DRAYTEK Vigor 2600 VGST

(Verzia 1.3S)

Úvod

Táto inštalačná príručka pre rýchlu inštaláciu Vigor2600VGST je určená pre užívateľov DrayTek Vigor2600VGST. Informácie v tejto príručke boli dôsledne skontrolované, avšak pri zistení nezrovnalosti s postupom pri inštalácii Vás prosíme o zaslanie informácii na adresu **attel@attel.sk.** Najnovšie informácie o produktoch a najnovších funkciách nájdete na adrese: **www.draytek.sk**

Revízia

Ver.2.5.7_ST, September 2005, ver. Fw2.5.7_ST

Autorské práva

Slovenská verzia: ATTEL s.r.o (22.9.2005)

Obchodné značky

Microsoft je registrovaná obchodná značka Microsoft Corp. Windows, Windows 95, Windows 98 a Windows NT, Windows XP sú obchodné značky Microsoft Corp. Ostatné obchodné značky a registrované značky produktov uvádzaných v tejto príručke sú vlastníctvom príslušných vlastníkov.

Bezpečnostné informácie

- Prosím pred tým než začnete nastavovať router prečítajte si dôkladne túto príručku.
- Router môže byť použitý iba s ADSL linkou
- Router je zložité elektronické zriadenie, ktoré môže byť opravované iba autorizovaným servisom (ATTEL s.r.o.). Nesnažte sa otvárať a sami opravovať router.
- Neumiestňujte router do vlhkého prostredia ako napr. kúpeľňa
- Router môže byť používaný v krytom prostredí v rozsahu teplôt od +5 až +40 stupňov Celzia.
- Nevystavujte router priamemu slnečnému žiareniu alebo iným tepelný zdrojom. Kryt a elektronické súčasti môžu byť poškodené priamym slnečným žiarením alebo pôsobením iných tepelných zdrojov
- Vyhýbajte sa tomu aby sa dostalo balenie od routra do rúk deťom
- Ak budete router vyhadzovať, prosím dodržujte pravidlá ochrany životného prostredia

Obsah balíka

Vaše balenie routra série Vigor2600VGST by malo obsahovať nasledovné položky:

- 1 x Rýchla príručka,
- 1 x CD-ROM : obsahuje užívateľskú príručku v elektronickej forme , posledný dostupný firmware a utility,
- 1 x ADSL kábel RJ45 – RJ11,
- 1 x AC/AC adaptér (čierny), vstup AC100-230V , výstup AC 12V/1,5A ,
- 1 x Ethernet UTP LAN kábel (modrý) na spojenie s PC alebo HUBom,
- 2 x anténa.

Ak hociktorá z doleuvedených súčastí chýba prosím kontaktujte Vášho distributéra

DrayTek produktov, alebo priamo ATTEL, s.r.o. .

1.1 LED ukazovatele a zadný panel

LED ukazovatele

Na prednom panely je umiestnených 11 LED diód ACT, QoS, FXS1 a FXS2, WL, LINE, PRINTER, P1, P2, P3, P4.

ACT (Activity)

Bliká ak je router napájaný zo zdroja a je normálne funkčný

Skupina PHONE (FXS1 a FXS2):

Jednotlivé kontrolky FXS portov svietia podľa toho, či sa porty používajú

WL

Svieti ak je úspešné aktivované WLAN

LINE

Svieti ak je modem pripojený k DSLAM, bliká ak sa pokúša pripojiť k DSLAM providera

PRINTER

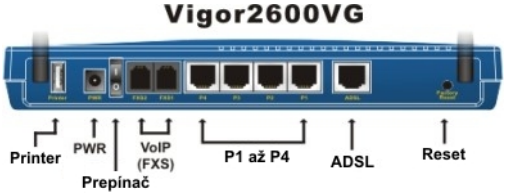
Svieti ak je pripojená tlačiarne. Bliká ak pretekajú dáta do tlačiarne

Skupina LAN:

P1 až P4

Svieti oranžovo ak je pripojené sieťové zariadenie 10BaseT, a na zeleno ak je 100BaseT, ak bliká tak sú prenášané pakety na danom porte.

Popis zadného panela



Vigor2600VGST má na zadnom panely reset tlačidlo (Factory Reset), konektor na napájanie (PWR), prepínač napájania (0 – vypnuté, 1 - zapnuté), ADSL RJ45 konektor pre pripojenie ADSL linky, štyri RJ-45 LAN 10/100BaseT porty, dva RJ-11 konektory pre pripojenie koncových analógových telefónov (FXS), jeden USB-female konektor pre pripojenie tlačiarne a dva SMA - Female konektory pre pripojenie Wi-Fi antén.

PWR

Iba adaptér DrayTek 12VAC 1,5A môže byť zapojený to konektora pre napájanie

Printer

Pre pripojenie USB tlačiarne do vstavaného LPR print servera.

Podporuje operačné systémy WIN 95/98/98SE/ME, a je kompatibilný so systémami Windows 2000/XP/Server2003/Mac OS 9/Mac OS X, ktoré obsahujú ovládače pre LPR print server.

Reset

Pre aktualizáciu firmvéru: stlačiť a držať stlačené tlačítko a potom zapnúť napájanie. ACT a LNK LED budú naraz blikať.

Pre výrobné nastavenie: Pokiaľ zariadenie je zapnuté, stlačiť tlačítko a držať ho stlačené viac ako 5 sekúnd. Ak ACT LED začne blikať rýchlejšie pustiť Reset tlačítko. Router sa reštartuje do výrobného nastavenia.

1.2 Kľúčové vlastnosti

Router Vigor2600VGST je ADSL router určený k pripojeniu Vašej lokálnej siete k internetu rýchlosťou až 8Mb/s pomocou 4 LAN portov 10/100BaseT a zároveň pomocou bezdrôtového pripojenia s prenosovou rýchlosťou 54 Mb/s podľa štandardu IEEE 802.11b/g, čiže slúži ako prístupový bod pre zdieľanie pripojenia na internet pre klientske počítače komunikujúce pomocou bezdrôtových sieťových kariet.

Podporuje aj množstvo ďalších funkcií potrebných pre zvýšenie bezpečnosti, prenos hlasu(VoIP), vzdialený prístup(RAS), multimediálnu podporu a vytváranie virtuálnych privátnych sietí cez internet(VPN) v jednom kompaktnom zariadení vrátane možnosti pripojenia zdieľanej tlačiarne(LPR Print Srver).

Router má vstavaný DHCP server, firewall, ochranu proti útokom z internetu, kryptovaný prenos cez WIFI, prekladanie adries, dokáže vytvárať virtuálne privátne siete a to simultánne 16 VPN tunelov.

Router Vigor2600VGST umožňuje veľa vstavaných serverových a softwarových funkcií.

1. Network Address Translation (NAT) – umožňuje viacerým používateľom pripojiť sa k ISP poskytovateľovi požitím jedného internetového konta
2. Firmware Upgrade (TFTP) Server: Za pomoci softvéru Firmware Upgrade Utility môžete ľahko upgradovať firmware routra na aktuálnu verziu.
3. Web (HTTP) Server: Web prehliadač je najpoužívanejší softvér k surfovaniu po internete a pomocou neho môžete jednoducho nakonfigurovať router.
4. Remote Access Server (RAS): poskytuje vzdialený dial-in prístup do LAN siete pre prácu z domu, alebo z pobočky. Routre Vigor2600VGST majú podporu pre 10 užívateľských dial-in profilov, vrátane autentifikačného mechanizmu pomocou CHAP/PAP metódy a CLID, bezpečnú funkciu spätného volania a 16 LAN-to-LAN užívateľských profilov.
5. Routing Information Protocol (RIP) Support: využíva sa pri LAN-to-LAN aplikáciách. RIP protokol vymieňa routovacie informácie medzi routrami
6. Domain Name Server (DNS) Proxy: DNS proxy uchováva DNS cache, vrátane mapovacej tabuľky doménových mien a IP adries. Proxy si taktiež pamätá DNS požiadavky paketov posielaných cez router a ukladá si ich do vlastnej DNS

cache. Pre zrýchlenie prístupu, keď príde požiadavka paketu o DNS proxy sa ju najprv snaží nájsť vo vlastnej DNS cache a ak sa tam nenachádza tak až potom vysiela požiadavku pre WAN DNS server.

7. Telnet Terminal Server: Telnet ako užívateľské rozhranie je efektívny spôsob ako konfigurovať a riadiť router. Pracuje v rozhraní bežného príkazového riadku a je určený pre podrobnú konfiguráciu a riadenie routra, ako aj vzdialených routrov.
8. Dynamic Host Configuration Protocol (DHCP) Klient na WAN porte: router podporuje DHCP klienta na WAN porte. Tento klient automaticky dostane nastavenie IP adresy, masky podsiete, hlavného prístupového servera.
9. Dynamic Host Configuration Protocol (DHCP) Server: Server poskytuje ľahko konfigurovateľné funkcie pre vašu lokálnu IP sieť. Dokáže automaticky priradiť IP sieťovú konfiguráciu per lokálne PC, ako napr. IP adresu, masku podsiete, IP adresy brány, Domain name server, atd.
10. Built-in Flash ROM: udržiava si uložený firmware a konfiguráciu ak dôjde k výpadky napájania.
11. Point-to-Point Protocol over Ethernet (PPPoE) Client Support: Ak ste ADSL používateľom tak router má podporu vstavaného ADSL klienta, pre spojenie ADSL linky s poskytovateľom pripojenia. Nie je potrebné inštalovať ďalší softvér.
12. Firewall: oproti zabudovanému NAT mechanizmu router podporuje iný silný ochranný mechanizmus, na ochránenie vašej lokálnej siete. Takisto môže zabrániť užívateľom LAN v prístupe k nepovoleným službám.
13. Remote Management: Systémový správca môže na diaľku nastavovať a ovládať router pomocou ADSL vzdialeného prístupu alebo aj DSL WAN rozhrania.
14. Wireless LAN Access Point: umožňuje väčšiu voľnosť viacerým užívateľom pripojených pomocou bezdrôtového pripojenia presne tak ako keby boli pripojený káblom.
15. Wired Equivalent Privacy (WEP): Bezdrôtové terminály, ktoré disponujú správnym bezpečnostný kľúčom môžu pristupovať do siete.
16. Virtual Private Network (VPN) s IPSec kryptovaním: Aktivuje pripojenie vzdialenej siete a vzdialených užívateľov cez Internet pomocou autentifikovaných a kryptovaním chránených tunelov.
17. Wi-Fi Protected Access (WPA): metóda kódovania, ktorá bráni neautorizovanému prístupu na sieť pomocou nastavenia hesla (pre osobné používanie), alebo overovanie užívateľov siete cez server (pre používanie vo firme).
18. Virtual LAN (VLAN): Každý z Ethernet portov LAN je možné oddeliť od ostatných funkcií Virtuálnej lokálnej siete.
19. LPR tlačový server. Umožňuje pripojenie tlačiarne cez USB port. Podporuje Win98/98SE/ME LPR printer. Kompatibilita s OS Win2000/XP/MacOS 9/Mac OSX so vstavaným LPR printer ovládačom.

Výrobné nastavenia

Vigor2600VGST je dodávaný s nasledovnou výrobnou konfiguráciou:

Sieťové nastavenia

IP adresa:	192.168.1.1
Maska podsiete:	255.255.255.0
DHCP server	Aktivovaný
Štartovacia IP adresa:	192.168.1.10
Rozsah IP:	50

Web konfigurátor

Užívateľské meno:	admin
Heslo:	(žiadne, t.j. miesto pre zadanie hesla nechajte prázdne)

Telnet

Heslo:	(žiadne, t.j. miesto pre zadanie hesla nechajte prázdne)

Obsluha cez Internet

Nie je povolená

WIFI kryptovanie

Nenastavené

ADSL nastavenie

VPI:1

VCI:32

Zapuzdrenie: LLC/SNAP

Protokol: PPPoE

Modulácia: G.DMT

2.1 Inštalácia hardware

2.1.1 Pripojenie napájania

1. Zapojte adaptér do zásuvky v stene a do PWR konektoru na zadnom paneli routra.
2. Dióda ACT by mala blikať každé 2 sekundy

2.1.2 Pripojenie do Ethernetu

A. Pripojenie k PC

1. Zapojte ethernetový kábel do LAN1 portu alebo do hociktorého z P1 až P4 portov.
2. Opačný koniec ethernetového kábla zapojte do vašej sieťovej karty v počítači.
3. LED diódy na obidvoch koncoch, čiže aj na sieťovej karte a na routri by mali svietiť.

Poznámka: Ak ethernetový kábel nieje dostatočne dlhý, zakúpte si dlhší ethernetový kábel kategórie 5, UTP alebo STP.

2.1.3 Pripojenie k ADSL linke

1. Nájdite ADSL kábel
2. Zapojte RJ-45 konektor ADSL kábla do ADSL portu na routri
3. Opačný koniec ADSL kábla zapojte do portu Splitra

2.1.4 Pripojenie pomocou bezdrôtovej siete

Router podporuje pripojenie bezdrôtovou sieťou (WIFI) 802.11b a 802.11g

1. Zapojte WIFI kartu do Vašeho PC, nainštalujte.
2. V ovládacom programe k Vašej WIFI karte by ste mali nájsť dostupný router Vigor2600VGST s SSID: default
3. Na routri nie je od výroby nastavené žiadne kryptovanie na WIFI.

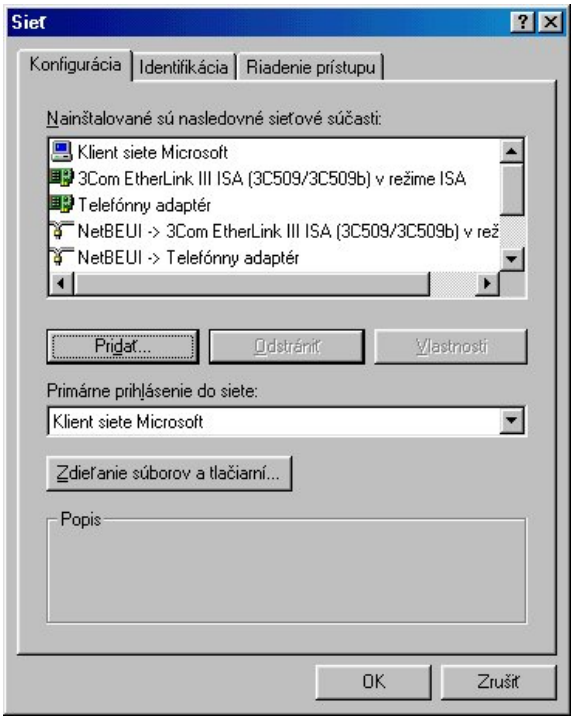
Hardwarová inštalácia je teraz kompletná. Nasledujúce časti príručky vám pomôžu nastaviť a spravovať PC a pripojenie do internetu.

2.2 Nastavenie v prostredí Windows 95/98

2.2.1 Kontrola sieťovej IP konfigurácie

1. Na pracovnej ploche nájdite ikonu "Počítače v sieti" a kliknite na ňu pravým tlačítkom myši. Z ponuky, ktorá sa následne zobrazí, zvoľte kurzorom myši položku "Vlastnosti". Po kliknutí na túto položku sa zobrazí nasledujúce okno.

Vaše systémové nastavenia sa môžu odlišovať od uvedeného príkladu. Pohybujúc posuvnou lištou skontrolujte, či má váš počítač správne nainštalovaný ovládač sieťovej karty a TCP/IP protokol. Pokiaľ tomu tak nie je, bude najprv potrebné previesť inštaláciu ovládačov vašej sieťovej karty podľa dokumentácie dodávanej jej výrobcom.

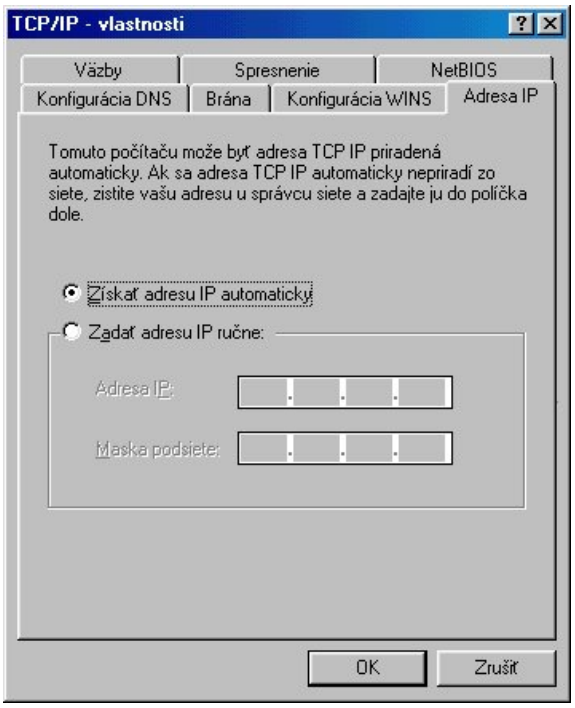


2. Potom, čo ste nainštalovali ovládače sieťovej karty, otvorte rovnakým spôsobom predošlé okno Sieť a v ňom stlačte tlačítko "Pridať". V skupine Protokol/Microsoft zvoľte TCP/IP protokol. V prípade že zvolíte pre špecifikovanú sieťovú kartu TCP/IP protokol, je potrebné reštartovať váš počítač za účelom aktualizácie systémových nastavení. Preto po zobrazení nasledujúceho okna stlačte tlačítko "Áno". Váš počítač sa reštartuje.

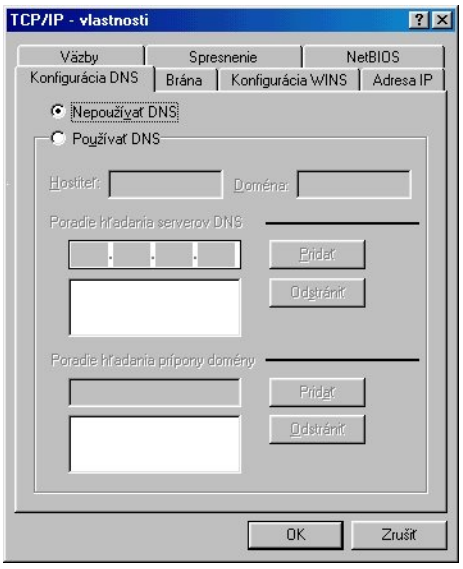
3. Za účelom správneho nakonfigurovania komunikačného protokolu TCP/IP vykonajte postupnosť nasledovných krokov.

2.2.2 Konfigurácia TCP/IP protokolu

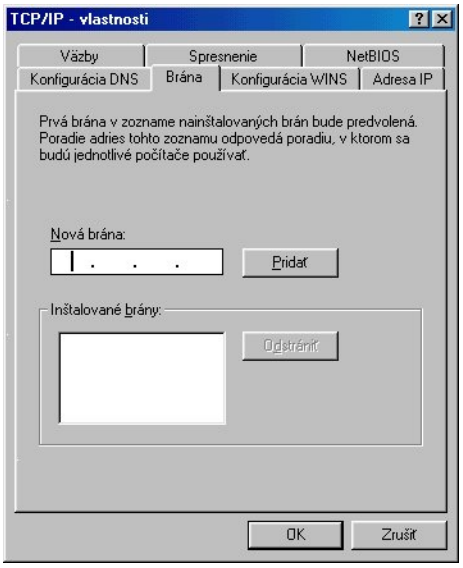
1. Zvoľte "TCP/IP" v okne Sieť a stlačte "Vlastnosti". V nasledujúcom okne môžete nastaviť ďalšie detaily.



2. Keďže Vigor2600VGST umožňuje použitie DHCP (Dynamic Host Configuration Protocol - Protokol pre dynamické prideľovanie IP adries) servera, po kliknutí na voľbu "Adresa IP" nakonfigurujte váš počítač na voľbu "Získať IP adresu automaticky", tak ako je implicitne predvolené. Pri tomto nastavení získa váš počítač IP adresu, masku podsiete či iné požadované IP sieťové nastavenia dynamicky cez Vigor2600VGST.
3. V ďalšom kroku kliknite na položku "Konfigurácia DNS" a zvoľte položku "Nepoužívať DNS" .



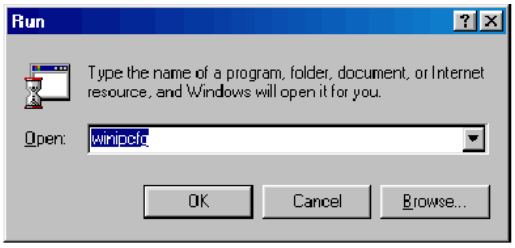
4. Kliknutím na položku "Brána" skontrolujte, či zostali textové polia pri položkách "Nová brána" a "Inštalované brány" prázdne, ako je uvedené:

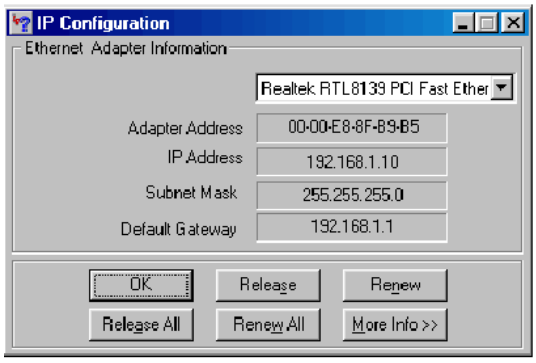


5. Po prevedení požadovaných zmien sa zobrazí nasledujúce okno. Stlačte "Áno". Systém sa reštartuje.

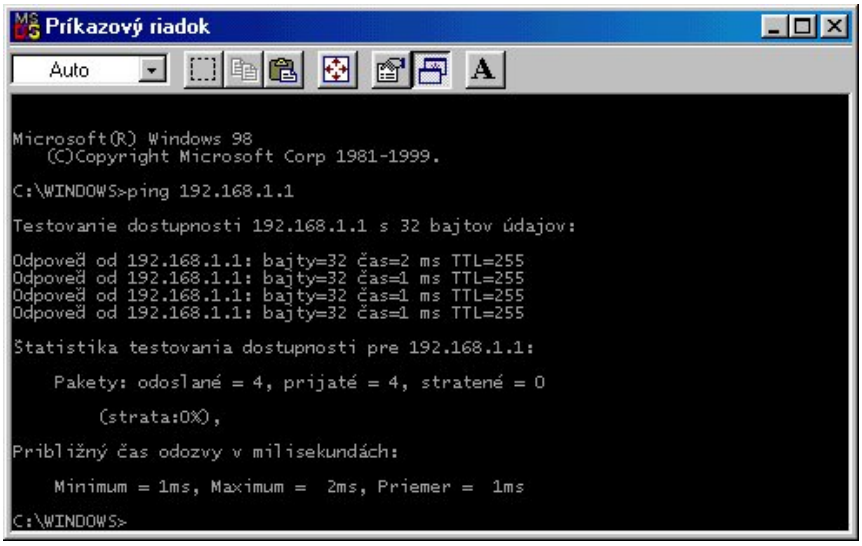
2.2.3 Kontrola nastavení TCP/IP:

1. Po splnení predchádzajúcich krokov, kliknite v ponuke START na RUN (Spusti) a do dialógového okna napíšte **winipcfg**. Otvorí sa okno IP konfigurácie. Ak počítač nezobrazí IP adresy v rozpätí **192.168.1.2** do **192.168.1.254**, kliknite na tlačidlo **Release** pre spustenie aktuálnej konfigurácie. Počkajte niekoľko sekúnd, kliknite na **Renew** a získate aktuálnu konfiguráciu z routra.





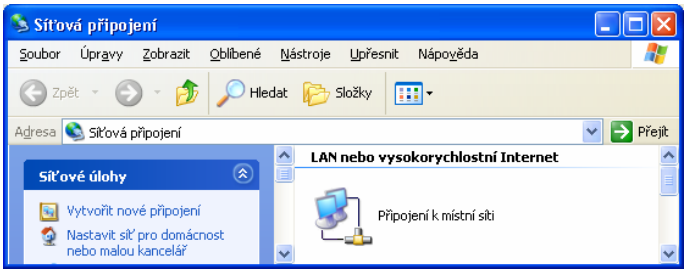
2. Ak je IP konfigurácia správna, môžete použiť diagnostický obslužný program PING, ktorý je súčasťou operačného systému Microsoft Windows, a odskúšať komunikáciu s Vigor2600VGST. "Štart" -> "Programy" -> "Príkazový riadok". Otvorí sa okno príkazového módu systému MS-DOS. Napíšte "ping 192.168.1.1" (implicitná IP adresa pre Vigor2600VGST). Dôjde k overenie sieťového spojenia. Ak prebehla hardwarová a softwarová inštalácia správne, váš počítač obdrží odozvu od Vigor2600VGST, ako uvádza nasledujúce okno. Ak nie , skontrolujte, či je správne pripojený sieťový kábel. Taktiež by ste mali vidieť rozsvietenú Ethernet port LED diódu na čelnom paneli prístroja.



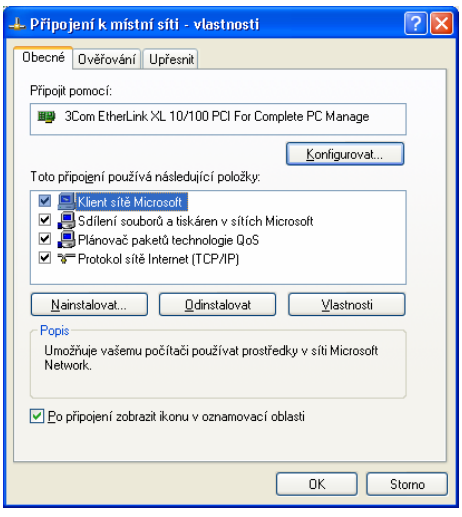
2.3 Nastavenie v prostredí Windows XP

2.3.1 Kontrola sieťovej IP konfigurácie

1. Na pracovnej ploche (príp. ovládacie panely – sieťové pripojenia) nájdite ikonu "Počítače v sieti" a kliknite na ňu pravým tlačítkom myši. Z ponuky, ktorá sa následne zobrazí, zvoľte kurzorom myši položku "Vlastnosti". Po kliknutí na túto položku sa zobrazí nasledujúce okno.



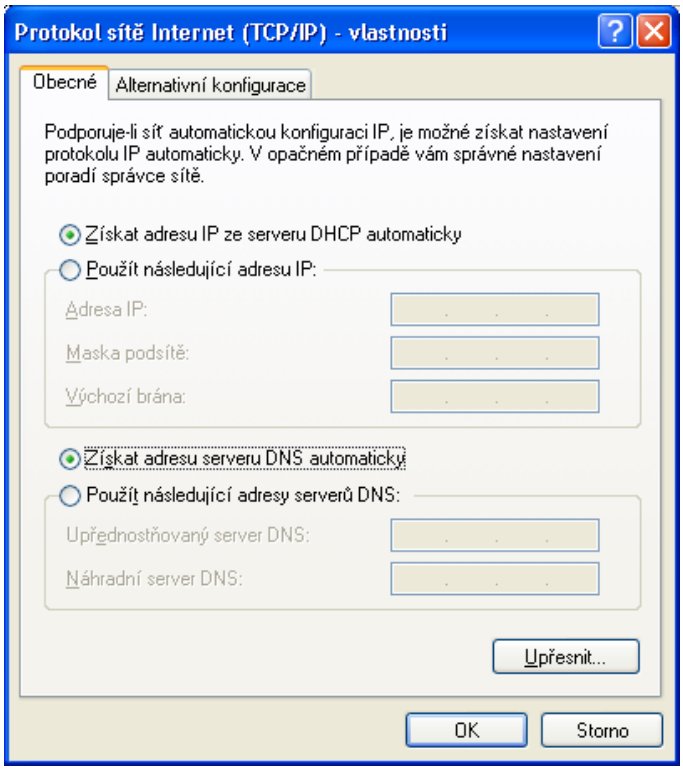
2. Kliknete znovu pravým tlačidlom na ikonu Pripojenie k miestnej sieti, zvoľte vlastnosti a zobrazí sa nasledujúce okno:



3. Vaše systémové nastavenia sa môžu odlišovať od uvedeného príkladu. Pohybujúc posuvnou lištou sa skontrolujte, či má váš počítač správne nainštalovaný ovládač sieťovej karty a TCP/IP protokol. Pokiaľ tomu tak nie je, bude najprv potrebné previesť inštaláciu ovládačov vašej sieťovej karty podľa dokumentácie dodávanej jej výrobcom.
4. Potom, čo ste nainštalovali ovládače sieťovej karty, otvorte rovnakým spôsobom predošlé okno Sieť a v ňom stlačte tlačítko "Nainstalovat". V skupine Protokol/Microsoft zvoľte TCP/IP protokol. V prípade že zvolíte pre špecifikovanú sieťovú kartu TCP/IP protokol, je potrebné reštartovať váš počítač za účelom aktualizácie systémových nastavení. Preto po zobrazení nasledujúceho okna stlačte tlačítko "Áno".
5. Za účelom správneho nakonfigurovania komunikačného protokolu TCP/IP vykonajte postupnosť nasledovných krokov.

2.3.2 Konfigurácia TCP/IP protokolu

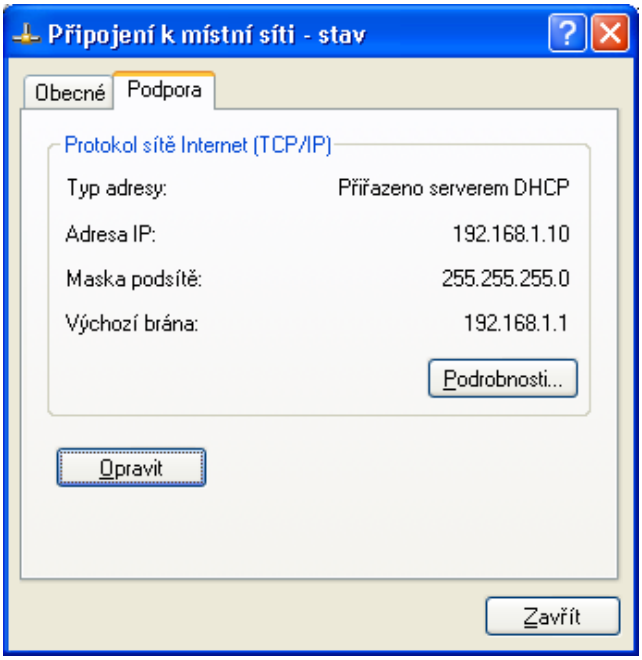
1. Zvoľte "TCP/IP" v okne Sieť a stlačte "Vlastnosti". V nasledujúcom okne môžete nastaviť ďalšie detaily.



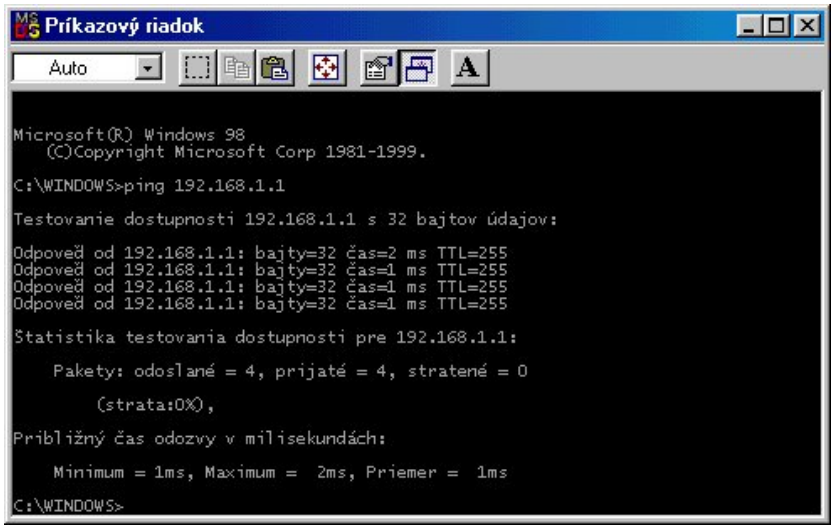
2. Keďže Vigor2600CGST umožňuje použitie DHCP (Dynamic Host Configuration Protocol - Protokol pre dynamické prideľovanie IP adries) servra, po kliknutí na voľbu "Adresa IP" nakonfigurujte váš počítač na voľbu "Získať adresu IP zo serveru DHCP automaticky", tak ako je implicitne predvolené. Pri tomto nastavení získa váš počítač IP adresu, masku podsiete či iné požadované IP sieťové nastavenia dynamicky cez Vigor2600VGST.
3. V ďalšom kroku kliknite na položku "Získať adresu serveru DNS automaticky" .

2.3.3 Kontrola nastavení TCP/IP:

1. Na pracovnej ploche nájdite ikonu "Počítače v sieti" a kliknite na ňu pravým tlačítkom myši. Z ponuky, ktorá sa následne zobrazí, zvoľte kurzorom myši položku "Vlastnosti". Po kliknutí na túto položku sa zobrazí nasledujúce okno.
2. Kliknete znovu pravým tlačidlom na ikonu Pripojenie k miestnej sieti, zvoľte stav a zložku podpora a zobrazí sa nasledujúce okno:



3. Pokiaľ je IP konfigurácia správna, môžete použiť diagnostický obslužný program PING, ktorý je súčasťou operačného systému Microsoft Windows, a odskúšať komunikáciu s Vigor2600VGST. Postupne stlačte "Štart" -> "Programy" -> "Príkazový riadok". Otvorí sa okno príkazového módu systému MS-DOS. Napíšte "ping 192.168.1.1" (implicitná IP adresa pre Vigor2600VGST). Dôjde k overenie sieťového spojenia. Pokiaľ prebehla hardwarová a softwarová inštalácia správne, váš počítač obdrží odozvu od Vigor2600VGST, ako uvádza nasledujúce okno. Pokiaľ tomu tak nie je, skontrolujte, či je správne pripojený sieťový kábel. Taktiež by ste mali vidieť rozsvietenú Ethernet port LED diódu na čelnom paneli prístroja.



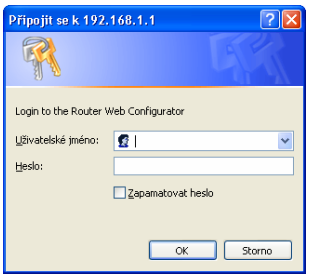
2.4 Router Tools

Inštalácia nástrojov Router Tools

1. Vložte DrayTek CD-R médium do CD-ROM mechaniky vášho počítača. Kliknite na ikonu CD-ROM a otvorte adresár Nástroje, ďalej zvolíte podadresár podľa typu vášho operačného systému (win), ďalej podadresár Router Tools a kliknete na ikonku Rtsetup.exe.
2. Spustí sa inštalácia, ktorá do vášho operačného systému nainštaluje Quick Start Wizard, Firmware Upgrade Utility a Sys Log.

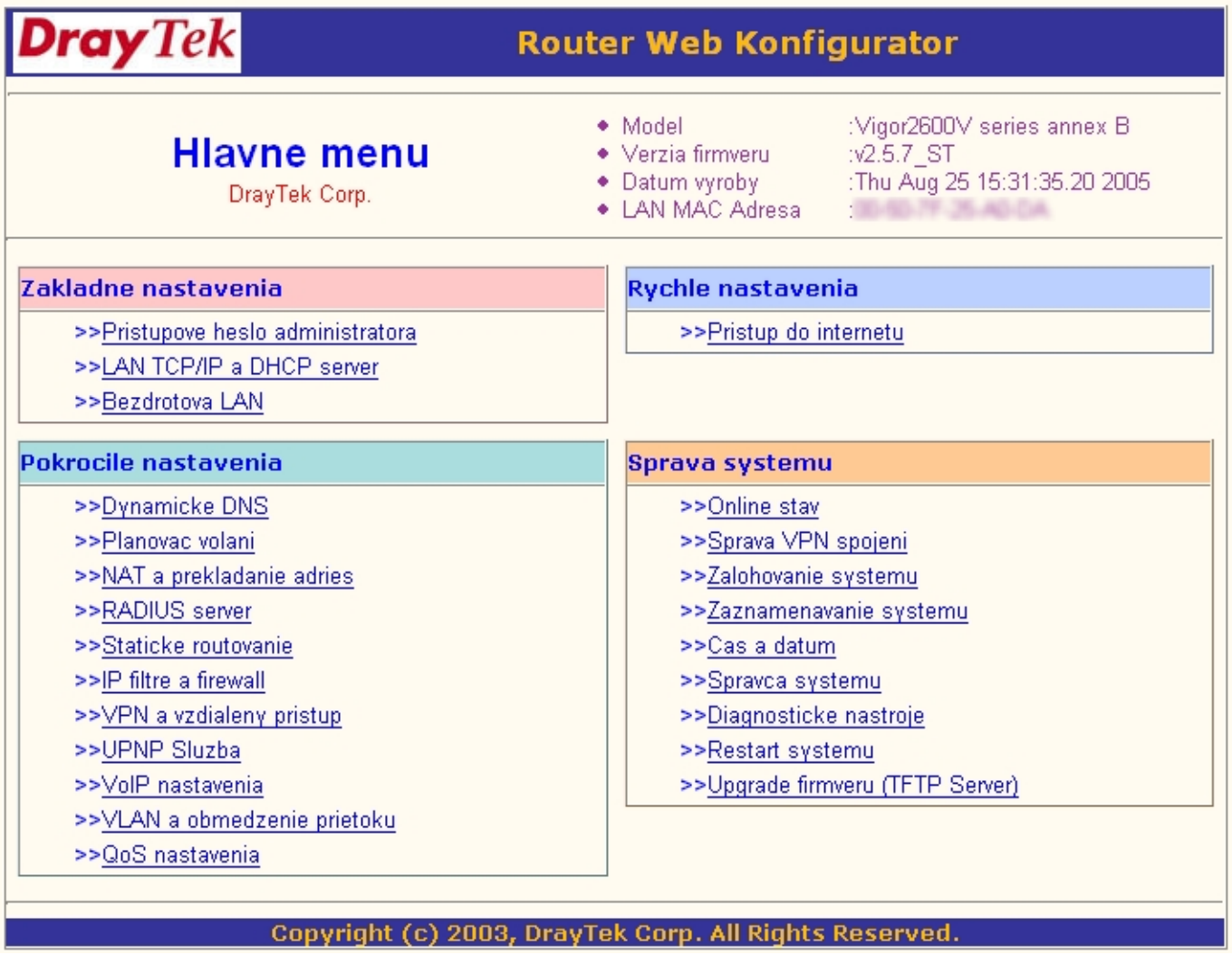
2.5 Web konfigurátor

2.5.1 Nastavenie prístupu na Internet cez Router Web Configurátor



1. Skôr než sa pripojíte na Web Configurator, objaví sa autentifikačné dialógové okno. Textové pole "Meno používateľa" nechajte nevyplnené. Napíšte heslo v textovom poli "Heslo", default nastavenie je bez hesla. V našom príklade je použitý prehliadač Microsoft ™ Internet Explorer. Ak používate prehliadač Netscape™, toto okno môže byť odlišné.

2. Po stlačení tlačítka "OK" sa zobrazí Hlavné menu.



3. Úvodné Menu obsahuje štyri užitočné položky: Model, Verzia firmvéru, Dátum/čas (Dátum a čas vydania) a MAC adresa (MAC adresa v lokálnej sieti Ethernet). V tomto príklade je verzia firmvéru v2.5.7_ST , dátum 25 august 2005 15:31. Tieto položky Vás informujú o aktuálnosti vnútorného softvérového vybavenia.

2.5.2 Prehľad funkcií WEB konfigurátora

Hlavné menu sa skladá zo štyroch základných skupín:

- Základné nastavenia,
- Rýchle nastavenia,
- Pokročilé nastavenia,
- Správa systému.

- **Základné nastavenia**
  - Prístupové heslo administrátora: Umožňuje nastaviť alebo zmeniť heslo administrátora prístupu do routra.
  - LAN TCP/IP a DHCP Server: Mení IP adresu a DHCP nastavenie routra
  - Bezdrôtová LAN: Umožňuje nastaviť bezdrôtovú sieť, kryptovanie a bezpečnosť WIFI.
- **Rýchle nastavenia**
  - Prístup do internetu: Nastavenie pripojenia na internet (poskytne poskytovateľ internetu)
- **Pokročilé nastavenia**

Tieto nastavenia slúžia iba pre rozšírenú správu. Tieto položky nie je treba konfigurovať pre bežné pripojenie na internet.

  - Dynamické DNS: Umožňuje povoliť a aktivovať Dynamický DNS účet
  - Plánovač volaní: Nastavenie obmedzení pomocou časových pásiem.
  - NAT a prekladanie adries: Nastavenie NAT, Presmerovanie portov, DMZ a otvorenie skupiny portov.
  - RADIUS server: Nastavenie overovania prístupu vzdialeného užívateľa do siete.
  - Statické routovanie: Umožní nastaviť 10 pravidiel routovania pre statické routovanie. Je tu možnosť pridať, odobrať, aktivovať a deaktivovať statické routovanie
  - IP Filtre a firewall: Router má zabudovaný silný firewall, dokáže nastaviť až 84 volacích a dátových filtrov, Obsahové filtrovanie URL, DoS.
  - VPN and vzdialený prístup: Umožňuje nastavenie max. 16 VPN tunelov a aktivovanie volacích účtov atď.
  - UPnP služba: Umožňuje spoluprácu so softvérom, ktorý podporuje túto funkciu.
  - VoIP nastavenia: Router umožňuje nastavenie dvoch FXS portov, telefónneho zoznamu, zvonenia a atď.
  - VLAN a obmedzenia prietoku: umožňuje vytvoriť skupiny VLAN portov a na každý port aktivovať limitovanie prietoku.
  - QoS nastavenia: nastavenie garancie včasného a bezpečného doručenia paketov cez sieť.
- **Správca systému**
  - Online stav: Kliknutím na túto položku môžete vidieť aktuálny stav a štatistiky routra
  - Sprava VPN spojení: Možnosť manuálneho aktivovania VPN tunela, a zobrazenie informácií o vytvorenom VPN spojení
  - Zálohovanie nastavenia: Možnosť zálohovania a obnovenia zálohy nastavenia routra. Ukladá sa formou súboru na HDD.
  - Zaznamenávanie systému: Nastavenie sprístupnenia zaznamenávania systému a Upozornenie pomocou e-mailu
  - Čas a dátum: Nastavenie času
  - Správca systému: Nastavenie limitovaného počtu užívateľov, ktorí môžu spravovať router, povolenie vzdialeného prístupu do routra
  - Diagnostické nástroje: Nástroje pre diagnostiku routra a siete, ako napr. ARP tabuľka, routovacia tabuľka, mapovanie NAT portov, stav DHCP servera atd.
  - Reštart systému: Umožňuje reštartovať router s výrobným nastavením, alebo s aktuálnym nastavením
  - Upgrade Firmvéru: Aktivuje TFTP server pre upgrade firmwaru.

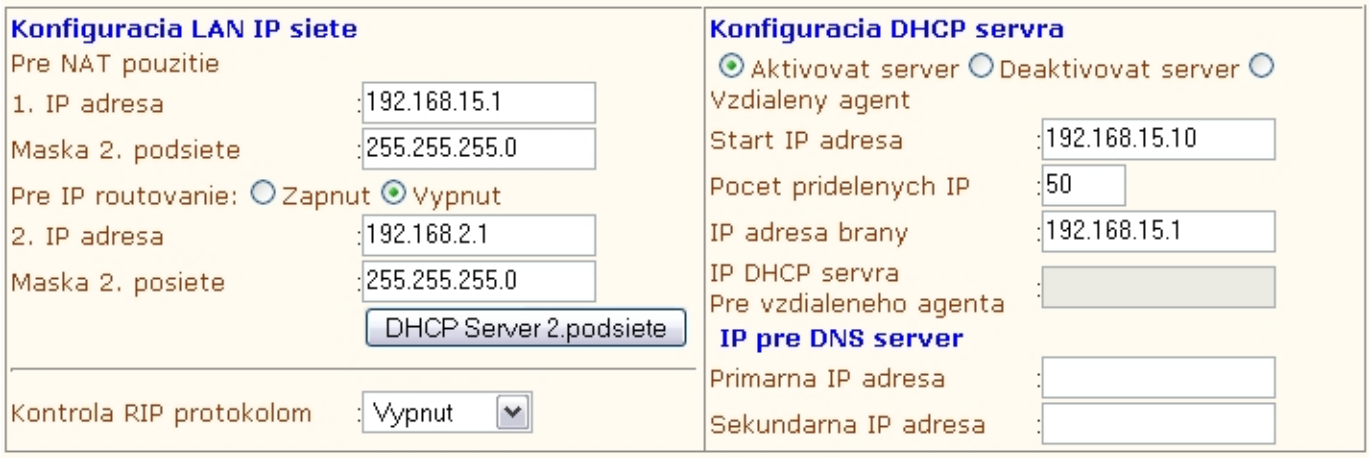
3.1 Prístupové heslo administrátora

Skôr než budete môcť nastaviť rôzne druhy prístupu, musíte prejsť nastavením Základné nastavenia. Po kliknutí na položku Prístupové heslo sa zobrazí nasledujúce dialógové okno.

- **Staré heslo**: Ak nastavujete router po prvýkrát, nechajte toto textové pole nevyplnené, keďže router nemá prednastavené žiadne heslo.
- **Nové heslo**: Napíšte nové heslo administrátora obsahujúce menej než 16 znakov.
- **Znovu nové heslo**: Potvrďte zadané heslo jeho opätovným prepísaním v uvedenom textovom poli.

3.2 LAN TCP/IP and DHCP Server

Router obsahuje dve nezávisle LAN rozhrania. Tieto IP adresy majú určité obmedzenie pre rozličné sieťové aplikácie. Ak chcete používať router len pre jednoduché IP zdieľanie alebo ako NAT router (štandardné pripojenie k Internetu), použite iba prvú IP adresu, druhá IP adresa je pre verejných užívateľov.



Konfigurácia LAN IP siete:

For NAT Usage (Pre NAT)

- **1.IP Adresa**: Prvá IP adresa je len pre použitie NAT. To znamená, že podsieť môže byť smerovaná cez NAT na ADSL rozhranie alebo iný router pripojený na ethernetovské rozhranie.
- **Maska 1 podsiete**: maska podsiete pre privátnu sieť

For IP Routing Usage (Pre IP Routing)

- **Zapnut**: aktivuje použitie IP smerovania
- **Vypnut**: deaktivuje použitie IP smerovania
- **2. IP adresa:** Druhá IP adresa je použitá pre IP smerovanie. To znamená, že podsieť nebude schovávaná za NAT, ale bude priamo routovaná (pri zakúpení skupiny IP od ISP). Pri tomto nastavení sa vyžaduje statický routing u providera. Táto položka je voliteľná.

- **Maska 2 podsiete**: maska podsiete pre verejnú IP adresu

Konfigurácia DHCP servra:

- **Zapnutý**: Prepnutím prepínača na voľbu "Zapnut" umožníte použitie DHCP servera.
- **Vypnutý:** Voľba "Disable" použitie DHCP servera znemožňuje
- **Služba Relay Agent:** klient na wan porte**:** Používa sa ak je v sieti iný router ktorý poskytuje DHCP, označením voľby sa deaktivuje DHCP a určí sa IP adresa kde je iný DHCP
- **Štart IP adresa**: Štandardne disponuje DHCP server fondom IP adries na vybavovanie jednotlivých DHCP klientov. Táto položka určuje počiatočnú IP adresu z intervalu adries, ktorými DHCP server disponuje. Počiatočná IP adresa môže byť zvolená buď z podsiete 1 alebo z podsiete 2.
- **IP Pool count (Počet pridelených IP)**: Toto číslo definuje množstvo IP adries, ktoré možno prideliť DHCP klientom (maximálny počet DHCP klientov).
- **IP adresa brány**: Ak router nie je default bránou v sieti, máte možnosť definovať túto položku.
- **IP adresa DHCP servera pre službu Relay Agent:** IP adresa pre Relay Agent

IP adresa pre DNS server:

Dve nasledujúce IP adresy by mali byť oznámené každému DHCP klientovi. Odporúča sa použiť DNS server vášho poskytovateľa alebo DNS server ním odporúčaný. Ušetríte tým čas routra potrebný na vybavenie žiadostí o názov domény odoslaných z interných počítačov. Ak necháte obidve položky textových polí nevyplnené, router poskytne DHCP klientom IP adresu routra, pričom bude fungovať ako DNS proxy server.

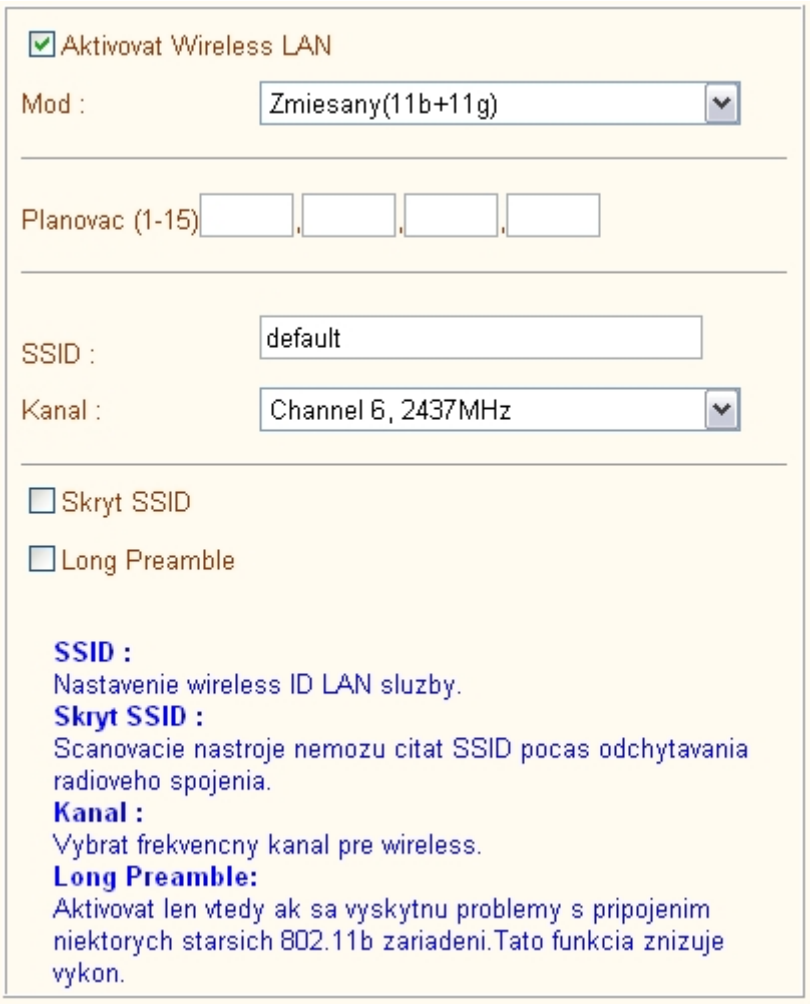
- **Primárna IP adresa**: IP adresa primárneho DNS servera.
- **Sekundárna IP adresa**: IP adresa sekundárneho DNS servera.

3.3 Wireless LAN

Vigor je vybavený bezdrôtový (WIFI) rozhraním wireless LAN s protokolom 11MBit/s IEEE 802.11b a 54 Mbit/s IEEE 802.11g. Wireless LAN poskytuje vysoký stupeň mobility, prístup viacerých užívateľov k službám siete LAN, ako napr. Internet, alebo WAN prístup.

3.3.1 Hlavné nastavenia

- **Aktivióvať Wireless LAN)**: Aktivuje bezdrôtové rozhranie zariadenia.
- **Mód**: Možnosť vybrať či má fungovať iba 802.11b alebo aj 802.11g.
- **Plánovač**: Umožňuje zadefinovať skupiny časových plánov, nastavených v Plánovači volaní do jednotlivých skupín. Zadaná skupina umožní alebo zakáže pripojenie WIFI v zvolenom časovom pásme.
- **SSID**: Nastavte SSID tak ako je nastavené vo Vašej WIFI karte notebooku pre umožnenie klientskemu PC prístup do siete cez toto zariadenie. Od výroby je SSID default.
- **Kanál**: Vyberte prenosový kanál pre Vigor2600VGST, pričom od výroby je nastavený kanál 6.
- **Skryť SSID**: Počas odchytávania WIFI klientom nebude viditeľné SSID.



3.3.2 Bezpečnostné nastavenia

- **Mód**: Voľba či má byť kryptovanie(WEP, WPA, WPA/PSK) vypnuté alebo zapnuté
- **WPA**: Zdieľaný kľúč: miesto pre zadefinovanie zdieľaného kľúča pre WPA kryptovanie (8 až 63 ASCII znakov)
- **WEP**: Má za účel zvýšiť bezpečnosť prenosu WIFI dátových paketov. WEP kryptuje vybraným kľúčom každý rámec posielaný od rádiového užívateľa. Kryptovanie môže byť aktivované vybraním jedného z 64bit., alebo 128bit. kľúčov.

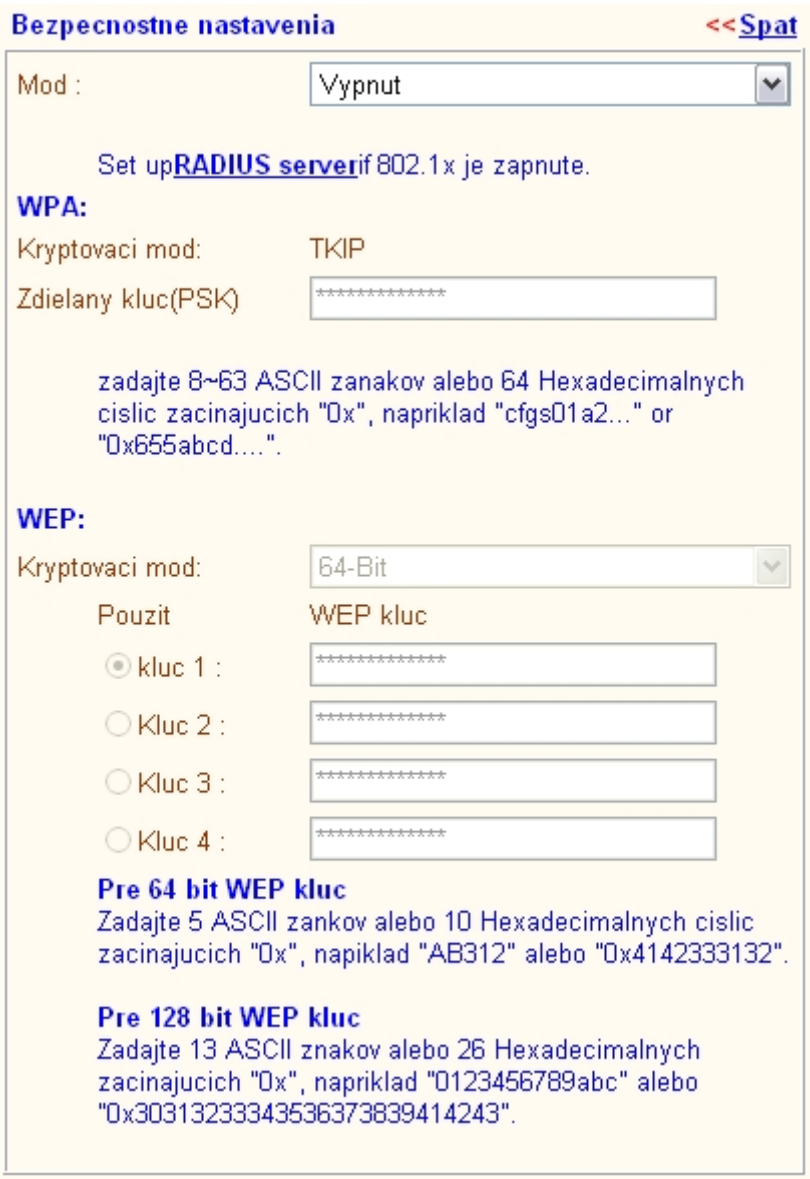
V ponuke sú 4 kryptovacie kľúče, pričom si vyberiete jeden z nich. Kľúč môžete definovať v ASCII alebo Hexadecimálnom formáte.

Pre 64bitový WEP kľúč 5 ASCII znakov, alebo 10 Hexadecimálnych znakov začínajúcich na **0x**.

Napríklad **ABCDE**, alebo **0x4142434445**.

Pre 128bitový WEP kľúč 13 ASCII znakov, alebo 26 Hexadecimálnych znakov začínajúcich na **0x**.

Napríklad **ABCDEFGHIJKLM** alebo **0x1234567891011121314151 61**.



3.3.3 Kontrola prístupu

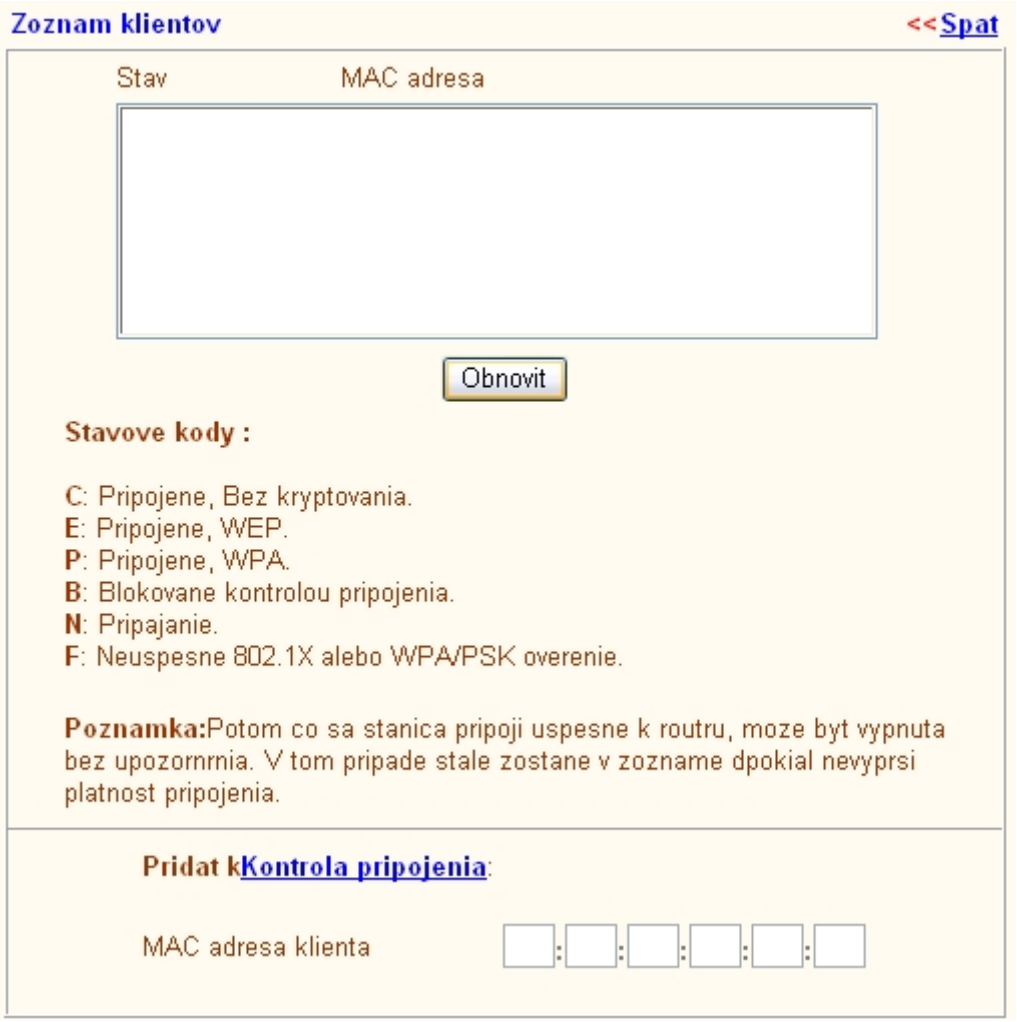
Ako prídavnú formu bezpečnosti WIFI prístupu pre užívateľov poskytuje router kontrolu klientskej MAC adresy. Iba platná a vami uložená MAC adresa bude mať umožnený prístup.

- **Povoliť kontrolu prístupu**: Zaškrtnutím aktivujete túto formu bezpečnosti.
- **MAC adresa**: zadajte konkrétnu PC MAC adresu klienta, ktorému chcete umožniť prístup, ak má klient inú MAC tak nemá prístup k routru.
- **Pridať**: Kliknutím pridáte vami napísanú MAC adresu do zoznamu povolených prístupov.
- **Odstrániť**: Kliknutím zmažete vybranú adresu.
- **Zmeniť**: Kliknutím máte možnosť zmeniť vybranú adresu.
- **Zrušiť**: Kliknutím zrušíte práve nastavovanú MAC adresu.
- **Vymazať všetko**: Kliknutím zmažete všetky nastavené prístupy.
- **OK**: Uloží všetky nastavené MAC adresy do routra.

3.3.4 Zoznam klientov

Táto funkcia umožňuje sledovať stav a počet pripojených klientov k routru

- **Stav**: podľa tabuľky kódu stavov informuje o stave pripojeného klienta
- **MAC adresa**: MAC adresa pripojeného klienta
- **Obnov:** obnoví zoznam klientov
- **Pridať:** označením MAC adresy adresa pribudne v políčku MAC adresa klienta v spodnej časti web rozhrania a tlačidlom pridať je možné túto MAC adresu pridať do zoznamu povolených užívateľov


Zoznam klientov
<<Spat
Stav
MAC adresa
Obnovit
Stavove kody :
C: Pripojene, Bez kryptovania.
E: Pripojene, WEP.
P: Pripojene, WPA.
B: Blokovane kontrolou pripojenia.
N: Pripajanie.
F: Neuspesne 802.1X alebo WPA/PSK overenie.
Poznamka:Potom co sa stanica pripoji uspesne k routru, moze byt vypnuta bez upozornrnia. V tom pripade stale zostane v zozname dpokial nevyprsi platnost pripojenia.
Pridat kKontrola pripojenia:
MAC adresa klienta

4.1 Prístupu do internetu

Router poskytuje dve možnosti prístupu uvedených nižšie: Môžete si zvoliť, ktorý s prístupových režimov vyhovuje vášmu prostrediu. (Pre SR sa používa PPPoE)

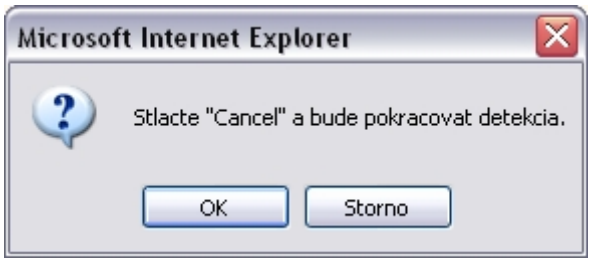
Automatické ATM/DSL nastavenie: Umožňuje automaticky nastaviť ADSL hodnoty ako VPI, VCI, protokol, zapúzdrenie.

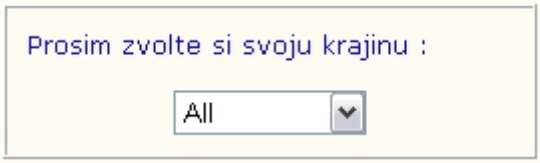
PPPoE/PPPoA: Pripojenie pomocou módu PPPoE alebo PPPoA (používa sa na Slovensku).

MPoA (RFC1483/2684): Pripojenie pomocou módu MPoA.

4.1.1 Automatické ATM/DSL nastavenie

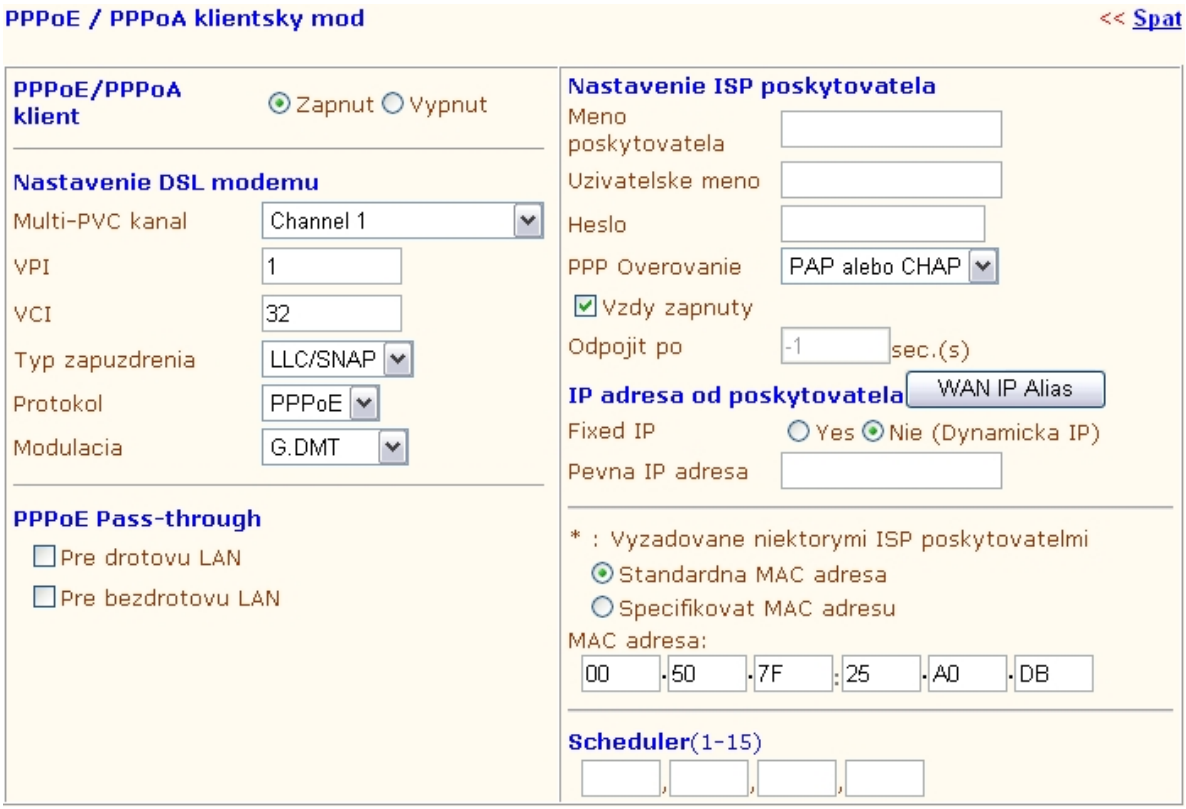
V časti menu Rýchle nastavenia kliknite na odkaz *Prístup do internetu*, na nasledovnej stránke kliknite na odkaz *Automatické ATM/DSL nastavenie*, potom na tlačítko Storno a v nasledujúcom okne na Potvrdiť. Asi po 1 až 2 minútach sa modem automaticky nastaví. Ak sa nenastaví použite manuálne nastavenie v kap.3.3.2 (PPPOE/PPPoA)





4.1.2 PPPoE / PPPoA

Klinknite na *PPPoE / PPPoA* , tým nastavíte ADSL pripojenie manuálne a zobrazí sa stránka PPPoE / PPPoA mód klienta:



PPPoE/PPPoA klient: Zapne alebo vypne možnosť pripájať sa k ADSL pomocou tohto módu

Nastavenie DSL modemu:

VPI: nastavuje sa hodnota VPI (pre SR: 1)

VCI: nastavuje sa hodnota VCI (pre SR: 32)

Typ zapuzdrenia: druh zapuzdrenia (pre SR: LLC/SNAP)

Protokol: výber typu protokolu (pre SR PPPoE)

Modulácia: druh modulácie (pre SR G.DMT)

PPPoE prechod

Pre drôtovú LAN: umožní prechádzať paketom PPPoE cez drôtovú LAN

Pre bezdrôtovú LAN: umožní prechádzať paketom PPPoE cez bezdrôtovú LAN

Nastavenie ISP poskytovateľa: Získate od Vášho poskytovateľa ADSL pripojenia

Meno poskytovateľa: názov poskytovateľa ADSL pripojenia

Užívateľské meno: meno (získate od poskytovateľa ADSL pripojenia)

Heslo: heslo (získate od poskytovateľa ADSL pripojenia)

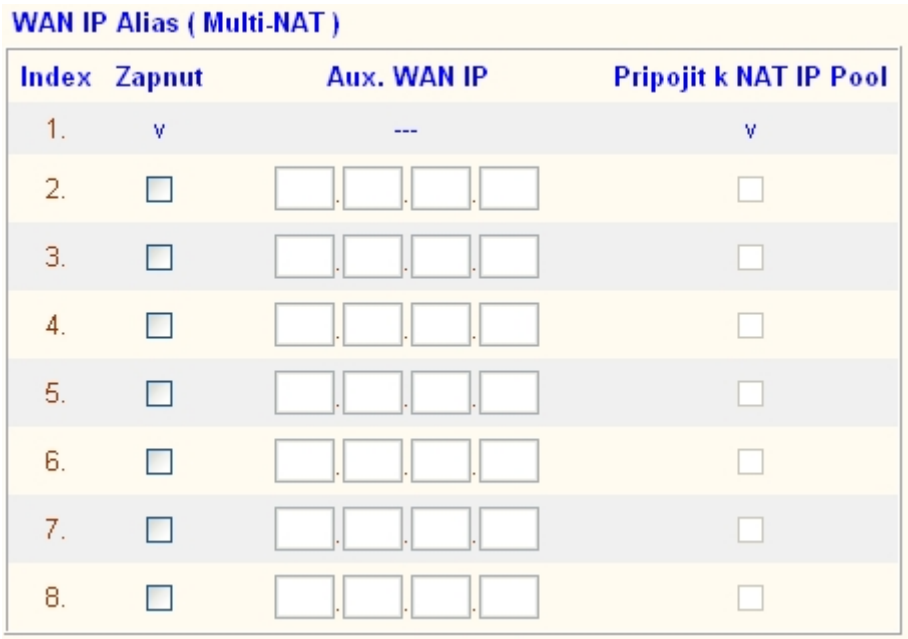
PPP overovanie: druh overovania PAP alebo CHAP

Vždy zapnutý: Router bude k ADSL pripojený nonstop

Odpojiť po: Nastavuje sa čas, za ktorý sa router automaticky odpojí z internetu pokiaľ po túto dobu nie je smerovaná žiadna požiadavka na internet

IP adresa od poskytovateľa

WAN IP ALIAS: Možnosť zadefinovať viac pevných IP adries, ak to poskytuje ISP



Zapnuté: zaškrtnutím sa aktivuje IP adresa

AUX WAN IP (Pomocná WAN IP): Verejná IP adresa

Pripojiť k NAT IP Pool: Ak sú IP adresy nasledujúce za sebou tak treba povoliť túto voľbu

Pevná IP: Aktivuje sa Pevná IP alebo je ponechaná dynamicky prideľovaná IP

Pevná IP adresa: Hodnota pevnej IP, ak je pevná IP povolená

Štandardná MAC adresa: Ak poskytovateľ požaduje overovanie pomocou MAC adresy, tak tu sa nachádza hodnota MAC adresy na ADSL.

Vlastná MAC adresa: Možnosť zmeniť MAC adresu pre ADSL rozhranie

Plánovač: Umožňuje zadefinovať skupiny časových plánov, nastavených v Plánovači volaní do jednotlivých skupín. Zadaná skupina umožní alebo zakáže pripojenie k ADSL v zvolenom časovom pásme.

Po nastavení všetkých parametrov je potrebné nastavenie potvrdiť a uložiť do routra stlačením tlačidla OK, tým je router nakonfigurovaný k pripojeniu na internet.

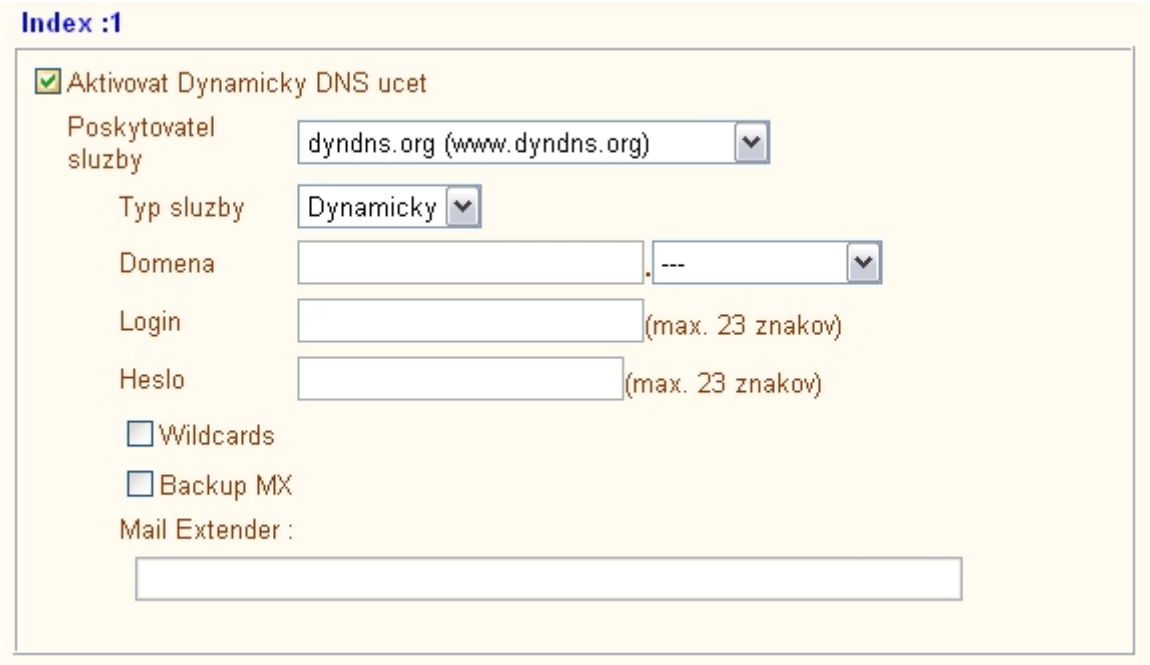
5.1 Dynamické DNS

Umožní nastaviť dynamické DNS servery.

Zobraziť log: Zobrazí záznam o dynamických DNS

Urýchliť obnovenie: urýchli obnovenie DNS záznamov (Refresh)

Index 1-3: možnosť zadefinovať 3 skupiny DNS záznamov



Zapnúť dynamický DNS účet: Aktivuje účet

Poskytovateľ služby: Výber poskytovateľa služby

Typ služby: Môže byť Dynamický, Statický, Vlastný

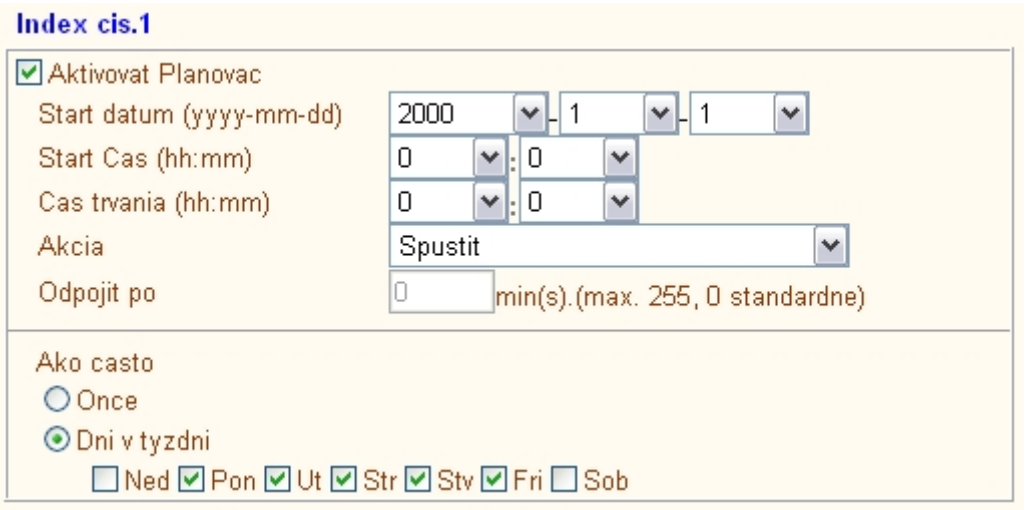
Meno domény: názov domény

Prihlasovacie meno: Poskytne poskytovateľ DNS servera

Heslo: Poskytne poskytovateľ DNS servera

5.2 Plánovač volaní

Umožní naplánovať 15 skupín časových pásiem v ktorých je alebo nie je možné vykonať nejakú akciu, v ktorej sa používa nastavenie Plánovača volaní. (Napr. aktivovať v danom časovom pásme WIFI rozhranie).



Aktivovať plánovač: Aktivuje nastavené časové pásmo

Štart dátum: Počiatočný dátum

Štart čas: Počiatočný čas

Dĺžka trvania: Dĺžka trvania

Akcia: Zodvihnúť alebo položiť (Povoliť alebo zakázať)

Odpojiť po: Po zadanom čase sa odpojí

Ako často: nastavuje či samá daný plánovač použiť jedenkrát alebo v konkrétnych dňoch pravidelne

Poz.: nastavenie v príklade odpojí napr. ADSL linku každý piatok o 23.55 a pripojí o 10minút. Samozrejme musí byť daný plán aktivovaný pri konkrétnej funkcii (napr. PPPoE) a musí byť nastavené automatické nastavovanie času routra (4.6 Čas a dátum).

5.3 NAT - Prekladanie adries

Najčastejšie budete router používať s aktivovanou funkciou NAT - "Network Address Translation" Preklad sieťovej adresy. To znamená, že router získa jednu alebo viac globálne presmerovateľných IP adries od ISP. Miestny užívateľ bude používať privátnu IP adresu definovanú cez RFC-1918 pre komunikáciu s routrom. Router prekladá privátnu sieťovú adresu na verejnú IP adresu, ktorá sa potom používa pre prístup na internet. Nastavenie NAT bližšie špecifikujú aplikácie.

Kliknite na ponuku "**NAT – prekladanie adries**, pričom sa vám otvorí stránka nastavení, kde sa zobrazia privátne adresy definované cez RFC-1918. Obvykle sa pre podsieť routra používa 192.168.1.0/24.

5.3.1 Tabuľka presmerovania portov

Tabuľka presmerovania portov môže byť použitá pre sprístupnenie interných serverov pre verejné domény, alebo pre otvorenie portu so špeciálnym číslom pre interného užívateľa. Interný užívateľ môže WAN IP adresu použiť pre prístup k takým službám Internetu, ako je napríklad FTP, WWW a podobne. Nasledujúci príklad ponúka možnosť sprístupnenia interného FTP servera verejnej doméne. Interný FTP server funguje na lokálnej užívateľskej adrese 192.168.1.10.

Tabulka presmerovania portov << Spat

Index	Meno sluzby	Protokol	Verejny port	Privatna IP	Privatny port	aktivne
1	FTP	TCP	21	192.168.1.10	21	☑
2		---	0		0	☐
3		---	0		0	☐
4		---	0		0	☐
5		---	0		0	☐
6		---	0		0	☐
7		---	0		0	☐
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

Ako je to vyššie zobrazené, "**Tabuľka presmerovania portov**" poskytuje 10 portov nastaviteľných pre vstup interného užívateľa:

- **Názov služby**: zadáte názov sprístupňovanej sieťovej služby.
- **Protokol**: zadáte protokol transportnej vrstvy (TCP alebo UDP)
- **Verejný port:** zadáte port, ktorý bude pridelený internému užívateľovi.
- **Vnútorná IP:** zadáte privátnu IP adresu interného užívateľa poskytujúceho danú službu.
- **Vnútorný port**: zadáte číslo privátneho portu služby poskytovanej interným užívateľom.
- **Aktívne**: zaškrtnutím položky aktivujete nastavenie portov.

Kliknite na "**OK**".

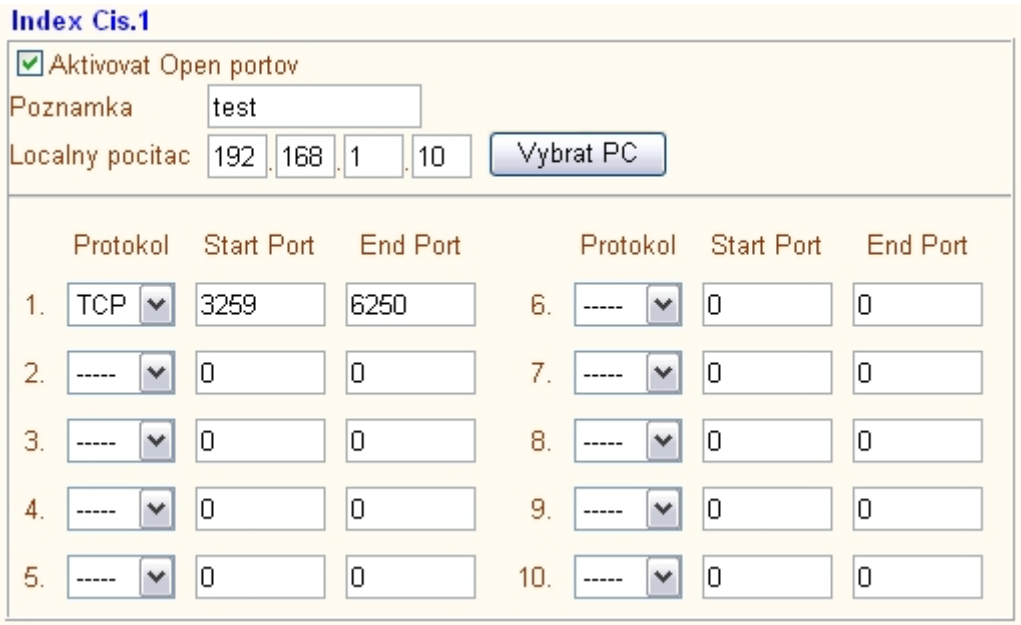
5.3.2 DMZ hostiteľ

Kliknutím na "**DMZ hostiteľ**" sa otvorí stránka nastavenia. DMZ hostiteľ umožňuje preddefinovanému internému užívateľovi mať sprístupnené cez Internet špeciálne aplikácie, ako napríklad NetMeeting, Internetové hry a podobne:

- **Zapnuté:** zaškrtnutím položky aktivujete funkciu DMZ hostiteľ
- **Súkromná IP**: zadajte IP adresu DMZ hostiteľa

5.3.3 Tabuľka presmerovania portov

Slúži na otvorenie skupiny alebo viacerých skupín portov.



Zapnúť otvorenie portov: aktivuje nastavenú skupinu portov

Lokálny počítač: výber IP adresy lokálneho počítača pre ktorý sa táto skupina otvára

Protokol: výber protokolu transportnej vrstvy TCP, UDP

Start Port (Prvý port): počiatočný port

End Port (Posledný port): konečný port

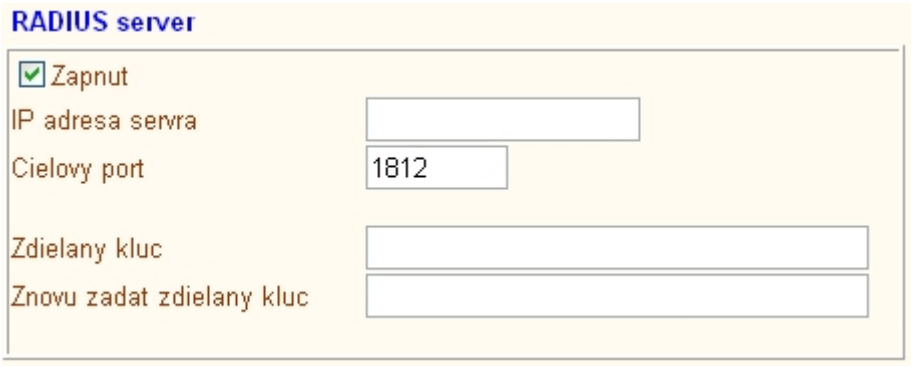
5.3.4 Zoznam najpotrebnejších portov

Táto stránka poskytuje pre vaše potreby zoznam najpotrebnejších portov, ich čísla a protokoly.

Zoznam znamych portov << Spat

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

5.4 RADIUS server



Slúži na zadanie RADIUS (RemoteDialInUserSetup) servera, ktorý slúži na overovanie prístupu užívateľov do siete.

Zapnutý: aktivácia RADIUS servera

IP adresa servera: IP adresa servera (verejná)

Cieľový port: port cez ktorý komunikuje

Zdieľaný kľúč: kryptovací kľúč na zabezpečenie komunikácia medzi serverom a routrom

5.5 Statické routovanie

Router môže byť nastavený ako IP router. V ponuke "**LAN TCP/IP a DHCP Server**" zadefinujete konfiguráciu IP siete pre LAN1 rozhranie vyplnením druhej IP adresy a druhej masky podsieťe. V ponuke " **Prístup do internetu">>" PPPoE / PPPoA** " zadefinujete konfiguráciu IP siete pre LAN2 rozhranie taktiež vyplnením IP adresy a masky podsieťe.

Poznámka: Router Vigor2600VGST má v pôvodnom nastavení vstavané RIP "Routing Information Protcol". Ak majú aj vzdialené routre tento protokol, RIP je v takomto prípade použité na výmenu vzájomných informácií. Nastavenie statického routovania poskytuje cestu, ako previesť staticky určené IP pakety cez určený router.

V tejto aplikácii je možné popísať a presne definovať pravidlá statického routovania pre LAN1 a LAN2. Router má priestor pre 10 rôzne konfigurovateľných statických routovacích pravidiel. Kliknutím na číslo v stĺpec "**Index**" otvoríte okno ku konkrétnemu nastaveniu.

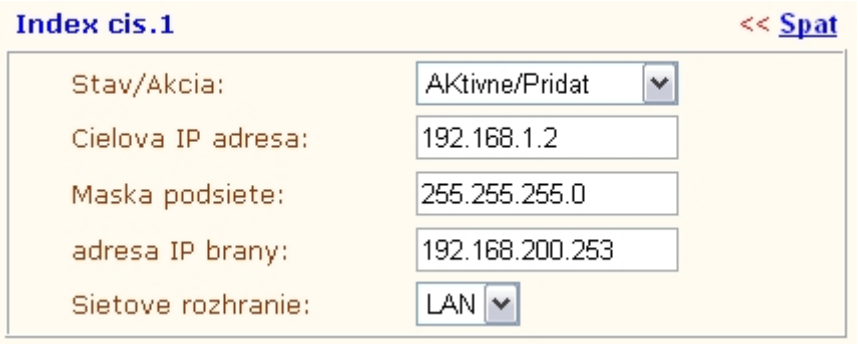
Pre LAN:

Pre konfiguráciu rozhrania LAN1 pre IP routovanie, kliknite na "**LAN1 TCP/IP and DHCP Setup**".

Zaškrtnite "**Zapnut**" a do kolónky "**2.IP adresa**" napíšte 192.168.100.1, do kolónky "**2.maska podsiete**" zase 255.255.255.0. Momentálne máte routovateľnú sieť 192.168.100.0/24 pripojenú k LAN1 rozhraniu.

5.5.1 Pridanie statického routovania

Ak chcete, aby siete 192.168.202.0/24 a 192.168.100.0/24 mali k sebe vzájomne prístup, pridajte statické routovanie v routri Vigor2200 a takisto aj v routri s IP adresou 192.168.200.253. Nasledujúce nastavenie zobrazuje konfiguráciu statického routovania vo Vigore2600VGST.



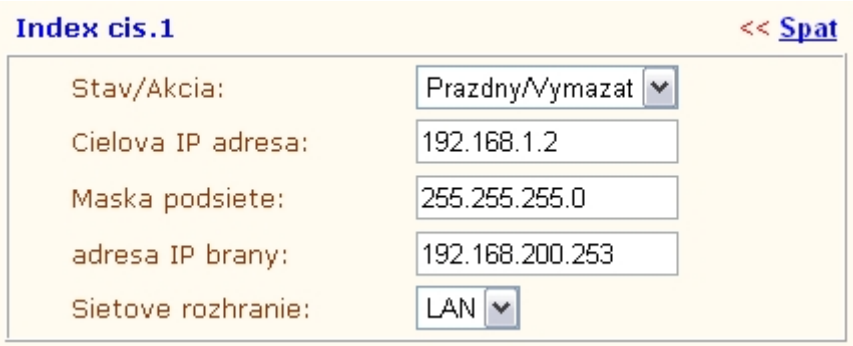
- **Stav/Akcia**: nastavte na "**Aktívny**/**Pridať**".
- **Cieľová IP adresa:** špecifikujte IP cieľovej siete, alebo IP hostiteľa. V tomto príklade použijeme sieť s IP 192.168.202. ako routovací cieľ.
- **Maska podsiete**: špecifikujte cieľovú sieťovú masku. V našom príklade je maska podsiete 192.168.202.0.
- **IP adresa brány:** špecifikujte IP adresu ďalšieho routra. V našom príklade zadáme 192.168.200.253, pričom sieť za routrom má IP 192.168.202.0.
- **Sieťové rozhranie**: špecifikujte sieťové rozhranie, v našom prípade to bude LAN, keďže na ňom je pripojený ďalší router 192.168.200.253.

Kliknite na "**OK**".

Poznámka: Aby statické routovanie fungovalo, je potrebné nastaviť ho aj v ďalšom routri, aby boli všetky IP pakety 192.168.100.0/24 posielané do routra Vigor2600VGST. Po kliknutí na "**OK**" bude pridaný router zobrazený v tabuľke aktuálne spustených routovaní. Pre kontrolu kliknite na "**Zobrazenie aktuálnej routovacej tabuľky**".

5.5.2 Vymazanie statického routovania.

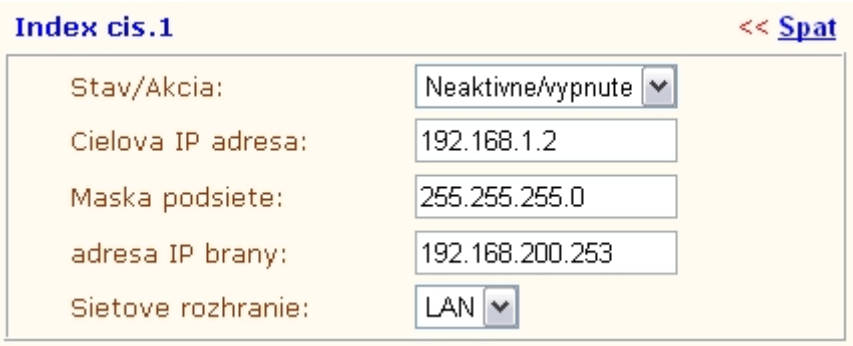
Pre vymazanie nastavení a samotného statického routovania, v ponuke "**Stav/Akcia**" vyberte " **Prázdny/Vymazať**".



Kliknite na "**OK**". Všetky položky predchádzajúceho nastavenia budú vymazané a odstránené z tabuľky aktuálne spustených routovaní.

5.5.3 Deaktivácia prednastaveného statického routovania.

Niekedy je potrebné prednastavené statické routovanie deaktivovať, ale nie vymazať, keďže počítame s jeho obnovením. V ponuke "**Stav/Akcia**" vyberte " **Neaktívny/Odobrať**". Kliknite na "**OK**" a prednastavené statické routovanie bude zablokované.



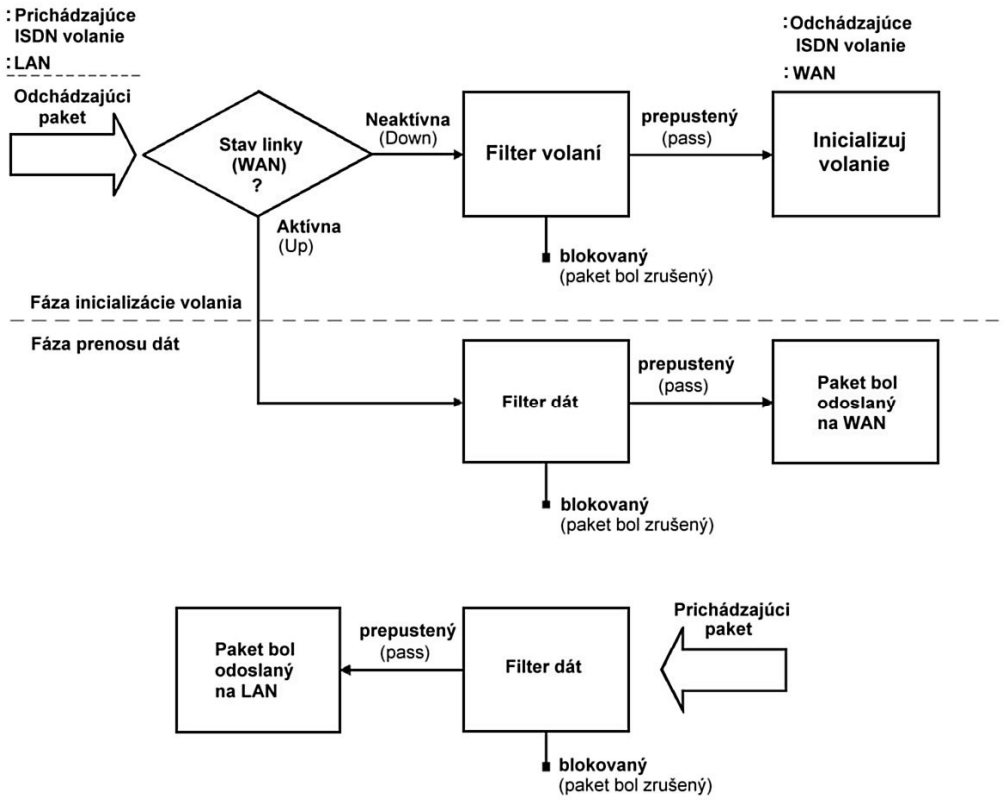
5.6 IP filter a Firewall

Funkcia IP Filtrov / Firewall je užitočná pre ochranu lokálnej siete pred útokmi zvonku. Poskytuje takisto aj formu obmedzenia pre užívateľov lokálnej siete pri prístupe na Internet. V zásade dokáže vyfiltrovať špecifikované pakety, na základe ktorých router spustí vonkajšie spojenie.

5.6.1 Opis Firewallu

IP Filter / Firewall v sebe obsahuje dva typy filtrov: Call Filter (filter volaní) a Data Filter (filter dát). Call Filter je navrhovaný tak, aby blokoval alebo prepúšťal IP pakety, na základe ktorých router spustí vonkajšie spojenie. Data Filter je navrhovaný tak, aby blokoval alebo prepúšťal definovaný druh IP paketov, ktoré majú umožnený priechod cez router, keď je nadviazané WAN spojenie. V zásade, keď je odchádzajúci paket presmerovaný do WAN, IP Filter rozhodne, či má byť presmerovaný na Call Filter, alebo Data Filter.

Ak nie je nadviazané WAN spojenie, paket bude presmerovaný na Call Filter. Ak daný paket nemá umožnené spustiť router, aby nadviazal vonkajšie spojenie, bude zrušený. V opačnom prípade bude inicializované volanie pre nadviazanie WAN spojenia.



Ak WAN spojenie nadviazané je, paket bude v tomto prípade presmerovaný na Data Filter. Ak je paket v nastaveniach definovaný pre blokovanie, bude zrušený. Prípadne aj prichádzajúci paket prejde cez WAN rozhranie, prechádza priamo Data Filtrom. Ak je paket v nastaveniach definovaný pre blokovanie, bude zrušený. V opačnom prípade bude poslaný do vnútornej LAN. Schéma filtrov je zobrazená nižšie.

Nasledujúce kapitoly popisujú rozsiahlejšie nastavenie IP Filtrov / Firewallu cez Web konfigurátor. Je možné nastaviť 12 skupín filtrov, a pre každý jeden 7 charakteristík. To je spolu 84 filtrovacích predpisov pre nastavenie IP Filtrov / Firewallu. V default nastavení je Call Filter definovaný vo Filtrovej skupine 1 a Data Filter vo filtrovej skupine 2.

- Hlavne nastavenie
- Kontrola MAC adries
- Blokovanie IM aplikacii (rychle spravy)
- Blokovanie P2P aplikacii (bod-bod)
- DoS obrana
- Obsahove filtrovanie
- Nastavnie Filtrovania >>Nastavit vyrobne nastavenie

Set	Poznamky	Set	Poznamky
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

- **Hlavné nastavenia**: Všeobecné nastavenia IP filtrov.
- **Kontrola MAC adries**: Kontrola prístupu podľa MAC adries.
- **Blokovanie IM aplikácií (rýchle správy):** Možnosť zakázať posielanie rýchlych správ (napr. Messenger)
- **Blokovanie P2P aplikácií:** Zakázanie používania peer-to-peer sietí
- **DoS obrana:** Ochrana pred útokom z internetu.
- **Obsahové filtrovanie:** Možnosť zakázať prístup na konkrétne stránky, prípadne zakázať sťahovanie niektorých prvkov.
- **Nastavenie filtrovania:** Tabuľka s 12 skupinami filtrov pre nastavenie konfigurácie.
- **Nastaviť výrobné nastavenie:** Kliknutím na túto položku môžete vymazať hodnoty "**IP filtrov / nastavení Firewallu**" a vrátiť hodnoty do výrobného nastavenia.

5.6.2 Hlavné nastavenia

Na stránke všeobecných nastavení môžete aktivovať/zablokovať volací filter alebo Dátový filter a popísať štartovaciu skupinu pre každý z nich. Môžete tu taktiež konfigurovať prihlasovacie nastavenia a zadať MAC adresu pre duplikáciu prihlasovaných paketov.

- **Filter volaní:** Voľbou "**Zapnutý**" zvolíte možnosť filtrovania pre odosielanie voľby čísla, pričom však musíte zvoliť jeden počiatočný filter. Zaškrtnutím "Vypnut" (zablokovať) zakážete filtrovanie volaní.
- **Dátový filter**: Voľbou "**Zapnutý**" zvolíte možnosť filtrovania prietoku dát, pričom však musíte zvoliť jeden počiatočný filter. Zaškrtnutím "Vypnut" (zablokovať) zakážete filtrovanie dát.
- **Log Flag (Príznak zaznamenávania)**: Funkcia vhodná pre servisné záznamy prípadných problémov.
  - **Žiadny**: Funkcia zaznamenávania nie je aktívna.
  - **Blokovať**: všetky blokované pakety budú zaznamenané.
  - **Poslať**: všetky pakety, ktoré prejdú filtrami, budú zaznamenané.
  - **Nerovná sa**: zaznamenajú sa všetky pakety, ktoré nezodpovedajú pravidlám filtrovania.

Poznámka: Filtrovací záznam sa vám zobrazí v Telnete, ak zadáte príkaz "log-f".

- **MAC adresa pre duplikované zaznamenávané pakety**: Ak chcete duplikovať niektoré zaznamenané pakety smerované z routra na iné vzdialené sieťové zariadenie, zapíšte do tejto položky MAC adresu zariadenia v HEXa formáte. Ak chcete zakázať duplikáciu paketov, potom do položky vpíšte hodnotu "**0**"-nula (viď kapitola "Duplikácia v LAN"). Funkcia je veľmi užitočná pre Ethernet zariadenia.

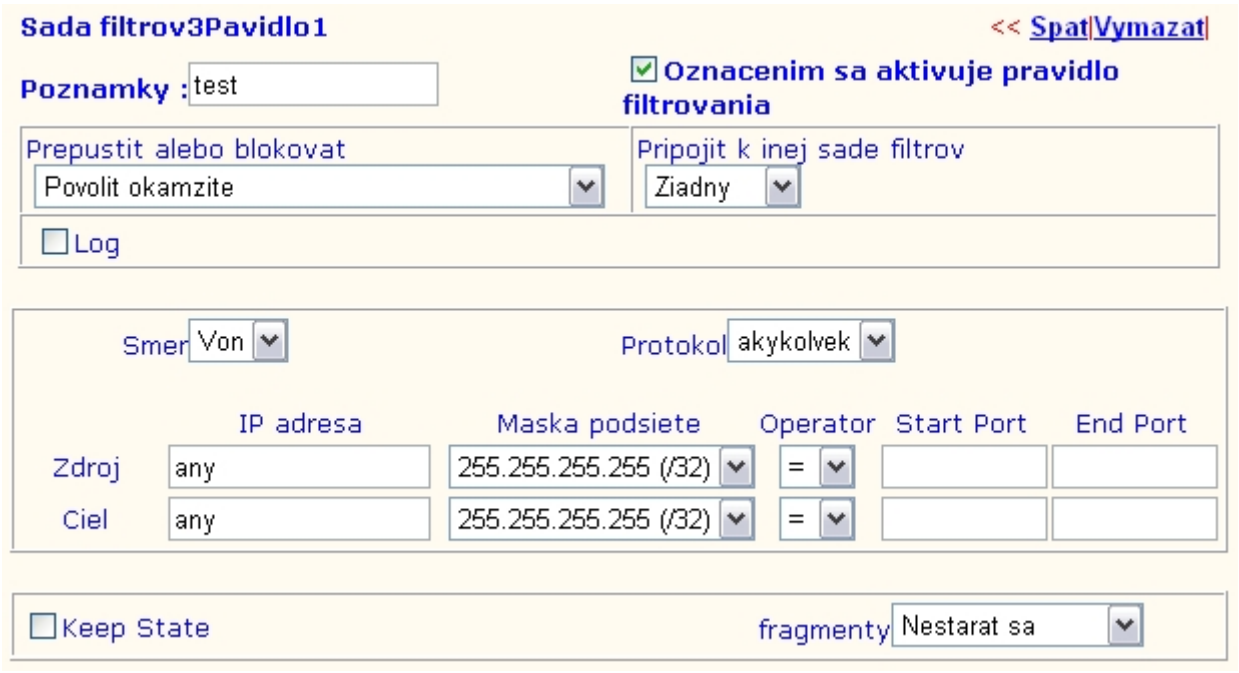
5.6.3 Nastavenie a zmena filtrovacích skupín.

- **Poznámky**: táto kolónka je určená pre zápis poznámok, alebo popis filtrovacej skupiny. Maximálna dĺžka je 23 znakov.
- **Pravidlo filtrovania:** kliknutím na tlačítka 1-7 nastavujete a meníte pravidlá pre filtre.
- **Zapnuté**: označenie tejto položky znamená, že pravidlo je aktívne, neoznačenie znamená neaktívne pravidlo.
- **Nasledovná sada filtrov**: môžete priradiť nasledujúcu sadu filtrov do reťazca pravidiel pre filtrovanie. POZOR: Pri reťazení filtrov nesmiete vytvoriť uzatvorenú slučku.

5.6.4 Nastavenie a zmena pravidiel filtrovania

Kliknutím na ponuku "**Pravidlo filtrovania**" sa dostanete na stránku nastavovania pravidiel filtrovania pre konkrétny filter. Popis každej konfigurovateľnej položky:

- **Poznámky**: táto kolónka je určená pre zápis poznámok, alebo popis pravidla. Maximálna dĺžka je 14 znakov.
- **Aktivovať pravidlo filtrov**: zaškrtnutím aktivujete pravidlo filtrovania.
- **Pošli alebo blokuj:** špecifikujte následne vykonanú činnosť v prípade, že paket zodpovedá pravidlu.
  - **Blokovať okamžite**: paket zodpovedajúci pravidlu bude okamžite blokovaný.
  - **Poslať okamžite** paket zodpovedajúci pravidlu bude okamžite prepustený.
  - **Blokovať ak žiadny ďalší nevyhovuje**: paket, ktorý síce vyhovuje danému pravidlu, ale nevyhovuje ďalším, bude blokovaný.
  - **Poslať ak žiadny ďalší nevyhovuje**: paket, ktorý aj keď nevyhovuje ďalším pravidlám, ale vyhovuje danému pravidlu, bude prepustený.



- **Vetviť s inou skupinou filtrov:** keď je paket prepustený daným pravidlom filtrovania, potom táto vetva bude pokračovať na ďalšiu sadu filtrov, definovanú v tomto poli. Takáto filozofia konštrukcie filtrov umožňuje definovať rozsiahle, a pritom veľmi efektívne štruktúry podmienok pre filtrovanie.
- **Duplikovať do LAN:** ak chcete prepúšťané pakety duplikovať do niektorých ďalších sieťových zariadení (PC v LAN), zaškrtnite dané políčko. Fyzickú adresu sieťového zariadenia definujete v ponuke "**Hlavné nastavenia**">>" **MAC adresa pre duplikované zaznamenávané pakety**". táto funkcia je užitočná pre tzv. off-host protokolizáciu špecifikovaných paketov využívajúcu sieťový sniffer.
- **Zaznamenávať**: zaškrtnutím políčka zvolíte zaznamenávanie do tzv. Log poľa. Pre zobrazenie záznamu v Telnete zadajte príkaz "**log-f**". Príkazy pre Telnet nájdete v kapitole 8.1 Používanie terminálových príkazov pre Telnet.
- **Smer**: pole pre výber smerovania paketov vo vzťahu k Routru. (Pre Call Filter je toto pravidlo irelevantné).

Pre dátový filter:

  - **Dnu**: prichádzajúce pakety.
  - **Von**: odchádzajúce pakety.

- **Protokol:** pole pre výber protokolu.
  - **Akýkoľvek**: pakety rôznych protokolov.
  - **TCP**: Transmission Control Protocol/Internet Protocol
  - **UDP**: User Datagram Protokcol
  - **TCP/UDP**: pakety s protokolom TCP/IP alebo UDP
  - **ICMP**: Internet Control Message Protocol
  - **IGMP**: Internet Group Management Protocol
- **Zdroj**: riadok definície pre zdroj paketov.
- **Cieľ**: riadok definície smerovania paketov.
- **IP adresa**: pole pre definovanie zdrojovej a cieľovej IP adresy daného pravidla filtrovania. Znak "**!**" pred IP adresou znamená inverziu (NOT). V podstate to znamená "nie z tejto adresy", alebo "nie na túto adresu" podľa smerovania paketov. Ak sa namiesto IP adresy v tomto políčku napíše "**any**", znamená to ktorúkoľvek IP adresu.

- **Maska podsiete**: Vyberte jednu masku podsiete pre danú IP adresu. 255.255.255.0(/24) je maska podsiete pre celú sieť typu "C" (255 identifikovateľných zariadení v sieti LAN). Hodnota v zátvorkách znamená počet zľava maskovaných bitov. 255.255.255.252(/30) je maska pre časť podsiete typu "C" (štyri identifikovateľné adresy danej podsiete).
- **Operátor:** položka špecifikácie čísla portu. Ak je položka "**Začiatočný port**" prázdna, potom "**Začiatočný port**" a "**Cieľový port**" budú ignorované. Pravidlo filtrovania vyfiltruje každé číslo portu. V nasledujúcej tabuľke sú popísané jednotlivé možnosti:

tab. = ak je pole " **Cieľový port** " prázdne, potom je jeho hodnota zhodná s hodnotou " **Začiatočný port** ". V ostatných prípadoch sú kontrolované hodnoty portov v rozsahu od " **Začiatočný port** " po "**End Port**" vrátane.

! = ak je pole " **Cieľový port** " prázdne, potom je jeho hodnota zhodná s hodnotou "Start Port". V ostatných prípadoch sú kontrolované hodnoty portov mimo rozsahu definovaného v políčkach od " **Začiatočný port** " po " **Cieľový port** " vrátane.

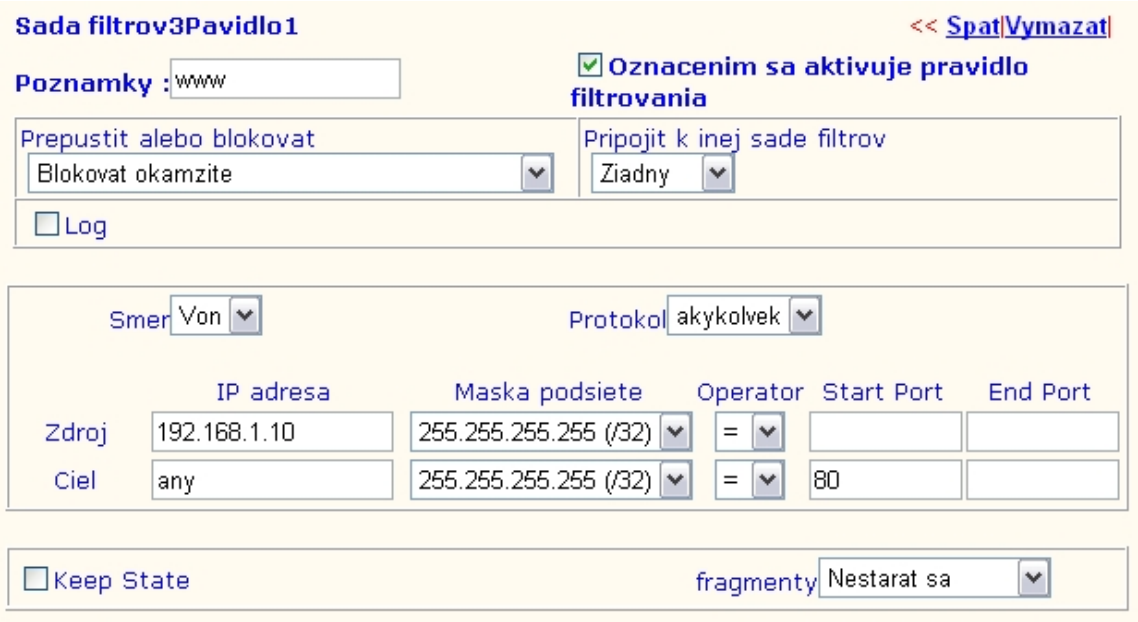
> číslo portu je väčšie ako hodnotia v poli " **Začiatočný port** " vrátane.

< číslo portu je menšie ako hodnota v poli " **Začiatočný port** " vrátane.

- **Udržovať pravidlo aktívne**: zaškrtnutím políčka získate informácie o danom spojení v protokole TCP/UDP/ICMP. V políčku "**protokol**" však musí byť niektorý s protokolov zvolený. (TCP, UDP, TCP/UDP alebo ICMP).
- **Fragmenty**: v ponuke špecifikujte spôsob rozdelenia paketov na fragmenty.
  - **Nestarať sa**: znamená žiadne fragmentové podmienky v aplikácii pravidla.
  - **Nefragmentované**: použije pravidlo filtrácie na nefragmentované pakety.
  - **Fragmentované**: použije pravidlo filtrácie na fragmentované pakety.
  - **Veľmi krátke**: aplikuje pravidlo iba na veľmi krátke pakety, neobsahujúce hlavičku.

5.6.5 Obmedzené neautorizované internetové služby

Táto sekcia zobrazuje jednoduchý príklad ako niekomu obmedziť prístup k www službám. V konkrétnom príklade je IP adresa užívateľa, ktorý bude mať obmedzený prístup, 192.168.1.10. Pravidlo filtrovania je vytvorene v položke Data Filter a je zobrazené nasledovne. Port 80 je http protokolové číslo portu pre www služby.



5.7 VPN a vzdialený prístup

5.7.1 Úvod do Vzdialeného prístupu

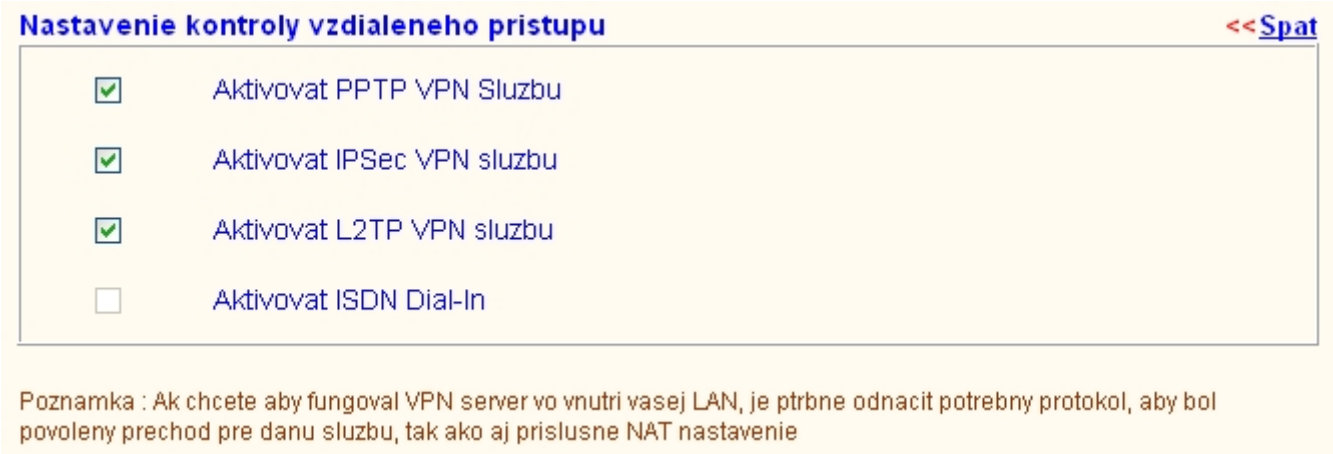
Termín „Vzdialený prístup“, používaný pri týchto zariadeniach v sebe zahŕňa dva druhy prístupov.

Prvý typ, **Profil vzdialeného užívateľa** (teleworker) znamená, že router umožňuje pripojenie sa normálnemu užívateľovi, alebo NAT routru, pre zdieľanie sieťových zdrojov lokálnej siete, alebo surfovať po Internete cez broadband divíziu pripojenú k WAN portu.

Druhým typom je **LAN-LAN profily:** poskytujúce riešenie pre prepojenie dvoch nezávislých LAN pre vzájomné zdieľanie sieťových zdrojov.

5.7.2 Kontrola vzdialeného prístupu

Aktivuje ktoré protokoly môže byť použité pri zostavovaní VPN



5.7.3 PPP hlavné nastavenie

Slúži ako kontrola prístupu užívateľov pristupujúcich smerom dnu.

PPP/MP protokol

- **PPP overovanie volania dnu**:
  - **PAP**: Užívatelia dial-in prístupu budú overovaný protokolom PAP.
  - **PAP alebo CHAP**: Na overenie prístupu použije router najprv protokol CHAP. Ak tento nie je podporovaný druhou stranou, použije protokol PAP.
- **Vzájomné overovanie PAP**: Toto nastavenie aktivujte iba vtedy, ak si ho priamo vyžaduje pripájaný router. Pôvodné nastavenie je **No**.

Prideľovanie IP adresy pre užívateľov volajúcich dnu

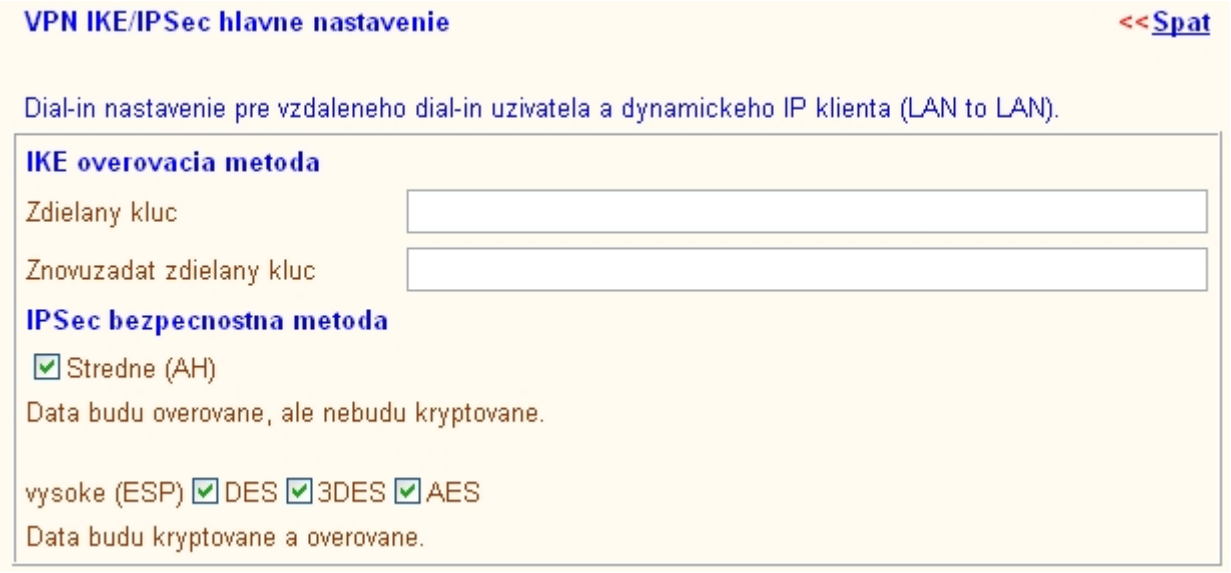
- **Štartovacia IP adresa:** Zadajte štartovaciu IP adresu pridelenú spojeniu dial-in PPP. Môžete si vybrať IP adresu z lokálnej siete. Napríklad, ak je lokálna sieť 192.168.1.0/255.255.255.0, môžete zvoliť ako štartovaciu adresu 192.168.1.200.

  Prvý bude mať pridelenú štartovaciu IP adresu, druhý štartovaciu IP adresu plus 1.

Kliknite na **Potvrdiť**.

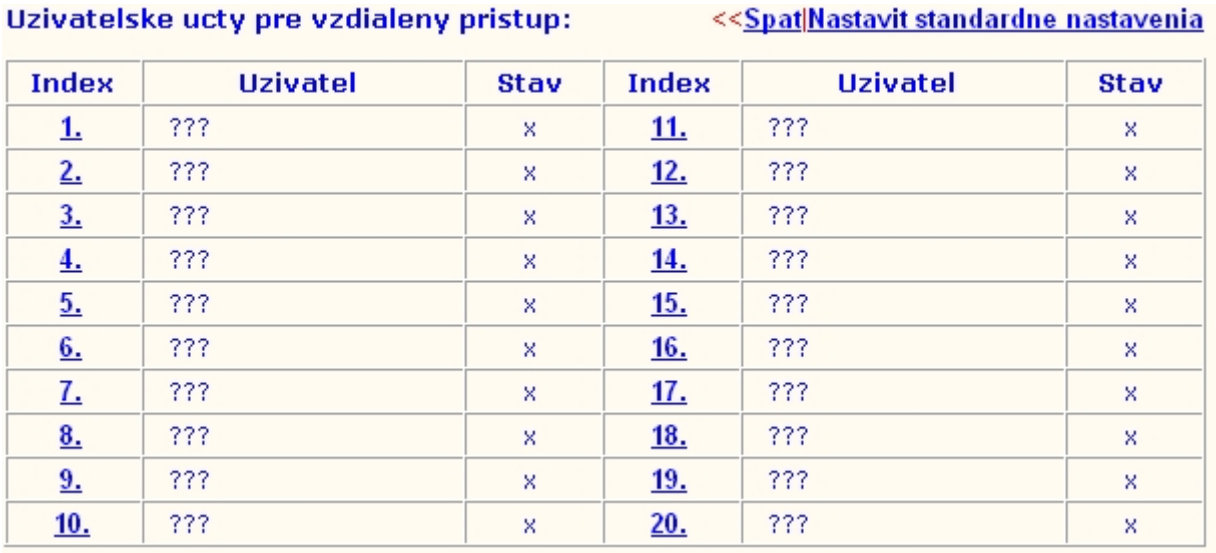
5.7.4 VPN IKE/IPSEC hlavné nastavenie

Nastavenie kryptovacieho kľúča pre užívateľov volajúcich dnu.



5.7.5 Tvorba prístupových účtov

Po aktivácii dial-in funkcií musíte vytvoriť prístupový účet pre každého jedného užívateľa. Kliknite v hlavnom menu na ponuku **Profil vzdialeného užívateľa**. Z nasledujúceho okna vidíte, že router poskytuje miesto pre dvadsať užívateľov.



Index	Uzivatel	Stav	Index	Uzivatel	Stav
1.	???	x	11.	???	x
2.	???	x	12.	???	x
3.	???	x	13.	???	x
4.	???	x	14.	???	x
5.	???	x	15.	???	x
6.	???	x	16.	???	x
7.	???	x	17.	???	x
8.	???	x	18.	???	x
9.	???	x	19.	???	x
10.	???	x	20.	???	x

- **Nastaviť štandardné nastavenie**: Kliknutím na ponuku vymažete všetky užívateľské účty.
- **Index** (P.č.): Kliknutím na poradové číslo v zozname otvoríte detailné nastavenie pre konkrétny užívateľský účet.
- **Užívateľ**: **???** znamená, že daný účet je voľný. Ak bol účet nakonfigurovaný, v kolónke sa zobrazí vami zadané užívateľské meno.
- **Stav**: Aktivitu účtu vyjadruje symbol **v**, **x** znamená, že účet nie je aktívny.

Kliknite na poradové číslo, zobrazí sa stránka pre detailné nastavenie konkrétneho užívateľského účtu.

Užívateľský účet a overovanie

- **Zapnúť tento účet**: Aktivuje tento účet
- **Meno**: Vpíšte užívateľské meno konkrétneho dial-in užívateľa.
- **Heslo**: Heslo, ktoré bude používať pre vzdialený prístup.
- **Odpojiť po**: Pôvodné nastavenie je 300 sekúnd. Ak je užívateľ nečinný nad zadaný limit, router preruší spojenie.
- **Špecifikovať vzdialený uzol**: Pre zvlášť bezpečný prístup je možné povoliť dial-in užívateľovi prístup iba z konkrétneho čísla. CLID - Calling Line Identification - Identifikácia volajúcej linky.
- **Peer ID** (číslo náprotivnej strany): Ak ste aktivovali overenie cez CLID, do tejto kolónky zadajte číslo užívateľa.

IPSec bezpečnostná metóda

- **Stredná (AH)**: kryptuje sa iba hlavička paketu
- **Vysoká :** DES, 3DES a najsilnejšie kryptovanie AES

Funkcia spätného volania

Funkcia spätného volania poskytuje dial-in užívateľom callback službu, čo znamená, že náklady za spojenie pôjdu na ťarchu majiteľa routra.

- **Zapnutie funkcie spätné volanie:** Zaškrtnite pre aktiváciu funkcie spätného volania)
- **Zadajte číslo pre spätné volanie**: Možnosť poskytujúca zvýšenie bezpečnosti. Jej aktiváciou bude router vytáčať iba vami definované číslo.
- **Číslo spätného volania**: Ak ste predošlú funkciu aktivovali, sem zadajte konkrétne číslo.
- **Zapnutie kontroly poplatkov spätného volania**: V pôvodnom nastavení má táto funkcia ako úsporu nastavené časové obmedzenie, čo znamená, že po prekročení limitu bude spojenie automaticky ukončené.
- **Poplatky spätného volania** (Úspora –jednotiek : minút): Zadajte konkrétne obmedzenie.

5.7.6 Prístup LAN-to-LAN

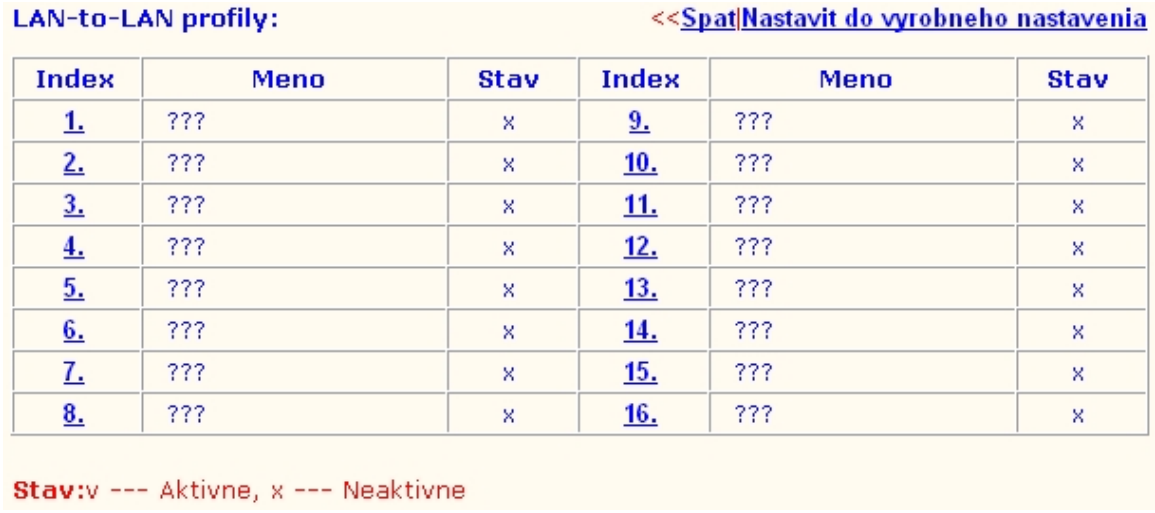
Nasledujúca kapitola vychádza z hore zobrazeného plánu siete pre lepšie znázornenie, ako nastaviť LAN-to-LAN profil spojenia dvoch privátnych sietí. V hore uvedenom príklade, privátna sieť 192.168.1.0/24 je definovaná ako ústredie a na druhej strane je sieť pobočky, 192.168.2.0/24.

Pred nastavovaním LAN-to-LAN profilu musíte mať k dispozícii všetky informácie zobrazené na nákrese.

	Ústredie	Pobočka
ID siete	192.168.1.0/24	192.168.2.0/24
IP adresa routra/maska siete	192.168.1.1/24	192.168.2.1/24
IP adresa pridelená pre dial-in spojenie	192.168.1.200	192.168.2.200
Prístupový účet	Už.m.: head	Už.m.: head
	Heslo: head	Heslo: head

5.7.7 Tvorba profilu LAN-LAN volaného

Pre aktivovanie VPN služby musíte vytvoriť LAN-LAN profil pre každú sieť. Kliknite v hlavnom menu na ponuku **LAN-LAN profily**.



Router umožňuje vytvoriť 16 rôznych profilov pre 16 rôznych vzdialených sietí.

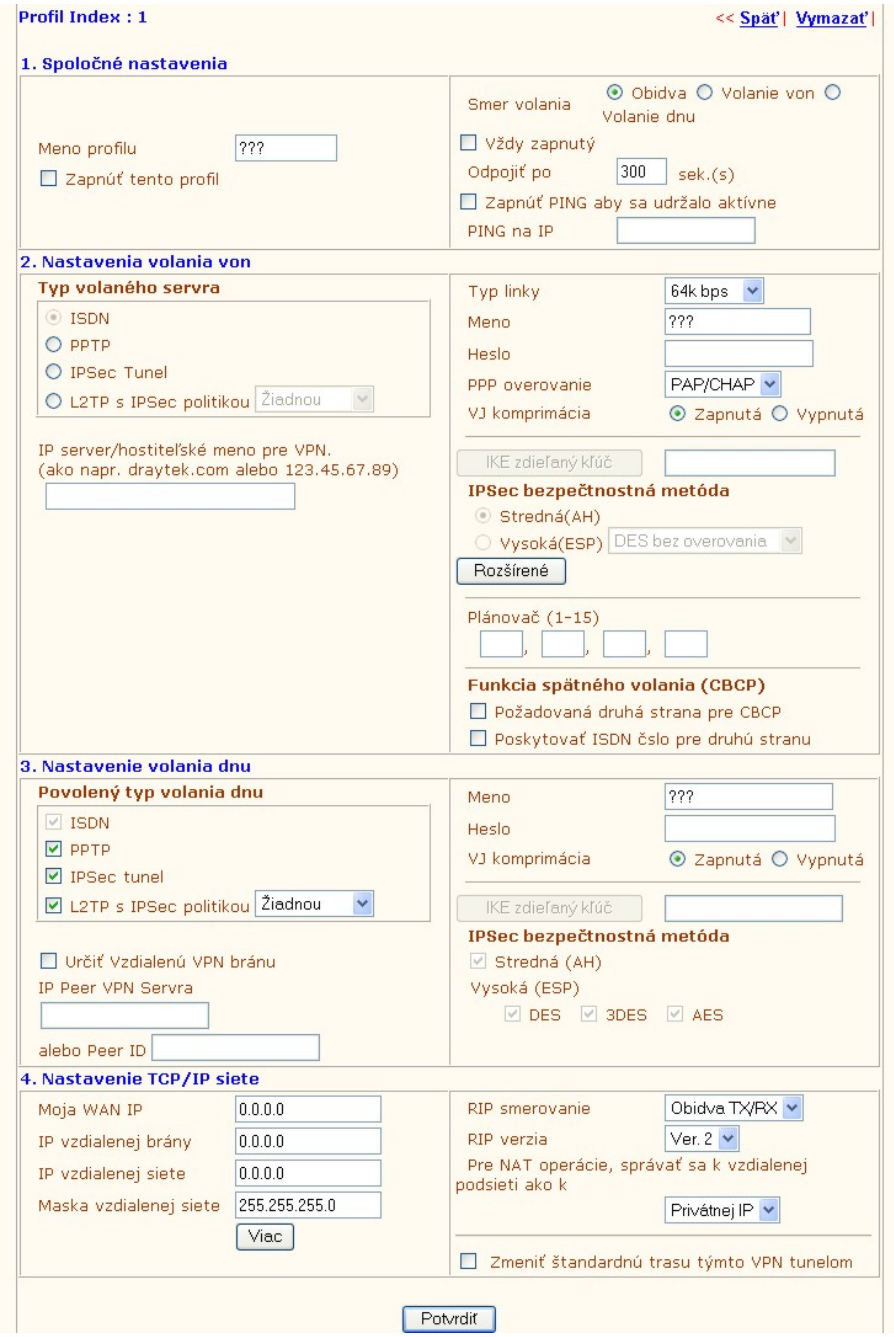
- **Nastaviť štandardné nastavenie:** Kliknutím vymažete všetky LAN-LAN profily.
- **Index** (P.č.): Kliknutím na číslo otvoríte stránku pre detailné nastavenie konkrétneho profilu.
- **Meno**: V tejto kolónke sa zobrazuje názov daného profilu. **???** indikuje prázdny profil.
- **Stav**: Aktivitu daného profilu indikuje symbol **v**, **x** znamená, že profil nie je aktívny.

Kliknite na poradové číslo. Otvorí sa stránka pre detailné nastavenie konkrétneho LAN-LAN profilu.

Každý profil obsahuje štyri podskupiny: Spoločné nastavenia, Nastavenia volania von, Nastavenia volania a Nastavenie TCP/IP siete.

Spoločné nastavenia

- **Meno profilu**: Vpíšte názov vzdialenej siete.
- **Zapnúť tento profil**: Zaškrtnutím profil aktivujete.
- **Smer volania**: Definujte smerovanie volania. **Obidva** znamená, že môže byť použitý pre prichádzajúce aj odchádzajúce volania, **Volanie von**, že môže byť použitý iba pre odchádzajúci prístup, **Volanie dnu** iba pre prichádzajúci.
- **Vždy zapnutý:** pri potvrdení bude tunel stále aktívny
- **Odpojiť po**: Pôvodné nastavenie je 300 sekúnd. Ak je užívateľ nečinný nad zadaný limit, router preruší spojenie.
- **Zapnúť Ping aby sa udržalo aktívne**: aktivuje sa ping na IP adresu aby sa spojenie udržovalo aktívne



Nastavenia volania von

- **Typ volaného servera**
  - **PPTP:** Point to Point Tunnelig protocol – najnižšia bezpečnosť kryptovania
  - **IPSec tunel:** IPSec tunel – vyššia bezpečnosť kryptovania
  - **L2TP s IPSec politikou:** najvyššia bezpečnosť kryptovania
- **IKE zdieľaný kľúč**: IKE kryptovací kľúč
- **IP server**: Zadajte IP adresu volaného servera, príp. hostiteľské meno
- **Meno:** Zadajte meno, ktoré bude vzdialený router používať pre overenie prístupu.
- **Heslo**: Zadajte heslo jeho prístupu.
- **PPP overovanie**: Definuje spôsob overenia. Najčastejšie sa používa PAP/CHAP naraz.
- **VJ komprimácia** Znamená protokol TCP/IP pre kompresiu hlavičky. Najčastejšie nastavenie je **Zapnutá** pre zlepšenie využitia spojenia.

IPSec bezpečnostná metóda

- **Stredná:** iba kryptovanie hlavičky
- **Vysoká:** DES, 3DES, AES
- **Rozšírené:** Rozšírené nastavenia pre AES kryptovanie

Plánovač - Umožňuje zadefinovať skupiny časových plánov, nastavených v Plánovači volaní do jednotlivých skupín. Zadaná skupina umožní alebo zakáže pripojenie WIFI v zvolenom časovom pásme.

Nastavenia volania dnu

- **Povolený typ volaného servera**
  - **PPTP:** Point to Point Tunnelig protocol – najnižšia bezpečnosť kryptovania
  - **IPSec tunel:** IPSec tunel – vyššia bezpečnosť kryptovania
  - **L2TP s IPSec politikou:** najvyššia bezpečnosť kryptovania
- **Meno:** Zadajte meno, ktoré bude vzdialený router používať pre overenie prístupu.
- **Heslo**: Zadajte heslo jeho prístupu.
- **Určiť vzdialénú VPN bránu**: Obmedzuje vzdialenú stranu na volanie iba z preddefinovanej IP adresy alebo servera.
- **VJ komprimácia** Znamená protokol TCP/IP pre kompresiu hlavičky. Najčastejšie nastavenie je **Zapnutá** pre zlepšenie využitia spojenia.

IPSec bezpečnostná metóda

- **Stredná:** iba kryptovanie hlavičky
- **Vysoká:** DES, 3DES, AES
- **Rozšírené:** Rozšírené nastavenia pre AES kryptovanie
- **IKE zdieľaný kľuč**: IKE kryptovací kľúč

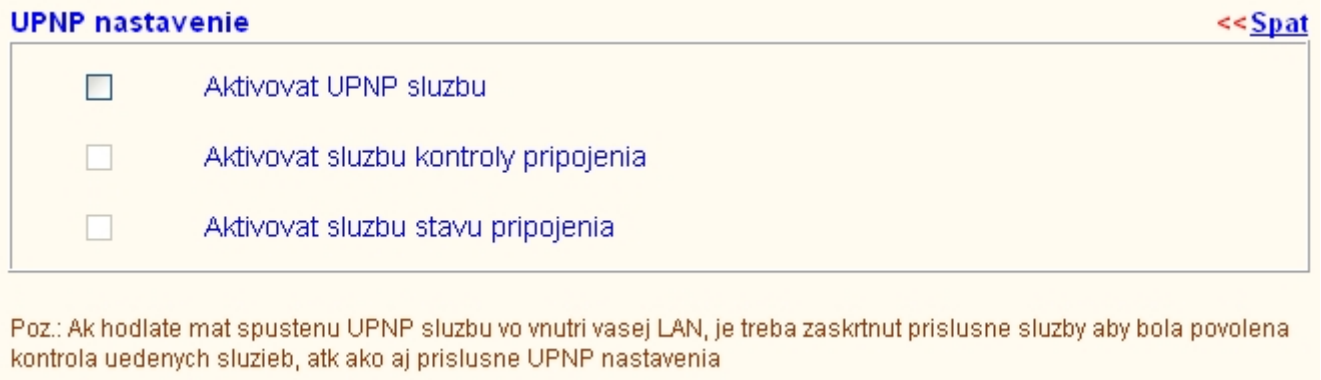
Nastavenia TCP/IP siete

Nasledujúce nastavenia sú požadované pri niektorých LAN-to-LAN operáciách.

- **Moja WAN IP**: Vo väčšine prípadov môžete nechať pôvodné nastavenie v tejto položke, a to 0.0.0.0. Router získa WAN IP adresu od vzdialenej strany počas IPCP overovacej fázy. Ak je WAN IP adresa fixne daná vzdialenou stranou, zadajte sen danú hodnotu.
- **IP vzdialenej brány:** Zadajte IP adresu vzdialeného routra. Nastavuje iba ak je na druhej strany iný router ako Draytek Vigor
- **IP vzdialenej siete**: Zadajte sieťovú identifikáciu vzdialenej siete.
- **Maska vzdialenej siete**: Zadajte sieťovú masku vzdialenej siete.
- **RIP smerovanie**: Špecifikovanie smerovania RIP paketov cez WAN spojenie. RIP – Routing Information Protocol – Routovací Informačný Protokol.
- **RIP verzia**: verzia RIP protokolu

Vzhľadom k popisom v kapitole by nastavenie v našom prípade vyzeralo nasledovne.

5.8 UPnP služba



Táto služba sa aktivuje vtedy ak ju podporuje softvér na PC pripojený k routru a operačný systém.

5.9 VoIP nastavenia

Prenos hlasu cez IP (VoIP) je nový trend prenosu hlasových služieb po sieťach IP. Táto konvergencia hlasových a dátových služieb si vyžaduje používanie nových protokolov a typov signalizácie. Pre prenos hlasu sú najviac používané SIP, H.323, MGCP protokoly. Tieto protokoly nie sú voči sebe vždy kompatibilné. Router 2600VGST zatiaľ podporuje len populárny protokol SIP. Tento protokol nahrádza protokol H.323. SIP protokol podporuje volanie peer-to-peer a môže volať aj cez SIP proxy server (podobná funkcia ako gatekeeper pri sieťach H.323). Neskôr bude nasledovať podpora protokolu MGCP s architektúrou slave-master a v poslednej rade bude implantovaný protokol H.323.

Volanie v IP sieti je podobné ako v telefónnej komutovanej PSTN. Hlasový tok je prenášaný pomocou Real-Time Transport Protocol (RTP) a vložených kodekov. Vigor podporuje typy G.711 A-law, G.711 mu-law, G.729 A & B, G.723.1 a G.726. Každý z týchto kodekov má iné nároky na šírku pásma, a tým aj na kvalitu hlasu. Tá je teda závislá aj na užívateľskej ADSL prípojke, zvlášť na rýchlosti up-stream.

V tejto časti budú vysvetlené základné funkcie VoIP a ich nastavenie na smerovači.

5.9.1 Nastavenie funkcie VoIP

V hlavnej ponuke, sekcii **Advanced Setup** kliknite na položku **VoIP Setup**.

Otvorí sa konfiguračná ponuka VoIP.

5.9.2 Telefónny zoznam

Konfiguracia rychlej volby << Spat

Index	Telefonne cislo	Zobrazovane meno	SIP URL	Stav
1.	21	85492	85492@sip.vvn.telecom.sk	v
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x
11.				x
12.				x
13.				x
14.				x
15.				x
16.				x
17.				x
18.				x
19.				x
20.				x

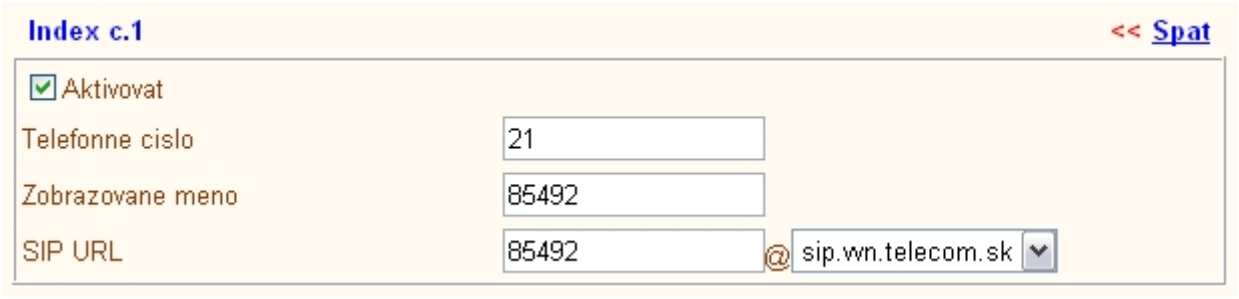
>>Next

Stav:v --- Aktivny, x --- Neaktivny, ? --- Prazdny

NOTE: Stav Pokiaľ je položka neaktívna (Aktivovat nie je zaškrtnutý), je zobrazený znak X. Pokiaľ je aktívna, je zobrazený znak V.

V okne je zobrazený telefónny zoznam s položkami 1,2,3…..60.

Pre nastavenie napr. položky č.7 zoznamu, kliknite na Index č.7



Zobrazia sa políčka pre editovanie položky telef. zoznamu.

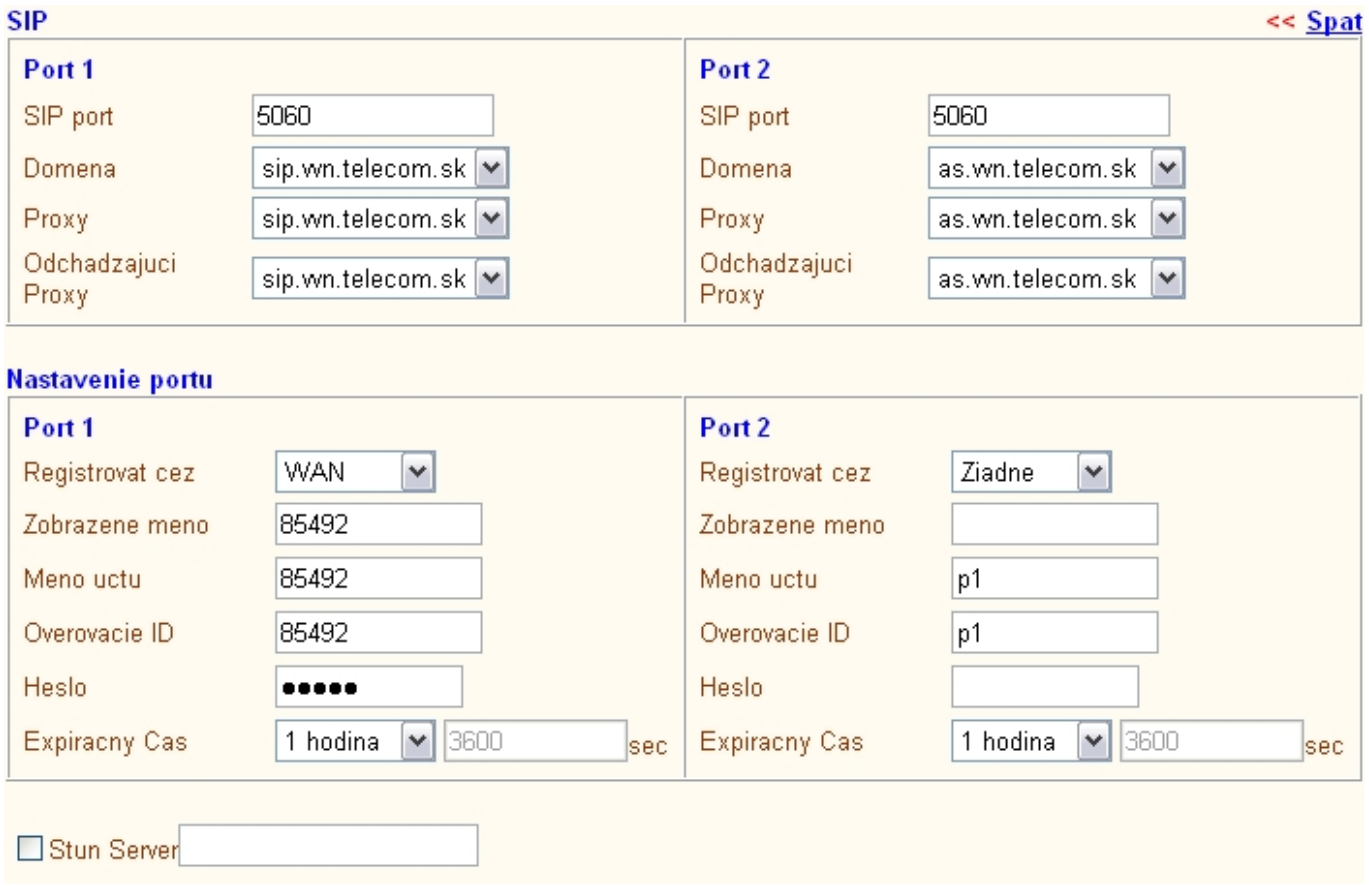
- Aktivovať: Umožňuje aktiváciu a zobrazenie telef. čísla v telef. zozname, pod ktorým vytočíte účastníka.

- Telef. číslo: Ľubovoľné číslo, ktoré si zvolíte pre rýchlu voľbu účastníka. Môžete použiť číslice 0-9 a znak *. Pozn.: pokiaľ zadáte číslo, ktoré už je v telef. zozname uvedené, systém nedovolí vašu novú položku uložiť.

- Zobrazovaný názov: Hodnota v tomto políčku sa zobrazí na LCD displeji volaného účastníka(za predpokladu že telefónny prístroj volaného účastníka má LCD display, a podporu pre CLIP protokoly DTMF a FSK).

- SIP URL: Prvé políčko vyplňte menom (pokiaľ sa používa SIP protokol), alebo číslom. Toto číslo alebo meno musí byť totožné s údajom mena portu uloženom u volaného účastníka v položke „SIP Related Functions Setup/ Port Setting/ Port 1 (alebo Port 2)“. Druhé políčko obsahuje adresu SIP servera, na ktorom je zaregistrovaný volaný účastník.

5.9.3 Nastavenie funkcií SIP



SIP port: Je to číslo portu pre odosielanie / príjem SIP správ v procese vytvárania spojenia. Prednastavená hodnota je 5060 a vy ju môžete kedykoľvek zmeniť na inú hodnotu, ale pamätajte, že spolupracujúca strana musí mať nastavené zhodné číslo portu.

Doména: Obsahuje výber pevne definovaných SIP serverov. Samozrejme, pred prvým použitím sa musíte najprv na serveri zaregistrovať a vytvoriť svoj účet.

Proxy: Obsahuje výber pevne definovaných Proxy SIP serverov.

Odchádzajúci PROXY: Obsahuje výber pevne definovaných Proxy SIP serverov pre odchádzajúce hlasové služby.

Registrovať cez: Môžete si zvoliť cez ktoré rozhranie sa budete registrovať na SIP server. Vigor2600VGST zaregistruje na SIP serveri cez zvolené rozhranie a vy potom môžete využívať služby poskytované daným serverom.

Doporučená hodnota : WAN

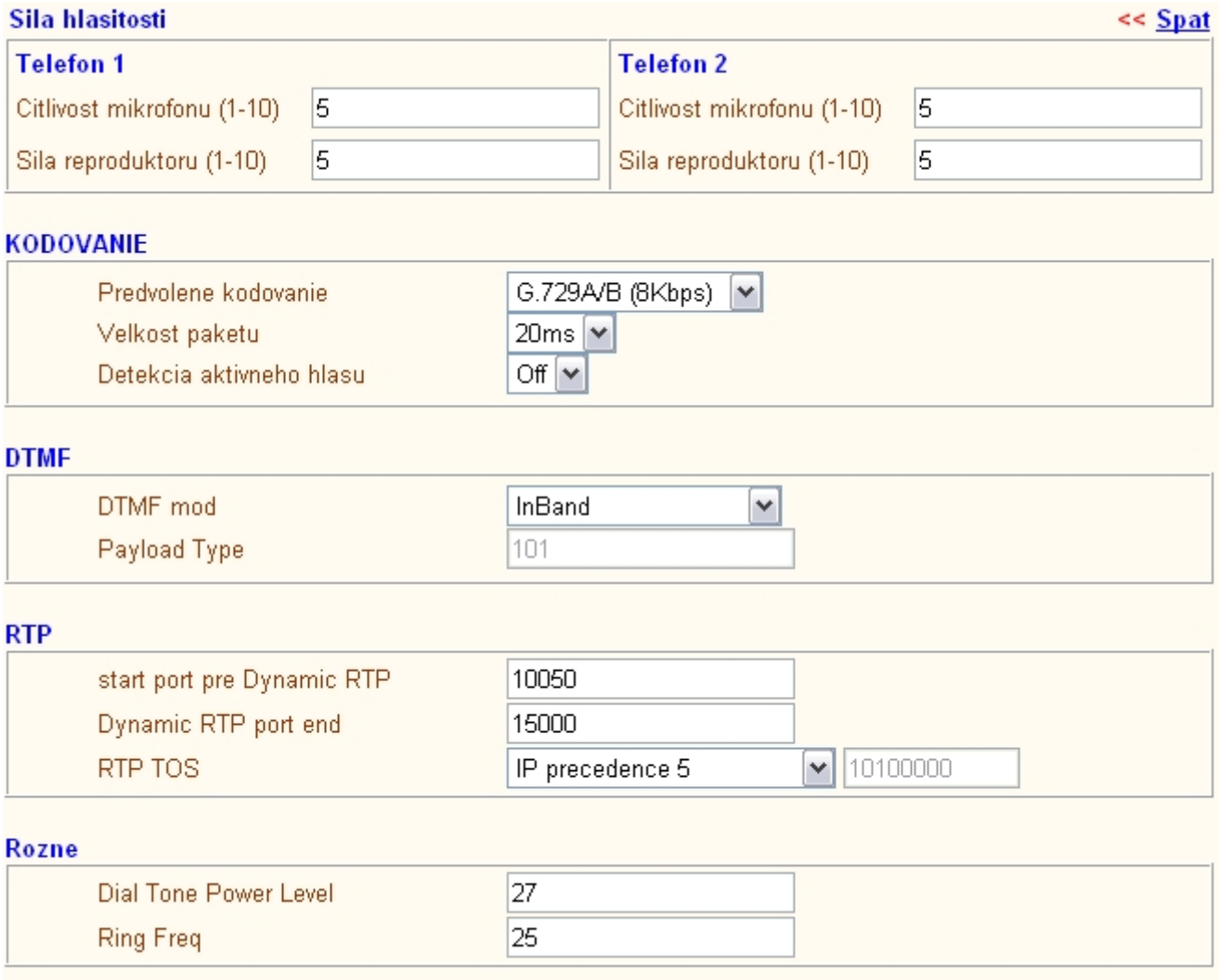
Meno účtu: Pomenovanie portu vo Vigor2600VGST a zároveň názov zaregistrovaného účtu na SIP serveri, ktoré je súčasťou SIP URL pri volaní. Toto meno musí byť taktiež uložené v rovnakom znení v telefónnom zozname (Dial Plan), v prvej položke „SIP URL“ vzdialeného účastníka, ktorý vám bude volať.

Overovacie ID: súčasť overovania zaregistrovaného účtu na SIP serveri.(Poskytne Váš ISP).

Heslo: Vložte heslo, ktoré ste obdržali pri registrácii na SIP serveri. Položku ponechajte prázdnu, pokiaľ nepoužívate registráciu na SIP serveri.

Expiračný čas: Doba vypršania platnosti registrácie, t.j. doba, na ktorú bude zaregistrovaná Vaša požiadavka. Po uplynutí doby platnosti musí Vigor2600VGST odoslať novú požiadavku o registráciu na dobu, ktorá je nastavená v tejto položke.

5.9.4 CODEC / RTP / DTMF - nastavenie



Kódovanie

Predvolené kódovanie: Ako prednastavený sa dá zvoliť jeden z piatich typov kodekov, t.j. ten, ktorý bude prednostne požadovaný pri vytváraní nového spojenia. Pred každým novým spojením sa však obe zariadenia dohodnú na type kodeku, ktorý budú pre dané spojenie používať.

Od výrobcu je prednastavený kodek G.729 A/B (8kbps), ktorý zaberá pomerne malé spektrum (len 8 kbit/s) a pritom je dosahovaná pomerne dobrá kvalita hlasu.

V našich podmienkach ADSL Home pripojenia je výhodnejšie použiť kodek G.723 (6,4kbit/s).

Pozn.: Kodek je prevodník analóg. signálu na digitálny a naopak.

Veľkosť paketu: Nastavená hodnota vyjadruje veľkosť paketu, ktorý obsahuje hlasové dáta za nastavenú dobu v milisekundách. To znamená, že každých 20 milisekúnd je odoslaný paket, ktorý obsahuje hlasové dáta za danú dobu. Jeho veľkosť je daná taktiež použitým kodekom.

Tabuľka veľkosti dátovej hlasovej zložky paketu v závislosti na type kodeku a doby odosielania:

	G.711 MU (64kbit/s)	G.711 A (64kbit/s)	G.726 (32kbit/s)	G.729 A/B (8kbit/s)	G.723 (6,4kbit/s)
10 ms	80 Byte	80 Byte	40 Byte	10 Byte	8 Byte
20 ms	160 Byte	160 Byte	80 Byte	20 Byte	16 Byte
30 ms	240 Byte	240 Byte	120 Byte	30 Byte	24 Byte
40 ms	320 Byte	320 Byte	200 Byte	40 Byte	32 Byte
50 ms	400 Byte	400 Byte	280 Byte	50 Byte	40 Byte
60 ms	480 Byte	480 Byte	320 Byte	60 Byte	48 Byte

DTMF

InBand (Tónová voľba v kanále): Vigor2600VGST prenáša DTMF okamžite po stlačení tlačítka na telefóne ako hlasovú zložku vo vytvorenom kanále. DTMF voľba zaberá rovnaké spektrum ako hlas.

OutBand (Tónová voľba mimo kanál): Vigor2600VGST prenáša DTMF ako kód odpovedajúci volenému číslu. V procese detekcie dekóduje tóny, ktoré prenesie na druhú stranu a tam prijímač opäť vygeneruje dané tóny. Tento postup je výhodný tam, kde je malý prietok paketov, pretože zaberá minimálne spektrum a kvalita voľby je dokonalá.

Payload Type (Hodnota vyťažovania linky): Zvoľte číslo medzi 96 až 127. Prednastavená hodnota je 101.

RTP

Špecifikuje začiatočný a koncový port pre RTP (prenosový protokol pre prenos dát v reálnom čase), ktorý je používaný pre prietok hlasových paketov. Prednastavené hodnoty sú 10050 pre začiatok a 15000 pre koniec.

5.10 VLAN a obmedzenie prietoku

VLAN je skratkou pre "Virtual LAN". V systéme spínaných sietí sú broadcast pakety, alebo pakety s neznámou MAC adresou, posielané na všetky porty. To výrazne znižuje výkon dátových sietí. Po združení fyzických portov do VLAN, sa broadcast pakety posielajú len v rámci danej VLAN, čo neovplyvní výkon ostatných fyzických portov patriacich do iných VLAN. Oblasti vysielania jednotlivých VLAN sú navzájom nezávislé a preto všetky pakety ľubovoľného fyzického portu z jednej VLAN neprechádzajú do iných VLAN. Jedna VLAN môže združovať viac portov (viac portov môže patriť do jednej VLAN). Jeden port môže byť zdieľaný medzi niekoľkými VLAN (jeden port môže patriť do viac VLAN). VLAN výrazne zvyšuje efektivitu a bezpečnosť siete.

Funkcia riadenia dátového prietoku umožňuje nastaviť dátový prietok pre konkrétny fyzický port v smere von i dovnútra. Túto funkciu môžeme využiť v prípadoch, kedy potrebujeme zamedziť monopolnému využitiu prietoku z jedného portu (napríklad hraním on-line hier, sťahovaním enormne veľkých súborov a podobne). Ďalšie využitie tejto funkcie je v možnosti rozdelenia prenosového výkonu na každý port nezávisle.

5.10.1 VLAN Konfigurácia

Zapnúť: zaškrtnutím aktivujeme funkciu VLAN.

U routra Vigor2600VGST sú k dispozícii 4 skupiny VLAN: VLAN0/ VLAN1/ VLAN2/ VLAN3. Označením portu určíme do ktorej skupiny VLAN bude patriť. Tzn., že v prípade, kedy nebudú označené žiadne porty, budú všetky patriť do rovnakej skupiny VLAN a môžu komunikovať s WAN portom. Pokiaľ však bude označený minimálne jeden port, znamená to, že iba tento je zaradený do skupiny VLAN a iba tento má prístup na WAN port. Ostatné nedefinované porty strácajú povolenie komunikovať s WAN portom. Komunikáciu s WAN portom získavajú potom len definované porty priradené k VLAN.

P1: LAN port 1.

P2: LAN port 2.

P3: LAN port 3.

P4: LAN port 4.

5.10.2 Obmedzenie prietoku

Zapnut: zaškrtnutím aktivujeme funkciu riadenia prietoku. Pre každý z LAN portov (P1, P2, P3 a P4) je možnosť zvoliť hornú hranicu prietoku dát nezávisle v oboch smeroch. Označením políčka IN, alebo Out, voľbou rýchlosti Rate a potvrdením OK sa dá nastaviť a uložiť riadenie prietoku u každého portu.

Von: označením sa aktivuje riadenie prietoku LAN portu smerom von (upload) na WAN port.

Dnu: označením sa aktivuje riadenie prietoku LAN portu smerom dovnútra (download) z WAN portu.

Prietok: Zadávajte požadovanú hornú hranicu prietoku. Zadaná hodnota musí byť násobkom 32 (napr. 32, 64, 96, 128 ...), nie však viac ako 100 000. Zadané číslo predstavuje maximálny prietok portom a je udávaný v jednotkách kbit/s (t.j. 1000 bitov za sekundu).

5.11 QoS nastavenia

Quality of Service (**QoS**) – Kvalita služby, je tým myslená schopnosť siete doručiť dáta s minimálnym oneskorením a sieťové metódy používané k poskytnutiu prietoku pre real-time multimediálne aplikácie.

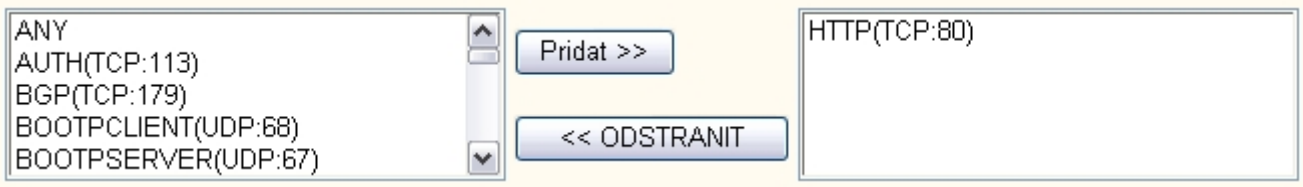
Draytek QoS povoľuje užívateľom kontrolovať prenos dát cez porty. Prenosový prietok router zatrieďuje do štyroch prenosových tried. Každá trieda má svoju vlastnú prioritu, rezervovanú podielom prietoku, pričom užívateľ môže definovať prvé tri triedy podľa svojich požiadaviek, teda prideliť vyššiu prioritu pre niektoré, na oneskorenie citlivé, aplikácie, ako napr. rezervovať prietok pre použitie hlasového prenosu VoIP atď.

ADSL Router Vigor2600VGST, sám automaticky zisťuje prietok a vypočíta príslušnú hodnotu prietoku dát smerom von a dnu.

Prosím všimnite si, že QoS má rozšírené nastavenia prideľované pre lokálnu LAN, preto nezávisí či je klasifikovaný prietok smerom dnu alebo von, zdrojovú IP v rozšírenom nastavení je potrebné nastaviť ako lokálnu LAN IP.

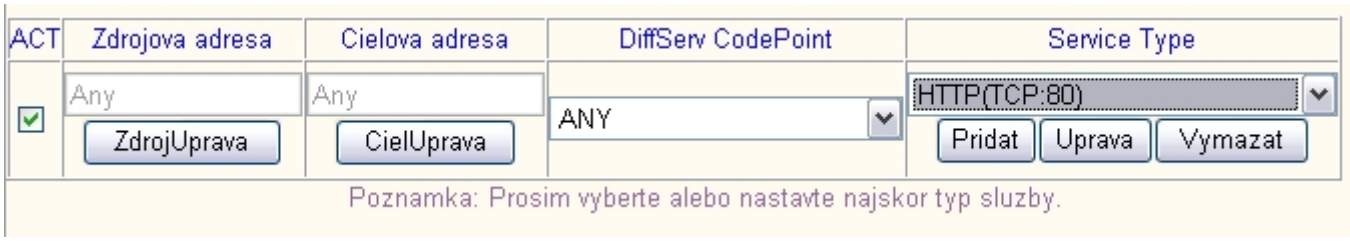
Napríklad, ak potrebujeme zatriediť 10% prietoku pre http prenos smerom dnu (napr. sťahovanie súborov) pre lokálne PC 192.168.1.10, nastavíme takto:

1) pridajte HTTP (TCP : 80) cez QoS základné nastavenia.



2) Vložiť pravidlo ako zdrojovú IP 192.168.1.10 cez QoS rozšírené nastavenia.

(Je nesprávne ak nastavíte 192.168.1.10 ako cieľovú IP)

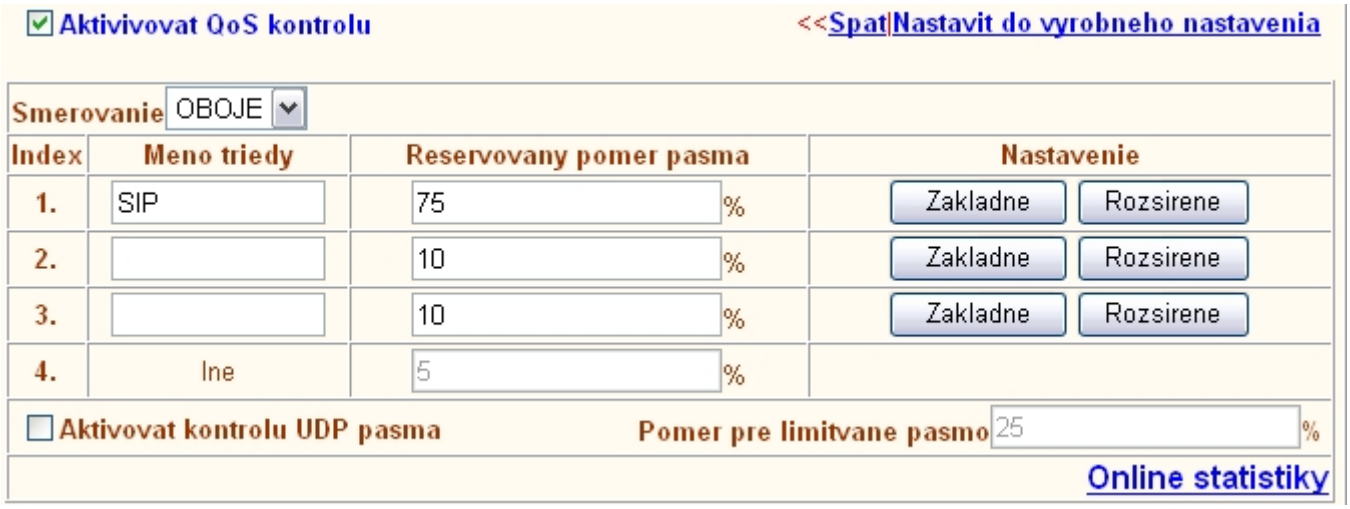


DrayTek Vigor 2600VGST už má implementované nastavenie Vysokej priority pre vstavaný VoIP prenos od výroby. Preto odporúčame len ponechať "QoS" aktivované pre zabezpečenie najvyššej kvality prenosu hlasu.

Nastavenie QoS VoIP SIP prietoku pre VoIP aplikácie v sieti :

VoIP aplikácie sú široko používané v spoločnosti ABC, preto je VoIP prenosu vždy pridelená taká šírka pásma, akú potrebuje. Môžeme roztriediť SIP VoIP prenos (prechádzajúci cez Vigor) s vyšším pomerom šírky pásma vo Vigor QoS nastavení.

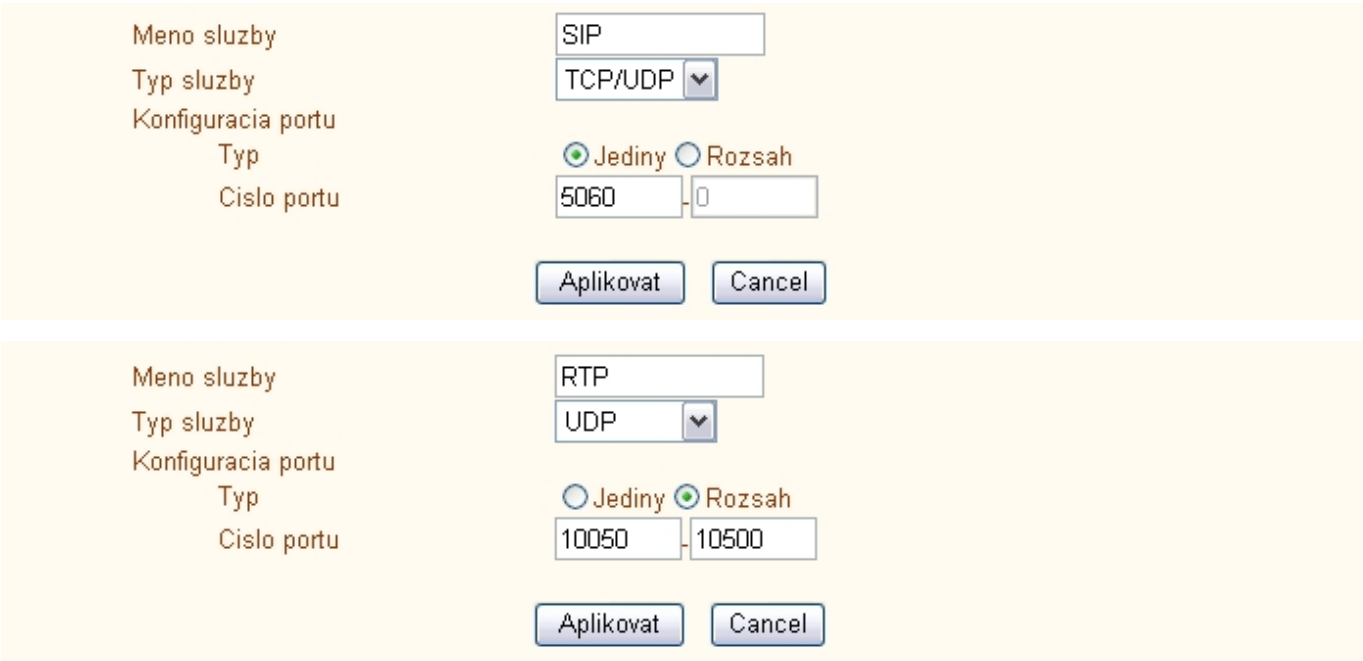
1. Aktivujte QoS kontrolu, vyberte smer "oboje" a určite pomer šírky pásma, ktorý by ste chceli rezervovať pre SIP VoIP prenos.



2. SIP protokol (UDP:5060) nie je definovaný v QoS základnom nastavení, preto je potrebné pridať nový typ služby cez QoS rozšírené nastavenia.

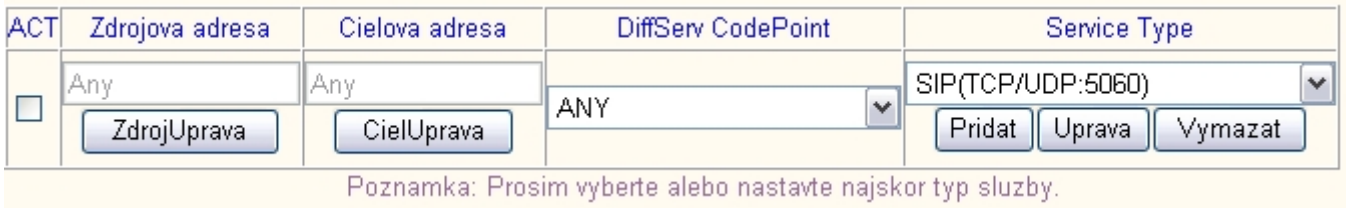
3. RTP (real-time transport protocol), ktorý je používaný pre poskytovanie end-to-end sieťových prenosových funkcií, vhodných pre aplikácie real-time prenosu dát, tak ako audio, video alebo simulované dáta. Tiež nie je definovaný v QoS základných nastaveniach, preto je potrebné pridať nový typ služby cez QoS rozšírené nastavenia.

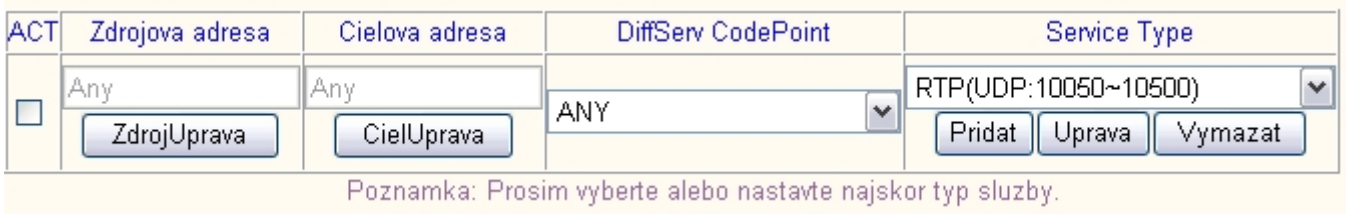
4. Vložte názov služby, vyberte typ služby a definujte čísla portu.



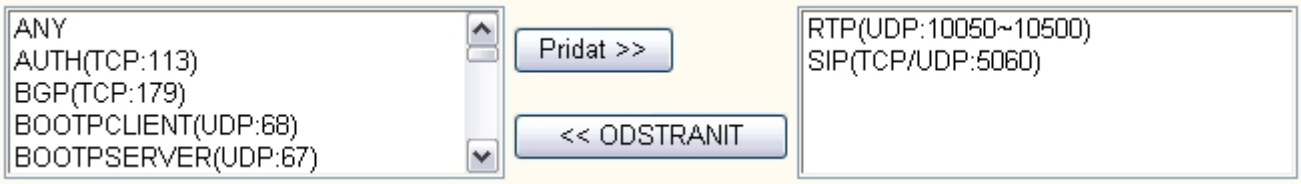
Prosím, všimnite si: UDP 10050 port do UDP 15000 port je RTP port špecifikovaný Vigorom, ostatné VoIP zariadenia môžu mať svoju vlastnú definíciu RTP portu.

4. Potom môžete vybrať nový typ služby a aktivovať pravidlo.



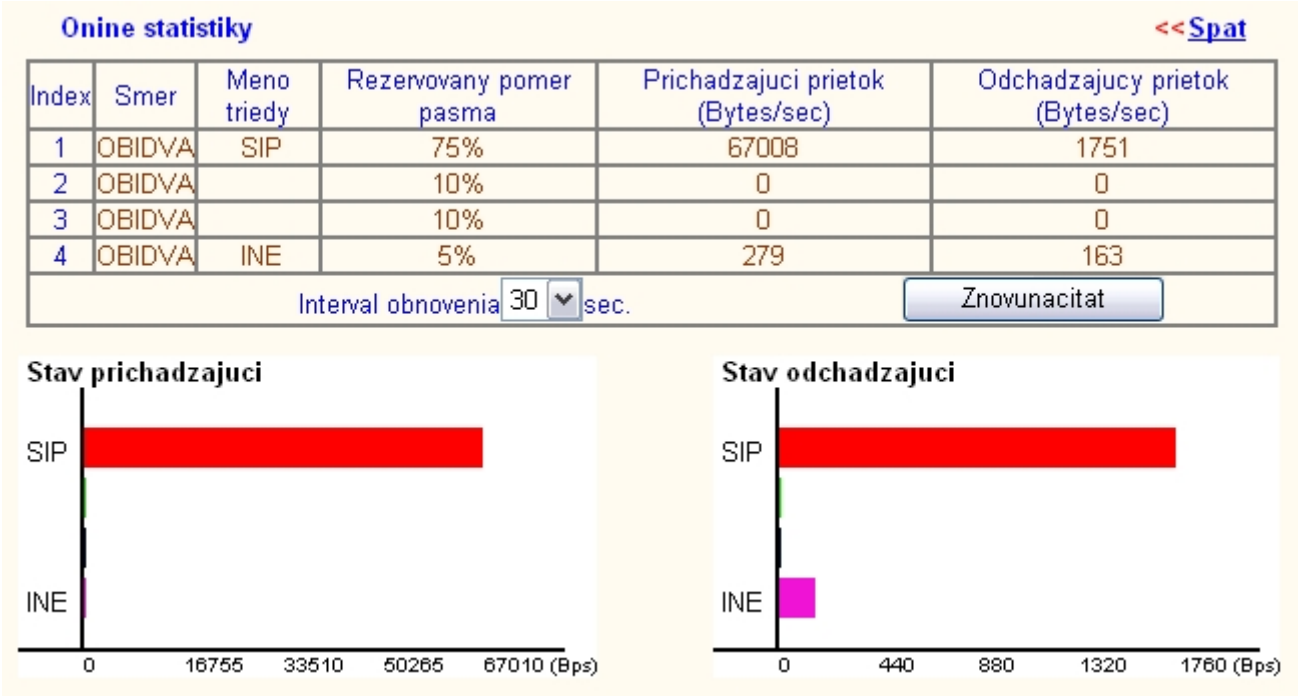


5. Skontrolujte, či SIP(UDP:5060) a RTP(UDP:10050~15000) sú pridané v QoS základných nastaveniach.



6. Teraz si môžeme pozrieť stav QoS šírky pásma v QoS Online štatistike.

Je potrebné poznamenať ešte jednu vec - UDP port 5060 je používaný iba pre založenie spojenia, preto ak potrebujeme kontrolovať plný VoIP prenos, potrebujeme do tejto triedy pridať reálne používané porty (obyčajne dynamické porty).



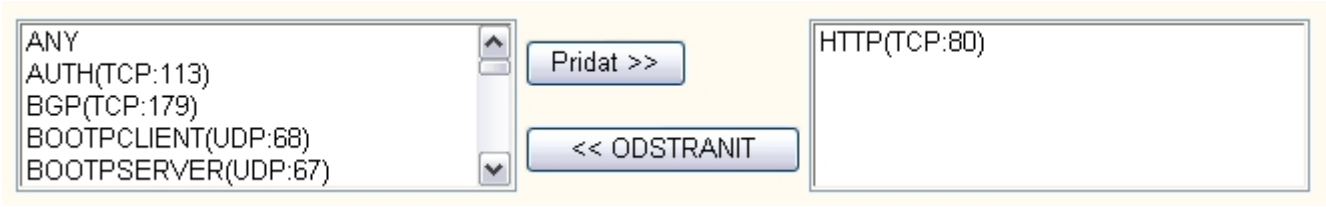
Nastavenie QoS pre http a e-mail prenos :

Janina e-mailová príloha je dôležitá zmluva a Dávidov súbor na stiahnutie je počítačovou hrou, je samozrejmé, že Dávid môže počkať dlhší čas, pretože to má pre firmu nízku prioritu.

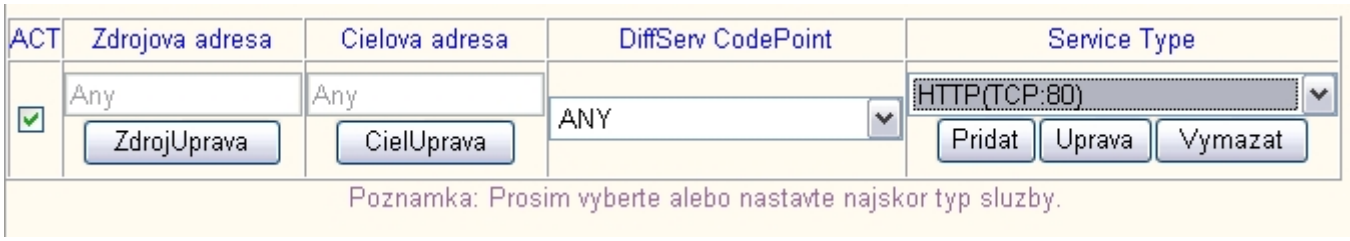
V prípade, že môžeme nastaviť limit http sťahovania na nízku prioritu - 10% a sťahovanie e-mailov na vyššiu prioritu - 50% postupujte nasledovne:

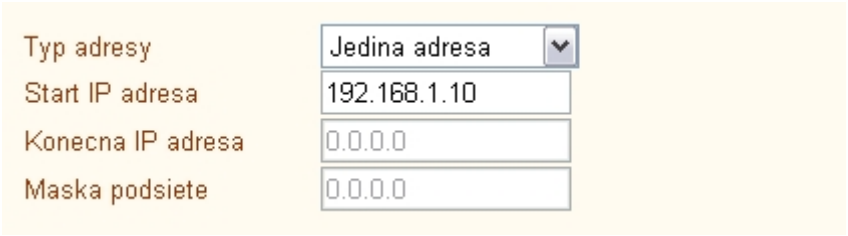
1. Aktivujte QoS kontrolu, vyberte "IN" a určite pomer šírky pásma, ktorý by ste chceli rezervovať pre typy služieb v QoS kontrolnom nastavení.

2. Pridajte http(TCP:80) typ služby do deliaceho indexu 1 (class index 1) v základnom.

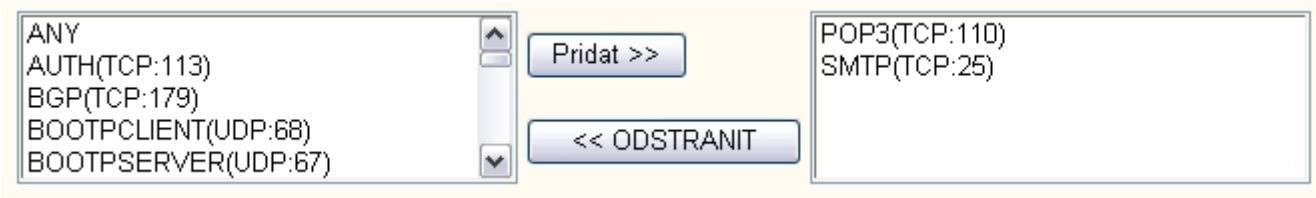


3. Upravte existujúce pravidlo v rozšírenom nastavení. Potrebujeme zmeniť zdrojovú IP adresu z „ANY“ na 192.168.1.10 (IP adresa Dávidovho počítača) v tomto príklade.

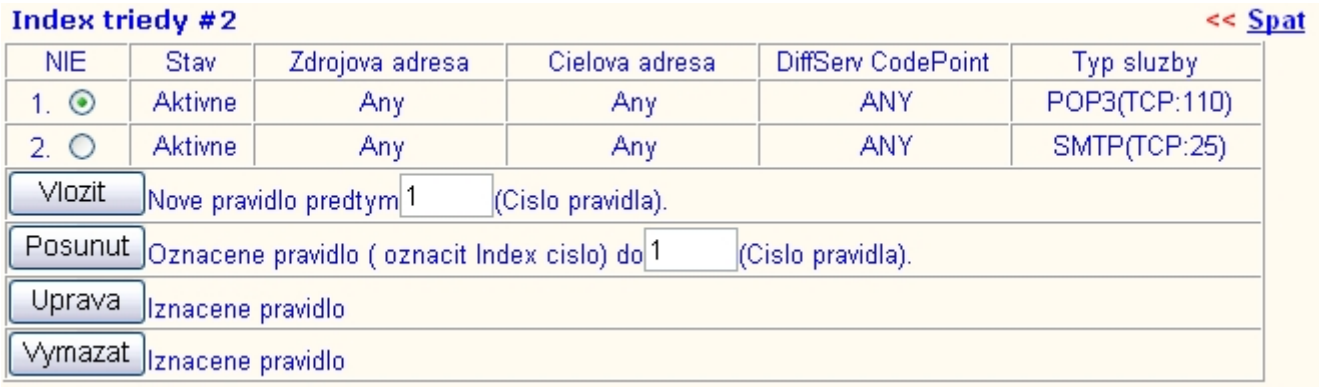




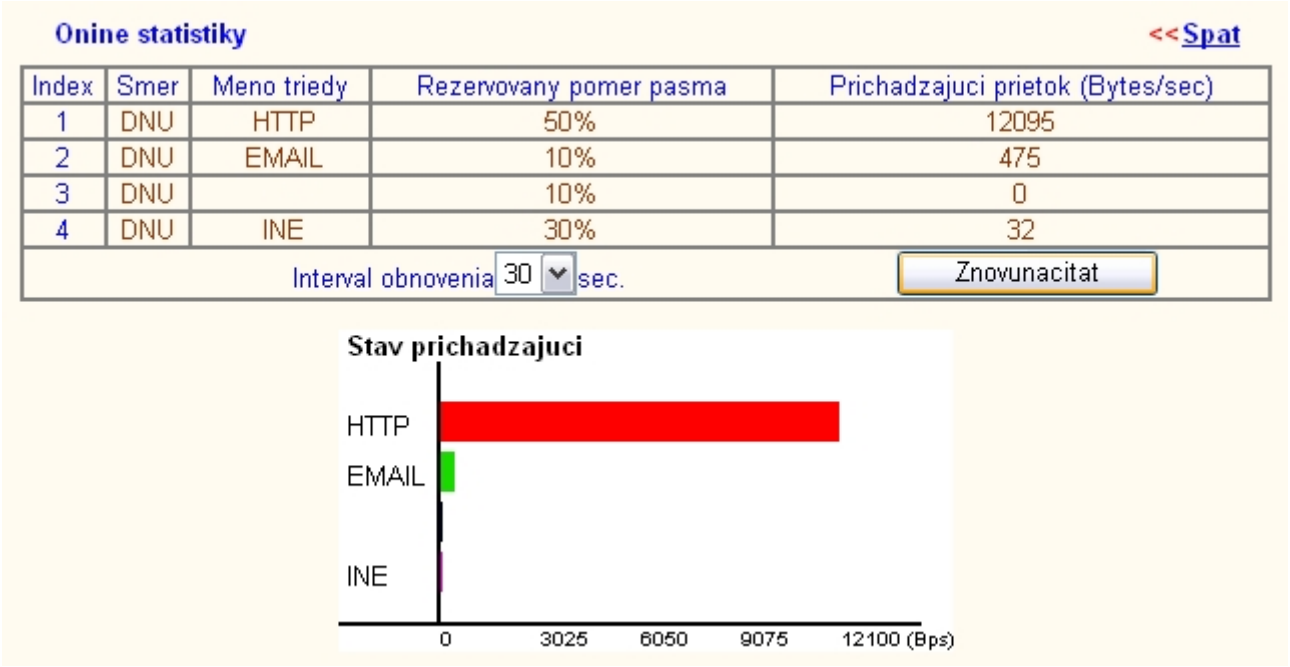
4. Pridajte POP3(TCP:110) a SMTP(TCP:25) typy služieb do deliaceho indexu 2 (class index 2) v základnom nastavení.



5. Upravte existujúce pravidlo v rozšírenom nastavení. Potrebujeme zmeniť zdrojovú IP adresu z „ANY“ na 192.168.1.11(IP adresa Janinho počítača) v tomto príklade.



6. Teraz si môžeme pozrieť stav šírky pásma v QoS Online štatistike. (Ak nie je zaplnená šírka pásma pre e-mailovú službu, ľavá šírka pásma bude pridelená pre ostatné služby.)



Nastavenie QoS pre VPN prietok :

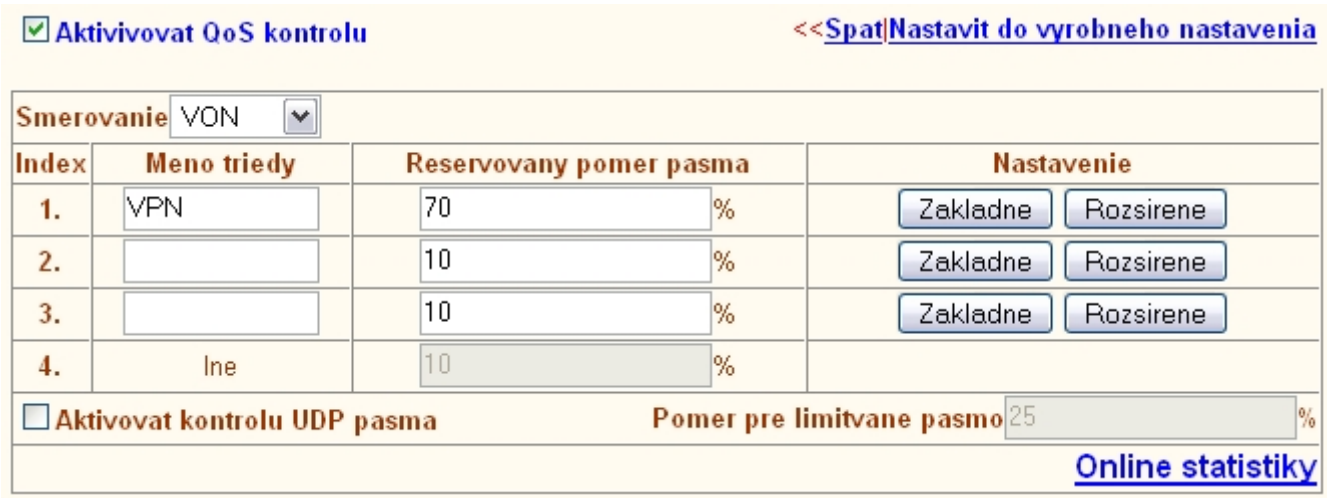
Krok 1: Prosím, najprv si pozrite nasledujúci príklad nastavenia LAN to LAN VPN.

Krok 2: Nastavte QoS

Vložte šírku pásma WAN prietoku dnu/von.

Špecifikujte názov triedy a rezervovaný pomer šírky pásma.

Kliknite na tlačidlo "Advance".



Upravte lokálnu podsieť ako zdrojovú adresu a vzdialenú podsieť ako cieľovú adresu.

ACT	Zdrojova adresa	Cielova adresa	DiffServ CodePoint	Service Type
☑	192.168.15.0(mask ZdrojUprava	192.168.3.0(mask: CielUprava	ANY	ANY Pridat Uprava Vymazat

Poznamka: Prosim vyberte alebo nastavte najskor typ sluzby.

Index triedy #1 << Spat

NIE	Stav	Zdrojova adresa	Cielova adresa	DiffServ CodePoint	Typ sluzby
1. ◉	Aktivne	192.168.15.0(mask:255.255.255.0)	192.168.3.0(mask:255.255.255.0)	ANY	ANY

Vlozit Nove pravidlo pred 1 (Cislo pravidla).

Posunut Oznacene pravidlo (oznacit Index cislo) do 1 (Cislo pravidla).

Uprava Oznacene pravidlo

Vymazat Oznacene pravidlo

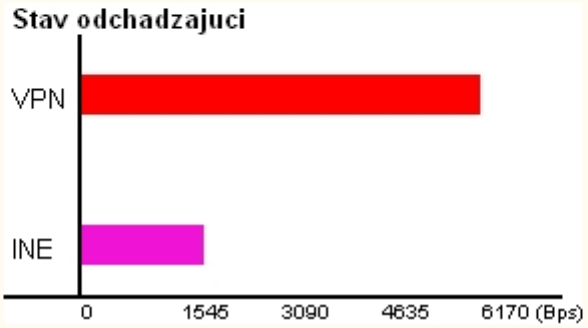
Teraz si môžete pozrieť stav šírky pásma v QoS Online štatistike.

(Ak nie je rezervovaná šírka pásma pre VPN prenos plne používaná, ľavá šírka pásma bude pridelená ostatným službám.)

Onine statistiky <<Spat

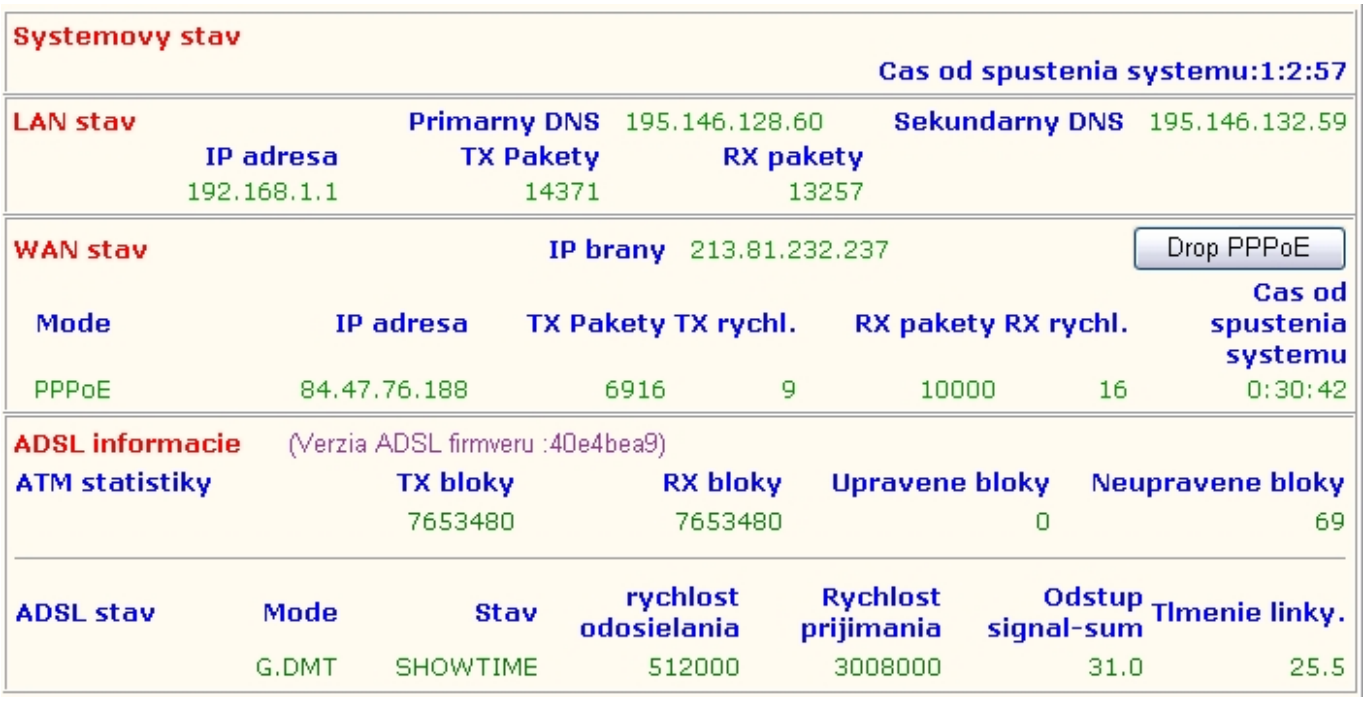
Index	Smer	Meno triedy	Rezervovany pomer pasma	Odchadzajucy prietok (Bytes/sec)
1	VON	VPN	70%	6161
2	VON		1%	0
3	VON		1%	0
4	VON	INE	28%	1901

Interval obnovenia 5 sec. Znovunacitat



6.1 Online Stav

Kliknite na ponuku "**Online Stav**". V zobrazenom príklade je stav LAN, WAN, ADSL.



Systemovy stav

Cas od spustenia systemu:1:2:57

LAN stav — Primarny DNS 195.146.128.60 — Sekundarny DNS 195.146.132.59

IP adresa	TX Pakety	RX pakety
192.168.1.1	14371	13257

WAN stav — IP brany 213.81.232.237 — Drop PPPoE

Mode	IP adresa	TX Pakety	TX rychl.	RX pakety	RX rychl.	Cas od spustenia systemu
PPPoE	84.47.76.188	6916	9	10000	16	0:30:42

ADSL informacie (Verzia ADSL firmveru :40e4bea9)

ATM statistiky	TX bloky	RX bloky	Upravene bloky	Neupravene bloky
	7653480	7653480	0	69

ADSL stav	Mode	Stav	rychlost odosielania	Rychlost prijimania	Odstup signal-sum	Tlmenie linky.
	G.DMT	SHOWTIME	512000	3008000	31.0	25.5

Stránka "**On-line Stav**" obsahuje štyri kategórie: " **Systémový stav**"(Systémový stav), "**LAN stav** " (stav LAN), "**WAN stav** " (stav WAN) a **ADSL Informacie** (ADSL informácie)

System status (Stav systému)

- Čas od spustenie systému**:** Čas od spustenie systému

LAN Status (stav LAN):

- **Primary DNS:** IP adresa prvého DNS
- **Secondary DNS:** IP adresa druhého DNS
- **IP Adresa** (IP adresa): IP adresa rozhrania LAN1.
- **TX Packets**: celkový počet prenesených IP paketov poslaných počas aktivity routra (aktivitou sa myslí, že router bol zapnutý v napájaní).
- **TX Rate:** prenosová rýchlosť odchádzajúcich dát. Jednotkou je cps (character per second) čiže znak za sekundu.
- **RX Packets**: celkový počet prijatých IP paketov počas aktivity routra.
- **RX Rate**: : celkový počet prijatých IP paketov počas aktuálneho pripojenia.

WAN Status (stav WAN):

- **GW IP Addr**: zobrazuje IP adresu brány (gateway).
- **Mode** (režim): zobrazuje, ktorý širokopásmový prístupový režim je aktívny. V závislosti od širokopásmového prístupového režimu môžete vidieť PPPoE, PPPoA, alebo MPoA.
- **IP Address** (IP adresa): IP adresa rozhrania WAN.
- **TX Packets**: celkový počet prenesených IP paketov počas aktuálneho pripojenia.
- **TX Rate**: prenosová rýchlosť odchádzajúcich dát. Jednotkou je cps (character per second) čiže znak za sekundu.
- **RX Packets**: celkový počet prijatých IP paketov počas aktuálneho pripojenia.

- **RX Rate**: rýchlosť príjímania pre prichádzajúce dáta. Jednotkou je cps (character per second) čiže znak za sekundu.
- **Up Time**: celkový čas pripojenia vo forme HH:MM:SS (hodiny:minúty:sekundy).
- **Drop PPPoE** (zhoď PPPoE alebo PPTP): kliknutím zrušíte spojenie PPPoE, alebo PPTP. Alebo **Dial PPPoE (Vytočenie PPPoE)**- zobrazí sa ak nie je PPPoE vytočené

ADSL Information (Informácie o ADSL)

- **ADSL Firmvare version**: zobrazuje verziu ADSL firmvéru.

ATM Statistics: Informácie na ATM vrstve

- **TX Blocks:** celkový počet prenesených blokov
- **RX Blocks:** celkový počet prijatých blokov
- **Corrected blocks:** celkový počet upravovaných blokov
- **Uncorrected blocks** : celkový počet neupravovaných blokov

ADSL Status (ADSL stav): Informácie o ADSL

Mode: použitý mód ADSL

State: stav ADSL linky

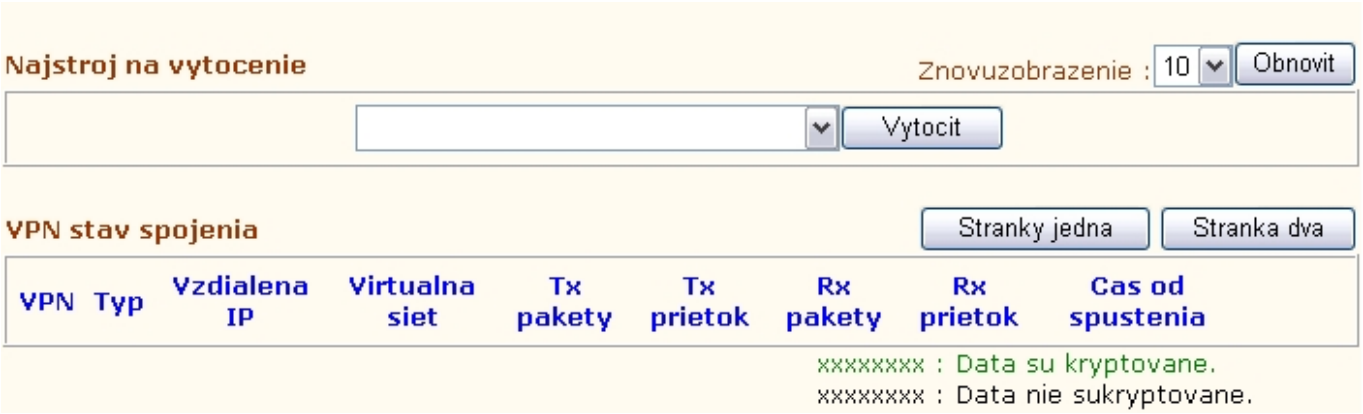
Up speed: max. rýchlosť smerom od routra k DSLAM

Down Speed: max. rýchlosť smerom od DSLAM k routru

SNR Margin: Hodnota odstupu signál-šum

Loop Att.: Hodnota tlmenia linky

6.2 VPN Spojenia



Vytočiť: Možnosť vytočiť VPN spojenie(ak je nakonfigurované).

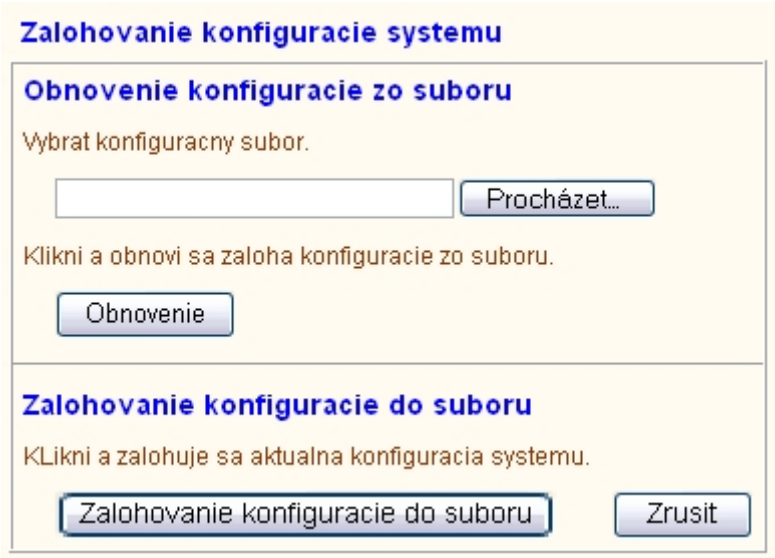
Stav VPN spojenia: Sledovanie stavu VPN spojenia

6.3 Zálohovanie nastavenia

Vybrať konfiguračný súbor: umožní vybrať konfiguračný súbor predchádzajúcej zálohy na disku

Obnoviť: kliknutím aktivuje nastavenie uložené vo vybranom konfiguračnom súbore

Zálohovať: umožní do súboru zálohovať aktuálne nastavenie routra a neskôr ho pomocou obnovenia vyvolať .



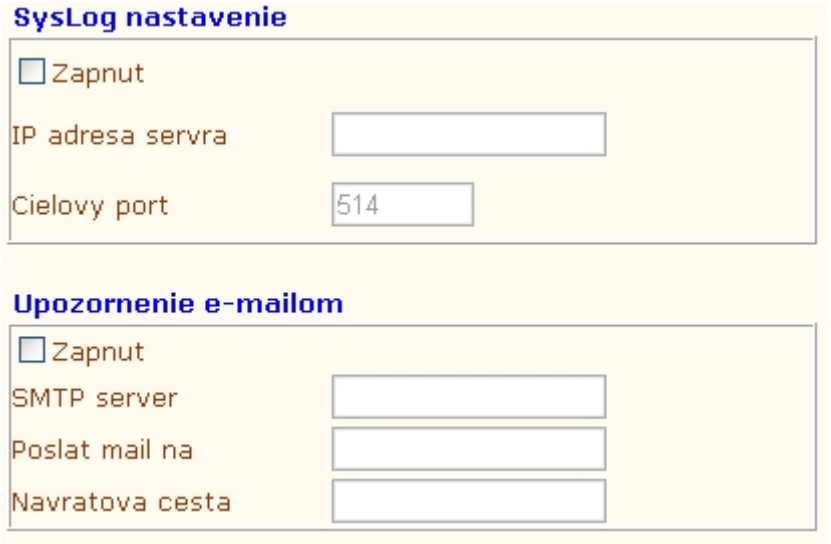
6.4 Zaznamenávanie systému

Spustenie zaznamenávania systému

Zapnuté: Aktivuje zaznamenávanie činnosti routra (je potrebné nainštalovať aplikáciu Router Tools z inštalačného CD, nainštaluje sa softvér SysLog, ktorým môžete tieto záznamy prehliadať)

IP adresa servera: IP adresa počítača a ktorom je nainštalovaná aplikácia SysLog

Cieľový port: komunikačný port



Upozornenie pomocou e-mailu

Zapnuté: aktivuje posielanie správ na e-mail ak dôjde k útoku na router z internetu

SMTP server: SMTP server pre e-maily

e-mail: emailová adresa

6.5 Čas a dátum

Informácie o čase

Získať čas: nastaví čas a dátum routra z operačného systému

Nastavenie času

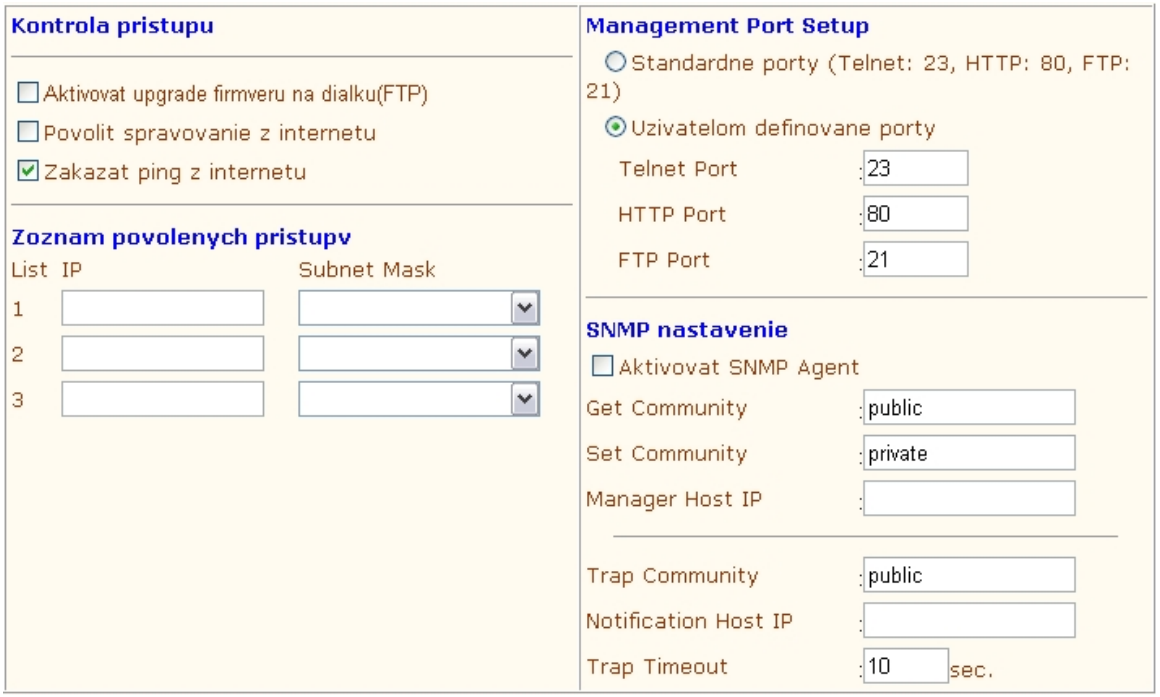
Použiť čas z prehliadača: použije čas a dátum, ktorý získa z PC

Použiť klienta internetového času: zadefinovaním NTP servra a časovej zóny získava router čas v pravidelných intervaloch z časových servrov v internete

6.6 **Management Setup** (Správa systému)

Router može byť konfigurovaný a spravovaný cez akýkoľvek Telnet, alebo Web prehliadač bežiaci pod ktorýmkoľvek operačným systémom. Nemá žiadne obmedzenia pre prídavný operačný systém, či príslušenstvo. Jednako však pre špeciálne prostredia môže byť užitočné zmeniť čísla portov na serveri pre zabudovaý Telnet, alebo HTTP server, vytvoriť prístupový zoznam kôli bezbečnosti, alebo neprijať systémového administrátora prihlasovaného z Internetu.

Kliknite na ponuku "**Správa systému**". Zobrazí sa nasledujúca stránka:



Nastavenie kontroly prístupu

- **Povoliť vzdialený upgrade firwaru (FTP)**: zaškrtnutím povolíte systémovému administrátorovi upgradovať firmware z internetu
- **Povoliť spravovanie z internetu**: zaškrtnutím povolíte systémovému administrátorovi prihlasovanie sa cez Internet. Výrobné nastavenie je "nepovoliť", čiže kolónka nie je zaškrtnutá.
- **Zakázať PING z Internetu**: zaškrtnutím zakážete odpovedať routru na príkaz ping

Zoznam povolených prístupov

Je možné špecifikovať, že systémový administrátor sa môže prihlásiť jedine z preddefinovaného hostiteľa, alebo siete. Maximálne môžu byť definované tri prístupy.

- **Zoznam IP**: zadajte IP adresu, ktorej má byť povolené prihlásenie sa do routra.
- **Maska podsiete**: zadajte masku podsiete, ktorej má byť povolené prihlásenie sa do routra.

Nastavenie riadiacich portov

- **Štandardné porty**: zaškrtnutím tejto možnosti budú použité prednastavené čísla portov pre Telnet a HTTP server.
- **Užívateľom definované porty**: zaškrtnutím budú pre Telnet a HHTP server použité ďalej definované čísla portov.
- **Telnet Port**: vpíšte číslo portu pre Telnet
- **HTTP Port**: vpíšte číslo portu pre HTTP server.
- **FTP Port:** vpíšte číslo portu pre FTP server.

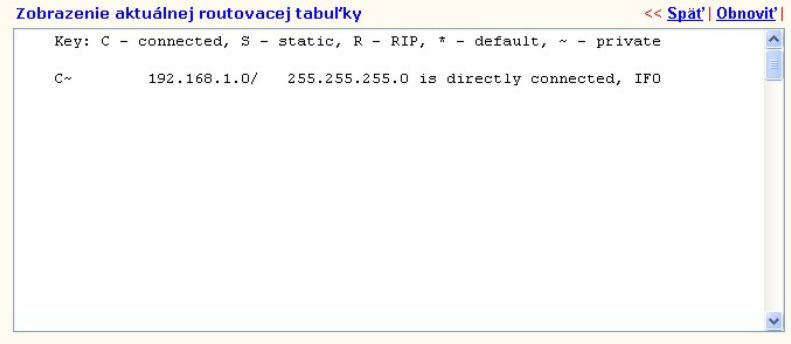
Nastavenie SNMP

- **Povolený SNMP agent**: povolí používanie SNMP agenta

6.7 Diagnostické nástroje

Nástroje diagnostiky zariadenia sú užitočné hlavne pre prezeranie činnosti, alebo diagnostikovanie routra. Kliknutím na ponuku "**Diagnostické nástroje**" sa zobrazí nasledujúca stránka.

PPPoE/PPPoA diagnostika: Kliknite na ponuku "**PPPoE/PPPoA diagnostika**". Nižšie zobrazená stránka má iba referenčný charakter, keďže každá sieť bude zobrazovať svoje individuálne prostredie.



Tabuľka poskytuje náhľad na aktuálne IP routovacích informácií uložených v routri. Vľavo od každého routovacieho pravidla sa nachádza kľúč.

- **C** --- priamo pripojený
- **S** --- statická cesta (static route)
- **R** --- RIP
- ***** --- deafault route

Vpravo sa nachádza identifikácia rozhrania pre to ktoré routovacie pravidlo.

- **IF0** --- rozhranie lokálnej LAN
- **IF3** --- WAN(LAN2) rozhranie

Zobrazenie tabuľky ARP Cache

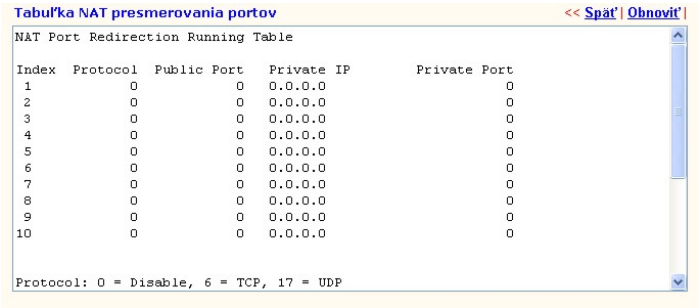
Kliknutím na položku "**Zobrazenie tabuľky ARP Chache**" sa zobrazí ARP vzrovnávací protokol uložený v routri. Tabuľka zobrazuje priraďovanie MAC adries (Ethernet hardwarových adries) a IP adries.

Zobraziť DHCP servrom pridelené IP adresy

Stránka poskytuje informácie o určovaní IP adries, ktoré sú veľmi užitočné najmä pri diagnostikovaní sieťových problémov, ako napríklad konflikty IP adries a podobne.

Zobraziť tabuľku NAT presmerovania portov

Ak je nastavené v ponuke "**NAT prekladanie adries**">>presmerovanie portov"" presmerovanie na porte, kliknutím je možné odkontrolovať požadované nastavenia pre presmerovanie špecifických čísel portov na konkrétnych interných užívateľov.



Zobraziť tabuľku NAT aktívnych spojení

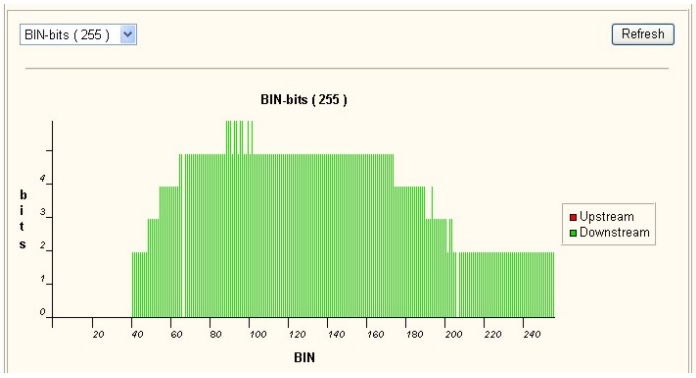
Ak sa router pripája na Internet cez vstavané NAT, kliknutím na položku "**Zobraziť tabuľku NAT aktívnych spojení**" uvidíte, ktoré aktívne vonkajšie spojenie je online.

Každý riadok na obrazovke indikuje aktívne spojenie, pričom sú zobrzené nasledovné informácie:

- **Private IP, Port** (súkromné IP, port): IP adresa interného užívateľa a číslo portu.
- **#Pseudo Port**: číslo verejného portu.
- **Peer IP, Port**: IP adresa vzdialeného užívateľa a číslo portu.
- **Info**: vyjadruje rozhranie, definované nasledovne:
- **0** --- LAN rozhranie
- **3** --- WAN(LAN2) rozhranie

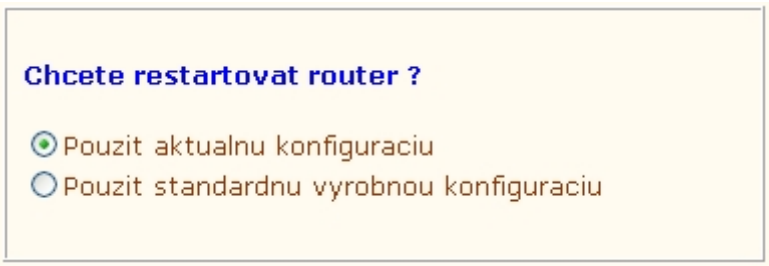
Analýza ADSL sektra

Zobrazí graf analýzy ADSL spektra



6.8 Reštart systému

Cez Web konfigurátor je možné reštartovať router. Kliknutím na položku "**reštart systému**" sa otvorí nasledovná stránka.



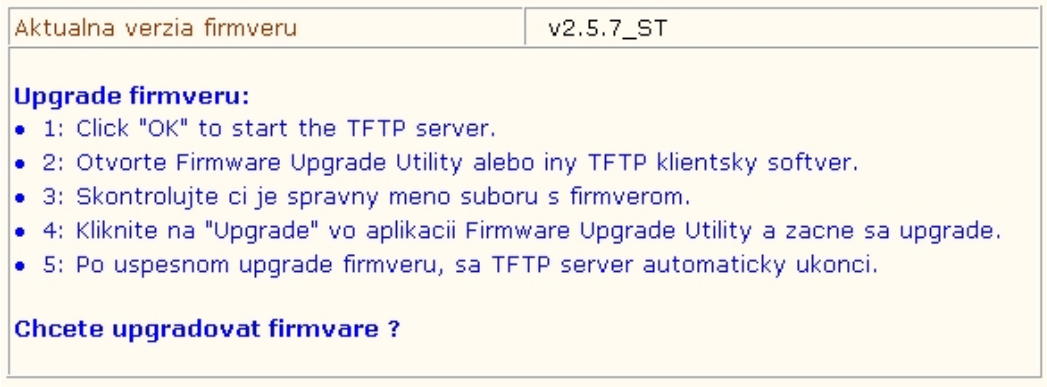
Pri voľbe reštartu máte na výber dve alternatívy: „**Použiť aktuálnu konfiguráciu**", alebo "**Použiť štandardnú konfiguráciu**". Podľa vlastnej potreby zaškrtnite vybranú alternatívu a kliknite na "**OK**". Do 3 až 5 sekúnd bude router reštartovaný.

6.9 TFTP Server

Pred začatím upgradu musíte mať nainštalované "**Router Tools**", pretože nástroj pre upgrade firmwaru "**Firmware Upgrade Utility**" je priamo obsiahnutý v "**Router Tools**". Nasledujúci popis vás povedie pri upgrade.

Poznámka: Nasledujúce príklady vychádzajú z prostredia OS Windows.

1. Stiahnite si poslednú verziu firmwaru z internetových stránok, alebo ftp servra (http://www.draytek.sk , ftp://ftp.draytek.sk) alebo použite inštalačné CD
2. Vo Web konfigurátore kliknite na položku "Firmware Upgrade (TFTP Server)". Otvorí sa nasledujúca stránka.



3. Kliknite na "**Potvrdiť**" pre umožnenie upgrade firmwaru.
4. Vojdite do ponuky "**Start** >> **Programs** >> **Router Tools** >> **Firmware Upgrade Utility**" pre spustenie nástrojov upgradu.

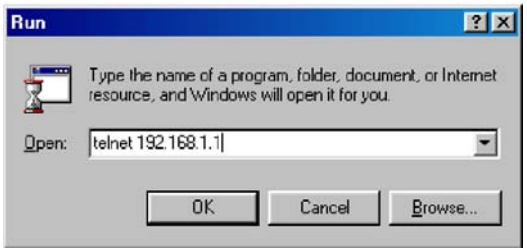
V políčku "**Router IP**" musí byť zadaná IP vášho routra. **Firmware file:** Kliknite na "**Browse**" a vyberte aktuálny firmware, ktorý ste stiahli zo stránok. Názov súboru na obrázku je len informačný, najnovšia verzia firmwaru bude mať istotne odlišný názov, a vy sa musíte riadiť cestou na vašom počítači. AK je na routry zadané heslo treba ho zadať do políčka Password, potom kliknite na "**Send**". Stav upgradu sa zobrazí v spodnej časti okna. Aktuálnu verziu firmwaru môžete odkontrolovať aj v hlavnom menu Web konfigurátora, kde je v pravo hore napísaná.

Nasledujúca kapitola popisuje, ako diagnostikovať sieťové probémy cez implementovaný ladiaci nástroj s použitím Telnetu, a terminálových príkazov. V príkladoch je použitý software Windows Telnet. Ak ste Mac užívateľ, nainštalujte si "third-party" Telnet klient software. V zásade však Linux Telenet software obsahuje.

7.1 Použitie príkazov v Telnete

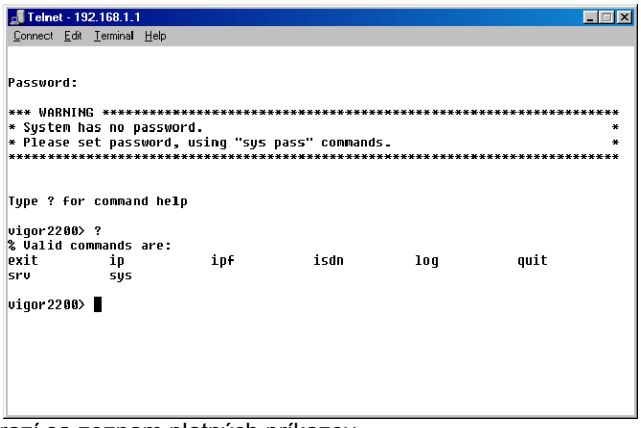
Vojdite do ponuky "**Start** >> **Spustit**". Vpíšte "**Telnet 192.168.1.1**".

Poznámka: IP adresa je len informatívna, je to IP adresa routra podľa výrobného nastavenia. Ak ste jeho IP adresu zmenili, musíte vpísať aktuálnu.



Kliknite na "**OK**". Otvorí sa Telnet terminál. Ak ešte nebolo definované užívateľské heslo, podľa zobrazených krokov ho zadajte.

```
*** WARNING ************************************************************
* System has no password.                                               *
* Please set password, using "sys pass" commands.                       *
*************************************************************************
```



Potom napíšte "**?**" a potvrďte, zobrazí sa zoznam platných príkazov.

.

Pomocný príkaz

Ak nie ste veľmi oboznámený s prostredím a príkazmi v telnete, potom tento príkaz "**?**" zadávaný za nie veľmi známym príkazom, bude pre vás veľkým prínosom. Príklad použitia: príkaz "**ip**" je prvoúrovňový. Ak zadáte "**ip ?**", zobrazia sa na obrazovke všetky príkazy druhej úrovne.

```
vigor2200> ip ?
% Valid subcommands are:
addr          arp           dhcpc         ping          route         wanaddr

vigor2200>
```

Znovuvyvolanie príkazov

Terminál Telnet poskytuje možnosť vyvolať spätne zadávané príkazy. Použitím kláves "šípka hore" a "šípka dole" listujete v už zadávaných príkazoch.

Odchod z terminálu

Zadajte príkaz "**quit**", alebo "**exit**".

7.2 Zobrazenie zaznamenaných volaní

Funkcia zanamenávania volaní je užitočná pri riešení problémov nastavení volaní, alebo problémov vo WAN spojení. V pôvodnom nastavení routra je definované zaznamenávanie správ o WAN spojeniach. Ak obsahu rozpisu nerozumiete, môžete ho veľmi jednoducho uložiť a poslať servisnému technikovi. Postup vyvolania zaznamenaných volaní:

1. Pripojte sa k terminálu Telnet.
2. Zadajte príkaz "**log -F c**" pre uvoľnenie všetkých zaznamenaných volaní.
3. Urobte ping na akéhokoľvek vonkajšieho užívateľa, aby ste inicializovali router k vonkajciemu volaniu.
4. Zadajte príkaz "**log -c**" pre zobrazenie posledných zaznamenaných volaní.

Príklad na PPPoE:

```
vigor2200> log -c
15:04:10.320 >>> Dial-up triggered by user : 192.168.1.18
             proto=icmp, to 168.95.1.1
15:04:10.760 PPP Start (PPPoE)
15:04:13.310 PAP Login OK (PPPoE)
15:04:13.450 IPCP Opening (PPPoE)
             Own IP Address : 168.95.186.16  Peer IP Address : 168.95.186.254
             Primary DNS : 168.95.192.1  Secondary DNS : 168.95.1.1
vigor2200>
```

7.3 Zobrazenie PPP záznamov

1. Pripojte sa k terminálu Telnet.
2. Zadajte príkaz "**log -F w**" pre uvoľnenie všetkých PPP záznamov.
3. Urobte ping na akéhokoľvek vonkajšieho užívateľa, aby ste inicializovali router k vonkajciemu volaniu.
4. Zadajte príkaz "**log -p**" pre zobrazenie posledných PPP zaznamov. Pre zobrazenie všetkých PPP záznamov, zadajte príkaz "**log -p -t**".

```
vigor2200> log -p
16:07:00.000 >>>>B1 Len=27
    Protocol:LCP(c021)
        ConfReq Identifier:0x00
            Protocol Field Compression
            Address/Control Field Compression
            MRRU: 1500
            Short Sequence Number Header Format
            Endpoint Discriminator
                Locally Assigned Address: 00 0f 77 24 00 0f ##

16:07:00.970 >>>>B1 Len=27
    Protocol:LCP(c021)
        ConfReq Identifier:0x01
            Protocol Field Compression
            Address/Control Field Compression
            MRRU: 1500
            Short Sequence Number Header Format
            Endpoint Discriminator
                Locally Assigned Address: 00 0f 77 24 00 0f ##
```

Záznami PPP sú užitočné pri riešení komunikačných problémov s normálnym ISDN dialup, alebo PPPoE a PPTP dialup cez DSL modem.

7.4 Zobrazenie WAN záznamov,

Najjednoduchšia cesta zobrazenia všetkých WAN záznamov, vrátane tých na ISDN D-kanále a PPP/PPPoE/PPTP je nasledovná:

1. Pripojte sa k terminálu Telnet.
2. Zadajte príkaz "**log -F w**" pre uvoľnenie všetkých PPP/PPPoE/PPTP a ISDN záznamov.
3. Urobte ping na akéhokoľvek vonkajšieho užívateľa, aby ste inicializovali router k vonkajciemu volaniu.

4. Zadajte príkaz "**log -w**" pre zobrazenie posledných WAN záznamov. Pre zobrazenie všetkých WAN záznamov, zadajte príkaz "**log -w -t**".

7.5 Riešenie problému DHCP klienta na WAN rozhraní

V prostredí káblového prístupu na Internet je DHCP klient (dznamic IP) veľmi populárny. Pre diagnostikovanie tohto prístupu zadajte v Telnete príkaz "**ip dhcpc...**". Tento príkaz má rovnakú funkciu ako nástroje typu **ipconfig.exe**, alebo **winipcfg.exe** v prostredí MS Windows OS.

Ak zadáte príkaz "**ip dhcp?**", zobrazia sa príkazy tretej úrovne.

```
vigor2200> ip dhcpc ?
% Valid subcommands are:
release      renew        status

vigor2200>
```

Vyčistenie IP adries

Zadaním príkazu "**ip dhcpc release**" budú všetky IP nastavenia na rozhraní WAN vyčistené.

```
vigor2200> ip dhcpc release
vigor2200> ip dhcpc status

DHCP Client Status:

DHCP Server IP : 0.0.0.0
WAN IP         : 0.0.0.0
WAN Netmask    : 0.0.0.0
WAN Gateway    :
Primary DNS    :
Secondary DNS  :
Leased Time    : 0
Leased Time T1 : 0
Leased Time T2 : 0

vigor2200>
```

Obnovenie IP adries

Pre získanie nových IP adries od poskytovateľa zadajte príkaz "**ip dhcpc renew**".

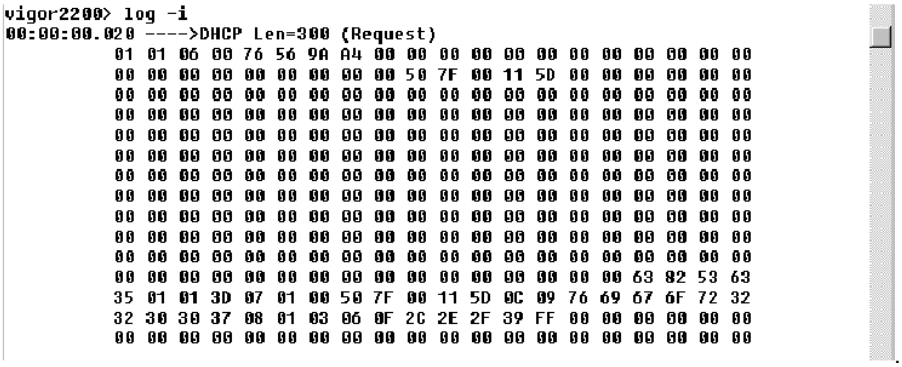
```
vigor2200> ip dhcpc renew
vigor2200> ip dhcpc statu

DHCP Client Status:

DHCP Server IP : 192.168.3.1
WAN IP         : 192.168.3.83
WAN Netmask    : 255.255.255.0
WAN Gateway    : 192.168.3.1
Primary DNS    : 168.95.1.1
Secondary DNS  : 192.168.3.1
Leased Time    : 259200
Leased Time T1 : 129600
Leased Time T2 : 226800

vigor2200>
```

Zobrazenie nastavení na WAN

Pre zobrazenie nastavení DHCP klienta na rzhraní WAN zadajte príkaz "**ip dhcpc status**".

Zobrazenie DHCP záznamov

V niektorých špeciálnych prípadoch môže byť dôležité deatailne vyjadriť DHCP správy vysielané medzi rozhraním WAN a prístupovým serverom. Tie získate zadaním príkazu "**log -i**". Je však dôležité, aby WAN rozhranie malo prednastavené automatické získavanie IP adresy (**Obtain IP address automaticaly**).



```
vigor2200> log -i
00:00:00.020 ---->DHCP Len=300 (Request)
           01 01 06 00 76 56 9A A4 00 00 00 00 00 00 00 00 00 00 00 00
           00 00 00 00 00 00 00 00 00 50 7F 00 11 5D 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 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 00 00 00 00 00 00 00 00 00 00 00 00 63 82 53 63
           35 01 01 3D 07 01 00 50 7F 00 11 5D 0C 09 76 69 67 6F 72 32
           32 30 30 37 08 01 03 06 0F 2C 2E 2F 39 FF 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
```

8.1 Príkazy v programe Telnet (Commands in Telnet)

8.1.1 Príkazy pre filtrovanie IP paketov

Používanie príkazov:

ipf [-VzZ] [-l] [blokované | prepustené | nevykonané]

- V Vypíš informácie o verzii IP filtra. Taktiež bude zobrazená informácia o jeho aktuálnom stave (či už je zaznamenávanie aktívne, či je nastavené implicitné filtrovanie, a pod.).

Príklad:

```
vigor2000>                                        ipf                                        -V
ipf:                    IP                    Filter:                    v3.3.1                    (148)
Kernel:                             IP                             Filter:                             v3.3.1
Running:                                                                                                yes
Log                 Flags:                 0x0                 =                 none                 set
Default: pass all, Logging: available
```

-z Pre každé pravidlo vo vstupnom súbore nastav jeho štatistické údaje na „0“ a spätne ich zobraz ako vynulované.

Príklad:

```
vigor2000> ipf -z
```

-Z Vynuluj globálne štatistické údaje držané v jadre len za účelom filtrovania (toto neovplyvní štatistiky fragmentácie ani stavové štatistiky).

Príklad:

```
vigor2000> ipf –Z

input packets:         blocked 0 passed 0 nomatch 0 counted 0

output packets:        blocked 0 passed 0 nomatch 0 counted 0

input packets logged:  blocked 0 passed 0

output packets logged: blocked 0 passed 0

packets logged:        input 0 output 0

log failures:          input 0 output 0

fragment state(in):    kept 0  lost 0

fragment state(out):   kept 0  lost 0

packet state(in):      kept 0  lost 0

packet state(out):     kept 0  lost 0

ICMP replies:   0      TCP RSTs sent:  0

Result cache hits(in): 0       (out):  0

IN Pullups succeeded:  0       failed: 0

OUT Pullups succeeded: 0       failed: 0

TCP cksum fails(in):   0       (out):  0

Packet log flags set: (0)

None
```

-l Prepne implicitné zaznamenávanie paketov. Platné argumenty pre túto voľbu sú „prepustené“(pass), „blokované“ (block) a „nevykonané“ (nomatch). Akýkoľvek iný argument spôsobí zablokovanie tejto funkcie. Pokiaľ je nastavená niektorá z platných volieb, akýkoľvek paket, ktorý opustí filter a vyhovuje nastavenej kategórii, bude zaprotokolovaný. To je veľmi užitočné pre protokolovanie všetkých paketov, ktoré nespĺňajú aspoň jedno z nastavených pravidiel filtrovania.

8.1.2 Príkazy pre zobrazenie „ipf view“

Používanie príkazov:

ipf view [-acdfhiorstz] [-g <group>] [-l <line>]

-a Zobraz účtovací zoznam filtrovania a vypíš opäť načítané bajty zo všetkých predpisov.

Príklad:

```
vigor2000> ipf view -a
Call Filter Rules
 empty !
Data Filter Rules
Incoming Filter Rules
 empty !
Outgoing Filter Rules
 empty !
```

-c Zobraz pravidla pre aktívny filter volaní.

Príklad:

```
vigor2000> ipf view -c
Call Filter Rules
278 0 @1 block in quick from any port 136 > < 140 to any
```

-d Zobraz pravidla pre aktívny filter dát.

Príklad:

```
vigor2000> ipf view -d
Data Filter Rules
Incoming Filter Rules
 empty !
Outgoing Filter Rules
0 0 @1 block out quick from any port 136> <140 to any port = domain
```

-f Zobraz štatistické informácie o stave fragmentov a drž ich, ak sú prítomné.

Príklad:

```
vigor2000> ipf view -f
IP fragment states:
        0 new
        0 expired
        0 hits
```

```
        0 no memory
        0 already exist
        0 inuse
```

-h Zobraz čísla ako počet všetkých zásahov podľa každého pravidla.

Príklad:

```
vigor2000> ipf view -h
input packets:         blocked 278 passed 557 nomatch 384 counted 0
 output packets:       blocked 0 passed 430 nomatch 96 counted 0
input packets logged:  blocked 0 passed 0
output packets logged: blocked 0 passed 0
 packets logged:       input 0 output 0
 log failures:         input 0 output 0
fragment state(in):    kept 0  lost 0
fragment state(out):   kept 0  lost 0
packet state(in):      kept 0  lost 0
packet state(out):     kept 0  lost 0
ICMP replies:   0      TCP RSTs sent:  0
Result cache hits(in): 230     (out):  334
IN Pullups succeeded:  0       failed: 0
OUT Pullups succeeded: 0       failed: 0
TCP cksum fails(in):   0       (out):  0
Packet log flags set: (0)
        none
```

-n Pre neaktívnu sadu filtrov.

Príklad:

```
vigor2000> ipf view -n
input packets:        blocked 278 passed 557 nomatch 384 counted 0
output packets:        blocked 0 passed 430 nomatch 96 counted 0
 input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
 packets logged:       input 0 output 0
 log failures:         input 0 output 0
fragment state(in):    kept 0  lost 0
fragment state(out):   kept 0  lost 0
packet state(in):      kept 0  lost 0
packet state(out):     kept 0  lost 0
ICMP replies:   0      TCP RSTs sent:  0
Result cache hits(in): 230     (out):  334
```

```
IN Pullups succeeded:  0       failed: 0

OUT Pullups succeeded: 0       failed: 0

TCP cksum fails(in):   0       (out):  0

Packet log flags set: (0)

        none
```

-o Ukáž bežiace „volacie a dátové“ podmienky filtrovania.

Príklad:

```
vigor2000> ipf view -o

Usage:

 ipf view [-acdfhiorstz] [-g <group>] [-l <line>]

-a          for 'account' filter list

-c          show the running call filter rules

-d          show the running data filter rules

-f          for 'fragment' states

-h          show hit-number of the filter rule

-n          for the inactive filter set

-r          show the running (call & data) filter rules

-s          for IP state status

-t          display to the end

-z          clear the statistics after this command

-g <group>  specify the group number

-l <line>   specify the rule's line number within a list/group
```

-s Zobraz štatistickú informáciu o toku paketov a pozastav túto stavovú informáciu, ak je prítomná.

Príklad:

```
vigor2000> ipf view –s

IP states added:

        0 TCP

        0 UDP

        0 ICMP

        0 hits

        1265 misses

        0 maximum

        0 no memory

        buckets in use  0

        0 active

        0 expired

        0 closed
```

-t Zobraz do konca (deaktivuj funkciu Telnetu 'more')

Príklad:

```
Vigor2000> ipf view -t
```

-z Vymaž štatistické dáta po zadaní tohto príkazu.

Príklad:

```
vigor2000> ipf view -z
```

-g <skupina> Špecifikuj číslo skupiny (<group>).

Príklad:

```
vigor2000> ipf view -g <skupina>
```

-l <riadok> Špecifikuj číslo riadku pravidla podľa zoznamu a skupiny.

Príklad:

```
vigor2000> ipf view -l <riadok>
```

8.1.3 Príkazy pre zaznamenávanie „log“

Používanie príkazov:

log [-cfhipstwx?][-F a|c|f|s|w]

-c Zobraz záznam volaní (Display the call log)

Príklad:

```
vigor2000> log -c
08:30:59.500 >>> Dial-up triggered by user : 0.6.234.255
             proto=0, to 255.255.226.77
08:30:59.500 Dialing ISP (test) : 7454565
08:31:00.000 PPP Start (B1)
08:31:02.910 CHAP Login OK (B1)
08:31:02.940 IPCP Opening (B1)
        Own IP Address : 192.168.2.200  Peer IP Address : 192.168.2.1
        Primary DNS : 194.51.83.1  Secondary DNS : 194.98.0.1
08:34:04.630 PPP Closed : Idle Time-out (B1)
08:34:04.950 Disconnect (B1): Cause #0 (unknown)
```

-f Zobraz záznam filtrov

(Display the filter log)

Príklad:

```
vigor2000> log –f
08:31:02.940 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
08:31:33.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
08:32:04.040 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
08:32:34.740 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
08:33:05.540 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
08:33:36.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
```

-F vyprázdni vyrovnávaciu pamäť záznamov

(Flush the log buffers)

podľa nasledujúceho atribútu príkazu. Atribút príkazu musí byť oddelený medzerou (tak ako je uvedené v nasledujúcich riadkoch).

-F a Vyprázdni všetky záznamy

(flush all logs)

Príklad:

```
vigor2000> log -F a
8161 bytes flushed from the call log
26604 bytes flushed from the wan log
```

-F c Vyprázdni záznam volaní

(flush the call log)

Príklad:

```
vigor2000> log -F c
8161 bytes flushed from the call log
```

-F f Vyprázdni záznam filtrov

(flush the filter log)

Príklad:

```
vigor2000> log -F f
456 bytes flushed from the filter log
```

-F s Vyprázdni záznam stavov

(flush the state log)

Príklad:

```
vigor2000> log -F s
```

-F w Vyprázdni záznam WAN /ISDN a PPP/ portov

(flush the wan /ISDN and PPP/ log)

Príklad:

```
vigor2000> log -F w
26604 bytes flushed from the wan log
```

-h Zobrazenie tejto ponuky (For this usage help)

-I Zobraz záznam D-kanála ISDN z časti záznamu WAN portov (Display the ISDN D-channel part of the wan log)

Príklad:

```
vigor2000> log –i
01:32:43.540 ---->D Len=4 LAPD TE R  SAPI=0  TEI=79  RR   P/F=0 NR=4
01:32:51.800 <----D Len=36 LAPD NT C  SAPI=0  TEI=79  INFO P=0 NR=3
NS=4  bytes  ETSI  102
  Dest    CR=0x23      PD=Q.931 DISCONNECT
 1  00001000 INFORMATION  ELEMENT : Cause
```

```
 2  00000010 IE length : 2   octets
 3  1------- Extension bit : not continued
    -00----- Coding standard:CCITT standard coding as described below
    ---0---- Spare
    ----0101 Location : private network serving the remote user
 4  1------- Extension bit : not continued
    -0010010 Cause Value : No user responding
 1  00011100 INFORMATION  ELEMENT : Facility
 2  00010110 IE length : 22  octets
 3  1------- Extension bit : not continued
    -00----- Spare
    ---10001 Service discriminator:supplementary service applications
 4  10------ Class : context-specific
    --1-----  Form : constructor
    ---00001 Component tag : invoke
 5  0--- ---- Length format : reserved
    -0010011 Length of component : 19
 6  ******** Component contents : 02 02 03 0D 02 01 22 30 0A A1 05
                  30 03 02 01 00 82 01 01
01:32:51.800 ---->D Len=4 LAPD TE R  SAPI=0  TEI=79  RR   P/F=0 NR=5
01:32:51.810 <----C Len=14 0e 00 0a 00 04 82 b6 00 01 05 00 00 12 34
```

-p Zobraz záznam PPP/MP z časti záznamu WAN portov

(Display the PPP/MP part of the wan log)

Príklad:

```
vigor2000> log -p
08:31:02.900 >>>>B1 Len=29
    Protocol:CHAP(c223)
        Response Identifier:0x01 10 ef dc a5 17 aa e0 11 71 05 cf 19 79 dd 6b 45
 6d 72 6f 75 74 65 72 ##
 08:31:02.910 <<<<B1 Len=38
    Protocol:CHAP(c223)
        Success Identifier:0x01Welcome to Vigor2000 isdnRouter. ##
08:31:02.910 >>>>B1 Len=24
    Protocol:IPCP(8021)
        ConfReq Identifier:0x00
            IP Address: 0 0 0 0
            Primary Domain Name Server: 0 0 0 0
            Secondary Domain Name Server: 0 0 0 0 ##
```

```
08:31:02.920 <<<<B1 Len=18

    Protocol:IPCP(8021)

        ConfReq Identifier:0x00

            Compression Type:

                Van Jacobson Compressed TCP/IP  0f 00

            IP Address: 192 168 2 1 ##
```

-s Zobraz záznam stavov

(Display the state log)

-t Zobraz do konca (deaktivuj funkciu 'more' v zobrazení Telnetu)

(Display to the end. (Disable the 'more' function of the Telnet display)

Príklad:

```
vigor2000> log –t

08:31:02.940 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52

08:31:33.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72

08:32:04.040 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52

08:32:34.740 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72

08:33:05.540 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52

08:33:36.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
```

-w Zobraz záznam WAN /ISDN a PPP/ portov

(Display the wan (ISDN and PPP) log)

Príklad:

```
vigor2000> log -w

08:30:59.990 <----D Len=21 LAPD NT C  SAPI=0  TEI=97  INFO P=0 NR=1    NS=1

        17   bytes  ETSI  102

    Dest    CR=0x42      PD=Q.931 CONNECT

 1  00101001 INFORMATION  ELEMENT : Data/Time

 2  00000101 IE length : 5   octets

 3  00000000 Year : 0

 4  00001010 Month : 10

 5  00011010 Day : 26

 6  00001000 Hour : 8

 7  00011111 Minute : 31

 8  01001100 INFORMATION  ELEMENT : 0x4C

 9  00000100 IE length : 4   octets

 10 ******** HEX contents : 01 83 37 34

08:31:00.000 ---->D Len=4 LAPD TE R  SAPI=0  TEI=97  RR   P/F=0 NR=2

08:31:00.000 <----C Len=15 0f 00 0a 00 03 82 00 00 01 05 01 00 00 00 00

08:31:00.000 >>>>B1 Len=12
```

```
    Protocol:LCP(c021)
        ConfReq Identifier:0x00
            Protocol Field Compression
            Address/Control Field Compression ##
08:31:00.000 <----C Len=20 14 00 0a 00 08 82 01 00 01 05 00 00 29 00 05 00 0a 1a
 08 1f
08:31:00.000 ---->C Len=12 0c 00 0a 00 03 83 00 00 01 05 01 00
```

-x Ak je nejaký paket, potom telo paketu zobraz v HEXa tvare.

(For packet body hex dump, if any)

Príklad:

```
vigor2000> log –x
08:31:02.940 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
45 00 00 34 00 02 00 00 01 11 17 05 c0 a8 02 01      E..4............
e0 00 00 09 02 08 02 08 00 20 93 75                  ......... .u
08:31:33.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
45 00 00 48 00 04 00 00 01 11 16 ef c0 a8 02 01      E..H............
e0 00 00 09 02 08 02 08 00 34 d1 91                  .........4..
08:32:04.040 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
45 00 00 34 00 06 00 00 01 11 17 01 c0 a8 02 01      E..4............
e0 00 00 09 02 08 02 08 00 20 93 75                  ......... .u
08:32:34.740 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
45 00 00 48 00 08 00 00 01 11 16 eb c0 a8 02 01      E..H............
e0 00 00 09 02 08 02 08 00 34 d1 91                  .........4..
08:33:05.540 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 52
45 00 00 34 00 0a 00 00 01 11 16 fd c0 a8 02 01      E..4............
e0 00 00 09 02 08 02 08 00 20 93 75                  ......... .u
08:33:36.440 wan @65535:0 p 192.168.2.1,520 -> 224.0.0.9,520    PR udp len 20 72
45 00 00 48 00 0c 00 00 01 11 16 e7 c0 a8 02 01      E..H............
e0 00 00 09 02 08 02 08 00 34 d1 91                  .........4..
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

8.2 Print Server

Print server sa využíva pre pripojenie tlačiarne do siete, kde každý užívateľ LAN siete môže túto tlačiareň využívať bez nastavenia zdieľania tlačiarni v sieti.

Vigor print server nemá buffer pre tlačenie, Iba priamo prenáša dáta do tlačiarne a neukladá ich do buffra. Vigor print server neposkytuje nasledovné funkcie:

•zhromažďovať výstupné dáta z PC, a potom ich tlačiť.

•zhromažďovať dáta naraz z viacerých konkurenčných PC , a vytlačiť všetky dokumenty jeden za druhým.

•Manažment fronty prijatých dokumentov, vrátane možnosti vymazania alebo znovuvytlačenia dokumentov.

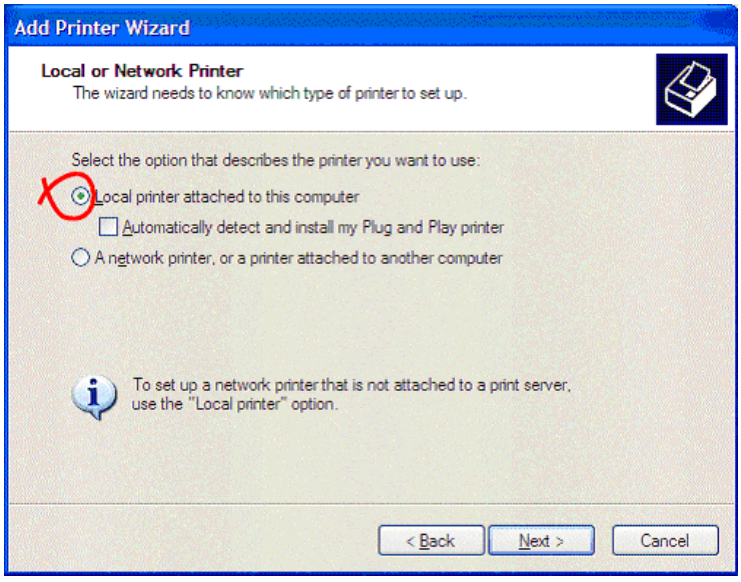
Router má niekoľko obmedzení pre USB Print port:

1. Nepodporuje bi-directional printer rozhranie.
   Napríklad ak Vaša tlačiareň používa utilitu alebo ovládač ktorý detekuje spotrebu farby v náplniach, táto funkcia nebude funkčná.
2. Nepodporuje iné modely multifunkčných tlačiarní so skenerom alebo faxom.

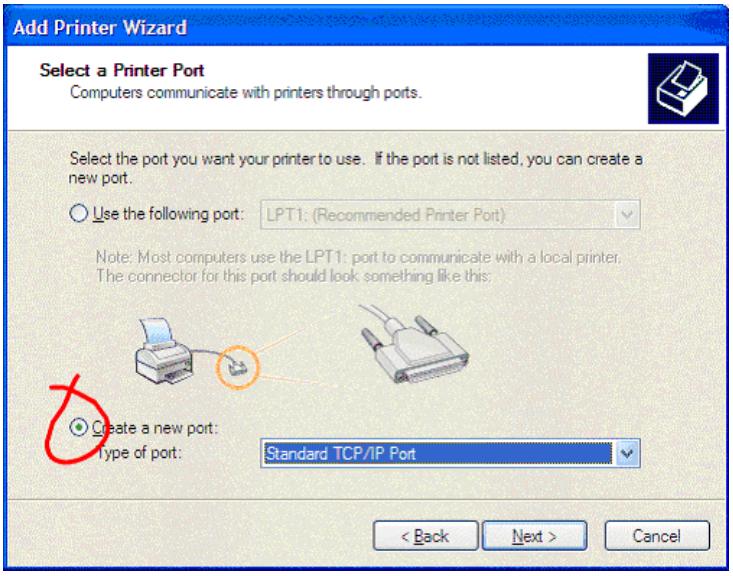
Inštalácia USB tlačiarne pripojenej k routru Vigor2600VGST

Príklad ukazuje nainštalovanie USB tlačiarne do systému Win2000 a WinXP.

1. **[Start] -› [Settings] -› [Control Panel] -› [Printers] -› [Add Printer]**, vyberte "Next" -› "Local Printer" -› "Next".



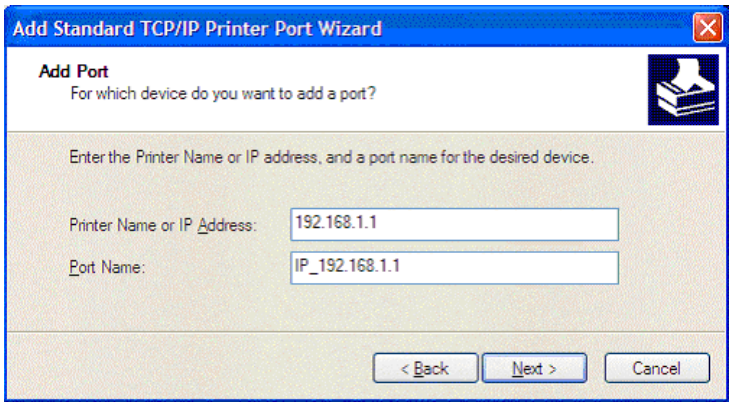
2. Zvoľte "Create a new port" -› "Standard TCP/IP" -› "Next" -› "Next".



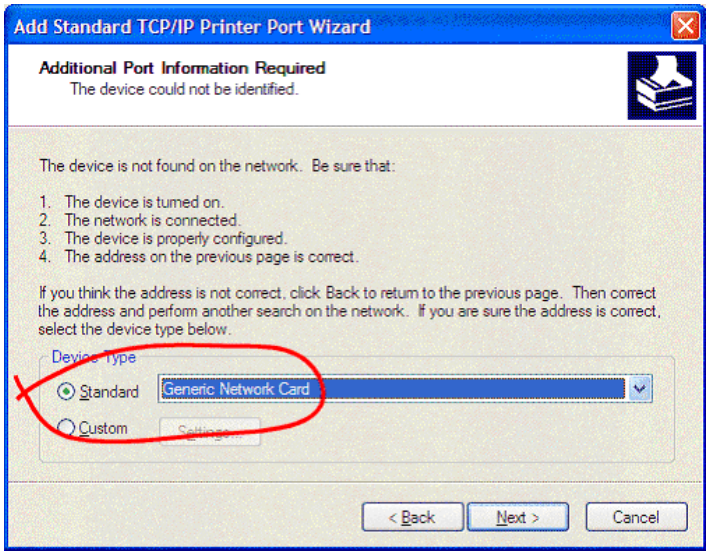
3. V poli Printer Name or IP Address ›Zadajte LAN IP adresu Vigor routra.

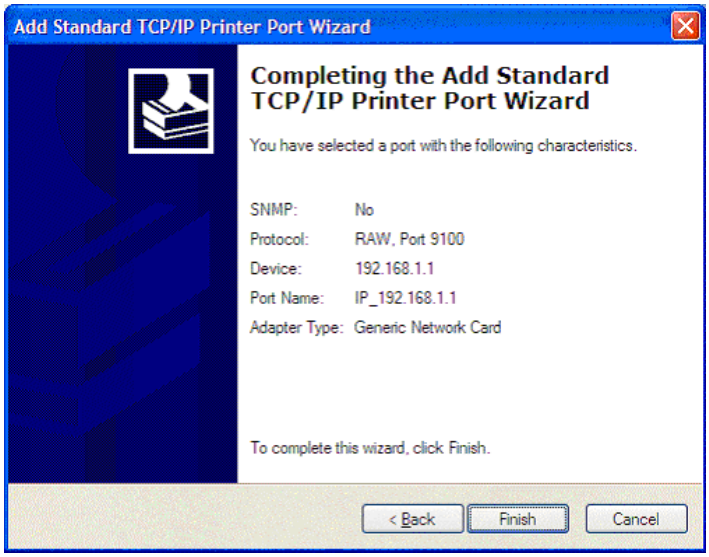
V poli Port Name, sa nastavá predvolené meno alebo zadajte iné meno.

Potom stlačte "Next".

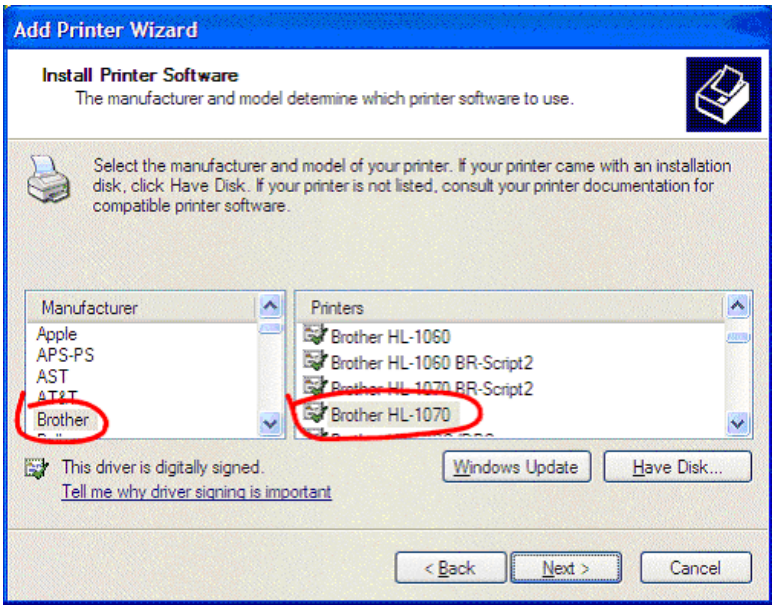


4. Vyberte "**Standard : Generic Network Card**" -› "Next" -›"Finish".

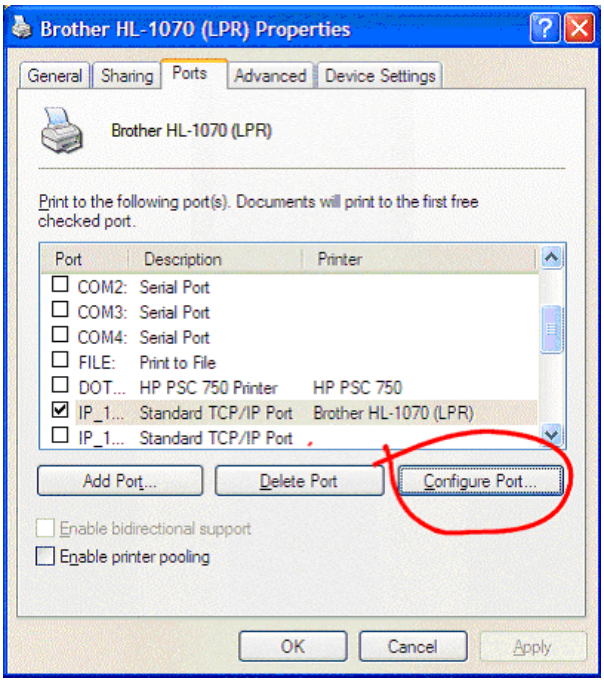




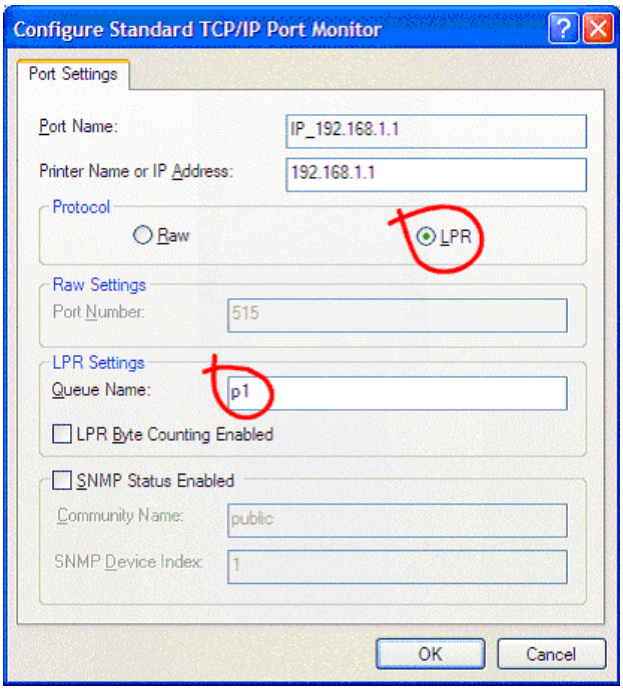
5. Po kliknutí na "**Finish**"', sprievodca pridaním tlačiarne Vás požiada o nastavenie detailov aktuálneho modelu tlačiarne, čiže treba vybrať správny ovládač pre Vašu tlačiareň:



6. Na koniec, je potrebné vrátiť sa späť do Control Panel -› Printers a editovať vlastnosti novo pridanej tlačiarne.:



7. vyberte "**LPR**" ako Protokol, zadajte **p1** (**p** a číslo **1**) ako Queue Name -› "OK".



8. A už môžete používať Vašu USB tlačiareň cez router Vigor2600VGST.

Poznámka: pre inicializáciu routra/tlačiarne, prosím

-› Vypnite router.

-› Vypnite tlačiareň.

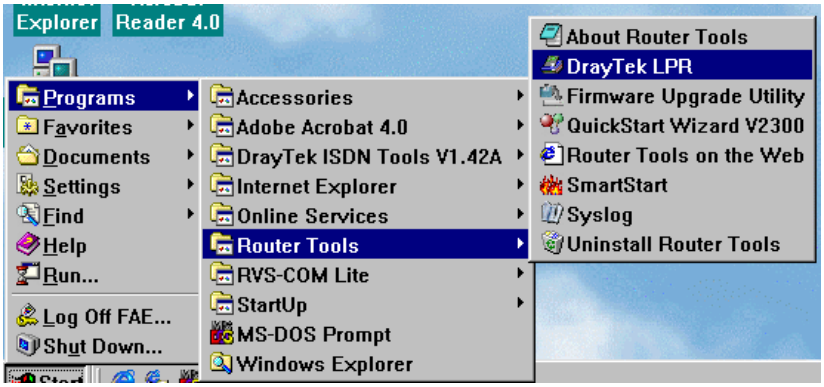
-› Zapnite tlačiareň ON.

-› Zapnite router ON.

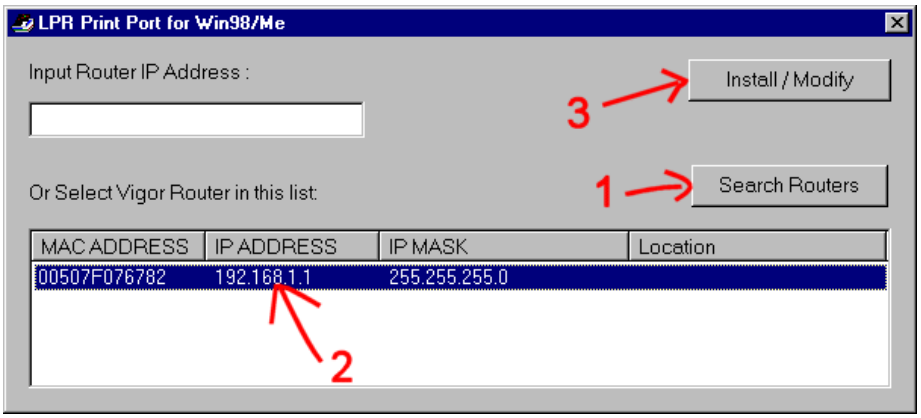
Príklad ukazuje nainštalovanie USB tlačiarne do systému Windows98/Me?

1.Z inštalačného CD k Vigor routru nainštalujte aplikáciu (tool) pre Windows98/ME do Vášho PC. Alebo si aplikáciu s tiahnite z www.attel.sk. Reštartujte PC.

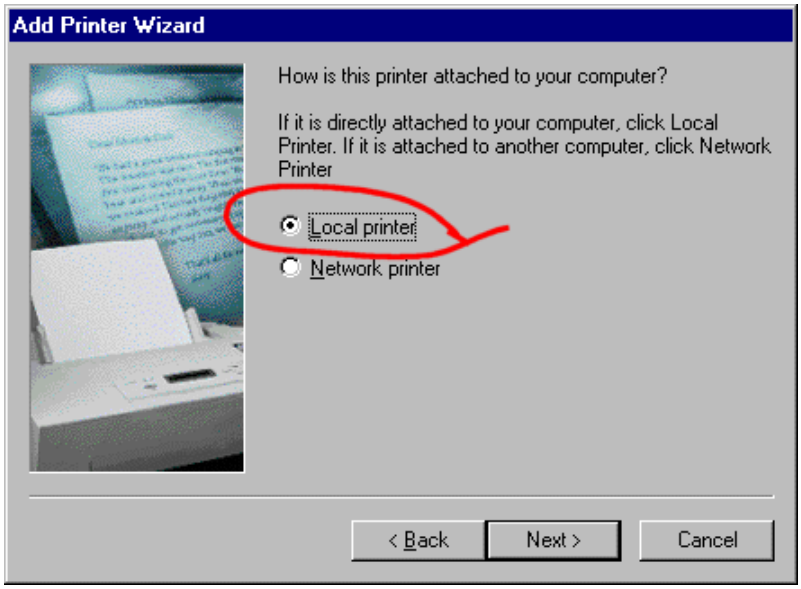
2. Spustite LPR utilitu z **[Start] -›[Programs] -›[Router Tools] -›[DrayTek LRP].**

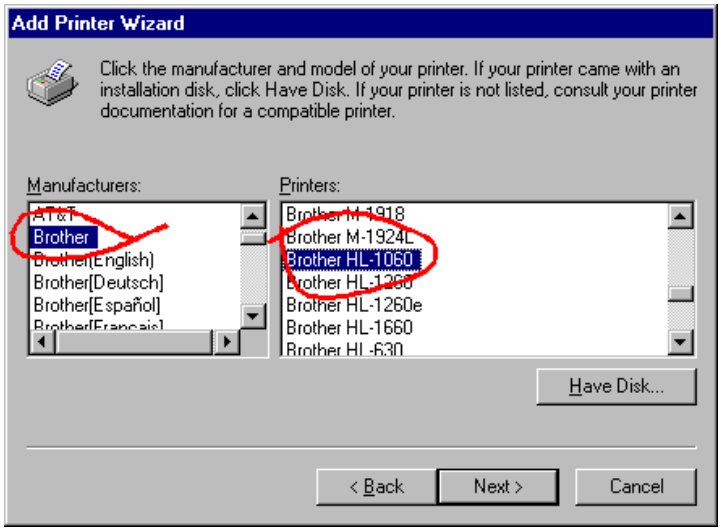


3. Vyberte **"Search Routers"** a vyberte router (podľa IP adresy) potom ho označte a stlačte **"Install/Modify"**. Toto označí port pre LPR tlačenie :

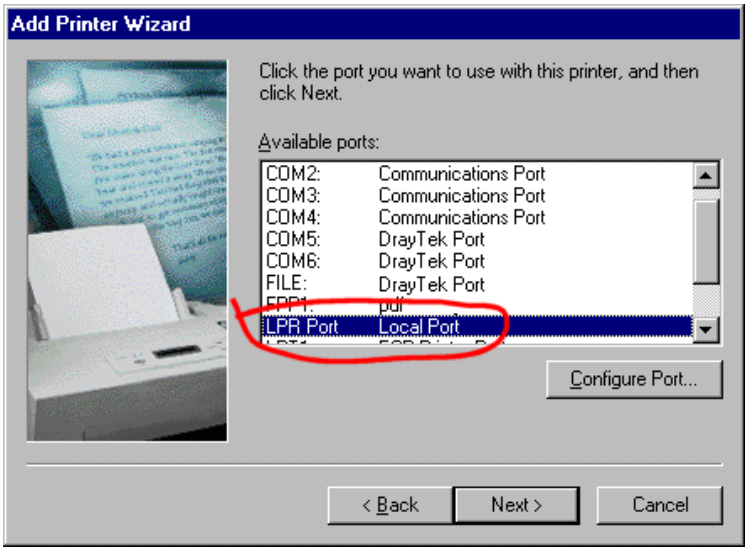


4. Potom je potrebné ísť na **[Start] -› [Settings] -› [Control Panel] -› [Printers] -› [Add Printer]** a nasledovať sprievodcu pridaním novej tlačiarne :





5. Vyberte **typ** Vašej tlačiarne -› "**Next**" -› "**LPR Port Local Port**" -› "**Next**" -› "**Next**" -› "**Finish**".



6. A už môžete používať Vašu USB tlačiareň cez router Vigor2600VGST.

Poznámka: pre inicializáciu routra/tlačiarne, prosím

-› Vypnite router.

-› Vypnite tlačiareň.

-› Zapnite tlačiareň ON.

-› Zapnite router ON.

Nastavenie LPR tlače v Linuxe

Riešenie je navrhol Kees van Hoof.

Nakonfigurovať CUPS použitím parametru lpd://192.168.1.1/p1.

Kompatibilné tlaičarne s rotrom Vigor2600VGST

Nasledové tlačiarne boli testované a kompatibilné s routrom Vigor2600VGST. Ale mnoho ďalších štandardných USB tlačiarní takisto je kompatibilných s routrom, len neboli otestované.

Epson	Visit Epson's Website
Epson C44UX	
Epson EPL5900 black and white Laser	
Epson PictureMate	
Epson Stylus C42	
Epson Stylus C44	
Epson Stylus C61	
Epson Stylus C82	
Epson Stylus Color 600	
Epson Stylus Color 740	
Epson Stylus Color 880	
Epson Stylus Color 1160	
Epson Stylus Photo 700	
Epson Stylus Photo 750	
Epson Stylus Photo 810	
Epson Stylus Photo 870	
Epson Stylus Photo 890	
Epson Stylus Photo R200	
Epson Stylus Photo R300	
Epson Stylus Photo R310	
Epson Stylus Photo R800	
Epson Stylus Photo RX500	

Samsung	Visit Samsung's Website
Samsung CLP-510	
Samsung ML 1250	
Samsung ML 1510	
Samsung ML 2150	

HP	Visit HP's Website
HP 3300 mfp	
HP Deskjet 1220C	
HP DeskJet 3820	
HP DeskJet 5550	
HP DeskJet 5652	
HP Deskjet 630C	
HP Deskjet 640C	
HP Deskjet 670cxi	
HP DeskJet 810C	
HP DeskJet 895Cxi	
HP DeskJet 930C	
HP DeskJet 930C	
HP DeskJet 940C	
HP DeskJet 970Cxi	
HP DeskJet 980Cxi	
HP DeskJet 990Cxi	
HP Photosmart 1215	
HP Photosmart 7550	
HP Photosmart 7690	
HP Photosmart P1000	
HP PSC 2110 All-in-One	
HP LaserJet 6P	
HP LaserJet 6L	
HP LaserJet 1010	
HP LaserJet 1100	
HP LaserJet 1200	
HP LaserJet 1300	

Xerox	Visit Xerox's Website
Xerox Docuprint M750	

Lexmark	Visit Lexmark's Website
Lexmark x6170	
Lexmark E320	

Brother	Visit Brother's Website
HL-1260	
HL-1430	
HL-5130	
HL-5150D	
MFC-8820D	
MFC-9070	

OKI	Visit OKI's Website
Okipage 4W	
Okipage 8W Lite	

Konica	Visit Konica's Website
Minolta 2300W	
Minolta PagePro 1300W	

HP LaserJet 2550L
HP LaserJet 3020
HP LaserJet 5P
HP Officejet 5110

Canon	Visit Canon's Website
Canon BubbleJet i450	
Canon 550i	
Canon i250	
Canon i320	
Canon i560	
Canon i865	
Canon i950	
Canon i965	

Kyocera	Visit Kyocera's Website
FS-1000	
FS-1010	

Dymo	Visit Dymo's Website
LabelWriter 400	