrážení DoS útoků
LAN (P1, P2, P3, P4)	zelená	Na nastaveném portu je aktivní připojení 100 Mb/s
	oranžová	Na nastaveném portu je aktivní připojení 10 Mb/s
	bliká	Přenos ethernetových paketů

Rozhraní	Popis
PWR	Slot pro připojení přiloženého napájecího adaptéru
Line	Připojení analogového telefonní linky z telefonní ústředny
Phone	Připojení analogového telefonu pro internetovou telefonii
ADSL	Přípojka ADSL linky pro připojení k internetu
Factory Reset	Obnova výchozího nastavení. Způsob použití: Zapněte směrovač (dioda ACT bliká), stiskněte tlačítko v otvoru a držte po dobu delší než 5 s. Až začne dioda ACT rychle blikat, pusťte tlačítko. Směrovač se poté restartujte s výchozím nastavením.
P1, PS, P3, P4	Pro připojení místních síťových zařízení

Vigor2500Vi



LED	Stav	Vysvětelní
ACT (Aktivita)	bliká	Napájení směrovače je v pořádku a směrovač funguje správně
ISDN/E-mail	svíti	ISDN síť je nastavena správně
	bliká	Na sledovaným mailserverech přibily nepřečtené e-maily
ADSL	svítí	ADSL je připojena
VoIP	zelená	Svítí při zvednutí sluchátka telefonu (vyvěšení)
		Bliká po dobu 0,3 s pokud jde přes smyčkové ISDN propojení
		Je-li telefon propojen přes VoIP bliká po dobu 2 sekund
	oranžová	Svítí pokud je hovor realizován přes telefonní linku ústředny
Firewall	svítí	Funkce firewall je zapnuta
	bliká	Odrážení DoS útoků
LAN (P1, P2, P3, P4)	zelená	Na nastaveném portu je aktivní připojení 100 Mb/s
	oranžová	Na nastaveném portu je aktivní připojení 10 Mb/s
	bliká	Přenos ethernetových paketů

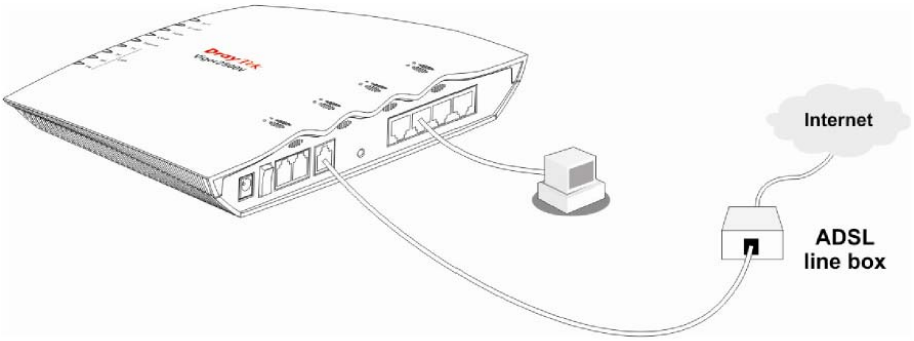
Rozhraní	Popis
PWR	Slot pro připojení přiloženého napájecího adaptéru
Line	Připojení analogového telefonní linky z telefonní ústředny
Phone	Připojení analogového telefonu pro internetovou telefonii
ADSL	Přípojka ADSL linky pro připojení k internetu
Factory Reset	Obnova výchozího nastavení. Způsob použití: Zapněte směrovač (dioda ACT bliká), stiskněte tlačítko v otvoru a držte po dobu delší než 5 s. Až začne dioda ACT rychle blikat, pusťte tlačítko. Směrovač se poté restartujte s výchozím nastavením.
P1, PS, P3, P4	Pro připojení místních síťových zařízení
ISDN	Připojeno k externí ISDN skříni NT1 nebo NT1+ vašeho poskytovatele

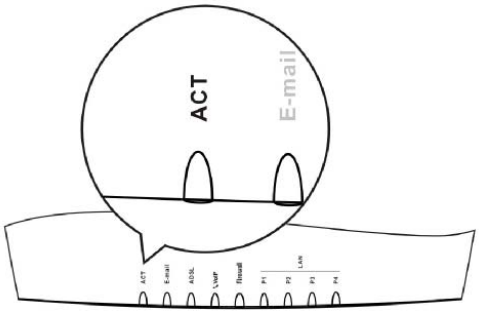
3. Řešení problémů

V této části vám poskytneme užitečné tipy pro řešení nestandardních situací. Při hledání závady postupujte podle následujících kroků (dodržte jejich pořadí).

3.1 Je hardwarové zapojení v pořádku?

1. Zkontrolujte správné zapojení kabelů ADSL/LAN.
2. Zapněte směrovač a poté zkontrolujte zda LED dioda ACT bliká s frekvencí 1x za sekundu a že dioda LAN nepřerušovaně svítí.



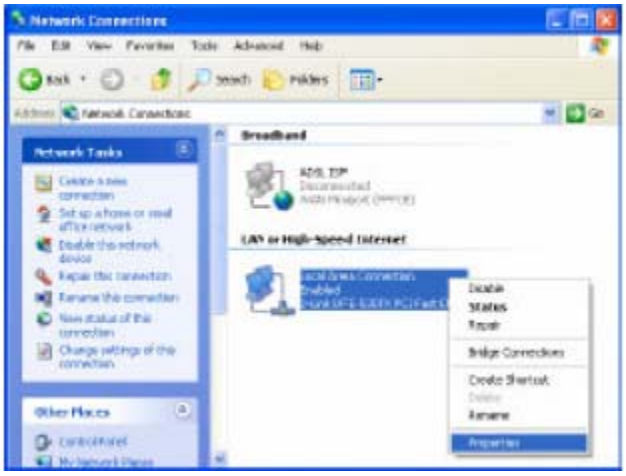


3.2 Je správně nastaveno síťové připojení na vašem počítači?

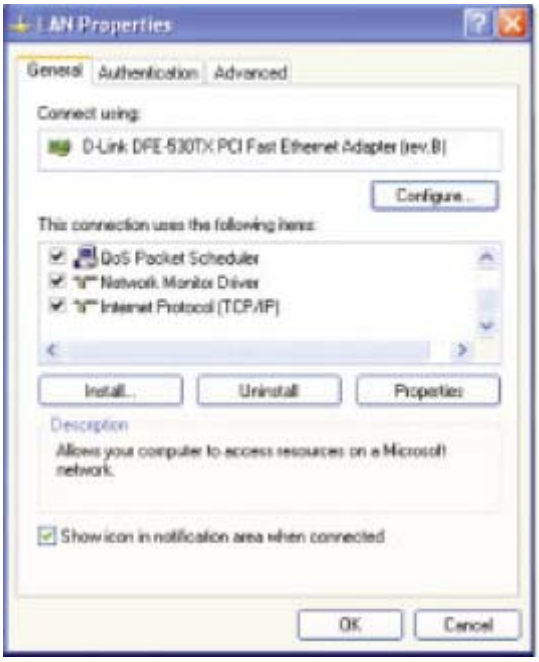
Následující modelový příklad je určen pro prostředí Windows XP, pokud používáte jiný operační systém, použijte nápovědu pro daný operační systém nebo si příslušné informace vyhledejte v části podpora na serveru www.draytek.com.

1. V menu "**Ovládací panely**" dvakrát klikněte na "**Síťová připojení**".

2. Pravým tlačítkem myši klikněte na **Místní připojení** a poté na **Vlastnosti**.



3. Vyberte **Internetový protokol (TCP/IP)** a klikněte na **Vlastnosti**.



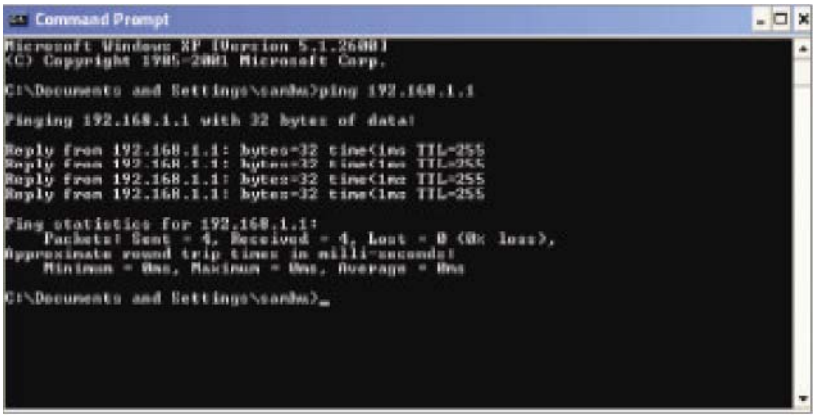
4. Zvolte možnost **Získat IP adresu automaticky** a **Získat adresu DNS serveru automaticky**.

3.3 Můžete z vašeho počítače směrovač "prozvonit"?

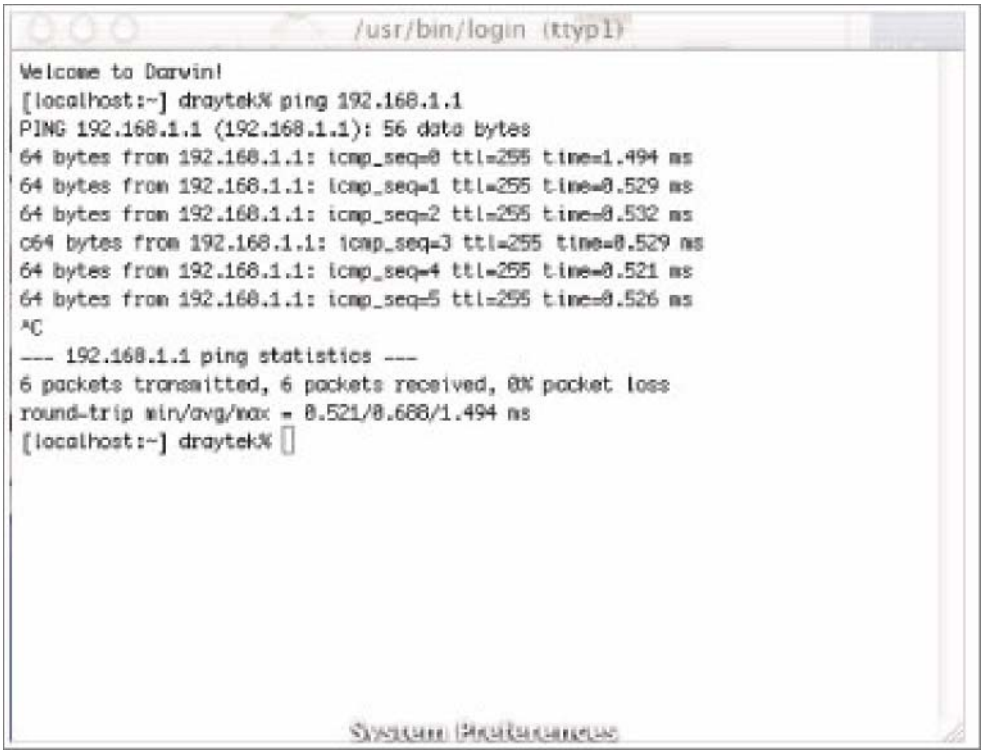
Standardní IP brána směrovače je 192.168.1.1. Ověřte zda je možné směrovač prozvonit z vašeho počítače.

A. Windows

1. Spusťte okno **Příkazového řádku** (z nabídky Start > Spustit)
2. Napište příkaz **command** (pro operační systémy Windows 95/98/ME) nebo **cmd** (pro operační systémy Windows NT/ 2000/XP).
3. Napište **ping 192.168.1.1** a stiskněte [**Enter**]



B. Mac (pracovní stanice)



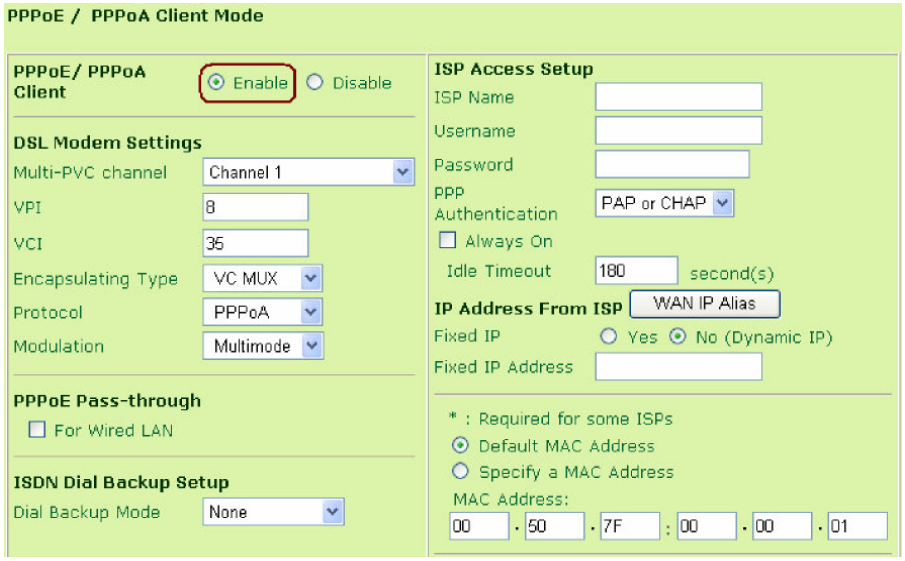
Sledujte zda váš počítač obdrží odpověď z adresy 192.168.1.1. Pokud ne, zkontrolujte IP adresu vašeho počítače PC. Doporučujeme, abyste při konfiguraci síťového připojení zaškrtli možnost "**Získat IP adresu automaticky**". (Viz. další část).

3.4 Jsou správné nastaveny informace o vašem poskytovateli připojení OK?

Klikněte na položku **Možnosti Internetu** a zkontrolujte zda jste správně zadali přihlašovací údaje pro připojení k vašemu poskytovateli.

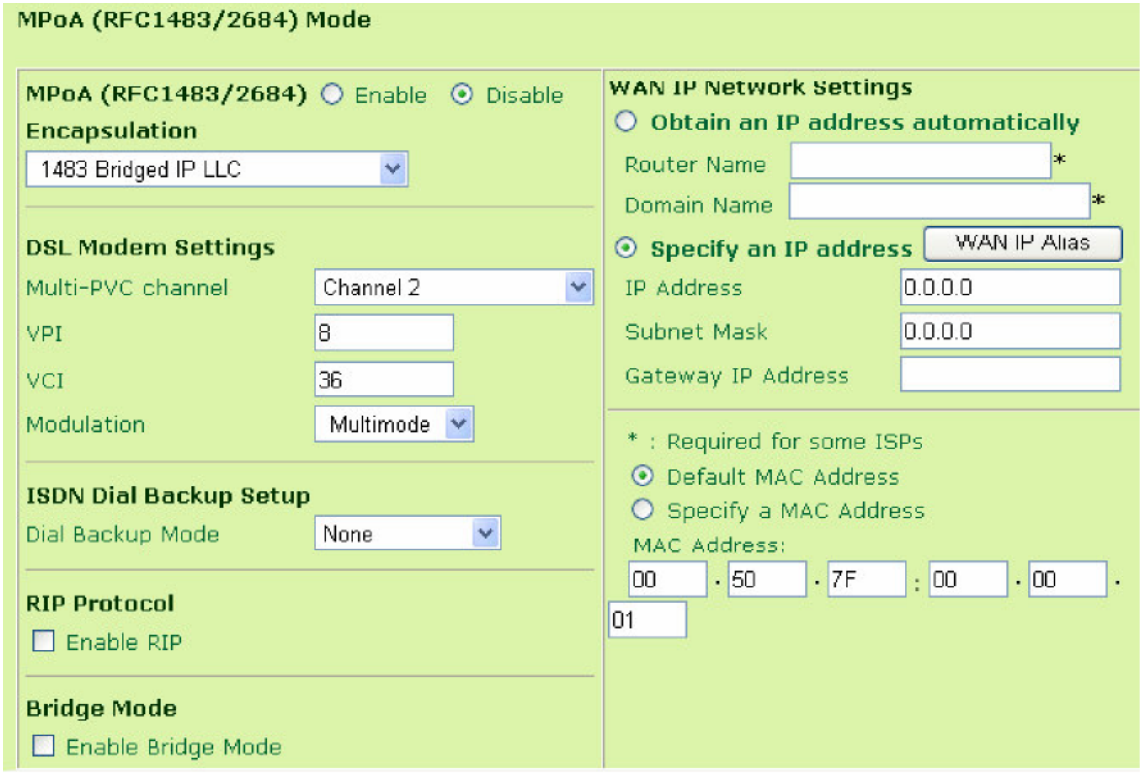
A. Uživatelé PPPoE/PPPoA (viz. obrázek níže)

1. Ověřte zda je zaškrtnuto pole **Enable** (Aktivovat).
2. Zkontrolujte správnost nastavení DSL modemu (porovnejte nastavení s údaji od vašeho poskytovatele).
3. Ověřte správné zadání uživatelského jména a hesla na zákaldě údajů od vašeho poskytovatele.



A. Uživatelé MPoA (RFC1483/2684) (viz. obrázek níže)

1. Ověřte zda je zaškrtnuto pole **Enable** (Aktivovat).
2. Zkontrolujte správnost nastavení DSL modemu (porovnejte nastavení s údaji od vašeho poskytovatele).
3. Zkontrolujte nastavení v polích IP Address (IP adresa), Subnet Mask (maska podsítě) a Gateway (brána) jsou nastaveny správně a zda váš poskytovatel požaduje používání DHCP klientů pro automatické získání IP adresy.



3.5 Zpráva pro poskytovatele připojení a prodejce pro technickou podporu

1. Pokud jsou všechny nastavení správná a přesto se vám nedaří spojení navázat, kontaktujte zástupce technické podpory vašeho poskytovatele připojení, který vám pomůže s nastavením jednotlivých parametrů.
2. Pokud směrovač nepracuje správně, obraťte se na vašeho prodejce. Vaše dotazy můžete také zasílat na e-mailovou adresu support@draytek.com

Rádi bychom na tomto místě shrnuli výhody směrovačů řady Vigor2500V:

Výhody směrovačů řady Vigor2500V

+ ADSL směrovač pro sdílení vašeho internetového připojení
+ robustní firewall pro lepší ochranu vašich počítačů
+ přijímání /uskutečňování hovorů přes připojení ADSL pomocí běžného telefonního přístroje (internetová telefonie)
+ možnost připojení vaší stávající telefonní linky s funkcí automatické ochrany při výpadku napájení
+ možnost volání zdarma přes VoIP jiným uživatelům VoIP
+ model Vigor2500Vi s přípojkou ISDN nabízí použití ISDN jako záložní telefonní linky, vzdálený ISDN přístup a funkci ISDN loop through (propojování)
+ kompatibilní s operačními systémy Windows a Mac OS

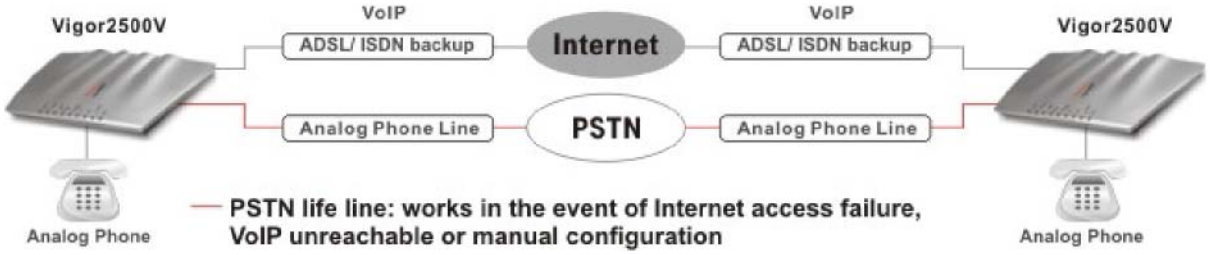
Stručný přehled funkcí

	Vigor2500V	Vigor2500Vi
Směrovač ADSL	*	*
VoIP	*	*
PSTN tel. linka	*	*
ISDN loop through	-	*
ISDN backup	-	*

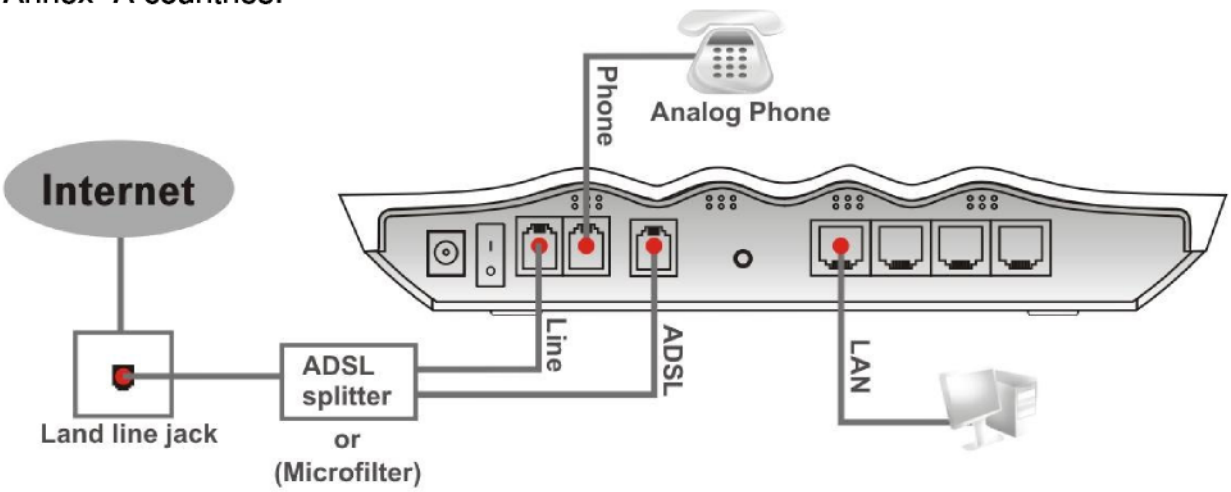
K čemu lze využít funkci ISDN loop through a možnost připojen analogové tel. linky z ústředny (PSTN) u směrovačů řady Vigor2500Vi?

Na zadní straně směrovače Vigor 2500V je port pro připojení standardní analogové telefonní linky (port "**Line**"). Funkci Loop Through lze použít pro nastavení alternativního telefonního čísla, které směrovač Vigor2500V vytočí namísto SIP adresy vaší kontaktní osoby v případě ztráty spojení ADSL, nebo v případě výpadku napájení. Funkce analogové linky (PSTN) tedy funguje jako záložní mechanismus pro případ výpadku internetové telefonie (VoIP). Tento záložní mechanismus se aktivuje automaticky, ale jeho nastavení lze též ručně měnit.

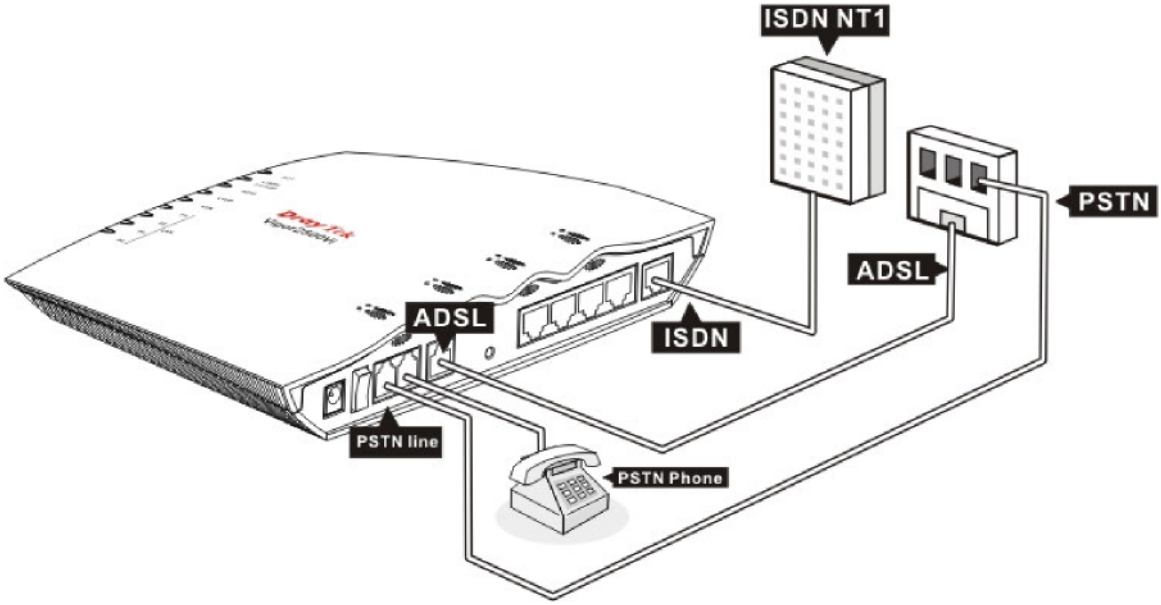
Směrovač řady Vigor2500Vi je dokonce vybaven i ISDN rozhraním, které můžete rovněž využít jako běžnou telefonní linku. Při výpadku napájení směrovače nebo při poruše internetové telefonie (VoIP) tak můžete stále telefonovat přes ISDN. ISDN linka tedy funguje jako záložní mechanismus pro případ výpadku internetové telefonie (VoIP).



Annex- A countries:



Annex – B countries



Přehled nejdůležitějších funkcí

VoIP

+ G.168 potlačení ozvěny linky
+ nastavení hlasitosti
+ vyrovnávání kolísání při přenosu hlasu - Jitter Buffer (250ms)
+ Hlasové kodeky: G.711 A/u law, G.729 A/B, VAD/CNG
+ Generování a detekce tónů: DTMF,
+ Vytáčení, obsazovací tón, zpětné volání
+ Protokol (Protocol): SIP, RTP/RTCP

Flexibilní filtrování obsahu URL

+ zablokování URL pomocí uživatelem definovaných klíčových slov
+ blokování přístupu k internetu pomocí IP adres
+ blokování prvků Java/ActiveX/cookies/proxy
+ blokování spustitelných/komprimovaných /multimediálních souborů
+ možnost nastavení časových plánů pro blokování

ADSL

+ Rychlost ADSL do 8 Mbps.
+ Podpora PPPoE, PPPoA, MPoA

LAN

+ 4 portový přepínač 10/100 Base-TX Ethernet
+ DHCP server pro přidělování IP adres (až 253 uživatelů)
+ DNS cache a proxy

Síť

+ DHCP server / relay
+ Dynamické DNS
+ Nastavení časových plánů pro vytáčení

Firewall

+ Analýza paketů (Stateful Packet Inspection)
+ Volitelná ochrana DoS/DDoS
+ prevence matení IP adres
+ uživatelsky nastavitelné filtrování paketů
+ NAT/PAT s Porty
+ Přesměrování/Předání dál & DMZ
+ Zasílání varovných e-mailových zpráv

Detekce elektronické pošty

+ informace o došlých zprávách elektronické pošty bez nutnosti zapnutí počítače.

Podpora aplikací

+ Windows Messenger, Yahoo Messenger, MSN Messenger V6.0, NetMeeting, ICQ2001b/2002a, většina on-line herních a multimediálních aplikací
+ podpora protokolu UPnP

Správa směrovače

+ webovské uživatelské rozhraní
+ podpora zadávání příkazů na příkazovém řádku (Telnet)
+ Telnetová podpora vzdáleného přístupu
+ zabudované diagnostické nástroje
+ Průvodce rychlým startem

+ zaílání varovných zpráv o útoku mailem
+ Syslog Monitoring

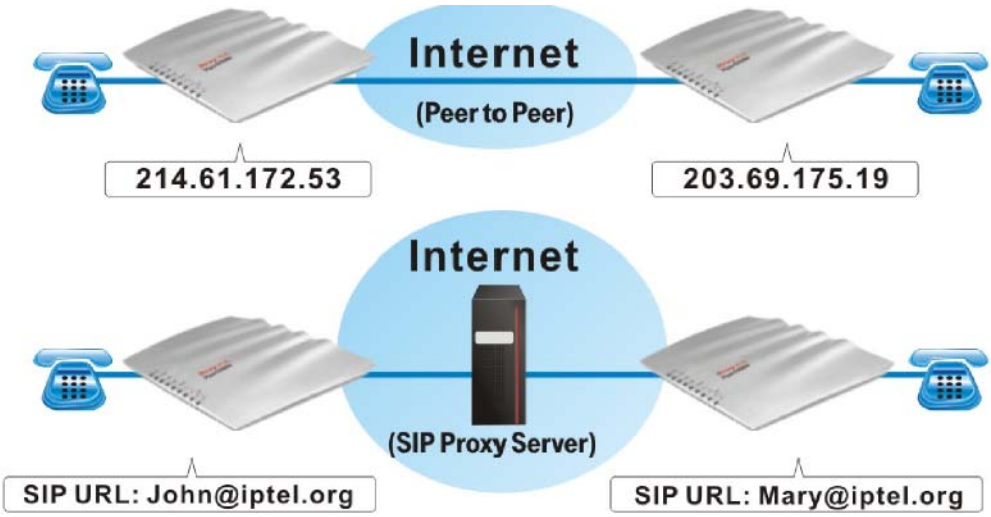
Funkce ISDN (pouze model Vigor2500Vi)
+ kompatibilita s Euro ISDN
+ automatický ISDN backup
+ podpora vícekanálového připojení - 64/128kbps (multilink-PPP)
+ systém BOD (automatické přepínání mezi jedním (64 kb/s) a dvěma (128 kb/s) kanály)
+ připojení LAN-to-LAN
+ Aktivace připojení na dálku
+ Virtual TA

Směrovací funkce
+ RIPv2 (nelze ve Velké Británii)
+ Static Route **(nelze ve Velké Británii)**

Robustní Firewall

Detekce elektronické pošty

Komunikace Peer to Peer VoIP:



Zapojení směrovače Vigor2500V se službou ITSP

Než začnete používat protokol SIP, musíte si vytvořit SIP účet u příslušného správce (např. IPTEL, DrayTEL [(www.draytel.org)].