

DrayTek

Série Vigor 2700

Uživatelská příručka

(verze 1.3, datum 9.10. 2006)

Obsah

Úvod	5
Popis Vigor2700	6
Popis Vigor2700G	7
Popis Vigor2700Gi	8
Popis Vigor2700V(2S1L).....	9
Popis Vigor2700V(2S).....	10
Popis Vigor2700VG(2S1L).....	11
Popis Vigor2700VG(2S).....	12
Popis Vigor2700VGi.....	13
Popis Vigor2700e.....	14
Popis Vigor2700Ge.....	15
1.1 Instalace hardware.....	16
Postup zapojení routeru.....	16
Zapnutí routeru.....	16
2. Základní nastavení.....	17
2.1 Změna hesla.....	17
2.2 Quick start wizard (Rychlé připojení k internetu)	19
2.2.1 Nastavení protokolu/ zapouzdření	19
2.2.2 PPPoE/PPPoA	21
2.2.3 Bridged IP.....	24
2.2.4 Routed IP	24
2.3 Online stav	24
2.4 Stavový řádek (Status bar).....	26
3. Rozšířené nastavení webu	27
3.1 Přístup k Internetu (Internet Access).....	27
3.1.1 Základy Internet Protokol (IP) síť	27
3.1.2 PPPoE/PPPoA.....	28
3.1.3 MPoA	31
3.1.4 MULTI - PVC	34
3.2 LAN.....	37
3.2.1 Základy LAN	37
3.2.2 Základní nastavení (General Setup).....	39
3.2.3 Statické routování.....	42
3.2.4. VLAN (Virtuální LAN).....	46
3.3 NAT	48
3.3.1 Přesměrování portů	48
3.2.3 DMZ.....	51
3.3.3 Otevření portů (Open Ports).....	53
3.3.4 Seznam známých portů (Well-Known Ports List).....	56
3. 4 Firewall	57
3.4.1 Základy firewallu	57
3.4.2 Základní nastavení (General Setup).....	60
3.4.3 Nastavení filtrování (Filter Setup).....	62
3.4.4 IM blokování (IM Blocking)	66

3.4.5 P2P blokování (P2P Blocking).....	67
3.4.6 DoS obrana (DoS Defense).....	67
3.4.7 URL obsahové filtrování (URL Content Filter).....	71
3.4.8 Web obsahové filtrování (Web Content Filter)	73
3.4.9 Vazba IP na MAC	74
3.5 Řízení pásma	75
3.5.1 Limit relací (Session Limit)	75
3.5.2 Limit šířky pásma.....	76
3.5.3 QoS - Kvalita služby	78
3.6 Aplikace.....	86
3.6.1 Dynamické DNS	86
3.6.2 Plánovač (Schedule)	88
3.6.3 Radius.....	90
3.6.4 UPnP	91
3.6.5. IGMP.....	93
3.6.6. Vzbuzení po LAN (Wake on LAN).....	94
3.7 VPN a vzdálený přístup (VPN and Remote Access)	95
3.7.1 Řízení vzdáleného přístupu (Remote Access Control)	95
3.7.2 PPP základní nastavení (PPP General Setup)	96
3.7.3 IPSec hlavní nastavení (IPSec General Setup)	97
3.7.4 IPSec Peer identita (IPSec Peer Identity)	98
3.7.5 Vzdálený Dial-in uživatel (Remote User profiles).....	100
3.7.6 LAN - LAN.....	103
3.7.7 Správa spojení (Connection Managemnt).....	111
3.8 Správa certifikátů (Certificate Management).....	112
3.8.1 Lokální certifikát (Local Certificate)	112
3.8.2 Důvěryhodný CA certifikát (Trusted CA Certificate)	114
3.9 VoIP.....	116
3.9.1 Konfigurace volání (Dial Plan)	118
3.9.2 SIP účty (SIP Account)	121
3.9.3 Nastavení telefonu (Phone Settings).....	126
3.9.4 Stav (Status).....	131
3.10 ISDN.....	133
3.10.1 Základní nastavení	133
3.10.2 Přístup na jednoho poskytovatele	134
3.10.3 Přístup na dva ISP.....	135
3.10.4 Virtuální TA.....	136
3.10.5 Call Control (Řízení volání)	140
3.11 Bezdrátová LAN (Wireless LAN).....	143
3.11.1 Základní koncept	143
3.11.2 Základní nastavení (General Settings).....	146
3.11.3 Bezpečnost (Security)	147
3.11.4 Řízení přístupu (Access Control).....	149
3.11.5 WDS	150
3.11.6 Vyhledání AP (AP Discovery).....	154
3.11.6 Seznam klientů (Station List).....	155

3.12 Údržba systému (System Maintenance)	156
3.12.1 Stav systému	156
3.12.2 Heslo administrátora (Administrator Password)	158
3.12.3 Zálohování (Configuration Backup)	159
3.12.4 Záznamy syst. (Syslog)/ e-mail (Mail Alert)	161
3.12.5 Čas a datum (Time and Date)	163
3.12.6 Správa (Management)	164
3.12.7 Restart systému (Reboot System)	166
3.12.8 Firmware upgrade	166
3.13. Diagnostika (Diagnostics)	168
3.13.1 WAN připojení (WAN Connection)	168
3.13.2 Dial-out Trigger	169
3.13.3 Routovací tabulka (Routing Table)	169
3.13.4 ARP Cache tabulka	170
3.13.5 DHCP tabulka	171
3.13.6 Tabulka NAT relací (NAT Active Sessions Table)	172
3.13.7 Ping Diagnostika	173
3.13.8 Monitor dat	174
3.13.9 Trace Route	175
4. Aplikace a příklady	176
4.1 LAN – LAN mezi pobočkou a centrálou	176
4.2 Vzdálený přístup mezi uživatelem teleworker (práce z domova) a centrálou	185
4.3 Příklady nastavení QoS	191
4.4 Příklady pro používání NAT	194
4.5 Příklady nastavení pro volání VoIP.	196
4.6 Upgrade firmware.	202
4.7 Žádosti a certifikáty z CA serveru na Windows CA server.	205
4.8 Žádost o CA certifikát a nastavení jako důvěryhodný pod Windows CA server.	209
5. Řešení problémů	212
5.1 Zkontrolujte, zda je provozní stav hardware v pořádku	212
5.2 Zkontrolujte, zda je stav nastavení síťového připojení v pořádku.	212
5.3 Zkontrolujte z vašeho počítače router pomocí funkce Ping	215
5.4 Zkontrolujte, zda je nastavení hodnot vašeho ISP v pořádku.	217
5.5 Konfigurace zařízení do výrobního nastavení.	219
6. Prohlášení o shodě	220

Úvod

Řada Vigor2700 je navržena pro potřeby uživatelů SOHO (Small Office and Home Office) i podnikových aplikací. Zařízení umožňují sdílený přístup k internetu rychlostí downstream až 12Mb/s (ADSL2), nebo 24Mb/s (ADSL2+) a podporují i množství dalších funkcí v jednom kompaktním zařízení.

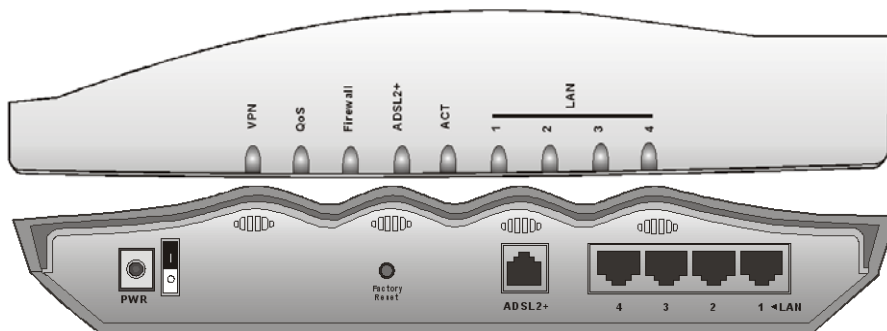
Pro zabezpečení vašeho systému poskytuje Vigor vyspělý firewall s prvky jako jsou např. Stateful Packet Inspection (stavová kontrola paketů - SPI) pro zabezpečení spolehlivosti sítě zjišťováním a zabráněním průniku paketů s nebezpečným obsahem, nebo útokům na DoS. Dále umožňuje kontrolu webu proti zobrazování stránek s nevhodným obsahem.

Vigor 2700G, Vigor2700Ge a Vigor2700VG obsahuje navíc bezdrátový modul 802.11g v módu Access Point, který dovoluje bezdrátový přístup rychlostí až 54Mb/s. Pro zabezpečení utajení dat Vigor umožňuje zakódování všech přenosů dat standardním šifrováním WEP a šifrováním WPA2 (IEEE 802.11i). Další vlastnosti zahrnují seznam bezdrátových klientů (Wireless Client List) a kontrolu MAC adres (MAC Address Control), které slouží k dohledu nad autorizací uživatelů ve vaší síti. Hidden SSID pak slouží pro utajení před vnějším prostředím proti skenování od možných útočníků.

Směrovače splňují v plném rozsahu směrnice Evropského parlamentu a rady 2002/95/EC (RoHS) platné od 1.6.2006!

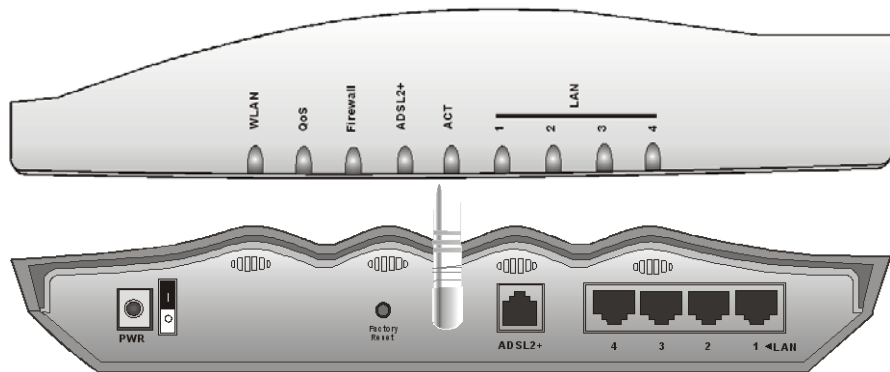
1. Indikační LED a konektory

Popis Vigor2700



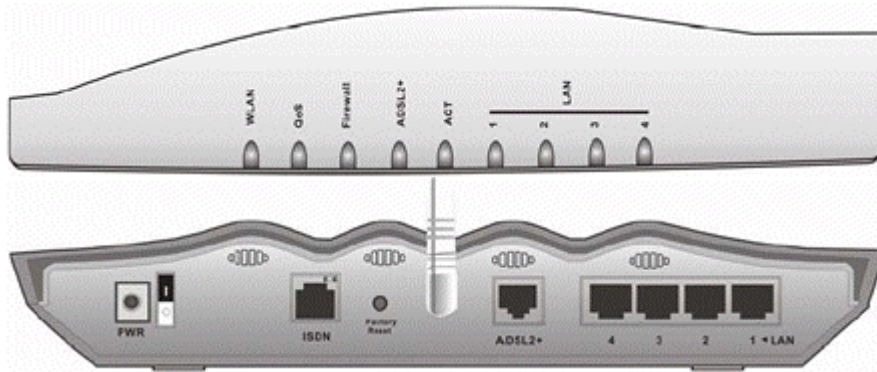
Indikační LED	Popis
VPN	Aktuální stav provozu VPN. Svítí pokud jsou na směrovači provozovány sítě VPN
QoS	Svítí při aktivaci funkce Quality of Service (kvalita služby) Nesvítí, pokud funkce QoS není aktivní
Firewall	Svítí, pokud je funkce DoS povolena Bliká při útoku DoS
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení Bliká zeleně po dobu navazování spojení Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700G



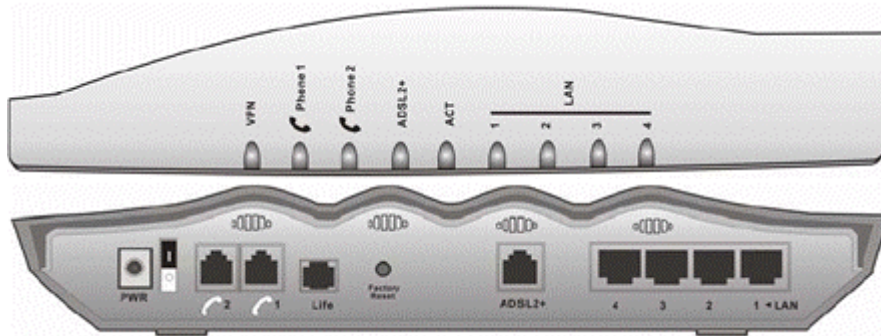
Indikační LED	Popis
WLAN	Nesvítí, pokud je rádiové rozhraní vypnuto
	Svítí, pokud je rádiové rozhraní zapnuto a pracuje korektně
	Bliká při přenosu dat
QoS	Svítí při aktivaci funkce Quality of Service (kvalita služby)
	Nesvítí, pokud funkce QoS není aktivní
Firewall	Svítí, pokud je funkce DoS povolena
	Bliká při útoku DoS
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení
	Bliká zeleně po dobu navazování spojení
	Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače
	Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně
	Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700Gi



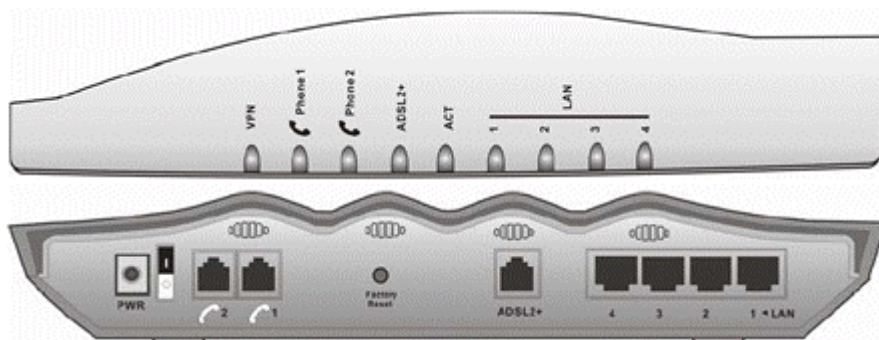
Indikační LED	Popis
WLAN	Nesvítí, pokud je rádiové rozhraní vypnuto
	Svítí, pokud je rádiové rozhraní zapnuto a pracuje korektně
	Bliká při přenosu dat
QoS	Svítí při aktivaci funkce Quality of Service (kvalita služby)
	Nesvítí, pokud funkce QoS není aktivní
Firewall	Svítí, pokud je funkce DoS povolena
	Bliká při útoku DoS
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení
	Bliká zeleně po dobu navazování spojení
	Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače
	Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně
	Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
ISDN	Konektor pro NT1 (NT1+)
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700V(2S1L)



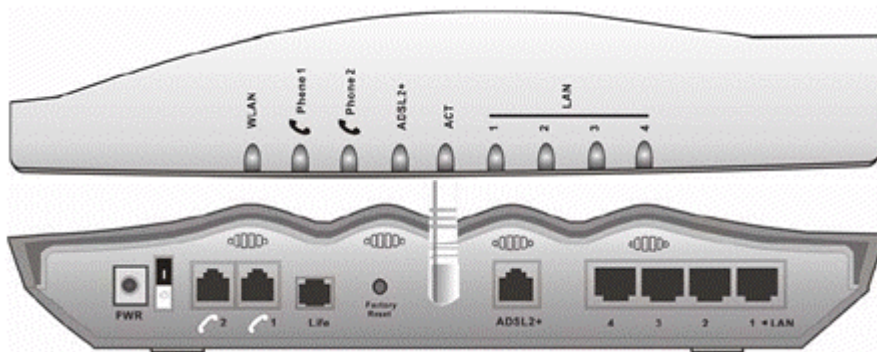
Indikační LED	Popis
VPN	Aktuální stav provozu VPN. Svítí pokud jsou na směrovači provozovány sítě VPN
Phone 1 & 2	Svítí při vyvěšeném telefonu Bliká pokud přichází telefonní hovor
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení Bliká zeleně po dobu navazování spojení Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
VoIP 1,2	Konektory k připojení analogových telefonů
Life	Konektor k připojení analog. PSTN telefonní linky
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700V(2S)



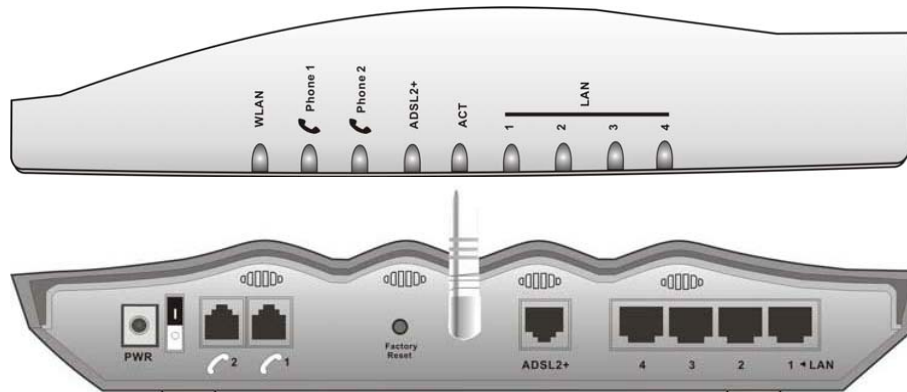
Indikační LED	Popis
VPN	Aktuální stav provozu VPN. Svítí pokud jsou na směrovači provozovány sítě VPN
Phone 1 & 2	Svítí při vyvěšeném telefonu Bliká pokud přichází telefonní hovor
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení Bliká zeleně po dobu navazování spojení Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
VoIP 1,2	Konektory k připojení analogových telefonů
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Připojky pro připojení lokálních PC.

Popis Vigor2700VG(2S1L)



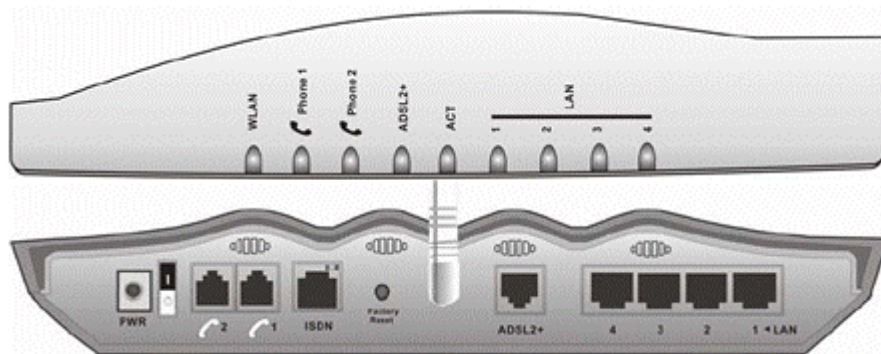
Indikační LED	Popis
WLAN	Nesvítí, pokud je rádiové rozhraní vypnuto
	Svítí, pokud je rádiové rozhraní zapnuto a pracuje korektně
	Bliká při přenosu dat
Phone 1 & 2	Svítí při vyvěšeném telefonu
	Bliká pokud přichází telefonní hovor
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení
	Bliká zeleně po dobu navazování spojení
	Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače
	Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně
	Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
VoIP 1,2	Konektory k připojení analogových telefonů
Life	Konektor k připojení analog. PSTN telefonní linky
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700VG(2S)



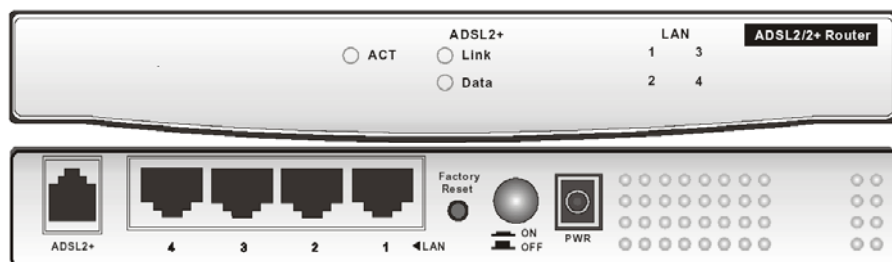
Indikační LED	Popis
WLAN	Nesvítí, pokud je rádiové rozhraní vypnuto
	Svítí, pokud je rádiové rozhraní zapnuto a pracuje korektně Bliká při přenosu dat
Phone 1 & 2	Svítí při vyvěšeném telefonu
	Bliká pokud přichází telefonní hovor
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení
	Bliká zeleně po dobu navazování spojení
	Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače
	Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně
	Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
VoIP 1,2	Konektory k připojení analogových telefonů
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700VGi



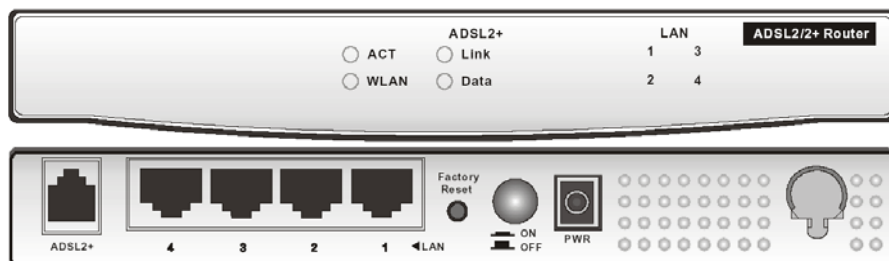
Indikační LED	Popis
WLAN	Nesvítí, pokud je rádiové rozhraní vypnuto
	Svítí, pokud je rádiové rozhraní zapnuto a pracuje korektně
	Bliká při přenosu dat
Phone 1 & 2	Svítí při vyvěšeném telefonu
	Bliká pokud přichází telefonní hovor
ADSL2+	Svítí zeleně, pokud je navázáno ADSL, ADSL2/2+ spojení
	Bliká zeleně po dobu navazování spojení
	Bliká oranžově při přenosu dat
ACT (aktivita)	Svítí při zapnutí síťového vypínače
	Bliká, pokud je směrovač ve správném pracovním stavu
LAN (1,2,3,4)	Svítí zeleně, pokud jsou síťová zařízení připojena korektně
	Bliká, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
PWR	Vstup pro konektor napájecího adaptéru
Vypínač	V pozici I - síťové napájení zapnuto, v pozici O - napájení vypnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
VoIP 1,2	Konektory k připojení analogových telefonů
ISDN	Konektor pro NT1 (NT1+)
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky.
LAN 4-1	Přípojky pro připojení lokálních PC.

Popis Vigor2700e



Indikační LED	Popis
ACT (aktivita)	Svíí při zapnutí síťového vypínače Bliká, pokud je směrovač ve správném pracovním stavu
ADSL2+ Link	Svíí, pokud je navázáno ADSL, ADSL2/2+ spojení Bliká po dobu navazování spojení
ADSL2+ Data	Bliká při přenosu dat
LAN	Svíí, pokud jsou síťová zařízení připojena korektně. Blikají, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky
P1,P2,P3,P4	Přípojky pro připojení lokálních PC.
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržejte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
Vypínač	Stisknuto - síťové napájení zapnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
PWR	Vstup pro konektor napájecího adaptéru

Popis Vigor2700Ge



Indikační LED	Popis
ACT (aktivita)	Svítlí při zapnutí síťového vypínače Bliká, pokud je směrovač ve správném pracovním stavu
WLAN	Nesvítlí, pokud je rádiové rozhraní vypnuto Svítlí, pokud je rádiové rozhraní zapnuto a pracuje korektně Bliká při přenosu dat
ADSL2+ Link	Svítlí, pokud je navázáno ADSL, ADSL2/2+ spojení Bliká po dobu navazování spojení
ADSL2+ Data	Bliká při přenosu dat
LAN	Svítlí, pokud jsou síťová zařízení připojena korektně. Blikají, pokud přes port procházejí Ethernet pakety
Zadní panel	Popis
ADSL2+	Vstup pro konektor ADSL, ADSL2/2+ linky
P1,P2,P3,P4	Přípojky pro připojení lokálních PC.
Factory Reset	Obnovení původních/výrobních nastavení: Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LEDka ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Směrovač se restartuje a obnoví se jeho výrobní nastavení.
Vypínač	Stisknuto - síťové napájení zapnuto. Upozornění! Zařízení musí být připojeno do sítě jen originálním adaptérem přibaleným k zařízení.
PWR	Vstup pro konektor napájecího adaptéru

1.1 Instalace hardware

Postup zapojení routeru

Propojte ADSL kabelem u Vigoru konektor RJ-45 s označením „ADSL2+“ (viz.č.1) se zásuvkou RJ-11 rozbočovače s označením „DSL“.

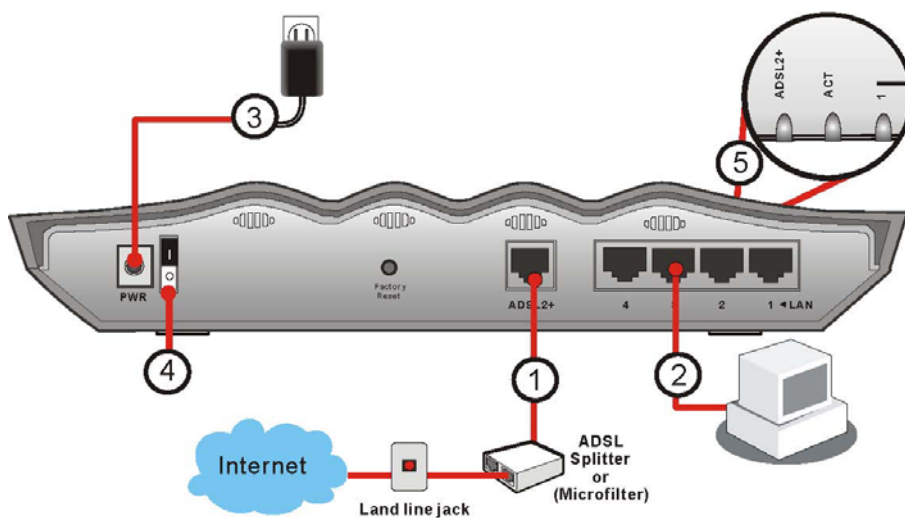
Propojte linkovým kabelem s konektory RJ-11 zásuvku rozbočovače „LINE“ s přívodní telefonní zásuvkou.

Propojte zásuvku „PHONE“ rozbočovače s NT ISDN boxem (RJ11), nebo analogovým telefonním přístrojem.

Propojte u Vigoru Ethernet kabelem jeden z portů označených 1-4 (viz.č.2) s Ethernet zásuvkou síťové karty počítače.

Zapnutí routeru

Pokud jste úspěšně postupovali podle předcházejících kroků připojte napájecí adaptér (viz.č.3) a můžete router zapnout. Rozsvítí se na přední straně přístroje indikační dioda ACT, ADSL2+ a příslušná indikační dioda LAN (viz.č.5).



2. Základní nastavení

Pro správné používání routeru je důležité kvůli bezpečnosti změnit heslo konfigurace webu a upravit základní nastavení.

Tato kapitola vysvětluje jak nastavit heslo administrátora a jak upravit základní nastavení pro úspěšné připojení k internetu. Uvědomte si, že pouze administrátor by měl být oprávněn měnit nastavení.

2.1 Změna hesla

Pokud chcete změnit heslo zařízení, musíte nejprve vstoupit na stránku nastavení prostřednictvím přednastaveného hesla. Zajistěte, aby byl počítač správně připojen k routeru.



Poznámka: Pokud je počítač nastaven na automatické přijetí IP adresy z DHCP serveru (doporučeno), postupujte následujícím způsobem.

Otevřete prohlížeč Internet Explorer a do příkazového řádku zadejte IP adresu směrovače (<http://192.168.1.1>). Otevře se pop-up okno které bude vyžadovat uživatelské jméno a heslo. V původním nastavení není heslo zadáno, proto klikněte přímo na OK.



Po kliknutí se zobrazí obrazovka s hlavním menu.

Vigor2700 Series
ADSL2/2+ Firewall Router

DrayTek
www.draytek.com

Quick Start Wizard
Online stav

Přístup k internetu
LAN
NAT
Firewall
Řízení pásma
Applikace
VPN a vzdaleny přístup
Správa certifikátu
VoIP
Bezdrátová LAN
Údržba systému
Diagnostika

Stav systému

Nazev modelu : Vigor2700 series
Verze Firmware : 2.6.3_1311302
Vytvoreno dat./cas : Sep 7 2006 13:26:22
Verze ADSL firmware : 1311302_B Annex B

LAN		WAN	
MAC adresa	: 00-50-7F-D8-A5-D8	Stav linky	: Odpojeno
1. IP adresa	: 192.168.1.1	MAC adresa	: 00-50-7F-D8-A5-D9
1. Maska podsítě	: 255.255.255.0	Spojění	: ---
DHCP Server	: Ano	IP adresa	: ---
		Default brána	: ---
		DNS	: 194.109.6.66

VoIP

Port	: 1	2
SIP registrator	:	
Učet ID	: 12	12
Registr	:	
Kodek	:	
Přichází volání	: 0	0
Odchází volání	: 0	0

Bezdrát. LAN

MAC adresa	: 00-50-7F-db-a5-d8
Frekvencni domena	: Europe
Verze Firmware	: 1.0.4.0

Zvolte položku **Údržba systému** (System Maintenance) a zvolte **Heslo administrátora** (Administrator Password).

[Údržba systému >> Nastavení hesla administrátora](#)

Heslo administrátora

Původní heslo	<input type="password"/>
Nové heslo	<input type="password"/>
Zopakovat zadání nového hesla	<input type="password"/>

OK

Zadejte vstupní heslo v poli **Původní heslo** (Old Password) (v původním nastavení není heslo zadáno). Zadejte nové do pole **Nové heslo** (New Password) a zadejte ho opakovaně do pole **Zopakovat zadání nového hesla** (Retype New Password). Pokračujte kliknutím na OK.

Vaše heslo bylo změněno. Při dalším otevření použijte již nové heslo pro přístup do konfiguratoru routeru.



2.2 Quick start wizard (Rychlé připojení k internetu)

Pokud Váš router může pracovat v prostředí s vysokorychlostním NAT, tato konfigurace Vám pomůže router velmi rychle nastavit a používat. První okno Quick Start Wizardu je vstupní heslo. V původním nastavení není heslo zadáno, pokračujte kliknutím na tlačítko **Další** (Next).

2.2.1 Nastavení protokolu/ zapouzdření

V Quick Start Wizardu, lze nakonfigurovat přístup routeru na internet pomocí různých protokolů, např. PPPoE, PPPoA, Bridged IP, nebo Routed IP.

Quick Start Wizard

2. Připojení do Internetu

VPI	<input type="text" value="8"/>	<input type="button" value="Autodetekce"/>
VCI	<input type="text" value="48"/>	
Protokol / Zapouzdření	<input type="text" value="PPPoA VC MUX"/>	
Pevná IP	<input type="radio"/> Ano <input checked="" type="radio"/> Ne(Dynamická IP)	
IP adresa	<input type="text"/>	
Maska podsítě	<input type="text"/>	
Default brána	<input type="text"/>	
Primární DNS	<input type="text"/>	
Sekundární DNS	<input type="text"/>	

Nyní nastavte vhodný typ síťového připojení na internet podle informací poskytnutých vaším poskytovatelem internetových služeb.

VPI

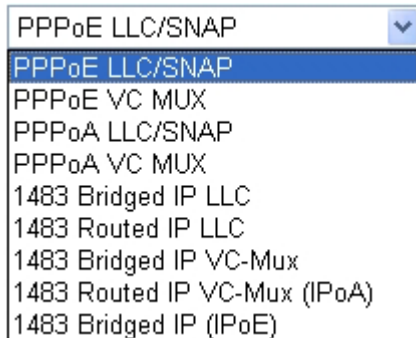
je zkratka pro Virtual Path Identifier (identifikátor virtuální cesty). Je to 8-bitová hlavička uvnitř každé ATM buňky, která indikuje kam má být buňka směrována. ATM je metoda posílání dat v malých paketech stejné velikosti. Používá se pro přenos dat do klientských počítačů.

VCI

je zkratka Virtual Channel Identifier (identifikátor virtuálního kanálu). Je to 16-bitová hlavička uvnitř každé ATM buňky která indikuje kam má být buňka směrována v době cesty sítě. Virtuální kanál je logické propojení mezi dvěma koncovými zařízeními sítě.

Protokol/ Zapouzdření (zapouzdření) (Protocol/ Encapsulation)

Zvolte režim rozhraní sítě IP. Je dostupných několik režimů přístupu na internet, např. PPPoE, PPPoA, Bridged IP a Routed IP.



Pevná IP (Fixed IP)

Klikněte na Ano (Yes) na specifikaci pevné IP adresy routeru. Jinak klikněte na **Ne (Dynamická IP)** abyste umožnili routeru volit si dynamickou IP adresu. Pokud zvolíte **Ne**, následující IP adresa, maska podsítě a zvolená brána se nezmění.

IP adresa (IP Address)

Přiřaďte IP adresu ke zvolenému protokolu.

Maska podsítě (Subnet Mask)

Přiřaďte hodnotu masky podsítě k protokolu Routed IP nebo Bridged IP.

Default brána (Default Gateway)

Přiřaďte IP adresu brány k protokolu Routed IP a Bridged IP.

Primární DNS (Primary DNS)

Přiřaďte IP adresu primární DNS.

Sekundární DNS (Second DNS)

Přiřaďte IP adresu sekundární DNS.

2.2.2 PPPoE/PPPoA

PPPoE je zkratka pro Point-to-Point Protocol over Ethernet (protokol bod-bod přes ethernet). Je založený na dvou uznávaných standardech – PPP a Ethernet. Spojuje uživatele přes ethernet a internet pomocí společného širokopásmového média, například DSL linka, bezdrátové spojení nebo kabelový modem. Všichni uživatelé ethernetu mohou sdílet společné připojení.

PPPoA znamená Point-to-Point Protocol over ATM (PPP přes ATM). PPPoA využívá PPP dial-up protokol s přenosem přes ATM.

PPPoE používá většina uživatelů DSL. Všichni místní uživatelé mohou pak sdílet jedno PPPoE nebo PPPoA připojení na internet. Váš poskytovatel internetových služeb vám poskytne uživatelské jméno, heslo a autentifikační režim.

Pokud tedy váš poskytovatel IS poskytuje připojení PPPoE nebo PPPoA, zvolte PPPoE nebo PPPoA.

Quick Start Wizard

3. Nastavit PPPoE / PPPoA

Jmeno ISP	<input type="text"/>
Uzivatske jmeno	<input type="text"/>
Heslo	<input type="text"/>
Potvrdit heslo	<input type="text"/>
<input checked="" type="checkbox"/> Vždy zapnuto	
Odpojení při necinnosti	<input type="text" value="-1"/> Vteriny

< Zpet

Dalsi >

Ukoncit

Zrusit

Jméno ISP (ISP Name)

Zadejte jméno podle požadavků poskytovatele internetových služeb.

Uživatelské jméno (User Name)

Zadejte platné uživatelské jméno poskytnuté poskytovatelem internetových služeb.

Heslo (Password)

Zadejte platné heslo poskytnuté poskytovatelem internetových služeb.

Potvrdit heslo (Confirm Password)
Zadejte heslo ještě jednou pro kontrolu.

Vždy zapnuto (Always On)
Zaškrtněte toto pole pro trvalé připojení k internetu.

Odpojení při nečinnosti (Idle Timeout)
Zadejte hodnotu ve vteřinách, po které bude připojení k internetu při nečinnosti odpojeno.

Klikněte na **Další** (Next) pro kontrolu a potvrzení zvolených nastavení.

Quick Start Wizard

4. Potvrďte vaše nastavení:

VPI	:	8
VCI	:	48
Protokol / Enkapsulace	:	PPPoE / LLC
Pevná IP	:	Ne
Primární DNS	:	
Sekundární DNS	:	
Vždy zapnuto	:	Ano

< Zpět

Další >

Ukončit

Zrusit

Klikněte na **Ukončit** (Finish). Zobrazí se **Online Stav** protokolu viz. okno níže.

Systemovy stav				Systemovy cas: 1:17:1			
LAN stav		Primarni DNS: 194.109.6.66		Sekundarni DNS: 194.98.0.1			
IP adresa		TX pakety	RX pakety				
192.168.1.1		5132	5094				
WAN stav		GW IP Addr: ---		Vytocit PPPoA			
Mod	IP adresa	TX pakety	TX rychl.	RX pakety	RX rychl.	Doba pripojeni	
---	---	0	0	0	0	00:00:00	
Message [PPP Shutdown]							
ADSL info		(Verze ADSL Firmware: 1311302_B)					
ATM statistiky	TX bloky	RX bloky	Opravene bloky	Neopravitelne bloky			
	0	0	0	0			
ADSL stav	Mod	Stav	Rychlost odesilani	Rychlost prijimani	Odstup signal-sum	Tlumeni linky.	
	-----	READY	0	0	0	0	

2.2.3 Bridged IP

Klikněte na protokol 1483 Bridged IP. Zadejte všechny informace obdržené od poskytovatele internetových služeb.

Po zadání všech informací na této stránce, klikněte na **Další** (Next) pro pokračování na další stránku. Zde klikněte na **Ukončit** (Finish). Zobrazí se **Online stav** protokolu.

2.2.4 Routed IP

Klikněte na protokol 1483 Routed IP. Zadejte všechny informace obdržené od poskytovatele internetových služeb.

Po zadání všech informací na této stránce, klikněte na **Další** (Next) pro pokračování na další stránku. Zde klikněte na **Ukončit** (Finish). Zobrazí se **Online stav** protokolu.

2.3 Online stav

Online stav zobrazuje stav systému, WAN síť, informace o ADSL a stavu součástí routeru na jedné straně. Pokud zvolíte PPPoE nebo PPPoA jako protokol, najdete na stránce Online Status tlačítko **Vytočit PPPoE** (Dial PPPoE) nebo **Vytočit PPPoA** (Vytočit PPPoA).

Online Stav

Systemovy stav			Systemovy cas: 1:17:1			
LAN stav		Primarni DNS: 194.109.6.66		Sekundarni DNS: 194.98.0.1		
IP adresa	TX pakety	RX pakety				
192.168.1.1	5132	5094				
WAN stav		GW IP Addr: ---		Vytocit PPPoA		
Mod	IP adresa	TX pakety	TX rychl.	RX pakety	RX rychl.	Doba pripojeni
---	---	0	0	0	0	00:00:00
Message [PPP Shutdown]						
ADSL info		(Verze ADSL Firmware: 1311302_B)				
ATM statistiky	TX bloky	RX bloky	Opravene bloky	Neopravitelne bloky		
	0	0	0	0		
ADSL stav	Mod	Stav	Rychlost odesilani	Rychlost prijimani	Odstup signal-sum	Tlumeni linky.
	-----	READY	0	0	0	0

Primární DNS (Primary DNS):
IP adresa primárního DNS serveru.

Sekundární DNS (Secondary DNS):
IP adresa sekundárního DNS serveru

IP adresa (IP Address) (v LAN Status):
IP adresa LAN.

TX pakety (TX Packets):
Celkový vyslaný počet IP paketů.

RX pakety (RX Packets):
Celkový počet přijatých IP paketů.

IP adresa brány (GW IP Addr):
IP adresa brány.

IP adresa (IP Address) (ve WAN Status):
IP adresa WAN.

RX rychl. (RX Rate):
Přenosová rychlost přicházejících dat. Jednotkou je znak/sek.

TX rychl. (TX Rate):
Přenosová rychlost odcházejících dat. Jednotkou je znak/sek.

Doba připojení (Up Time):
Celkový čas aktivního připojení.

TX bloky (TX Blocks):
Celkový počet vyslaných ATM bloků.

RX bloky (RX Blocks):
Celkový počet přijatých ATM bloků.

Upravene bloky (Corrected Blocks):
Celkový počet přijatých narušených, ale opravených ATM bloků.

Neupravene bloky (Uncorrected Blocks):
Celkový počet přijatých narušených a neopravených ATM bloků.

Mód (Mode):
Použitý modulační mód: G.DMT, G.Lite, nebo T1.413

Stav (State):
Aktuální stav DSL linky.

Rychlost odesílání (Up Speed):
Rychlost přenosu dat při uploadu (bit/s).

Rychlost příjmu (Down Speed):
Rychlost přenosu dat při downloadu (bit/s).

Odstup signál-šum (SNR Margin):

Odstup signál-šum (dB). Čím vyšší hodnota, tím lepší kvalita připojení.

Útlum linky (Loop Att.):

Útlum linky.

2.4 Stavový řádek (Status bar)

Při každém kliknutí na tlačítko OK obdržíte při ukládání nastavení odkazy, které Vám ukazují interakci systému s Vámi.

Stav: V pořádku

V pořádku (Ready)

Ukazuje že systém je v pořádku a připraven k další konfiguraci.

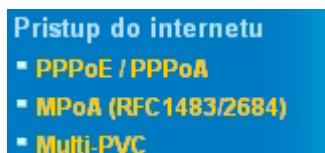
Nastavení uloženo (Settings Saved)

Znamená, že nastavení pokud kliknete na **Dokončit** (Finish) nebo **OK**, jsou uložena.

3. Rozšířené nastavení webu

Po ukončení základních nastavení routeru se snadno připojíte k Internetu. Pro uživatele kteří se chtějí seznámit s detailnějším nastavením a dalšími vlastnostmi produktu je určena další kapitola.

3.1 Přístup k Internetu (Internet Access)



3.1.1 Základy Internet Protokol (IP) sítě

Zkratka IP je Internet protokol. Každé zařízení v IP síti ať už je to router, print server, nebo počítač potřebují IP adresu pro jasnou lokalizaci v síti. Pro odstranění konfliktu adres ve veřejných sítích jsou tyto adresy registrovány v Síťovém informačním centru (NIC). Vlastnit unikátní adresy je nutné pouze pro zařízení pracující ve veřejných sítích. Z tohoto důvodu je používání veřejných adres celosvětově striktně kontrolováno.

Pro privátní a místní síť však není nutné a ani povinné a lze používat privátní IP adresy v tomto rozsahu:

od 10.0.0.0 do 10.255.255.255
od 172.16.0.0 do 172.31.255.255
od 192.168.0.0 do 192.168.255.255

Co jsou veřejné a privátní IP adresy

Router řídí, chrání a připojuje lokální síť-skupinu hostitelských PC. Každý z těchto PC má přidělenou privátní IP adresu z DHCP serveru umístěného ve Vigoru. Router používá přednastavenou IP adresu: 192.168.1.1 pro komunikaci s místními hostiteli. Router je také připojen k internetu a to přes veřejnou IP adresu. Aby data mohla přecházet z veřejného internetu k lokálnímu počítači a zpět musí router funkcí NAT umět překládat veřejnou adresu na privátní toho kterého počítače a opačně.

Tímto způsobem může více PC sdílet jedno připojení na Internet.

Přidělení veřejné IP adresy od poskytovatele ISP

Pro přidělení veřejné IP adresy pro router od vašeho poskytovatele ISP existují tři protokoly: Point to Point Protocol over Ethernet (PPPoE), PPPoA and MPoA. Multi-PVC nabízí pokročilejší nastavení.

Point to Point Protocol over Ethernet (PPPoE) spojuje síť hostitelských PC přes přístupové zařízení s koncentrátorem vzdáleného přístupu nebo agregačního koncentrátoru. Tato

implementace poskytuje kontrolu přístupu, účtování a typ služby na základě požadavků uživatele.

Pokud se router začne připojovat k poskytovateli, spustí se proces požadavků na spojení. Pak se následně vytvoří komunikace. Vaše uživatelské ID a heslo je ověřeno PAP nebo CHAP autentifikačním systémem RADIUS. Poskytovatelem vám bude přidělena IP adresa, DNS server a další požadované informace.

3.1.2 PPPoE/PPPoA

PPPoA, zahrnutý v RFC1483, může pracovat v Logical Link Control-Subnetwork Access Protocol nebo režimu VC-Mux jako zařízení CPE, router Vigor slouží pro transport na základě PPP session přes ADSL smyčku a Digital Subscriber Line Access Multiplexer (SDLAM) vašeho poskytovatele.

Pokud zvolíte PPPoE nebo PPPoA jako přístupový protokol na Internet, zvolte PPPoE/PPPoA z položky **Přístup k internetu**. Zobrazí se následující stránka:

[Přístup k internetu >> PPPoE / PPPoA](#)

PPPoE / PPPoA klient mod

PPPoE/PPPoA klient Zapnuto Vypnuto

Nastavení DSL modemu

Multi-PVC kanal

VPI

VCI

Typ zapouzdření

Protokol

Modulace

PPPoE Pass-through

Pro drát. LAN

Pro bezdrát. LAN

Nastavení přístupu ISP

Jmeno ISP

Uzivatelске jmeno

Heslo

PPP Overovani

Vždy zapnuto

Odpojeni pri necinnosti vterin

IP adresa od ISP

Pevna IP Ano Ne (Dynamicka IP)

Pevna IP adresa

* : Vyzadovano nekterymi ISP

Standardni MAC adresa

Specifikovat MAC adresu

MAC adresa : . . : . .

Index(1-15) in [Plan](#) Nastaveni:

, , ,

PPPoE/PPPoA klient (PPPoE/PPPoA Client)

Klikněte na **Zapnuto** (Enable), k aktivaci funkce. Pokud kliknete na **Vypnuto** (Disable) a všechna nastavení budou neplatná.

Nastavení DSL modemu (DSL Modem Settings)

Doplňte DSL parametry požadované vaším poskytovatelem. Jsou důležité na spuštění připojení DSL s vaším poskytovatelem.

Multi-PVC kanal (Multi-PVC channel)-Zde zobrazené volby jsou určeny stránkou **Přístup na Internet – Multi PVC** (Internet Access – Multi PVCs). Pokud zvolíte M-PVC Channel, znamená to že žádné možnosti nebudou zvoleny.

VPI-Zadejte hodnoty obdržené od poskytovatele.

VCI-Zadejte hodnoty obdržené od poskytovatele.

Typ zapouzdření (Encapsulation Type)-Otevřete seznam a zvolte typ určený poskytovatelem.

Protokol- Otevřete seznam a zvolte typ určený poskytovatelem. Pokud jste již nastavili protokol v Quick Start Wizardu, není nutné měnit nastavení v této skupině.

Modulace (Modulation)- Otevřete seznam a zvolte typ určený poskytovatelem.

PPPoE Pass-through

Router nabízí připojení PPPoE dial-up. Navíc lze zřídit spojení PPPoE přímo od místních klientů s poskytovatelem přes router Vigor.

Pro drát. LAN (For Wired LAN)

Pokud zaškrtnete toto pole, PC v té samé síti může použít další PPPoE session (jiné než hostitelské PC), aby se připojilo na Internet.

Pro bezdrát. LAN (For Wireless LAN)

Pokud zaškrtnete toto pole, PC v té samé síti může použít bezdrátové PPPoE session (jiné než hostitelské PC), aby se připojilo na Internet.

Nastavení přístupu ISP (ISP Access Setup)

Zadejte vaše uživatelské jméno, heslo a autentifikační parametry na základě informací poskytovatele. Pokud chcete být připojení k internetu trvale, zaškrtněte možnost **Vždy zapnuto** (Always On).

Jméno ISP (ISP Name)-Zadejte název poskytovatele (není nutné).

Uživatelské jméno (Username)-Zadejte uživatelské jméno určené poskytovatelem.

Heslo (Password)- Zadejte heslo určené poskytovatelem.

PPP ověřování (PPPAuthentication)-Zvolte „Pouze PAP“, nebo „PAP nebo CHAP“ pro PPP.

Vždy zapnuto (Always On)-Zaškrtněte pro trvalé připojení k Internetu.

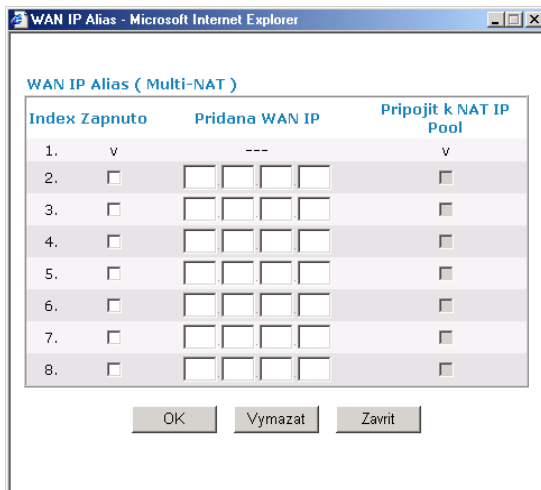
Odpojit při nečinnosti (Idle Timeout)- Zadejte hodnotu ve vteřinách, po které bude připojení k internetu při nečinnosti odpojeno.

IP adresa od ISP (IP Address From ISP)

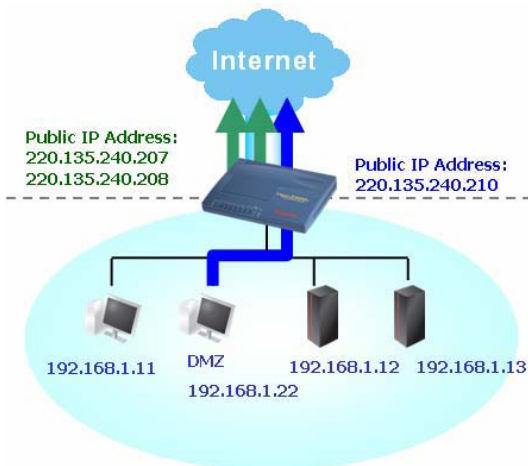
Poskytovatel většinou určuje IP adresu dynamicky při každém připojení. V některých případech může poskytovatel přidělit vždy stejnou IP adresu, pokud si ji objednáte. V tomto případě zadejte IP adresu do pole **Pevná IP adresa** (Fixed IP Address).

Pevná IP (Fixed IP)-Zaškrtněte pokud chcete využívat funkci „Pevná IP adresa“.

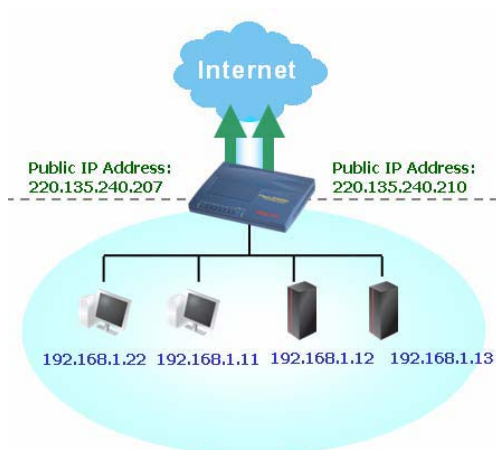
WAN IP Alias-Pokud máte hromadnou veřejnou IP adresu a rádi byste ji využili na rozhraní WAN sítě, použijte „WAN IP alias“. Lze nastavit 8 různých IP adres.



Zaškrtnutím políčka **Připojit k NAT IP Pool** (Join NAT IP Pool), budou data z NAT hostitelů přeposlána na bázi session.



Pokud políčko **Připojit k NAT IP Pool** nezaškrtnete, stále lze tyto veřejné IP adresy použít na jiné účely jako např. DMZ host, nebo Open Ports.



Standardní MAC adresa (Default MAC Address)

Specifikovat MAC adresu

Zadejte jinou než přednastavenou MAC adresu pro router pokud potřebujete.

MAC adresa (MAC Address)-Zadejte MAC adresu manuálně.

Index (1-15) v Plan Nastavení (Index 1-15 in Schedule Setup)

Lze zadat 4 časové údaje podle potřeby. Všechna nastavení musí být nastavena předtím na stránce Aplikace – Plánovač.

Po dokončení všech nastavení, klikněte prosím na OK pro aktivaci.

3.1.3 MPoA

MPoA je specifikace, která umožňuje službám ATM, aby byly integrované do existující místní sítě, která využívá ethernet, token-ring nebo TCP/IP protokol. Cílem je umožnit místním sítím na různých základech posílat pakety prostřednictvím ATM.

Abyste zvolili MpoA jako přístupový protokol, zvolte prosím MPoA z menu **Přístup k internetu** (Internet Access). Zobrazí se následující stránka:

MPoA (RFC1483/2684) Mod

<p>MPoA (RFC1483/2684) <input type="radio"/> Zap. <input checked="" type="radio"/> Vyp.</p>	
<p>Nastavení DSL modemu</p> <p>Multi-PVC kanál <input type="button" value="Vyber M-PVC kanál"/></p> <p>Zapouzdření <input type="text" value="1483 Bridged IP LLC"/></p> <p>VPI <input type="text" value="8"/></p> <p>VCI <input type="text" value="49"/></p> <p>Modulace <input type="text" value="Multimod"/></p>	
<p>RIP protokol</p> <p><input type="checkbox"/> Aktivovat RIP</p>	
<p>Bridge Mode</p> <p><input type="checkbox"/> Zapnout Bridge Mode</p>	
<p>Nastavení WAN IP site</p> <p><input type="radio"/> Získat IP adresu automaticky</p> <p>Jmeno routeru <input type="text"/> *</p> <p>Jmeno domeny <input type="text"/> *</p> <p><input checked="" type="radio"/> Specifikovat IP adresu <input type="button" value="WAN IP Alias"/></p> <p>IP adresa <input type="text" value="0.0.0.0"/></p> <p>Maska podsítě <input type="text" value="0.0.0.0"/></p> <p>IP adresa brány <input type="text"/></p>	
<p>* : Pozadovano nekterymi ISP</p> <p><input checked="" type="radio"/> Standardni MAC adresa</p> <p><input type="radio"/> Specifikovat MAC adresu</p> <p>MAC adresa : <input type="text" value="00"/> . <input type="text" value="50"/> . <input type="text" value="7F"/> : <input type="text" value="DB"/> . <input type="text" value="A5"/> . <input type="text" value="D9"/></p>	
<p>IP adresa DNS serveru</p> <p>Primarni IP adresa <input type="text"/></p> <p>Sekundarni IP adresa <input type="text"/></p>	

MPoA (RFC1483/2684)

Klikněte na **Zap.** (Enable) pro aktivaci této funkce. Pokud kliknete na **Vyp.** (Disable), budou všechna nastavení neplatná.

Nastavení DSL modemu (DSL Modem Settings)

Nastavte DSL parametry požadované poskytovatele. Jsou důležité na vybudování DSL připojení k vašemu poskytovateli.

Multi-PVC kanál (Multi-PVC channel)-Tyto možnosti jsou determinovány stránkou „Přístup k internetu – Multi PVC“ (Internet Access – Multi PVCs). Výběr **M-PVC kanál** znamená, že ani jedna možnost nebude zvolena.

Zapouzdření (Encapsulation Type)-Otevřete seznam a zvolte typ určený poskytovatelem.

VPI-Zadejte hodnoty obdržené od poskytovatele.

VCI-Zadejte hodnoty obdržené od poskytovatele.

RIP protokol

Routing Information Protocol RFC1058 specifikuje jak si routery vyměňují informace. Klikněte na **Aktivovat RIP** (Enable RIP), pokud chcete aktivovat tuto funkci.

Bridge Mode

Pokud zvolíte protokol Bridged IP, zaškrtněte toto políčko pro aktivaci této funkce. Router bude pracovat jako bridge modem.

Nastavení WAN IP sítě WAN IP Network Setting)

Tato skupina umožňuje automaticky získat IP adresu, nebo ji zadat manuálně.

Získat IP adresu automaticky (Obtain an IP address automatically)-Zaškrtněte toto pole pro získání IP adresy automaticky.

Jméno routeru (Router name)-Zadejte jméno routeru dodané poskytovatelem.

Jméno domény (Domain name)-Zadejte název vaší domény.

WAN IP Alias -pokud máte hromadné IP adresy a rádi byste je využili na rozhraní WAN sítě, použijte prosím WAN IP Alias. Lze nastavit 8 různých IP adres.

Index	Zapnuto	Přidána WAN IP	Připojit k NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

OK Vymazat Zavřít

Specifikovat IP adresu (Specify an IP address)-Zaškrtněte pole pro specifikaci dat.

IP adresa (IP Address)-Zadejte pevnou IP adresu.

Maska podsítě (Subnet Mask)-Zadejte masku podsítě.

IP adresa brány (Gateway IP Address)-Zadejte IP adresu brány.

Standardní MAC adresa (Default MAC Address)

Zadejte MAC adresu pro router. Lze použít Přednastavenou MAC adresu, nebo specifikovat jinou MAC adresu pokud potřebujete.

MAC adresa (MAC Address)-Zadejte MAC adresu manuálně.

IP adresa DNS serveru (DNS Server IP)-Zadejte primární IP adresu routeru. Pokud je třeba, zadejte i sekundární IP adresu.

Po dokončení všech nastavení, klikněte prosím na OK pro aktivaci.

3.1.4 MULTI - PVC

Vigor umožňuje vytvoření multi-PVC pro využívání různých přenosů dat. Přejděte na stránku **Přístup k internetu** (Internet Access) a zvolte **Multi-PVC** (Multi-PVC Setup). Systém umožňuje nastavení 8 kanálů, které je možné nastavit jako první PVC linku, která bude sloužit jako multi-PVC.

[Přístup k internetu >> Multi-PVC](#)

Multi-PVC

Zakladni		Bridge					
Kanal	Zapnout	VPI	VCI	Typ QoS	Protokol	Zapouzdreni	
1.	<input checked="" type="checkbox"/>	8	48	UBR	PPPoE	LLC/SNAP	
2.	<input type="checkbox"/>	8	49	UBR	MPoA	1483 Bridged IP LLC	
3.	<input type="checkbox"/>	8	50	UBR	PPPoE	LLC/SNAP	
4.	<input type="checkbox"/>	8	51	UBR	PPPoE	LLC/SNAP	
5.	<input type="checkbox"/>	8	52	UBR	PPPoE	LLC/SNAP	
6.	<input type="checkbox"/>	8	53	UBR	PPPoE	LLC/SNAP	
7.	<input type="checkbox"/>	8	54	UBR	PPPoE	LLC/SNAP	
8.	<input type="checkbox"/>	8	55	UBR	PPPoE	LLC/SNAP	

Pozn: VPI/VCI musí být unikátní pro každý kanál!

OK

Vymazat

Zrusit

Zapnout (Enable)

Zaškrtněte toto políčko abyste povolili kanál. Kanály, které jsou povolené, budou zobrazeny v menu **Multi-PVC** na stránce **Přístup k internetu** (Internet Access). I když lze povolit 8 kanálů, na stránce **Přístup k internetu** (Internet Access) lze zvolit jen jeden.

VPI

Zadejte hodnoty od poskytovatele.

VCI

Zadejte hodnoty od poskytovatele.

Typ QoS (QoS Type)

Vyberte správný typ QoS.

Typ QoS

UBR ▼

- UBR
- CBR
- ABR
- nrtVBR
- rtVBR

Protokol (Protocol)

Vyberte správný protokol pro daný kanál.

Zapouzdření (Encapsulation)

Vyberte správný typ pro daný kanál. Na základě nastavení protokolu budou typy různé.

Protokol		Zapouzdření
PPPoE ▼	Zapouzdření	1483 Bridged IP LLC
PPPoA	LLC/SNAP ▼	1483 Route IP LLC
PPPoE	VC MUX	1483 Bridged IP VC-Mux
MPoA	LLC/SNAP	1483 Routed IP VC-Mux(IPoA)
		1483 Bridged IP(IPoE)

Všeobecná stránka umožní nastavit první PVC. Pro nastavení druhého PVC, klikněte na záložku **Bridge**. Otevře se stránka konfigurace Bridge.

Multi-PVC

Základní		Bridge			
Kanal	Zapnout	P1	P2	P3	P4
1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pozn: 1.Kanal 1 az 4 rezervovany pro Nat/Route uziv.

2.P1 je rezervovano pro Nat/Route uziv.

OK

Vymazat

Zrusit

Zapnout (Enable)

Zaškrtněte toto políčko abyste povolili tento kanál. Mohou být povolené pouze kanály 5-8, protože kanály 1-4 jsou rezervovány pro použití NAT.

P1 až P4

Porty lokální sítě. Zaškrtněte políčko, abyste vyhradili port pro kanál 5-8.

Pokud kliknete na **Vymazat** (Clear), vymažete všechna nastavení na stránce. Pokud dokončíte konfiguraci klikněte na OK, abyste uložili nastavení a opustili stránku, nebo **Zrušit** (Cancel), abyste přerušili konfiguraci a opustili stránku.

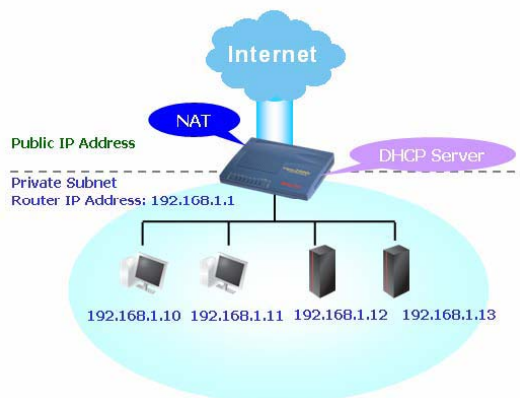
3.2 LAN

Local Area Network (lokální síť - LAN) je skupina podsítí řízená routerem. Určení struktury sítě záleží na tom, jaký typ veřejné IP adresy vám poskytuje poskytovatel.

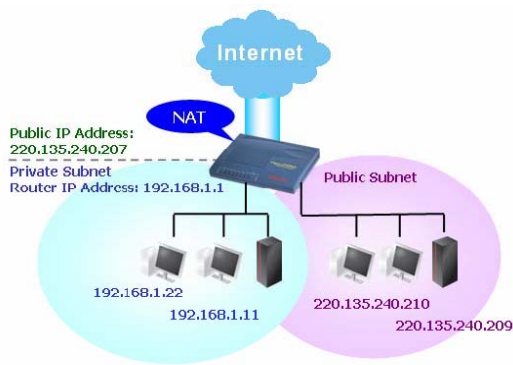


3.2.1 Základy LAN

Nejběžnější funkce routeru Vigor je NAT. Vytváří vaší privátní síť. Router komunikuje s veřejnými hostiteli pomocí veřejné IP adresy a místními hostiteli prostřednictvím privátní IP adresy. Překládá a přeposílá pakety hostiteli a od hostitele. Přitom má i zabudovaný DHCP server, který přiřazuje privátní IP adresu každému místnímu hostiteli, viz. diagram.



Ve výjimečných případech lze vlastnit veřejnou IP síť od poskytovatele jako např. 220.135.240.0/24. Tzn., že si můžete nastavit veřejnou podsít, příp. druhou podsít, ve které má každý hostitel svou veřejnou IP adresu. V tomto případě slouží router na routování IP adres, aby pomáhal hostitelům v této síti komunikovat s jinými veřejnými hostiteli. Za tím účelem bude sloužit jako brána pro veřejné hostitele.



Co je Routing Information Protokol (RIP)

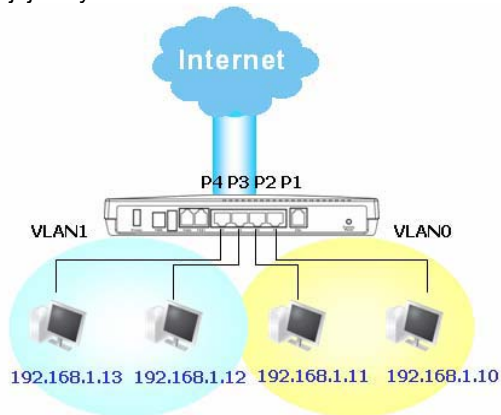
Router Vigor používá RIP na routování IP výměnou routovacích informací se sousedními routery. To umožňuje uživatelům změnit např. IP adresu a routery se informují o změně navzájem.

Co je Statické routování

Pokud máte několik podsítí ve vaší LAN, může být efektivnější a rychlejší spojit je prostřednictvím Statického routování. Jednoduše nastavíte pravidlo přeposílání dat z určité podsítě do druhé bez přítomnosti RIP.

Co jsou Virtuální LAN

Lze vytvořit skupinu místních hostitelů pomocí fyzických portů a vytvořit až 4 virtuální LAN. Abyste řídili komunikaci mezi skupinami, nastavíte pravidlo ve funkci Virtual LAN (VLAN) a jejich rychlost.



3.2.2 Základní nastavení (General Setup)

Tato stránka umožňuje všeobecná nastavení LAN. Klikněte na **LAN** abyste otevřeli stránku pro nastavení LAN a zvolte **Základní nastavení** (General Setup).

[LAN >> Základní nastavení](#)

Ethernet TCP / IP a DHCP nastavení

Konfigurace LAN IP site	Konfigurace DHCP serveru
Pro použití NAT	<input checked="" type="radio"/> Aktivovat server <input type="radio"/> Deaktivovat server
1. IP adresa <input type="text" value="192.168.1.1"/>	Relay Agent: <input type="radio"/> 1. podsít <input checked="" type="radio"/> 2. podsít
1. Maska podsítě <input type="text" value="255.255.255.0"/>	Start IP adresa <input type="text" value="192.168.1.10"/>
Pro užívání IP Routing <input type="radio"/> Zap. <input checked="" type="radio"/> Vyp.	Pocet přidělovaných IP <input type="text" value="50"/>
2. IP adresa <input type="text" value="192.168.2.1"/>	IP adresa brány <input type="text" value="192.168.1.1"/>
2. Maska podsítě <input type="text" value="255.255.255.0"/>	IP adresa DHCP <input type="text"/>
<input type="button" value="DHCP server 2. podsítě"/>	Pro vzdaleneho agenta <input type="text"/>
Kontrola RIP protokolem <input type="text" value="Vyp."/>	IP pro DNS server
	Primární IP adresa <input type="text"/>
	Sekundární IP adresa <input type="text"/>

1. IP adresa (1st IP Address)

Zadejte privátní IP adresu abyste se připojili k místní síti (předvolena je 192.168.1.1).

1. Maska podsítě (1st Subnet Mask)

Zadejte kód adresy, který určuje velikost sítě (předvolený je 255.255.255.0/ 24)

Pro užívání IP Routing (For IP Routing Usage)

Klikněte na **Zap.** (Enable) abyste aktivovali tuto funkci. Předvolená je možnost **Vyp.** (Disable).

2. IP adresa (2nd IP Address)

Zadejte sekundární IP adresu pro připojení do podsítě (předvolena je 192.168.2.1/ 24)

2. Maska podsítě (2nd Subnet Mask)

Zadejte kód adresy, který určuje velikost sítě (předvolený je 255.255.255.0/ 24)

DHCP server 2. podsítě (2nd DHCP Server)

Lze nakonfigurovat router aby sloužil jako DHCP server pro druhou podsít.

Sekundární DHCP server

Start IP adresa	<input type="text"/>
Pocet IP	<input type="text" value="0"/> (max. 10)

Index	Shodne MAC adresy	Pridelena IP adresa
<div style="border: 1px solid black; height: 100px;"></div>		

MAC adresa : : : : : :

Start IP adresa (Start IP Address)

Zadejte do pole počáteční IP adresu, aby DHCP server začal přidělovat IP adresy. Pokud je druhá IP adresa routeru 220.135.240.1, počáteční IP adresa musí být 220.135.240.2 a vyšší, ale méně než 220.135.240.254.

Počet IP (IP Pool Counts)

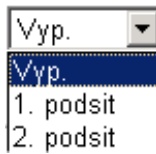
Zadejte počet přidělovaných IP adres. Maximum je 10. Příklad: pokud zadáte 3 a druhá IP adresa routeru je 220.135.240.1, rozsah IP adres bude od 220.135.240.2 do 220.135.240.4.

MAC adresa (MAC Address)

Zadejte MAC adresu hostitele a klikněte na **Přidat** (Add) abyste vytvořili seznam hostitelů, pro které má být IP adresa přidělena, změněna, nebo vymazána. Nastavte seznam MAC adres. Druhý DHCP server pomůže routeru přiřadit správné IP adresy správným podsítím a správným hostitelům, takže hostitelé v druhé podsíti nedostanou přidělené adresy náležící hostitelům v první podsíti.

Řízení RIP protokolu (RIP Protocol Control)

Vypnout (Disable) deaktivuje RIP protokol. To vede k zastavení výměny routovacích informací mezi routery.



1. podsít' (1st Subnet)

Router bude vyměňovat informace mezi první podsítí a sousedními routery.

2. podsít' (2nd Subnet)

Router bude vyměňovat informace mezi druhou podsítí a sousedními routery.

Konfigurace DHCP serveru

DHCP je zkratka pro Dynamic Host Configuration Protocol. Při firemních nastaveních routeru router slouží jako DHCP server. Automaticky oznamuje související IP nastavení každému místnímu uživateli, který je nastaven jako DHCP klient. Pokud nemáte v síti DHCP server, je doporučeno povolit routeru aby pracoval jako DHCP server. Pokud máte v síti jiný DHCP server, lze umožnit funkci Relay Agent pomoci přesměrovat požadavky DHCP do určených umístění:

Aktivovat server (Enable Server)-Umožní routeru přidělit IP adresu každému hostiteli v LAN.

Deaktivovat server (Disable Server)-Umožní přiřadit IP adresy manuálně.

Relay Agent (1. podsít'/2. podsít')- Určí které podsíti budou zasílány DHCP požadavky.

Start IP adresa (Start IP Address)-Zadejte hodnotu první adresy z rozsahu IP adres, které bude DHCP server přidělovat. Pokud je první IP adresa 192.168.1.1, počáteční musí být 192.168.1.2 a vyšší ale méně než 192.168.1.254.

Počet přidělovaných IP (IP Pool Counts)-Zadejte maximum počtu přidělovaných IP adres. Předvolených je 50 a maximum je 253.

IP adresa brány (Gateway IP Address)-Zadejte IP adresu brány. Je stejná jako IP adresa routeru, co znamená, že router je předvolená brána.

IP adresa DHCP Pro vzdáleného agenta (DHCP Server IP Address for relay Agent)-Nastavte IP adresu DHCP serveru kterou použijete, takže Relay Agent vám pomůže přeposílat požadavky serveru.

IP pro DNS server (konfigurace DNS serveru)

DNS znamená Domain Name System. Každý Internetový hostitel musí mít jedinečnou IP adresu a ta musí být v textovém tvaru a dobře zapamatovatelné jméno např. www.yahoo.com. DNS server konvertuje uživatelské jméno na ekvivalentní IP adresu.

Primární IP adresa (Primary IP Address)-Zapište první IP adresu DNS serveru, protože poskytovatel by vám měl poskytnout více než jeden DNS server. Pokud je poskytovatel neposkytne, router automaticky použije předvolenou IP adresu DNS serveru 194.109.6.66.

Sekundární IP adresa (Secondary IP Address)-Zapište další IP adresu DNS serveru, protože poskytovatel by vám měl poskytnout více než jeden DNS

server. Pokud je poskytovatel neposkytne, router automaticky použije předvolenou IP adresu DNS serveru 194.98.0.1.

Předvolená IP adresa DNS serveru může být nalezena také pomocí **Online stav** (Online Status): pokud je pole pro primární i sekundární IP adresu prázdné, router přiřadí svou vlastní IP adresu místním uživatelům jako DNS proxy server a použije DNS cache.

Systemový stav		Systemový čas: 0:22:20	
LAN stav	Primární DNS: 194.109.6.66	Sekundární DNS: 194.98.0.1	
IP adresa	TX pakety	RX pakety	
192.168.1.1	5311	4653	

Pokud IP adresa domény už je v DNS cache, router okamžitě rozliší název domény. V opačném případě přepoše router DNS paket externímu DNS serveru připojením se na WAN.

3.2.3 Statické routování

Přejděte na LAN abyste otevřeli stránku nastavení a zvolte **Statické routování** (Static Route)

[LAN >> Staticke routovani](#)

Nastavení statického routování			Zobrazit routovací tabulku		
<u>Index</u>	<u>Cílová adresa</u>	<u>Stav</u>	<u>Index</u>	<u>Cílová adresa</u>	<u>Stav</u>
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

Stav: v --- Aktivní, x --- Neaktivní, ? --- Prázdné

Index

Čísla 1-10 ve sloupci Index umožňují otevřít stránku nastavení statické cesty.

Cílová adresa (Destination Address)

Zobrazuje adresu destinace statické cesty.

Stav (Status)

Zobrazuje stav statického routování.

Index cis. 1

Stav/Akce	Aktivní/Přidat
IP cílové site	???
Maska podsítě	
IP adresa brány	
Sítové rozhraní	LAN

OK Zrusit

Diagnostika >> Routovací tabulka

Aktuální routovací tabulka

| [Obnovit](#) |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/ 255.255.255.0 is directly connected, IFO
```

Přidání statických cest do privátních a veřejných sítí

Zde je příklad nastavení statické cesty v hlavním routeru, tak že uživatelé A a B mohou spolu komunikovat ze dvou různých podsítí pomocí routeru za předpokladu, že přístup na internet je řádně nastaven a router správně pracuje.

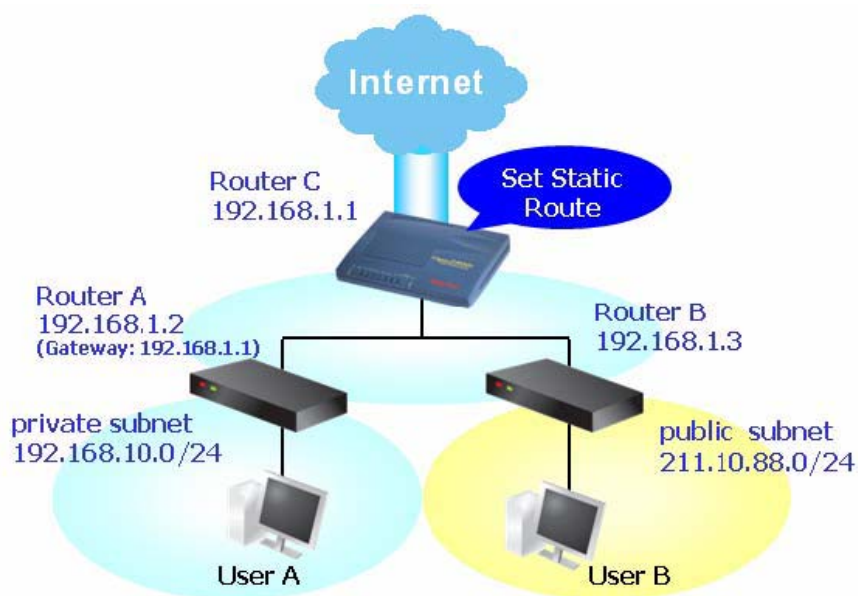
Použijte hlavní router na surfování po internetu.

Vytvořte privátní podsít' 192.168.10.0 pomocí interního routeru A (192.168.1.2)

Vytvořte veřejnou podsít' 211.100.88.0 pomocí interního routeru B (192.168.1.3)

Nastavte hlavní router 192.168.1.1 jako předvolenou bránu pro router A 192.168.1.2

Pokud nastavíte statickou cestu, uživatel A nemůže komunikovat s uživatelem B, protože router A může přeposílat rozpoznané pakety pouze hlavnímu routeru.



1. Přejděte na stránku LAN a klikněte na **Základní nastavení** (General Setup), zvolte 1. podsít' (1st Subnet) v menu **Řízení RIP protokolu** (RIP Protocol Control). Pak klikněte na OK.

Pozn.: Použití Řízení RIP protokolu na první podsíti musíme ze dvou důvodů. Za prvé rozhraní LAN může vyměňovat RIP pakety se sousedními routery pomocí první podsítě (192.168.1.0/24). Za druhé, hostitelé na interních privátních podsítích (192.168.10.0/24) mají přístup na Internet pomocí routeru a kontinuálně vyměňují routovací informace s různými podsítěmi.

2. Klikněte na **LAN-Statické routování** (LAN-Static Route) a na Index č. 1. Přidejte statickou cestu jak je znázorněno níže. Ta zabezpečí že všechny pakety směřované na 192.168.10.0 budou přesměrovány na 192.168.1.2. Klikněte na OK.

LAN >> Nastavení statického routování

Index čís. 1

Stav/Akce	<input type="text" value="Aktivní/Přidat"/>
IP cílové site	<input type="text" value="192.168.10.0"/>
Maska podsítě	<input type="text" value="255.255.255.0"/>
IP adresa brány	<input type="text" value="192.168.1.2"/>
Sítové rozhraní	<input type="text" value="LAN"/>

OK

Zrusit

3. Vraťte se na stránku **Nastavení statického routování** (Static Route Setup). Klikněte na další číslo v sloupci Index a přidejte další statickou cestu jako je znázorněno níže. Ta zabezpečí že všechny pakety směřované na 211.100.88.0 budou přeměřovány na 192.168.1.3.

LAN >> Nastavení statického routování

Index čís. 2

Stav/Akce	Aktivní/Přidat
IP cílové site	211.100.88.0
Maska podsítě	255.255.255.0
IP adresa brány	192.168.1.3
Sítové rozhraní	LAN

OK

Zrusit

4. Přejděte na **Diagnostika** (Diagnostics) a zvolte **Routovací tabulka** (Routing Table) abyste ověřili dosavadní routovací tabulku.

Diagnostika >> Routovací tabulka

Aktuální routovací tabulka

| [Obnovit](#) |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*      0.0.0.0/      0.0.0.0 via 195.72.7.1, IF3
S~    192.168.10.0/ 255.255.255.0 via 192.168.1.2, IF0
C~    192.168.1.0/   255.255.255.0 is directly connected, IF0
S~    211.100.88.0/ 255.255.255.0 via 192.168.1.3, IF0
```

Zakázat Statické routování

1. Klikněte na číslo statického routování ve sloupci Index, které chcete zakázat.
2. Zvolte z menu **Neaktivní/Vypnuto** (Inactive/Disable) a klikněte na tlačítko OK.

Aktivní/Přidat	▼
Prazdny/Vymazat	
Aktivní/Přidat	
Neaktivní/Vypnuto	

3.2.4. VLAN (Virtuální LAN)

Funkce Virtuální LAN poskytuje velmi výhodný způsob, jak řídit hostitele přiřazením do skupin pomocí fyzických portů. Také lze řídit in/out průtok každého portu. Přejděte do menu LAN a zvolte **VLAN**. Zobrazí se následující stránka. Klikněte na **Zapnuto** (Enable), abyste spustili funkci Virtuální LAN.

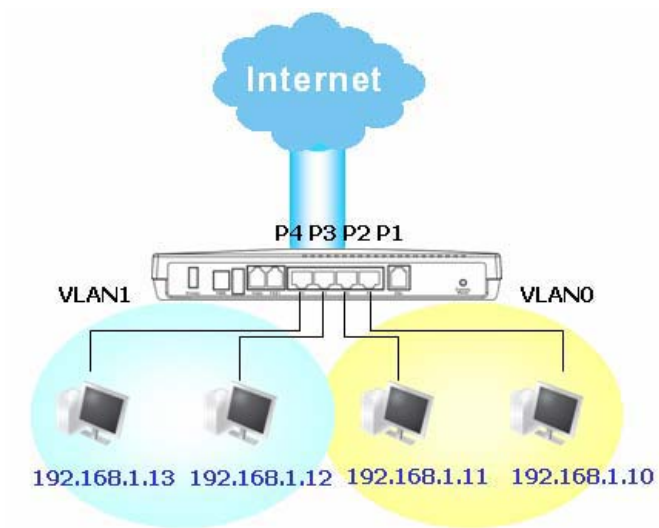
Konfigurace VLAN

<input type="checkbox"/> Zapnuto				
	P1	P2	P3	P4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK	Vymazat	Zrusit
----	---------	--------

Pokud chcete přidat nebo odstranit VLAN, postupujte podle následujícího příkladu.

1. VLAN 0 se skládá z hostitelů připojených na P1 a P2 a VLAN 1 se skládá z hostitelů připojených na P3 a P4.



2. Po zaškrtnutí políčka Aktivovat zaškrtnete políčka v tabulce podle potřeby jako na následujícím obrázku.

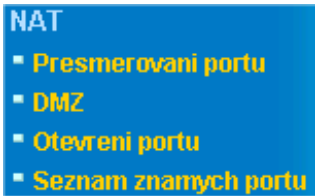
Konfigurace VLAN

<input checked="" type="checkbox"/> Zapnuto	P1	P2	P3	P4
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Vymazat Zrusit

3. Pro odstranění VLAN, zrušte zaškrtnutí políček a klikněte na OK.

3.3 NAT



Router většinou pracuje i jako NAT (Network Address Translation) router. NAT je mechanismus, který umožňuje že jedna nebo více privátních IP adres mohou být zobrazeny jako jedna veřejná. Veřejná IP adresa je většinou přiřazena vaším poskytovatelem jako placená služba. Privátní IP adresy jsou rozeznávány mezi interními hostiteli. Pokud odcházející pakety určené veřejnému serveru na Internetu dorazí NAT router, router změří zdrojovou adresu na veřejnou IP adresu routeru, určí dosažitelný veřejný port a přepoše je. Zároveň si zapíše do tabulky vztah adresy a portu. Pokud veřejný server odpovídá, příchozí data jsou směrována na veřejnou IP adresu routeru a router si to zapíše do vlastní tabulky. Proto interní hostitel může lehce komunikovat s veřejným.

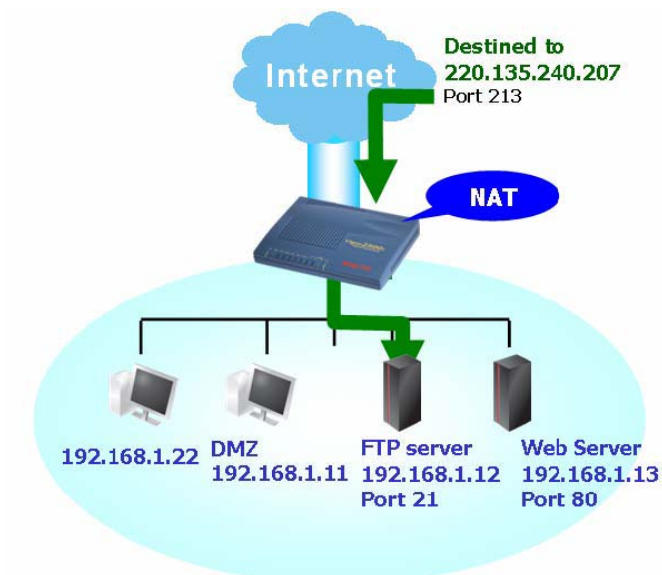
Výhody NAT:

- Šetří náklady při používání veřejných IP adres a zabezpečují efektivní využívání IP adres. NAT umožňuje interní IP adrese místního hostitele aby byla překonvertována na veřejnou, proto lze vlastnit pro všechny interní hostitele pouze jednu veřejnou IP adresu.
- Zvyšuje bezpečnost interní sítě skrytím IP adres. Mnoho útoků je směrováno na IP adresy. Proto pokud útočník nevidí IP adresy, je interní síť je zabezpečena.

Na stránce NAT jsou soukromé IP adresy definovány v RFC-1918. Obvykle používáme pro router podsíť 192.168.1.0/24. Zařízení NAT umožňuje spojit jednu nebo více IP adres nebo portů do různých služeb. Jinými slovy, funkce NAT může být dosažitelná použitím metod přiřazování portů.

3.3.1 Přesměrování portů

Přesměrování portů je většinou nastaveno pro služby související se serverem uvnitř místní sítě, jako web servery, FTP servery, e-mailové servery atd. Ve většině případů potřebujete veřejnou IP adresu pro každý server a tato IP adresa nebo název domény jsou známy všem uživatelům. V případě, že server je umístěn v místní síti, chráněný NAT routeru a identifikovaný IP adresou nebo portem, úlohou této funkce je přesměrovat všechny požadavky na přístup od externího uživatele k přiřazeným IP adresám nebo portům na serveru.



Přesměrování portů je možné použít pouze na přicházející informace.

Abyste použili tuto funkci, Přejděte na stránku **NAT** a zvolte **Přesměrování portů** (Port Redirection). Tabulka nabízí 10 vstupů na přiřazování portů pro interní hostitele.

NAT >> Přesmerování portu

Tabulka přesmerování portu

Index	Jméno služby	Protokol	Verejný port	Privátní IP	Privátní port	aktivní
1	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	---	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

OK

Jméno služby (Service Name)
Zadejte popis síťové služby.

Protokol

Zadejte protokol transportní vrstvy(TCP nebo UDP).

Veřejný port (Public Port)

Špecifikujte, který port může být přeměrován na určitou privátní IP adresu a port interního hostitele.

Privátní IP (Private Address)

Specifikujte privátní IP adresu interního hostitele poskytujícího službu.

Privátní port (Private Port)

Specifikujte číslo privátního portu služby nabízené interním hostitelům.

Aktivní (Active)

Zaškrtněte políčko k aktivaci vámi definovanému přiřazování portů.

Všimněte si, že router má zabudované vlastní služby (servery) jako Telnet, HTTP, FTP atd. Pokud jsou čísla portů těchto služeb (serverů) společná, bude asi třeba resetovat router, abyste se vyhnuli konfliktům.

Např. zabudovaný web-konfigurator v routeru, který má předvolený port 80, se může dostat do konfliktu s webovým serverem v místní síti <http://192.168.1.13:80>. Proto je potřeba změnit http routeru na jakékoliv jiné než 80, abyste se vyhnuli konfliktu, např. 8080. Toto nastavení je možné provést v **Údržba systému >> Správa** (System Maintenance >>Management). Přejdete do okna „Nastavení administrace portů“ a přidáte příponu 8080, t.j. <http://192.168.1.1:8080> namísto portu 80.

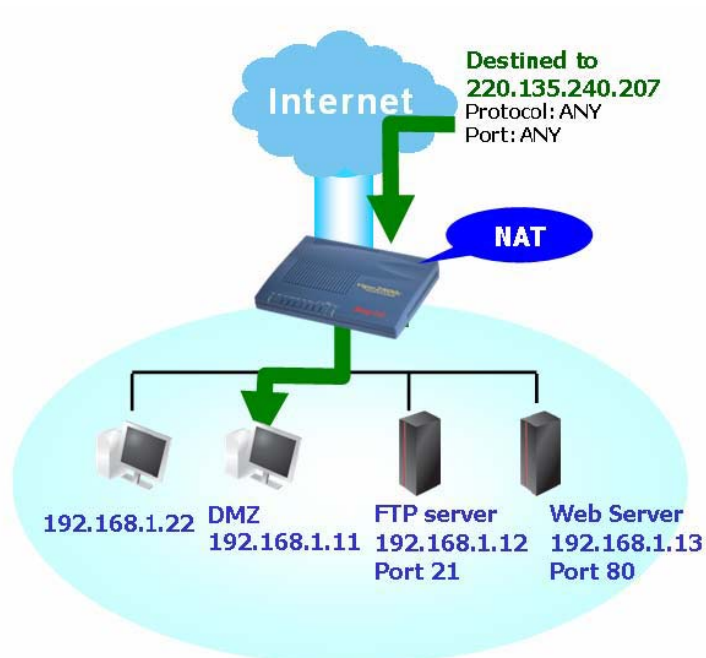
Nastavení spravy

<p>Kontrola přístupu</p> <p><input type="checkbox"/> Aktivovat vzdaleny upgrade firmware(FTP)</p> <p><input type="checkbox"/> Povolit spravu pres internet</p> <p><input checked="" type="checkbox"/> Zakazat ping z internetu</p> <hr/> <p>Seznam povolených přístupu</p> <table border="1"> <thead> <tr> <th>Seznam</th> <th>IP</th> <th>Maska podsítě</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Seznam	IP	Maska podsítě	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	<p>Nastavení administrace portu</p> <p><input type="radio"/> Default porty (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)</p> <p><input checked="" type="radio"/> Uživatelem definované porty</p> <p>Telnet Port <input type="text" value="23"/></p> <p>HTTP Port <input type="text" value="80"/></p> <p>HTTPS Port <input type="text" value="443"/></p> <p>FTP Port <input type="text" value="21"/></p> <hr/> <p>SNMP nastavení</p> <p><input type="checkbox"/> Aktivovat SNMP Agent</p> <p>Get Community <input type="text" value="public"/></p> <p>Set Community <input type="text" value="private"/></p> <p>Manager Host IP <input type="text"/></p> <p>Trap Community <input type="text" value="public"/></p> <p>Notifikace Host IP <input type="text"/></p> <p>Trap Timeout <input type="text" value="10"/> vterin</p>
Seznam	IP	Maska podsítě											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											

OK

3.2.3 DMZ

Jak bylo uvedeno, **Přesměrování portů** (Port Redirection) může přesměrovat přicházející TCP/UDP nebo jiný přenos na konkrétní privátní IP adresu nebo port hostitele v místní síti. Ostatní IP protokoly, např. 50 (ESP) a 51 (AH) se na pevném portu nemění. Router poskytuje možnost DMZ Host, která přiřazuje všechna vyžádaná data jakýmkoliv protokolem jedinému portu místní síti. Běžné surfování po webu a podobné internetové aktivity budou nerušeně fungovat. DMZ hostitel umožňuje definovanému internímu uživateli být viditelný na internetu, to pomáhá aplikacím jako např. Netmeeting, nebo hrám.



Pokud nastavíte DMZ hostitele, částečně tím obejdete bezpečnostní vlastnosti NAT. Navrhujeme přidat dodatečná pravidla filtru a sekundární firewall.

Klikněte na **DMZ** pro otevření následující stránky:

[NAT >> DMZ](#)

DMZ

Zapnout <input type="checkbox"/>	Privatní IP [] . [] . [] . []	Vybrat PC
-------------------------------------	--------------------------------------	-----------

OK

Pokud jste předtím nastavili WAN IP Alias v **Přístup k internetu>>PPPoE/PPPoA** (Internet Access>>PPPoE/PPPoA) nebo **Přístup k internetu>>MPoA** (Internet Access>>MPoA), najdete je v **Připojené WAN IP adresy** (Aux.WAN IP list).

DMZ

Index	Zapnout	Pridana WAN IP	Privatni IP	
1.	<input checked="" type="checkbox"/>	220.135.240.247	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="button" value="Vybrat PC"/>

Zapnout (Enable)

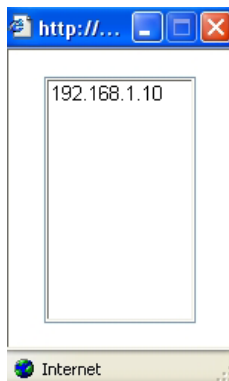
Zaškrtněte pro povolení funkce DMZ host.

Privátní IP (Private IP)

Zadejte privátní IP adresu hostitele DMZ, nebo klikněte na **Vybrat PC** (Choose PC) pro volbu.

Vybrat PC (Choose PC)

Klikněte na toto tlačítko a automaticky se zobrazí okno uvedené níže. Skládá se ze seznamu privátních IP adres všech hostitelů ve vaší místní síti. Zvolte jednu z nich, která bude hostitel DMZ.



Po tom co jste zvolili jednu z privátních IP adres, zobrazí se tato na následující stránce. Klikněte OK, pro uložení nastavení.

3.3.3 Otevření portů (Open Ports)

Otevření skupiny portů umožňuje otevřít rozsah portů pro přenos speciálních aplikací. Společné aplikace Open Ports zahrnují P2P aplikace (např. BT, KaZaA, Gnutella, WinMX, eMule a jiné), webovou kameru apod. Ujistěte se, že udržujete aplikaci aktualizovanou, abyste se vyhnuli útokům na bezpečnost vašeho systému.

Klikněte na **Otevření portů** (Open Ports) pro otevření následující stránky:

Otevreni portu

Index	Poznámka	. Pridana WAN IP	Lokalni IP adresa	Stav
1.				X
2.				X
3.				X
4.				X
5.				X
6.				X
7.				X
8.				X
9.				X
10.				X

Vymazat

Index

Indikuje číslo pro konkrétní vstup, jehož službu chcete provádět na místním hostiteli. Měli byste kliknout na konkrétní číslo, pokud chcete upravit nebo vymazat zodpovídající vstupy.

Poznámka (Comment)

Upřesněte název definované síťové služby.

Připojená WAN IP (Aux.WAN IP)

Zobrazí privátní IP adresu místního hostitele, kterou určíte ve WAN Alias. Toto pole se nezobrazí, pokud jste neurčili žádný Alias na stránce WAN Alias.

Lokální IP adresa (Local IP Address)

Zobrazí privátní IP adresu místního hostitele vykonávajícího službu.

Stav (Status)

Zobrazí stav zodpovídajícího vstupu. „**X**“ znamená **Neaktivní (Inactive)**, „**V**“ znamená **Aktivní (Active)**.

Abyste přidali, nebo změnili nastavení portů, klikněte na indexové číslo na stránce. Zobrazí se stránka nastavení indexových vstupů. Pro každý vstup lze určit 10 rozsahů portů pro různé služby.

Index Cis. 1

Aktivovat otevření portu

Poznámka

Lokální počítač

	Protokol	Start port	Koncový port		Protokol	Start port	Koncový port
1.	TCP	4500	4700	6.	----	0	0
2.	UDP	4500	4700	7.	----	0	0
3.	----	0	0	8.	----	0	0
4.	----	0	0	9.	----	0	0
5.	----	0	0	10.	----	0	0

Pokud jste nastavili WAN Alias v **Přístup k internetu >> PPPoE/PPPoA** (Internet Access>>PPPoE/PPPoA) nebo **Přístup k internetu >> MPoA** (Internet Access>>MPoA), WAN IP bude mezi volbami.

Aktivovat otevření portů (Enable Open Ports)

Zaškrtněte, pokud chcete povolit tento vstup.

Poznámka (Comment)

Zadejte název definované síťové aplikace/služby.

Lokální počítač (Local Computer)

Zadejte privátní IP adresu místního hostitele, nebo klikněte na **Vybrat PC** (Choose PC), pokud chcete zvolit.

Vybrat PC(Choose PC)

Klikněte na toto tlačítko a automaticky se zobrazí okno uvedené níže. Skládá se ze seznamu privátních IP adres všech hostitelů ve vaší místní síti. Zvolte jednu z nich, která bude hostitel.

Protokol

Určete protokol transportní vrstvy. Může to být TCP, UDP, nebo ----(žádný).

Start Port (Start Port)

Určete počáteční číslo portu vykonávající službu na místním hostiteli.

Koncový Port (End port)

Určete konečné číslo portu vykonávajícího službu na místním hostiteli.

Otevreni portu

Index	Poznamka	Lokalni IP adresa	Stav
1.	P2P	192.168.1.10	v
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

Vymazat

3.3.4 Seznam známých portů (Well-Known Ports List)

Tato stránka nabízí přehled známých portů.

[NAT >> Zobrazit seznam známých portu](#)

Seznam znamych portu

Sluzba/Aplikace	Protokol	Cislo portu
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

3. 4 Firewall



3.4.1 Základy firewallu

I když uživatelé širokopásmového internetu požadují větší rozsah pro multimédia, interaktivní aplikace, nebo dálkové studium, nejvíce pozornosti si vyžaduje bezpečnost. Firewall routeru pomáhá chránit vaši místní síť proti útokům neautorizovaných cizích osob. Kromě toho umožňuje restrikce vůči některým uživatelům v místní síti. Dále dokáže vyfiltrovat určité pakety, které spouštějí router, aby vybudoval neoprávněné spojení mimo síť.

Nejzákladnější koncept bezpečnosti je nastavení uživatelského jména a hesla při instalaci routeru. Administrátorské přihlášení tak zabrání neautorizované změně nastavení routeru.

[Udržba systému >> Nastavení hesla administrátora](#)

Heslo administrátora

Původní heslo	<input type="text"/>
Nové heslo	<input type="text"/>
Zopakovat zadání nového hesla	<input type="text"/>

OK

Příslušenství firewallu

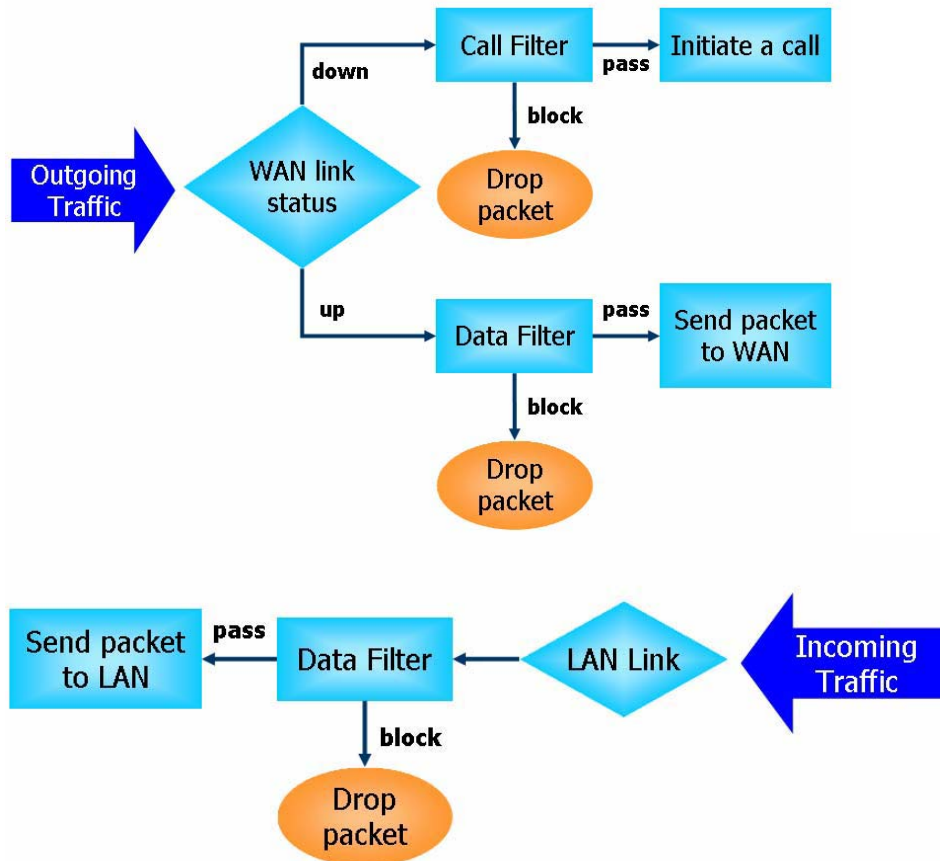
Uživatelé v místní síti jsou chráněni následujícími vlastnostmi:

- Uživatelem nastavitelný IP filtr (Call Filter/ Data Filter).
- Stavová inspekce paketů (SPI): vystopuje pakety a odmítá nežádaná data
- Volitelné Odmítnutí služby DoS (Denial of Service-DoS) /Distribované DoS (DDoS) je obrana proti útokům
- Filtrování obsahu URL

IP filtry

V závislosti na tom, zda jste připojeni k Internetu, jinými slovy „WAN link status je UP nebo DOWN“, architektura IP filtrů dělí přenos dat na dva: Filtr volání (Call Filter) a filtr dat (Data Filter).

- **Filtr volání (Call Filter)**-Pokud nejste připojeni na Internet aplikuje se na všechny odcházející přenosy. Kontroluje odcházející pakety. Pokud jsou povoleny, projdou. Pak router iniciuje „volání“ aby se připojil na Internet a pošle packet na Internet.
- **Filtr dat (Data Filter)**-Při připojení na internet router kontroluje odcházející i přicházející pakety, pokud je jejich obsah povolený, projdou routerem. Takto pracuje router s přicházejícími a odcházejícími přenosy.



Stavová inspekce (Stateful Packet Inspection - SPI)

Stavová inspekce je architektura firewallu, která pracuje v síťové vrstvě. Na rozdíl od legacy static packet filtering, které kontroluje paket na základě hlavičky, stateful inspection kontroluje všechna připojení probíhající přes jakékoliv rozhraní a ujistí se, že jsou odůvodněné. Proto stavová inspekce routeru Vigor nekontroluje jen hlavičky paketů, ale monitoruje i stav připojení.

Blokování aplikací Instant Messenger (IM) a Peer-to-Peer (P2P)

Jak roste popularita těchto aplikací, komunikace již nemůže být jednodušší. I když některá odvětví prohlašují tyto aplikace za skvělé nástroje spojení svých zákazníků, některé mohou mít rezervovanější přístup, protože potřebují snížit jejich používání v pracovních hodinách, případně eliminovat bezpečnostní mezery. Podobná situace je při sdílení souborů pomocí peer-to-peer aplikací, které je výhodné ale nebezpečné zároveň. Kvůli tomu nabízí router schopnost blokovat IM a P2P aplikace.

Obrana před zastavením provozu služeb (DoS) (Denial of Service-DoS Defense)

DoS Defense pomáhá detekovat a zmírnit útoky na provoz služeb. Obvykle jsou dělené na dva druhy – záplavové a poruchové. Záplavové útoky se budou snažit vyčerpat všechny systémové zdroje, když poruchové se budou snažit paralyzovat systém útokem na poruchovost protokolu nebo systému.

DoS Defense umožňuje routeru prohlédnout každý přicházející paket, který má příznaky shodné s pakety v databázi znaků útoku. Každý zlomyslný paket, který by se mohl duplikovat, aby paralyzoval hostitele v bezpečné místní síti, bude blokován a jako varování bude odeslána zpráva Syslog, pokud nastavíte server Syslog. Router také monitoruje přenos. Každý přenos, který odporuje předdefinovaným parametrům, jako např. počet prahů, je identifikován jako útok a router aktivuje mechanismy, aby zmírnil útok v reálném čase.

DoS/DDoS defense může detekovat následující útoky:

- | | |
|----------------------|--------------------------|
| 1. SYN flood attack | 9. Smurf attack |
| 2. UDP flood attack | 10. SYN fragment |
| 3. ICMP flood attack | 11. ICMP fragment |
| 4. TCP Flag scan | 12. Tear drop attack |
| 5. Trace route | 13. Fraggle attack |
| 6. IP options | 14. Ping of Death attack |
| 7. Unknown protocol | 15. TCP/UDP port scan |
| 8. Land attack | |

Filtrování obsahu (Content Filtering)

Abychom poskytli uživatelům průměrný virtuální prostor, je router vybaven filtrem obsahu URL nejen aby omezil ilegální přenos z a na nevhodné web stránky, ale omezuje i jiné webové součásti, které mohou obsahovat škodlivý kód.

Pokud uživatel zadá, nebo klikne na URL s nevhodnými klíčovými slovy, zařízení na blokování klíčových slov zamítne HTTP požadavek na přístup a omezí přístup uživatele. URL Content filter (filtr obsahu URL) si lze představit jako dobře vyškoleného prodávče,

který nebude prodávat dětem časopisy pro dospělé. V kanceláři poskytuje pracovní prostředí spojené jen s výkonem práce a tím zvyšuje efektivitu práce pracovníků. Jak může URL Content Filter pracovat lépe než tradiční firewall? Protože kontroluje řetězce URL nebo některé pakety HTTP, které ukrývají data, zatímco firewall prohlíží pouze pakety na základě TCP/IP hlavičky.

Na druhou stranu router zabrání nepozorným uživatelům stáhnout si škodlivý kód z webových stránek. Je známo, že se škodlivé kódy skrývají ve spustitelných objektech jako ActiveX, Java Applet, komprimované soubory a další samospustitelné soubory. Po stáhnutí těchto souborů nastává velké riziko ohrožení systému. Např. prvky Active X se používají na provoz interaktivních součástí stránky. Pokud skrývají škodlivý kód, může napadnout uživatelův systém.

Filtrování webu (Web Filtering)

Všichni víme že obsah internetu je jako všechna ostatní média a někdy může být nevhodný. Jako zodpovědný rodič nebo zaměstnavatel byste měli před nebezpečím chránit ty co vám důvěřují. Se službou Web Filtering (filtrování webu) lze chránit vaši firmu před snižováním produktivity, ohrožení sítě apod. Jako rodiče lze chránit vaše děti před stránkami s obsahem pro dospělé.

Pokud jste v routeru aktivovali službu Web Filtering a určili kategorie webových stránek které chcete zakázat, bude každá požadovaná URL (např. www.bbc.co.uk) ověřena v databázi spravující SurfControl. Databáze pokrývá 70 řečí v 200 zemích, asi miliardu webových stránek rozdělených do lehce srozumitelných 40 kategorií. Je denně aktualizována globálním týmem webových výzkumníků. Server vyhledá URL a vrátí routeru kategorii. Ten se pak rozhodne zda přístup povolí, nebo ne podle kategorií, které jste si určili. Všimněte si, že tato činnost neovlivní rychlost prohlížení stránek, protože servery dokáží zpracovávat milióny požadavků na kategorizaci.

3.4.2 Základní nastavení (General Setup)

Základní nastavení umožní upravit nastavení IP filtru a jejich základní možnosti. Můžete povolit nebo zakázat Call Filter nebo Data Filter. Za jistých okolností mohou vaše filtry fungovat postupně. Takže určíte jen Start Filter Set (počáteční filtr). Také lze nakonfigurovat nastavení Log Flag a povolit SPI Drop non-http connection on TCP port 80, a Accept incoming fragmented UDP packets.

Klikněte na **Firewall** a **Základní nastavení (General Setup)** abyste otevřeli stránku všeobecných nastavení.

Zakladni nastaveni

Filtr volani	<input checked="" type="radio"/> Zapnuto <input type="radio"/> Vypnuto	Startovací sada filtru <input type="text" value="Sada#1"/>
Datovy filtr	<input checked="" type="radio"/> Zapnuto <input type="radio"/> Vypnuto	Startovací sada filtru <input type="text" value="Sada#2"/>
Priznak logovani	<input type="text" value="Zadny"/>	
<input type="checkbox"/> Zapnout stateful packet inspection <input type="checkbox"/> Pouzit IP filtr pro prichazi VPN pakety <input type="checkbox"/> Zrus pripojeni na TCP portu 80 pokud není http <input checked="" type="checkbox"/> Akceptovat prichazi fragmentovane UDP pakety (pro hry, napr. CS)		

OK

Filtr volání (Call Filter)

Zaškrtněte **Zapnuto** (Enable) pro aktivaci funkce. Určete počáteční sadu pro Filtr volání.

Datový filtr (Data Filter)

Zaškrtněte **Zapnuto** (Enable) pro aktivaci funkce. Určete počáteční sadu pro Datový Filtr.

Příznak logování (Log Flag)

Pro řešení problémů musíte specifikovat záznamy filtru.

Žádný (None)-Funkce není aktivovaná.

Blokovat (Block)-Všechny blokové pakety budou zaznamenány.

Propustit (Pass)-Všechny propuštěné pakety budou zaznamenány.

Nevyhovuje (No Match)-Budou zaznamenány všechny nezařazené pakety.

Pozn.: všechny záznamy budou zobrazeny na terminálu Telnet pokud zadáte příkaz log -f.

Některé online hry (např. Half Life) budou používat velké množství UDP paketů na přenos dat hry. Router instinktivně odmítne tyto částečné pakety, aby zamezil útoku, pokud si nenastavíte povolit "Akceptovat přicházející fragmenty UDP paketů". Zaškrtnutím tohoto pole lze hrát tento druh her. Pokud je vaší prioritou bezpečnost, nemusíte toto povolit.

3.4.3 Nastavení filtrování (Filter Setup)

Klikněte na **Firewall** a **Nastavení filtrování** (Filter Setup) pro otevření stránky nastavení.

[Firewall >> Nastavení filtrování](#)

Nastavení filtrování		Nastavit výrobní nastavení	
Set	Poznámky	Set	Poznámky
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Klikněte na číslo sady, pokud chcete přidat nebo upravit individuální skupinu. Zobrazí se následující stránka. Každý filtr obsahuje 7 pravidel. Klikněte na číslo pravidla abyste ho mohli upravit. Zaškrtněte **Aktivní** (Active) abyste pravidlo povolili.

[Firewall >> Nastavení filtru >> Uprava sady filtru](#)

Sada filtru 1

Poznámky :

Pravidlo filtru	Aktivní	Poznámky
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios
<input type="text" value="2"/>	<input type="checkbox"/>	
<input type="text" value="3"/>	<input type="checkbox"/>	
<input type="text" value="4"/>	<input type="checkbox"/>	
<input type="text" value="5"/>	<input type="checkbox"/>	
<input type="text" value="6"/>	<input type="checkbox"/>	
<input type="text" value="7"/>	<input type="checkbox"/>	

[Další sada filtru](#)

OK

Vymazat

Zrusit

Pravidlo filtrů (Filter Rule)

Klikněte na očíslované tlačítko (1 ~ 7), pokud chcete upravit pravidlo filtru. Kliknutím na tlačítko otevřete stránku **Pravidla filtru** (Edit Filter Rule). Podrobněji viz. další stránka.

Aktivní (Active)

Povolte nebo zakažte pravidlo filtru.

Poznámky (Comment)

Napište poznámky nebo popis filtru, maximálně 23 znaků.

Další sada filtrů (Next Filter Set)

Nastavte odkaz na další sadu filtru, který má být vykonán po spuštění filtru. Nedávejte mnoho filtrů do smyčky.

Abyste nastavili pravidla filtru, klikněte na tlačítko s číslem **Pravidlo filtru** a vstupte na stránku **Pravidla filtru** (Filter Rule setup).

[Firewall >> Nastavení sady filtru >> Nastavení pravidla filtru](#)

Sada filtru 1 Pravidlo 1

Poznámky :

Označením se aktivuje pravidlo filtrování

Propustit nebo blokovat		Připojit k jiné sadě filtru			
<input type="text" value="Blokovat okamžitě"/>		<input type="text" value="Žadny"/>			
<input type="checkbox"/> Log					
Smer	<input type="text" value="IN"/>	Protokol	<input type="text" value="TCP/UDP"/>		
Zdroj	IP adresa	Maska podsítě	Operator	Start Port	Konc.Port
	<input type="text" value="any"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text" value="137"/>	<input type="text" value="139"/>
Cil	<input type="text" value="any"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Kontrola každého paketu		Fragmenty <input type="text" value="Nestarat se"/>			

Poznámky (Comments)

Napište poznámky nebo popis filtru, maximálně 14 znaků.

Označením se aktivuje pravidlo filtrování (Check to enable the Filter Rule)

Zaškrtněte, pokud chcete povolit pravidlo filtru.

<input type="text" value="Propustit okamzite"/>
<input checked="" type="text" value="Blokovat okamzite"/>
<input type="text" value="Propustit pokud nesplnuje predchazejici pravidlo"/>
<input type="text" value="Blokovat pokud nesplnuje predchazejici pravidlo"/>

Propustit nebo blokovat (Pass or Block)

Upřesňuje co sa bude dít s paketem, pokud zodpovídá pravidlu.

Propustit okamžitě (Pass Immediately)-Pakety budou okamžitě propuštěny.

Blokovat okamžitě (Block Immediately)-Pakety budou okamžitě zamítnuty.

Propustit pokud nesplňuje předcházející pravidlo (Pass If No Further Match)-Paket zodpovídající pravidlu, který nezodpovídá žádnému jinému pravidlu bude propuštěn.

Blokovat pokud nesplňuje předcházející pravidlo (Block If No Further Match)-
Paket zodpovídající pravidlu, který nezodpovídá žádnému jinému pravidlu bude zamítnutý.

Připojit k jiné sadě filtrů (Branch to other Filter)

Pokud paket zodpovídá pravidlu, další pravidlo se přidá do sady filtru. Určete další pravidlo z menu.

Log

Zaškrtněte, abyste povolili funkci log. Použijte Telnet příkaz `log-f` abyste zobrazili záznamy.

Směr (Direction)

Nastavte směrování toku paketů. Slouží jen pro Datový filtr. Pro Filtr volání toto nastavení neplatí, protože tento filtr slouží jen při odesílání.

Protokol

Určete protokol/protokoly, které má filtr aplikovat.

IP adresa (IP Address)

Určete zdrojovou a cílovou IP adresu, na kterou má filtr pravidlo aplikovat. Pokud zadáte symbol „!“ před IP adresu, pravidlo nebude aplikováno. Aby bylo aplikováno na všechny IP adresy, zadejte **any** (jakýkoliv), nebo nechte pole prázdné.

Maska podsítě (Subnet Mask)

Zvolte masku podsítě, na kterou má být pravidlo aplikováno, z menu.

Operator, Start Port a Konc. Port

Kolonka Operátor specifikuje nastavení čísel portů. Pokud je pole Start Port prázdné, Start Port a Konc. Port budou ignorovány. Pravidlo filtru bude aplikováno na jakýkoliv filtr. (=) Pokud je prázdné pole Konc. Port, pravidlo nastaví číslo portu jako Start Port. (=)V jiném případě rozsah čísel platí od Start Port do Konc. Port včetně jejich čísel. (!=) Pokud je pole Konc. Port prázdné, číslo se nerovná hodnotě v poli Start Port. V jiném případě toto číslo není mezi Start Port a Konc. Port včetně jejich hodnot. (>) Specifikuje číslo portu větší než Start Port včetně čísla Start Port.

Kontrola každého paketu (Keep State)

Tato funkce pracuje najednou se směrováním, protokolem, IP adresou, maskou podsítě, operátorem, Start Portem a End Portem. Používá se jen pro Datový filtr.

Pojem Keep State je podobný jako pojem Stateful Packet Inspection. Stopuje pakety a akceptuje pakety, které jsou uznané protokolem. Odmítá nevyžádané data. Můžete nastavit jakýkoliv protokol mezi TCP, UDP, TCP/UDP, ICMP a IGMP.



Fragmenty

Specifikuje co se bude dít s fragmentovanými pakety. Používá se jen pro Datový filtr. **Nestarat se** (Don t care)-Fragmentované pakety budou ignorovány.

Nefragmentované (Unfragmented)-Aplikuje pravidlo na nefragmentované pakety.
Fragmentované (Fragmented)-Aplikuje pravidlo na fragmentované pakety.
Příliš krátké (Too Short)-Aplikuje pravidlo jen na pakety, které jsou příliš krátké na to, aby obsahovali úplnou hlavičku.

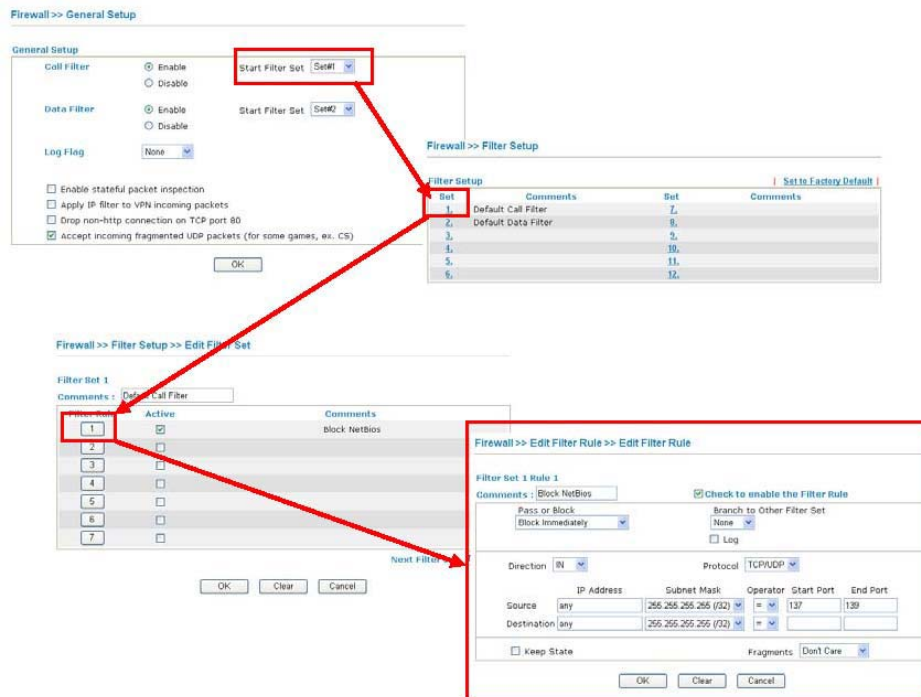
Příklad

Každý přenos bude oddělený a posouzený jedním ze dvou IP filtrů – Filtr volání (call filter) nebo Datový filtr (data filter). Lze předvolit 12 call filtrů a data filtrů ve Filter Setup a nastavit je aby fungovali postupně. Každá sada filtrů je složena ze sedmi pravidel, které mohou být dále definovány. Pak v Základním nastavení (General Setup), lze specifikovat jednu sadu pro Filtr volání (call filter) a jeden pro Datový filtr (data filter), který má být spuštěn první.

The image shows four screenshots from Mikrotik WinBox illustrating firewall configuration steps:

- Firewall >> General Setup:** Shows the 'General Setup' tab. The 'Call Filter' is set to 'Enable' and 'Start Filter Set' is set to 'Set#1'. The 'Data Filter' is also set to 'Enable' and 'Start Filter Set' is set to 'Set#2'. An 'OK' button is visible at the bottom.
- Firewall >> Filter Setup:** Shows the 'Filter Setup' table with 12 filter sets. The first two are highlighted with red boxes:

Set	Comments	Set	Comments
1	Default Call Filter	7	
2	Default Data Filter	8	
3		9	
4		10	
5		11	
6		12	
- Firewall >> Filter Setup >> Edit Filter Set:** Shows 'Filter Set 1' with 'Comments: Default Call Filter'. A red box highlights rule '1' in the list, which is active and has the comment 'Block Netbios'. A 'Next Filter' button is at the bottom right.
- Firewall >> Edit Filter Rule >> Edit Filter Rule:** Shows 'Filter Set 1 Rule 1' configuration. The 'Comments' field contains 'Block Netbios'. The 'Pass or Block' dropdown is set to 'Block Immediately'. The 'Direction' is 'IN' and the 'Protocol' is 'TCP/UDP'. The 'Source' is 'any' with a subnet mask of '255.255.255.255 (/32)'. The 'Destination' is 'any' with a subnet mask of '255.255.255.255 (/32)'. The 'Start Port' is '137' and the 'End Port' is '139'. The 'Fragments' dropdown is set to 'Don't Care'. An 'OK' button is at the bottom.



3.4.4 IM blokování (IM Blocking)

Klikněte na **Firewall** a **IM blokování** (IM Blocking) abyste otevřeli stránku nastavení. Uvidíte seznam běžných IM (jako MSN, Yahoo, ICQ/AQL). Zaškrtněte **Aktivovat IM blokování** (Enable IM Blocking) a zvolte ty, které chcete blokovat. Pokud je chcete blokovat v určitých časových rozmezích, nastavte je v programu **Aplikace >> Plánovač** (Applications>>Schedule).

Firewall >> IM blokovani

Blokovani Messenger aplikaci

- Aktivovat IM blokovani
- Blokovat MSN Messenger
 - Blokovat Yahoo Messenger
 - Blokovat ICQ/AOL

Casovy planovac

Index(1-15) v [Plan](#) nastaveni: , , ,

Pozn.: Akce a nastaveni casu necinnosti budou ignorovana.

OK Zrusit

3.4.5 P2P blokování (P2P Blocking)

Klikněte na **Firewall** a **P2P blokování** (P2P Blocking) abyste otevřeli stránku nastavení. Uvidíte seznam běžných aplikací P2P. Zaškrtněte **Aktivovat P2P blokování** (Enable P2P Blocking) a zvolte ty, které chcete blokovat. Pokud je chcete blokovat v určitých časových rozmezích, nastavte je v programu **Aplikace >> Plánovač** (Applications>>Schedule).

[Firewall >> P2P blokovani](#)

Nastavení blokování sdílení Peer-to-Peer aplikací

Aktivovat P2P blokování

Protokol	Aplikace	Akce
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit <input type="radio"/> Nepovolit upload
FastTrack	KazaA, iMesh, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit
BitTorrent	BitTorrent	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit

Casovy planovac

Index(1-15) in [Plan](#) Nastaveni: , , ,

Pozn: Akce a odpojeni pri necinnosti budou ignorovana.

OK

Zrusit

Akce (Action)

Specifikuje činnost každého protokolu.

Povolit (Allow)-Dovolí klientovi přístup k aplikaci přes specifikovaný protokol.

Nepovolit (Disallow)-Zakáže klientovi přístup k aplikaci přes specifikovaný protokol.

Nepovolit upload (Disallow upload)-Zakáže klientovi přístup k aplikaci přes specifikovaný protokol při downloadu. Upload je povolen.

3.4.6 DoS obrana (DoS Defense)

V nastavení DoS obrany je 15 typů funkcí na detekci a obranu, jako podpoložka funkce IP Filtru/Firewallu. Nastavení DoS obrany je předvoleno jako „zakázané“.

Klikněte na **Firewall** a **DoS obrana** (DoS Defense) k otevření stránky pro nastavení.

DoS obrana

<input type="checkbox"/> Aktivovat DoS ochranu			
<input type="checkbox"/> Aktivovat SYN flood ochranu	Mez citl.	<input type="text" value="50"/>	pakety / vt.
	Odpojit na	<input type="text" value="10"/>	vt.
<input type="checkbox"/> Aktivovat UDP flood ochranu	Mez citl.	<input type="text" value="150"/>	pakety / vt.
	Odpojit na	<input type="text" value="10"/>	vt.
<input type="checkbox"/> Aktivovat ICMP flood ochranu	Mez citl.	<input type="text" value="50"/>	pakety / vt.
	Odpojit na	<input type="text" value="10"/>	vt.
<input type="checkbox"/> Aktivovat detekci skenovani portu	Mez citl.	<input type="text" value="150"/>	pakety / vt.
<input type="checkbox"/> Blokovat IP varianty	<input type="checkbox"/> Blokovat TCP flag skenovani		
<input type="checkbox"/> Blokovat Land	<input type="checkbox"/> Blokovat Tear Drop		
<input type="checkbox"/> Blokovat Smurf	<input type="checkbox"/> Blokovat Ping of Death		
<input type="checkbox"/> Blokovat trace route	<input type="checkbox"/> Blokovat ICMP fragment		
<input type="checkbox"/> Blokovat SYN fragment	<input type="checkbox"/> Blokovat neznamy Protokol		
<input type="checkbox"/> Blokovat Fraggle utok			

OK Vymazat Zrusit

Aktivovat DoS ochranu (Enable DoS Defense)

Zaškrtněte pro aktivaci funkce DoS obrany (DoS Defense Funkcionalita).

Aktivovat SYN flood ochranu (Enable SYN flood defense)

Zaškrtněte pro aktivaci funkce. Pokud paket překročí prahovou hodnotu (mez citlivosti) TCP SYN, Vigor začne náhodně rušit další pakety na dobu, která je definovaná v poli **Odpojit na** (Timeout). Cílem je zabránit paketům TCP SYN, které se snaží vyčerpat omezené prostředky routeru. Hodnoty množství a času jsou předvoleny na 50 paketů za 10 vteřin.

Aktivovat UDP flood ochranu (Enable UDP flood defense)

Zaškrtněte pro aktivaci funkce. Pokud hodnota přijatých UDP paketů z internetu překročí určenou hranici (mez citlivosti), router začne náhodně vymazávat další UDP pakety na čas stanovený v **Odpojit na** (Timeout). Hodnoty množství a času jsou předvoleny na 150 paketů za 10 vteřin.

Aktivovat ICMP flood ochranu (Enable ICMP flood defense)

Zaškrtněte pro aktivaci funkce. Pokud hodnota přijatých ICMP paketů z internetu překročí určenou hranici (mez citlivosti), router začne náhodně vymazávat další ICMP pakety na čas stanovený v **Odpojit na** (Timeout) Hodnoty množství a času jsou předvoleny na 50 paketů za 10 vteřin.

Aktivovat detekci skenování portů (Enable PortScan detection)

Útoky skenováním portů útočí na router posláním velkých množství paketů na více portů, aby útočník našel průnikové nezabezpečené místo. Zaškrtněte políčko pro aktivaci detekce skenování portů. Vždy, když router detekuje posílání paketů nad určitý počet (mez citlivosti), které by mohlo být škodlivé, upozorní vás na to. Předvolené množství je 150 paketů za vteřinu.

Blokovat IP options (Block IP options)

Zaškrtněte pro aktivaci funkce. Router bude ignorovat IP pakety s IP option v hlavičce datagramu. Omezit tyto IP options je vhodné kvůli bezpečnosti místní sítě. Obsahuje totiž informace o bezpečnosti, TCC (uzavřená skupina uživatelů) parametry, internetové adresy, směrovací odkazy apod. Útočník se tak může dozvědět soukromé detaily o vaší síti.

Blokovat Land (Block Land)

Zaškrtněte políčko, pokud chcete posilnit obranu routeru proti útoku Land-Attack. Land-Attack kombinuje útok SYN s IP spoofing. Objeví se, když útočník zasílá falešné SYN pakety s identickou zdrojovou i cílovou adresou i číslem portu napadeného.

Blokovat Smurf (Block Smurf)

Zaškrtněte pro aktivaci funkce. Router bude ignorovat každý požadavek vysílání ICMP echo.

Blokovat trace router (Block trace router)

Zaškrtněte, pokud chcete aby router nepřeposílal trace route pakety (stopovací pakety).

Blokovat SYN fragment (Block SYN fragment)

Zaškrtněte pro aktivaci funkce. Router propustí všechny pakety označené SYN a vícefragmentové sady bitů.

Blokovat Fraggle útok (Block Fraggle Attack)

Zaškrtněte pro aktivaci funkce. Bude blokováno každé vysílání UDP paketů přijatých z internetu. Aktivace obrany DoS/DDoS defense může blokovat i některé legální pakety. Např. pokud aktivujete obranu Fraggle attack, všechny UDP pakety z internetu jsou blokovány, proto mohou být puštěné RIP pakety.

Blokovat TCP flag skenování (Block TCP flag scan)

Zaškrtněte pro aktivaci funkce. Budou vyloučeny všechny TCP pakety. Toto skenování zahrnuje no flag scan, FIN without ACK scan, SYN FINscan, Xmas scan a full Xmas scan.

Blokovat Tear Drop (Block Tear Drop)

Zaškrtněte pro aktivaci funkce. Při příjmu ICMP datagramů se mnohé přístroje mohou zhroutit, pokud tyto překračují maximální délku. Aby jsme se vyhnuli tomuto typu útoku, router je schopen vymazat jakýkoliv fragmentovaný ICMP paket delší než 1024 octetů.

Blokovat Ping of Death (Block Ping of Death)

Zaškrtněte pro aktivaci funkce. Tímto útokem posílá útočník překrývající se pakety cílovým hostitelům, takže ti zůstávají nečinní pokud nejsou pakety zrekonstruovány. Router zablokuje všechny pakety provádějící tento typ útoku.

Blokovat ICMP Fragment (Block ICMP Fragment)

Zaškrtněte pro aktivaci funkce. Všechny ICMP pakety s více bitovými sadami fragmentů jsou vyloučeny.

Blokovat neznámý protokol (Block Unknown Protocol)

Zaškrtněte pro aktivaci funkce. Individuální IP paket má v datagramové hlavičce pole protokolu, aby indikoval typ protokolu v horní vrstvě. Typy protokolů větší než 100 nejsou definovány. Proto router může takové pakety odmítnout.

Výstražné zprávy (Warning Messages)

Router poskytuje funkci Syslog, aby uživatel mohl obdržet zprávu o stavu DoS. Router posílá zprávy jako Syslog klient.

Všechny výstražné zprávy na základě DoS obrany jsou posílány uživateli, který si je může prohlížet přes Syslog daemon. Naleznete-li ve zprávě heslo DoS následované jménem lze zjistit jaký typ útoku byl detekován.

Zaznamy systému(Syslog) / Upozorneni

Zaznamy systemu (SysLog)

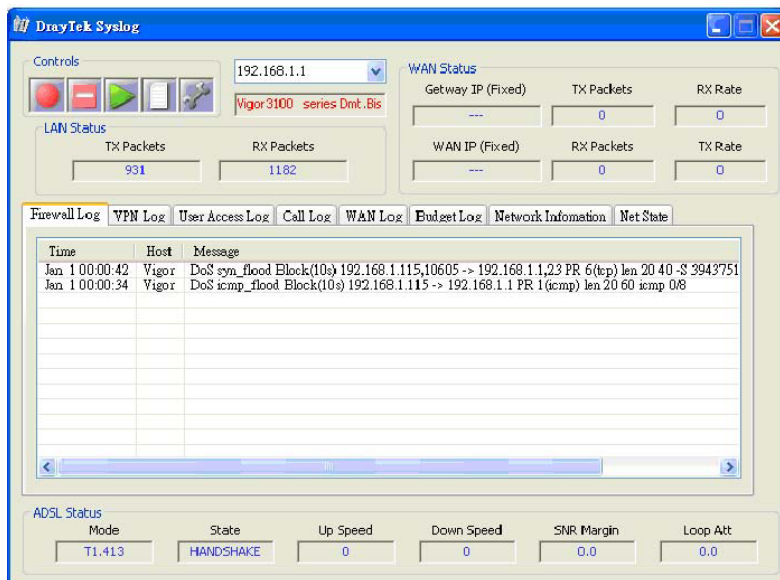
Zapnout

IP adresa serveru

Cilovy port

Zapnout syslog zpravy:

- Firewall zaznamy
- VPN zaznamy
- Zaznamy uzivatel. pristupu
- Zaznamy volani
- WAN Log
- Router/DSL informace



3.4.7 URL obsahové filtrování (URL Content Filter)

Na základě seznamu hesel definovaných uživatelem, prohlíží router řetězce URL při každém HTTP požadavku. Zda už je URL úplná nebo částečná. Pokud obsahuje definované heslo, router přeruší spojení HTTP.

Např. pokud vložíte slovo „sex“, router omezí přístup na stránky typu „www.sex.com“, „www.backdoor.net/images/sex/p_386.html“. Případně můžete určit i částečnou URL jako např. „sex.com“.

Router také zamítne každý požadavek, který se snaží získat škodlivý kód.

Klikněte na **Firewall** a **URL obsahové filtrování** (URL Content Filter) pro otevření stránky nastavení.

Obsahove filtrovani

Aktivovat blokovani pristupu na URL

Black List (blokovani vybranych klic. slov)

White List (povolena vybrana klicova slova)

C.	Akt	Retezec	C.	Akt	Retezec
1	<input type="checkbox"/>	<input type="text"/>	5	<input type="checkbox"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	6	<input type="checkbox"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	7	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	8	<input type="checkbox"/>	<input type="text"/>

moznost zadat retezce slov oddelene mezerou, napr: [hotmail yahoo msn](#)

Zamezeni pristupu na internet z IP adres

Aktivovat zakaz pristupu na web stranky

Java ActiveX Komprimovane soubory Samospustitelne soubory Multimedialni soubory

Cookie Proxy

Aktivovat vyjimky podsiti

C.	Akt	IP adresa		Maska podsiti
1	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>

Casovy planovac

Index(1-15) [Plan](#) nastaveni: , , ,

Pozn: Nastaveni pracovniho casu a casu necinnosti budou ignorovana.

Aktivovat blokování přístupu na URL (Enable URL Access Control)

Zaškrtněte pro aktivaci funkce.

Black List (blokování shodných slov)

Klikněte na tlačítko, pokud chcete zablokovat přístup na stránky obsahující shodné klíčové slovo.

White List (povolení shodných slov)

Klikněte na tlačítko, pokud chcete povolit přístup na stránky obsahující shodné klíčové slovo.

Řetězec (Keyword)

Router poskytuje pro uživatele 8 rámců pro definice hesel. Každý z nich podporuje hromadná hesla. Může to být slovo, část slova, nebo úplný řetězec URL. Hromadná hesla v rámci jsou oddělena mezerou, čárkou, nebo středníkem. Maximální délka je 32 znaků. Po určení hesla router odmítne přístup ke stránkám, které ho obsahují. Čím je heslo jednodušší, tím efektivnější ochranu zabezpečí.

Zamezení přístupu na internet z IP adresy (Prevent web access from IP address)

Zaškrtněte, pokud chcete zabránit surfování po webu s použitím IP adresy např. http://202.6.3.2.. Účelem je nemožnost obejít URL Access Control.

Aby filtrování obsahu URL fungovalo správně, musíte nejprve vymazat cache vašeho prohlížeče.

Aktivovat zákaz přístupu na web stránky (Enable Restrict Web Feature)

Zaškrtněte pro aktivaci funkce.

Java-Zaškrtněte, pokud chcete blokovat objekty Java. Router vyloučí objekty Java přijímané z Internetu.

ActiveX-Zaškrtněte, pokud chcete blokovat objekty Active X. Router vyloučí objekty Active X přijímané z Internetu.

Komprimované soubory (Compressed file)-Zaškrtněte, pokud chcete blokovat přijímání komprimovaných souborů. Budou to soubory s následující příponou: zip, rar, .arj, .ace, .cab, .sit

Spouštěcí soubory (Executable file)-Zaškrtněte, pokud chcete aby router odmítl stahování spustitelných souborů z Internetu, které obsahují přípony: .exe, .com, .scr, .pif, .bas, .bat, .inf, .reg

Cookie-Zaškrtněte, pokud chcete aby router filtroval přenos souborů cookie pro ochranu soukromí uživatele.

Proxy-Zaškrtněte, pokud chcete odmítnout všechny přenosy proxy. Abyste si efektivně uhlídali omezenou šířku přenosu, je vhodné blokovat stahování multimediálních souborů z Internetu které obsahují přípony: .mov .mp3 .rm .ra .au .wmv .wav .asf .mpg .mpeg .avi .ram

Aktivovat výjimky podsítí (Enable Excepting Subnets)

U kontroly přístupu URL je možné vyjmout 4 IP adresy nebo podsítě. Abyste povolili vstup, klikněte na prázdné políčko nazvané ACT před daným vstupem.

Časový plánovač (Time Schedule)

Specifikuje program v jakém čase bude filtr činný.

3.4.8 Web obsahové filtrování (Web Content Filter)

Klikněte na **Firewall** a **Web obsahové filtrování** (Web Content Filter) k otevření stránky pro nastavení.

Tato sekce je podrobně popsána v samostatné příručce **Web obsahové filtrování** (Web Content Filter).

3.4.9 Vazba IP na MAC

Pomocí této funkce je možné přidělovat DHCP serverům vždy stejné IP adresy pro konkrétní MAC adresy, podle definic v tomto okně.

[Firewall >> Vazba IP na MAC](#)

Vazba IP na MAC

Pozn.: Pokud je vybrána Striktní vazba, ostatní IP nevázané na MAC nemohou přistupovat do Internetu.

Zapnout Vypnout Striktní vazba

ARP tabulka | [Vybrat vse](#) | [Druh](#) | [Obnov](#) | **Seznam IP vazeb** | [Vybrat vse](#) | [Druh](#) |

IP adresa	Mac adresa
192.168.1.10	00-0C-76-37-60-3B

Index	IP adresa	Mac adresa
-------	-----------	------------

Přidat a editovat

IP adresa

Mac adresa : : : : :

3.5 Řízení pásma

Rízení pásma

- Limit relací
- Limit šířky pásma
- Kvalita služby (QoS)

3.5.1 Limit relací (Session Limit)

Pomocí této funkce je možné nastavit limit používaných relací (session) pro konkrétní IP adresu.

Relace (Session) – je to každý požadavek přístupu a spojení do internetu jakékoliv aplikace v PC.

[Rízení pásma >> Limit relací](#)

Limit relace

Zap. Vyp.

Default Max relací:

Seznam omezení

Index	Start IP	konec IP	Max relací
-------	----------	----------	------------

Specifická omezení

Start IP: konec IP:

Max počet relací:

Časový plánovač

Index(1-15) [Plan](#) nastavení: , , ,

Pozn.: Akce a nastavení odpojení při nečinnosti budou ignorována.

Zap. (Enable)

Aktivuje funkci limitování relací (session).

Vyp. (Disable)

Deaktivuje funkci limitování session.

Default Max relací (Default Sessions Limit)

Pokud je funkce zapnuta není přidán žádný záznam do Seznamu omezení a bude pro každou IP v LAN použita zadaná hodnota.

Seznam omezení (Limitation List)

Zobrazí vytvořené záznamy.

Start IP (Start IP)

Počáteční IP nového záznamu.

Koncová IP (End IP)

Konečná IP nového záznamu.

Maximum relací (Sessions Limit)

Počet povolených relací (session) pro záznam.

Přidat (Add)

Přidat nový záznam z pole Start IP, Konečná IP a Limit relací

Editovat

Upravit označený záznam v okně Seznamu limitování.

Vymazat (Remove)

Odstranit označený záznam v okně Seznamu limitování

Časový plánovač (Time Schedule)

Umožňuje funkci limitace relací zahrnout do plánovače

3.5.2 Limit šířky pásma

Pomocí této funkce je možné limitovat průtok pro zadané IP adresy v síti LAN, a to směrem ven i dovnitř.

Limit sirky pasma

Zap. Vyp.

Default TX limit: Kbps Default RX Limit: kb/s

Seznam omezeni

Index	Start IP	Konecna IP	TX limit	RX limit

Specifika omezeni

Start IP: Konecna IP:

TX limit: Kbps RX Limit: kb/s

Casovy planovac

Index(1-15) [Plan](#) nastaveni: , , ,

Pozn.: Akce a nastaveni odpojeni pri necinnosti budou ignorovana.

Zap. (Enable)

Aktivuje funkci limitace šírky pásma.

Vyp. (Disable)

Deaktivuje funkci limitace šírky pásma.

Default TX limit

Pokud je funkce zapnuta není přidán žádný záznam do Seznamu omezení. Pro každou IP v LAN bude použita zadaná hodnota a bude limitovaný průtok vysílaných paketů.

Default RX limit

Pokud je funkce zapnuta není přidán žádný záznam do Seznamu omezení. Pro každou IP v LAN bude použita zadaná hodnota a bude limitovaný průtok přicházejících paketů.

Seznam omezení (Limitation List)

Zobrazí vytvořené záznamy

Start IP

Počáteční IP nového záznamu.

Koncová IP (End IP)
Konečná IP nového záznamu.

TX limit
Hodnota limitace odesílaných paketů v kb/s.

RX limit
Hodnota limitace přijímaných paketů v kb/s.

Přidat
Přidat nový záznam z pole Start IP, Konečná IP a TX limit a RX limit.

Edit
Upravit označený záznam v okně Seznam omezení.

Vymazat (Remove)
Odstranit označený záznam v okně Seznam omezení.

Časový plánovač (Time Schedule)
Umožňuje funkci limitace šířky pásma zahrnout do plánovače.

3.5.3 QoS - Kvalita služby

Řízení kvality služby zaručuje, že všechny aplikace budou mít k dispozici dostatečnou úroveň služeb a dostatečnou šířku přenosu, aby vyhověli očekáváním. To je důležitý aspekt moderní podnikové sítě.

Důvodem pro QoS je, že aplikace na bázi TCP stále zvyšují rychlost vysílání a spotřebovávají celou šířku přenosu. To se nazývá pomalý start TCP. Pokud nejsou ostatní aplikace chráněné QoS, omezí to jejich výkon v přeplněné síti. To je důležité hlavně pro ty aplikace, které se těžce vyrovnávají ze ztrátou, zpožděním, nebo chvěním jako např. voice over IP, videokonference, streamované video nebo data.

Další důvod souvisí s tím, že při ucpání intersekcí, jejichž rychlosti jsou rozdílné, pakety se nahromadí a přenos se sníží. Pokud není nadefinovaná priorita specifikovat, který paket má být vymazán z řady, pakety z aplikací uvedených výše mohou být ty které vypadnou.

Jak to ovlivní výkon aplikací?

Klasifikace: identifikace kritických aplikací nebo aplikací s nízkou latencí a označení za vysokou prioritu při přenosu po síti

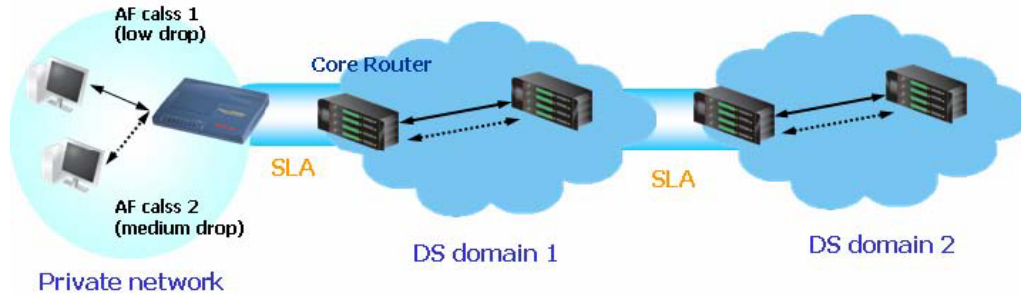
časové programování založené na klasifikaci při přiřazování paketů do řad a asociovaných typů služeb.

Základní implementace QoS v routeru zahrnuje klasifikaci a časové naprogramování paketů založené na hlavičce IP. Např. vzdálený pracovník může na spojení s ústředím použít index řízení QoS aby si rezervoval dostatečnou šířku přenosu pro spojení HTTPS při používání několika aplikací najednou.

Širší implementace je aplikovat DSCP (Differentiated Service Code Point) a IP Precedence na 3. vrstvě. V porovnání s odkazem, IP precedence používající pole IP hlavičky Type of Service (ToS), které definuje 8 tříd služeb, DSCP je jeho následovník vytvářející 64 tříd se

zpětnou kompatibilitou na IP Precedence. V síti se spuštěnou QoS nebo systémem Differentia ted Service (DiffServ nebo DS) vlastník DS domény může podepsat Service License Agreement (Smlouvu o licenci služby - SLA) s jinými vlastníky domén DS, aby si zadefinovali úroveň služby poskytované přenosu z různých domén. Potom každý DS uzel v těchto doménách bude zpracovávat přenos prioritně. Nazývá se per-hop-behavior (chování na skok PHB). Definice PHB zahrnuje Expedited Forwarding (zrychlené přeposílání - EF), Assured Forwarding (zajištěné přeposílání - AF), a Best Effort (nejlepší snaha - BE). AF definuje 4 třídy doručení (nebo přeposlání) a tři úrovně přednosti propadnutí v každé třídě.

Router Vigor jako okrajové routery domén DS zkontrolují hodnoty DSCP v IP hlavičce přenosu aby takto přidělili určité množství zdrojů na provedení zodpovídající kontroly, klasifikace a časového naprogramování. Jádrové routery na páteři provedou stejnou kontrolu než provedou zpracování, aby zajistili konzistenci úrovně služby celou sítí s povoleným QoS.



I tak může mít každý uzel různý postoj k paketům s vysokou prioritou i když jsou spojeny dohodou SLA mezi různými vlastníky DS domén. Je těžké docílit deterministický a konzistentní přenos QoS celou sítí i při snaze routeru Vigor.

Pro efektivnější nastavení QoS, byste měli zkontrolovat dosažené rychlosti ADSL upstream a downstream na stránce Online Stav, pokud budete konfigurovat nastavení QoS.

ADSL info (Verze ADSL Firmware: 131812_B)									
ATM statistiky		TX bloky		RX bloky		Opravené bloky		Neopravitelné bloky	
		2036		2278		0		3	
ADSL stav	Mod	Stav	Rychlost odesílání	Rychlost přijímání	Odstup signal-sum	Tlumení linky.			
	G.DMT	SHOWTIME	320000	3072000	10	49			

Následující taktiky QoS budou definovány ve formě rychlosti poměru upstream/downstream. Jako vodítko k dosažení tohoto cíle vám poskytneme aplikaci QoS requirement. Hodnoty nastavení se budou měnit v závislosti na podmínkách sítě.

Klikněte na Řízení pásma>>Kvalita služby (QoS). Zobrazí se následující okno.

Kvalita sluzby QoS | [Nastavit do vyrobnihho nastaveni](#)

Aktivovat rizeni QoS

Smerovani

Index	Nazev skupiny	Rezerva pasma	Nastaveni	
1.	<input type="text"/>	<input type="text" value="25"/> %	Zakladni	Rozsirene
2.	<input type="text"/>	<input type="text" value="25"/> %	Zakladni	Rozsirene
3.	<input type="text"/>	<input type="text" value="25"/> %	Zakladni	Rozsirene
4.	Jine	<input type="text" value="25"/> %		

Aktivovat rizeni UDP pasma

Pomer pro limitovane pasmo %

[Online statistiky](#)

Aktivovat řízení QoS (Enable the QoS Control)

U modelů V je již předvoleno.

Směrování (Direction)

Definujte, na který přenos mají být nastavení aplikovaná. IN – pouze na přicházející přenosy. OUT – Na odcházející přenosy.

Index

Indexové číslo nastavení řízení QoS. Celkově jsou 4 skupiny.

Název skupiny (Class name)

Definujte název skupiny.

Rezerva pásma (Reserved Bandwidth Ratio)

Je rezervováno pro skupinu ve formě podílu rezervované šířky pásma přenosu a rychlosti upstream a rezervované šířky pásma přenosu a rychlosti downstream.

Nastavení (Setup)

Jsou dvě úrovně nastavení: Základní – Rezervovaná šířka pásma přenosu na základě typu přenosové služby. Poskytlí jsme vám seznam běžných typů služeb. Rozšířené – nastavení rezervované šířky pásma přenosu na základě zdrojové adresy, cílové adresy DiffServ CodePoint a typu služby.

Aktivovat řízení UDP pásma (Enable UDP Bandwidth Control)

Zaškrtněte a nastavte omezenou šířku pásma v pravém poli „Poměr pro limitované pásmo“. Toto ochrání TCP aplikace, pokud přenos UDP aplikací, jako např. streamované video, vyčerpá většinu šířky pásma.

Poměr pro limitované pásmo (Limited bandwidth Ratio)

Tento poměr je používán na omezení celkové šířky pásma používaného UDP aplikacemi.

Základní tlačítko (Basic button)

Klikněte na toto tlačítko, pokud chcete otevřít základní konfiguraci každého indexu.

Management sirky pasma >> Kvalita sluzby QoS

Zakladni nastaveni

Index tridy #1

ANY AUTH(TCP:113) BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67) CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53) FINGER(TCP:79)	PRIDAT >> << ODSTRANIT	
--	-------------------------------	--

Pozn.: V zakladnim nastaveni nastavujeme pouze typ sluzby.
Zdrojova/cilova adresa bude nahrazena pokud stlacite "OK".

OK Vymazat Zrusit

Zvolte jednu z položek z levého boxu a klikněte na ADD>>. Zvolená položka se objeví v pravém. Abyste odstranili položku z pravého boxu, označte ji a klikněte na <<Remove.

Rozšířené tlačítko (Advanced button)

Klikněte na toto tlačítko, pokud chcete otevřít rozšířenou konfiguraci indexu. Na této stránce můžete vkládat, přesouvat, upravovat nebo vymazávat pravidla.

Management sirky pasma >> Kvalita sluzby QoS

Kvalita sluzby (QoS)

Index tridy #1

NE	Stav	Zdrojova adresa	Cilova adresa	DiffServ CodePoint	Typ sluzby
1.	Prazdny	-	-	-	-

Vlozit Nove pravidlo pred (Cislo pravidla).

Posunout Vybrane pravidlo (vybrat Index cislo) do (Cislo pravidla).

Editovat Vybrane pravidlo

Vymazat Vybrane pravidlo

Zrusit

Pokud chcete vložit pravidlo, klikněte na Vložit (Insert) na následující stránce.

Management sirky pasma >> Kvalita služby QoS

Kvalita služby (QoS)

ACT	Zdrojova adresa	Cilova adresa	DiffServ CodePoint	Typ služby
<input type="checkbox"/>	Any <input type="button" value="ZdrojUprava"/>	Any <input type="button" value="CilUprava"/>	ANY <input type="button" value="Pridat"/> <input type="button" value="Uprava"/> <input type="button" value="Vymazat"/>	ANY <input type="button" value="Pridat"/> <input type="button" value="Uprava"/> <input type="button" value="Vymazat"/>

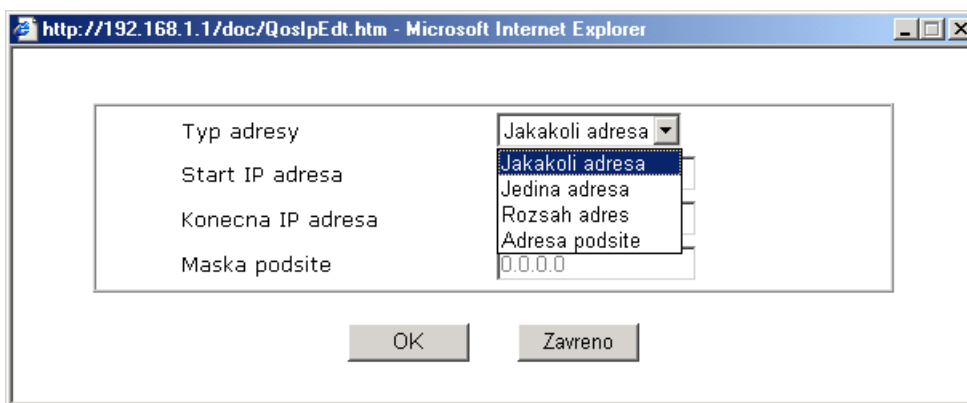
Pozn.: Vyberte, nebo nejprve nastavte typ služby.

ZdrojÚprava (SrcEdit)

Umožňuje upravovat informace o zdrojové adrese.

CílÚprava (DestEdit)

Umožňuje upravovat informace o cílové adrese. Pokud kliknete na jedno z tlačítek, uvidíte následující dialogové okno.



The screenshot shows a Microsoft Internet Explorer window with the address bar displaying "http://192.168.1.1/doc/QosIpEdt.htm". The main content area contains a dialog box with the following fields and options:

- Typ adresy: Dropdown menu with "Jakakoli adresa" selected.
- Start IP adresa: Text input field.
- Konecna IP adresa: Text input field.
- Maska podsítě: Text input field with "0.0.0.0" entered.

At the bottom of the dialog box are two buttons: "OK" and "Zavreno".

Ze seznamu **Typ adresy** si zvolte daný typ adresy. Zadejte počáteční a konečnou IP adresu a masku podsítě.

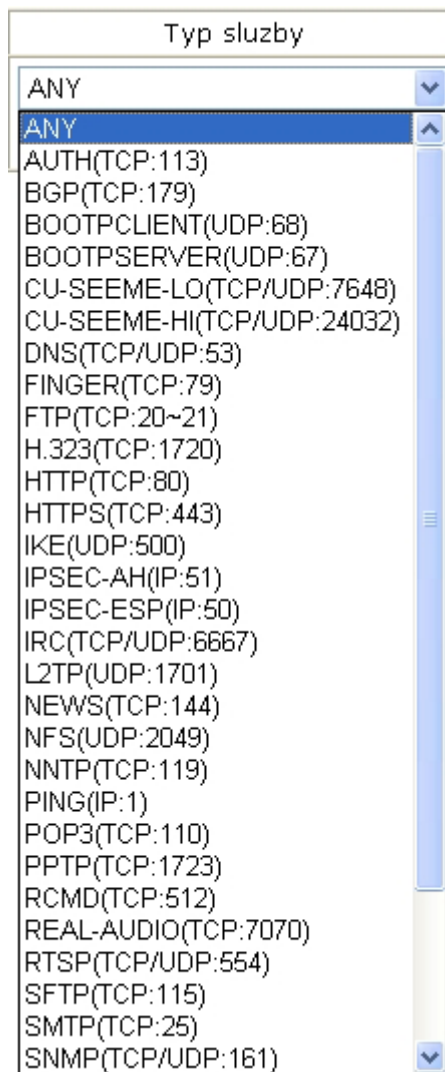
DiffServ CodePoint – všechny pakety budou rozděleny do dvou úrovní a zpracovány podle typu úrovně. Zvolte si úroveň dát na zpracování s kontrolou QoS.

DiffServ CodePoint

ANY

- ANY
- IP precedence 1
- IP precedence 2
- IP precedence 3
- IP precedence 4
- IP precedence 5
- IP precedence 6
- IP precedence 7
- AF Class1 (Low Drop)
- AF Class1 (Medium Drop)
- AF Class1 (High Drop)
- AF Class2 (Low Drop)
- AF Class2 (Medium Drop)
- AF Class2 (High Drop)
- AF Class3 (Low Drop)
- AF Class3 (Medium Drop)
- AF Class3 (High Drop)
- AF Class4 (Low Drop)
- AF Class4 (Medium Drop)
- AF Class4 (High Drop)
- EF Class

Typ služby (Service Type) – Předurčuje typ služby zpracování dat s QoS Control. Může být upravován. Klikněte na Přidat/Úprava/Vymazat (Add/Edd/Delete) a dostanete se na následující stránku.



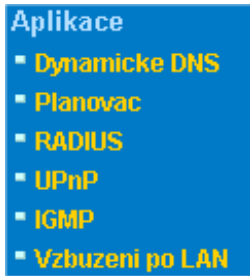
Pokud potřebujete, lze zadat nový název služby. Můžete také upravit nebo vymazat službu (Edit/Delete), kterou jste přidali předtím.

Typ služby

Jmeno služby	<input type="text"/>
Typ služby	<input type="text" value="TCP"/>
Konfigurace portu	
Typ	<input checked="" type="radio"/> Jediný <input type="radio"/> Rozsah
Cislo portu	<input type="text" value="0"/> - <input type="text" value="0"/>

Zadejte prosím **Jméno služby** (Service name) a zvolte **Typ služby** (Service type) (TCP/UDP a obě). Dále zvolte jeden z typů konfigurace portu (jediný nebo rozsah) a zadejte rozsah počtu portů v **Číslo portu** (Port Number).

3.6 Aplikace



3.6.1 Dynamické DNS

Poskytovatel většinou poskytuje na připojení k Internetu dynamickou IP adresu. To znamená, že veřejná IP adresa vašeho routeru se mění při každém připojení. Dynamické DNS umožňuje přiřadit název domény k dynamické IP adrese. Dovoluje routeru aktualizovat souhrn IP adres na určitém dynamickém DNS serveru. Od připojení routeru online budete moci používat registrovaný název domény nebo interní virtuální server z internetu. Je to praktické, pokud poskytujete hostitelský web server, FTP server, nebo jiný server za routerem.

Pokud použijete Dynamické DNS, musíte požádat poskytovatele služby DDNS o DDNS. Router poskytuje tři účty u tří různých poskytovatele DDNS. Router je kompatibilní s www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamichostnameserver.com. Pro registraci navštivte jejich webové stránky.

Povolte funkci a přidejte účet na Dynamické DNS.

Za předpokladu že máte zaregistrovanou DDNS doménu u poskytovatele DDNS, např. hostname.dyndns.org a účet s uživatelským jménem `test` a heslem `test`.

V menu nastavení **Dynamické DNS** zaškrtněte **Aktivovat Dynamické DNS**.

[Aplikace >> Dynamicke DNS](#)

Dynamicke DNS

Aktivovat Dynamicke DNS Zobr. Log

Úcty :

Index	Doména	Aktivováno
1.	---	x
2.	---	x
3.	---	x

Zvolte index 1 a přidejte účet pro router. Zaškrtněte **Aktivovat Dynamické DNS** a vyberte poskytovatele služby: dyndns.org, zadejte registrované hostitelské jméno a příponu dyndns.org do bloku doména. Do následujících polí by mělo být zadáno jméno a heslo „test“.

[Aplikace >> Dynamicke DNS >> Dynamicky DNS ucet](#)

Index : 1

<input checked="" type="checkbox"/>	Aktivovat Dynamicky DNS ucet
Poskytovatel služby	dyndns.org (www.dyndns.org) ▾
Typ služby	Dynamicky ▾
Doména	<input type="text"/> .- ▾
Přihlasovací jméno	<input type="text"/> (max. 23 znaku)
Heslo	<input type="text"/> (max. 23 znaku)
<input type="checkbox"/>	Divoka karta
<input type="checkbox"/>	Zaloha MX
Mail Extender	<input type="text"/>

Poskytovatel služby (Service Provider)

Zvolte poskytovatele služby.

Typ služby (Service Type)

Zvolte typ služby (Dynamic, Custom, Static).

Doména (Domain Name)

Vyplňte název domény.

Přihlašovací jméno (Login)

Přihlašovací jméno nastavené pro použitou doménu.

Heslo (Password)

Zadejte heslo nastavené pro použitou doménu.

Klikněte na tlačítko OK pro aktivaci nastavení. Zobrazí se uložené nastavení.

Součástí Wildcard a Záložní MX nejsou poskytovateli Dynamických DNS podporovány. Podrobnější informace získáte z jejich stránek.

Zrušit funkci a všechny účty DNS

V menu nastavení DDNS odškrtněte **Aktivovat Dynamický DNS účet** (Enable Dynamic DNS Setup) a klikněte na tlačítko **Vymazat** (Clear all).

Vymazat účet DNS

V menu nastavení DDNS klikněte na **Index**, který chcete vymazat a klikněte na tlačítko **Vymazat** (Clear all).

3.6.2 Plánovač (Schedule)

Router má zabudované hodiny reálného času, jejichž čas se aktualizuje manuálně nebo automaticky podle Network Time Protocol (síťových časových protokolů – NTP). To znamená, že lze nastavit router nejen aby se připojil v určitém času, ale také zakázat přístup na Internet v určitých hodinách, takže uživatelé se mohou připojit na Internet v určitých hodinách, např. pracovních. Program je aplikovatelný i na jiné funkce.

Než nastavíte program, musíte nastavit čas. V menu **Údržba systému>> Čas a datum** (System Maintenance>>Time Setup) klikněte v oddíle Informace o čase na tlačítko **Nastavit čas** (Inquire Time) a nastavte čas routeru podle vašeho PC. Při odpojení routeru z elektrické sítě nebo jeho resetování se resetují i hodiny. Jiným způsobem lze nastavit čas požadavků na NTP server (časový server), aby synchronizoval hodiny routeru. Tento způsob lze aplikovat až po připojení na internet.

[Applikace >> Planovac](#)

Planovac:

Index	Stav	Index	Stav
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

Stav: v --- Aktivni, x --- Neaktivni

Vymazat

Lze nastavit až 15 programů a aplikovat je na přístup na internet
Pro nastavení programu klikněte na index a nastavte jej viz. níže.

Index cis. 1

Aktivovat Planovac

Start datum (rrrr-mm-dd) 2000 - 1 - 1

Start Cas (hh:mm) 0 : 0

Cas trvani (hh:mm) 0 : 0

Akce Spustit

Odpojit po 0 min.(max. 255, 0 pro default)

Jak casto

Jedenkrat

Dny v tydnu

Ne Po Ut St Ct Pa So

Aktivovat Plánovač (Enable Schedule Setup)

Zaškrtněte abyste aktivovali program.

Start Datum (rrrr-mm-dd) (Start Date)

Upřesněte datum začátku programu.

Start Čas (hh:mm) (Start Time)

Upřesněte počáteční čas programu.

Čas trvání (hh:mm) (Duration Time)

Upřesněte trvání programu.

Akce (Action)

Upřesněte, na kterou činnost program volání má být aplikován v čase trvání programu. **Spustit** (Force On)-Udržovat připojení.

Vypnuto (Force Down)-Udržovat připojení odpojené.

Aktivovat vytáčení na vyžádání (Enable Dial-On-Demand)-specifikujte, že připojení má být navázáno na požádání a nastavte hodnotu kedy má být nečinné v poli Idle Timeout.

Deaktivovat vytáčení na vyžádání (Disable Dial-On-Demand)-Uřčete, že připojení bude udrženo dokud probíhá na lince přenos. Pokud je připojení nečinné, delší než nastavený Idle Timeout, připojení se zruší a už se nenaváže.

Odpojit po (Idle Timeout)

Uřčete dobu trvání programu.

Jak často (How often)-specifikujte jak často bude program aplikován.

Jedenkrát (Once)-program bude aplikován jen jednou.

Dny v týdnu (Weekdays)-určete, které dni v týdnu bude program aplikován.

Příklad

Pokud chcete, aby přístup PPPoE Internet byl připojen neustále (Spustit) od 9:00 do 18:00 celý týden, ostatní čas bude Internet odpojen (Vypnout).

(Spustit)Po - Ne 9:00 do 18:00



- Ujistěte se že PPPoE připojení a nastavení času řádně pracují.
- Nakonfigurujte vždy zapnuto od 9:00 do 18:00 na celý týden.
- Nakonfigurujte **Vypnuto** (Force Down) od 18:00 po další den do 9:00 na celý týden.
- Přiřaďte tyto dva profily k profilu přístupu PPPoE Internet. Nyní bude přístup PPPoE Internet připojen podle programu.

3.6.3 Radius

Remote Authentication Dial-In User Service (RADIUS) je protokol bezpečnostní autentifikace mezi klientem a serverem, které podporuje autentifikaci, autorizaci a účtování. Je široce používaný poskytovateli IS. Je to nejpoužívanější způsob autentifikace a autorizace uživatelů dial-up připojení a tunelovaných sítí.

Zabudované příslušenství routeru RADIUS client umožňuje routeru asistovat vzdálenému dial-in uživateli nebo bezdrátové stanici a RADIUS serveru při vykonávání vzájemné autentifikace. Umožňuje centralizovanou autentifikaci se vzdáleným přístupem pro správu sítě..

[Applikace >> RADIUS](#)

RADIUS server

<input type="checkbox"/> Zapnuto	
IP adresa serveru	<input type="text"/>
Cilovy port	<input type="text"/>
Sdíleny klic	<input type="text"/>
Znovu zadat sdíleny klic	<input type="text"/>

OK

Vymazat

Zrusit

Zapnuto (Enable)

Zaškrtněte, abyste zapnuli RADIUS.

IP adresa serveru (Server IP Address)

Zadejte IP adresu serveru RADIUS.

Cílový port (Destination Port)

Číslo UDP portu, které RADIUS server používá. Předvolená hodnota na základě RFC 2138 je 1812.

Sdílený klíč (Shared Secret)

Server a klient sdílejí klíč který se používá na ověřování zpráv mezi nimi. Obě strany musí mít nakonfigurován stejný klíč.

Zopakovat sdílený klíč (Re-type Shared Secret)

Zadejte klíč ještě jednou pro kontrolu.

3.6.4 UPnP

UPnP (Universal Plug and Play) je protokol který umožňuje instalovat a připojovat zařízení na síť s lehkostí, s jakou se instalují periférie počítače pomocí již existujícího Windows Plug and Play systému. Pro routery NAT je hlavní součástí UPnP "NAT Traversal". NAT Traversal umožňuje aplikacím před firewallem automaticky otvírat porty které potřebují. Je to spolehlivější než vyžadovat od routeru aby sám určil které porty mají být otevřené. Kromě toho uživatel nemusí manuálně nastavovat sdružování portů nebo DMZ. UPnP je k dispozici na Windows XP a router poskytuje potřebnou podporu plnému využití hlasových, video možností i zpráv na MSN Messengeru.

[Aplikace >> UPnP](#)

UPnP

<input type="checkbox"/> Služba UPnP zapnuta
<input type="checkbox"/> Aktivovat službu řízení připojení
<input type="checkbox"/> Aktivovat službu stavu připojení

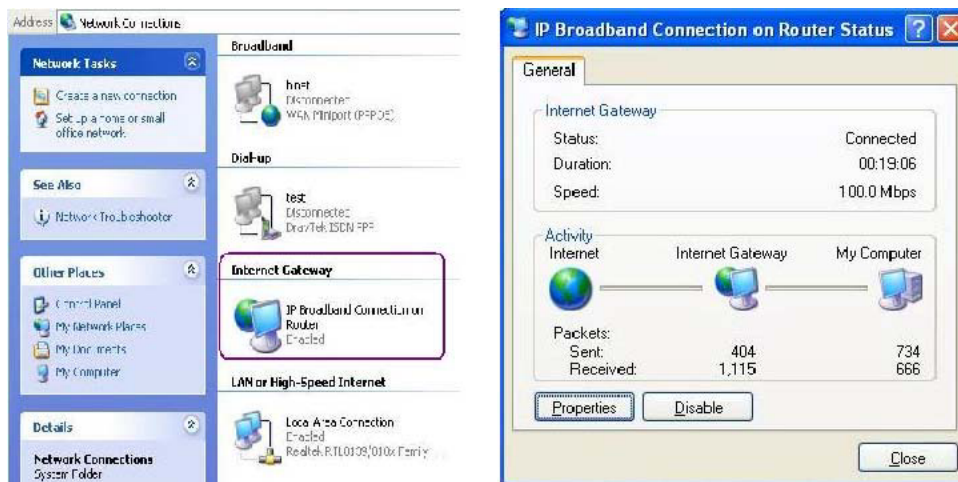
Pozn.: Pokud chcete aby ve vaší vnitřní LAN fungovala služba UPnP, je potřeba službu zapnout a zvolit typ služby.

Služba UPnP zapnuta (Enable UPnP Service)

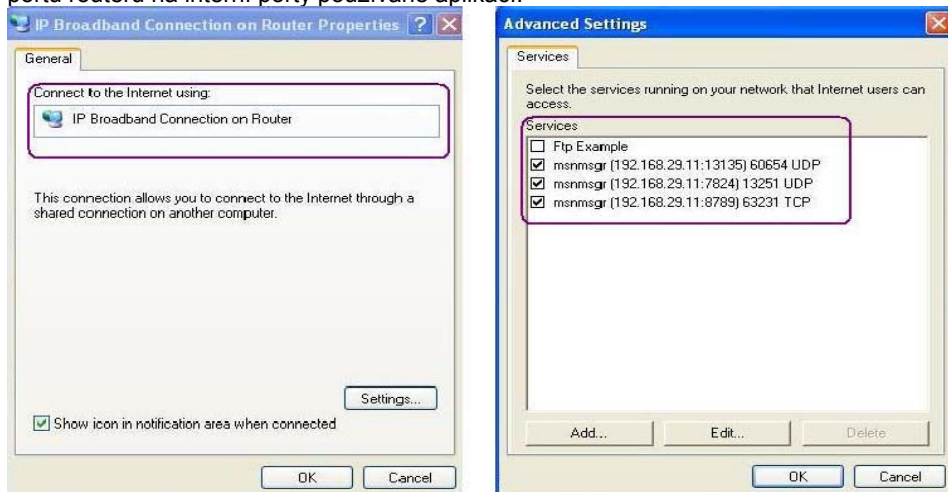
Můžete aktivovat buď **službu řízení připojení** (Connection Control Service) nebo **službu stavu připojení** (Connection Status Service).

Jakmile nastavíte **Služba UPnP zapnuta** (Enable UPnP Service) zobrazí se ikona **IP Broadband Connection on Router** on Windows XP/Network Connections. Stav připojení a stav řízení může být aktivován. NAT Traversal UPnP umožňuje multimediálním

příslušenstvím aplikací pracovat. Sdružování portů je nastaveno manuálně nebo jinou metodou. Obrázky ukazují možnosti tohoto zařízení.



Zařízení UPnP v routeru umožňuje aplikacím, které poznají UPnP, jako např. MSN Messenger, zjistit co se nachází za NAT routerem. Aplikace rozezná i externí IP adresu a nakonfiguruje mapování portů na routeru. Toto zařízení pak přepoše pakety z externího portu routeru na interní porty používané aplikací.



Nemůže pracovat s firewallovým software

Povolení firewallových aplikací na vašem PC může způsobit, že UPnP nebude pracovat správně. Je to z toho důvodu, že tyto aplikace zablokují možnost přístupu na některé porty.

Bezpečnost

Aktivace funkce UPnP ve vaší síti může způsobit ohrožení bezpečnosti. Proto před její aktivací byste měli zvážit rizika.

- Některé operační systémy Microsoft zjistili slabá místa UPnP, proto byste měli mít stáhnuté všechny ServicePacks a záplaty
- Neprivilegovaní uživatelé mohou řídit některé funkce routeru, jako je přidávání a odstraňování mapování portů.

UPnP dynamicky přidává mapování na základě UPnP aplikací. Pokud se aplikace neukončí řádně tato mapování nesmí být odstraněna.

3.6.5. IGMP

IGMP je zkratka pro Internet Group Management Protocol. Je to komunikační protokol využívaný hlavně na řízení členství ve skupinách Internet Protocol multicast. Pro spuštění služby IGMP Snooping, zaškrtněte **Zapnout IGMP Proxy**.

[Aplikace >> IGMP](#)

IGMP

Zapnout IGMP Proxy

IGMP Proxy funguje jako multicast proxy pro hostitele na strane LAN. Zapnout IGMP Proxy, pokud nebude přístupovat do zadne multicast skupiny. Ale tato funkce **nebere v uvahu pokud je zapnut Bridge Mode**.

Zapnout IGMP Snooping

Zapnutí IGMP Snooping, multicast prenosu je pouze presmerovani na porty ktere maji clenstvi v teto skupine.

Vypnute IGMP snooping, multicast provoz je osetren stejnym zpusobem jako broadcast provoz.

OK

Zrusit

[Obnovit](#)

Pracovni Multicast skupiny

Index	Group ID	P1	P2	P3	P4
-------	----------	----	----	----	----

Zapnout IGMP Proxy (Enable IGMP Proxy)

Zaškrtněte, pokud chcete povolit funkci. Aplikace multi-vysílání bude provedena přes port WAN síť.

Zapnout IGMP Snooping (Enable IGMP Snooping)

Zaškrtněte, pokud chcete povolit funkci. Aplikace multi-vysílání bude provedena pro klienty místní síť.

Group ID

Toto pole zobrazuje ID portu skupiny multi-vysílání. Rozsah začíná od 224.0.0.0 do 239.255.255.254.

P1 až P4

Indikace LAN portů používaných pro multi-vysílání.

Obnovit (Refresh)

Klikněte na tuto linku k obnově stavu Click this link to renew the working multicast group status.

Pokud zaškrtnete jen Zapnout IGMP Proxy (Enable IGMP Proxy) , dostanete se na následující stránku. Všechny multicast skupiny budou v seznamu a všechny LAN porty (P1 až P4) jsou použitelné.

Pokud zaškrtnete jen Zapnout IGMP Snooping (Enable IGMP Snooping), dostanete se na následující stránku. I když budou v seznamu všechny skupiny, všechny LAN porty (P1 až P4) ale nejsou použitelné.

Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4
1.	224.0.0.9	v	v	v	v
2.	239.255.255.250	v	v	v	v
3.	225.0.0.1	v	v	v	v

3.6.6. Vzbuzení po LAN (Wake on LAN)

Tato funkce umožňuje z LAN vzbudit PC ze spícího režimu. Tuto funkci musí podporovat i síťová karta v PC a musí být také aktivována.

[Aplikace >> Vzbuzení po LAN](#)

Vzbudit po LAN

Pozn.: Vzbudit po LAN je integrováno s [Vazba IP na MAC](#) funkcí, pouze vazbou určená PC se vzbudí přes IP.

Vzbudit dle:

IP adresa:

MAC adresa:

Vysledek

3.7 VPN a vzdálený přístup (VPN and Remote Access)

VPN a vzdálený přístup
▪ Rízení vzdáleného přístupu
▪ PPP základní nastavení
▪ IPSec základní nastavení
▪ IPSec Peer Identita
▪ Vzdálený Dial-in uživatel
▪ LAN to LAN
▪ Správa spojení

Virtual Private Network (virtuální privátní síť - VPN) je rozšíření LAN sítě o vzdálené sítě a jejich sdílení přes veřejnou síť Internetu. Ve zkratce lze touto technologií posílat data z počítače na počítač přes veřejnou nebo sdílenou síť způsobem jako by šlo o privátní linku point-to-point. Router umožňuje simultánně používat 2 VPN tunely.

3.7.1 Řízení vzdáleného přístupu (Remote Access Control)

Povolte službu VPN. Pokud ale zamýšlíte provozovat VPN server v rámci vaší místní sítě, měli byste VPN routeru tuto službu zakázat, abyste umožnili přechod VPN tunelu a i nastavení NAT jako např. DMZ nebo Otevření portů.

[VPN a vzdálený přístup >> Nastavení vzdáleného přístupu](#)

Nastavení vzdáleného přístupu

<input checked="" type="checkbox"/>	Aktivovat PPTP VPN službu
<input checked="" type="checkbox"/>	Aktivovat IPSec VPN službu
<input checked="" type="checkbox"/>	Aktivovat L2TP VPN službu
<input type="checkbox"/>	Aktivovat ISDN Dial-In

Pozn.: Pokud chcete aby VPN server fungoval ve vaší vnitřní LAN, je potřeba označit správný protokol, aby byl povolen přechod pro danou službu a příslušné nastavení NAT.

OK Vymazat Zrusit

Aktivovat PPTP VPN Službu (Enable PPTP VPN Service)

Zaškrtněte, pokud chcete aktivovat službu VPN přes PPTP protokol.

Aktivovat IPSec VPN Službu (Enable IPSec VPN Service)

Zaškrtněte, pokud chcete aktivovat službu VPN přes IPSec protokol.

Aktivovat L2TP VPN Službu (Enable L2TP VPN Service)

Zaškrtněte, pokud chcete aktivovat službu VPN přes L2TP protokol.

Aktivovat ISDN Dial-IN (Enable ISDN Dial-IN)
Toto políčko bude výhodné pro uživatele v Evropě.

3.7.2 PPP základní nastavení (PPP General Setup)

Toto menu je aplikovatelné jen na připojení VPN spojené s PPP jako např. PPTP, L2TP, L2TP přes IPSec.

[VPN a vzdálený přístup >> PPP hlavní nastavení](#)

PPP hlavní nastavení

PPP/MP Protokol	Přidělování IP adres pro Dial-In uživatele
Dial-In PPP autentifikace <input type="text" value="PAP nebo CHAP"/>	Start IP adresa <input type="text" value="192.168.1.200"/>
Dial-In PPP kryptování(MPPE) <input type="text" value="Volitelně MPPE"/>	
Oboustranná autentifikace (PAP) <input type="radio"/> Ano <input checked="" type="radio"/> Ne	
Uživatelské jméno <input type="text"/>	
Heslo <input type="text"/>	

OK

Dial-In PPP autentifikace (Dial-In PPP)

Zvolte tuto možnost, pokud chcete aby router ověřil příchozí volání.

Pouze PAP (Authentication PAP Only)-Uživatelé pouze s PAP protokolem.

PAP nebo CHAP (PAP or CHAP)-Zvolení této možnosti znamená, že router bude autentifikovat dial-in uživatele nejprve protokolem CHAP. Pokud uživatel tento protokol nepodporuje, použije router na autentifikaci PAP protokol.

Dial-IN PPP kryptování (Dial-In PPP Encryption)

Tato možnost znamená, že router použije při vzdáleném uživateli dial-in kódovací metodu MPPE. Pokud vzdálený dial-in uživatel tuto metodu nepodporuje, router vyšle pakety „no MPPE encrypted (nekódované MPPE)“. Jinak bude na kódování dat použito kódovací schéma MPPE.

<input type="text" value="Volitelně MPPE"/>
<input checked="" type="text" value="Volitelně MPPE"/>
<input type="text" value="podmíněně MPPE(40/128 bit)"/>
<input type="text" value="Maximálně MPPE(128 bit)"/>

Podmíněně MPPE (40/128bitů) (Require MPPE)-Zvolením této možnosti přikážete routeru kódovat pakety kódovacím algoritmem MPPE. Kromě toho vzdálený uživatel použije na kódování 128 bitové kódování namísto 40 bitového. Jinými slovy, pokud není dostupná 128 bitová metoda, bude použita 40 bitová.

Maximálně MPPE-Tato možnost indikuje, že router použije na kódování jen schéma s maximem bitů (128 bitů).

Vzájemná autentifik. (Mutual Authentication (PAP))

Tato funkce se používá zvláště u jiných routerů nebo klientů, kteří potřebují obousměrnou autentifikaci pro vyšší úroveň bezpečnosti, např. routery Cisco. Pokud váš router vyžaduje vzájemnou autentifikaci, měli byste tuto funkci povolit. Kromě toho byste měli zadat Uživatelské jméno (User name) a heslo (Password).

Start IP Adresa (Start IP Address)

Zadejte počáteční IP adresu dial-in PPP připojení. Měli byste zvolit IP adresu z vaší privátní sítě. Např. pokud adresa vaší sítě je 192.168.1.0/255.255.255.0, měli byste zvolit jako počáteční IP adresu 192.168.1.200. Ale nezapomeňte, že první dvě adresy 192.168.1.200 a 192.168.1.201 jsou rezervovány pro uživatele dial-in ISDN.

3.7.3 IPSec hlavní nastavení (IPSec General Setup)

Ve všeobecném nastavení IPSec se nacházejí dvě hlavní části konfigurace. IPSec má dvě fáze.

- Fáze 1: dohodnutí parametrů IKE včetně kódování, rušení, hodnot parametrů Diffie-Hellman, dobu ochrany následujících IKE výměn, autentifikace obou peerů, které používají buď společný klíč nebo digitální podpis (x.509). Peer, který začne vyjednávání podá návrh postupu vzdálenému peeru a vzdálený peer se snaží najít adekvátní postup s nejvyšší prioritou. Nakonec je nastaven bezpečný tunel pro Fázi 2.
- Fáze 2: vyjednání bezpečnostních metod IPSec včetně autentifikační hlavičky (Authentication Header (AH)) nebo Encapsulating Security Payload (ESP), pro následující výměnu IKE a vzájemné přezkoušení zřízeného bezpečného tunelu.

Existují dvě metody zapouzdření, které jsou používány v IPSec, Transport a Tunnel. Transportní režim přidá AH/ESP objem a použije originální IP hlavičku aby zapouzdřil jen objem dat. Může to být aplikováno jen na místní paket, např. L2TP přes IPSec. Tunelový režim nejen přidá objem AH/ESP ale použije i novou (tunelovou)IP hlavičku aby zapouzdřil původní IP paket. Autentifikační hlavička (Authentication Header (AH)) poskytuje autentifikaci dat integrity IP paketů poslaných mezi dvěma VPN peery. Na to slouží klíčová funkce jednosměrného rozdělení, která vytvoří souhrn zpráv. Tento souhrn je přidán do AH a vysílán spolu s pakety. Na straně příjemce proběhne stejné rozdělení a hodnoty se porovnají s hodnotami v přijaté AH. Encapsulating Security Payload (Zapouzdřující bezpečnostní objem - ESP) je bezpečnostní protokol, který datům poskytuje důvěrnost a ochranu s možností autentifikace a detekce opakování.

VPN IKE/IPSec zakladni nastaveni

Dial-in nastaveni pro vzdaleneho dial-in uzivatele a dynamickeho IP klienta (LAN to LAN).

IKE overovací metoda	
Predsdileny klic	<input type="text"/>
Znovu zadat predsdil. klic	<input type="text"/>
IPSec bezpecnostni metoda	
<input checked="" type="checkbox"/> Stredni (AH)	Data budou overovana, ale nebudou kryptovana.
<input type="checkbox"/> vysoky (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Data budou kryptovana a overovana.	

Autentifikační metoda IKE (IKE Authentication Method)

Obyčejně se aplikuje na ty vzdálené dial-in uživatele nebo uzly (LAN-to-LAN), které používají dynamickou IP adresu a připojení VPN vztahující se na IPSec – připojení jako L2TP přes IPSec a IPSec tunel.

Sdílený klíč (Pre-Shared Key)-specifikujte klíč na IKE ověření.

Znovu zadat sdílený klíč (Re-type Pre-Shared Key)-zadejte klíč znovu.

IPSec bezpečnostní metoda (IPSec Security Method)

Střední (Medium)-(AH) data budou ověřována ale nebudou kryptována

Vysoká (High)-(ESP) data budou ověřovány i kryptována. Lze stanovit kryptovací Data Encryption Standard (DES), Triple DES (3DES) a AES.

3.7.4 IPSec Peer identita (IPSec Peer Identity)

Zde lze upravovat tabulku certifikátů peer, pokud chcete používat digitální certifikáty na autentifikaci peerů v připojení LAN-to-LAN nebo vzdáleném dial-in připojení.

VPN a vzdaleny pristup >> IPSec Peer identita

Ucty X509 Peer ID: [Zmenit do vyrobnihho nastaveni](#)

Index	Jmeno	Index	Jmeno
1.	???	9.	???
2.	???	10.	???
3.	???	11.	???
4.	???	12.	???
5.	???	13.	???
6.	???	14.	???
7.	???	15.	???
8.	???	16.	???

<< [1-16](#) | [17-32](#) >> [Dalsi](#) >>

Změnit do výrobního nastavení (Set to Factory Default)

Klikněte, pokud chcete vymazat všechny indexy.

Index

Klikněte na číslo ve sloupci Index, pokud chcete vstoupit na stránku nastavení totožnosti IPSec Peer.

Jméno (Name)

Zobrazí jméno indexu.

Další (Next)

Klikněte a přistoupíte na další stránku pro nastavení dalších účtů.

Klikněte na každý index, pokud chcete upravit digitální certifikát peeru. Jsou tři úrovně bezpečnosti autentifikace digitálním podpisem. Vyplňte každé pole, abyste autentifikovali vzdálený peer. Následující vysvětlení vás provede vyplňování polí.

[VPN a vzdaleny pristup >> IPSec Peer identita](#)

Index profilu : 1

Jmeno profilu	<input data-bbox="491 651 671 680" type="text" value="???"/>
<input checked="" type="radio"/> Neakceptovat Peer ID	
<input type="radio"/> Akceptovat alternativni jmeno subjektu	
Typ	<input data-bbox="707 808 858 837" type="text" value="IP adresa"/>
<input type="radio"/> Akceptovat jmeno subjektu	
Zeme (C)	<input data-bbox="707 902 778 931" type="text"/>
Stat (ST)	<input data-bbox="707 943 1082 972" type="text"/>
Lokalita (L)	<input data-bbox="707 983 1082 1012" type="text"/>
Organizace (O)	<input data-bbox="707 1023 1082 1052" type="text"/>
Organizacni jednotka (OU)	<input data-bbox="707 1064 1082 1093" type="text"/>
Obecne jmeno (CN)	<input data-bbox="707 1104 1082 1133" type="text"/>
Email (E)	<input data-bbox="707 1144 1082 1173" type="text"/>

OK

Vymazat

Zrusit

Jméno profilu (Profile Name)

Zadejte jméno profilu.

Akceptovat libovolné Peer ID

Zaškrtněte, pokud chcete akceptovat každý peer nezávisle na identitě.

Akceptovat alternativně (Accept Subject Alternative)

Zaškrtněte, pokud chcete akceptovat jedno specifické pole.

Jméno (Name)

Jméno osoby digitálního podpisu peeru se zodpovídající hodnotou. Může to být IP adresa, doména, nebo e-mailová adresa. Pole pod polem typ se zobrazí na základě zvoleného typu.

Akceptovat název subjektu (Accept Subject Name)

Zaškrtněte, pokud chcete akceptovat specifické pole digitálního podpisu peeru s zodpovídající hodnotou. Pole zahrnuje zemi (C), stát (ST), místo (L), organizace (O), organizační jednotka (OU), běžné jméno (CN) a E-mail (E).

3.7.5 Vzdálený Dial-in uživatel (Remote User profiles)

Lze řídit vzdálený přístup tabulkou účtů vzdálených uživatelů, takže uživatelé mohou být autentifikováni při dial-in nebo navázat spojení VPN. Lze nastavit parametry včetně upřesněného spojení peer ID, typ připojení (VPN včetně PPTP, IPsec Tunel a L2TP samotné nebo přes IPsec) a zodpovídající bezpečnostní metody apod.

Router poskytuje 32 přístupových účtů uživatelů dial-in. Přitom lze rozšířit účty na RADIUS server přes zabudovanou funkci RADIUS klient. Následující obrázek znázorňuje sumární tabulku.

VPN a vzdaleny pristup >> Vzdaleny Dial-in uzivatel

Ucty vzdaleneho uzivatele:

[Zmenit do vyrobnihho nastaveni](#) |

Index	Uzivatel	Stav	Index	Uzivatel	Stav
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< [1-16](#) | [17-32](#) >>[Dalsi](#) >>

Stav: v --- Aktivni, x --- Neaktivni

Změnit do výrobního nastavení (Set to Factory Default)

Klikněte, pokud chcete vymazat všechny indexy.

Index

Klikněte na číslo indexu, abyste přešli na stránku nastavení vzdáleného uživatele.

Uživatel ((User)

Zobrazuje uživatelské jméno dial-in uživatele účtu LAN-to-LAN. Symbol ??? znamená, že účet je prázdný.

Stav (Status)

Zobrazuje stav přístupu určitého uživatele. Symbol V a X znázorňuje zda je uživatel aktivní nebo neaktivní.

Další (Next)

Klikněte pro přechod na další stránku na nastavení dalších účtů.

Klikněte na každý index, pokud chcete upravit účet jednoho vzdáleného uživatele. Každý typ Dial-in vyžaduje vyplnění zodpovídajících polí vpravo. Pokud jsou pole šedá, znamená to, že je lze nechat prázdná. Následující vysvětlení vás provede vyplňováním důležitých polí.

VPN a vzdaleny pristup >> Vzdaleny Dial-in uzivatel

Index c. 1

Uzivatsky ucet a autentifikace <input type="checkbox"/> Aktivovat tento ucet Odpojit po <input type="text" value="300"/> vterin	Uzivatske jmeno <input type="text" value="???"/> Heslo <input type="text"/>
Typ povoleneho volani Dial-In <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec tunel <input checked="" type="checkbox"/> L2TP s IPSec principy <input type="text" value="Zadna"/>	Autentifikacni metoda IKE <input checked="" type="checkbox"/> Sdileny klic Sdileny klic IKE <input type="text"/> <input type="checkbox"/> Digitalni podpis (X.509) <input <="" td="" type="text" value="???"/>
<input type="checkbox"/> Specifikovat vzdaleny uzal IP vzdaleneho klienta nebo ISDN cislo <input type="text"/> nebo lokalni ID <input type="text"/>	IPSec bezpecnostni metoda <input checked="" type="checkbox"/> Stredni (AH) Vysoka (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalni ID <input type="text"/> (volitelne)
	Funkce zpetneho volani <input type="checkbox"/> Aktivovat funkci zpetne volani <input type="checkbox"/> Specifikovat cislo zpetneho volani Cislo zpetneho volani <input type="text"/> <input checked="" type="checkbox"/> Aktivace uctu zpetneho volani Ucet zpetneho volani <input type="text" value="30"/> minut

Aktivovat tento účet (Enable this Account)

Zaškrtněte, pokud chcete povolit funkci.

Odpojit po (Idle Timeout)-Pokud je uživatel nečinný po udaném limitu, router zruší připojení. Předvolené nastavení je 300 vteřin.

ISDN

Povolíte vzdálené připojení ISDN dial-in. Lze také nastavit funkci zpětného volání. Měli byste nastavit Uživatelské jméno a heslo vzdáleného uživatele. Toto příslušenství obsahuje jen model *i*.

PPTP

Umožníte vzdálenému uživateli vytvořit připojení PPTP VPN přes internet. Nastavte uživatelské jméno a heslo.

IPSec Tunel

Umožníte vzdálenému uživateli vytvořit IPSec VPN připojení přes internet

L2TP

Umožníte vzdálenému uživateli vytvořit připojení L2TP VPN přes Internet. Lze zvolit L2TP samotné nebo s IPSec. Zvolte si mezi:

Žádná (None)-Neaplikuje politiku IPSec. Vzhledem k tomu může být připojení VPN s L2TP bez IPSec politiky zobrazeno jako jediné L2TP připojení.

Mohla by být (Nice to Have)-Aplikuje nejprve politiku IPSec, pokud je při vyjednávání aplikovatelná. V opačném případě zůstane připojení VPN jen L2TP.

Musí být (Must)-Specifikujte IPSec politiku, aby byla aplikovaná na L2TP připojení.

Specifikovat vzdálený uzel (Specify Remote Node)

Zaškrtnuté políčko-Lze specifikovat IP adresu vzdáleného uživatele nebo peer ID (použitím agresivního režimu IKE).

Nezaškrtnuté políčko-Zvolený typ připojení použije bezpečnostní a autentizační metody nastavené v hlavním nastavení.

Uživatelské jméno (User Name)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ bez IPSec politiky.

Heslo (Password)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ bez IPSec politiky.

Autentizační metoda IKE (IKE Authentication Method)

Tato skupina polí je aplikovatelná na IPSec tunely a L2TP s IPSec politikou, pokud upřesníte IP adresu vzdáleného uzlu. Jediná výjimka je digitální podpis (X.509). Může být nastaven pokud zvolíte IPSec tunel s/ bez upřesnění IP adresy vzdáleného uzlu.

Sdílený klíč (Pre-Shared Key)-Zaškrtněte, pokud chcete spustit funkci a zadejte požadované znaky (1-63).

Digitální podpis (X.509) (Digital Signature (X.509))-Zaškrtněte, pokud chcete spustit tuto funkci a zvolte si předdefinované v účtech X.509 Peer ID.

IPSec bezpečnostní metoda (IPSec Security Method)

Tato skupina polí je důležitá pro IPSec tunely a L2TP s IPSec politikou, pokud upřesníte vzdálený uzel. Abyste zvolili bezpečnostní metodu, zaškrtněte Medium, DES, 3DES nebo AES.

Střední (Medium) (AH) znamená, že data budou ověřena, ale ne kódována. Toto je předvolená možnost. Lze odškrtnout políčko, pokud ji chcete zakázat.

Vysoká (High) (ESP)-znamená, že obsah (data) budou ověřena a zakódována. Lze zvolit kódovací algoritmus Data Encryption Standard (DES), Triple DES (3DES) a AES.

Lokální ID (Local ID)-Upřesněte místní ID, které má být použito na nastavení dial-in v nastavení účtu LAN-to-LAN. Tato položka je volitelná a může být použita jen v agresivním režimu IKE.

Funkce zpětného volání (Callback Funkcion)

Tato funkce poskytuje službu zpětného volání jen pro uživatele ISDN (model i). Vlastníkovi routeru bude telekomunikační společností zaúčtovaný poplatek za připojení. Zaškrtněte, pokud chcete funkci aktivovat (Check to enable Callback function).

Specifikovat číslo zpětného volání (Specify the callback number)-slouží pro vyšší bezpečnost. Pokud specifikujete číslo, router bude volat zpět jen na zadané číslo.

Aktivace účtu zpětného volání (Check to enable callback budget control)-Upřesněte časový rozpočet pro uživatele. Rozpočet bude automaticky snížen při připojení zpětným voláním.

3.7.6 LAN - LAN

Zde lze spravovat připojení LAN-to-LAN pomocí tabulky účtů připojení. Můžete nastavit parametry včetně směrování připojení (dial-in – dovnitř nebo dial-out - ven), peer ID, typ připojení (VPN s PPTP, IPSec Tunel a L2TP samotné nebo s IPSec) a zodpovídající bezpečnostní metody atd.

Router poskytuje 32 účtů, co znamená že podporuje 32 VPN simultánních tunelů.

Následující obrázek znázorňuje sumární tabulku.

[VPN a vzdaleny pristup >> LAN - LAN](#)

LAN - LAN profily:

[Zmenit do vyrobnihho nastaveni](#)

Index	Jmeno	Stav	Index	Jmeno	Stav
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< [1-16](#) | [17-32](#) >>

[Dalsi >>](#)

Stav: v --- Aktivni, x --- Neaktivni

Změnit do výrobního nastavení (Set to Factory Default)

Klikněte, pokud chcete vymazat všechny indexy.

Jméno (Name)

Indikuje jméno účtu LAN-to-LAN. Symbol ??? ukazuje, že účet je prázdný.

Stav (Status)

Indikuje stav individuálního účtu. Symboly V a X ukazují, zda je účet aktivní, nebo neaktivní.

Klikněte na každý index, pokud chcete upravit účet a dostanete se na další stránku. Každý účet obsahuje 4 podskupiny. Pokud jsou pole šedá, znamená to, že je lze nechat volné. Následující výklad vás provede vyplněním důležitých polí:

VPN a vzdaleny pristup >> LAN - LAN

Profil Index : 2

Obecna nastaveni

Jmeno profilu <input data-bbox="560 439 691 465" type="text" value="???"/>	Smer volani <input checked="" type="radio"/> Oba <input type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input type="checkbox"/> Aktivovat tento profil	<input type="checkbox"/> Vždy zapnuto
	Odpojit po <input data-bbox="999 510 1066 537" type="text" value="300"/> vterin
	<input type="checkbox"/> Aktivovat PING aby tunel zustal aktivni
	PING na IP <input data-bbox="999 577 1169 604" type="text"/>

Nastaveni Dial-Out

Typ volaneho serveru <input checked="" type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec tunel <input type="radio"/> L2TP se zasadami IPsec <input data-bbox="596 786 730 813" type="text" value="Zadny"/>	Typ linky <input data-bbox="1050 656 1145 683" type="text" value="64kb/s"/> Uzivatelске jmeno <input data-bbox="1050 696 1225 723" type="text" value="???"/> Heslo <input data-bbox="1050 734 1225 761" type="text"/> PPP overovani <input data-bbox="1050 772 1169 799" type="text" value="PAP/CHAP"/> VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto
Jmeno server IP/Host pro VPN. (jako draytek.com nebo 123.45.67.89) <input data-bbox="352 907 649 934" type="text"/>	Autentifikacni metoda IKE <input checked="" type="radio"/> Sdílený klic <input data-bbox="815 929 1002 956" type="text" value="Sdílený klic IKE"/> <input data-bbox="1050 929 1252 956" type="text"/> <input checked="" type="radio"/> Digitalni podpis(X.509) <input data-bbox="815 996 874 1023" type="text" value="???"/>
	IPsec bezpecnostni metoda <input checked="" type="radio"/> Stredni(AH) <input checked="" type="radio"/> Vysoka (ESP) <input data-bbox="999 1115 1185 1142" type="text" value="DES bez overovani"/> <input data-bbox="815 1153 930 1180" type="text" value="Rozsirene"/>
	Index(1-15) v Plan Setup: <input data-bbox="847 1238 906 1265" type="text"/> , <input data-bbox="930 1238 989 1265" type="text"/> , <input data-bbox="1013 1238 1072 1265" type="text"/> , <input data-bbox="1096 1238 1155 1265" type="text"/>
	Funkce zpetneho volani (CBCP) <input type="checkbox"/> Vyzaduje vzdalene zpetne volani <input type="checkbox"/> Poskytnout ISDN cislo vzdalene strane

Jméno profilu (Profile Name)

Jméno profilu připojení.

Aktivovat tento profil (Enable this profile)

Zaškrtněte, pokud chcete aktivovat tento profil.

Směr volání (Call Direction)

Zadejte povolený směr volání tohoto LAN-to-LAN profilu:

Oba (Both)- iniciátor/odpovídající

Dial Out-jen iniciátor (volání odchozí)

Dial-In-jen odpovídající (příchozí volání)

Vždy zapnuto (Always On)-Zaškrtněte, pokud chcete trvalé připojení VPN.

Odpojit po (Idle Timeout)-Předvolená hodnota je 300 vteřin. Pokud je připojení nečinné nad tuto hodnotu, router připojení zruší.

Aktivovat PING aby tunel zůstal aktivní (Enable PING to keep alive)

Tato funkce pomáhá routeru předurčit stav IPSec VPN připojení, je hlavně užitečná v případě nezvyklého narušení tunelu. Pro podrobnější informace viz. poznámka níže. Zaškrtněte aktivovat přenos PING paketů určité IP adresy.

PING na IP (PING to the IP)

Zadejte IP adresu vzdáleného hostitele umístěného na druhém konci tunelu.

Poznámka:

Aktivovat PING aby tunel zůstal aktivní se používá při nezvyklém přerušení IPSec VPN připojení. Poskytne stav připojení VPN, aby se router rozhodl zda bude volat znovu. Pokud chce za normálních okolností jeden peer ukončit spojení, měla by následovat výměna paketů, aby se navzájem informovali. Pokud se odpojí vzdálený peer bez upozornění, router nebude vědět vyhodnotit situaci. Pro řešení tohoto dilema router kontinuálním posíláním paketů pozná skutečný stav spojení. Je to nezávislé na DPD (dead peer detection – mrtvá detekce peeru).

ISDN

Naváže ISDN spojení se serverem. Měli byste nastavit typ linky a identitu jako uživatelské jméno a heslo pro ověření vzdáleného serveru. Lze dále nastavit zpětné volání (CBCP). Toto příslušenství je pouze pro model *i*.

PPTP

Naváže PPTP VPN spojení se serverem přes internet. Měli byste nastavit typ linky a identitu jako uživatelské jméno a heslo pro ověření vzdáleného serveru.

IPSec tunel

Naváže se serverem spojení IPSec VPN přes Internet.

L2TP se zásadami IPSec

Naváže spojení L2TP VPN přes Internet. Lze zvolit samotné L2TP alone nebo s IPSec.

Žádný (None): Neaplikuje IPSec politiku. Vzhledem na spojení VPN figuruje jako samostatné L2TP spojení.

Mohla by být (Nice to have): Aplikuje nejprve politiku IPSec při vyjednávání. V opačném případě volání ven přes spojení VPN bude samostatné spojení L2TP.

Musí (Must): IPSec politka bude určitě aplikovaná na spojení L2TP.

Uživatelské jméno (User name)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky.

Heslo (Password)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky.

PPP ověřování (PPP Authentication)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky. PAP/CHAP je nejběžnější možnost při divoké kompatibilitě.

VJ komprimace (VJ compression)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky. VJ komprimace je používána pro protokolovou hlavičku TCP/IP protokolu. Normálně se nastavuje na Ano (Yes), aby bylo zlepšeno využití šířky pásma přenosu.

Autentifikační metoda IKE (IKE Authentication Method)

Tato skupina polí je aplikovatelná na IPSec tunely a L2TP s IPSec politikou.

Sdílený klíč (Pre-Shared key)-Zadejte 1-63 znaků klíče.

Digitální podpis (X.509) (Digital Signature (X.509))-Určete jeden z předdefinovaných X.509 Peer ID profilů.

Bezpečnostní metoda IPSec (IPSec Security Method)

Tato skupina polí je důležitá pro IPSec tunely a L2TP s IPSec politikou.

Střední (Medium)

Ověřovací hlavička (Authentication Header) (AH)-Znamená, že data budou ověřována, ale ne kódována. Tato volba je předvolena jako aktivní.

Vysoká (High) (ESP-Encapsulating Security Payload)-Znamená, že objem (data) budou zakódována a ověřována. Zvolte:

DES bez ověřování (DES without Authentication)-Použije DES kódovací algoritmus a nepoužije žádné ověřovací schéma.

DES s ověřováním (DES with Authentication)-Použije kódovací algoritmus DES a MD 5 nebo SHA-1 ověřovací algoritmus.

3DES bez ověřování (3DES without Authentication)-Použije trojitý kódovací algoritmus DES neaplikuje žádné ověřovací schéma.

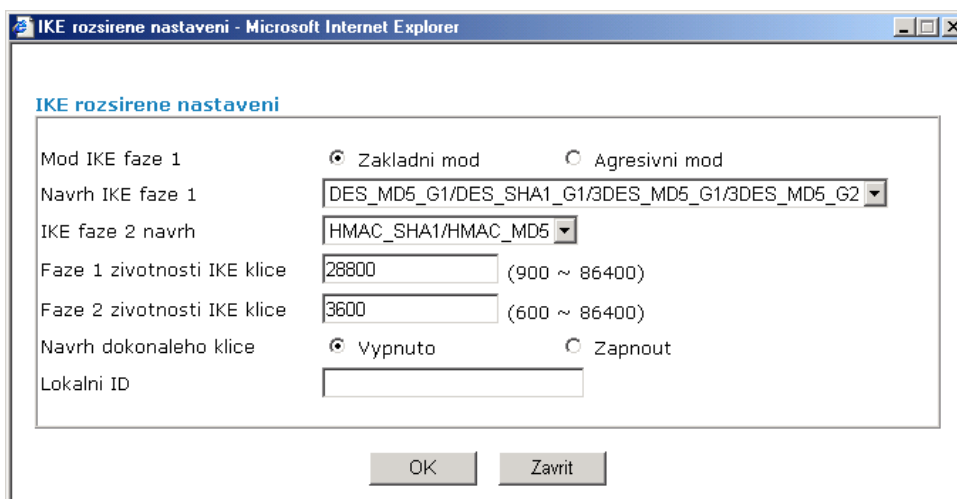
3DES s ověřováním (3DES with Authentication)-Použije trojitý kódovací algoritmus DES a aplikuje MD5 nebo SHA-1 ověřovací algoritmus.

AES bez ověřování (AES without Authentication)-Použije kódovací algoritmus AES a neaplikuje žádné ověřovací schéma.

AES s ověřováním (AES with Authentication)-Použije kódovací algoritmus AES a aplikuje MD5 nebo SHA-1 ověřovací algoritmus.

Rozšířené

Upřesnit mód, návrh a životnost klíče každé IKE fáze, bránu atd. Okno rozšířeného nastavení je znázorněno níže:



Mód IKE fáze 1 (IKE phase 1 mode)-Zvolte základní nebo agresivní mód. Výstupem je výměna bezpečnostních návrhů, aby byl vytvořen bezpečný kanál. Základní mód je bezpečnější než agresivní, protože při více výměnách je realizováno bezpečným kanálem pro nastavení IPSec session. Agresivní mód je rychlejší. Předvolený je základní mód.

Návrh IKE fáze 1 (IKE phase 1 proposal)-Navrhne místní dostupné schéma ověření a algoritmus kódování VPN peerom a přijme odezvu, aby našel shodu. Jsou dostupné dvě kombinace pro agresivní a devět pro základní mód. Navrhujeme, abyste zvolili kombinaci, která pokryje co nejvíce schémat.

Návrh IKE fáze 2 (IKE phase 2 mode)-Navrhne místní dostupné schéma ověření a algoritmus kódování VPN peerom a přijme odezvu, aby našel shodu. Jsou dostupné tři kombinace pro každý mód. Navrhujeme, abyste zvolili kombinaci, která pokryje co nejvíce algoritmů.

Fáze 1 životnosti IKE klíče (IKE phase 1 key lifetime)-Měla by být definovaná z bezpečnostních důvodů. Předvolená hodnota je 28800 vteřin. Lze zadat hodnotu mezi 900 a 86400 vteřinami.

Fáze 2 životnosti IKE klíče (IKE phase 2 key lifetime)- Měla by být definovaná z bezpečnostních důvodů. Předvolená hodnota je 3600 vteřin. Lze zadat hodnotu mezi 600 a 86400 vteřinami.

Návrh dokonalého klíče (PFS) (Perfect Forward Secret (PFS))-Klíč IKE Fáze 1 bude znovu použitý, abychom se vyhnuli přesdílené komplikovanosti zpracování v druhé fázi. Předvolená hodnota je nečinná.

Lokální ID (Local ID)-V agresivním módo slouží lokální ID namísto IP adresy při ověřování se vzdáleným VPN serverem. Délka je omezena na 47 znaků.

Funkce zpětného volání (Require Remote to Callback) (pouze modely *i*)-Tato funkce poskytuje službu zpětného volání odděleně od PPP jen pro uživatele ISDN volání dovnitř. Vlastníkovi routeru bude účtován poplatek za připojení telekomunikační společností.

Vyžadovat zpětné volání od vzdáleného (Provide ISDN Number to Remote)- Aktivujte, pokud chcete aby router vyžadoval vzdálený peer, aby volal zpět na pozdější spojení.

Nastavení Dial-In

Typ povoleného volání Dial-In		
<input checked="" type="checkbox"/> ISDN	Uživatelské jméno <input data-bbox="1046 129 1252 159" type="text" value="???"/>	
<input checked="" type="checkbox"/> PPTP	Heslo <input data-bbox="1046 170 1252 199" type="text"/>	
<input checked="" type="checkbox"/> IPsec tunel	VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto	
<input checked="" type="checkbox"/> L2TP se zasadami IPsec <input data-bbox="595 241 735 271" type="text" value="Zadny"/>		
<input type="checkbox"/> Specifikovat vzdalenou VPN branu pripojovaneho VPN serveru IP <input data-bbox="343 371 549 400" type="text"/>		
nebo lokalni ID <input data-bbox="488 412 691 441" type="text"/>		
Autentifikacni metoda IKE		
<input checked="" type="checkbox"/> Sdilený klic	<input data-bbox="815 331 1002 360" type="text" value="Sdileny klic IKE"/>	
<input type="checkbox"/> Digitalni podpis(X.509)	<input data-bbox="815 405 874 434" type="text" value="???"/>	
IPsec bezpecnostni metoda		
<input checked="" type="checkbox"/> Stredni (AH)		
<input type="checkbox"/> Vysoka (ESP)		
<input checked="" type="checkbox"/> DES	<input checked="" type="checkbox"/> 3DES	<input checked="" type="checkbox"/> AES
Funkce zpetneho volani (CBCP)		
<input type="checkbox"/> Aktivovat funkci zpetneho volani		
<input type="checkbox"/> Pouzit nasledujici cislo pro zpetne volani		
Cislo zpetneho volani	<input data-bbox="1046 707 1252 736" type="text"/>	
Poplatky zpetneho volani	<input data-bbox="1046 748 1121 777" type="text" value="0"/> min.	

Nastavení TCP/IP site

Moje WAN IP	<input data-bbox="560 831 740 860" type="text" value="0.0.0.0"/>	RIP smerovani	<input data-bbox="1046 831 1161 860" type="text" value="TX/RX oba"/>
IP vzdalene brany	<input data-bbox="560 871 740 900" type="text" value="0.0.0.0"/>	Pro NAT operace, zachazet se vzdalenu podsiti jako s	
IP vzdalene site	<input data-bbox="560 911 740 940" type="text" value="0.0.0.0"/>		<input data-bbox="1046 922 1161 952" type="text" value="Privatni IP"/>
Maska vzdalene site	<input data-bbox="560 952 740 981" type="text" value="255.255.255.0"/>		
	<input data-bbox="560 992 635 1021" type="button" value="Vice"/>	<input type="checkbox"/> Zmenit default route pres tento tunel	

Typ povoleného volání Dial-In (příchozí) (Allowed Dial-In Type)

Předdefinuje typ spojení pro příchozí volání.

ISDN

Povolí jen příchozí ISDN dial-in volání. Lze nastavit funkci zpětného volání. Měli byste nastavit uživatelské jméno a heslo pro ověření volajícího vzdáleného uživatele (dial-in). Toto příslušenství je užitečné jen pro model *i*.

PPTP

Povolí vzdáleným dial-in uživatelům PPTP VPN spojení přes internet. Měli byste nastavit uživatelské jméno a heslo pro ověření volajícího vzdáleného uživatele (dial-in).

IPsec Tunnel

Povolí vzdáleným dial-in uživatelům IPsec VPN spojení přes Internet.

L2TP

Umožníte vzdálenému uživateli vytvořit připojení L2TP VPN přes Internet. Lze zvolit L2TP samotné nebo s IPSec. Zvolte si mezi:

Žádná (None)-Neaplikuje politiku IPSec. Vzhledem k tomu může být připojení VPN s L2TP bez IPSec politiky zobrazeno jako jediné L2TP připojení.

Mohla by být (Nice to Have)-Aplikuje nejprve politiku IPSec, pokud je při vyjednávání aplikovatelná. V opačném případě zůstane připojení VPN jen L2TP.

Musí (Must)-Specifikujte IPSec politiku, aby byla aplikovaná na L2TP připojení.

Specifikovat vzdálenou VPN bránu připojovaného VPN serveru IP, nebo lokální ID (Specify CLID or Remote VPN gateway)

Lze specifikovat IP adresu vzdáleného Dial-in uživatele nebo peer ID (mělo by být stejné s ID nastavením u typu volání Dial-in) zaškrtnutím políčka. Pokud zvolíte ISDN (jen model „i“) zadejte číslo peer ISDN. Také byste měli podrobněji specifikovat zodpovídající bezpečnostní metodu v základním nastavení.

Pokud nezaškrtnete políčko, typ spojení použije bezpečnostní metodu nastavenou v základním nastavení.

Uživatelské jméno (User name)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky.

Heslo (Password)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky.

VJ komprimace (VJ Compression)

Toto pole je aplikovatelné, pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky. VJ komprimace je používána pro protokolovou hlavičku TCP/IP protokolu. Normálně se nastavuje na Ano (Yes), aby bylo zlepšeno využití šířky pásma přenosu.

Autentifikační metoda IKE (IKE Authentication Method)

Tato skupina polí je aplikovatelná na IPSec tunely a L2TP s IPSec politikou pokud specifikujete IP připojovaného VPN serveru, nebo číslo ISDN vzdálené VPN brány, nebo IP peeru VPN serveru.

Sdílený klíč (Pre-Shared key)-Zadejte 1-63 znaků klíče.

Digitální podpis (X.509) (Digital Signature (X.509))-Určete jeden z předdefinovaných X.509 Peer ID profilů.

IPSec bezpečnostní metoda (IPSec Security Method)

Tato skupina polí je důležitá pro IPSec tunely a L2TP s IPSec politikou.

Střední (Medium)

Ověřovací hlavička (Authentication Header) (AH)-Znamená, že data budou ověřena, ale ne kódována. Tato volba je předvolena jako aktivní.

Vysoká (High) (ESP-Encapsulating Security Payload)-Znamená, že objem (data) budou zakódována a ověřena. Lze zvolit kódovací algoritmus Data Encryption Standard (DES), trojitě DES a AES.

Funkce zpětného volání (Callback Funkcion)

Tato funkce poskytuje službu zpětného volání jen pro příchozí volání dial-in vzdálených uživatelů ISDN (model *i*). Vlastníkovi routeru bude zaúčtován poplatek za připojení.

Aktivovat funkci zpětného volání (Check to enable Callback function)

Zaškrtněte pro aktivaci funkce.

Číslo zpětného volání (Callback Number)-je pro velmi vysokou bezpečnost. Pokud ho aktivujete, bude vám moci volat pouze zvolené číslo.

Poplatky zpětného volání (Callback budget)-Je předvolen určitý čas zpětného volání.

Pokud jsou poplatky vyčerpány, funkce bude deaktivována.

Poplatky zpětného volání (jednotka:minuty) (Callback budget)(Unit:minutes)-Upřesněte velikost doby určenou pro volání dial-in uživatele. Hodnota se čerpáním automaticky snižuje. Nastavení hodnoty 0 znamená, že není žádné omezení.

Moje WAN IP (My WAN IP)

Toto pole je aplikovatelné jen pokud zvolíte PPTP nebo L2TP s/ nebo bez IPSec politiky. Předvolená hodnota je 0.0.0.0, co znamená, že router dostane PPP IP adresu v době fáze vyjednávání. Pokud je nastavena fixní adresa na vzdálené straně, specifikujte ji i zde.

IP vzdálené brány (Remote Gateway IP)

Toto pole je funkční při volbě PPTP nebo L2TP s/ nebo bez IPSec politiky. Předvolená hodnota je 0.0.0.0, co znamená, že router dostane PPP IP adresu vzdálené brány v době fáze vyjednávání. Pokud je nastavena fixní adresa na vzdálené straně, specifikujte ji i zde.

IP vzdálené sítě/Maska vzdálené sítě (Remote Network IP/ Remote Network Mask)

Přidejte statický router pro nasměrování všech přenosů směrovaných na tuto IP vzdálené sítě/masky vzdálené sítě přes spojení VPN. Pro IPSec je ID cílového klienta fází 2 rychlého módu.

Více (More)

Přidejte statický router pro nasměrování všech přenosů směrovaných na více IP adres vzdálených sítí nebo masek vzdálených sítí přes spojení VPN. Toto se obvykle používá, pokud je za VPN routerem více podsítí.

RIP směrování (RIP Direction)

Tato možnost specifikuje směrování RIP (Routing Information Protocol – protokol routovacích informací) paketů. Lze ji aktivovat nebo deaktivovat. Jsou nabízeny 4 možnosti: TX/RX, jenTX, jen RX a Zakázat.

RIP verze (RIP Version)

Zvolte verzi protokolu RIP. Pro největší kompatibilitu zvolte verzi 2.

Pro NAT operace zacházet se vzdálenou podsítí jako s (For NAT operatin, treat remote sub-net as)

Při komunikaci se vzdálenou podsítí s ní může router zacházet jako s privátní sítí posíláním paketů s privátní IP adresou routeru, nebo jako s veřejnou podsítí posíláním paketů s veřejnou IP adresou routeru.

3.7.7 Správa spojení (Connection Management)

Dostupná je sumární tabulka všech připojení VPN. Lze odpojit každé VPN připojení kliknutím na tlačítko Zrušit. Také lze volat ven v agresivním módu kliknutím na tlačítko vytočit v nástroji na vytočení VPN tunelu.

[VPN a vzdaleny pristup >> Sprava spojeni](#)

nastroj Dial-out Cas obnoveni : 10

Stav VPN spojeni

Aktualni stranka: 1

VPN Typ	Vzdalena IP	Virtualni sit	Tx pakety	Tx prtok	Rx pakety	Rx prtok	Čas od spusteni

xxxxxxxx : Data jsou kryptovana.
xxxxxxxx : Data nejsou kryptovana.

Vytočit (Dial)

Klikněte pokud chcete provést odchozí volání.

Čas obnovení (Refresh Seconds)

Zvolte si čas obnovení z možností 5, 10, a 30 vteřin.

Obnovit (Refresh)

Klikněte pro obnovení stavu připojení.

3.8 Správa certifikátů (Certificate Management)

Sprava certifikatu

- **Lokální certifikát**
- **Důvěryhodný CA certifikát**

Digitální certifikát pracuje jako elektronická identita, která je vydaná důvěryhodným zdrojem (certification authority – CA). Obsahuje informace jako je vaše jméno, sériové číslo, datumy expirace atd. Digitální podpis tohoto zdroje si může příjemce ověřit, tzn., že certifikát je skutečný. Router podporuje digitální certifikáty standardu X.509.

Každá entita, která chce využívat digitální certifikát musí o něho nejdříve požádat na CA serverech.

Zde lze spravovat generování a správu lokálních certifikátů a nastavovat důvěryhodné CA certifikáty. Nezapomeňte nastavit čas routeru pro získání platného časového rozsahu certifikátu.

3.8.1 Lokální certifikát (Local Certificate)

[Sprava certifikatu >> Lokalni certifikat](#)

Konfigurace lokálního X509 certifikátu

Jmeno	Subjekt	Stav	Zmena
Lokalni	---	---	<input type="button" value="Zobrazit"/> <input type="button" value="Vymazat"/>

Lokalni X509 certifikat

Generovat (Generate)

Klikněte na tlačítko, pokud chcete otevřít okno generování certifikátů.

Generovat požadavek na certifikát

Alternativní jméno subjektu	
Typ	<input type="text" value="IP adresa"/>
IP	<input type="text"/>
Jméno subjektu	
Zeme (C)	<input type="text"/>
Stat (ST)	<input type="text"/>
Lokalita (L)	<input type="text"/>
Organizace (O)	<input type="text"/>
Organizační jednotka (OU)	<input type="text"/>
Obecné jméno (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Typ klíče	<input type="text" value="RSA"/>
Velikost klíče	<input type="text" value="1024 Bit"/>

Zadejte všechny požadované informace a opět klikněte **Generovat**.

Import

Klikněte na toto tlačítko pro import uloženého souboru s informacemi o certifikátu.

Obnovit (Refresh)

Klikněte pro obnovu informací.

Zobrazit (View)

Klikněte pro podrobnější nastavení požadavku na certifikát.

Po kliknutí na **Generovat** se informace zobrazí v okně níže:

Konfigurace lokalniho X509 certifikatu

Jmeno	Subjekt	Stav	Zmena
Lokalni		Requesting	Zobrazit vymazat
GENEROVAT IMPORT OBNOVIT			
Zadost na lokalni X509 certifikat			
<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBPzCBqQIBADAAAMIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBggQCOE7aDk1qC EpjkOEoObnqsjojhneOSS8FqnrclmWR/HK10i04HsJ5hd6pMHsoyGgHpaFvHv+uL PIh/1d5gkgvA10vZyH4nJ6pr/g87Y1AEJEmrLvqIy6Z/P3ckpqqx2PuxcTGTCGcp Bk85zNqKkQ0+tudLR8UnuyrKenE1xJ1SIwIDAQABoAAwDQYJKoZIhvcNAQEFBQAD gYEAfHudp1/2PLXcCIPDMtmtSWWNnLkCuJAQqifqXhn1Rglms082DFKxYKEhv1dL 91kwe631s3JX3t6LOzm9QsaSY1zVCqo9IgbeZKW4vrntmkGtrzWNStU1uejcn990 9sK1bKz9B0DmHg0whh4J7Vn07kh8JQxAdXaQpt4E+OmRHTs= -----END CERTIFICATE REQUEST----- </pre>			

3.8.2 Důvěryhodný CA certifikát (Trusted CA Certificate)

Důvěryhodný CA certifikát má v seznamu 3 sady certifikátů.

[Sprava certifikatu >> Duveryhodny CA certifikat](#)

X509 konfigurace duveryhodneho CA certifikatu

Jmeno	Subjekt	Stav	Modify
Duveryhodny CA-1	---	---	Zobrazit Smazat
Duveryhodny CA-2	---	---	Zobrazit Smazat
Duveryhodny CA-3	---	---	Zobrazit Smazat

IMPORT

OBNOVIT

Abyste importovali uložený certifikát, klikněte na **IMPORT** abyste otevřeli následující okno. Použijte **Prohledávat...** abyste našli požadovaný soubor. Pak klikněte na **Import**. Importovaný certifikát bude na seznamu certifikátů v okně **Důvěryhodný CA certifikát**. Pak klikněte na **Import**, abyste použili uložený soubor.

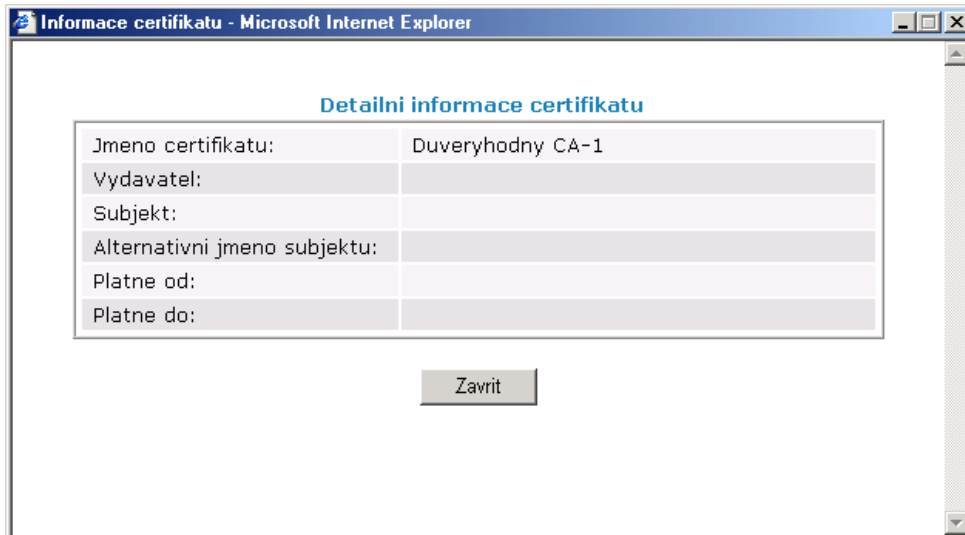
Import X509 důvěryhodného CA certifikátu

Vyber souboru důvěryhodného CA certifikátu.

Procházet...

Klik [Import](#) stáhnutí certifikace.

Klikněte na **Zobrazit** (View), pokud chcete zobrazit každý Důvěryhodný CA certifikát v podrobném informačním okně. Pokud chcete certifikát vymazat, zvolte jej a klikněte na **Vymazat** (Delete). Odstraní se všechny informace o certifikátu.



3.9 VoIP



Síť Voice over IP (hlas přes IP - VoIP) umožňuje používat širokopásmové připojení k Internetu pro hlasový přenos vysoké kvality.

Je mnoho signálových protokolů, metod kterými zařízení VoIP spolu komunikují. Nejpopulárnější protokoly jsou SIP, MGCP, Megaco a H.323. Tyto protokoly však nejsou navzájem kompatibilní (kromě soft-switch serveru).

Vigor podporuje protokol SIP. Má širokou podporu a je proto ideální pro ITSP (poskytovatel telefonních služeb - Internet Telephony Service Provider) a softphone. SIP je end-to-end (konec-konec) signálový protokol, který zřizuje uživateli přítomnost a mobilitu ve struktuře VoIP. Každý, kdo chce komunikovat používá jeho SIP Uniform Resource Identifier – tzv. SIP adresu. Standardní formát SIP URI je

sip: cislo@voi.t-com.sk: port

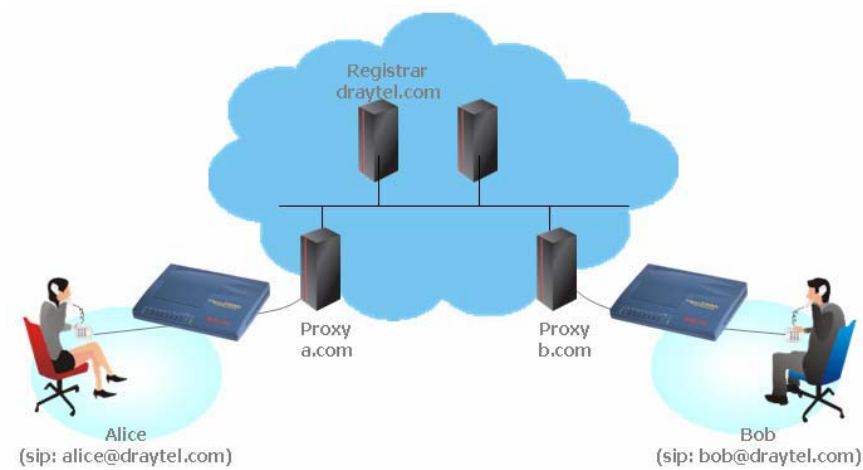
Některá pole u různých druhů využití mohou být volitelná. Všeobecně t-com.sk je doména. "Userinfo" (informace o uživateli) zahrnují pole „user“, heslo pole „password a následuje znak@. Je to podobné jako URL a je možné to nazývat "SIP URL". SIP podporuje přímé peer-to-peer volání a také volání přes SIP proxy server (role podobná jako strážce brány v sítích H.323), pokud protokol MGCP používá architekturu klient/server a způsob volání se podobá dnešním sítím PSTN.

Pokud je hovor navázán, plyne hlasový přenos pomocí RTP (Real-Time Transport Protocol – protokol přenosu v přímém čase). Do RTP paketů mohou být vsazeny různé kodeky (metody komprese a kódování). Modely Vigor (V modely) poskytují různé kodeky včetně G.711 A/μ-law, G.723, G.726 a G.729 A & B. Každý kodek používá různou šířku pásma přenosu a proto poskytuje různou kvalitu přenosu hlasu. Čím širší pásmo kodek využívá, tím lepší je kvalita hlasu. Kodek se však musí přizpůsobit k internetovému připojení.

Volání přes SIP servery

Nejprve se Vigor zaregistruje na SIP zasláním registračních zpráv, aby se ověřila jeho platnost. Pak SIP proxy servery obou stran přepošlou sekvence zpráv volajícímu, aby zřídily hovor.

Pokud se oba zaregistrují u stejného SIP serveru, nastane následující:



Největší výhodou tohoto módu je, že si nemusíte pamatovat IP adresu vašeho přítele, která se může, pokud je dynamická, často měnit. Namísto toho použijete programování volání (dial plan), nebo přímo vytočíte jméno účtu (account name) vašeho přítele pokud jste zaregistrováni u stejného SIP serveru.

Peer-to-Peer

Před voláním je nutné znát IP adresu protějščí strany. Router VoIP pak provede spojení mezi oběma stanicemi.



Vigor řady V nejprve vybere k daným podmínkám a šířce pásma nejefektivnější kodek a zajistí automatickou kvalitu služby (QoS). QoS služba upřednostňuje hlasové pakety posílané přes internet. Těmito funkcemi zajistí Vigor neoptimálnější řešení přenosu hlasu přes internet.

3.9.1 Konfigurace volání (Dial Plan)

Tato stránka umožňuje nastavit si telefonní seznam (Phone Book) a číselnou tabulku (Digit Map) pro funkce VoIP. Klikněte na stránce na Telefonní seznam nebo Číselnou tabulku pro vstup na další stránky nastavení Programování volání.

[VoIP >> Konfigurace volani](#)

Konfigurace volani

Telefonni seznam Ciselna tabulka Nastaveni PSTN

Telefonní seznam (Phone Book)

V této sekci lze zadat do telefonního seznamu telefonní kontakty. Použitím tzv. **rychlého vytáčení** lze navázat hovory rychleji než vytukáváním celého čísla. V nabídce je 60 položek – SIP adres, které si lze uložit v **Programování volání**.

[VoIP >> Konfigurace volani](#)

Telef. seznam

Index	Telefonni cislo	Zobrazovane jmeno	SIP URL	Pristup na nahradni linku	Nahradni telef. cislo	Stav
1.				None		x
2.				None		x
3.				None		x
4.				None		x
5.				None		x
6.				None		x
7.				None		x
8.				None		x
9.				None		x
10.				None		x
11.				None		x
12.				None		x
13.				None		x
14.				None		x
15.				None		x
16.				None		x
17.				None		x
18.				None		x
19.				None		x
20.				None		x

<< [1-20](#) | [20-40](#) | [40-60](#) >>

[Dalsi >>](#)

Stav: v --- Aktivni, x --- Neaktivni, ? --- Prazdny

Klikněte na jakékoliv číslo indexu pro zobrazení stránky položky Programování volání.

[VoIP >> Nastavení rychlého vytaceni](#)

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	
Telefonní číslo	<input type="text" value="20"/>
Zobrazované jméno	<input type="text" value="pepik"/>
SIP URL	<input type="text" value="12345"/> @ <input type="text" value="iptel.org"/>
Přístup na nahradní linku	<input type="text" value="None"/>
Nahradní telef. číslo	<input type="text"/>

OK

Vymazat

Zrusit

Aktivovat (Enable)

Klikněte pro aktivaci.

Telefonní číslo (Phone Number)

Číslo rychlého volání tohoto indexu. Může to být jakékoliv vámi zvolené číslo složené z čísel 0-9 a * .

Zobrazované jméno (Display Name)

Identifikace volajícího, kterou chcete aby se zobrazila na displeji při příchozím volání.

SIP URL

Zadejte telefonní číslo účastníka.

Číselná tabulka (Digit Map)

Tato stránka umožňuje uživateli upravit číslo prefixu účtu SIP přidáním čísla, odstraněním čísla nebo výměnou čísla. Používá se pro rychlé a jednoduché volání přes VoIP rozhraní.

Nahradit (Replace) V tomto módu bude OP číslo nahrazeno číslem prefixu při volání přes určité rozhraní. Jak je uvedeno na obrázku výše, OP číslo 8863 bude nahrazeno číslem 003, protože je číslo prefixu zadáno 003.



OP číslo (OP Number)

Číslo které sem zadáte je první část čísla účtu, ze kterého chcete provést určitou funkci (vzhledem na určený mód) použitím čísla prefixu.

Min délk. (Min Len)

Nastavte minimální délku volaného čísla na aplikování čísla prefixu. Jak je zobrazeno výše, pokud je číslo mezi 7 a 9, číslo může použít nastavení čísla prefixu.

Max délk. (Max len)

Nastavte maximální délku volaného čísla, které může aplikovat nastavení čísla prefixu.

Rozhraní (Interface)

Zvolte rozhraní, které chcete aktivovat na číslo prefixu. Výběr ze dvou uložených SIP účtů.

3.9.2 SIP účty (SIP Account)

V této sekci lze upravit vlastní nastavení SIP účtů. Pokud požádáte o účet, váš poskytovatel služby SIP vám dodá jméno účtu (Account Name) nebo uživatele, SIP registrar, proxy a název domény (Domain Name) (poslední tři položky mohou být identické). Pak už jen oznámíte přátelům vaše telefonní číslo ve formě **Jméno účtu@název domény**.

Pokud zapnete Vigor VoIP router, ten se zaregistruje u SIP Registrar autorizací uživatel@doména/oblast. Potom bude váš hovor veden přes SIP proxy k destinaci použitím identity jméno účtu@doména/oblast.

Obsah SIP účtu

Obnovit

Index	Profil	Doména/Oblast	Proxy	Jmeno účtu	Port	Stav
1	VOI	iptel.org		change_me	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
2				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
3				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
4				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
5				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
6				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-

R: uspesna registrace na SIP server
 -: chyba registrace na SIP serveru

Nastavení NAT Traversal

STUN server:	<input type="text"/>
Externí IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> vt.

OK

Index

Klikněte pro vstup na stránku nastavení účtu SIP.

Profil

Zobrazí jméno profilu účtu.

Doména/Oblast (Domain/Realm)

Zobrazí název domény nebo IP adresu SIP Registrar serveru.

Proxy

Zobrazí název domény nebo IP adresu SIP proxy serveru.

Jméno účtu (Account Name)

Zobrazí jméno účtu telefonního čísla před @.

Port (Ring Port)

Specifikujte, který port bude zvonit při příchozím hovoru.

Stav (Status)

Zobrazuje stav zodpovídající SIP účtu. **(R)** znamená, že účet je úspěšně zaregistrován na SIP serveru. **(-)** znamená, že účet se nezaregistroval.

STUN Server

Zadejte IP adresu STUN serveru.

Externí IP (External IP)

Zadejte IP brány.

SIP PING interval

Předvolená hodnota je 150 vteřin. Je důležitá pro Nortel NAT server traversal support.

VoIP >> SIP ucty

SIP uctet Index c. 1

Jméno profilu	<input type="text" value="VOI"/> (max 11 znaku)
Registrace přes	<input type="text" value="Zadna"/> <input type="checkbox"/> telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text" value="iptel.org"/> (max 63 znaku)
Proxy	<input type="text"/> (max 63 znaku)
	<input type="checkbox"/> Pracovat jako odchozí proxy
Zobrazene jmeno	<input type="text"/> (max 23 znaku)
Cislo uctu/Jmeno	<input type="text" value="change_me"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text"/> (max 63 znaku)
Cas platnosti	<input type="text" value="10 min."/> <input type="text" value="600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvoneni	<input type="text" value="1"/>

Jméno profilu (Profile Name)

Přiřaďte jméno profilu pro identifikaci. Lze zadat jméno podobné názvu domény. Např. pokud je název domény *draytel.org*, lze zadat *draytel-1*.

Registrace přes (Register via)

Pokud chcete volat přes VoIP bez registraci osobních údajů, zvolte **Žádná** (None) a zaškrtněte políčko. Některé SIP servery umožňují uživatelům využívat VoIP funkce bez registrace. Pro takový server zaškrtněte Volání bez registrace (make call without register). Doporučeno je zvolit **Auto**.)

<input type="text" value="Zadna"/>
<input checked="" type="checkbox"/> Zadna
<input type="checkbox"/> Auto
<input type="checkbox"/> WAN
<input type="checkbox"/> LAN/VPN

SIP Port

Zadejte číslo portu pro posílání/příjem SIP zpráv k uskutečnění hovoru. Předvolená je hodnota 5060. Váš peer musí nastavit stejnou hodnotu u jeho SIP Registrar.

Doména/Oblast (Domain/Realm)

Zadejte název domény nebo IP adresu SIP Registrar serveru.

Proxy

Nastavte jméno domény nebo IP adresu SIP proxy serveru. Lze zadat: číslo portu, pokud chcete upřesnit cílový port přenosu dat (např. nat.draytel.org:5065)

Pracovat jako odchozí proxy (Act as Outbound Proxy)

Zaškrtněte, pokud chcete, aby proxy pracoval jako Outbound proxy.

Zobrazené jméno (Display Name)

ID volajícího, které chcete zobrazit na displeji přátel.

Číslo účtu/Jméno (Account Number/Name)

Zadejte jméno účtu nebo telefonní číslo, např. celý text před @.

Autentifikace ID (Authentication ID)

Zaškrtněte, pokud chcete aktivovat funkci a zadejte jméno nebo číslo používané na SIP ověřování u SIP Registrar. Nemusíte zadávat, pokud je stejné jako jméno účtu.

Heslo (Password)

Heslo, které jste obdrželi při registraci u SIP.

Čas platnosti (Expiry Time)

Čas, po který si bude SIP Registrar udržovat váš záznam. Před vypršením času zašle router SIP Registrar další požadavek.

Podpora NAT Traversal

Pokud se router, který používáte připojí na internet jiným zařízením, musíte nastavit tuto funkci podle potřeby.



Žádná (None)-Deaktivuje funkci.

Stun-Pokud je pro váš router poskytnutý Stun server.

Manuálně-Pokud chcete nastavit externí IP adresu jako NAT transversal podporu.

Nortel-pokud soft-switch, který využíváte, podporuje řešení Nortel, zvolte tuto možnost.

Port (Ring Port)

Zaškrtněte VoIP 1 nebo VoIP 2 jako předvolený vyzváněcí port.

Typ zvonění (Ring Pattern)

Zvolte vyzváněcí tón.

- 1 ▾
- 1
- 2
- 3
- 4
- 5
- 6

Níže je znázorněn př. seznamu SIP účtů.

[VoIP >> SIP účty](#)

Obsah SIP účtu

Obnovit

Index	Profil	Domena/Oblast	Proxy	Jmeno účtu	Port	Stav
1	VOI	iptel.org		change_me	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
2				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
3				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
4				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
5				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
6				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-

R: uspesna registrace na SIP server
 -: chyba registrace na SIP serveru

Nastavení NAT Traversal

STUN server:	<input type="text"/>
Externi IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> vt.

OK

3.9.3 Nastavení telefonu (Phone Settings)

Tato stránka umožňuje uživateli upravit nastavení telefonu buď pro VoIP 1 nebo VoIP 2.
[VoIP >> Nastavení telefonu](#)

telef. seznam

Index	Port	Vlastnosti volání	Kodek	Ton	Hlasitost (Mik/Repro)	Default SIP ucet	DTMF prenos
1	VoIP1		G.729A/B	User Defined	5/5	VOI	InBand
2	VoIP2		G.729A/B	User Defined	5/5	VOI	InBand

RTP

<input type="checkbox"/> Symmetrické RTP	
Dynamický RTP port start	<input type="text" value="10050"/>
Dynamický RTP port cíl	<input type="text" value="15000"/>
RTP TOS	<input type="text" value="IP precedence 5"/> <input type="text" value="10100000"/>

OK

RTP

Symetrické RTP (Symmetric RTP)-Zaškrtněte pro aktivaci funkce. Aby přenos dat prošel na obě strany a neztratil se kvůli ztrátě IP (např. při posílání dat z veřejné IP adresy vzdáleného routeru na privátní IP adresu místního routeru), zaškrtnutím políčka vyřešíte tento problém.

Dynamický RTP port start (Dynamic RTP Port start)-Specifikuje počáteční port RTP streamu. Předvolená hodnota je 10050.

Dynamický RTP port cílový (Dynamic RTP Port end)-Specifikuje konečný port RTP streamu. Předvolená hodnota je 15000.

RTP TOS-Rozhoduje o úrovni balíku VoIP. Vyberte si ze seznamu.

IP precedence 5

- Manual
- IP precedence 1
- IP precedence 2
- IP precedence 3
- IP precedence 4
- IP precedence 5
- IP precedence 6
- IP precedence 7
- AF Class1 (Low Drop)
- AF Class1 (Medium Drop)
- AF Class1 (High Drop)
- AF Class2 (Low Drop)
- AF Class2 (Medium Drop)
- AF Class2 (High Drop)
- AF Class3 (Low Drop)
- AF Class3 (Medium Drop)
- AF Class3 (High Drop)
- AF Class4 (Low Drop)
- AF Class4 (Medium Drop)
- AF Class4 (High Drop)
- EF Class

Klikněte na číslo 1 nebo 2 ve sloupci index a vstupte na následující stránku pro konfigurování nastavení telefonu.

VoIP >> Nastavení telefonu

Telef. Index c. 1

Vlastnosti		Kodeky	
<input type="checkbox"/> Hotline	<input type="text"/>	Preferovaný kodek	G.729A/B (8kb/s)
<input type="checkbox"/> Délka spojení	3600 vt.	<input type="checkbox"/> Pouze tento kodek	
<input type="checkbox"/> T.38 Fax funkce		Velikost paketu	20ms
Automat. přesmerování	vypnuto	Detektor hlas. aktivity	Vyp.
SIP URL	<input type="text"/>	Default SIP účet	1-VOI
Čas přesmer.	30 vt.	<input type="checkbox"/> Používat oznam. ton pouze pokud byl účet zaregistrovan	
<input type="checkbox"/> DND mod(Nerisit)	Index(1-15) v Plan Nastavení:		
	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		
Pozn.: Nastavení Akce a Čas nečinnosti budou ignorována.			
<input type="checkbox"/> Čekající volání			
<input type="checkbox"/> Manual.přesmerování			

OK Zruseno Rozsirene

Hotline

Zaškrtněte políčko pro aktivaci funkce. Zadejte SIP URL, která bude automaticky volaná pokud zdvihnete telefon.

Délka spojení (Session Timer)

Zaškrtněte pro aktivaci funkce. Pokud po dobu kterou zadáte do pole, nebude žádná odpověď, automaticky se spojení ukončí.

T.38 Fax funkce (T.38 Fax function)

Pokud podporuje tuto funkci faxu i protější strana, lze ji zaškrtnutím povolit.

Automat. přesměrování (Call Forwarding)

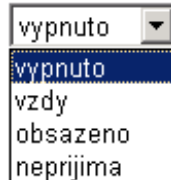
Automatické přesměrování volání. Existují 4 možnosti.

Vypnuto (Disable)-Zavře funkci přesměrování.

Vždy (Always)-Všechny hovory budou přesměrovány na SIP URL bezpodmínečně.

Obsazeno (Busy)-Přicházející hovory budou přesměrovány, pokud je místní systém obsazen.

Nepřijímá (No Answer)-Pokud přicházející hovory zůstávají bez odpovědi, budou po uplynutí nastaveného času přesměrovány na danou SIP URL.



SIP URL-Zadejte SIP URL (např. aaa@draytel.org nebo abc@t-com.sk)

Čas přesměrování (Time out)-Nastavte časovač pro přesměrování volání, předvolených je 30 vteřin.

DND mód (Nerušit) (DND (Do Not Disturb) mod)

Nastavte čas kdy nechcete být vyrušováni VoIP hovory. V této době obdrží volající obsazovací tón a místní uživatel neobdrží vyzvánění.

Plán (Schedule)-Zadejte index plánovacího profilu, abyste řídili DND podle předvoleného plánu, viz. sekce 3.5.2.

Čekající volání (Call Waiting)

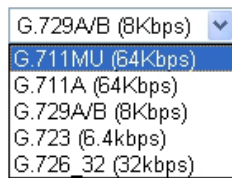
Zaškrtněte pro aktivaci funkce. Zazní tón upozornění, že nový hovor očekává odpověď. Klikněte na háček abyste zdvihli.

Manuál. přesměrování (Call Transfer)

Zaškrtněte pro aktivaci funkce manuální přesměrování hovoru. Klikněte pro aktivaci dalšího hovoru. Pokud se spojení podaří, zavěste. Druhé dvě strany mohou komunikovat.

Preferovaný kodek (Prefer Codec)

Zvolte jeden z 5 kodeků jako předvolený pro vaše VoIP hovory. Kodeky by si měli obě strany vyjednat mezi sebou před každou relací, proto někdy může být použit i jiný typ kodeku než předvolený. Předvolený kodek G.729A/B potřebuje malou šířku pásma a udržuje dobrou kvalitu hlasu. Při rychlosti odesílání dat (upstream) 64 kb/s však tento kodek nepoužívejte. Nejvhodnější je pro upstream 256 kb/s.

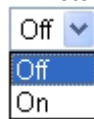


Pouze tento kodek (Single Codec)-Pokud je políčko zaškrtnuto, bude aplikován pouze zvolený kodek.

Velikost paketu (Packet Size)-Množství dat, které jeden paket obsahuje, předvolená hodnota je 20 ms, co znamená, že paket bude obsahovat 20 ms hlasu.



Detektor hlasové aktivity (Voice Active Detector)-Tato funkce detekuje, zda je hlas na obou stranách aktivní nebo ne. Pokud není, router ušetří šířku pásma. Klikněte na **On** pro aktivaci a **Off** na deaktivaci.



Default SIP účet (Default SIP Account)

Jsou dvě skupiny účtů SIP, které lze nastavit. Vyberte z menu jméno profilu a účet, který chcete předvolit.

Používat oznamovací tón jen pokud byl účet zaregistrován (Play dial tone only when account registered)

Zaškrtněte pro aktivaci funkce.

Rozšířená nastavení telefonu

Tato možnost se zobrazí po kliknutí na tlačítko **Rozšířené** v menu VoIP – Nastavení telefonu – Index.1.

Zde je možné nastavit tón ve sluchátku telefonu připojeného do FXS portu pomocí nabídky **Region**, kde jsou pro jednotlivé státy předvoleny frekvence tónů. Pokud nejsou v nabídce, lze je nastavit i manuálně.

Příklad pro ČR.

[VoIP >> Nastavení telefonu](#)

Rozšířené nastavení >> Telef. index c. 1

Nastavení tónu						
Region	[Definice uživatele ▼]		Typ zobrazení ID			
			[FSK_ETSI ▼]			
	Spodní kmitocet (Hz)	Horní kmitocet (Hz)	T on 1 (msek)	T off 1 (msek)	T on 2 (msek)	T off 2 (msek)
Oznamovací ton	425	0	330	330	660	660
Vyzvanecí ton	425	0	1000	4000	0	0
Obsazovací ton	425	0	330	330	0	0
Ton nepruchodnosti	425	0	165	165	0	0

Nastavení hlasitosti		DTMF	
Hlasitost mikr.(1-10)	[5]	DTMF mod	[OutBand (RFC2833) ▼]
Hlasitost repro.(1-10)	[5]	Payload Type(rfc2833)	[101]
MISC			
Hlasitost oznam. tonu	[27]		
Vyzvanecí kmitocet	[25]		

OK

Zrusit

Region

Vyběr regionu, s předvolenými hodnotami.

Typ zobrazení ID

Možnost výběru normy pro zobrazování ID (Caller ID)

Hlasitost mikr.

Nastavení hlasitosti mikrofonu ve sluchátku připojeného telefonu.

Hlasitost repro.

Nastavení hlasitosti reproduktoru ve sluchátku připojeného telefonu.

DTMF mód

InBand nebo OutBand

3.9.4 Stav (Status)

V části VoIP Stav je uveden stav kodeku, připojení a další informace o stavu hovoru pro oba VoIP porty.

[VoIP >> Stav](#)

Stav		cas obnoveni : <input type="text" value="10"/> <input type="button" value="Obnovit"/>									
Port	Stav	Kodek	PeerID	Gas spojeni	Tx Pkt	Rx Pkt	Rx ztrac	Rx Jitter (ms)	Prichozi volani	Odchozi volani	Hlasitost repro
VoIP1	IDLE			0	0	0	0	0	0	0	5
VoIP2	IDLE			0	0	0	0	0	0	0	5

Log

Date (mm-dd-yyyy)	Time (hh:mm:ss)	Duration (sec)	In/Out	Peer ID
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-
00-00-	0	00:00:00	0	-

Čas obnovení (Refresh Seconds)

Specifikujte interval obnovení informací o volání VoIP. Informace jsou aktualizovány hned, když kliknete na tlačítko Obnovit.

Port

Zobrazuje stav připojení portů VoIP1 a VoIP2.

Stav (Status)

Zobrazuje stav připojení VoIP.

Nečinný (IDLE)-Funkce je nečinná.

Zavěšeno (HANG_UP)-Připojení se neuskutečnilo (tón obsazeno)

Spojuje (CONNECTING)-Uživatel volá.

Očekává odpověď (WAIT_ANS)Hovor byl iniciován a čeká na odpověď vzdáleného uživatele.

Upozorňuje (ALERTING)-Přicházející hovor.

Aktivní (ACTIVE)-Spojení VoIP je aktivní.

Kodek (Codec)

Zobrazuje použitý kodek.

PeerID

Současné ID peeru volajícího ven nebo dovnitř (formát může být IP nebo doména).

Čas spojení (Connect Time)

Formát ve vteřinách.

Tx Pkt (Tx Pkts)

Celkový počet přenesených hlasových paketů při hovoru.

Rx Pkt (Rx Pkts)

Celkový počet přijatých hlasových paketů při hovoru.

Rx ztrac. (Rx Losses)

Celkový počet ztracených hlasových paketů při hovoru.

Rx Jitter

Kolísání při příjmu hlasových paketů.

Příchozí volání (In Calls)

Akumulovaný čas přicházejících hovorů.

Odchozí volání (Out Calls)

Akumulovaný čas odcházejících hovorů.

Hlasitost repro (Speaker Gain)

Hlasitost hovoru.

Log

Zobrazuje záznamy o hovorech VoIP.

3.10 ISDN

ISDN (Integrated Services Digital Network) je komunikační standard pro posílání hlasu, videa a dat přes digitální linku.

Poz.: Pouze pro modely Vigor (i)

3.10.1 Základní nastavení

ISDN >> General Setup

ISDN Setup

ISDN Port <input checked="" type="radio"/> Enable <input type="radio"/> Disable	Blocked MSN numbers for the router
Country Code: <input type="text" value="International"/>	1. <input type="text"/>
Own Number: <input type="text"/>	2. <input type="text"/>
<small>'Own Number' means that the router will tell the remote end the ISDN number when it's placing an outgoing call.</small>	3. <input type="text"/>
MSN numbers for the router	4. <input type="text"/>
1. <input type="text"/>	5. <input type="text"/>
2. <input type="text"/>	
3. <input type="text"/>	
<small>'MSN Numbers' means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.</small>	

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 (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.

Blocked MSN Nummbers for the router (Blokování MSN čísel na routeru)

Volání na router z čísel uvedených v těchto polích jsou blokována.

3.10.2 Přístup na jednoho poskytovatele

ISDN >> Dialing to a Single ISP

Single ISP

ISP Access Setup	PPP/MP Setup
ISP Name: <input type="text" value="dlin"/>	Link Type: <input type="text" value="Dialup BOD"/>
Dial Number: <input type="text" value="30"/>	PPP Authentication: <input type="text" value="PAP or CHAP"/>
Username: <input type="text" value="dlin"/>	Idle Timeout: <input type="text" value="180"/> second(s)
Password: <input type="password" value="••••"/>	IP Address Assignment Method (IPCP)
<input type="checkbox"/> Require ISP callback (CBCP)	Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)
Index(1-15) in Schedule Setup:	Fixed IP Address: <input type="text"/>
=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	

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, zaškrtněte toto pole.

Scheduler (1-15) - Časový plán

Zadejte čísla jednotlivých časových programů pro přístup k internetu, tak jak jste si vaše časové plány nastavili.

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 64kb/s: Pro připojení k internetu bude použit jeden ISDN kanál (B). **Dialup 128kb/s:** 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 router využívat pouze jeden B kanál. Po naplnění kapacity B kanálu router 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 vteřin. Pokud tento parametr nastavíte na 0, zůstane ISDN připojení trvale aktivní.

Fixed IP (pevná IP)

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**.

Fixed IP Address (pevná IP adresa)

Vyplňte přidělenou veřejnou IP adresu.

3.10.3 Přístup na dva ISP

Zařízení umožňuje najednou připojení ke dvěma ISP. Tuto funkci lze např. využít pokud ISP nepodporuje sdružování kanálů (Multiple-Link PPP).

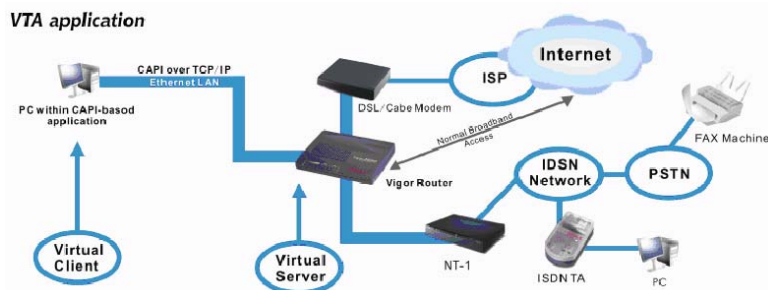
Dual ISP	
<p>Common Settings</p> <p>1. <input checked="" type="checkbox"/> Enable Dual ISPs Function</p> <p>2. <input type="checkbox"/> Require ISP callback (CBCP)</p>	<p>PPP/MP Setup</p> <p>Link Type: <input type="text" value="Dialup BOD"/></p> <p>PPP Authentication: <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout: <input type="text" value="180"/> second(s)</p>
<p>Primary ISP Setup</p> <p>ISP Name: <input type="text" value="dlin"/></p> <p>Dial Number: <input type="text" value="30"/></p> <p>Username: <input type="text" value="dlin"/></p> <p>Password: <input type="text" value="••••"/></p> <p>IP Address Assignment Method (IPCP)</p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address: <input type="text"/></p>	<p>Secondary ISP Setup</p> <p>ISP Name: <input type="text" value="prima"/></p> <p>Dial Number: <input type="text" value="66"/></p> <p>Username: <input type="text" value="prima"/></p> <p>Password: <input type="text" value="•••••"/></p> <p>IP Address Assignment Method (IPCP)</p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address: <input type="text"/></p>
<input type="button" value="OK"/>	

Konfigurace většiny parametrů je stejná jako v předchozím případě. Výše uvedený obrázek ukazuje příklad konfigurace.

3.10.4 Virtuální TA

Virtual TA je funkce, která umožňuje počítačům nebo ethernetovým síťovým zařízením využívat CAPI software (například RVS-COM nebo BVRP) pro přístup k routeru, pro zaslání 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 instalovaném ve směrovačích Vigor, vezměte na vědomí níže uvedená omezení.

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



Jak je uvedeno ve výše, může klient Virtual TA přijímat telefonní hovory, nebo realizovat odchozí volání, odesílat nebo přijímat faxové zprávy přes připojené faxové zařízení nebo ISDN TA, apod.

Dříve než budete konfigurovat Virtual TA, musíte jej nejprve nainstalovat. Vložte CD-ROM, které jste dostali s vaším routerem 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. Postupujte podle pokynů instalátoru na obrazovce. Po dokončení instalace budete vyzváni k restartu počítače. Kliknutím na tlačítko **OK** restartujte počítač.

Po restartu počítače se v navigační liště zobrazí ikona VT (obvykle v pravém dolní rohu obrazovky vedle hodin - viz. obrázek níže).



Pokud svítí text v ikoně ZELENE, 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.



Klikněte na Virtual TA (Remote CAPI) Setup ve skupině Quick Setup.

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 Setup

Virtual TA Server : Enable Disable

Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Virtual TA Server

Zapnout (Enable): Zaškrtněte pro aktivaci serveru.

Zakázat: Zaškrtněte pro deaktivaci serveru. Všechny aplikace Virtual TA budou zastaveny.

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

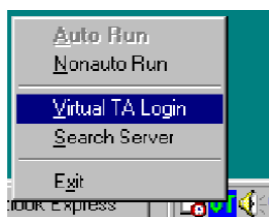
Pokud vytvoříte uživatelský účet, bude přístup k serverové straně Virtual TA omezen pouze na majitele příslušného uživatelského účtu.

V následujících odstavcích předpokládáme, že nemáte sjednanou MSN službu s vaším poskytovatelem služby ISDN.

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.

Virtual TA Users Profiles						
	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	••••				<input checked="" type="checkbox"/>

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



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

Virtual TA Login

User Name :

Password :

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.

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

Virtual TA Users Profiles						
	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	••••	123			<input checked="" type="checkbox"/>

Nastavte příslušné MSN 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.

3.10.5 Call Control (Řízení volání)

Pro správnou funkci některých aplikací je nutné, aby váš router (týká se pouze routeru s podporou ISDN) mohl být na dálku "požádán" o navázání spojení s vaším poskytovatelem přes rozhraní ISDN.

Před následující konfigurací nastavte nejprve funkci **Dialing to a Single ISP**.

ISDN >> Call Control

Call Control Setup

Dial Retry	<input type="text" value="0"/> times	Remote Activation	<input type="text"/>
Dial Delay Interval	<input type="text" value="0"/> second(s)		

PPP/MP Dial-Out Setup

Basic Setup		Bandwidth On Demand (BOD) Setup	
Link Type	<input type="text" value="Dialup BOD"/>	High Water Mark	<input type="text" value="7000"/> cps
PPP Authentication	<input type="text" value="PAP or CHAP"/>	High Water Time	<input type="text" value="30"/> second(s)
TCP Header Compression	<input type="text" value="None"/>	Low Water Mark	<input type="text" value="6000"/> cps
Idle Timeout	<input type="text" value="180"/> second(s)	Low Water Time	<input type="text" value="30"/> second(s)

OK

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 routeru.

Dial Delay Interval

Zadejte interval mezi opakováním vytáčení. Standardně je tato hodnota nastavena na 0 vteřin.

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.

Link Type (způsob připojení)

Protože ISDN má dva B kanály (64kb/s na kanál) lze specifikovat který B kanál se má použít samostatně, nebo oba, případně BOD (Bandwidth on Demand). Lze použít čtyři módy: 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).

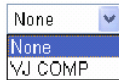


PPP Authentication (ověření PPP)

Uvedte způsob ověření pro připojení PPP/MP. Doporučujeme nastavení PAP/CHAP pro pokrytí většiny možností.

Kompresa 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.

High Water Mark a High Water Time

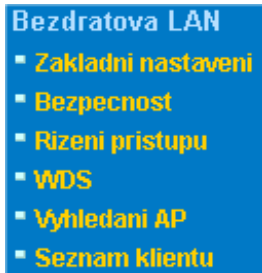
BOD znamená šířka pásma na přání pro Multiple-Link PPP (ML-PPP nebo MP). Parametry **High Water Mark/ High Water Time/ Low Water Mark/ Low Water Time** jsou aplikovány pouze pokud je nastavena **Link Type** na **Dialup BOD**. Pokud nastavíte typ připojení na Dial BOD, bude ISDN linka obvykle při připojení 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 128 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.

3.11 Bezdrátová LAN (Wireless LAN)



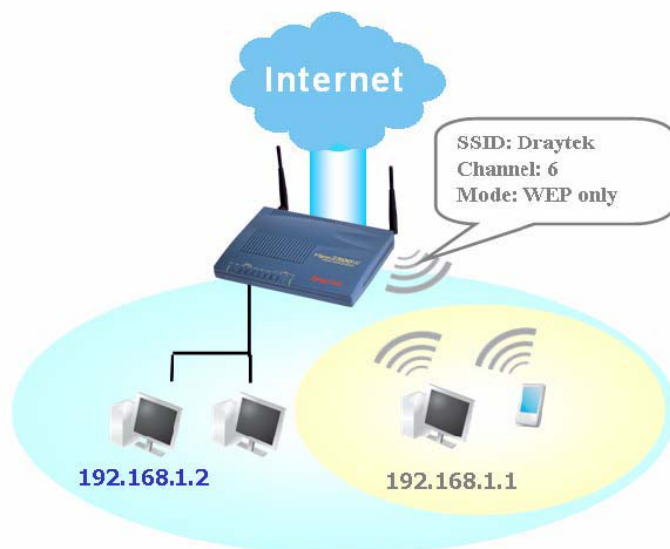
V posledních letech roste trh s bezdrátovými komunikacemi. Bezdrátová technologie je schopná virtuálně pokrýt každý kout světa. Stamilióny lidí si denně vyměňují informace pomocí bezdrátových přístupů. Model s označením „G“, nazývaný Vigor wireless router je vyvinut pro co nejvyšší flexibilitu a efektivnost v malé kanceláři/ domácnosti. Každý autorizovaný zaměstnanec může přes zabudovanou WLAN připojit svůj notebook, PDA do konference bez instalace kousku kabelu a stavebních úprav. Bezdrátová LAN umožňuje vysokou mobilitu a jejich uživatelé mohou využívat všechny možnosti LAN jako u drátové včetně připojení na internet.

Vigor wireless routery jsou vybaveny bezdrátovým rozhraním LAN s protokolem IEEE 802.11g. Pro větší výkon jsou některé typy Vigorů vybaveny pokročilou technologií Super G, s rychlostí až 108 Mb/*.

Díky tomu si lze vychutnat streamové video nebo hudbu.
Poznámka: * Aktuální propustnost závisí na podmínkách sítě a okolí, včetně velikosti přenosu a režie sítě.

3.11.1 Základní koncept

V módu wireless má Vigor funkci přístupového bodu (Access Point – AP) spojujícího množství bezdrátových klientů nebo stanic (STA). Všechny stanice se tak dělí o stejné internetové připojení jako ostatní hostitelé přes pevnou, drátovou LAN. Základní nastavení umožňují nastavit informace o této bezdrátové síti včetně SSID, identifikace, kanál a podobně.



Přehled bezpečnosti

Hardwarové kryptování v reálném čase : Vigor je vybaven AES hardwarovým kryptováním, takže může poskytovat přenášeným datům nejvyšší ochranu bez ovlivňování výkonu u přenosu dalších aplikací.

Volba celkového standardu bezpečnosti: Pro zajištění bezpečnosti vaší bezdrátové komunikace, nabízíme několik hlavních standardů na trhu.

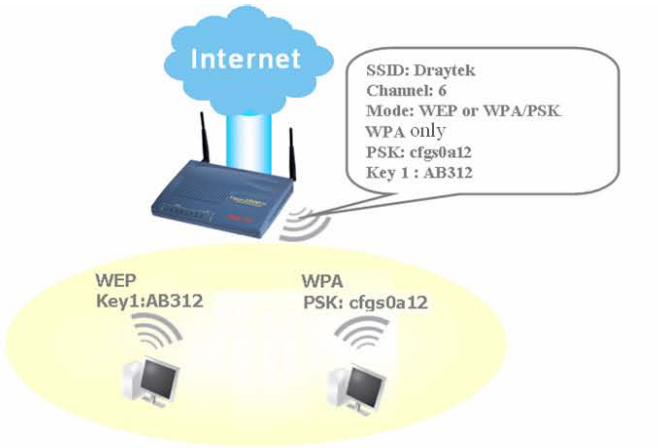
WEP (Wired Equivalent Privacy) je metoda kryptující každý rámec vysílaný přes rádio používající 64-bit nebo 128-bitový klíč. Obvykle přístupový bod nastaví 4 klíče a komunikuje s každou stanicí jedním z nich.

WPA (Wi-Fi Protected Access), je dominantní průmyslový bezpečnostní mechanismus rozdělený do dvou kategorií: osobní WPA - WPA sdílený klíč (WPA/PSK) a WPA-Enterprise tzv. WPA/802.1x.

V osobním WPA je použit při přenosu dat pro kryptování předdefinovaný klíč. WPA aplikuje Temporal Key Integrity Protocol (TKIP) protokol pro kryptování dat a WPA2 aplikuje AES. WPA-Enterprise kombinuje kryptování i ověřování.

Pokud se ukáže, že WEP je napadnutelný, lze zvážit použití WPA na nejbezpečnější připojení. Měli byste zvolit vhodné bezpečnostní mechanismy podle potřeby. Nezávisle nad tím jaké metody bezpečnostních mechanismů zvolíte, všechny zlepšují ochranu dat přenášených vzduchem a ochranu vaší bezdrátové sítě. Vigor wireless router je velmi flexibilní a podporuje hromadné bezpečné připojení s WEP i WPA najednou.

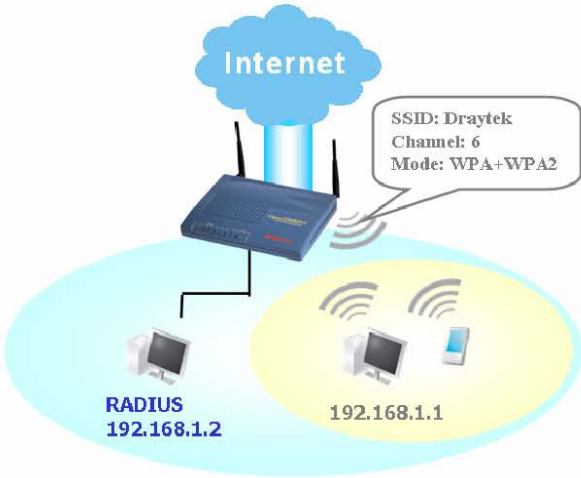
Example 1



Example 2



Example 3



Oddělení drátové a bezdrátové LAN – Izolace WLAN umožňuje izolovat bezdrátovou LAN od drátové LAN, buď za účelem karantény nebo omezeného přístupu. Znamená to, že obě části nemají mezi sebou vzájemný přístup. Např. lze ve firmě nastavit bezdrátovou LAN jen pro návštěvníky, aby se mohli připojit na internet bez toho, aby vás obtěžovali stahováním důvěrných informací. Pro flexibilnější nastavení lze přidat filtr MAC adresy, aby byl izolován od drátové LAN pouze přístup jednoho uživatele.

Rízení bezdrátových stanic - seznam stanic - zobrazí všechny stanice bezdrátové sítě a stav jejich připojení.

3.11.2 Základní nastavení (General Settings)

Kliknutím na **Základní nastavení** se otevře web stránka, pro konfiguraci SSID a bezdrátového kanálu.

[Bezdrátova LAN >> Základní nastavení](#)

Základní nastavení (IEEE 802.11)

<input type="checkbox"/> Aktivovat bezdrát. LAN
Mod : <input type="text" value="Mix(11b+11g)"/>
Index(1-15) in Plan Nastavení: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
SSID : <input type="text"/>
Kanal : <input type="text"/>
<input type="checkbox"/> Skryté SSID
<input type="checkbox"/> Dlouhá inicializace
Skryté SSID : prevence proti skenování SSID. Dlouhá inicializace : nutné pouze pro starší 802.11b zařízení (snižuje výkon).

OK

Zrusit

Aktivovat bezdrát. LAN (Enable Wireless LAN)

Zaškrtněte pro aktivaci funkce.

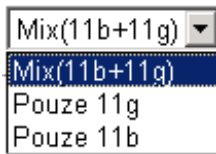
Mód (Mode)

Zvolte vhodný přenosový mód.

Smišený (11b+11g)-router komunikuje standardem 802.11b a 802.11g simultánně.

Pouze 11g-router komunikuje pouze standardem 802.11g.

Pouze 11b-router komunikuje pouze standardem 802.11b.



Index(1-15) v Plán nastavení

Nastavte bezdrátovou LAN, aby pracovala jen v určité době. Lze vybrat 4 programy z 15 předdefinovaných v **Aplikace>Plánovač** (Applications > Schedule).

SSID a kanál (SSID and Channel)

Předvolené SSID je „default“.

SSID-je identifikace bezdrátové LAN. Může být definována jakýmikoliv znaky.

Kanál-je frekvence bezdrátové sítě. Předvolený kanál je 6. Pokud je kanál vystaven rušení, lze jej změnit.

Skryté SSID (Hide SSID)

Zvolte jako ochranu před neoprávněným skenováním sítě. Ochrana zabraňuje připojení neoprávněných klientů tím, že síť není viditelná.

Dlouhá inicializace (Long Preamble)

Tato možnost definuje délku synchronizačního pole v paketu 802.11. Nejmodernější bezdrátové sítě používají short preamble s 56 bitovým polem namísto long preamble se 128 bitovým. Některá 11b bezdrátová zařízení, pokud s nimi chcete komunikovat podporují pouze long preamble.

3.11.3 Bezpečnost (Security)

Tato stránka umožňuje nastavit bezpečnostní nastavení v různých módech. Po konfiguraci nastavení klikněte na OK abyste je uložili a spustili.

Bezpecnostni nastaveni

Mod:	Vypnuto
WPA:	
Sdílený klic(PSK):	*****
Zadejte 8~63 ASCII znaku nebo 64 Hexadecimalnich cislic zacinajicich "0x", napr. "cfgs01a2..." nebo "0x655abcd...".	
WEP:	
Delka klíce	64-Bit
<input type="radio"/> klic 1 :	*****
<input type="radio"/> Klic 2 :	*****
<input type="radio"/> Klic 3 :	*****
<input type="radio"/> Klic 4 :	*****
Pro 64 bit WEP klic	
Zadejte 5 ASCII znaku nebo 10 Hexadecimalnich cislic zacinajicich "0x", napr. "AB312" nebo "0x4142333132".	
Pro 128 bit WEP klic	
Zadejte 13 ASCII znaku nebo 26 Hexadecimalnich zacinajicich "0x", napr. "0123456789abc" nebo "0x30313233343536373839414243".	

OK Zrusit

Mód

Vypnuto (Disable)-Vypne kryptovací mechanismus. Pro bezpečnost routeru zadejte kryptovací mód.

WEP-Akceptuje pouze WEP klienty a klíč má být zadán ve WEP klíči.

WPA/PSK-Akceptuje pouze WPA klienty a klíč má být zadán v PSK.

WPA2/PSK-Akceptuje pouze WPA2 klienty a klíč má být zadán v PSK.

Mix (WPA+ WPA2)/PSK-Akceptuje WPA a WPA2 klienty simultánně a kryptovací klíč by měl být v PSK.

Vypnuto
Vypnuto
WEP
WPA/PSK
WPA2/PSK
Mix(WPA+WPA2)/PSK

WPA

WPA kryptuje každý frame vysílaný rádiem použitím klíče, nebo PSK (sdílený) zadáný manuálně nebo automaticky a vyjednaný přes ověřování 802.1x, nebo přes znaky 8~63

ASCII jako např. 012345678 (nebo 64 hexadecimálních čísel začínajících 0x jako např. "0x321253abcde...").

WEP

Pro 64 bitový WEP klíč-Zadejte 5 ASCII znaků jako např. 12345(nebo 10 hexadecimálních čísel začínajících 0x jako např. "0x321253abcde...").

Pro 128 bitový WEP klíč-Zadejte 13 ASCII znaků jako např. ABCDEFGHIJKLM (nebo 26 hexadecimálních čísel začínajících 0x jako např. "0x3B2D1A2D5B3ABCD3457BDA34D...").

Všechna bezdrátová zařízení musí podporovat stejnou bitovou délku WEP kryptování a mít stejný klíč. Lze zadat 4 klíče, ale zvolen může být pouze jeden. Mohou být zadány v ASCII nebo hexadecimálně. Klikněte na klíč který chcete použít.

3.11.4 Řízení přístupu (Access Control)

Pro zvýšenou bezpečnost bezdrátového přístupu **Řízení přístupu** umožňuje zakázat přístup k síti kontrolou LAN MAC adresy klienta. Jen platná MAC adresa, která byla nakonfigurována, může mít přístup přes bezdrátové LAN rozhraní. Kliknutím na **Řízení přístupu** se zobrazí následující stránka, na které lze přidat MAC adresy, které chcete povolit.

[Bezdrátova LAN >> Řízení přístupu](#)

Řízení přístupu

Aktivovat řízení přístupu
Zasady : Aktivace filtru MAC adresy

MAC adresa filtru

Index	Charakteristika	MAC adresa

MAC adresa klienta : : : : : :

s: Izolovat stanici z LAN

Přidat Odstranit Uprava Zrusit

OK Vymazat

Aktivovat řízení přístupu (Enable Access Control)

Zvolte pro aktivaci funkce Řízení přístupu.

MAC adresa (MAC Address)
Zadejte MAC adresu manuálně.

Přidat (Add)
Přidejte novou MAC adresu do seznamu.

Odstranit (Remove)
Odstraňte MAC adresu ze seznamu.

Edit
Upravte MAC adresu uloženou v seznamu.

Zrušit (Cancel)
Zrušte nastavování řízení přístupu.

OK
Uložení nastavení.

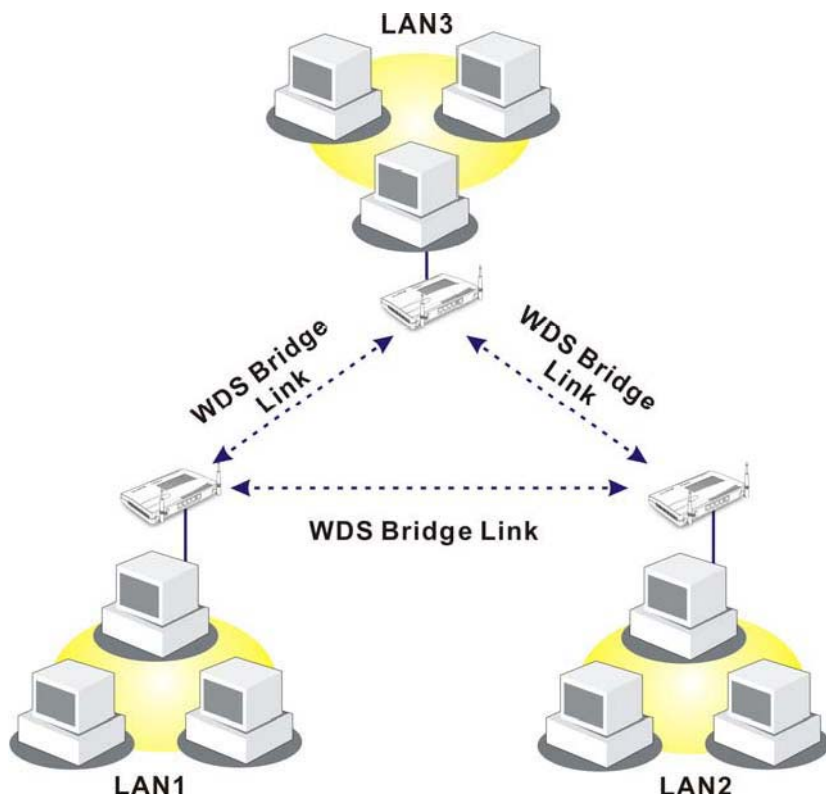
Vymazat (Clear All)
Vymaže všechny zadané hodnoty.

3.11.5 WDS

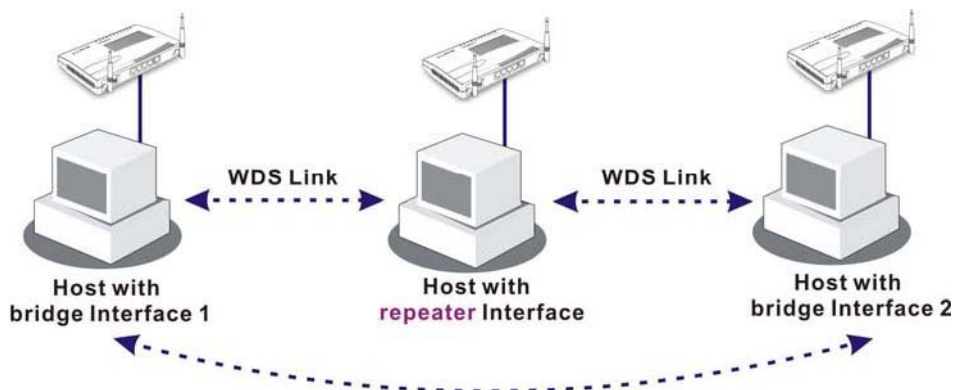
WDS znamená bezdrátový distribuční systém (Wireless Distribution System). Je to protokol sloužící na bezdrátové spojení dvou přístupových bodů (Access Point - AP). Většinou se používá na aplikace:

- Přemostění dvou LAN vzduchem.
- Zvětšení rozsahu pokrytí WLAN.

Pro splnění výše uvedeného požadavku jsou v routeru implementovány dva WDS módy – Bridge (most) a Repeater (opakovač). Funkce je znázorněna níže na obrázku:

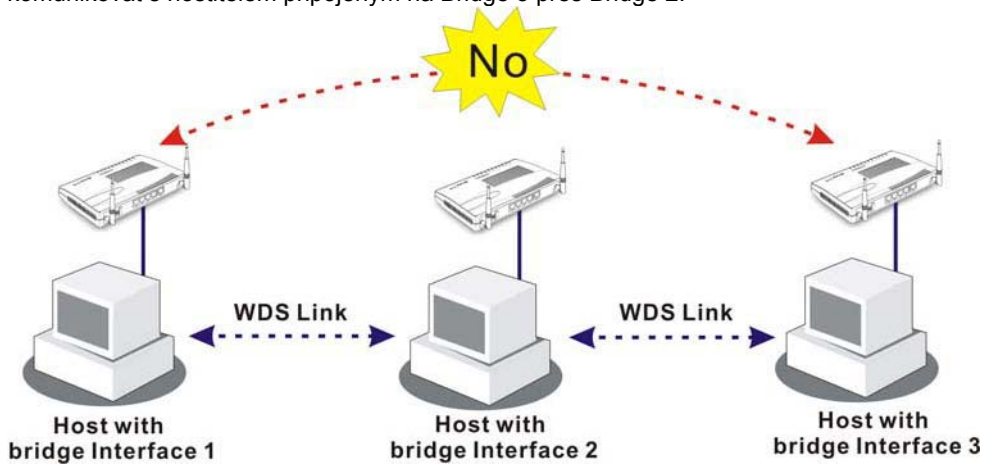


Aplikace pro WDS-Repeater mód:



Hlavní rozdíl mezi módy je, že v módu Repeater pakety přijaté z jednoho AP peeru mohou být zopakovány dalšímu AP peeru přes linku WDS, pokud v módu Bridge pakety přijaté z linky WDS budou přeposlány místnímu hostiteli, je jedno zda drátovému nebo bezdrátovému. Jinými slovy, v módu Repeater je možné přeposílat pakety z WDS do WDS.

V následujících příkladech hostitelé připojení na Bridge 1 nebo 3 komunikují s hostitelem připojeným na Bridge 2 přes linku WDS. Hostitel připojený na Bridge 1 však nemůže komunikovat s hostitelem připojeným na Bridge 3 přes Bridge 2.



Klikněte na **WDS** z menu **Bezdrátová LAN**. Zobrazí se následující stránka.

[Bezdrátová LAN >> Nastavení WDS](#)

Nastavení WDS

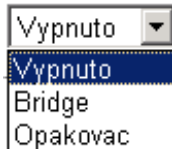
<p>Mod: <input type="text" value="Vypnuto"/></p> <hr/> <p>Bezpecnost: <input checked="" type="radio"/> Vypnuto <input type="radio"/> WEP <input type="radio"/> Sdílený klic</p> <hr/> <p>WEP: Použijte stejné nastavení WEP klíče v Bezpečnostní nastavení.</p> <hr/> <p>Sdílený klic: Typ : TKIP Klic : <input type="text" value="*****"/></p> <p>zadejte 8~63 ASCII znaku nebo 64 hexadecimalních číslic začínajících "0x", napr.: "cfigs01a2..." nebo "0x655abcd....".</p>	<p>Bridge Zapnuto Peer MAC adresa</p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <p>Pozn.: Vypnete nepoužívání linky pro získání vyššího výkonu.</p> <hr/> <p>Repeater Zapnuto Peer MAC adresa</p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <p><input type="checkbox"/> <input type="text" value=": : : : : :"/></p> <hr/> <p>Funkce Access Point: <input checked="" type="radio"/> Zapnuto <input type="radio"/> Vypnuto</p>
---	---

OK Vymazat Zrusit

Mód

Zvolte si mód nastavení WDS.

Vypnuto (Disable)-nevyvolá žádné nastavení.
Bridge-mód je navržen tak, aby provedl první typ aplikace.
Repeater-druhý typ aplikace.



Bezpečnost (Security)

Lze nastavit tři typy bezpečnosti.

Vypnuto (Disable), **WEP** a **Sdílený klíč** (Pre-shared Key). Zvolené nastavení umožní zaškrtnutí jednoho z polí.

WEP

Zvolte, pokud chcete použít stejný klíč, jaký jste nastavili na stránce bezpečnostních nastavení. Pokud jste žádný nenastavili, toto políčko nebude zvýrazněné.

Nastavení (Settings)

Encryption Mode-Pokud jste zaškrtnuli políčko **Použijte stejné nastavení WEP klíče** ... nemusíte volit 64 nebo 128 bitový kryptovací mód. Pokud jste ho nezaškrtnuli, lze ho nastavit na této stránce. **Index klíče** (Key Index)-zvolte jaký klíč chcete použít po zvolení kryptovacího módu. **Klíč** (Key)-Zadejte obsah klíče.

Sdílený klíč (Pre-shared key)

Zadejte 8 ~ 63 ASCII znaků nebo 64 hexadecimálních číslic začínajících na "0x".

Bridge

Pokud si za mód připojení zvolíte Bridge, zadejte prosím MAC adresu peeru. Je povolených najednou 6 MAC adres. Abyste dosáhli lepší výkon, deaktivujte nepoužité linky. Pokud chcete vyvolat MAC adresu peeru, zaškrtněte **Zapnuto** (Enable).

Repeater

Pokud si za mód připojení zvolíte Opakovač (Repeater), zadejte prosím MAC adresu peeru. Jsou povoleny dvě najednou. Podobně jako v předcházejícím případě zaškrtněte **Zapnuto** (Enable).

Funkce Acces Point (přístupový bod)

Klikněte na **Zapnuto** (Enable) aby router pracoval jako přístupový bod, **Vypnuto** (Disable) abyste funkci vypnuli.

Stav (Status)

Umožňuje uživateli poslat peerům odkaz „hello“. Je platný jen pokud peer také podporuje tuto funkci.

3.11.6 Vyhledání AP (AP Discovery)

Router může skenovat všechny kanály a vyhledávat pracující přístupové body (AP) v okolí. Na základě výsledků skenování mají uživatelé k dispozici informaci, který volný kanál mohou použít bez rušení. Také se tím ulehčí nalezení AP pro linku WDS. Při skenovacím procesu (asi 5 vteřin) se k Vigoru nepřipojí žádný klient.

Tato stránka se používá pro skenování existence AP u bezdrátové LAN. Nalezeny však mohou být pouze ty AP, které jsou na stejném kanálu jako router. Klikněte na **Vyhledat** (Scan), pro vyhledání všech přístupových bodů.

[Bezdrátová LAN >> Vyhledání AP](#)

Seznam Access Pointu

BSSID	Kanal	SSID
<input type="button" value="Vyhledat"/>		

Viz. [Statistiky](#).

Pozn.: Během skenovacího procesu (~5 vt.), se žádná stanice nemůže spojit s routerem.

Přidat do [WDS nastavení](#) :

AP MAC adresy : : : : :

Vyhledat (Scan)

Používá se pro vyhledání všech připojených AP. Výsledek se zobrazí v okně.

Přidat (Add)

Pokud chcete, aby nalezený bod byl AP aplikován na vaše WDS nastavení, zadejte MAC adresu AP na konci stránky a klikněte na **Přidat** (Add). Později bude AP přidán na stránku nastavení WDS.

3.11.6 Seznam klientů (Station List)

Seznam klientů poskytuje informace o aktuálním připojení bezdrátových klientů se stavovým kódem. Pro lepší pochopení je zde jejich sumarizace. Pro výhodnou kontrolu přístupů lze zvolit WLAN klienta a kliknout na **Přidat k Řízení přístupu** (Access Control).

[Bezdrátova LAN >> Seznam klientu](#)

Seznam klientu

Stav	MAC adresa
<input type="button" value="Obnovit"/>	

Stavové kody :
C: Připojeno, bez kryptování.
E: Připojeno, WEP.
P: Připojeno, WPA.
A: Připojeno, WPA2.
B: Blokováno řízením přístupu.
N: Připojeno.
F: Neúspěšná 802.1X nebo WPA/PSK autentifikace.

Pozn.: Po úspěšném připojení k routeru, může být stanice odpojena bez upozornění. V takovém případě stále zůstává v seznamu, pokud nevyprší platnost připojení.

Přidat k Řízení přístupu :

MAC adresa klienta : : : : :

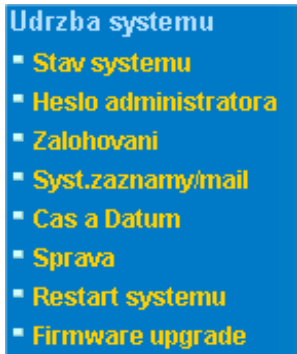
Obnovit (Refresh)

Klikněte na tlačítko pokud chcete obnovit seznam.

Přidat (Add)

Klikněte na tlačítko pokud chcete přidat zadanou MAC adresu do seznamu.

3.12 Údržba systému (System Maintenance)



Pro údržbu systému je několik položek, které je potřeba vědět jak nastavit: Stav (Status), heslo administrátora (Administrator Password), záloha konfigurace (Configuration Backup), Syslog, čas a datum (Time and Date), Reboot System a Firmware Upgrade.

3.12.1 Stav systému

Stav systému poskytuje základní informace o nastavení sítě routeru včetně rozhraní LAN a WAN. Zde lze zjistit také aktuální verzi firmwaru.

Vigor2700 Series
ADSL2/2+ Firewall Router

DrayTek
www.draytek.com

Quick Start Wizard
Online stav

Přístup k internetu
LAN
NAT
Firewall
Řízení pásma
Aplikace
VPN a vzdálený přístup
Sprava certifikátu
VoIP
Bezdrátová LAN
Údržba systému
Diagnostika

Stav systému

Název modelu	: Vigor2700 series	
Verze Firmware	: 2.6.3_1311302	
Vytvoreno dat./cas	: Sep 7 2006 13:26:22	
Verze ADSL firmware	: 1311302_B Annex B	

LAN		WAN	
MAC adresa	: 00-50-7F-D8-A5-D8	Stav linky	: Odpojeno
1. IP adresa	: 192.168.1.1	MAC adresa	: 00-50-7F-D8-A5-D9
1. Maska podsítě	: 255.255.255.0	Spojění	: ---
DHCP Server	: Ano	IP adresa	: ---

VoIP		Bezdrát. LAN	
Port	: 1 2	MAC adresa	: 00-50-7f-db-a5-d8
SIP registrátor	:	Frekvencní doména	: Europe
Učet ID	: 12 12	Verze Firmware	: 1.0.4.0
Registr	:		
Kódek	:		
Příchozí volání	: 0 0		
Odchozí volání	: 0 0		

Název modelu (Model Name)
Zobrazuje název modelu routeru.

Verze Firmware (Firmware Version)
Zobrazuje aktuální verzi firmware.

Vytvořeno dat./ čas (Build Date&Time)
Zobrazuje datum a čas výroby firmware.

LAN:

MAC adresa (MAC Address)
Zobrazuje MAC adresu LAN rozhraní.

1. IP adresa (1st IP Address)
Zobrazuje IP adresu LAN rozhraní.

1. Maska podsítě (1st Subnet Mask)
Zobrazuje adresu masky 1.podsítě LAN rozhraní.

DHCP Server
Zobrazuje aktuální stav DHCP serveru v LAN rozhraní.

WAN:

MAC adresa (MAC Address)
Zobrazuje MAC adresu WAN rozhraní.

IP adresa (IP Address)
Zobrazuje IP adresu WAN rozhraní

Default brána (Default Gateway)
Zobrazuje přidělené IP adresy přednastavené brány.

DNS
Zobrazuje přidělenou IP adresu primárního DNS.

VOIP:

Port
Zobrazuje číslo FXS portu.

SIP registrar
Registrace SIP serveru, zobrazuje název SIP serveru pro IP telefonování (Yes – Ano, No - Ne)

Účet
Zobrazuje název účtu pro VoIP, který poskytuje ISP.

Registr
Zobrazuje stav FXS portů, zda jsou registrovány nebo ne.

Kodek

Zobrazuje typ předvoleného kodeku pro daný FXS port.

Příchozí volání

Zobrazuje počet příchozích volání.

Odchozí volání

Zobrazuje počet odchozích volání.

Bezdrát. LAN:**MAC adresa (MAC Address)**

Zobrazuje MAC adresu rozhraní bezdrátové sítě.

Frekvenční doména (Frequency Domain)

Zobrazuje dostupný kanál podporovaný bezdrátovým zařízením. Závisí na zemi. Evropa (13 kanálů), USA (11 kanálů).

Verze Firmware (Firmware Version)

Zobrazuje informace o ovladačích karty WLAN.

3.12.2 Heslo administrátora (Administrator Password)

Tato stránka umožňuje nastavit nové heslo.

[Udržba systému >> Nastavení hesla administrátora](#)

Heslo administrátora

Původní heslo	<input type="text"/>
Nové heslo	<input type="text"/>
Zopakovat zadání nového hesla	<input type="text"/>

OK

Původní heslo (Old Password)

Zadejte původní heslo. U výrobního nastavení je heslo prázdné.

Nové heslo (New Password)

Do tohoto pole zadejte nové heslo.

Zopakovat zadání nového hesla (Retype New Password)

Zadejte znovu nové heslo. Pokud kliknete OK, zobrazí se okno se zadáním nových přihlašovacích údajů. Použijte nové heslo pro přístup do WEB konfiguratoru routeru.

3.12.3 Zálohování (Configuration Backup)

Podle následujících kroků lze provést zálohu nastavení routeru.

Přejděte do **Údržba systému >> Zálohování** (System Maintenance >> Configuration Backup). Otevře se následující okno.

Údržba systému >> Zálohování konfigurace

Záloha konfigurace/ Obnova

Obnova konfigurace

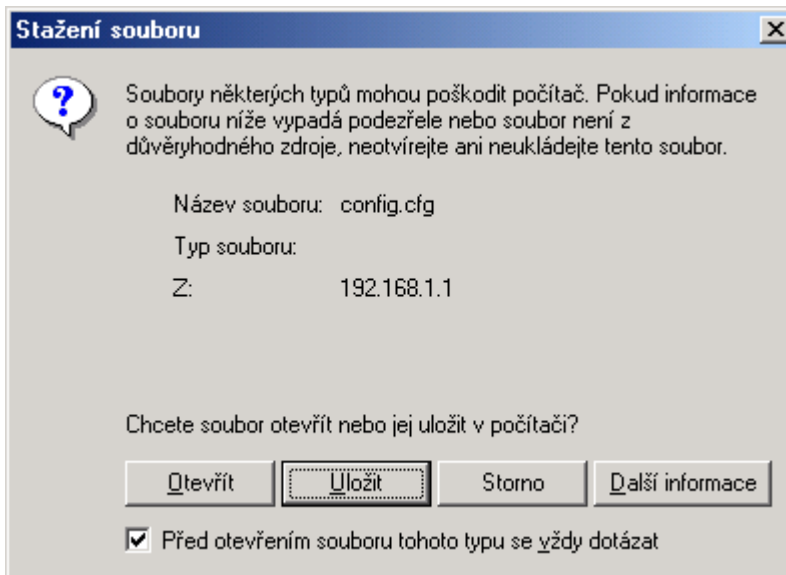
Vyber konfiguračního souboru.

Klikni pro obnovu ze zálohy.

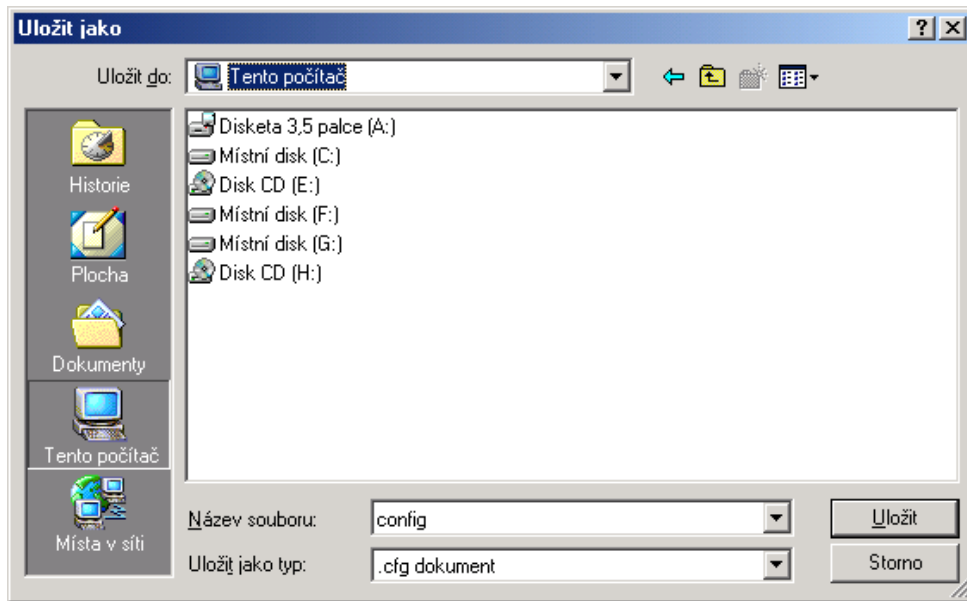
Zálohování

Klikni pro zálohu aktuální konfigurace systému.

Klikněte na **Zálohování** (Backup) zobrazí se následující okno. Klikněte na **Uložit** (Save) a otevře se další okno pro uložení konfigurace.



V ukládacím (Save As) dialogu je přednastavený název zálohy **config.cfg**. Lze ho změnit. Pokud kliknete na **Uložit** (Save), bude uložena pod jménem **config.cfg**.



V příkladu je použita platforma **Windows**. **Mac** nebo **Linux** bude mít odlišné zobrazení oken, ale funkce zálohování je stále stejná.

Obnova (Restore Configuration)

Klikněte na **Údržba systému >> Zálohování** (System Maintenance >> Configuration Backup). Otevře se následující okno.

[Údržba systému >> Zálohování konfigurace](#)

[Zaloha konfigurace/ Obnova](#)

<p>Obnova konfigurace</p> <p>Vyber konfiguračního souboru.</p> <input type="text"/> <input type="button" value="Procházet..."/> <p>Klikni pro obnovu ze zálohy.</p> <input type="button" value="Obnovení"/>
<p>Zalohování</p> <p>Klikni pro zálohu aktuální konfigurace systému.</p> <input type="button" value="Zalohování"/> <input type="button" value="Zrusit"/>

Klikněte na tlačítko **Procházet** (Browse) pro výběr konfiguračního souboru, kterým chcete obnovit nastavení v routeru.
Klikněte na tlačítko **Obnovení** (Restore) a počkejte než Vám další okno oznámí, že proces zálohování byl úspěšný.

3.12.4 Záznamy syst. (Syslog)/ e-mail (Mail Alert)

Funkce SysLog je poskytována uživatelům pro monitorování routeru. Není třeba vstupovat do WEB konfigurace a zjišťovat v nastaveních stavy jednotlivých činností routeru.

[Udržba systému >> Zaznamy systemu\(Syslog\) / Upozorneni e-mailem](#)

Zaznamy systemu(Syslog) / Upozorneni e-mailem

Zaznamy systemu (SysLog)	Upozorneni e-mailem
<input type="checkbox"/> Zapnout	<input type="checkbox"/> Zapnout
IP adresa serveru <input type="text"/>	SMTP server <input type="text"/>
Cilovy port <input type="text" value="514"/>	Poslat mail na <input type="text"/>
Zapnout syslog zpravy:	Navratova cesta <input type="text"/>
<input checked="" type="checkbox"/> Firewall zaznamy	<input type="checkbox"/> Autentifikace
<input checked="" type="checkbox"/> VPN zaznamy	Uzivatske jmeno <input type="text"/>
<input checked="" type="checkbox"/> Zaznamy uzivate. pristupu	Heslo <input type="text"/>
<input checked="" type="checkbox"/> Zaznamy volani	
<input checked="" type="checkbox"/> WAN Log	
<input checked="" type="checkbox"/> Router/DSL informace	

Záznamy systému (Syslog):

Zapnout (Enable)

Klikněte pro aktivaci této funkce.

IP adresa serveru (Syslog Server IP)

IP adresa serveru (nebo počítače v LAN), kde je spuštěna aplikace Syslog (součást balíčku Router Tools).

Cílový port (Destination Port)

Přidělený port pro komunikaci s aplikací Syslog.

Upozornění e-mailem (Mail Alert):

Zapnout (Enable)

Klikněte pro aktivaci této funkce.

SMTP Server

IP adresa SMTP serveru.

Poslat mail na (Mail to)

Přidělení mailové adresy pro odesílání směrem ven.

Návratová cesta (Return-Path)

Přidělení cesty pro přijímání mailu.

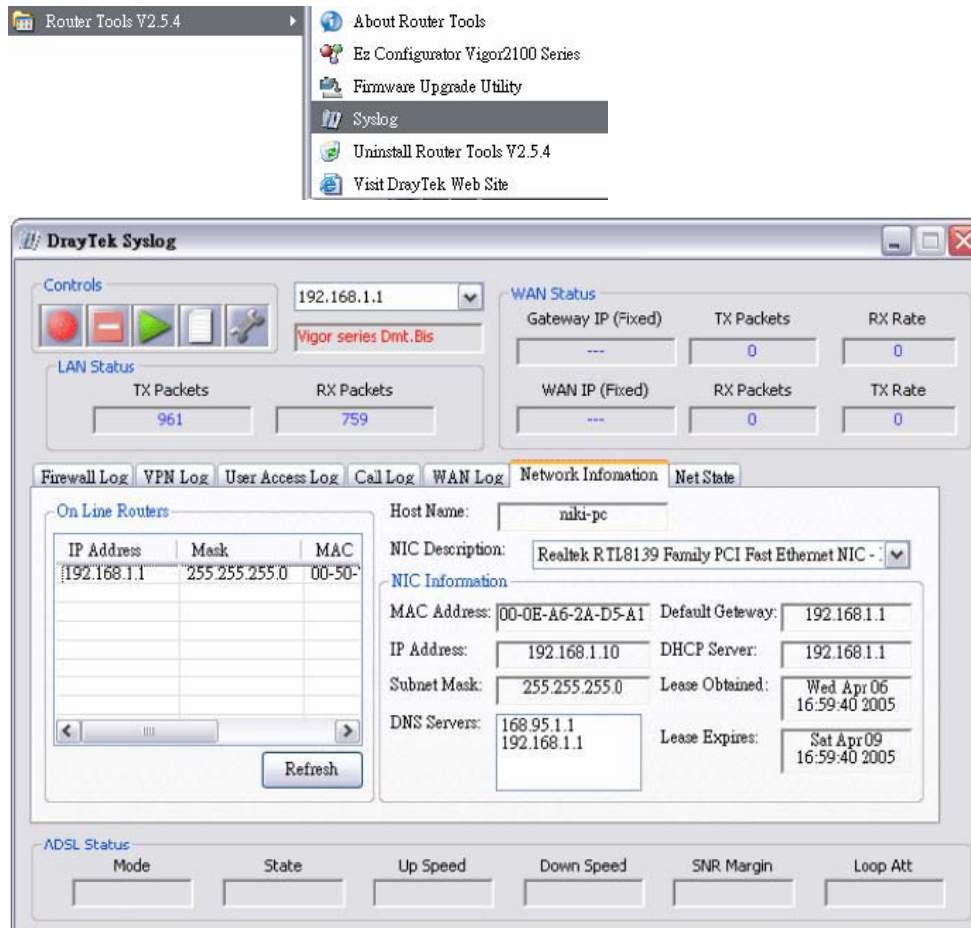
Klikněte na OK pro uložení nastavení.

Pro zobrazení aplikace Syslog, proveďte prosím následující:

Nastavte IP adresu vašeho PC, kde bude spuštěna aplikace Syslog do pole Server IP Address a aktivujte tuto funkci zaškrtnutím položky Enable.

Nainstalujte utility Router Tools z příloženého CD. Po instalaci, klikněte v menu programů na **Router Tools>>Syslog**.

Na obrazovce Syslog, vyberte router který chcete monitorovat. Nezapomeňte v **Network Information** označit síťový adaptér pro spojení s routerem, který chcete monitorovat. Jinak nelze získávat informace z routeru.



3.12.5 Čas a datum (Time and Date)

Umožňuje specifikovat odkud a jak se mají získávat informace o času, pro systémový čas routeru.

[Udržba systému >> Cas a datum](#)

Informace o case

Aktuální systémový čas	2000 Jan 1 Sat 1 : 15 : 28	Zjistit čas
------------------------	----------------------------	-------------

Nastavení času

<input checked="" type="radio"/> Použit čas z prohlizece	
<input type="radio"/> Použit klienta internetoveho casu	
Časový protokol	NTP (RFC-1305)
IP adresa serveru	
Časová zóna	(GMT) Greenwich Mean Time : Dublin
Aktivace letního času	<input type="checkbox"/>
Interval zjišťování	30 vt.

OK

Zrusit

Aktuální systémový čas (Current System Time)

Klikněte na tlačítko **Zjistit čas** pro zobrazení aktuálního času.

Použit čas z prohlížeče (Use Browser Time)

Označte tuto možnost, pokud chcete aby router získal čas z hostitelského PC a nastavil ho jako systémový čas routeru.

Použit klienta internetového času (Use Internet Time)

Označte tuto možnost, pokud chcete aby se čas získával z časových serverů z internetu.

Časový protokol (Time Protocol)

Vyberte časový protokol.

IP adresa serveru (Server IP Address)

Zadejte IP adresu, nebo DNS název časového serveru.

Časová zóna (Time Zone)

Zadejte časovou zónu ve které se router nachází.

Aktivace letního času

Označením aktivujete přechod na letní čas při změně letního na zimní a opačně.

Interval zjišťování (Automatically Update Interval)

Zadejte časový interval ve kterém se bude aktualizovat čas z NTP serveru.

Klikněte na **OK** pro uložení nastavení.

3.12.6 Správa (Management)

Tato stránka umožňuje správu přístupu, seznam povolených přístupů, nastavení portů a nastavení SNMP. Např. kontrola přístupu, číslo portu je použito na odesílání/příjem SIP message pro sestavení session. Přednastavená hodnota je 5060 a toto musí korespondovat s registrací při uskutečňování VoIP volání.

[Udržba systému >> Správa](#)

Nastavení spravy

Kontrola přístupu <input type="checkbox"/> Aktivovat vzdálený upgrade firmware(FTP) <input type="checkbox"/> Povolit správu přes internet <input checked="" type="checkbox"/> Zakázat ping z internetu	Nastavení administrace portu <input type="radio"/> Default porty (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21) <input checked="" type="radio"/> Uživatelem definované porty Telnet Port <input type="text" value="23"/> HTTP Port <input type="text" value="80"/> HTTPS Port <input type="text" value="443"/> FTP Port <input type="text" value="21"/>
Seznam povolených přístupů Seznam IP Maska podsítě 1 <input type="text"/> <input type="text"/> 2 <input type="text"/> <input type="text"/> 3 <input type="text"/> <input type="text"/>	SNMP nastavení <input type="checkbox"/> Aktivovat SNMP Agent Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/> Notifikace Host IP <input type="text"/> Trap Timeout <input type="text" value="10"/> vterin

OK

Aktivovat vzdálený upgrade firmware (Enable remote firmware upgrade (FTP))

Označte toto pole pro povolení možnosti vzdáleně změnit firmware v zařízení přes FTP (používá se firmware s příponou .all)

Povolit správu přes internet (Allow management from the Internet)

Označte toto pole pro možnost přihlášení administrátora přes internet. Standardně není povoleno.

Zakázat ping z internetu (Disable PING from the Internet)

Označte toto pole pro odmítnutí všech PING paketů z internetu. Pro zvýšení bezpečnosti je tato funkce standardně aktivována.

Seznam povolených přístupů (Access List)

Je možné specifikovat aby se systémový správce mohl připojit k routeru ze specifické IP adresy, nebo sítě definované v seznamu. Maximálně 3 IP/sítové masky. Pokud není

v seznamu definována žádná IP adresa a maska, je přístup povolen z jakékoliv IP adresy, pokud je tato funkce aktivována.

Seznam IP (List IP)-Indikuje IP adresu, která má povolený přístup k routeru.

Maska podsítě (Subnet Mask)-Reprezentuje masku podsítě povolenou pro přihlášení k routeru.

Nastavení administrace portů:

Default porty (Default Ports)

Označit pro použití standardních portů pro Telnet a http servery.

Uživatелеm definované porty (User Defined Ports)

Označit pro specifikaci čísel portů uživatelem.

SNMP nastavení:

Aktivovat SNMP Agent (Enable SNMP Agent)

Označit pro aktivaci této funkce.

Get Community

Nastavit jméno pro získání community zadáním správného popisu. Default nastavení je **public**.

Set Community

Nastavit community zadáním správného jména. Default nastavení je **private**.

Manager Host IP

Nastavit jednoho hostitele pro správu a provoz funkce SNMP. Zadáte IP adresu hostitele.

Trap Community

Nastavte trap community zadáním správného jména. Default nastavení je **public**.

Notifikace Host IP (Notification Host IP)

Nastavit IP adresu hostitele, který bude přijímat trap community.

Trap Timeout

Default nastavení je 10 vteřin.

3.12.7 Restart systému (Reboot System)

Pro restart routeru lze použít WEB prohlížeč. Klikněte na **Restart systému** (Reboot Systém) v **Údržbě systému** (Systém Maintenance) pro otevření následující stránky.
[Udržba systému >> Restart systému](#)

Restart systému

Opravdu restartovat router ?

Použít aktuální nastavení
 Použít výrobní nastavení

OK

Při restartu routeru s aktuální konfigurací označte pole **Použít aktuální nastavení** (Using current configuration) a klikněte na **OK**. Pro reset do výrobního nastavení označte pole **Použít výrobní nastavení** (Using factory default configuration) a klikněte na OK. Router bude asi do 5 vteřin restartován.

3.12.8 Firmware upgrade

Před provedením upgrade firmware je potřeba nainstalovat do PC program Router Tools. **Firmware Upgrade Utility** je součástí dodávky. Stáhněte si aktuální firmware ze stránek výrobce nebo distributora (www.attel.cz). Klikněte na **Údržba systému >> Firmware Upgrade** (Systém maintenance >> Firmware Upgrade) pro spuštění Firmware Upgrade Utility.

[Udržba systému >> Firmware Upgrade](#)

Firmware Upgrade

Aktuální verze Firmware : 2.6.2_131812


Upgrade firmware:

- 1. Kliknete na "OK" k aktivaci TFTP serveru.
- 2. Otevřete Firmware Upgrade Utility nebo jiný TFTP klientský software.
- 3. Ověřte zda je název firmware správný.
- 4. K odstartování upgrade kliknete v aplikaci Firmware Upgrade Utility na "Upgrade".
- 5. Po úspěšném upgrade firmware, se TFTP server automaticky ukončí.

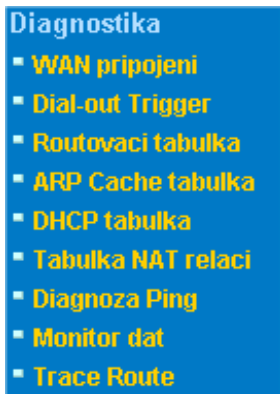
Chcete upgradovat firmware ?

OK

Klikněte na OK a zobrazí se následující stránka.

 TFTP server je aktivní. Prosim spusťte program Firmware Upgrade Utility pro upgrade routeru. Tento server se automaticky ukončí po skončení upgrade firmwaru.

3.13. Diagnostika (Diagnostics)



Diagnostika umožňuje **zobrazovat** a **diagnostikovat** stav routeru.

3.13.1 WAN připojení (WAN Connection)

Klikněte na **Diagnostika** (Diagnostics) a na **WAN připojení** pro otevření následující stránky.

[Diagnostika >> WAN připojení](#)

PPPoE/PPPoA diagnostika

| [Obnovit](#) |

Mod/Stav širokopásmového přístupu	---
Internetový přístup	>> Vytocit PPPoE/PPPoA
WAN IP adresa	---
Rozpojit spojení	>> Rozpojit PPPoE/PPPoA

Obnovit (Refresh)

Pro získání posledních aktuálních informací. Klikněte pro opětovné načtení stránky.

Mód/Stav širokopásmového přístupu (Broadband Access Mode/Status)

Zobrazí stav a mód širokopásmového přístupu. Pokud je širokopásmové připojení aktivní, zobrazí, že Internetový přístup je aktivní. Pokud ne zobrazí se "---".

WAN IP adresa (WAN IP Address)

WAN IP adresa pro aktivní spojení.

Vytočit (Rozpojit) PPPoE/ PPPoA

Kliknout pro vytvoření, nebo zrušení spojení PPPoE, nebo PPPoA

3.13.2 Dial-out Trigger

Klikněte na **Diagnostika** (Diagnostics) a **Dial-out Trigger** (Dial-out spouštěcí mechanismus) pro otevření následující stránky. Internetové spojení (PPPoE, PPPoA) je spouštěno a uskutečněno aktivací paketem z konkrétní IP adresy v síti, pokud není nastavena funkce „Vždy připojený“.

[Diagnostika >> Dial-out spousteći mechanismus \(Dial-out Trigger\)](#)

Paket který zpusobil vytoceni pripojeni na internet

| [Obnovit](#) |

```
HEX format:
00 00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00

Dekodovany format:

0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

HEX format

Zobrazuje zdrojový paket v HEX kódu.

Dekódovaný formát (Decoded Format)

Zobrazuje zdrojovou IP (lokální), cílovou IP (vzdálenou) adresu protokolu délky paketu.

Obnovit (Refresh)

Klikněte pro opětovné načtení (obnovu) stránky.

3.13.3 Routovací tabulka (Routing Table)

Klikněte na **Diagnostika** (Diagnostics) a na **Routovací tabulka** (Routing Table) pro otevření následující stránky.

Aktualní routovací tabulka

| [Obnovit](#) |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/  255.255.255.0 is directly connected, IFO
```

Obnovit (Refresh)

Klikněte pro opětovné načtení (obnovu) stránky.

3.13.4 ARP Cache tabulka

Klikněte na **Diagnostika** a **ARP Cache tabulka** pro zobrazení obsahu ARP cache (Address Resolution Protocol) uloženém v routeru. Tabulka zobrazuje mapování mezi ethernet hardware adresou (MAC Address) a IP adresou.

Diagnostika >> ARP Cache tabulka

Ethernet ARP Cache tabulka

| [Vycistit](#) | [Obnovit](#) |

IP Address	MAC Address
192.168.1.10	00-0C-76-37-60-3B

Obnovit (Refresh)

Klikněte pro opětovné načtení (obnovu) stránky.

Vyčistit (Clear)

Klikněte pro vymazání celé tabulky.

3.13.5 DHCP tabulka

Umožní zobrazit informace o přidělených IP adresách DHCP serverem. Tyto informace jsou důležité při diagnostice síťových problémů (např. konflikt IP adres).

Klikněte na **Diagnostika** (Diagnostics) a **DHCP tabulka** (DHCP Table) pro otevření následující stránky.

[Diagnostika >> DHCP tabulka](#)

Tabulka IP adres přidelených DHCP | [Obnovit](#) |

DHCP server: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID
1	192.168.1.1	00-50-7F-DB-A5-D8	ROUTER IP	
2	192.168.1.10	00-0C-76-37-60-3B	0:00:07.320	computer

Index

Zobrazuje číslo připojení.

IP Address

Zobrazuje IP adresu přidělenou routerem pro konkrétní PC.

MAC Address

Zobrazuje MAC adresu pro konkrétní PC pro které byla DHCP přidělena IP adresa.

Leased Time

Zobrazuje pronajatý čas platnosti přidělené IP adresy pro PC.

HOST ID

Zobrazuje hostitelské ID jméno konkrétního PC.

Obnovit (Refresh)

Klikněte pro opětovné načtení (obnovu) stránky.

3.13.6 Tabulka NAT relací (NAT Active Sessions Table)

Klikněte na **Diagnostika** (Diagnostics) a **Tabulka NAT relací** (Nat Active Sessions Table) pro otevření následující stránky.

[Diagnostika >> Tabulka NAT relací](#)

Tabulka aktivních NAT relací | [Obnovit](#) |

Private IP :Port	#Pseudo Port	Peer IP :Port	Ifno	Status
------------------	--------------	---------------	------	--------

Private IP:Port

Zobrazuje zdrojovou IP adresu a port pro lokální PC.

#Pseudo Port

Zobrazuje dočasný port routeru použitý pro NAT.

Peer IP:Port

Zobrazuje cílovou IP adresu a port vzdáleného hostitele.

Ifno

Zobrazuje předdefinované číslo pro rozdílné rozhraní.

0: LAN

1~2: ISDN (nepoužito v tomto modelu)

3: WAN

4 a více: VPN

Status

Stavové hodnoty jsou definovány následovně:

0: jiný TCP stav

1: TCP fin incoming

2: TCP fin out

3: TCP fin closing

4: TCP syn

5: TCP syn,ack

6: TCP ack

Obnovit (Refresh)

Klikněte pro opětovné načtení (obnovu) stránky.

3.13.7 Ping Diagnostika

Funkce umožňuje zadat do pole **IP adresa**, IP adresu na které se provádí funkce PING a která se používá k ověření, zda je daná IP adresa dostupná či ne. Po zadání IP adresy stisknete **Spustit** a po pár vteřinách se zobrazí výsledek.

[Diagnostika >> Diagnoza Ping](#)

Diagnoza Ping

Ping na: Host / IP IP adresa:

Spustit

Vysledek | [Vycistit](#) |

Vyčistit

Umožní vymazat obsah okna s výsledkem PING.

IP adresa

IP adresa zařízení využívající připojení do internetu.

TX rychl. (kb/s)

Průtok odeslaných paketů.

RX rychl. (kb/s)

Průtok přijatých paketů.

Relace

Počet relací (sessions), které daná IP adresa využívá.

Akce

Lze zvolit možnost Blokovat pro zastavení průtoku pro specifickou IP adresu na dobu 5 minut

3.13.9 Trace Route

Funkce Trace Route (sledování trasy paketu) umožňuje po zadání Hosta nebo IP adresy spustit funkci „tracert“ s tím, že po stlačení tlačítka **Spustit** vypíše výsledek do okna **Výsledek**. Funkce **Vyčistit** vymaže všechna data z okna.

[Diagnostika >> Trace Route](#)

Trace Route

Host / IP adresa:

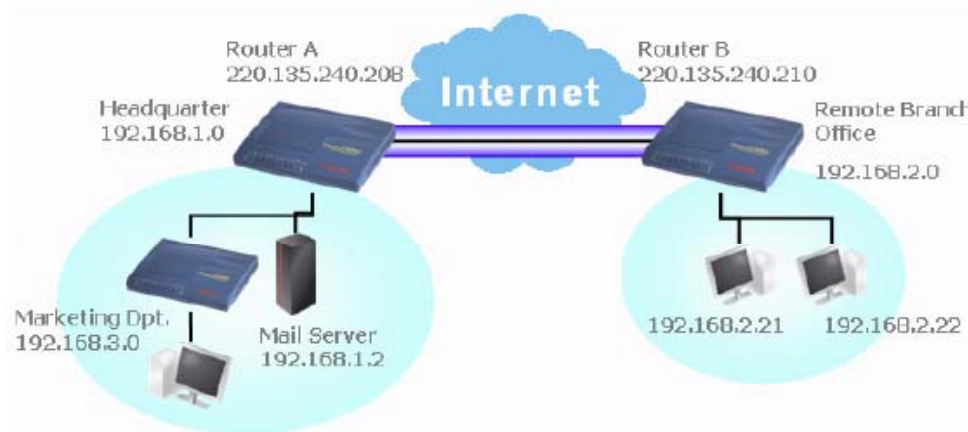
Výsledek [Vyčistit](#)

4. Aplikace a příklady

4.1 LAN – LAN mezi pobočkou a centrálou

Většina VPN aplikací se týká propojení centrály s pobočkou firmy. Následující příklady vás seznámí s nastavením profilů.

Upozorňujeme, že obě LAN sítě nesmí mít stejnou adresu.



Nastavení routeru v centrále:

- Otevřete v základním menu položku VPN a vzdálený přístup (VPN and Remote Access) a vyberte Řízení vzdáleného přístupu (Remote Access Control). Vyberte typ služby VPN který chcete používat a klikněte na OK.
- Pro aplikace spojené s PPP jako jsou PPTP, L2TP budete provádět základní nastavení v okně PPP základní nastavení (PPP General Setup).

PPP hlavni nastaveni

PPP/MP Protokol	Pridelovani IP adres pro Dial-In uzivatele
Dial-In PPP autentifikace <input type="text" value="PAP nebo CHAP"/>	Start IP adresa <input type="text" value="192.168.1.200"/>
Dial-In PPP kryptovani(MPPE) <input type="text" value="Volitelne MPPE"/>	
Oboustranna autentifikace (PAP) <input type="radio"/> Ano <input checked="" type="radio"/> Ne	
Uzivatelске jmeno <input type="text"/>	
Heslo <input type="text"/>	

OK

Pro aplikace spojené s IPsec jako jsou IPsec, nebo L2TP s IPsec policy budete provádět základní nastavení v okně **IPsec hlavní nastavení** (IPsec General Setup). Pozor sdílený klíč se musí stejný pro obě strany.

VPN a vzdaleny pristup >> IPsec zakladni nastaveni

VPN IKE/IPsec zakladni nastaveni

Dial-in nastaveni pro vzdaleneho dial-in uzivatele a dynamickeho IP klienta (LAN to LAN).

IKE overovaci metoda
Predsílenny klic <input type="text"/>
Znovu zadat predsil. klic <input type="text"/>
IPsec bezpecnostni metoda
<input checked="" type="checkbox"/> Stredni (AH) Data budou overovana, ale nebudou kryptovana.
vysoky (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data budou kryptovana a overovana.

OK

Zrusit

- Přejděte na položku **LAN – LAN** (LAN-to-LAN) a klikněte na číslo indexu pro editaci nového profilu.
- Konfigurace **Obecná nastavení** (Common Settings) je následující. Pokud zaškrtnete **Oba** (Both) ve **Směr volání** (Call Direction), mají obě strany nezávisle na sobě možnost vytvářet VPN tunel (tzn., že spojení vytváří strana A, nebo strana B).

Profil Index : 1

Obecná nastavení

Jmeno profilu <input type="text" value="draytek"/>	Smer volani <input checked="" type="radio"/> Oba <input type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Aktivovat tento profil	<input type="checkbox"/> Vzdy zapnuto
	Odpojit po <input type="text" value="300"/> vterin
	<input type="checkbox"/> Aktivovat PING aby tunel zustal aktivni
	PING na IP <input type="text"/>

- Vyplňte **Nastavení Dial-Out** (Dial-Out-Settings) jak je uvedeno v následujícím obrázku pro volání a vytvoření VPN tunelu na protější router B.

Jestli-že je vybrána a použita služba **IPSec**, je třeba specifikovat pro spojení Dial-Out vzdálenou peer IP adresu, Autentifikační metodu IKE (IKE Authentication Method) a IPSec bezpečnostní metodu (IPSec Security Method).

Nastavení Dial-Out

Typ volaného serveru	
<input type="radio"/> ISDN	
<input type="radio"/> PPTP	
<input checked="" type="radio"/> IPSec tunel	
<input type="radio"/> L2TP se zásadami IPSec <input type="text" value="Žadny"/>	
Jmeno server IP/Host pro VPN. (jako draytek.com nebo 123.45.67.89)	
<input type="text"/>	
Typ linky	<input type="text" value="64kb/s"/>
Uzivatelске jmeno	<input type="text" value="???"/>
Heslo	<input type="text"/>
PPP overovani	<input type="text" value="PAP/CHAP"/>
VJ komprimace	<input checked="" type="radio"/> On <input type="radio"/> vypnuto
Autentifikacni metoda IKE	
<input checked="" type="radio"/> Sdilený klic	
<input type="button" value="Sdilený klic IKE"/>	<input type="text" value="*****"/>
<input type="radio"/> Digitalni podpis(X.509)	
<input type="text" value="???"/> <input type="text"/>	
IPSec bezpecnostni metoda	
<input checked="" type="radio"/> Stredni(AH)	
<input type="radio"/> Vysoka (ESP) <input type="text" value="DES bez overovani"/>	
<input type="button" value="Rozsirene"/>	
Index(1-15) v Plan Setup:	
<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	
Funkce zpetneho volani (CBCP)	
<input type="checkbox"/> Vyzaduje vzdalene zpetne volani	
<input type="checkbox"/> Poskytnout ISDN cislo vzdalene strane	

Jestli-že je vybrána a použita služba **PPP**, je třeba specifikovat pro spojení Dial-Out vzdálenou peer IP adresu, uživatelské jméno (Username), heslo (Password), PPP autentifikaci a VJ kompresi.

Nastavení Dial-Out

Typ volaného serveru	
<input type="radio"/> ISDN	
<input checked="" type="radio"/> PPTP	
<input type="radio"/> IPSec tunel	
<input type="radio"/> L2TP se zásadami IPSec	<input type="text" value="Žadny"/>

Jmeno server IP/Host pro VPN.
(jako draytek.com nebo 123.45.67.89)

Typ linky	
Typ linky	<input type="text" value="64kb/s"/>
Uzivatelске jmeno	<input type="text" value="draytek"/>
Heslo	<input type="text" value="*****"/>
PPP overovani	<input type="text" value="PAP/CHAP"/>
VJ komprimace	<input checked="" type="radio"/> On <input type="radio"/> vypnuto

Autentifikacni metoda IKE

Sdilený klic

Digitalni podpis(X.509)

IPSec bezpecnostni metoda

Stredni(AH)

Vysoka (ESP)

Index(1-15) v [Plan](#) Setup:

, , ,

Funkce zpetneho volani (CBCP)

Vyzaduje vzdalene zpetne volani

Poskytnout ISDN cislo vzdalene strane

- Vyplňte **Nastavení Dial-In** (Dial-In Settings) jak je uvedeno v následujícím obrázku pro povolení vytvoření VPN tunelu z protějšího routeru B.

Jestli-že je vybrána a použita služba **IPSec**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, Autentifikační metodu IKE (IKE Authentication Method) a IPSec bezpečnostní metodu (IPSec Security Method). Bude platit nastavení definované v okně **IPSec základní nastavení** (IPSec General Setup).

Nastavení Dial-In

Typ povoleného volání Dial-In	
<input checked="" type="checkbox"/> ISDN	Uživatelské jméno <input data-bbox="944 123 1120 145" type="text" value="???"/>
<input type="checkbox"/> PPTP	Heslo <input data-bbox="944 156 1120 179" type="password"/>
<input checked="" type="checkbox"/> IPsec tunel	VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto
<input type="checkbox"/> L2TP se zásadami IPsec <input data-bbox="555 212 673 235" type="text" value="Zadny"/>	
Autentifikační metoda IKE	
<input checked="" type="checkbox"/> Sdílený klic	<input checked="" type="checkbox"/> Sdílený klic IKE <input data-bbox="944 291 1120 313" type="text"/>
<input type="checkbox"/> Digitální podpis(X.509)	<input data-bbox="742 347 794 369" type="text" value="???"/>
IPsec bezpečnostní metoda	
<input checked="" type="checkbox"/> Střední (AH)	
Vysoká (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Funkce zpetného volání (CBCP)	
<input type="checkbox"/> Aktivovat funkci zpetného volání	
<input type="checkbox"/> Použít následující číslo pro zpetné volání	Císlo zpetného volání <input data-bbox="944 616 1120 638" type="text"/>
Poplatky zpetného volání	<input data-bbox="944 649 1024 672" type="text" value="0"/> min.

Jestli-že je vybrána a použita služba **PPP**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, uživatelské jméno (Username), heslo (Password), PPP autentifikaci a VJ kompresi.

Nastavení Dial-In

Typ povoleného volání Dial-In	
<input checked="" type="checkbox"/> ISDN	Uživatelské jméno <input data-bbox="944 884 1120 907" type="text" value="draytek"/>
<input checked="" type="checkbox"/> PPTP	Heslo <input data-bbox="944 918 1120 940" type="password" value="*****"/>
<input type="checkbox"/> IPsec tunel	VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto
<input type="checkbox"/> L2TP se zásadami IPsec <input data-bbox="555 974 673 996" type="text" value="Zadny"/>	
Autentifikační metoda IKE	
<input checked="" type="checkbox"/> Sdílený klic	<input checked="" type="checkbox"/> Sdílený klic IKE <input data-bbox="944 1052 1120 1075" type="text"/>
<input type="checkbox"/> Digitální podpis(X.509)	<input data-bbox="742 1108 794 1131" type="text" value="???"/>
IPsec bezpečnostní metoda	
<input checked="" type="checkbox"/> Střední (AH)	
Vysoká (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Funkce zpetného volání (CBCP)	
<input type="checkbox"/> Aktivovat funkci zpetného volání	
<input type="checkbox"/> Použít následující číslo pro zpetné volání	Císlo zpetného volání <input data-bbox="944 1377 1120 1400" type="text"/>
Poplatky zpetného volání	<input data-bbox="944 1411 1024 1433" type="text" value="0"/> min.

- Nastavte vzdálenou IP síť/ masku v **TCP/IP network Settings** tak, aby router A mohl nasměrovat pakety přímo na vzdálenou síť routeru B přes VPN tunel.

Nastavení routeru B v pobočce:

- Otevřete v základním menu položku VPN a vzdálený přístup (VPN and Remote Access) a vyberte Řízení vzdáleného přístupu (Remote Access Control). Vyberte typ služby VPN který chcete používat a klikněte na OK.
- Pro aplikace spojené s PPP jako jsou PPTP, L2TP budete provádět základní nastavení v okně **PPP základní nastavení** (PPP General Setup).

PPP hlavní nastavení

PPP/MP protokol		Přidělování IP adres pro Dial-In uživatele	
Dial-In PPP autentifikace	<input type="text" value="PAP nebo CHAP"/>	Start IP adresa	<input type="text" value="192.168.2.200"/>
Dial-In PPP kryptování(MPPE)	<input type="text" value="Volitelně MPPE"/>		
Vzájemná autentifikace (PAP)	<input type="radio"/> Ano <input checked="" type="radio"/> Ne		
Uživatelské jméno	<input type="text"/>		
Heslo	<input type="text"/>		

OK

Pro aplikace spojené s IPSec jako jsou IPSec, nebo L2TP s IPSec policy budete provádět základní nastavení v okně **IPSec hlavní nastavení** (IPSec General Setup). Pozor sdílený klíč se musí stejný pro obě strany.

VPN IKE/IPSec základní nastavení

Dial-in nastavení pro vzdáleného dial-in uživatele a dynamického IP klienta (LAN to LAN).

Autentifikační metoda IKE	
Sdílený klíč	<input type="text" value="*****"/>
Znovu zadat sdílený klíč	<input type="text" value="*****"/>
Bezpečnostní metoda IPSec	
<input checked="" type="checkbox"/> Střední (AH)	Data budou overována, ale nebudou kryptována.
Vysoký (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	Data budou kryptována a overována.

OK

Zrusit

- Přejděte na položku **LAN – LAN** (LAN-to-LAN) a klikněte na číslo indexu pro editaci nového profilu.
- Konfigurace **Obecná nastavení** (Common Settings) je následující. Pokud zaškrtnete **Oba** (Both) ve **Směr volání** (Call Direction), mají obě strany nezávisle na sobě možnost vytvářet VPN tunel (tzn., že spojení vytváří strana A, nebo strana B).

Profil Index : 1

Obecná nastavení

Jmeno profilu <input type="text" value="pobočka 1"/>	Smer volani <input checked="" type="radio"/> Oba <input type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Aktivovat tento profil	<input type="checkbox"/> Vždy zapnuto
	Odpojit po <input type="text" value="300"/> vterin
	<input type="checkbox"/> Aktivovat PING aby tunel zustal aktivni
	PING na IP <input type="text"/>

Vyplňte **Nastavení Dial-Out** (Dial-Out-Settings) jak je uvedeno v následujícím obrázku pro volání a vytvoření VPN tunelu na protější router A.

Jestli-že je vybrána a použita služba **IPSec**, je třeba specifikovat pro spojení Dial-Out vzdálenou peer IP adresu, Autentifikační metodu IKE (IKE Authethication Method) a IPSec bezpečnostní metodu (IPSec Security Method).

Nastavení Dial-Out

<p>Typ volaneho serveru</p> <p><input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec tunel <input type="radio"/> L2TP se zasadami IPSec <input type="text" value="Zadny"/></p> <p>Jmeno server IP/Host pro VPN. (jako draytek.com nebo 123.45.67.89)</p> <input type="text" value="220.135.240.208"/>	<p>Typ linky <input type="text" value="64kb/s"/></p> <p>Uzivatelске jmeno <input <="" p="" type="text" value="???"/><p>Heslo <input type="text"/></p><p>PPP overovani <input type="text" value="PAP/CHAP"/></p><p>VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto</p><p>Autentifikacni metoda IKE</p><p><input checked="" type="radio"/> Sdilený klic <input type="text" value="Sdileny klic IKE"/> <input type="text" value="*****"/></p><p><input type="radio"/> Digitalni podpis(X.509) <input <="" p="" type="text" value="???"/><p>IPSec bezpecnostni metoda</p><p><input checked="" type="radio"/> Stredni(AH) <input type="radio"/> Vysoka (ESP) <input type="text" value="DES bez overovani"/></p><p><input type="button" value="Rozsirene"/></p><p>Index(1-15) v Plan Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p><p>Funkce zpetneho volani (CBCP)</p><p><input type="checkbox"/> Vyzaduje vzdalene zpetne volani <input type="checkbox"/> Poskytnout ISDN cislo vzdalene strane</p></p></p>
---	--

Jestli-že je vybrána a použita služba **PPP**, je třeba specifikovat pro spojení Dial-Out vzdálenou peer IP adresu, uživatelské jméno (Username), heslo (Password), PPP autentifikaci a VJ kompresi.

Nastavení Dial-Out

Typ volaného serveru	
<input type="radio"/> ISDN	
<input checked="" type="radio"/> PPTP	
<input type="radio"/> IPSec tunel	
<input type="radio"/> L2TP se zásadami IPSec	Zadny

Jmeno server IP/Host pro VPN.
(jako draytek.com nebo 123.45.67.89)

Typ linky	64kb/s
Uzivatelске jmeno	draytek
Heslo	*****
PPP overovani	PAP/CHAP
VJ komprimace	<input checked="" type="radio"/> On <input type="radio"/> vypnuto

Autentifikacni metoda IKE

Sdilený klic

Sdilený klic IKE

Digitalni podpis(X.509)

???

IPSec bezpecnostni metoda

Stredni(AH)

Vysoka (ESP) DES bez overovani

Rozsirene

Index(1-15) v [Plan](#) Setup:

 , , ,

Funkce zpetneho volani (CBCP)

Vyzaduje vzdalene zpetne volani

Poskytnout ISDN cislo vzdalene strane

- Vyplňte **Nastavení Dial-In** (Dial-In Settings) jak je uvedeno v následujícím obrázku pro povolení vytvoření VPN tunelu z protějšího routeru A.

Jestli-že je vybrána a použita služba **IPSec**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, Autentifikační metodu IKE (IKE Authentication Method) a IPSec bezpečnostní metodu (IPSec Security Method). Bude platit nastavení definované v okně **IPSec základní nastavení** (IPSec General Setup).

Nastavení Dial-In

Typ povoleného volání Dial-In	
<input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec tunel <input type="checkbox"/> L2TP se zásadami IPsec <input type="text" value="Žadný"/>	Uživatelské jméno <input type="text" value="???"/> Heslo <input type="text"/> VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto
<input checked="" type="checkbox"/> Specifikovat vzdálenou VPN bránu pripojovaného VPN serveru IP <input type="text" value="220.135.240.210"/> nebo lokální ID <input type="text"/>	Autentifikační metoda IKE <input checked="" type="checkbox"/> Sdílený klic <input type="text" value="Sdílený klic IKE"/> <input type="checkbox"/> Digitální podpis(X.509) <input <="" td="" type="text" value="???"/>
	IPsec bezpečnostní metoda <input checked="" type="checkbox"/> Střední (AH) Vysoká (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	Funkce zpetného volání (CBCP) <input type="checkbox"/> Aktivovat funkci zpetného volání <input type="checkbox"/> Použít následující číslo pro zpetné volání Číslo zpetného volání <input type="text"/> Poplatky zpetného volání <input type="text" value="0"/> min.

Jestli-že je vybrána a použita služba **PPP**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, uživatelské jméno (Username), heslo (Password), PPP autentifikaci a VJ kompresi.

Nastavení Dial-In

Typ povoleného volání Dial-In	
<input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec tunel <input type="checkbox"/> L2TP se zásadami IPsec <input type="text" value="Žadný"/>	Uživatelské jméno <input type="text" value="draytek"/> Heslo <input type="text" value="*****"/> VJ komprimace <input checked="" type="radio"/> On <input type="radio"/> vypnuto
<input checked="" type="checkbox"/> Specifikovat vzdálenou VPN bránu pripojovaného VPN serveru IP <input type="text" value="220.135.240.210"/> nebo lokální ID <input type="text"/>	Autentifikační metoda IKE <input checked="" type="checkbox"/> Sdílený klic <input type="text" value="Sdílený klic IKE"/> <input type="checkbox"/> Digitální podpis(X.509) <input <="" td="" type="text" value="???"/>
	IPsec bezpečnostní metoda <input checked="" type="checkbox"/> Střední (AH) Vysoká (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	Funkce zpetného volání (CBCP) <input type="checkbox"/> Aktivovat funkci zpetného volání <input type="checkbox"/> Použít následující číslo pro zpetné volání Číslo zpetného volání <input type="text"/> Poplatky zpetného volání <input type="text" value="0"/> min.

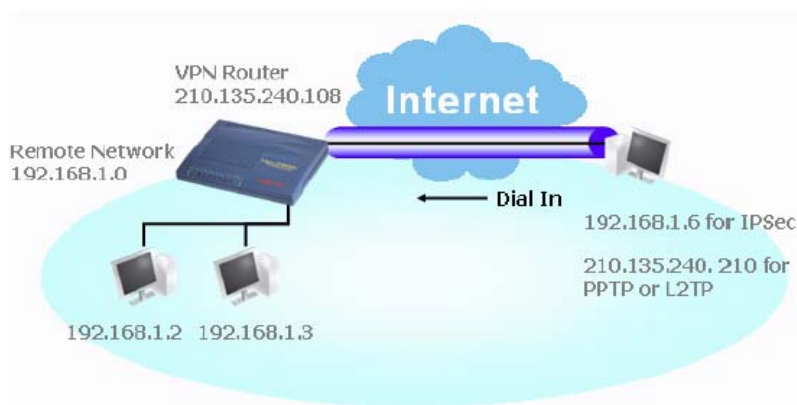
- Nastavte vzdálenou IP síť/ masku v **TCP/IP network Settings** tak, aby router B mohl nasměrovat pakety přímo na vzdálenou síť routeru A přes VPN tunel.

Nastavení TCP/IP site

Moje WAN IP	<input type="text" value="0.0.0.0"/>	RIP smerovani	<input type="text" value="TX/RX oba"/>
IP vzdalene brany	<input type="text" value="0.0.0.0"/>	Pro NAT operace, zachazet se vzdalenu podsiti jako s	
IP vzdalene site	<input type="text" value="192.168.2.0"/>	<input type="text" value="Privatni IP"/>	
Maska vzdalene site	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Zmenit default route pres tento tunel	
<input type="button" value="Vice"/>			

4.2 Vzdálený přístup mezi uživatelem teleworker (práce z domova) a centrálou.

Další aplikací je, pokud se chcete jako teleworker přihlásit vzdáleně na centrálu a pracovat z domova v podnikové síti. Síťová struktura je zobrazena na níže uvedeném obrázku a v dalším textu je zpracována konfigurace routeru i VPN klienta.



- Otevřete v základním menu položku VPN a vzdálený přístup (VPN and Remote Access) a vyberte Řízení vzdáleného přístupu (Remote Access Control). Vyberte typ služby VPN který chcete používat a klikněte na OK.
- Pro aplikace spojené s PPP jako jsou PPTP, L2TP budete provádět základní nastavení v okně **PPP základní nastavení** (PPP General Setup).

PPP hlavní nastavení

PPP/MP protokol Dial-In PPP autentifikace <input type="text" value="PAP nebo CHAP"/> Dial-In PPP kryptování(MPPE) <input type="text" value="Volitelně MPPE"/> Vzájemná autentifikace (PAP) <input type="radio"/> Ano <input checked="" type="radio"/> Ne Uživatelské jméno <input type="text"/> Heslo <input type="text"/>	Přidělování IP adres pro Dial-In uživatele Start IP adresa <input type="text" value="192.168.2.200"/>
--	---

OK

Pro aplikace spojené s IPSec jako jsou IPSec, nebo L2TP s IPSec policy budete provádět základní nastavení v okně **IPSec hlavní nastavení** (IPSec General Setup). Pozor sdílený klíč se musí stejný pro obě strany.

VPN IKE/IPSec základní nastavení

Dial-in nastavení pro vzdáleného dial-in uživatele a dynamického IP klienta (LAN to LAN).

Autentifikační metoda IKE Sdílený klíč <input type="text" value="*****"/> Znovu zadat sdílený klíč <input type="text" value="*****"/>
Bezpečnostní metoda IPSec <input checked="" type="checkbox"/> Střední (AH) Data budou overována, ale nebudou kryptována. Vysoký (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data budou kryptována a overována.

OK

Zrusit

- Přejděte do položky **Vzdálený Dial-In uživatel** (Remote Dial-In Users). Klikněte na číslo indexu pro editaci profilu.
- Vyplňte Dial-In nastavení jak je uvedeno v následujícím obrázku pro vzdáleného dial-in uživatele k vytvoření VPN tunelu.

Jestliže je vybrána a použita služba **IPSec**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, Autentifikační metodu IKE (IKE Authentication Method) a IPSec bezpečnostní metodu (IPSec Security Method). Bude platit nastavení definované v okně **IPSec základní nastavení** (IPSec General Setup).

Index c. 1

<p>Uzivatel'sky ucet a autentifikace</p> <p><input checked="" type="checkbox"/> Aktivovat tento ucet</p> <p>Odpojit po <input type="text" value="300"/> vterin</p> <hr/> <p>Typ povoleného volání Dial-In</p> <p><input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec tunel <input type="checkbox"/> L2TP s IPSec principy <input type="text" value="Zadna"/></p> <p><input checked="" type="checkbox"/> Specifikovat vzdaleny uzel IP vzdaleneho klienta nebo ISDN cislo <input type="text" value="200.135.240.210"/> nebo lokalni ID <input type="text"/></p>		<p>Uzivatel'ske jmeno <input data-bbox="944 188 1121 215" type="text" value="???"/></p> <p>Heslo <input data-bbox="944 224 1121 250" type="password"/></p> <hr/> <p>Autentifikacni metoda IKE</p> <p><input checked="" type="checkbox"/> Sdileny klic <input data-bbox="746 331 906 358" type="text" value="Sdileny klic IKE"/> <input data-bbox="944 331 1121 358" type="password" value="*****"/></p> <p><input type="checkbox"/> Digitalni podpis (X.509) <input data-bbox="746 394 794 421" type="text" value="???"/></p> <hr/> <p>IPSec bezpecnostni metoda</p> <p><input checked="" type="checkbox"/> Stredni (AH) Vysoka (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalni ID <input data-bbox="842 555 1018 582" type="text"/> (volitelne)</p> <hr/> <p>Funkce zpetneho volani</p> <p><input type="checkbox"/> Aktivovat funkci zpetne volani <input type="checkbox"/> Specifikovat cislo zpetneho volani Cislo zpetneho volani <input data-bbox="944 689 1121 716" type="text"/></p> <p><input checked="" type="checkbox"/> Aktivace uctu zpetneho volani Ucet zpetneho volani <input data-bbox="944 752 976 779" type="text" value="30"/> minut</p>
---	--	---

Jestli-že je vybrána a použita služba **PPP**, je třeba specifikovat pro spojení Dial-In vzdálenou peer IP adresu, uživatelské jméno (Username), heslo (Password), PPP autentifikaci a VJ kompresi.

Index c. 1

Uzivatel'sky ucet a autentifikace <input checked="" type="checkbox"/> Aktivovat tento ucet Odpojit po <input type="text" value="300"/> vterin		Uzivatelske jmeno <input type="text" value="???"/> Heslo <input type="text"/>
Typ povoleného volání Dial-In <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec tunel <input type="checkbox"/> L2TP s IPSec principy <input type="text" value="Žadna"/>		Autentifikacni metoda IKE <input checked="" type="checkbox"/> Sdílený klic <input type="text" value="Sdílený klic IKE"/> <input type="checkbox"/> Digitalní podpis (X.509) <input type="text" value="???"/>
<input checked="" type="checkbox"/> Specifikovat vzdaleny uzel IP vzdaleneho klienta nebo ISDN cislo <input type="text" value="200.135.240.210"/> nebo lokalni ID <input type="text"/>		IPSec bezpecnostni metoda <input checked="" type="checkbox"/> Stredni (AH) Vysoka (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalni ID <input type="text"/> (volitelne)
Funkce zpetneho volani <input type="checkbox"/> Aktivovat funkci zpetne volani <input type="checkbox"/> Specifikovat cislo zpetneho volani <input type="text" value="Cislo zpetneho volani"/> <input checked="" type="checkbox"/> Aktivace uctu zpetneho volani Ucet zpetneho volani <input type="text" value="30"/> minut		

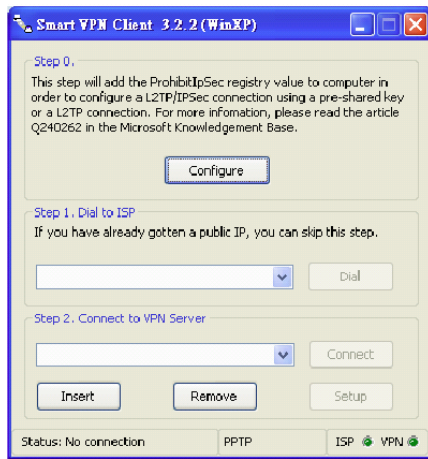
OK

Vymazat

Zrusit

Nastavení vzdáleného klienta (remote host)

- Pro Win98/ME použijte k nastavení PPTP tunelu na router Vigor funkci „Dial-up networking“. Pro Win2000/XP použijte funkci „Network and Dial-up connections“ nebo „Smart VPN Client“, který pomůže s rychlým nastavením tunelu PPTP, L2TP a L2TP přes IPSec. Software je dostupný na přiloženém CD, nebo na stránkách www.draytek.com.
- Po úspěšné instalaci klikněte nejprve na krok 0, tlačítko **Configure** pro Reboot hosta.

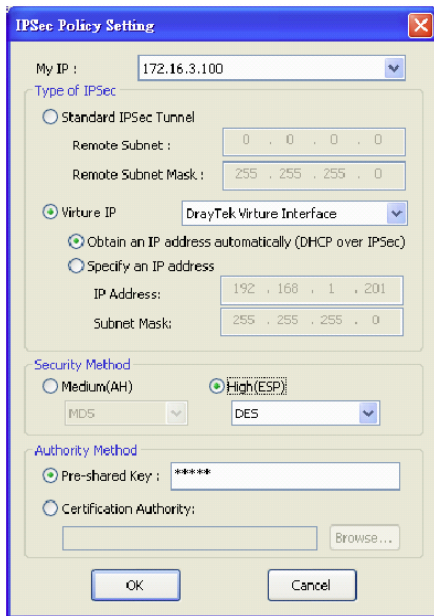


- Krok 2. Spojení na VPN server. Klikněte na tlačítko Insert pro přidání nového záznamu.

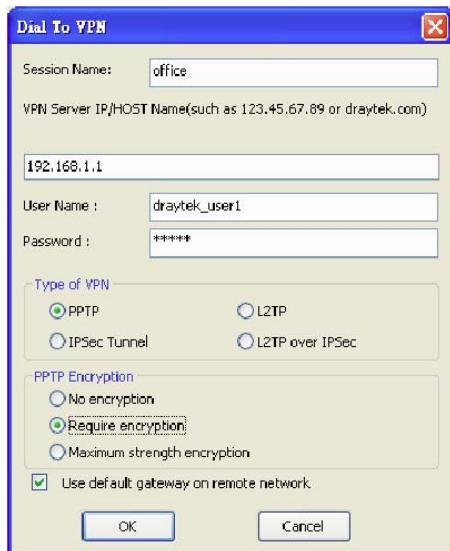
Jestli-že je vybrána služba IPsec nastavení je následující.



Lze specifikovat další nastavení jako jsou IP adresa, kryptovací a autentifikační metodu. Pokud je vybrán sdílený klíč, musí být stejný jako ve VPN routeru.



Pokud je vybrána služba PPP, je třeba specifikovat IP adresu vzdáleného VPN serveru, uživatelské jméno, heslo a kryptovací metodu. Uživatelské jméno a heslo musí souhlasit s nastavením ve VPN routeru. Zaškrtnutí položky „Use default gateway on remote network“ znamená, že všechny pakety ze vzdáleného klienta budou směrovány přes internet přímo na VPN server a vzdálený host bude moci pracovat v podnikové síti.



- Klikněte na tlačítko **Connect** pro vytvoření spojení. Pokud je spojení úspěšné, rozsvítí se zelená kontrolka v pravém dolním rohu obrazovky.

4.3 Příklady nastavení QoS

Při používání funkce Teleworker můžete pracovat přes VPN s firemními daty z domova a při tom třeba hlídat děti. Pro svou nerušenou práci, si vyčleníte šířku pásma, kterou nutně potřebujete pro provoz a zbývající šířku pásma poskytnete dětem na VoIP telefonování apod.

- Klikněte na Řízení pásma >> Kvalita služby QoS. Ujistěte se zda máte zatržené pole Aktivovat řízení QoS (Enable the QoS Control) a v nabídce Směrování (Direction) vyberte OBA (BOTH).

Kvalita služby QoS

Aktivovat řízení QoS

Smerovani

Index skupiny

OBA

- Napište Název skupiny (Class Name) Indexu 1. V tomto Indexu nastavíte šířku pásma pro e-mail používající protokol POP3 a SMTP. Klikněte vpravo na tlačítko Základní (Basic).

Index	Název skupiny	Rezerva pasma	Nastaveni	
1.	E-mail	25 %	Zakladni	Rozsirene
2.		25 %	Zakladni	Rozsirene

- Vyberte POP3 a SMTP v levém sloupci a klikněte na PŘIDAT (Add) pro převedení do pravého sloupce. Klikněte na OK pro odchod.

<ul style="list-style-type: none"> NFS(UDP:2049) NNTP(TCP:119) PING(IP:1) POP3(TCP:110) PPTP(TCP:1723) RCMD(TCP:512) REAL-AUDIO(TCP:7070) RTSP(TCP/UDP:554) SFTP(TCP:115) 	<p>PRIDAT >></p> <p><< ODSTRANIT</p>	
---	--	--

- Vejděte do Nazvu skupiny (Class Name) Indexu 2. V tomto Indexu nastavíte šířku pásma pro HTTP. Klikněte vpravo na tlačítko Základní (Basic).

Index	Nazev skupiny	Rezerva pasma	Nastaveni	
1.	E-mail	25 %	Zakladni	Rozsirene
2.	HTTP	25 %	Zakladni	Rozsirene

- Vyberte HTTPS ze seznamu v levém sloupci a klikněte na PŘIDAT (Add) pro převedení do pravého sloupce. Klikněte na OK pro odchod.

CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53) FINGER(TCP:79) FTP(TCP:20~21) H.323(TCP:1720) HTTP(TCP:80) IKE(UDP:500) IPSEC-AH(IP:51)	<input type="button" value="PRIDAT »"/> <input type="button" value="« ODSTRANIT"/>	HTTPS(TCP:443)
--	---	----------------

- Zaškrtněte pole Aktivovat řízení UDP pásma (Enable UDP Bandwith Control) pro zamezení enormních toků UDP paketů u VoIP ovlivňujících jiné aplikace.

Kvalita služby QoS | [Nastavit do výrobního nastavení](#) |

Aktivovat řízení QoS

Smerovani:

Index	Nazev skupiny	Rezerva pasma	Nastaveni	
1.	E-mail	25 %	Zakladni	Rozsirene
2.	HTTP	25 %	Zakladni	Rozsirene
3.		25 %	Zakladni	Rozsirene
4.	Jine	25 %		

Aktivovat řízení UDP pásma Pomer pro limitovane pasmo: %

[Online statistiky](#)

Pokud je vzdálený klient spojen do centrály užíváním host-host VPN tunelu. (viz. kapitola 3-VPN pro detailnější informace) musí pro to nakonfigurovat index. Vejděte do Názvu skupiny (Class Name) Indexu 3. V tomto indexu lze v tomto případě rezervovat šířku pásma pro 1 VPN tunel.

Klikněte vpravo na tlačítko Rozšířené (Advanced).



Klikněte na tlačítko Vložit (Edit) pro otevření dalšího okna. Nejprve zaškrtněte pole ACT. Pak klikněte na ZdrojÚprava (SrcEdit) pro nastavení masky podsítě vzdáleného klienta. Klikněte na CílÚprava (DestEdit) pro nastavení masky podsítě centrály. Po nastavení klikněte na OK.

Kvalita služby (QoS)

ACT	Zdrojova adresa	Cilova adresa	DiffServ CodePoint	Typ služby
<input checked="" type="checkbox"/>	192.168.1.0 <input type="button" value="ZdrojÚprava"/>	192.168.2.0 <input type="button" value="CílÚprava"/>	ANY <input type="button" value="ZdrojÚprava"/>	ANY <input type="button" value="Přidat"/> <input type="button" value="Úprava"/> <input type="button" value="Vymazat"/>

Pozn.: Vyberte, nebo nejprve nastavte typ služby.

4.4 Příklady pro používání NAT.

Příklad default nastavení a odpovídající zapojení je v následujícím obrázku. Default IP adresa/ maska podsítě routeru Vigor je 192.168.1.1/255.255.255.0. Používá se vestavěný DHCP server Vigoru a ten přiřazuje každému lokálnímu NATovanému hostu IP adresu z rozsahu 192.168.1.x začínající od 192.168.1.10.



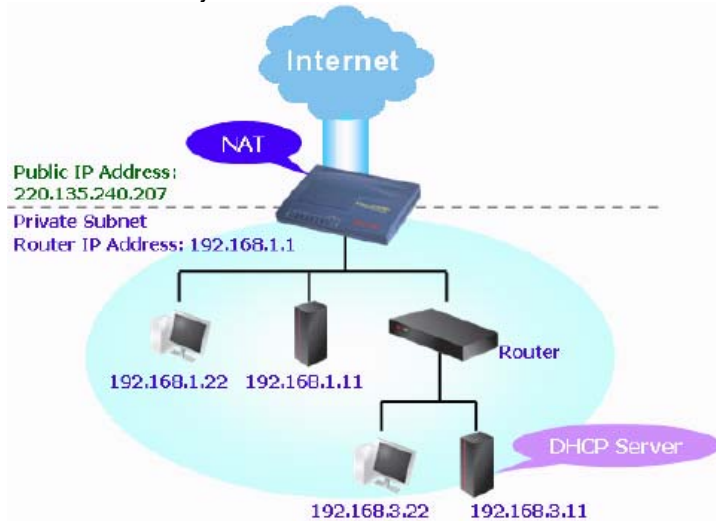
Nyní lze nastavit konfiguraci uvnitř červených obdélníků tak jak požadujete pro používání NAT (kterou síť potřebujete schovat za NAT).

Ethernet TCP / IP a DHCP nastavení

Konfigurace LAN IP site	Konfigurace DHCP serveru
Pro použití NAT	<input checked="" type="radio"/> Aktivovat server <input type="radio"/> Deaktivovat server
1st IP adresa: 192.168.1.1	Relay Agent: <input type="radio"/> 1. podsit <input checked="" type="radio"/> 2. podsit
1st Maska podsítě: 255.255.255.0	Start IP adresa: 192.168.1.10
Pro užívání IP Routing: <input type="radio"/> Zap. <input checked="" type="radio"/> Vyp.	Pocet přidělovaných IP: 50
2. IP adresa: 192.168.2.1	IP adresa brány: 192.168.1.1
2. Maska podsítě: 255.255.255.0	IP adresa DHCP pro vzdaleneho agenta: []
DHCP server 2.podsítě	
Rizeni RIP protokolem: Vyp.	IP pro DNS server
	Primarni IP adresa: []
	Sekundarni IP adresa: []

OK

Při používání jiného DHCP serveru v síti než toho, který je vestavěný ve Vigoru, je nastavení následující.



Nyní lze nastavit konfiguraci uvnitř červených obdélníků tak jak požadujete pro používání NAT (kterou síť potřebujete schovat za NAT).

Ethernet TCP / IP a DHCP nastavení

Konfigurace LAN IP site		Konfigurace DHCP serveru	
Pro použití NAT		<input type="radio"/> Aktivovat server <input checked="" type="radio"/> Deaktivovat server	
1st IP adresa	<input type="text" value="192.168.1.1"/>	Relay Agent:	<input type="radio"/> 1. podsít <input checked="" type="radio"/> 2. podsít
1st Maska podsítě	<input type="text" value="255.255.255.0"/>	Start IP adresa	<input type="text" value="192.168.1.10"/>
Pro užívání IP Routing <input type="radio"/> Zap. <input checked="" type="radio"/> Vyp.		Pocet přidělovaných IP	<input type="text" value="50"/>
2. IP adresa	<input type="text" value="192.168.2.1"/>	IP adresa brány	<input type="text" value="192.168.1.1"/>
2. Maska podsítě	<input type="text" value="255.255.255.0"/>	IP adresa DHCP pro vzdaleneho agenta	<input type="text" value="192.168.3.11"/>
<input type="button" value="DHCP server 2.podsítě"/>		IP pro DNS server	
Rizeni RIP protokolem	<input type="text" value="Vyp."/> ▼	Primarni IP adresa	<input type="text"/>
		Sekundarni IP adresa	<input type="text"/>

4.5 Příklady nastavení pro volání VoIP.

4.5.1 Volání přes SIP server

Příklad 1. Honza a David mají SIP adresy od různých SIP poskytovatelů.

Honzovo SIP URL je: 1234@draytel.org, Davidovo URL je: 4321@iptel.org

Nastavení pro Honzu

Telef.seznam Index č. 1

Telef. číslo: 1111

Zobraz. jméno: David

SIP URL: 4321@iptel.org

SIP účet

Jméno profilu: draytel 1

Registrace přes: Auto

SIP port: 5060 (default)

Doména/Oblast: draytel.org

Proxy: draytel.org

Pracovat jako odchoz. proxy:
nezatrženo

Zobraz. jméno: Honza

Číslo účtu/Jméno: 1234

Autentifikace ID: nezatrženo

Heslo: ****

Čas platnosti: (použít default
hodnotu)

VoIP >> Nastavení rychlého vytaceni

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	Telefonní číslo	<input type="text" value="1111"/>
	Zobrazované jméno	<input type="text" value="David"/>
	SIP URL	<input type="text" value="4321"/> @ <input type="text" value="iptel.org"/>
	Přístup na náhradní linku	<input type="text" value="None"/>
	Náhradní telef. číslo	<input type="text"/>

VoIP >> SIP ucety

SIP ucet Index c. 1

Jméno profilu	<input type="text" value="draytel 1"/> (max 11 znaku)
Registrace přes	<input type="text" value="Auto"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text" value="draytel.org"/> (max 63 znaku)
Proxy	<input type="text" value="draytel.org"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="Honza"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="1234"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1"/> hod. <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

CODEC/RTP/DTMF

(použít default hodnotu)

Honza volá Davida

Zvedne telefon a vytočí 1111#. (Telef. seznam, telef. číslo Davida)

Nastavení pro Davida
Telef.seznam Index č.1
Telef. číslo: 2222
Zobraz. jméno: Honza
SIP URL: 1234@draytel.org

SIP účet

Jméno profilu: iptel 1
Registrace přes: Auto
SIP port: 5060 (default)
Doména/Oblast: iptel.org
Proxy: iptel.org
Pracovat jako odchoz. proxy:
nezatrženo
Zobraz. jméno: David
Číslo účtu/Jméno: 4321
Autentifikace ID: nezatrženo
Heslo: ****
Čas platnosti: (použít default
hodnotu)

CODEC/RTP/DTMF

(použít default hodnotu)

VoIP >> Nastavení rychlého vytaceni

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	Telefonní číslo	<input type="text" value="2222"/>
	Zobrazované jméno	<input type="text" value="Honza"/>
	SIP URL	<input type="text" value="1234@draytel.org"/>
	Přístup na náhradní linku	<input type="text" value="None"/>
	Náhradní telef. číslo	<input type="text"/>

OK Vymazat Zrusit

VoIP >> SIP ucety

SIP ucet Index c. 1

Jméno profilu	<input type="text" value="iptel 1"/> (max 11 znaku)
Registrace přes	<input type="text" value="Auto"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text" value="iptel.org"/> (max 63 znaku)
Proxy	<input type="text" value="iptel.org"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="David"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="4321"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1"/> hod. <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

OK Zrusit

David volá Honzu

Zvedne telefon a vytočí 2222#. (Telef. seznam, telef. číslo Honzy)

Příklad 2. Honza a David mají SIP adresy od stejného SIP poskytovate.
Honzo SIP URL je:1234@draytel.org, Davidovo URL je: 4321@draytel.org

Nastavení pro Honzu

Telef.seznam Index č.1
Telef. číslo: 1111
Zobraz. jméno: David
SIP URL: 4321@draytel.org

SIP účet

Jméno profilu: draytel 1
Registrace přes: Auto
SIP port: 5060 (default)
Doména/Oblast: draytel.org
Proxy: draytel.org
Pracovat jako odchoz. proxy:
nezatrženo
Zobraz. jméno: John
Číslo účtu/Jméno: 1234
Autentifikace ID: nezatrženo
Heslo: ****
Čas platnosti: (použít default
hodnotu)

CODEC/RTP/DTMF

(použít default hodnotu)

VoIP >> Nastavení rychlého vytáčení

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	
Telefonní číslo	<input type="text" value="1111"/>
Zobrazované jméno	<input type="text" value="David"/>
SIP URL	<input type="text" value="4321"/> @ <input type="text" value="draytel.org"/>
Přístup na náhradní linku	<input type="text" value="None"/>
Náhradní telef. číslo	<input type="text"/>

OK

Vymazat

Zrusit

VoIP >> SIP účty

SIP ucet Index c. 1

Jméno profilu	<input type="text" value="draytel 1"/> (max 11 znaku)
Registrace přes	<input type="text" value="Auto"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text" value="draytel.org"/> (max 63 znaku)
Proxy	<input type="text" value="draytel.org"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="Honza"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="1234"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1 hod."/> <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Žádná"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

OK

Zrusit

Honza volá Davida

Zvedne telefon a vytočí 1111#. (Telef. seznam, telef. číslo Davida) nebo,
Zvedne telefon a vytočí 4321#. (Davidovo číslo účtu)

Nastavení pro Davida
Telef.seznam Index č.1
Telef. číslo: 2222
Zobraz. jméno: John
SIP URL: 1234@draytel.org

SIP účet

Jméno profilu: iptel 1
Registrace přes: Auto
SIP port: 5060 (default)
Doména/Oblast: draytel.org
Proxy: draytel.org
Pracovat jako odchoz. proxy:
nezatrženo
Zobraz. jméno: David
Číslo účtu/Jméno: 4321
Autentifikace ID: nezatrženo
Heslo: ****
Čas platnosti: (použít default
hodnotu)

CODEC/RTP/DTMF
(použít default hodnotu)

VoIP >> Nastavení rychlého vytáčení

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	Telefonní číslo	<input type="text" value="2222"/>
	Zobrazované jméno	<input type="text" value="Honza"/>
	SIP URL	<input type="text" value="1234"/> @ <input type="text" value="draytel.org"/>
	Přístup na náhradní linku	<input type="text" value="None"/>
	Náhradní telef. číslo	<input type="text"/>

OK Vymazat Zrusit

VoIP >> SIP účty

SIP ucet Index c. 1

Jméno profilu	<input type="text" value="draytel 1"/> (max 11 znaku)
Registrace přes	<input type="text" value="Auto"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text" value="draytel.org"/> (max 63 znaku)
Proxy	<input type="text" value="draytel.org"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="David"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="4321"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1 hod."/> <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

OK Zrusit

David volá Honzu

Zvedne telefon a vytočí 2222#. (Telef. seznam, telef. číslo Honzy), nebo
Zvedne telefon a vytočí 1234#. (Honzovo číslo účtu)

4.5.2 Volání Peer-to Peer

Příklad 3. Adam a Petra nemají routery Vigor zaregistrovány na SIP server. Nejdříve musí oba vlastnit veřejnou IP adresu a dále přiřadit pro port, který budou používat pro telefonování jméno účtu.

Adamovo SIP URL je:1234@214.81.172.53, Petry URL je: 4321@203.69.175.24

Nastavení pro Adama

Telef.seznam Index č.1

Telef. číslo: 1111

Zobraz. jméno: Petra

SIP

1234@203.69.175.24

URL:

SIP účet

Jméno profilu: Petra

Registrace přes: Žádná

SIP port: 5060 (default)

Doména/Oblast: prázdné

Proxy: prázdné

Pracovat jako odchoz. proxy:
nezatrženo

Zobraz. jméno: Adam

Číslo účtu/Jméno: 1234

Autentifikace ID: nezatrženo

Heslo: prázdné

Čas platnosti: (použít default
hodnotu)

VoIP >> Nastavení rychlého vytáčení

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	
Telefonní číslo	<input type="text" value="1111"/>
Zobrazované jméno	<input type="text" value="Petra"/>
SIP URL	<input type="text" value="4321"/> @ <input type="text" value="203.69.175.24"/>
Přístup na náhradní linku	<input type="text" value="None"/>
Náhradní telef. číslo	<input type="text"/>

VoIP >> SIP účty

SIP ucet Index c. 1

Jméno profilu	<input type="text" value="Petra"/> (max 11 znaku)
Registrace přes	<input type="text" value="Zadna"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text"/> (max 63 znaku)
Proxy	<input type="text"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="Adam"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="1234"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1 hod."/> <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

CODEC/RTP/DTMF

(použít default hodnotu)

Adam volá Petru

Zvedne telefon a vytočí 1111#. (Telef. seznam, telef. číslo pro Petru)

Nastavení pro Petru
Telef.seznam Index č.1
Telef. číslo: 2222
Zobraz. jméno: Adam
SIP URL: [1234@214.81.172.53](tel:1234@214.81.172.53)

SIP účet

Jméno profilu: Adam
Registrace přes: Žádná
SIP port: 5060 (default)
Doména/Oblast: prázdné
Proxy: prázdné
Pracovat jako odchoz. proxy:
nezatrženo
Zobraz. jméno: Petra
Číslo účtu/Jméno: 4321
Autentifikace ID: nezatrženo
Heslo: prázdné
Čas platnosti: (použít default
hodnotu)

CODEC/RTP/DTMF

(použít default hodnotu)

VoIP >> Nastavení rychlého vytáčení

Telef.seznam Index c. 1

<input checked="" type="checkbox"/> Aktivovat	Telefonní číslo	<input type="text" value="2222"/>
	Zobrazované jméno	<input type="text" value="Adam"/>
	SIP URL	<input type="text" value="1234"/> @ <input type="text" value="214.81.172.53"/>
	Přístup na náhradní linku	<input type="text" value="None"/>
	Náhradní telef. číslo	<input type="text"/>

VoIP >> SIP ucty

SIP uctet Index c. 1

Jméno profilu	<input type="text" value="Adam"/> (max 11 znaku)
Registrace přes	<input type="text" value="Zadna"/> <input type="checkbox"/> Telefonovat bez registrace
SIP Port	<input type="text" value="5060"/>
Doména/Oblast	<input type="text"/> (max 63 znaku)
Proxy	<input type="text"/> (max 63 znaku)
<input type="checkbox"/> Pracovat jako odchozí proxy	
Zobrazované jméno	<input type="text" value="Petra"/> (max 23 znaku)
Číslo účtu/Jméno	<input type="text" value="4321"/> (max 63 znaku)
<input type="checkbox"/> Autentifikace ID	<input type="text"/> (max 63 znaku)
Heslo	<input type="text" value="****"/> (max 63 znaku)
Čas platnosti	<input type="text" value="1"/> hod. <input type="text" value="3600"/> vt.
Podpora NAT Traversal	<input type="text" value="Zadna"/>
Port	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Typ zvonění	<input type="text" value="1"/>

Petra volá Adama

Zvedne telefon a vytočí 2222#. (Telef. seznam, telef. číslo pro Adama)

4.6 Upgrade firmware.

Před upgrade firmware nainstalujte na Váš počítač program Router Tools. Utilita pro upgrade je obsažena v tomto programu.

- 1.Vložte příložené CD
- 2.Přes prohlížeč webových stránek vyhledejte menu Utility a klikněte na ni.
- 3.Po otevření klikněte na Install Now pro instalaci programu.

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

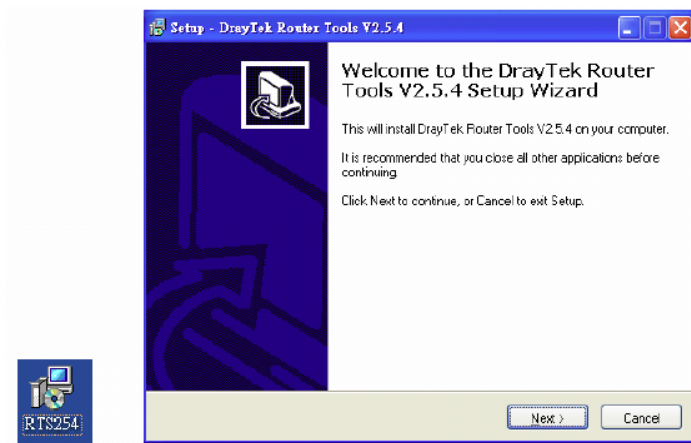
Install Now!

- 4.Soubor RTSxxx.exe bude požádán na kopírování do počítače. Nezapomeňte místo uložení tohoto exe souboru.
- 5.Přejděte na stránku www.draytek.com a vyhledejte nejnovější verzi firmware.
6. Po přístupu na Support Center>Downloads vyhledejte model routeru který používáte a klikněte na linku firmware. Nabídka programů Tools pro Vigory vypadá následovně.

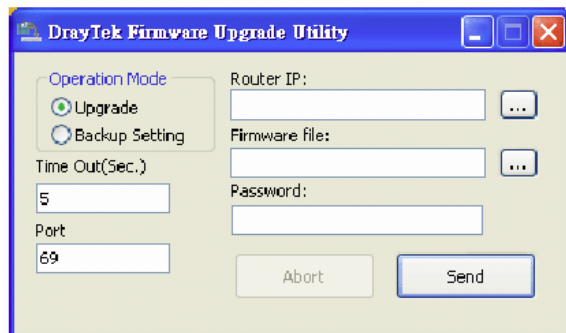
Note : first introduction for Tools

Tools of Vigor						
Name	Version	Language	Release Date	OS	File	Size
Router Tools	2.4.5	English	07/11/2005	MacOSX	dmg	10.4 MB
Router Tools	2.5.4	English	07/11/2005	Windows	zip	0.61 MB
Smart VPN Client	3.2.2	English	07/11/2005	Windows2000/XP	zip	0.54 MB

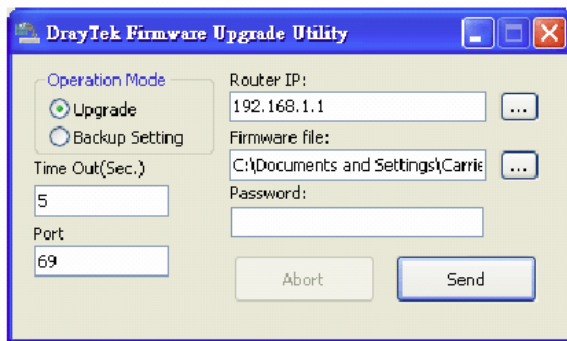
- 7.Vyberte z nabídky pro správný operační systém, který používáte a klikněte na linku na správnou verzi firmware (soubor zip).
- 8.Dekomprimujte tento soubor.
- 9.Dvojitým kliknutím klikněte na ikonu Router Tools. Pro spuštění pomocníka při instalaci.



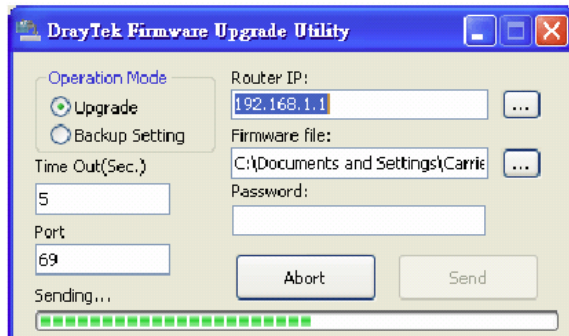
10. Proveďte instalaci dle instrukcí a klikněte na Finish pro ukončení instalace.
11. Přes menu Start/ Programy vyhledejte program Router Tools XXX a položku Firmware Upgrade Utility.



12. Vyplňte IP adresu routeru, např. 192.168.1.1
13. Klikněte na tlačítko vpravo od vyplňované adresy. Vyhledejte místo kde máte umístěny soubory s firmware. Verze xxx.all (zachová stávající nastavení), verze xxx.rst (resetuje do výrobního nastavení).

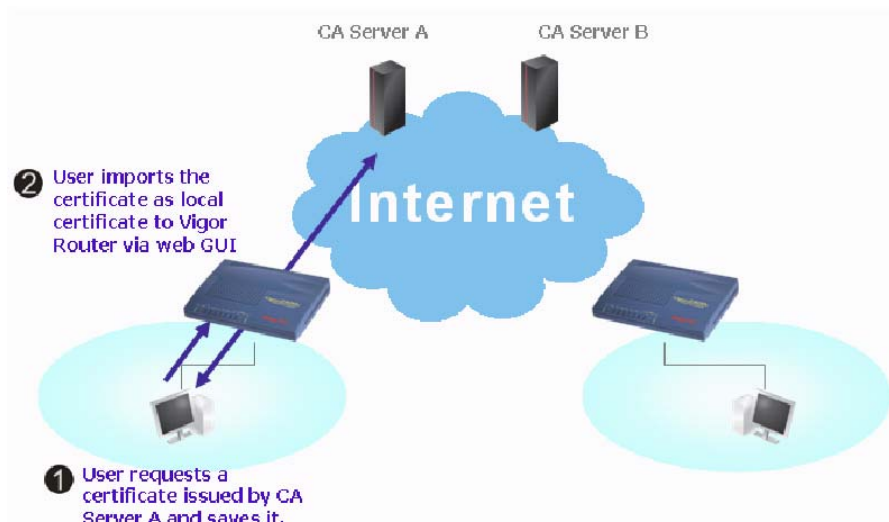


14. Klikněte na Send.



15. Nyní je update firmware ukončen.

4.7 Žádosti a certifikáty z CA serveru na Windows CA server.



1. Přejděte na Správa certifikátů (Certificate Management) a vyberte Lokální certifikát (Local Certificate).

[Správa certifikátu >> Lokální certifikát](#)

Konfigurace lokálního X509 certifikátu

Jmeno	Subjekt	Stav	Zmena
Lokální	---	---	Zobrazit Vymazat

GENEROVAT IMPORT OBNOVIT

Lokální X509 certifikát

2. Lze kliknout na tlačítko GENEROVAT (GENERATE) pro start editace žádosti. Potvrďte informace v žádosti o certifikát.

Generovat požadavek na certifikát

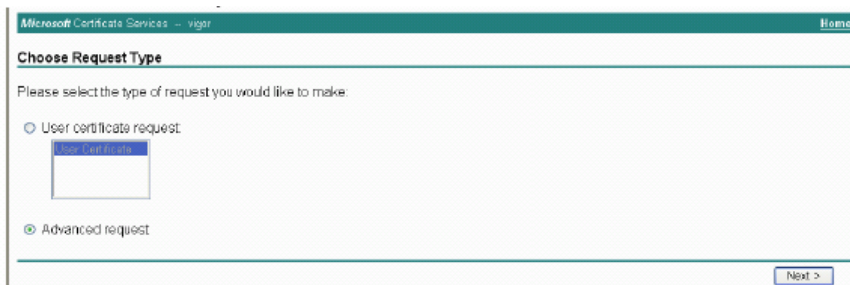
Alternativní jméno subjektu	
Typ	Jmeno domeny ▾
Jmeno domeny	draytek.com
Jméno subjektu	
Zeme (C)	TW
Stat (ST)	
Lokalita (L)	
Organizace (O)	Draytek
Organizacni jednotka (OU)	
Obecne jmeno (CN)	
Email (E)	press@draytek.com
Typ klíče	RSA ▾
Velikost klíče	1024 Bit ▾

3. Zkopírujte a uložte Žádost o lokální certifikát X509 jako textový soubor a uložte pro pozdější použití.

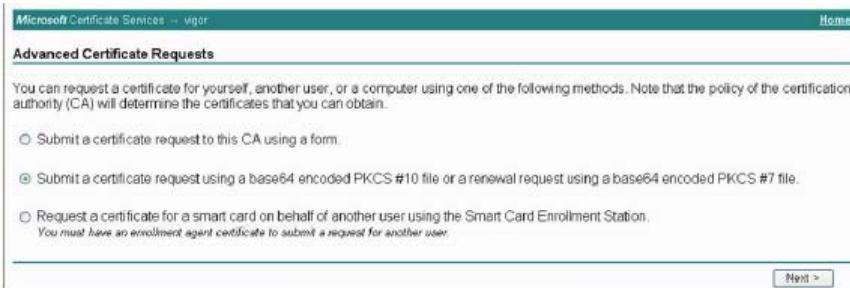
Konfigurace lokálního X509 certifikátu

Jmeno	Subjekt	Stav	Zmena
Lokalni	/C=TW/O=Draytek/emailAddress...	Requesting	Zobrazit Vymazat
GENEROVAT IMPORT OBNOVIT			
Zadost na lokalni X509 certifikat			
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBqjCCARMCAQAwQTElMAkGA1UEBhMCVFcxEDAOBgNVBaoTB0RyYX10ZWsxIDAe BgkqhkiG9wOBCQEWEYyZmZlZmZlZmZlZmZlZmZlZmZlZmZlZmZlZmZlZmZlZmZl A4GNADCBiQKBggQSC9TAwPY5xNQenXxmhjmfIPyRcVrvXXcWFFYsLAWdNs6jC4WLYY OmzHsuXrOwmrgvRe2iPwZXyh3Wi8uw3JLYNqAyfILM4M8cYGkMvmFMSLtDgIJnjQ hpq8YxdxoAPLixEhTEUEBp4J6mSeznyDG273gu67Wmdpyd+dip3IBLQURwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANgggtkcmF5dGVrLmNvbTANBgkq hkiG9wOBAQUFAAOBgQCMIJpTnhHyAJZgc1uihKOWQ6jDbTQWV9v1ItHnvLhdXId7 6L14ZW6OnoFFLN2ZJz85SOHAUmpUZM10551nnIL4sG0FFZaYFdJbA0Fet5vroyme DEA3ETFxny4L/sqEfg4zWuBCpJBFOV1pdNzcAp5KU3IFH0wR92z3xWiEHVS4IQ== -----END CERTIFICATE REQUEST-----</pre>			

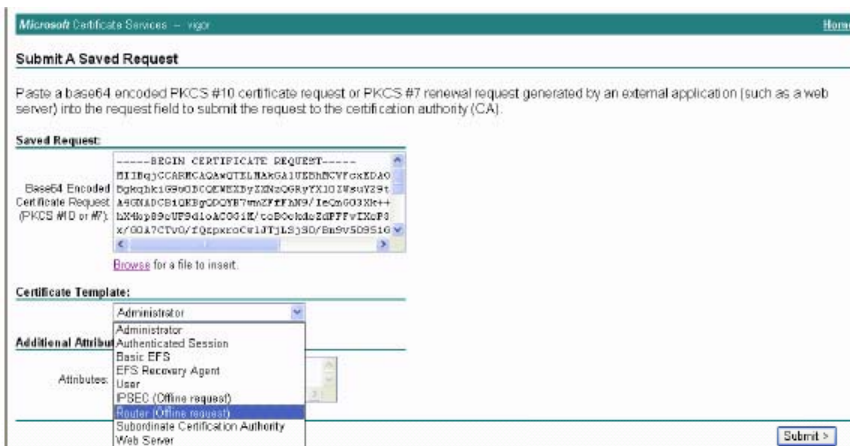
4. Připojte se na CA server přes prohlížeč webových stránek. Následují instrukce pro postoupení žádosti. Například pod Windows 2000 CA server. Vyberte Žádost o certifikát. Vyberte Progresivní žádost.



Vyberte Submit a certificate.....



Importujte Žádost o lokální certifikát X509 v textovém souboru. Vyberte Router (Offline request) nebo IPsec (Offline request).



Po podání žádosti vám server vydá certifikát. Vyberte certifikát Base 64 encoded a Dowload CA certificate. Nyní byste měli obdržet certifikát (soubor .cer) a uložit jej.

5.Vraťte se do routeru Vigor, přejděte na Lokální certifikát (Local Certificate). Klikněte na tlačítko IMPORT a prohlédněte si soubor k importu certifikátu (soubor .cer) do Vigoru. Po ukončení klikněte na Obnovit (Refresh) a naleznete následující okno.

Konfigurace lokálního X509 certifikátu

Jmeno	Subjekt	Stav	Zmena
Lokalni	/C=TW/O=Draytek/emailAddress...	Requesting	Zobrazit Vymazat

Zadost na lokalni X509 certifikat

```

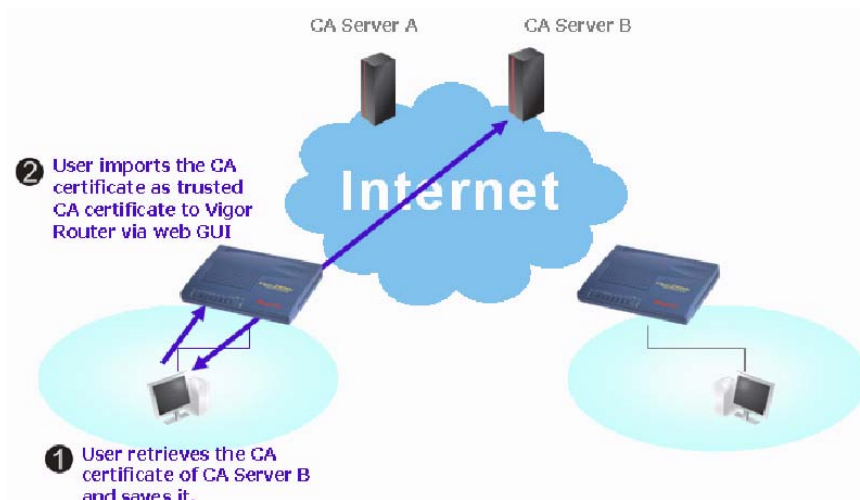
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMAQAwwQTELMakGA1UEBhMCVFcxEEDAOBgNVBAoTBORyYX10ZWsxIDAe
BgkqhkiG9w0BCQEWEEXByZXNzQGRyYX10ZWsuY29tMIGfMAOGCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQC9TawPY5xNQenXxmhjmFiPyRcVrvXXcWFFYsLAWdNs6jC4WLXY
OmzHsuXrOmmrgvRe2iPwZXYh3W18uw3JLYNqAyfILM4M8cYgkMvmFMslTDgIJnjQ
hpq8YdxoAPLixEHTEUEBp4J6mSeznyDG273gu67Wmdpyd+dip3IBLQURwIDAQAB
oCkwwYyJKozIhvcNAQkOMRowGDAWBgNVHREEdzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQCMiJpTnhHyAJZgc l uihKOWQ6jDbTQWV9v1ItHnvLhdXId7
6L14ZW6OnoFFLN2ZJz85SOHAUmpUZM10551nnIL4sG0FFZaYFdJbAOFet5vroyme
DEA3ETFxny4L/sqEfg4zWuBCpJBFOV1pdNzcAp5KU3IFHOwR92z3xWiEHVS4IQ==
-----END CERTIFICATE REQUEST-----
    
```

6. Po kliknutí na tlačítko Zobrazit (View) lze zkontrolovat detailní informace o certifikátu.

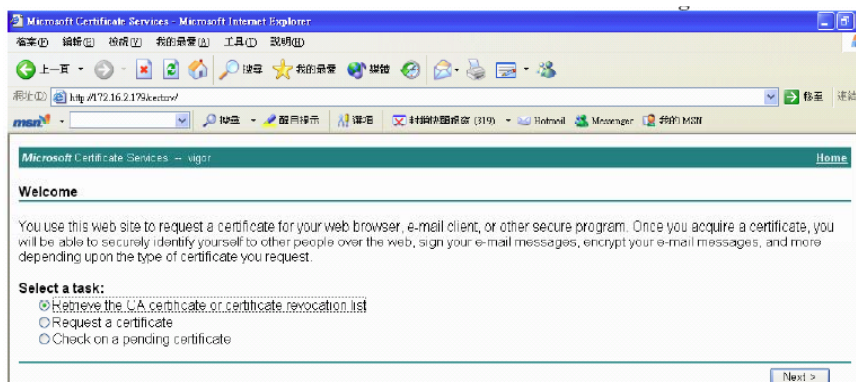
Certificate Request Information

Name :	Local
Issuer :	
Subject :	/C=TW/O=Draytek/emailAddress=press@draytek.com
Subject Alternative Name :	DNS: draytek.com
Valid From :	
Valid To :	

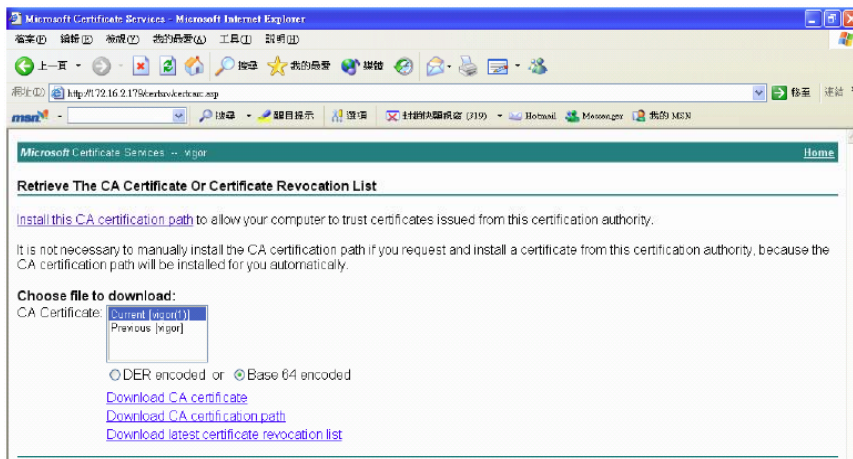
4.8 Žádost o CA certifikát a nastavení jako důvěryhodný pod Windows CA server.



1. Pokud chcete opravit CA certifikát, připojte se na CA server přes prohlížeč webových stránek. Klikněte na Retrieve the CA certificate, nebo certificate recording list.



2. Vyberte soubor pro download, klikněte CA certificate Current a Base 64 encoded a Download CA certificate k uložení souboru .cer.



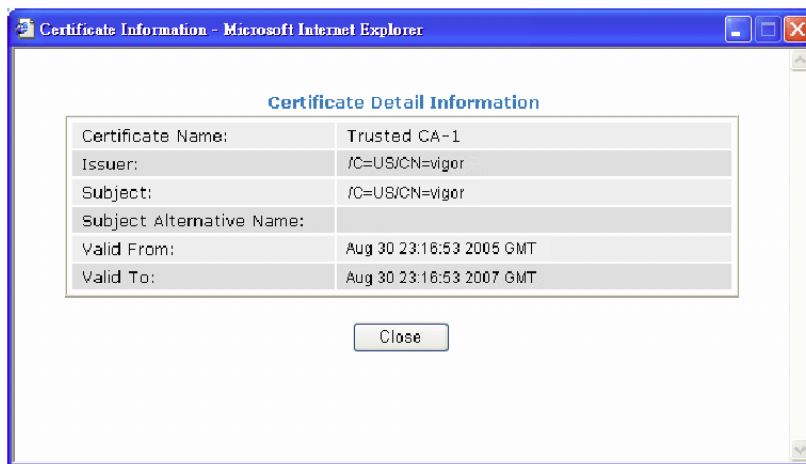
3. Vraťte se na router Vigor a přejděte na Důvěryhodný CA certifikát (Trusted CA Certificate). Klikněte na tlačítko IMPORT prohlédněte si soubor k importu certifikátu (soubor .cer) do Vigoru. Po ukončení klikněte na Obnovit (Refresh) a naleznete následující okno.

Sprava certifikátu >> Důvěryhodný CA certifikát

X509 konfigurace důvěryhodného CA certifikátu

Jmeno	Subjekt	Stav	Upravit	
Důvěryhodný CA-1	---	---	Zobrazit	Smazat
Důvěryhodný CA-2	---	---	Zobrazit	Smazat
Důvěryhodný CA-3	---	---	Zobrazit	Smazat

4. Po kliknutí na tlačítko Zobrazit (View) lze zkontrolovat detailní informace o certifikátu



Pozn.: Před konfigurací certifikátu přejděte do Údržba systému (System Maintenance) >> Čas a datum (Time and Date) a nejprve resetujte nastavený čas.

5. Řešení problémů

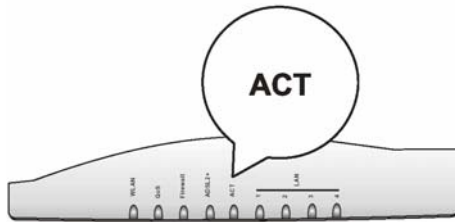
Tato kapitola vás provede situacemi, kdy se Vám po ukončení konfigurace nepodaří připojení na Internet. Při kontrole postupujte podle následujících bodů.

- Zkontrolujte, zda je provozní stav hardware v pořádku.
- Zkontrolujte, zda je stav nastavení síťového připojení v pořádku.
- Zkontrolujte z vašeho počítače router pomocí funkce Ping.
- Zkontrolujte, zda je nastavení hodnot vašeho ISP v pořádku.
- Konfigurace zařízení do výrobního nastavení.

5.1 Zkontrolujte, zda je provozní stav hardware v pořádku.

V následujících krocích prověřte stav hardware.

1. Zkontrolujte připojení napájecího adaptéru a kabelů LAN. (viz. kapitola 1.1 Instalace hardware)
2. Pokud je v pořádku, indikační LED - ACT bliká ve vteřinových intervalech a příslušná LED - LAN pro LAN port ve kterém máte připojený kabel svítí.



3. Pokud ne, zkontrolujte opět zapojení dle kapitoly 1.1.

5.2 Zkontrolujte, zda je stav nastavení síťového připojení v pořádku.

Většinou nefunkční připojení způsobuje špatné nastavení síťové konfigurace.

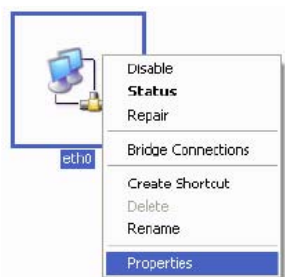
Pro Windows

Pozn.: Příklad je pro Windows XP. V případě jiných operačních systémů jsou kroky obdobné. Použijte nápovědu pro daný operační systém, nebo je najdete také na stránkách výrobce www.dratek.com.

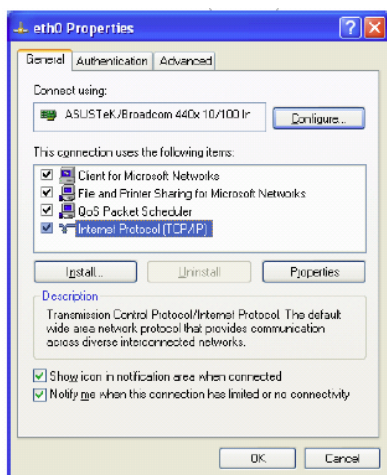
1. V menu Ovládací panely dvakrát klikněte na Síťová připojení.



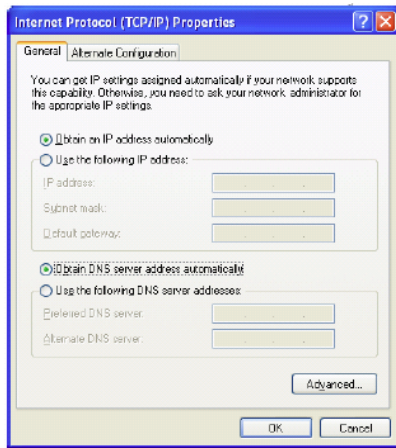
2. Právým tlačítkem myši klikněte na Místní připojení a poté na vlastnosti.



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

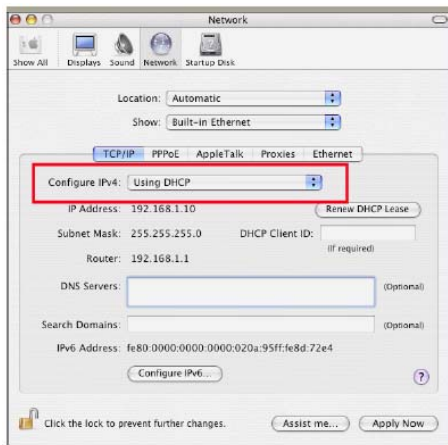


4. Zvolte možnost Získat IP adresu automaticky a Získat adresu DNS serveru automaticky.



Pro Mac OS

5. Klikněte dvakrát na MacOS na vašem monitoru.
6. Otevřete adresář Application a přejděte do Network.
7. V Network vyberte ze seznamu Using DHCP u položky Configure IPv4.

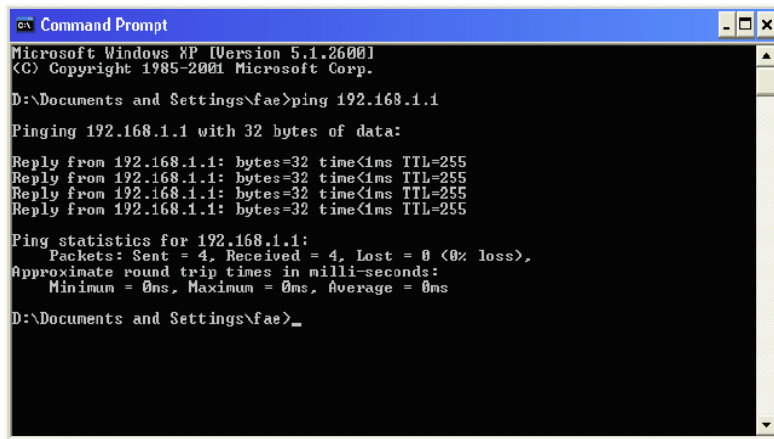


5.3 Zkontrolujte z vašeho počítače router pomocí funkce Ping.

Původní nastavená IP brána pro router je 192.168.1.1. Zkontrolujte, zda lze bez problémů provést "ping" na router.

Pro OS Windows

1. Otevřete okno příkazového řádku (z nabídky Start > Spustit).
2. Napište příkaz **Command** (pro OS Win 95/98/Me), nebo **cmd** (pro OS Win NT/2000/XP)



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\Documents and Settings\fae>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:\Documents and Settings\fae>_
```

3. Napište příkaz ping 192.168.1.1 a stiskněte Enter na klávesnici. Dojde k ověření síťového spojení. Pokud proběhla hardwarová a softwarová instalace správně, váš počítač obdrží od Vigoru odezvu, jak uvádí výše uvedené okno.
4. Pokud tomu tak není, zkontrolujte nastavení IP adresy ve vašem počítači.

Pro MacOs (Pracovní stanice)

1. Klikněte dvakrát na MacOS na vašem monitoru.
2. Otevřete adresář Application a přejděte do Utilities.
3. Klikněte dvakrát na Terminal. Otevře se okno terminalu (pracovní stanice).
4. Napište ping 192.168.1.1 a stiskněte (potvrďte). Pokud je linka v pořádku obdrží počítač odezvu.

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```


5.4 Zkontrolujte, zda je nastavení hodnot vašeho ISP v pořádku.

Přístup do internetu

- PPPoE / PPPoA
- MPoA (RFC 1483/2684)
- Multi-PVC

Pro uživatele PPPoE/ PPPoA

1. Zkontrolujte, zda je zaškrtnuto pole Zapnuto (Enable).
2. Zkontrolujte vyplněná pole Uživatelské jméno a heslo (Username and Password) podle hodnot, které jste obdrželi od vašeho ISP.

Přístup k internetu >> PPPoE / PPPoA

PPPoE / PPPoA klient mod

PPPoE/PPPoA klient Zapnuto Vypnuto

Nastavení DSL modemu

Multi-PVC kanal: Channel 1

VPI: 8

VCI: 48

Typ zapouzdření: VC MUX

Protokol: PPPoE

Modulace: G.DMT

PPPoE Pass-through

Pro drát. LAN

Pro bezdrát. LAN

Nastavení přístupu k ISP

Jmeno ISP:

Uzivatelске jmeno: 251811639

Heslo:

PPP overovani: PAP nebo CHAP

Vždy zapnuto

Odpojeni pri necinnosti: -1 vterin

IP adresa od ISP WAN IP alias

Pevna IP Ano Ne (Dynamicka IP)

Pevna IP adresa:

* : Vyzadovano nekterymi ISP

Standardni MAC adresa

Specifikovat MAC adresu

MAC adresa : 00 . 50 . 7F ; DB . 9A . E1

Index(1-15) v [Plan](#) nastaveni:

, , ,

OK

Pro uživatele MpoA

1. Zkontrolujte, zda je zaškrtnuto pole Enable pokud je vybrán přístup broadband.

Přístup k internetu >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Mod

<p>MPoA (RFC1483/2684) <input type="radio"/> Zap. <input checked="" type="radio"/> Vyp.</p> <p>Nastavení DSL modemu</p> <p>Multi-PVC kanal <input type="text" value="Channel 2"/></p> <p>Zapouzdření <input type="text" value="1483 Bridged IP LLC"/></p> <p>VPI <input type="text" value="8"/></p> <p>VCI <input type="text" value="49"/></p> <p>Modulace <input type="text" value="Multimode"/></p> <p>RIP protokol</p> <p><input type="checkbox"/> Aktivovat RIP</p> <p>Bridge mod</p> <p><input type="checkbox"/> Zapnout Bridge mod</p>	<p>Nastavení WAN IP site</p> <p><input type="radio"/> Získat IP adresu automaticky</p> <p>Jmeno routeru <input type="text" value=""/>*</p> <p>Jmeno domeny <input type="text" value=""/>*</p> <p><input checked="" type="radio"/> Specifikovat IP adresu <input type="button" value="WAN IP alias"/></p> <p>IP adresa <input type="text" value="192.168.1.100"/></p> <p>Maska podsítě <input type="text" value="255.255.255.0"/></p> <p>IP adresa brány <input type="text" value="192.168.1.1"/></p> <p>* : Pozadovano nekterymi ISP</p> <p><input checked="" type="radio"/> Standardni MAC adresa</p> <p><input type="radio"/> Specifikovat MAC adresu</p> <p>MAC adresa : <input type="text" value="00"/> . <input type="text" value="50"/> . <input type="text" value="7F"/> . <input type="text" value="DB"/> . <input type="text" value="9A"/> . <input type="text" value="E1"/></p> <p>IP adresa DNS serveru</p> <p>Primarni IP adresa <input type="text" value=""/></p> <p>Sekundarni IP adresa <input type="text" value=""/></p>
--	---

2. Zkontrolujte, zda jsou vyplněna všechna pole parametry oddílu Nastavení DSL modemu (DSL Modem Settings) správnými hodnotami v souladu s vaším ISP. Zvláště zkontrolujte výběr Zapouzdření (Encapsulation). (musí být stejná jako v nastavení Quick Start Wizard)
3. Zkontrolujte, zda IP adresa, maska podsítě a brány jsou správné (musí být identické s hodnotami od vašeho ISP).

5.5 Konfigurace zařízení do výrobního nastavení.

Pokud předcházející, nebo některé dílčí kroky nevedly k úspěchu, doporučujeme provést reset zařízení do základního firemního nastavení.

Pozn.:

Pozor, pokud provedete nastavení Factory default, všechna vaše uživatelská nastavení budou vymazána. Doporučujeme pro uživatelské nastavení profilu uložit do zálohy.

Softwarový reset

V hlavním menu v položce Údržba systému (System Maintenance) klikněte na položku Restart systému (Reboot systém).

[Udržba systému >> Restart systému](#)

Restart systému

Opravdu restartovat router ?

Použít aktuální nastavení

Použít výrobní nastavení

OK

Zaškrtněte položku Použít výrobní nastavení (Using factory default configuration) a stikněte tlačítko OK.

Po několika vteřinách se router vyresetuje a nastaví do výrobního nastavení.

Hardwarový reset

Pokud se nepodaří přes počítač otevřít konfigurační okna, lze provést tzv. hardwarový reset.



Stlačte tlačítko a přidržte minimálně 5 vteřin při zapnutém směrovači (LED ACT bliká). Až LED ACT začne blikat rychleji, tlačítko pusťte. Router se restartuje a obnoví se jeho výrobní nastavení.

6. Prohlášení o shodě



Declaration of Conformity

We DrayTek Corp. , office at No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C., declare under our sole responsibility that the product:

- Product name : ADSL 2+ Router
- Model number : Vigor 2700

Produced by:

- Company Name : DrayTek Corp.
- Company Address: No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue date
EMC	Telecommunication Network Equipment	EN 300 386 V1.6.1	2004-11
	Common technical requirements	EN 301 489-1 V1.5.1	2003-12
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 1999/5/EEC

TheTCF-File is located at:

- Company Name : VigorKom GmbH
- Company Address : Pettenkofenstr. 15-17, D-68169 Mannheim, Germany

Hsinchu 4th May, 2006
(place) (date)

Calvin Ma
Calvin Ma / President
(Legal Signature)



Declaration of Conformity

We DrayTek Corp. , office at No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C., declare under our sole responsibility that the product:

- Product name : ADSL 2+ Wireless Router
- Model number : Vigor 2700G

Produced by:

- Company Name : DrayTek Corp.
- Company Address: No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue date
EMC	Telecommunication Network Equipment	EN 300 386 V1.6.1	2004-11
	Specific conditions for 2.4GHz wideband transmission systems and 5GHz high performance WLAN equipment	EN 301 489-17 V1.2.1	2002-08
	Common technical requirements	EN 301 489-1 V1.5.1	2003-12
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 1999/5/EEC

TheTCF-File is located at:

- Company Name : VigorKom GmbH
- Company Address : Pettenkoferstr. 15-17, D-68169 Mannheim, Germany

Hsinchu 4th May, 2006
(place) (date)

Calvin Ma
Calvin Ma / President
(Legal Signature)



Declaration of Conformity

We DrayTek Corp., office at No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan, R.O.C., declare under our sole responsibility that the product:

- Product name : ADSL 2+ VoIP Router
- Model number : Vigor 2700V

Produced by:

- Company Name : DrayTek Corp.
- Company Address: No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan, R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue date
EMC	Telecommunication Network Equipment	EN 300 386 V1.6.1	2004-11
	Common technical requirements	EN 301 489-1 V1.5.1	2003-12
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 1999/5/EEC

The TCF-File is located at:

- Company Name : VigorKom GmbH
- Company Address : Pettenkoferstr. 15-17, D-68169 Mannheim, Germany

Hsinchu 4th May, 2006
(place) (date)

Calvin Ma
Calvin Ma / President
(Legal Signature)



Declaration of Conformity

We DrayTek Corp. , office at No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C., declare under our sole responsibility that the product:

- Product name : ADSL 2+ VoIP / Wireless Router
- Model number : Vigor 2700VG

Produced by:

- Company Name : DrayTek Corp.
- Company Address: No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue date
EMC	Telecommunication Network Equipment	EN 300 386 V1.6.1	2004-11
	Specific conditions for 2.4GHz wideband transmission systems and 5GHz high performance RLAN equipment	EN 301 489-17 V1.2.1	2002-08
	Common technical requirements	EN 301 489-1 V1.5.1	2003-12
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 1999/5/EEC

TheTCF-File is located at:

- Company Name : VigorKom GmbH
- Company Address : Pettenkoferstr. 15-17, D-68169 Mannheim, Germany

Hsinchu 4th May, 2006
(place) (date)

Calvin Ma
Calvin Ma / President
(Legal Signature)



Declaration of Conformity

We DrayTek Corp. office at No 26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 303, Taiwan, R.O.C., declare under our sole responsibility that the product:

* Product Name : ADSL2/2+ Firewall Router with 4-port 10/100M Base TX switch

* Model Number : Vigor2700e

Produced by

* Company Name : DrayTek Corp.

* Company Address : No 26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 303, Taiwan, R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue Date
EMC	Telecommunication network equipment	EN 300 386 V1.3.2	2003
	Current Harmonic	EN 61000-3-2 Class A	2000
	Voltage Fluctuation and Flicker	EN 61000-3-3	1995+A1:2001
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 93/68/EEC - 73/23/EEC.

The TCF-File is located at:

* Company Name : VigorKom GmbH

* Company Address : Pettenkofer Str. 15-17, 68619 Mannheim Germany

HsinChu
(Place)

1 March, 2006
(Date)

Calvin Ma
Calvin Ma / President
(Legal Signature)



Declaration of Conformity

We DrayTek Corp. office at No 26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 303, Taiwan, R.O.C., declare under our sole responsibility that the product:

- * Product Name : ADSL2/2+ Firewall Router with 4-port 10/100M Base TX switch, 802.11g WLAN
- * Model Number : Vigor2700Ge

Produced by

- * Company Name : DrayTek Corp.
- * Company Address : No 26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 303, Taiwan, R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard Issue Date
EMC	Telecommunication network equipment	EN 300 386 V1.3.2	2003
	Current Harmonic	EN 61000-3-2 Class A	2000
	Voltage Fluctuation and Flicker	EN 61000-3-3	1995+A1:2001
	RF Standard (For Wireless Interface)	EN 300 328 V1.4.1	2003
		EN 301 489-1 V1.4.1	2002
		EN 301 489-17 V1.2.1	2002
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 99/5/EEC 、 93/68/EEC 、 73/23/EEC.

The TCF-File is located at:

- * Company Name : VigorKom GmbH
- * Company Address : Pettenkofer Str. 15-17, 68619 Mannheim Germany

HsinChu
(Place)

1 March, 2006
(Date)

Calvin Ma
Calvin Ma / President
(Legal Signature)