JOYCE
1-2-3. Spojeno.

JOYCE ČR, s.r.o., Fakturační adresa: Matzenauerova 8, 616 00 Brno, ČR, Korespondenční adresa: Venhudova 6, 614 00 Brno, ČR
IČO: 25317571, DIČ: CZ25317571, Tel.: +420 539 088 010, Fax: +420 539 088 000, E-mail: joyce@joyce.cz Web: www.joyce.cz

WELL PTI-1605G

Uživatelská příručka

OBSAH

1.1. AUTORSKÁ PRÁVA....5
1.2. OBCHODNÍ ZNAČKY....5
1.3. PROHLÁŠENÍ O SHODĚ....5
1.4. CHARAKTERISTIKA....6
1.5. ROZSAH....7
1.6. STRUKTURA DOKUMENTU....7
1.7. POŽADAVKY NA SYSTÉM....7
1.8. OBSAH BALENÍ....7

2. POPIS ZAŘÍZENÍ 8
2.1. POPIS ZAŘÍZENÍ WELL PTI-1605G....8
2.2. HARDWAROVÉ PŘIPOJENÍ:....9

3. KONFIGURACE PC 11
3.1. NASTAVENÍ TCP/IP VE WINDOWS....11
3.1.1. Než začnete....11
3.1.2. Windows XP....12
3.1.3. Windows Vista....12
3.1.4. Windows 95, 98....13
3.1.5. Windows NT 4.0 Workstation....13
3.1.6. Windows 2000....14
3.1.7. Windows ME....14
3.1.8. Statického nastavení IP Adresy na PC....16

4. SPRÁVA ZAŘÍZENÍ 17
4.1. PŘIHLÁŠENÍ....17
4.2. SETUP....18
4.2.1. SETUP – nastavení WAN....19
4.2.2. SETUP – LAN Setup....30
4.2.3. LAN Setup – Ethernet Switch....34
4.2.4. Log Out....34
4.3. ADVANCED....35
4.3.1. ADVANCED – UPnP....36
4.3.2. ADVANCED – SNTP....36
4.3.3. ADVANCED – SNMP....38
4.3.4. ADVANCED – TR-069....39
4.3.5. ADVANCED – Port Forwarding....40
4.3.6. ADVANCED – IP Filters....44
4.3.7. ADVANCED – LAN Clients....46
4.3.8. ADVANCED – LAN Isolation....46
4.3.9. ADVANCED – TR-068 WAN Access (Vzdálený přístup)....47
4.3.10. ADVANCED – Bridge Filters....48
4.3.11. ADVANCED – Web filtr....49
4.3.12. ADVANCED – Dynamic DNS Klient....50

4.3.13. ADVANCED – IGMP Proxy 51
4.3.14. ADVANCED – Static Routing 52
4.3.15. ADVANCED – Dynamic Routing 53
4.3.16. Quality of Service (QoS) – objasnění pojmů 55
4.3.17. ADVANCED – Ingrees 56
4.3.18. ADVANCED – Egress 60
4.3.19. ADVANCED – Shaper 62
4.3.20. ADVANCED – Policy Routing 64
4.3.21. ADVANCED – Web Access Control 65
4.3.22. ADVANCED – SSH Access Control 66
4.4. WIRELESS 67
4.4.1. WIRELESS – Setup 67
4.4.2. WIRELESS – Configuration 69
4.4.3. WIRELESS – Multiple SSID 70
4.4.4. WIRELESS – Security 71
4.4.5. WIRELESS – Management 75
4.4.6. WIRELESS – WDS 76
4.5. TOOLS 77
4.5.1. TOOLS – System Commands 77
4.5.2. TOOLS – Remote Log-Router 78
4.5.3. TOOLS – Remote Log-Voice 79
4.5.4. TOOLS – User Management 79
4.5.5. TOOLS – Update Gateway 80
4.5.6. TOOLS – Ping Test 82
4.5.7. TOOLS – Test modemu 82
4.6. STATUS 83
4.6.1. STATUS – Network Statistics 84
4.6.2. STATUS – Connection Status 85
4.6.3. STATUS – DDNS Update Status 85
4.6.4. STATUS – DHCP Clients 86
4.6.5. STATUS – QOS TCA NTCA Status 86
4.6.6. STATUS – Modem Status 87
4.6.7. STATUS – Product Information 87
4.6.8. STATUS – System Log 87
4.6.9. STATUS – WDS Report 88
4.7. HELP 88

PŘÍLOHA A: VÝKLAD POUŽÍVANÝCH POJMŮ **89**

PŘÍLOHA B: ČASTÉ OTÁZKY **90**

PŘÍLOHA C: ŘEŠENÍ POTÍŽÍ **92**

PŘÍLOHA D: UPNP NASTAVENÍ VE WINDOWS XP **94**

PŘÍLOHA E: SLOVNÍK **95**

SPECIFIKACE A INFORMACE OBSAŽENÉ V TOMTO MANUÁLU JSOU POUZE INFORMAČNÍ A MOHOU BÝT V ZÁVISLOSTI NA ZMĚNÁCH VLASTNOSTÍ FIRMWARE KDYKOLI ZMĚNĚNY BEZ PŘEDBĚŽNÉHO UPOZORNĚNÍ.

1.1. Autorská práva

1.2. Obchodní značky

1.3. Prohlášení o shodě

JOYCE ČR tímto prohlašuje, že WELL PTI-1605G je ve shodě se základními požadavky a s dalšími příslušnými ustanoveními Nařízení vlády České republiky č. 426/2000 Sb. Prohlášení o shodě je umístěno na www.joyce.cz.

1.4. Charakteristika

WELL ADSL router má následující znaky:

- v plném rozsahu vyhovuje standardům ANSI T1.413 vydání 2., ITU-TG.992.1 a ITU-T G.992.2. ITU-G.992.3, ITU 992.4, ITU G.992.5 a READSL2
- plně vyhovuje specifikacím Annex A/B/B(U-R2) ADSL
- rychlost datového toku na vstupu až 24Mb/s a na výstupu až 1Mb/s.
- PPPoE/PPP protokol pro dial-up ADSL služby
- podporuje funkci firewallu
- podporuje funkci UPnP
- webové rozhraní pro instalaci a správu
- vestavěný 8 portový 10/100 Mb/s switch pro LAN spojení
- vyhovuje specifikacím IEEE 802.3/802.3u a automatickému výběru mezi nimi
- podporuje plně duplexní provoz podle IEEE 802.3
- podporuje funkci filtrování paketů
- flash paměť pro upgrade firmwaru
- hardwarové resetové tlačítko pro rychlé obnovení původního nastavení
- LED diody pro indikaci spojení

ADSL standardy

- v plném rozsahu vyhovuje standardům ANSI T1.413 vydání 2., ITU-T G.992.1
- a ITU-T G.992.2.
- rychlost příchozího datového toku až 8Mb/s odchozího až 1Mb/s.
- podporuje funkci Dying Gasp

ATM protokoly

- podporuje PPPoA (RFC2364)
- podporuje PPPoE (RFC2516)
- routovaný/přemostěný (router/bridged) Ethernet přes ATM (RFC1483)
- klasická IP přes ATM (RFC1577)
- ATM forum UNI 3.1/4.0 PVC, ATM SAR, ATM AAL5 a OFM F4/F5

802.11g bezdrátová síť

- vyhovuje standardu IEEE 802.11g, podporuje i 11g+ standard
- OFDM modulace s rychlostí datového toku až 54Mb/s, OFDM (64QAM, 16QAM, QPSK, BPSK) and DSSS (DBPSK, DQPSK, CCK)
- podpora pásma frekvencí mezi 2.412GHz ~ 2.484GHz
- podporuje 64 bitové a 128 bitové WEP šifrování
- podporuje WPA, WPA2, 802.1x, TKIP a AES šifrování
- bezdrátový přístup může být omezen pomocí MAC adresy
- bezdrátové vysílání ID sítě může být vypnuto, takže se mohou připojit pouze zařízení se stejným ID (SSID)
- vestavěná SMA anténa s funkcí diversity

Mód routeru

- IP routování – RIPv1 a RIPv2
- statické routování
- DHCP server a klient
- podporuje DNS proxy
- podporuje NAT a NAPT
- podporuje VPN pass-through (IPSec, L2TP, PPTP)
- podporuje SNMP funkci
- podporuje ICMP a IGMP

Firewall

- podporuje firewallove funkce
- podporuje IP filtraci
- podporuje MAC filtraci
- podporuje URL filtraci
- podporuje filtrovací služby
- podporuje politiku přístupu

UPnP

- podporuje funkci UPnP

Ethernetové standardy

- vestavěný 8 portový 10/100Mb/s Ethernetový switch vyhovující IEEE 802.3x standardům
- automatický MDI/MDI-X crossover pro 10/100Base-T port

Řízení z webového rozhraní

- upgrade firmwaru přes FTP
- Návrat k továrnímu nastavení pomocí webového rozhraní nebo hardwarovým resetovacím tlačítkem
- statistika spojení WAN a LAN
- konfigurace statických cest a routovací tabulka, NAT/NAPT a VCs
- PPP uživatelská identifikace ID a heslo

1.5. Rozsah

Tento dokument poskytuje popis a použití webového rozhraní ADSL routeru, které slouží ke konfiguraci a k nastavení. Jsou uvedeny popisy a koncepty jak základního, tak pokročilého menu. Pro dokonalejší porozumění těmto webovým stránkám jsou některé otázky a odpovědi připojeny pod definici každé webové stránky spolu s dodatky na konci příručky.

Tento dokument je určen pro zákazníky, kteří si zakoupí ADSL router a používají dodaný firmware. Předpokládá se, že uživatel má základní povědomí o ADSL, bezdrátovém připojení a sítích.

1.6. Struktura dokumentu

Úvod, stručné seznámení s výrobkem a uživatelskou příručkou.
Popis, technická data a hardwarové zapojení přístroje ADSL2/2+ router.
Nastavení TCP/IP ve Windows, konfigurace sítě.
Správa zařízení, popis webových stránek, které se nacházejí v menu Admin. Na těchto stránkách může uživatel prohlížet, měnit, aktualizovat a ukládat nastavení nebo konfiguraci přístroje.

Příloha A	Použité termíny; výklad použitých technických termínů
Příloha B	Časté dotazy; soubor odpovědí na možné dotazy, týkající se ADSL2/2+ routeru.
Příloha C	Řešení potíží; soubor otázek a odpovědí na problémy, které se týkají Windows sítě a konfigurace ADSL2/2+ routeru.
Příloha D	Nastavení UPnP, průvodce konfigurací UPnP ve Windows XP
Příloha E	Slovník; definice pojmů a zkratek

1.7. Požadavky na systém

- Osobní počítač (PC/notebook s/bez nainstalovaného 11b nebo 11g bezdrátového adaptéru).
- Pentium II kompatibilní procesor a vyšší.
- Internetový prohlížeč
- 64 MB RAM nebo více.
- Minimálně 50 MB volného místa na disku
- Ethernet Network Interface Controller (NIC) RJ-45 port (Síťovou kartu).
- Ethernetový kabel (CAT5).
- CD-ROM mechaniku.

1.8. Obsah balení

- ADSL router
- CD-ROM (Manuál/Průvodce rychlým nastavením)
- Tištěná dokumentace
- Síťový adaptér
- RJ-11 ADSL kabely
- Ethernetové kabely

2. POPIS ZAŘÍZENÍ

2.1. POPIS ZAŘÍZENÍ WELL PTI-1605G

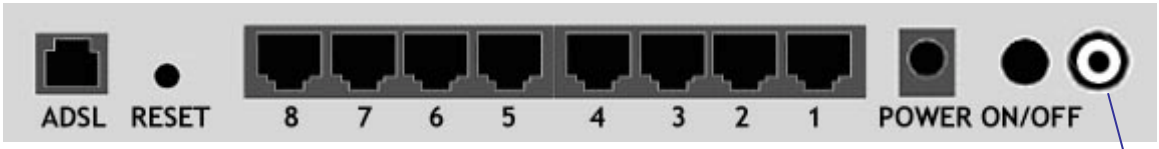
Čelní panel:

LED indikátory ADSL routeru zobrazují informace o stavu zařízení.

PWR	Svítí, když je router zapojen do sítě
WL ACK	Svítí, když je bezdrátová část je připravena poskytovat bezdrátové služby. Bliká, když je bezdrátová komunikace aktivní.
1 – 8 (LINK/ACT)	Ukazuje aktivitu Ethernetových (LAN) portů 1 – 8. Bliká, když router odesílá/přijímá data.
ADSL	Svítí, když je úspěšně navázáno ADSL spojení. Bliká, když dochází k migraci dat.
PPP	Svítí, když je navázáno PPP spojení.

Zadní panel:

Zadní panel ADSL routeru obsahuje LAN, ADSL, resetové tlačítko, připojení síťového adaptéru.



Anténa

ADSL	Port pro připojení poskytovatele ADSL služeb.
RESET	Vrátí router do továrního nastavení.
Porty 1 – 8	Osm 10/100MB/s Eth. portů pro připojení síťových zařízení.
POWER	Konektor pro síťový adaptér 9V AC/1A nebo 12V DC/1A
ON/OFF	Tlačítko pro zapnutí/vypnutí routeru.
Anténa	Konektor na vnější 2,4GHz dipólovou anténu (součástí balení).

Tlačítko RESET:

Restartuje a vrátí ADSL router do továrního nastavení. Držte tlačátko po dobu 10-15 sec. Za 30 sec. je router připraven k používání.

Všechny ethernetové porty ADSL routeru podporují automatické rozpoznání překříženého kabelu.

2.2. Hardwarové připojení:

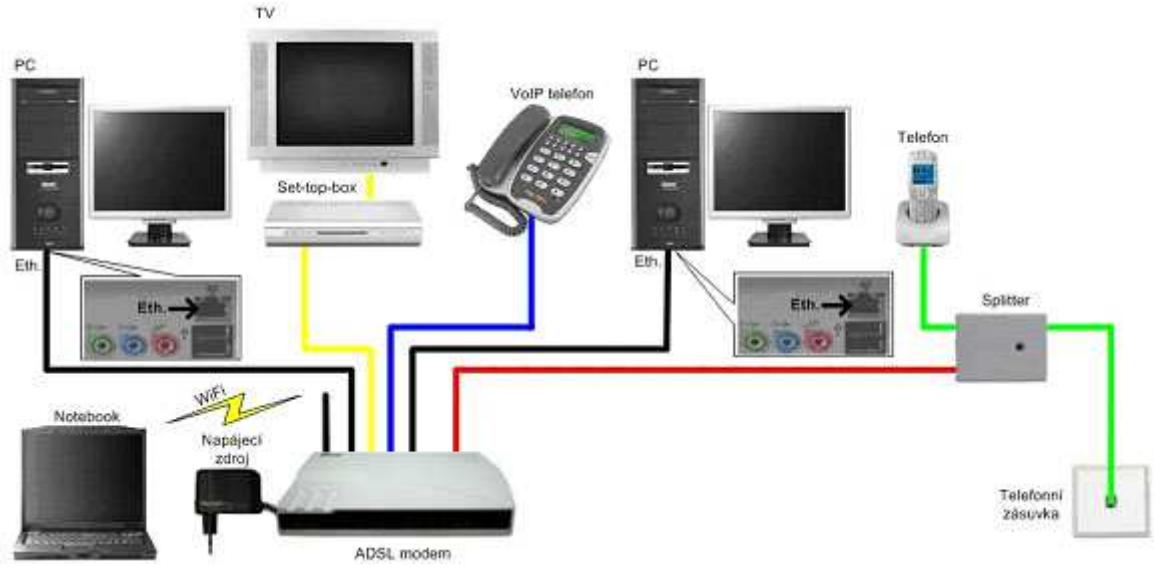
Tato sekce popisuje mechanismus hardwarového připojení vašeho routeru do vaší místní sítě (LAN), popisuje, jak nakonfigurovat váš ADSL router pro připojení k internetu nebo jak manuálně nakonfigurovat vaše internetové spojení.

Než budete moci zřídit internetové spojení pomocí ADSL routeru, budete si muset nejdříve připravit následující věci:

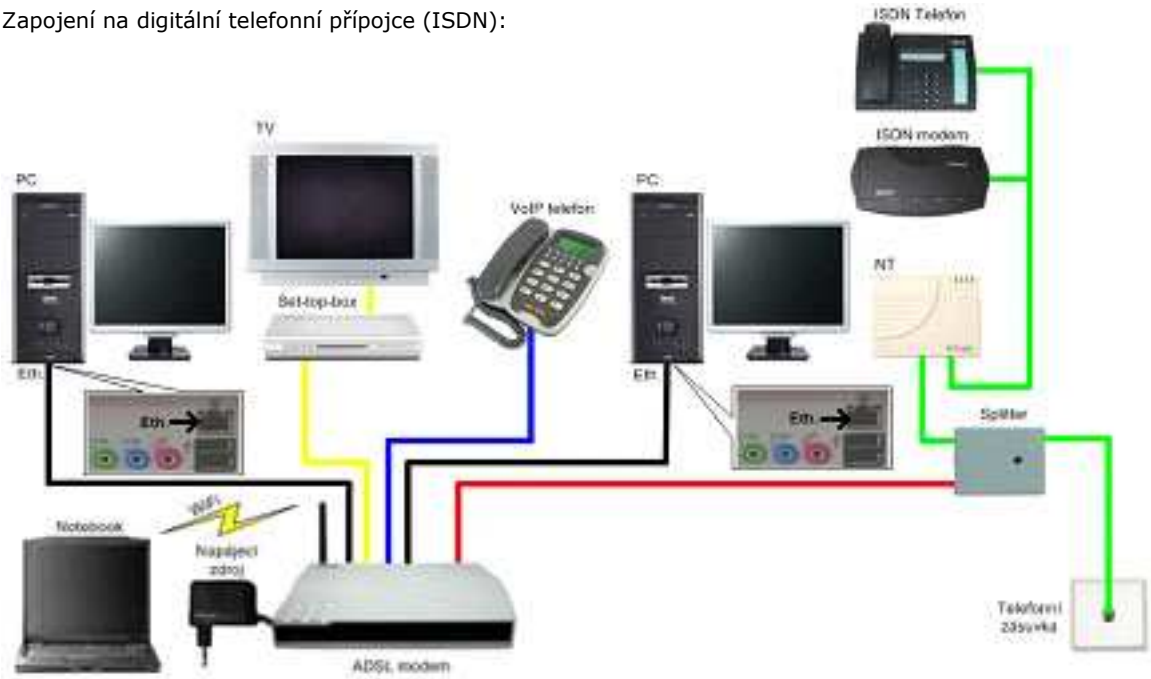
- Počítač (notebook), který musí mít nainstalovaný Ethernetový adaptér (síťovou kartu) a Ethernetový kabel.
- Počítač (notebook), který má nainstalovaný bezdrátový adaptér se standardem 802.11b nebo 802.11g.
- Účet služby ADSL a informace o jeho konfiguraci dodávané vaším poskytovatelem internetových služeb (ISP). Pro připojení vašeho ADSL routeru k internetu budete potřebovat jeden nebo více následujících konfiguračních parametrů:
  a) VPI/VCI parametry
  b) Multiplexní metodu
  c) Jména hostitele a domény
  d) Logovací jméno a heslo vašeho ISP
  e) Adresu doménového serveru (DNS) vašeho ISP
  f) Fixní nebo statickou IP adresu

Následující ilustrativní schéma ukazuje mechanismus hardwarového spojení Vašeho ADSL routeru.

Zapojení na standardní analogové telefonní přípojce:



Zapojení na digitální telefonní přípojce (ISDN):



Kroky ke správnému zapojení vašeho ADSL routeru:

1. Vypněte váš počítač (notebook).
2. Jeden konec RJ-11 kabelu vložte do ADSL portu vašeho ADSL routeru a druhý do zdířky pro ADSL linku na rozbočovači (splitteru).
3. Propojte počítač s ADSL routerem pomocí Ethernetového kabelu (RJ-45).
4. Zasuňte napájecí adaptér do ADSL routeru a zapojte ho do el. sítě.
5. Zapněte router.

Po zapnutí ADSL routeru bude svítit Power dioda.
Automatický diagnostický proces bude zapínat a vypínat LED diodu.

6. Zapněte váš počítač.
7. Nahlédněte do následující sekce pro nastavení a konfiguraci vašeho PC.

3. KONFIGURACE PC

3.1. Nastavení TCP/IP ve Windows

Instrukce v této kapitole vám pomohou nakonfigurovat váš počítač tak, aby mohl komunikovat s ADSL routerem.

Počítače používají pro vstup na Internet protokol nazvaný TCP/IP (Transmission Control Protocol / Internet Protocol). Každý počítač (notebook) ve vaší síti musí mít nainstalovaný TCP/IP a používat ho jako svůj síťový protokol. Pokud je ve vašem počítači nainstalována karta síťového rozhraní (NIC), pak je pravděpodobně nainstalován i TCP/IP.

Následující popis předpokládá, že ADSL router je v továrním nastavení. (Pokud ne, podržte alespoň 10 sekund resetovací tlačítko). Přednastavená IP adresa ADSL routeru je 10.0.0.138.

Následuje postup pro nastavení vašeho počítače (notebooku) jako DHCP klienta.

3.1.1. Než začnete

Standardně ADSL router automaticky přiřazuje všechna potřebná internetová nastavení připojeným počítačům sám. Na počítačích je jen třeba zajistit, aby tato nastavení akceptovaly.

V některých případech byste mohli chtít zadat informace pro připojení k Internetu všem nebo alespoň některým počítačům v síti ručně. V další části najdete návod, jak to udělat.

Následující návod vychází z toho, že Vaše počítače již jsou připojeny do sítě prostřednictvím síťového adaptéru.

Postupujte podle instrukcí odpovídajících nainstalovanému operačnímu systému.

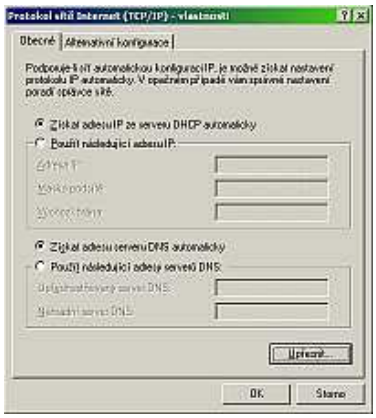
3.1.2. Windows XP

Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

1. Klikněte na tlačítko Start systému Windows a potom na **Ovládací panely**.
2. Poklepejte na ikonu **Síťová připojení**.
3. V oddíle „LAN nebo vysokorychlostní Internet" klikněte pravým tlačítkem na ikonu odpovídající vaší síťové kartě a vyberte **Vlastnosti**. Viz. obrázek napravo. (tato ikona je často nazvána *Připojení k místní síti*.)

4. Přesvědčte se, že je zaškrtnuto políčko vedle protokolu TCP/IP a klikněte na tlačítko **Vlastnosti**. Pokud protokol TCP/IP není přítomen, proveďte instalaci tohoto protokolu.

5. Zde zvolte možnosti **Získat IP adresu ze serveru DHCP automaticky** a **Získat adresu serveru DNS automaticky**.
6. Dvojím kliknutím na tlačítko OK potvrďte a uložte provedené změny.



Postup nastavení TCP/IP protokolu je v ostatních OS obdobný, jen v ostatních OS Windows se mohou lišit okna „Vlastnosti TCP/IP protokolu".

3.1.3. Windows Vista

Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

1. Klikněte na Start, pak **Nastavení** (*tato položka platí pouze v Klasickém módu zobrazení Windows Vista*) a **Ovládací Panely**.

2. Poklepejte na **Centrum sítí a sdílení**.

3. Klikněte na **Spravovat síťová připojení**.

4. Pravým tlačítkem myši klikněte na **LAN** (Local Area Connection) - může být popsáno jako **LAN – „název síťového adaptéru používaného pro připojení k LAN"**, a vyberte **Vlastnosti**. Pokud máte aktivní Řízení uživatelských účtů, potvrďte v dalším okně kliknutím na Pokračovat.

5. Klikněte na Protokol **TCP/IPv4 – Internet Protocol verze 4** a na tlačítko **Vlastnosti**. Pokud protokol TCP/IPv4 není přítomen, proveďte instalaci tohoto protokolu.

6. Zobrazte záložku **Obecné**, zvolte **Získat adresu IP ze serveru DHCP automaticky** a rovněž **Získat adresu serveru DNS automaticky**, poté klikněte na OK.

3.1.4. Windows 95, 98

Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

1. Klikněte na tlačítko Start systému Windows, ukažte na **Nastavení** a potom klikněte na **Ovládací panel**.
2. Poklepejte na ikonu Síť.

   Zobrazí se dialogový rámeček Síť se seznamem instalovaných síťových komponent. Najdete-li v seznamu položku TCP/IP, byl již protokol nainstalován. Pokračujte krokem 9.

3. Pokud mezi instalovanými komponentami protokol TCP/IP není, klikněte na tlačítko **Přidat** a zobrazí se dialog pro výběr typu síťové komponenty.
4. Vyberte **Potokol** a klikněte na tlačítko **Přidat**. Zobrazí se dialog pro výběr síťového protokolu.
5. V seznamu výrobců vyberte **Microsoft** a ze seznamu protokolů vyberte **TCP/IP**.
6. Klikněte na OK, čímž se vrátíte do dialogu síť a zde opět klikněte na OK.

   Pravděpodobně budete vyzváni ke vložení instalačního média (CD-ROM). Postupujte podle pokynů pro instalaci potřebných souborů.

7. Klikněte na OK po výzvě k restartu PC a dokončete instalaci TCP/IP.

   V dalších krocích nastavíme počítač, aby akceptoval IP informace z ADSL Wireless/Ethernet routeru.

8. Otevřete okno **Ovládacího panelu** a poklepejte na ikonu **Síť**.
9. Vyberte protokol TCP/IP a klikněte na tlačítko **Vlastnosti**.

   V případě, že je položka TCP/IP v seznamu uvedena vícekrát, zvolte tu, která je navázána na síťovou kartu.

10. V dialogu Vlastnosti TCP/IP vyberte záložku IP adresa.
11. Z nabízených možností vyberte **Získat IP adresu automaticky**.
12. Vyberte záložku Konfigurace DNS a zde opět vyberte možnost **Získat IP adresu automaticky**.
13. Dvojím kliknutím na OK potvrďte a uložte provedené změny.

    Budete vyzváni k restartování Windows.

14. Klikněte na **Ano**.

3.1.5. Windows NT 4.0 Workstation

Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

1. Klikněte na tlačítko Start systému Windows, ukažte na **Nastavení** a klikněte na **Ovládací panel**.
2. V okně ovládacího panelu poklepejte na ikonu Síť.
3. V dialogu Síť vyberte záložku Protokoly.

   Pod záložkou Protokoly najdete seznam instalovaných síťových protokolů. Obsahuje-li položku TCP/IP, potom byl již protokol nainstalován. Můžete pokračovat od bodu 9.

4. Pokud TCP/IP není mezi instalovanými komponentami, klikněte na tlačítko **Přidat**.
5. V dialogu pro výběr protokolu vyberte TCP/IP a klikněte OK.

   Pravděpodobně budete vyzváni k instalaci souborů z instalačního média. Postupujte podle pokynů pro instalaci souborů. Po instalaci souborů se zobrazí informace, že by mohla být nainstalována služba DHCP pro dynamické přidělování IP adres.

6. Zvolte **Ano** a potom klikněte na OK, budete-li vyzváni k restartu počítače.

Nyní nastavíme počítač, aby akceptoval IP informace z ADSL Ethernet /Wireless routeru.

7. Otevřete okno Ovládacího panelu a poklepejte na ikonu Síť.
8. V dialogu Síť vyberte záložku Protokoly.
9. Zde označte TCP/IP a klikněte na **Vlastnosti**.
10. Ve vlastnostech protokolu Microsoft TCP/IP zvolte možnost **Získat IP adresu z DHCP serveru**.
11. Dvojím kliknutím na tlačítko OK potvrďte a uložte provedené změny a zavřete Ovládací panel.

3.1.6. Windows 2000

Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

1. Klikněte na tlačítko Start systému Windows, ukažte na **Nastavení** a klikněte na **Ovládací panel**.
2. Poklepejte na ikonu Síťová a telefonická připojení.
3. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na ikonu Připojení k místní síti a vyberte **Vlastnosti**.

   Ve vlastnostech Připojení k místní síti se zobrazí seznam instalovaných síťových komponent. Obsahuje-li tento seznam položku TCP/IP, potom byl protokol již nainstalován. Můžete pokračovat od bodu 10.

4. Není-li mezi instalovanými komponentami protokol TCP/IP, klikněte **Nainstalovat...**.
5. V dialogu Vybrat typ síťové součásti vyberte **Protokol** a klikněte na **Přidat...**.
6. Zvolte **Protokol sítě Internet (TCP/IP)** a poté klikněte na OK.

   Může se zobrazit výzva k instalaci souborů z instalačního média. Postupujte podle pokynů na obrazovce.

7. Budete-li vyzváni, klikněte na OK, aby se počítač restartoval s novým nastavením.

   Nyní nakonfigurujeme počítač, aby akceptoval IP informace z ADSL Wireless/Ethernet routeru.

8. V Ovládacím panelu poklepejte na ikonu Síťová a telefonická připojení.
9. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na ikonu Připojení k místní síti a vyberte **Vlastnosti**.
10. Ve vlastnostech Připojení k místní síti vyberte **Protokol sítě Internet (TCP/IP)** a opět klikněte na **Vlastnosti**.
11. Ve vlastnostech protokolu TCP/IP vyberte možnost **Získat IP adresu automaticky**. Obdobně vyberte možnost **Získat adresu DNS serveru automaticky**.
12. Dvojím kliknutím na OK potvrďte a uložte provedené změny a zavřete Ovládací panel.

3.1.7. Windows ME

1. Klikněte na tlačítko Start systému Windows, ukažte na **Nastavení** a poté klikněte na **Ovládací panel**.
2. Poklepejte na ikonu Síťová a telefonická připojení.
3. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na **ikonu** Připojení k místní síti a vyberte **Vlastnosti**.

   Zobrazí se seznam instalovaných síťových komponent. Obsahuje-li tento seznam Protokol sítě Internet (TCP/IP), potom byl již protokol nainstalován. Pokračujte krokem 11.

4. Není-**li** Protokol sítě Internet mezi instalovanými položkami, klikněte **Přidat...**.
5. V dialogu Vybrat typ síťové součásti vyberte **Protokol** a klikněte **Přidat...**.
6. Ze seznamu výrobců vyberte **Microsoft**.
7. Vyberte z nabízených možností **Protokol sítě Internet (TCP/IP)** a klikněte na OK.

   Může se zobrazit výzva k instalaci souborů z instalačního média. Postupujte podle pokynů na obrazovce.

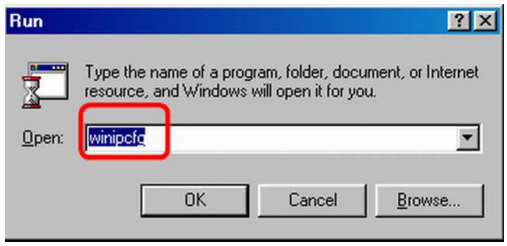
8. Budete-li vyzváni, klikněte na OK, aby se počítač restartoval s novým nastavením.

   Nyní nakonfigurujeme počítač, aby akceptoval IP informace z ADSL Wireless/Ethernet routeru.

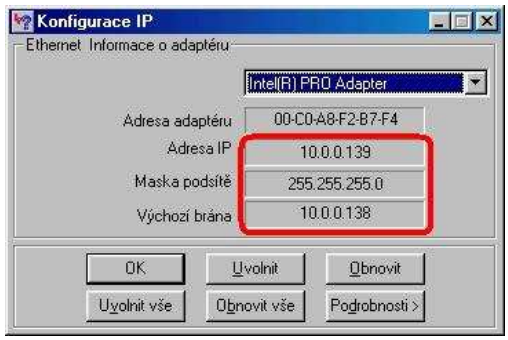
9. V Ovládacím panelu poklepejte na ikonu Síťová a telefonická připojení.
10. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na ikonu Síť a vyberte **Vlastnosti**.
11. Ve vlastnostech sítě vyberte **TCP/IP** a klikněte na tlačítko **Vlastnosti**.
12. V nastavení TCP/IP vyberte možnost **IP adresu přidělí server**. Podobně zvolte možnost **Adresu jmenného serveru přidělí server**.
13. Dvojím kliknutím na tlačítko OK potvrďte a uložte provedené změny a zavřete Ovládací panel.

Po nastavení restartujte PC a můžete se přesvědčit, že DHCP server ADSL routeru opravdu přidělil Vašemu PC IP adresu.

A. Windows 98/ME:

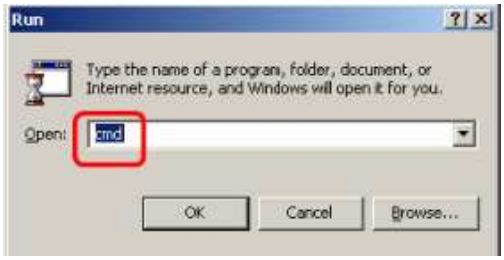


1. Klikněte na "Start" a "Spustit" ("Run").
2. Do pole Otevřít (Open) vepište "**winipcfg**", poté stiskněte "OK".



3. Objeví se okno, ve kterém budou zobrazeny informace o Ethernetovém adaptéru. Zkontrolujte, zda máte následující nastavení:
   - o IP adresa 10.0.0.x
   - o Maska podsítě 255.255.255.0
   - o Výchozí brána jako 10.0.0.138
4. Pokud IP adresa náhodou přidělena není, klikněte na Uvolnit (Release) a pak na Obnovit (Renew).
5. Na konci procesu klikněte na "OK".

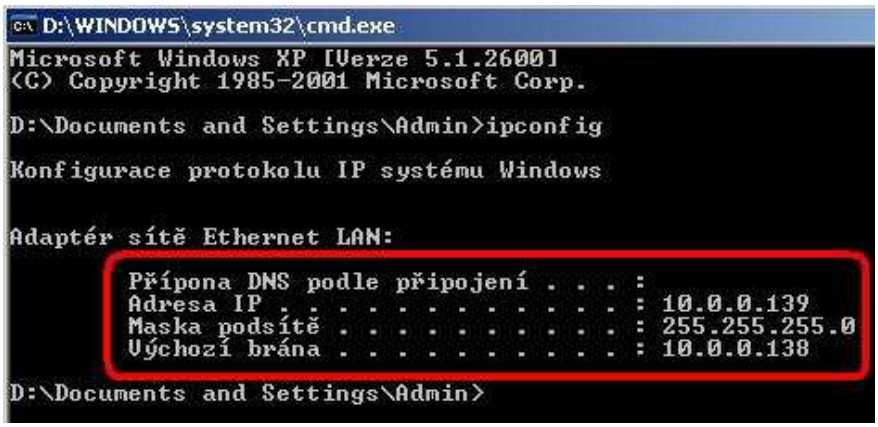
B. Windows 2000/XP/Vista:



1. a) (2000/XP) - Klikněte na "Start" a "Spustit" ("Run").

   b) (Vista) - Klikněte na "Start".
2. a) (2000/XP) - Do pole Otevřít (Open) vepište "**cmd**" a poté klikněte na "OK".

   b) (Vista) - Do pole pro vyhledávání („Zahájit hledání") vepište "**cmd**" a potvrďte klávesou "Enter".
3. V příkazovém řádku vepište "**ipconfig**", poté stiskněte "Enter".



V okně příkazového řádku budou zobrazeny veškeré informace o Ethernetovém adaptéru. Zkontrolujte, zda máte následující nastavení:

- o IP adresa 10.0.0.x
- o Maska podsítě 255.255.255.0
- o Výchozí brána 10.0.0.138

4. Pokud IP adresa náhodou přidělena není, zadejte příkaz „ipconfig /release" pro uvolnění IP a následně „ipconfig /renew" pro obnovení IP adresy
5. K uzavření okna napište "Exit" a stiskněte "Enter".

3.1.8. Statického nastavení IP Adresy na PC

V některých případech možná nebudete chtít, aby IP adresy přiděloval ADSL router, ale budete je zadávat některým, popř. všem počítačům v síti ručně (někdy se též používá termín „fixní IP"). Kdy lze s výhodou tuto možnost využít (ačkoliv to není nezbytné):

- Získali jste několik veřejných IP adres a chcete, aby určitý počítač používal určitou adresu (některý z počítačů plní např. úlohu veřejně přístupného webového serveru).
- Provozujete v síti několik podsítí.

Pokud ještě neznáte následující informace, obraťte se na Vašeho ISP:

- IP adresa a maska podsítě pro počítače, jimž chcete přidělit statické IP informace.
- IP adresa výchozí brány Vaší sítě. Ve většině případů jí bude IP adresa síťového portu ADSL routeru. Ve výchozím stavu má router pro tento port nastavenu adresu 10.0.0.138. (Tuto hodnotu můžete změnit, případně ji může změnit Váš ISP
- IP adresa DNS (Domain Name System) serveru Vašeho ISP.

U každého počítače, jemuž hodláte přidělit statické informace síťového připojení, postupujte podle výše uvedených pokynů (pro příslušný operační systém), alespoň pokud jde o instalaci IP protokolu. Namísto dynamického přidělování IP adres a souvisejících údajů však volte možnost **ručního zadání** a do příslušných polí zapište IP adresu počítače, IP adresy výchozí brány a DNS serveru.

Nezapomeňte, že Vaše počítače musí mít takovou IP adresu, která je řadí do stejné podsítě se síťovým portem ADSL Wireless/Ethernet routeru.

- Router byl nakonfigurován tak, aby počítači přidělil vhodnou IP Adresu. Budete-li chtít toto automatické přidělování IP adresy (DHCP server) používat, musíte nastavit PC tak, aby dynamicky přidělovanou adresu akceptoval. V předcházející části najdete návod jak postupovat, s přihlédnutím k použitému operačnímu systému.
- Chcete-li počítači přidělit statickou IP adresu, postupujte podle části „Přidělení statického internetového nastavení", viz výše. Použijte následující informace:

Příklad konfigurace Vašeho počítače:
IP adresa: 10.0.0.n, kde n je číslo od 3 do 253
Maska podsítě: 255.255.255.0
Výchozí brána: 10.0.0.138
DNS: 10.0.0.138

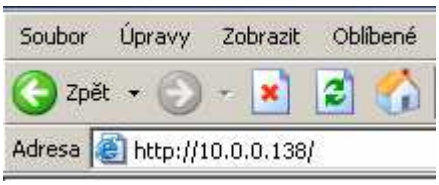
4. SPRÁVA ZAŘÍZENÍ

Pro usnadnění práce byly utility pro správu ADSL routeru naprogramované přímo do něj. Tato kapitola vysvětlí všechny funkce této utility. Veškerá správa ADSL routeru je prováděna přes tuto webovou utilitu.

4.1. Přihlášení

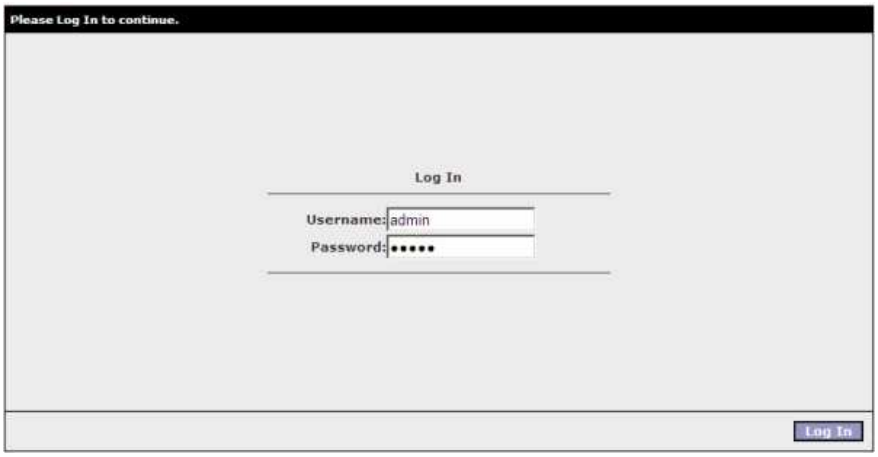
Pro přístup ke stránkám s konfigurací ADSL2/2+ routeru jsou potřeba následující kroky:

1. Otevřete Web prohlížeč (Internet Explorer, Netscape apod.)
2. Do adresového řádku vložte IP adresu ADSL2/2+ routeru http://10.0.0.138 a stiskněte Enter.



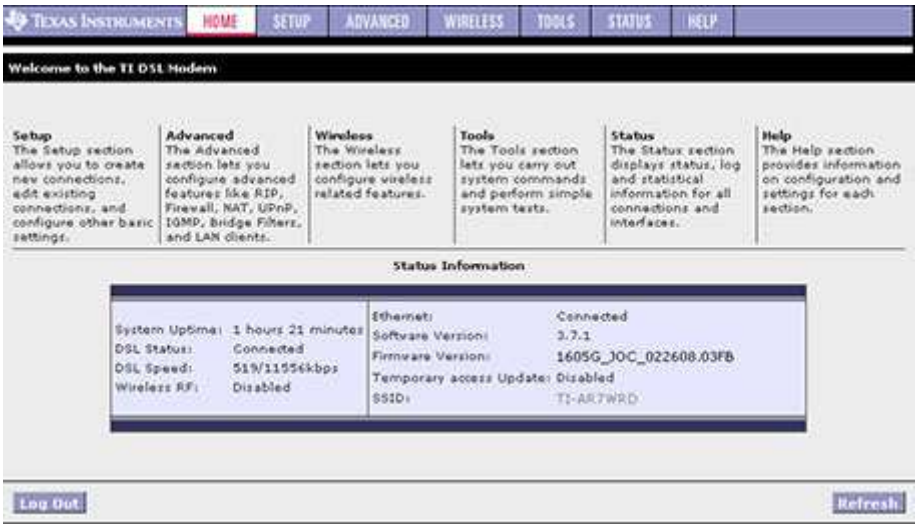
3. Zobrazí se výzva k zadání uživatelského jména a hesla. Výchozí uživatelské jméno je „**admin**" a heslo „**admin**".

Poznámka - Pozor, při zadávání rozlišujte velká a malá písmena.



Uživatelské jméno a heslo mohou být po přihlášení změněna v části **Tools-User Management**, postup je popsán v části Nástroje **(Tools)**.

Po zadání hesla z webového prohlížeče se načte HOME stránka s celkovým přehledem konfigurace.

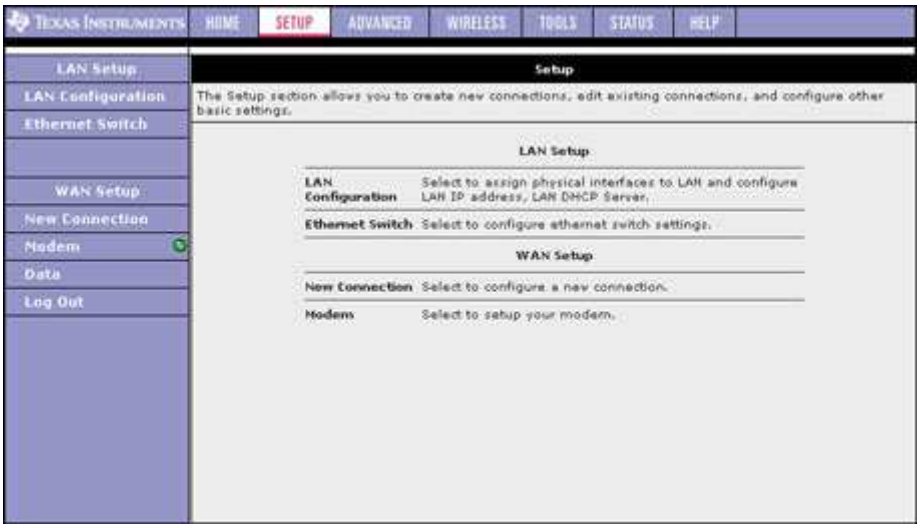


- **HOME**: Oddíl **Home** obsahuje celkový přehled konfigurace a odkazy k ostatním oddílům.
- **SETUP:** Zde můžete vytvářet nová spojení, editovat spojení existující a konfigurovat ostatní základní nastavení.
- **ADVANCED:** V oddíle **Advanced** můžete konfigurovat pokročilé funkce jako RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters a klienty LAN.
- **WIRELESS:** V oddílu **Wireless** je možno konfigurovat bezdrátové spojení a související funkce.
- **TOOLS:** Z oddílu **Tools** můžete spouštět jednoduché testy systému a zadávat systémové příkazy.
- **STATUS:** Oddíl **Status** zobrazuje status, přihlašovací a statistické informace pro všechna spojení a interface.
- **HELP:** Informace a pomoc při nastavování a konfiguraci v každém oddíle.
- **Status Information:** Zobrazení aktuálního stavu spojení.
  - **System Uptime:** Délka provozu ADSL2/2+ routeru od zapnutí.
  - **DSL Status:** Zobrazuje stav spojení ADSL2/2+ routeru.
  - **DSL Speed:** Rychlost proudu příchozích/odchozích dat v kilobitech za sekundu.
  - **Wireless RF:** Stav bezdrátového systému.
  - **Ethernet:** Stav Ethernetového připojení.
  - **Software Version:** Verze softwarového kódu.
  - **Firmware Version:** Verze firmwaru.
  - **SSID:** Název identifikující bezdrátovou síť.
- **Log Out: Zde klikněte pro odhlášení z webovské konfigurace routeru.**
- **Refresh: Zde klikněte pro znovunačtení zobrazované stránky.**

4.2. SETUP

Stránka konfigurace **SETUP** umožňuje vytvářet nová připojení, editovat připojení existující a konfigurovat další základní nastavení v modu WAN a LAN.

Menu konfigurace je rozděleno do dvou částí: nastavení LAN **(LAN Setup)** a WAN **(WAN Setup)**. První bude probráno nastavení WAN.



Je třeba, aby uživatel byl obeznámen s pojmy:

WAN (Wide Area Network) – vnější síť (v podstatě „internet")

LAN (Local Area Network) – vnitřní síť (síť místních počítačů a jiných zařízení)

WAN připojení

Na jedné straně routeru se nachází rozhraní WAN (neboli širokopásmové připojení). Typ připojení se pro jednotlivé poskytovatele připojení může lišit. Většina práce při konfiguraci bridge/routeru se týká nastavení WAN.

LAN připojení

Na druhé straně routeru se nachází rozhraní LAN. Sem jsou připojeny místní počítače, tiskárny, rozbočovače aj. RG ve výchozí konfiguraci podporuje všechny klienty LAN sítě, pokud jejich IP adresa je ve správném rozmezí.

4.2.1. SETUP – nastavení WAN

WAN Setup: Stránka konfigurace WAN umožňuje nastavit WAN/ADSL port. Připojení ADSL může být konfigurováno různými způsoby v závislosti na konfiguraci WAN poskytovatele a požadavcích vaší domácí nebo kancelářské sítě LAN. Tento ADSL2/2+ router podporuje následující typy ADSL připojení:

- **PPPoE** (RFC2516)
- **PPPoA** (RFC2364)
- **DHCP**
- **Statické**
- **Bridge** (RFC1483)

Pro konfiguraci těchto typů připojení budete potřebovat některé z následujících údajů:

- Uživatelské jméno a heslo k účtu u poskytovatele (k PPPoE a PPPoA)
- Nastavení VPI/VCI
- Typ zapouzdření/Multiplexování (LLC nebo VC, detaily si zjistěte u svého poskytovatele)
- ADSL Handshaking Mode (Výchozí nastavení je GDMT)
- Nastavení sítě pro operace v modu Bridge (most)

Pro spojení v režimu Bridge (RFC1483) budete botřebovat od svého poskytovatele následující údaje:

- DSL pevnou IP adresu
- Masku podsítě
- IP adresu výchozí brány
- IP adresu primárního DNS serveru

Můžete vytvořit a uložit až osm profilů WAN připojení.

V následující kapitole je detailně rozepsáno nastavení a uložení uvedených typů připojení.

4.2.1.1. SETUP – WAN Setup – New Connection

WAN připojení je virtuální spojení přes fyzickou DSL linku. Můžete definovat až osm různých virtuálních spojení. Máte-li definováno více virtuálních připojení, můžete pro ně uplatnit statické a dynamické směrování.

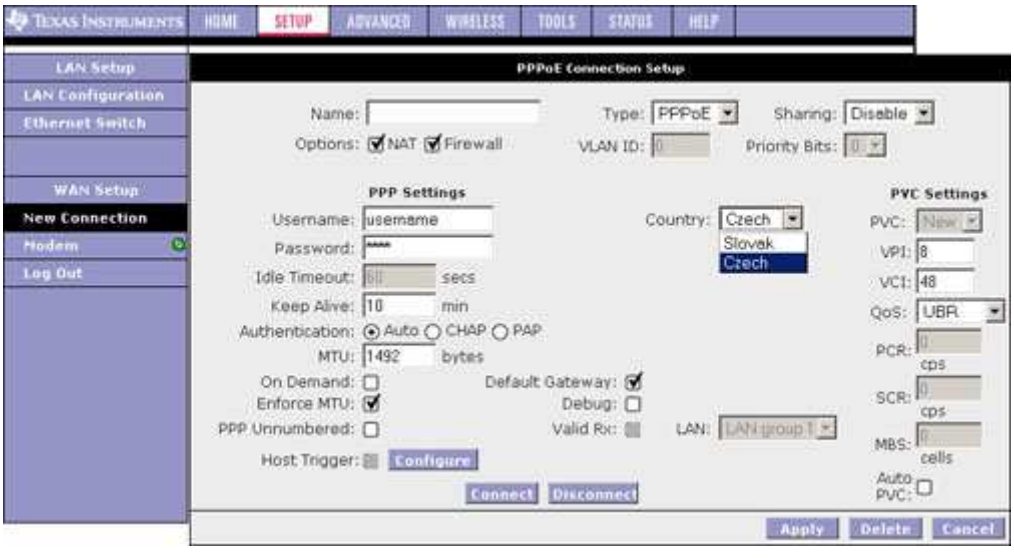
Před vytvořením nového WAN připojení musí být funkční DSL spojení. Správná funkce DSL modemu je signalizována zelenou LED ADSL.

Stránka **WAN Setup** umožňuje uživateli podle potřeby vytvářet, ukládat a vybírat profily připojení.

Ve většině případů bude stačit pouze jeden profil připojení, v jednom okamžiku může být aktivní pouze jeden profil.

4.2.1.1.1. Nové připojení – nastavení připojení PPPoE

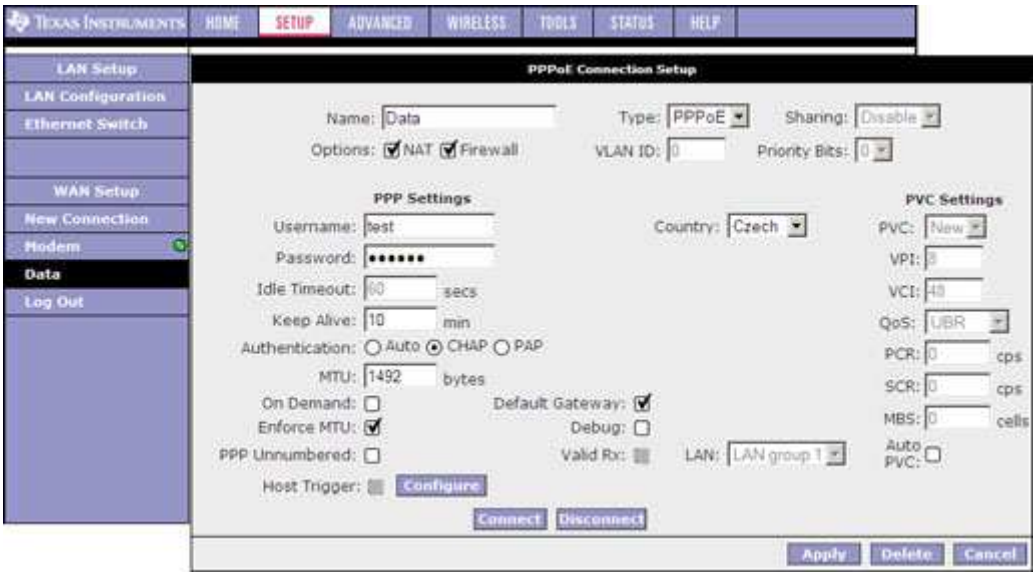
PPPoE: Po výběru možnosti **PPPoE** je zobrazeno následující okno. Protokol Point-to-Point (PPP) je způsob navázání spojení mezi dvěma hosty sítě. Protokol PPPoE, označovaný také jako RFC 2516, přizpůsobuje protokol PPP pro použití v síti Ethernet s ADSL připojením. PPPoE obsahuje mechanizmus autentizace uživatele prostřednictvím uživatelského jména a hesla a je to typ připojení používaný mnoha poskytovateli.



1. Na stránce **SETUP** klikněte na **New Connection**. Zobrazí se výchozí stránka **PPPoE Connection Setup**.

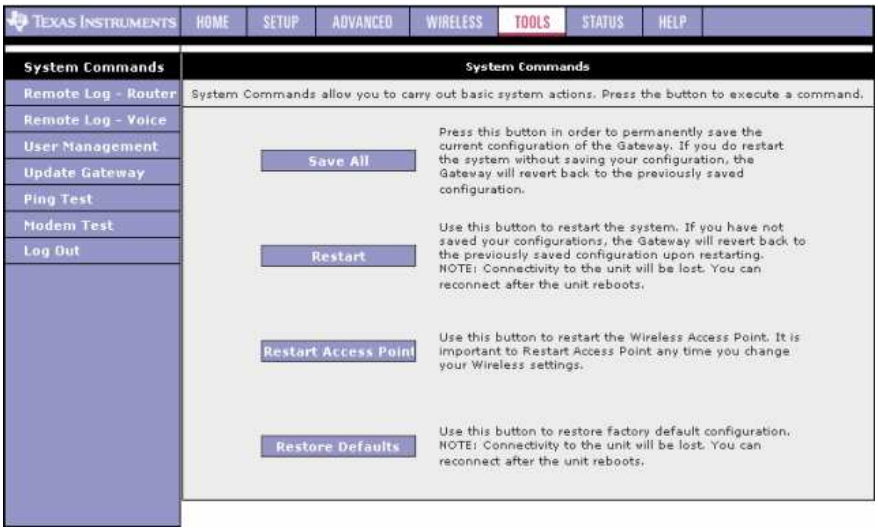
2. Do políčka **Name** napište Vámi zvolené jméno pro nově definované spojení. Jméno nesmí obsahovat mezery a musí začínat písmenem. Přednastavené je *Data*.
3. Volby **NAT** (překladač síťových adres) a **Firewall** ponechte zaškrtnuté.
4. Chcete-li zapnout VLAN, použijte údaje z tabulky 2 níže.
    - **Sharing (sdílení)** – zvolte VLAN – položky **VLAN ID** a **Priority Bits** se stanou aktivní.
    - **VLAN ID**
    - **Priority Bits**
5. **PPP Settings** – údaje pro tento oddíl Vám dodá poskytovatel internetového nebo DSL připojení nebo jsou již předkonfigurované.
6. **Country** – podle země, ve které se připojujete, zde vyberte Českou republiku (**Czech**) nebo Slovensko (**Slovak**). Tímto se, mimojiné, zároveň nastaví hodnoty VPI a VCI, které tak již následujícím bodě č. 7 nemusíte zadávat (doporučujeme ale hodnoty překontrolovat podle údajů, které Vám dodal Váš poskytovatel připojení).
7. **PVC** – po volbě země (**Country**) v předchozím bodě č. 6 by položky VPI a VCI v této části měli sloužit již jen pro kontrolu (dle údajů, které Vám musí dodat poskytovatel služeb připojení) – v následujícím příkladě jsou to hodnoty *8*, *48*.
8. **Quality Of Service** (QoS) – kvalita služby. Pokud si nejste jistí nastavení nebo Váš poskytovatel neurčí jinak, ponechte beze změny.
9. Nastavení odešlete tlačítkem **Apply**. Tím se právě nadefinované připojení dočasně aktivuje. Pokud celou konfiguraci neuložíte, budou ovšem zadané údaje při nejbližším vypnutí / rebootování ztraceny.

Obrázek PPPoE připojení s názvem Data:

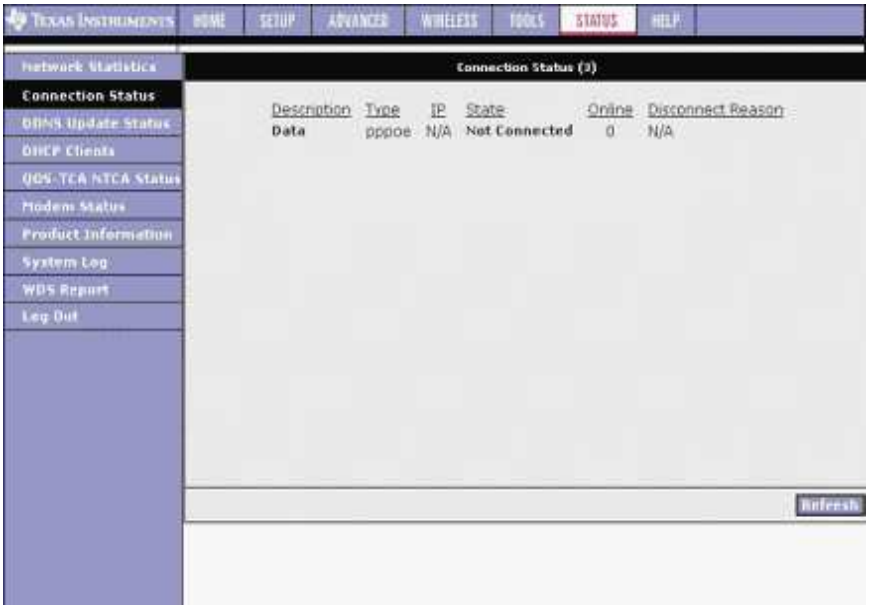


*V dolní části stránky jsou tlačítka pro navázání právě definovaného spojení nebo rozpojení (**Connect**, **Disconnect**), dále tlačítka pro uložení změn (**Apply**), smazání profilu (**Delete**) nebo zrušení provedených změn v nastavení (**Cancel**). Pro rychlý přístup k novému připojení bude navíc vytvořen odkaz s názvem připojení, umístěný v levém sloupci.*

9. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
10. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).



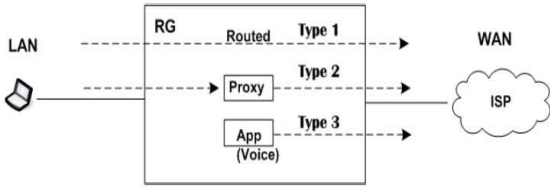
11. Stav spojení (status) si můžete zkontrolovat na stránce **Status** (horní lišta), dále **Connection Status**.



V následující tabulce je přehled prvků nastavení PPP na stránce **PPPoE Connection Setup**

Tabulka 1 Parametry nastavení PPP

Pole	Překlad	Popis
Username	Uživatelské jméno	Přihlašovací identifikátor pro spojení PPPoE. Dodá Váš poskytovatel DSL nebo internetu. Obsahuje písmena a číslice, začíná písmenem. Maximální délka je 64 znaků. Omezení ohledně použitelných znaků se netýká při konfiguraci přes CLI (Common Languague Interface).
Password	Heslo	Přihlašovací heslo pro PPPoE spojení. Dodá Váš poskytovatel služeb. Obsahuje písmena a číslice, začíná písmenem. Maximální délka je 128 znaků. Omezení ohledně použitelných znaků se netýká při konfiguraci přes CLI.
Idle Timeout	Max. délka nečinnosti (sekundy)	Není-li DSL linka aktivní po dobu **Idle Timeout** (sekundy), spojení PPPoE bude rozpojeno. Tato položka platí jen tehdy, je-li zaškrtnuto pole **On Demand** (Na vyžádání). Zadáte-li 0, linka bude stále aktivní.
Keep Alive	Udržovat aktivní	Není-li DSL linka aktivní po dobu **Keep Alive** (sekundy), spojení PPPoE bude rozpadeno. Tato položka se uplatní pouze, jestliže není zvoleno **On Demand** (Na vyžádání). Zadáte-li 0, linka bude stále aktivní. Můžete zadat libovolné celé kladné číslo.
Authentication	Ověřování	Jsou k dispozici tři možnosti • **Auto** • **CHAP** (Challenge handshake authentication protocol) • **Password auth. protocol** (PAP) Volby Auto a CHAP podporují také Microsoft CHAP v2, (nikoliv však MS CHAP v1)
MTU (Maximum transmit unit)	Maximální délka přenášeného paketu	Maximální délka datové jednotky v bytech, která může být přenášena přes DSL spojení k serveru poskytovatele služby. Výchozí hodnoty pro PPPoE jsou *1492 (max)* a pro PPPoA je to *1500 (max)*. Minimální použitelná hodnota je *64*.

On Demand	Na vyžádání	V tomto režimu je sledována aktivita linky – pokud je neaktivní po dobu **Idle Timeout**, spojení bude rozpojeno. Zaškrtnutím aktivujete další políčka: • Idle Timeout • Host Trigger • Valid Rx
Default Gateway	Výchozí brána	Je-li zaškrtnuto, bude toto WAN spojení vůči LAN vystupovat jako výchozí brána pro přístup k internetu
Enforce MTU	Respektovat MTU	Výchozí volba je zapnuto. V tomto případě všechen TCP provoz bude respektovat max. povolenou délku paketu, definovanou v MTU. Je-li vypnuto, můžou nastat problémy s přístupem na některé adresy.
Debugg	Ladění	Aktivuje funkce používané pro testování. Používá se pro simulaci příchozích paketů na straně WAN (pouze pro technické a vývojové pracovníky)
PPP Unnumbered		Speciální funkce. Umožňuje poskytovateli služeb (ISP) vymezit blok veřejných IP adres, které budou staticky přiřazeny k LAN. V podstatě se jedná o přemostěné spojení
LAN	LAN	Je aktivní pouze v režimu **PPP Unnumbered**. Specifikuje skupinu adres v LAN, na kterou budou pakety zasílány.
Host Trigger	Spouštěč	Tato volba je aktivní pouze je-li zapnuto **On Demand**. Na obrázku jsou tři druhy paketů:  • LAN pakety (typ 1) – pakety, které jsou prostřednictvím routeru směrované z LAN do WAN • Proxy pakety (typ 2) – pakety, které sestavuje router (např. DNS proxy) na základě paketů přijatých z LAN • Lokálně generované pakety (typ 3) – pakety vytvářené přímo router, např. při protokolu SNMP, telefonii apod. Pokud je zaškrtnuto **On Demand** a **Host Trigger** vypnuto, potom pouze pakety typu 1 udržují linku aktivní, tzn. že pokud RG nepřijme žádný paket typu 1 po dobu delší než **Time Out**, spojení vyprší. Pokud je zaškrtnuto **On Demand** + **Host Trigger**, potom pakety všech typů 1+2+3 udržují linku aktivní. Pakety typu 2+3 můžete konfigurovat na stránce **Trigger Traffic** (přístup tlačítkem **Configure**). Zde můžete definovat: • **Source Port** (port zdroje) – hvězdička * zastupuje *všechny* porty • **Destination Port** (port cíle) – hvězdička * zastupuje *všechny* porty • **Protocol** – zvolte *TCP, UDP,ICMP* nebo *Specify* + číslo protokolu

Valid Rx	Platí přijaté Rx	Toto pole je aktivní pouze, je-li zaškrtnuto **On Demand**. Je-li zapnuto **On Demand** a **Valid Rx** vypnuto, potom pouze odchozí pakety z LAN do WAN udržují linku aktivní. Po vypršení time-out nebudou moci být z WAN do LAN přijímány žádné pakety. Je-li **Valid Rx** zapnuto, pak i příchozí pakety linku udržují aktivní. Navíc je zde ale podmínka, že tyto příchozí pakety musí příslušet ke spojení, iniciovanému ze strany LAN.

Tabulka 2 Parametry nastavení VLAN

Pole	Překlad	Popis / význam
Sharing	Sdílení	Možnosti: **Disable** – zrušit **Enable** – povolit **VLAN** – jsou navíc aktivní pole **VLAN ID** a **Priority Bits**.
VLAN ID	VLAN ID	Identifikátor VLAN. Jsou podporovány vícenásobné spojení přes stejné PVC; v tomto případě musí WAN síť podporovat VLAN; DSLAM a routery na straně poskytovatele musejí podporovat tagy VLAN. Rozšířená podpora je také možná, potom je dovoluje vytvořit vícenásobné spojení přes jednoduché PVC bez podpory VLAN (speciální případ VLAN Tag *0*). V tomto režimu je přijatý paket vyslán do všech připojení.
Priority Bits	Prioritní bity	VLAN spojení má prioritu definovanou v rozsahu *0-7*. Všechny pakety vyslané přes VLAN obdrží určenou prioritu.

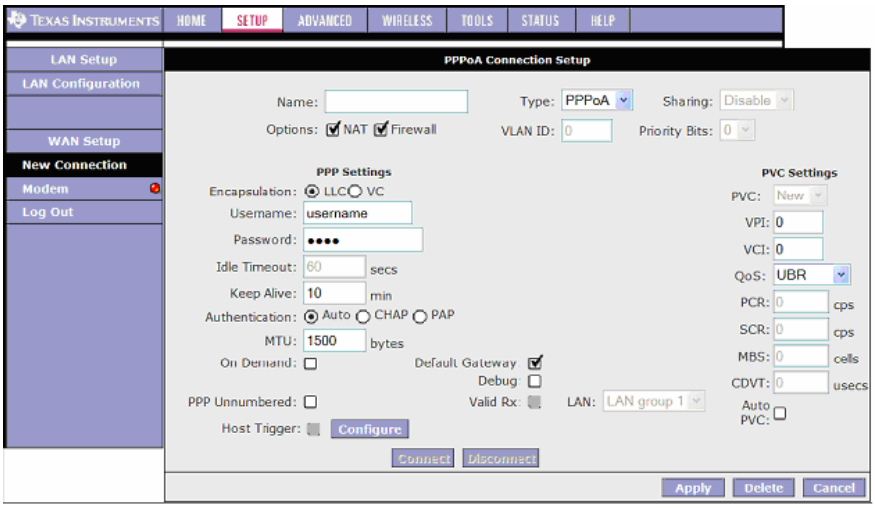
Tabulka 3 Parametry PVC nastavení

Pole	Popis / význam
PVC	Stálý virtuální okruh (Permanent virtual circuit). Je to pevný virtuální okruh mezi dvěma uživateli. Jedná se o pronajatou část veřejné datové sítě. Nejsou třeba žádné procedury pro nastavení nebo rušení.
VPI	Identifikátor virtuální cesty (Virtual path identifier).
VCI	Identifikátor virtuálního kanálu (Virtual channel identifier). Je to 16-bitový úsek v hlavičce ATM datové buňky. VCI spolu s VPI slouží k identifikaci příštího cíle datové buňky během průchodu přes ATM switch.
QoS	Kvalita služby (Quality of Service) – určuje, jak rychle a přesně mají být data sítí přenesena od cíle ke zdroji. Jsou k dispozici tři možnosti: • **Undefined Bit Rate** (UBR – nedefinovaná rychlost přenosu) – v tomto případě jsou pole PCR, SCR, MBS a CDVT neaktivní. • **Constant Bit Rate** (CBR – konstantní datový tok) – platí pole PCR a CDVT. • **Variable Bit Rate** (VBR – proměnný datový tok) – v tomto případě je možno nastavit PCR, SCR, MBS a CDVT. QoS jsou detailněji popsány v kapitole **Pokročilé - Advanced**
PCR	**Peak cell rate** – špičková frekvence buněk za sekundu, kterou zdroj nesmí překročit.
SCR	**Sustained cell rate** – stálá frekvence vysílání (buňky za sekundu) – průměrná hodnota vysílání, která během trvání spojení nesmí být překročena.

MBS	**Maximum burst size** – maximální velikost shluku buněk, která je vyslána rychlostí PCR
CDVT	**Cell delay variation tolerance** – maximální povolené kolísání zpoždění, které nabere buňka během průchodu sítí. Kolísání zpoždění je způsobeno průchody přes vyrovnávací paměti, multiplexováním a podobně.
Auto PVC	**Auto-Sensing permanent virtual circuit** – Stálý virtuální okruh s automatickým přepojováním (Auto-sensing). Celková operace auto-sensing je založena na OAM ping testu koncových bodů příslušného PVC. Existují dvě skupiny okruhů PVC: uživatelské výchozí PVC, které jsou definovány poskytovatelem OEM/ISP a záložní PVC. Výchozí VPI/VCI musí být 0/35. Seznam záložních PVC musí mít obsahovat některé z následující kombinací VPI/VCI: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51 a 8/59. Seznam PVC je definován v XML souboru a je nastavitelný. Auto-sensing mechanismus je možné vypnout. Během DSL synchronizace OAM ping testy koncových bodů jsou provedeny pro všechny definované výchozí PVC. Jestliže je nalezen okruh PVC, pro něhož ping funguje a není obsazen, PVC modul ho nastaví na obsazeno (*in-use*) a pokračuje v hledání. Pokud v seznamu výchozích PVC není nalezen žádný volný, pokračuje v hledání mezi záložními PVC. Pokud ani teď není nalezen volný PVC, modul oznámí koncovému uživateli, že žádný VCC nebyl nalezen. Po sestavení spojení je vybraný PVC uložen ve flash paměti jako výchozí PVC pro spojení. Po rebootování je tento PVC automaticky zvolen pro navázání spojení. Toto nastavení přepíše původní nastavení PVC spojení nahrané z XML. Během procesu sestavování spojení bude testovány nejprve tento první PVC. Pokud je OAM ping úspěšný, proces sestavení spojení pokračuje. V opačném případě začne hledat jiný vhodný PVC. Seznam výchozích a záložních PVC musí být globální pro správu všech spojení, jak Auto-Sensing, tak ostatních. Tento seznam dovoluje koncovému uživateli sestavit spojení, aniž by musel sledovat vhodné PVC.

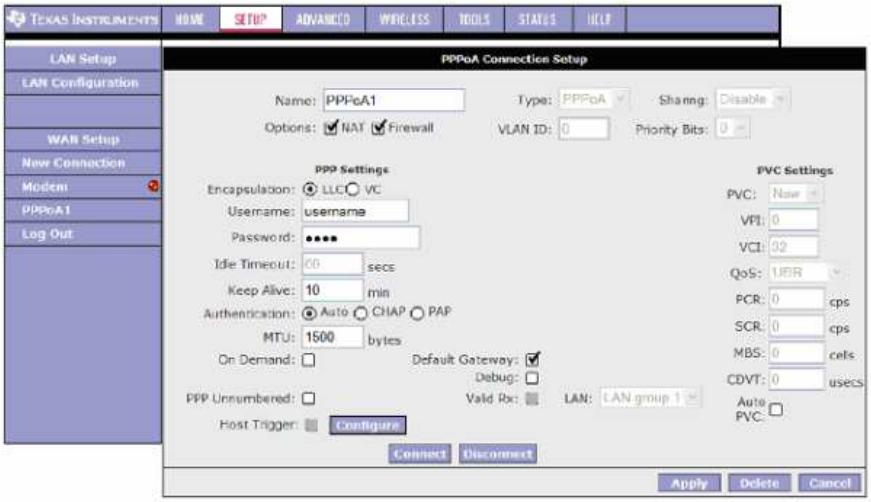
4.2.1.1.2. Nové připojení – nastavení PPPoA

PPPoA: Je-li zvolen mód **PPPoA**, objeví se následující okno. Protokol PPP (Point-to-Point) je způsob sestavení spojení mezi dvěma hosty sítě. PPPoA, označovaný také jako RFC 2346, upravuje PPP pro práci v sítích ATM s připojením ADSL. Záleží na poskytovateli DSL připojení, která z metod je použita.



1. Na stránce **SETUP** klikněte na **New Connection**. Zobrazí se výchozí stránka **PPPoE Connection Setup**.
2. V nabídce Typ připojení (**Type**) zvolte **PPPoA**. Načte se výchozí stránka **PPPoA Connection Setup**.
3. Do políčka **Name** napište Vámi zvolené jméno pro nově definované spojení. Jméno nesmí obsahovat mezery a musí začínat písmenem.
4. Volby **NAT** (překladač síťových adres) a **Firewall** ponechte zaškrtnuté.

5. Chcete-li zapnout VLAN, použijte údaje z tabulky 2.
   - **Sharing (sdílení)** – zvolte VLAN – položky **VLAN ID** a **Priority Bits** se stanou aktivní.
   - **VLAN ID**
   - **Priority Bits**
6. **PPP Settings** – vyberte typ zapouzdření (LLC nebo VC) . Pokud si nejste jisti, dotažte se poskytovatele nebo ponechte výchozí nastavení.
7. **PVC** – zde vyplňte VPI a VCI (všechny údaje Vám musí dodat poskytovatel služeb připojení) – v následujícím příkladě jsou to hodnoty *0*, *35*.
8. **Quality Of Service** (QoS) – kvalita služby. Pokud si nejste jistí nastavení nebo Váš poskytovatel neurčí jinak, ponechte beze změny.
9. Nastavení odešlete tlačítkem **Apply**. Tím se právě nadefinované připojení dočasně aktivuje. Pokud celou konfiguraci neuložíte, budou ovšem zadané údaje při nejbližším vypnutí / rebootování ztraceny.



9. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
10. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
11. Stav spojení (status) si můžete zkontrolovat na stránce **Status** (horní lišta), dále **Connection Status**.

Tabulka 4 Parametry nastavení PPP

Pole	Překlad	Popis/význam
Encapsulation	Zapouzdření	Technika vrstvení protokolů, kdy další transportní vrstva přidá k přenášené datové jednotce (PDU) vlastní hlavičku. V případě internetu přenášený paket obsahuje obvykle hlavičku linkové vrstvy, následuje hlavička síťové vrstvy (IP), dále hlavička transportní vrstvy (TCP) a nakonec hlavička aplikace, pro níž jsou data určena. Zde je možno zvolit *LLC* (Logical Link Control) nebo *VC* (Virtual Channel)
Username	Uživatelské jméno	Přihlašovací identifikátor pro spojení PPPoA. Dodá Váš poskytovatel DSL nebo internetu. Obsahuje písmena a číslice, začíná písmenem. Maximální délka je 64 znaků. Omezení ohledně použitelných znaků se netýká při konfiguraci založené na CLI.
Password	Heslo	Heslo pro ověřování spojení PPPoA. Dodá Váš poskytovatel DSL nebo internetu. Obsahuje písmena a číslice, začíná písmenem. Maximální délka je 64 znaků. Omezení ohledně použitelných znaků se netýká při konfiguraci založené na CLI.
Idle Timeout	Max. délka nečinnosti (sekundy)	Není-li DSL linka aktivní po dobu **Idle Timeout** (sekundy), spojení PPPoA bude rozpadeno. Tato položka platí jen tehdy, je-li zaškrtnuto pole **On Demand** (Na vyžádání). Zadáte-li 0, linka bude stále aktivní. Můžete zadat i vyšší hodnotu, než uvedených 10 sekund.

Keep Alive	Udržovat aktivní	Není-li DSL linka aktivní po dobu **Keep Alive** (sekundy), spojení PPPoE bude rozpadeno. Tato položka se uplatní pouze, jestliže není zvoleno **On Demand** (Na vyžádání). Zadáte-li 0, linka bude stále aktivní. Můžete zadat libovolné celé kladné číslo.
Authentication	Metoda ověřování	Jsou k dispozici tři možnosti • *Auto* • *CHAP* (Challenge handshake authentication protocol) • *Password auth. protocol* (PAP) Volby **Auto** a **CHAP** podporují také Microsoft CHAP v2, (nikoliv však MS CHAP v1)
MTU (Maximum transmit unit)	Maximální délka přenášeného paketu	Maximální délka datové jednotky v bytech, která může být přenášena přes DSL spojení k serveru poskytovatele služby. Výchozí hodnoty pro PPPoE jsou *1492 (max)* a pro PPPoA je to *1500 (max)*. Minimální použitelná hodnota je *64*.
On Demand	Na vyžádání	V tomto režimu je sledována aktivita linky – pokud je neaktivní po dobu **Idle Timeout**, spojení bude rozpojeno. Zaškrtnutím aktivujete další políčka: • Idle Timeout • Host Trigger • Valid Rx
Default Gateway	Výchozí brána	Je-li zaškrtnuto, bude toto WAN spojení vůči LAN vystupovat jako výchozí brána pro přístup k internetu
Debugg	Ladění	Aktivuje funkce používané pro testování. Používá se pro simulaci příchozích paketů na straně WAN (pouze pro technické a vývojové pracovníky)
PPP Unnumbered		Speciální funkce. Umožňuje poskytovateli služeb (ISP) vymezit blok veřejných IP adres, které budou staticky přiřazeny k LAN. V podstatě se jedná o přemostěné spojení
LAN		Je aktivní pouze v režimu PPP Unnumbered. Specifikuje skupinu adres v LAN, na kterou budou pakety zasílány.

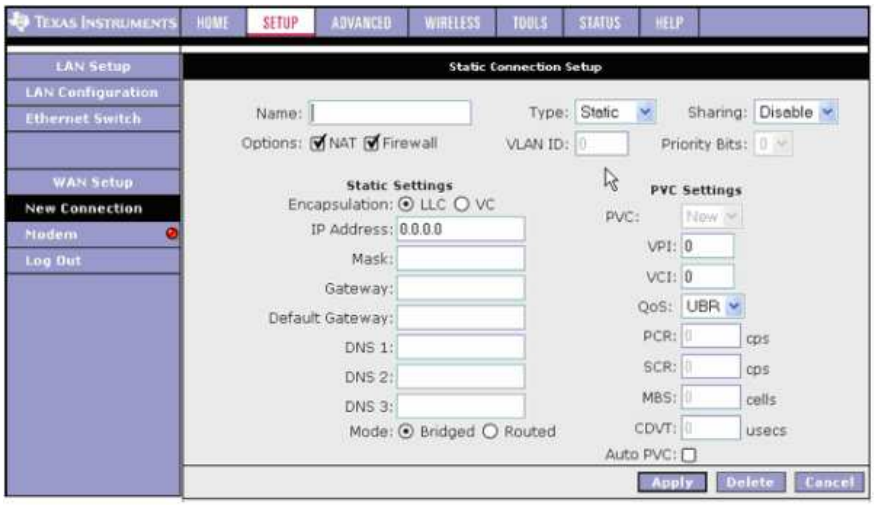
Parametry VLAN byly popsány v tabulce 2

Parametry PVC byly popsány v tabulce 3

4.2.1.1.3. Nové připojení–nastavení statického připojení

Statické: Je-li zvolen mód **Static**, zobrazí se následující okno. Většina internetových uživatelů je připojeno prostřednictvím dynamické adresy, která může být pro každé navázání spojení odlišná. V některých situacích je však potřeba použít pevnou IP adresu, například pokud se jedná o servery internetových stránek, telefonování přes internet (VoIP) nebo videokonference, kdy se ostatní uživatelé potřebují pravidelně připojovat k Vašemu počítači. Poskytovatelé pro tyto účely obvykle přidělují pevné IP adresy za příplatek.

Při statickém připojení je routeru přidělena stálá známá IP adresa. Dále je potřeba znát masku podsítě a adresu výchozí brány. Je možno definovat až tři DNS servery. DNS (Domain name server) obsahují databáze mapování IP adres serverů na člověku srozumitelné, snadno zapamatovatelné doménové názvy.



1. Na stránce **SETUP** klikněte na **New Connection**. Zobrazí se výchozí stránka **PPPoE Connection Setup**.
2. V nabídce Typ připojení (**Type**) zvolte **Static**. Načte se výchozí stránka **Static Connection Setup**.
3. Do políčka **Name** napište Vámi zvolené jméno pro nově definované spojení. Jméno nesmí obsahovat mezery a musí začínat písmenem.
4. Volby **NAT** (překladač síťových adres) a **Firewall** ponechte zaškrtnuté.
5. Zvolte typ zapouzdření (**Encapsulation Type**) LLC nebo VC . Pokud si nejste jisti, dotžte se poskytovatele nebo ponechte výchozí nastavení.
6. Podle údajů od poskytovatele služby zadejte přidělenou adresu **IP Address**, masku podsítě **Subnet Mask**, výchozí bránu (je-li určena), **Default Gateway** a DNS servery **DNS1 – 3** (pokud jsou určeny).
7. Při statickém připojení je třeba zvolit, jedná-li se o přemostění (**Bridged**) nebo směrování (**Routed**).
8. **PVC Settings** – zde vyplňte **VPI** a **VCI** (všechny údaje Vám musí dodat poskytovatel služeb připojení) – v následujícím příkladě jsou to hodnoty *0*, *35*..
9. **Quality Of Service** (QoS) – kvalita služby. Pokud si nejste jistí nastavení nebo Váš poskytovatel neurčí jinak, ponechte beze změny. Podle zvolené QoS jsou aktivní příslušející pole PCR, SCR, MBS a CDVT.
10. Nastavení aktivujete tlačítkem **Apply**. Tím se dočasně aktivuje právě nadefinované připojení. Pokud celou konfiguraci neuložíte, budou ovšem zadané údaje při nejbližším vypnutí / rebootování routeru ztraceny.
11. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
12. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
13. Stav spojení (status) si můžete zkontrolovat na stránce **Status** (horní lišta), dále **Connection Status**.

Tabulka 5 Parametry statického připojení

Pole	Překlad	Popis/význam
Encapsulation	Zapouzdření	Technika vrstvení protokolů, kdy další transportní vrstva přidá k přenášené datové jednotce (PDU) vlastní hlavičku. V případě internetu přenášený paket obsahuje obvykle hlavičku linkové vrstvy, následuje hlavička síťové vrstvy (IP), dále hlavička transportní vrstvy (TCP) a nakonec hlavička aplikace, pro níž jsou data určena. Zde je možno zvolit *LLC* (Logical Link Control) nebo *VC* (Virtual Channel)
IP Address	IP adresa	Statická IP adresa, přidělená poskytovatelem služeb (ISP)
Mask	Maska podsítě	Maska podsítě, přidělená poskytovatelem služeb (ISP)
Gateway	Brána	IP adresa Vaší brány, přidělená poskytovatelem
Default Gateway	Výchozí brána	IP adresa výchozí brány, přidělená poskytovatelem
DNS	DNS	IP adresa serveru doménových jmen, přidělená poskytovatelem služeb. Lze nastavit až tři různé adresy.
Mode	Režim	Jsou k dispozici režimy přemostění **Bridged** a směrování **Routed**.

Parametry VLAN byly popsány v tabulce 2

Parametry PVC byly popsány v tabulce 3

4.2.1.1.4. Nové připojení – nastavení DHCP

DHCP: V případě, že je zvolen mód DHCP, objeví s následující stránka. DHCP (Dynamic Host Configuration Protocol) dovoluje ADSL routeru získat svou IP adresu ze serveru automaticky. Tato volba je běžná v případech, kdy IP adresa je přidělovaná dynamicky a není dopředu známa.

1. Na stránce **SETUP** klikněte na **New Connection**. Zobrazí se výchozí stránka **PPPoE Connection Setup**.
2. V nabídce Typ připojení (**Type**) zvolte **DHCP**. Načte se výchozí stránka **DHCP Connection Setup**.
3. Do políčka **Name** napište Vámi zvolené jméno pro nově definované spojení. Jméno nesmí obsahovat mezery a musí začínat písmenem.
4. Volby **NAT** (překladač síťových adres) a **Firewall** ponechte zaškrtnuté.
5. Je-li DSL linka již zapojena a Váš poskytovatel služeb podporuje DHCP, tlačítkem **Renew** (Obnovit) zažádáte o přidělení IP adresy, masky podsítě a adresu brány. Tlačítkem **Release** (Uvolnit) můžete kdykoliv přidělenou adresu uvolnit pro jiné použití a opětovným **Renew** znovu zažádat o přidělení.
6. **PVC Settings** – zde vyplňte **VPI** a **VCI** (všechny údaje Vám musí dodat poskytovatel služeb připojení) – v následujícím příkladě jsou to hodnoty *0*, *35*..
7. **Quality Of Service** (QoS) – kvalita služby. Pokud si nejste jistí nastavení nebo Váš poskytovatel neurčí jinak,. ponechte beze změny. Podle zvolené QoS jsou aktivní příslušející pole PCR, SCR, MBS a CDVT.
8. Hodnoty formuláře odešlete tlačítkem **Apply**. Tím se právě nadefinované připojení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
9. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
10. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
11. Stav spojení (status) si můžete zkontrolovat na stránce **Status** (horní lišta), dále **Connection Status**.

Tabulka 6 Parametry dynamického připojení (DHCP)

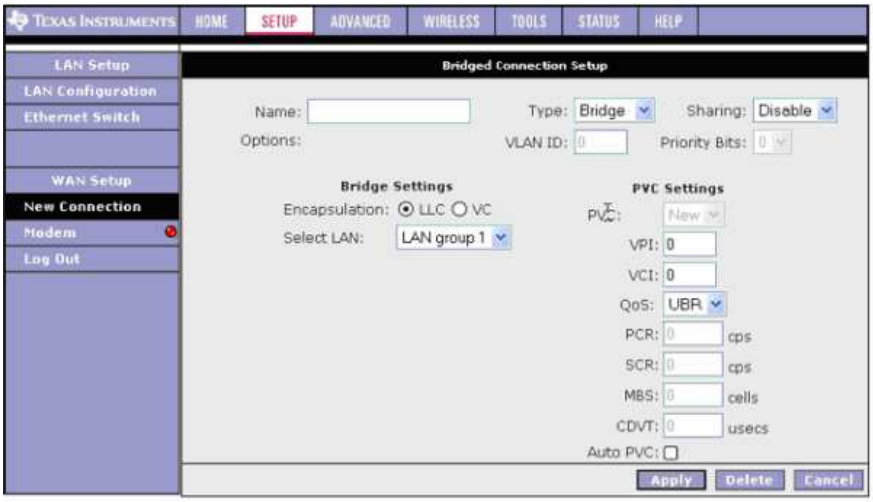
Pole	Překlad	Popis/význam
Encapsulation	Zapouzdření	Technika vrstvení protokolů, kdy další transportní vrstva přidá k přenášené datové jednotce (PDU) vlastní hlavičku. V případě internetu přenášený paket obsahuje obvykle hlavičku linkové vrstvy, následuje hlavička síťové vrstvy (IP), dále hlavička transportní vrstvy (TCP) a nakonec hlavička aplikace, pro níž jsou data určena. Zde je možno zvolit *LLC* (Logical Link Control) nebo *VC* (Virtual Channel)
IP Address	IP adresa	Statická IP adresa, přidělená poskytovatelem služeb (ISP)
Mask	Maska podsítě	Maska podsítě, přidělená poskytovatelem služeb (ISP)
Gateway	Brána	IP adresa Vaší brány, přidělená poskytovatelem
Default Gateway	Výchozí brána	IP adresa výchozí brány, přidělená poskytovatelem

Parametry VLAN byly popsány v tabulce 2

Parametry PVC byly popsány v tabulce 3

4.2.1.1.5. Nové připojení – nastavení mostu (bridge)

Bridge (most): Je-li zvolený mód bridge, objeví se následující okno. Spojení typu bridge v zásadě vypíná funkce routování, firewallu a NAT. ADSL2/2+ router v módu bridge vystupuje jako modem nebo hub a pouze přeposílá pakety mezi WAN a LAN portem. Spojení bridge předpokládá, že vypnutou funkci směrování přebírá jiné zařízení.



1. Na stránce **SETUP** klikněte na **New Connection**. Zobrazí se výchozí stránka **PPPoE Connection Setup**.
2. V nabídce Typ připojení (**Type**) zvolte **Bridge**. Načte se výchozí stránka **Bridge Connection Setup**.
3. Do políčka **Name** napište Vámi zvolené jméno pro nově definované spojení. Jméno nesmí obsahovat mezery a musí začínat písmenem.
4. **PVC Settings** – zde vyplňte **VPI** a **VCI** (všechny údaje Vám musí dodat poskytovatel služeb připojení) – v následujícím příkladě jsou to hodnoty *0*, *35*.
5. **Quality Of Service** (QoS) – kvalita služby. Pokud si nejste jistí nastavení nebo Váš poskytovatel neurčí jinak, ponechte beze změny. Podle zvolené QoS jsou aktivní příslušející pole PCR, SCR, MBS a CDVT.
6. Hodnoty formuláře odešlete tlačítkem **Apply**. Tím se právě nadefinované připojení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
7. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
8. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
9. Stav spojení (status) si můžete zkontrolovat na stránce **Status** (horní lišta), dále **Connection Status**.

Tabulka 7 Parametry přemostění (bridge)

Pole	Překlad	Popis/význam
Encapsulation	Zapouzdření	Technika vrstvení protokolů, kdy další transportní vrstva přidá k přenášené datové jednotce (PDU) vlastní hlavičku. V případě internetu přenášený paket obsahuje obvykle hlavičku linkové vrstvy, následuje hlavička síťové vrstvy (IP), dále hlavička transportní vrstvy (TCP) a nakonec hlavička aplikace, pro níž jsou data určena. Zde je možno zvolit *LLC* (Logical Link Control) nebo *VC* (Virtual Channel)
Select LAN	Zvolte LAN	Vyberte skupinu LAN pro přemostění: • *LAN Group 1* • *LAN Group 2* • *LAN Group 3* • *LAN Group 4* • *LAN Group 5* • *None* (žádná) Přemostění bude přiděleno zvolené skupině LAN. V případě volby **None** (žádná) bude zařazeno mezi nezařazená rozhraní v boxu **Interfaces** - viz stránka nastavení Chyba! Nenalezen zdroj odkazů. Podrobnější popis konfigurace skupin LAN je v kapitole Chyba! Nenalezen zdroj odkazů.

Parametry VLAN byly popsány v tabulce 2

Parametry PVC byly popsány v tabulce 3

4.2.1.1.6. Modifikace existujícího připojení

Změnu v nastavení již definovaného připojení je možno provést následujícím způsobem:

1. Na úvodní stránce **Setup** vyberte v levém sloupci spojení, jehož parametry chcete změnit.
2. Spojení jsou označeny názvy.
   Poznámka – lze uložit max. 8 různých připojení
3. Zobrazí se stránka zvoleného připojení – zde proveďte zamýšlené změny.
   Poznámka – Některá pole po počáteční definici již nelze měnit.
4. Údaje odešlete tlačítkem **Apply**. Tím se provedené změny dočasně uloží. Pokud celou konfiguraci neuložíte (viz dále), budou zadané údaje při nejbližším vypnutí / rebootování routeru ztraceny.
5. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
6. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

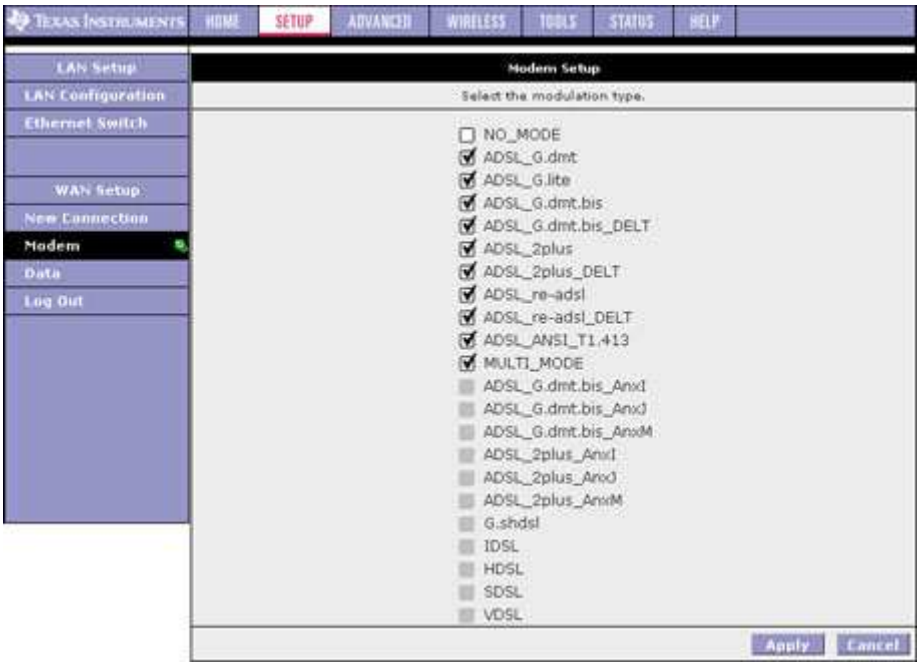
4.2.1.1.7. Smazání existujícího připojení

Již definované připojení můžete smazat následujícím způsobem:

1. Na úvodní stránce **Setup** vyberte v levém sloupci spojení, které chcete zrušit.
2. Spojení jsou označeny názvy Connection 1 až 8.
3. Zobrazí se stránka zvoleného připojení – zde klikněte na **Delete** (Smazat).
   Poznámka - Tlačítkem Delete smažete připojení pouze do příštího zapnutí / rebootování routeru. Pro trvalé smazání je třeba uložit změny – viz další krok.
4. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
5. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

4.2.1.2. SETUP – WAN Setup – Modem

Modem: V tomto poli je možno předepsat způsoby spojování/přihlašování modemu k síti (jsou povoleny všechny kombinace):



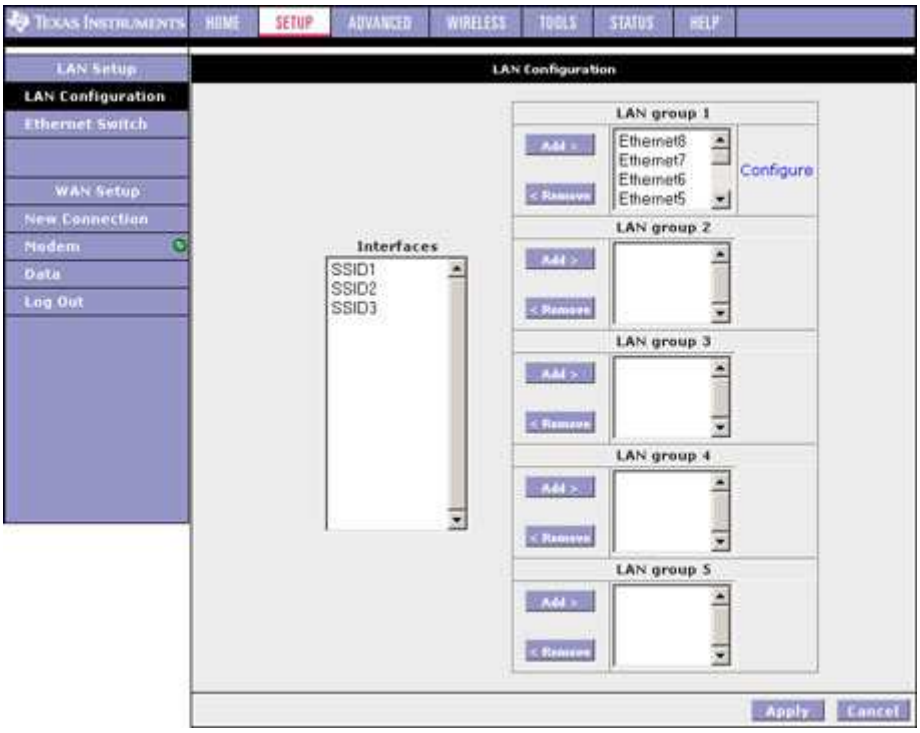
4.2.2. SETUP – LAN Setup

Na stránce **LAN Configuration** je možno LAN zařízení rozdělit do několika skupin (max. 5). LAN rozhraní mohou zahrnovat Ethernet, USB, WLAN (Primární SSID, SSID1, SSID2 a SSID3). Každé LAN rozhraní lze přiřadit k libovolné skupině, maximálně však jedné; navíc Ethernet musí zůstat zařazen ve skupině LAN 1.

Každá LAN skupina může být vybavena statickými nebo dynamickými (DHCP) adresami, nebo ponechána bez adres.

4.2.2.1. LAN Setup – LAN Configuration

Klikněte na LAN Configuration, zobrazí se následující obrazovka (názvy rozhraní a jejich počet se může ve Vašem případě od uvedeného příkladu lišit).



Poznámka – Následující rozhraní jsou platná pouze tehdy, je-li aktivováno vícenásobné SSID a přídavné SSID jsou nakonfigurovány:

SSID 1 (shoduje se s první sekundární SSID)

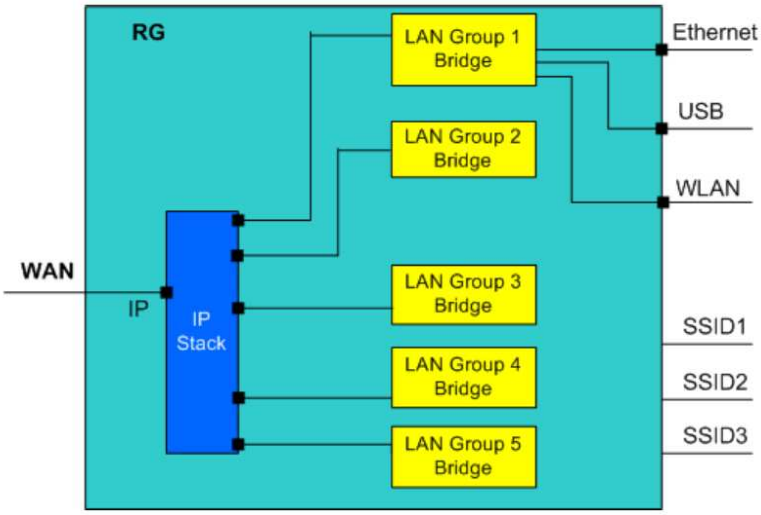
SSID 2 (shoduje se s druhou sekundární SSID)

SSID 3 (shoduje se s třetí sekundární SSID)

Více informací o vícenásobných SSID jsou v kapitole „Vícenásobné SSID" v oddíle Bezdrátová LAN (WLAN).

Na dalším obrázku je příklad směrování provozu mezi skupinou LAN 1 a WAN.

Směrování – skupiny LAN

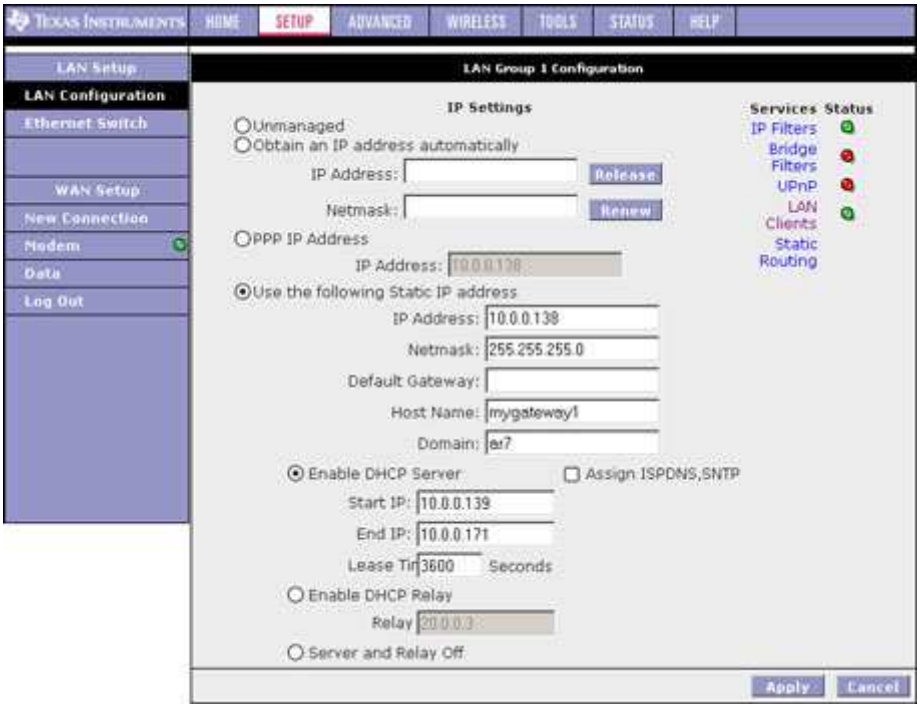


1. Klikněte na **Add** (Přidat) nebo **Remove** (Odstranit) u okna jednotlivé skupiny LAN. Funkce skupin LAN je podporována pouze v módu **Bridge**. Rozhraní spadající do stejné LAN skupiny (WLAN, Ethernet a USB) získají schopnost komunikovat navzájem mezi sebou. Přístup mezi rozdílnými LAN skupinami je odepřen.
2. Pro detailní nastavení klikněte na **Configure**. Detaily najdete v další kapitole.
3. Údaje odešlete tlačítkem **Apply**. Tím se provedené změny dočasně uloží. Pokud celou konfiguraci neuložíte (viz dále), budou zadané údaje při nejbližším vypnutí / rebootování routeru ztraceny.
4. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
5. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

4.2.2.1.1. Konfigurace skupin LAN

Na stránce Konfigurace skupin LAN (**LAN Configuration**) je možné nastavit parametry pro každou definovanou skupinu LAN zvlášť (po kliknutí na **Configure** u odpovídající LAN skupiny – **LAN Group**).

Dále je zde zobrazen status pokročilých služeb, které mohou být aktivovány pro každou LAN skupinu. Zelená znamená, že je služba aktivována; červená znamená služba vypnuta.



Tabulka 9 Parametry nastavení skupin LAN

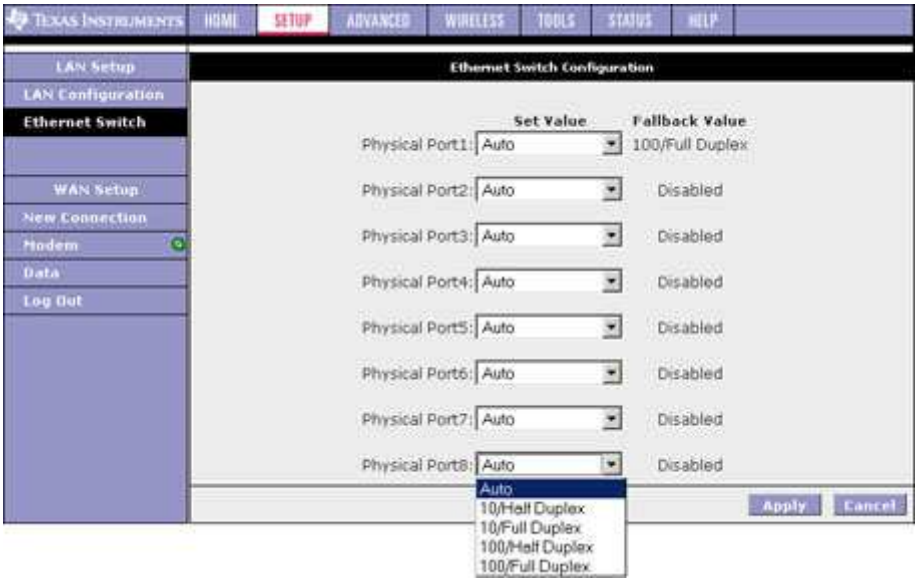
Skupina / pole	Pole	Překlad	Popis / význam
Unmanaged		Bez zařazení	V dané LAN skupině není zařazeno žádné rozhraní ani není přiřazena žádná IP adresa
Obtain an IP address automatically		Získat IP adresu automaticky	Router vystupuje vůči LAN jako klient a žádá o přidělení adresy z DHCP serveru, nacházejícího se v dané LAN
	IP Address	IP adresa	Tlačítky **Release** / **Renew** můžete uvolnit stávající nebo zažádat o novou dynamickou adresu
	Netmask	Maska podsítě	
PPP IP Address			Zapíná/vypíná funkce PPP Unnumbered
	IP Address	IP adresa	IP adresa musí být rozdílná od IP adresy WAN, musí se však nacházet ve stejné podsíti
Use the folowing Static IP address			Zde můžete změnit IP adresu routeru
	IP Address	IP adresa	Přednastavená IP adresa (viz obrázek) je *10.0.0.138*
	Netmask	Maska podsítě	Výchozí hodnota je *255.255.255.0*. Při této masce se může v LAN nacházet až 254 uživatelů. Pokud to nestačí, je třeba masku změnit.
	Default Gateway	Výchozí brána	Výchozí brána je adresa, na niž je směrován všechen provoz, který nenáleží do vnitřní sítě. Adresu výchozí brány Vám určí poskytovatel služby nebo je přidělena automaticky při spojení.

	Host Name	Jméno hostitele	Používá se společně s doménovým jménem k jednoznačné identifikaci routeru. Skládá se ze znaků a číslic, nesmí obsahovat mezery
	Domain	Doména	Spolu se jménem hostitele slouží k jednoznačné identifikaci. Pro přístup k webovým stránkám routeru můžete zadat buď IP adresu 10.0.0.138 nebo *mygateway1.ar7* (HostName.Domain)
Enable DHCP Server		Zapnout DHCP server	Výchozí volba je DHCP zapnuto (DHCP na straně LAN). Pokud již v LAN běží jiný DHCP server, je nutno jeden z nich vypnout
	Start IP	Počáteční IP adresa	První adresa z intervalu adres, z něhož DHCP server vybírá přidělované IP adresy. Musí být vyšší než IP adresa přiřazená samotné RG. Například IP adresa RG je *10.0.0.138*, takže počáteční adresa může být *10.0.0.139* nebo vyšší. Poznámka – Při změně počáteční nebo koncovou adresu intervalu se obě hodnoty musejí stále nacházet ve podsíti jako RG.
	End IP	Koncová IP adresa	Koncová adresa intervalu, z něhož DHCP vybírá přidělované dynamické IP adresy. Maximální hodnota posledního oktetu nesmí překročit 254 (např. *10.0.0.171*) . Vyčerpá-li DHCP server celý interval povolených adres, další uživatelům již bude přístup odepřen. V tomto případě můžete zvýšit hodnotu koncové IP adresy nebo může také pomoci zkrátit dobu pronájmu.
	Lease Time	Délka pronájmu	Časový úsek, po který přidělená dynamická adresa platí. Po jejím uplynutí bude pronájem obnoven nebo DHCP server přidělí adresu novou. Zadává se v sekundách. Výchozí hodnota je *3600* sekund (1 hod.). Maximum je 999999 sekund (cca 278 hod.)
Enable DHCP Relay		Zapnout DHCP relay	Kromě DHCP serveru podporuje RG také funkci DHCP přenosu (relay). Je-li konfigurován jako DHCP server, potom RG adresy přiděluje sám, zatímco v režimu DHCP relay vystupuje jako prostředník při vyjednávání mezi klienty a jiným DHCP serverem.
	Relay IP	IP adresa DHCP relay serveru	
Server and Relay off		Server i DHCP relay vypnuty	V tomto případě musí administrátor ručně nastavit pro každého klienta sítě jeho IP adresu, masku podsítě a DNS. Každý klient musí mít svou vlastní IP adresu. RG musí být ve stejné podsíti jako ostatní klienti.

4.2.3. LAN Setup – Ethernet Switch

Na stránce **Ethernet Switch** je možno nastavit LAN port do následujících módů (výchozí nastavení je **„Auto")**:

1. **Auto**: ADSL2/2+ router si sám automaticky zjistí, který mód by měl použít: 100Mbps plný duplex, 100Mbps poloviční duplex, 10Mbps plný duplex a 10Mbps poloviční duplex. Výchozí volba.
2. **10/Half Duplex**: Příjem a vysílání dat nemůže probíhat současně. Data mohou být například vyslána, po ukončení vysílání mohou být přijímána. Vše se děje rychlostí 10 Mbps.
3. **10/Full Duplex**: Data mohou být vysílána a přijímána současně, rychlost 10 Mbps.
4. **100/Half Duplex**: Příjem a vysílání dat nemůže probíhat současně. Data mohou být například vyslána, po ukončení vysílání mohou být přijímána. Vše se děje rychlostí 100 Mbps.
5. **100/Full Duplex**: Data mohou být vysílána a přijímána současně, rychlost 100 Mbps.
6. Údaje odešlete tlačítkem **Apply**. Tím se provedené změny dočasně uloží. Pokud celou konfiguraci neuložíte (viz dále), budou zadané údaje při nejbližším vypnutí / rebootování routeru ztraceny.
7. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
8. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).



4.2.4. Log Out

Kliknutím na **Log Out** (Odhlásit) v levém sloupci opustíte celou webovou stránku konfigurace routeru.

Postup:

1. Klikněte na **Log Out** v levém sloupci
2. Zobrazí se potvrzující dotaz („Chcete se skutečně odhlásit ?)
3. Potvrďte kliknutím na **Log Out** vpravo dole
4. Zobrazí se úvodní přihlašovací obrazovka (**Log In**)

4.3. ADVANCED

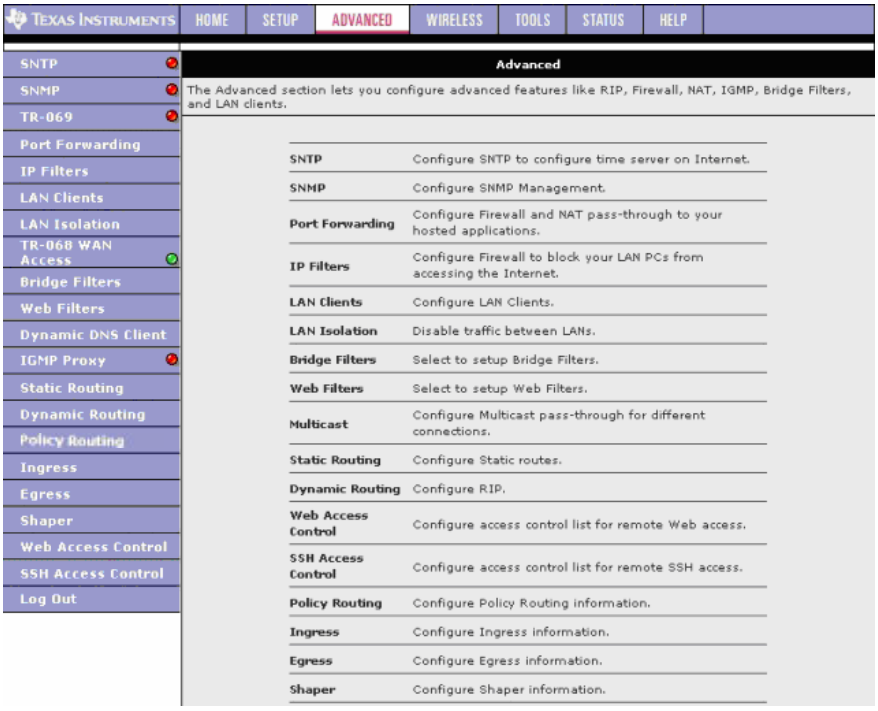
Mezi pokročilé funkce (Advanced) patří:

- Nastavení důležitých funkcí jako UpnP, SNTP, SNMP, TR-069, IP QoS, RIP, kontrola přístupu, TR-068 WAN přístup a multicasting.
- Zpracování QoS a politika směrování (policy routing)
- Správa LAN rozhraní, toku paketů a filtrace

Pokročilé funkce pro WAN (resp. LAN) lze nastavit, pokud existuje aspoň jedno spojení WAN (resp. LAN skupina).

Na následujícím obrázku je hlavní stránka **Advanced**, přístup je kliknutím na položku **Advanced** v horní tlačítkové liště. Je zde rozcestník na nastavení jednotlivých funkcí:

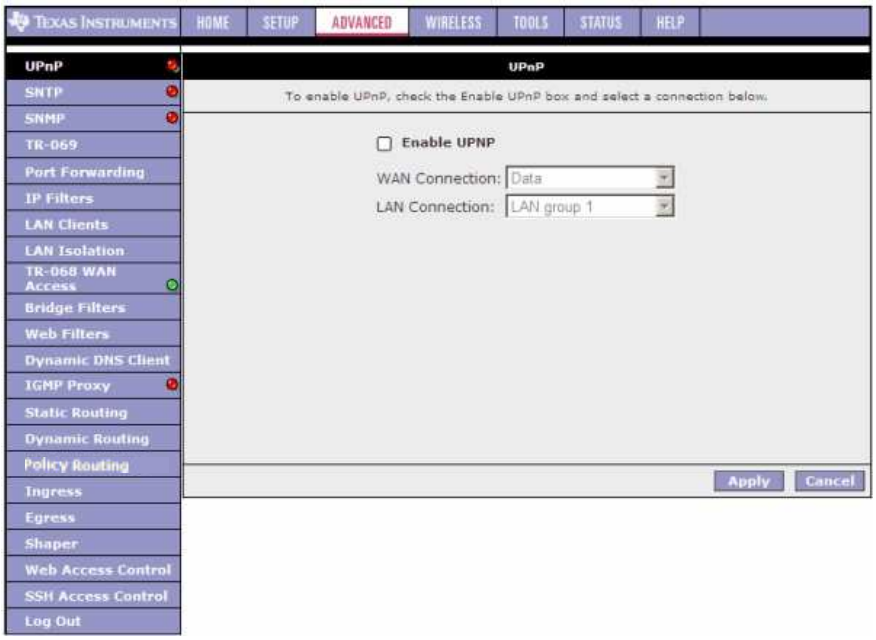
- UPnP – Universal Plug and Play
- SNTP – Nastavování časových serverů
- SNMP – Konfigurace SNMP
- TR-069
- Port Forwarding – Směrování portů
- IP Filters - Filtry pro blokování přístupu na Internet
- LAN Clients – Nastavení LAN klientů
- LAN Isolation – Vzájemná izolace mezi skupinami LAN
- TR-068 WAN Access – Vzdálená správa
- Bridge Filters
- Web Filters – Nastavení web filtrů pro všechny klienty LAN
- Dynamic DNS Client
- IGMP Proxy
- Static Routing – Statická směrovací tabulka
- Dynamic Routing – Dynamické směrováni
- Policy Routing
- Ingress – Pokročilé nastavování QoS pro vstup
- Egress – Pokročilé nastavování QoS pro výstup
- Shaper – Pokročilé ladění podle QoS
- Web Access Control – Vzdálený přístup přes HTTP
- SSH Access Control – Vzdálený přístup a správa přes SSH



4.3.1. ADVANCED – UPnP

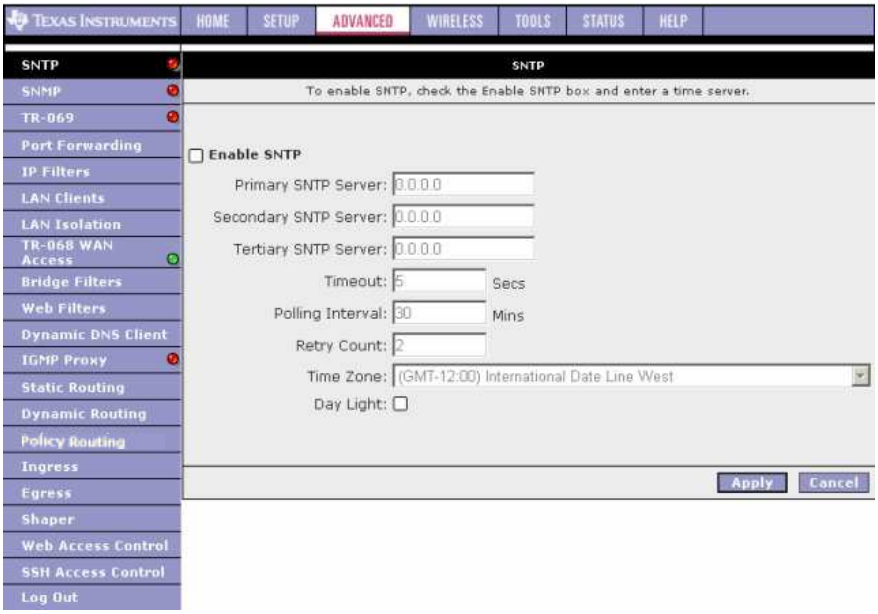
UPnP: Universal Plug and Play je protokol, který automatizuje propojení mezi zařízeními sítě, jako jsou počítače, herní zařízení, digitální kamery a další systémy komunikující prostřednictvím protokolu TCP/IP. Aplikace s vestavěným protokolem UPnP dokážou navázat spojení se zařízeními s aktivovaným-UPnP bez potřeby ručního nastavení.

Pro aktivaci UPnP zaškrtněte **Enable UPnP**. Tím se aktivuje okno Enable UPnP. Je nutné mít definované aspoň jedno aktivní WAN připojení. Připojené PC musí také podporovat UPnP. Pokud je aktivních více WAN připojení naráz, zvolte jedno, přes které jde příchozí provoz



4.3.2. ADVANCED – SNTP

SNTP: (Simple network timing protocol) je protokol používaný pro synchronizaci systémového času s veřejnými servery přesného času. Komunikace probíhá UDP protokolem na portu 123. Pro zapnutí funkce zaškrtněte políčko Enable SNTP.



Po aktivaci funkce SNTP zašle RG požadavek o přesný čas na adresu prvního (primary) SNTP serveru. Pokud do doby **Timeout** nedostane odpověď, učiní ještě několik pokusů (**Retry Count** = počet pokusů). Nejsou-li ani tyto pokusy úspěšné, zažádá stejným způsobem na adrese druhého (secondary) SNTP serveru, případně i třetího (tertiary). Celý cyklus je opakován s periodou **Polling Interval**.

Postup při nastavení:

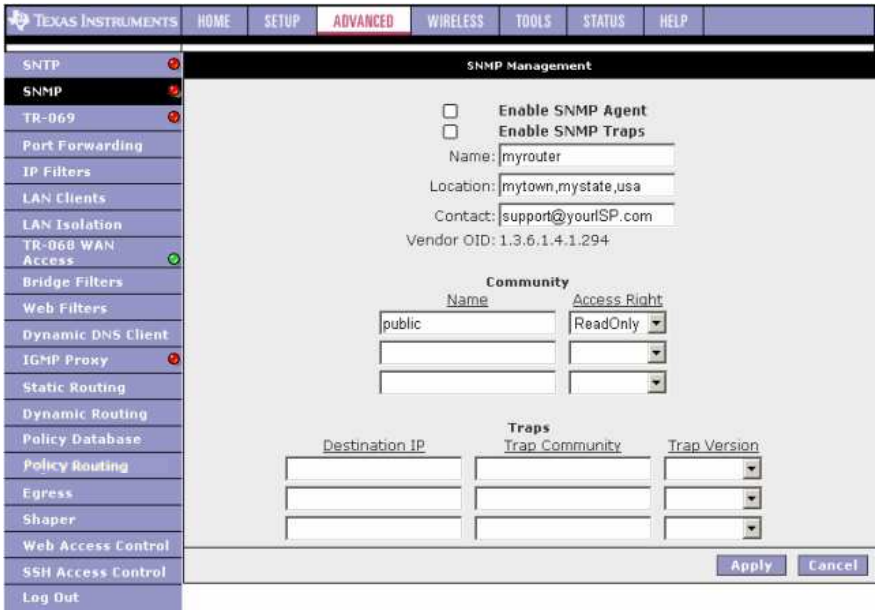
1. Zaškrtněte Enable SNTP
2. Podle tabulky 1 vyplňte následující
   - Primary SNTP
   - Secondary SNTP
   - Tertiary SNTP
   - Timeout
   - Polling Interval
   - Retry Count
   - Time Zone
   - Day Light
3. Údaje formuláře odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
4. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
5. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Tabulka 1 Parametry nastavení SNTP

Pole	Překlad	Popis / význam
Primary SNTP server	Primární SNTP server	IP adresa nebo hostname prvního SNTP serveru. Může být určeno poskytovatelem (ISP) nebo zvoleno uživatelem.
Secondary SNTP server	Druhý SNTP server	Záložní SNTP server
Tertiary SNTP server	Třetí SNTP server	Druhý záložní SNTP server
Timeout	Timeout (sekundy)	Pokud se nepodaří spojení s jedním SNTP serverem do doby dané hodnotou **Timeout**, bude se pokoušet u dalšího serveru
Polling Interval	Interval dotazování (minuty)	Po uplynutí doby **Polling Interval** od posledního úspěšného stažení časového údaje se celý proces opakuje. (tj. interval obnovování)
Retry Count	Počet pokusů	Maximální počet pokusů, které RG učiní u jednotlivého SNTP serveru.
Time Zone	Časové pásmo	ČR = GMT + 1
Day Light	Letní čas	Zaškrtnutím se hodiny přesunou na letní čas. Pozor – přepnutí neprobíhá automaticky podle kalendáře, je nutno dělat ručně.

4.3.3. ADVANCED – SNMP

SNMP: Simple Network Management Protocol je protokol na bázi UDP (port 161) používaná při správě počítačových sítí. Struktura SNMP se skládá různých komponent, jako SNMP agent (server), stanice správy sítě (NMS), protokoly správy sítě a databáze MIB.



Tabulka 2 Parametry SNMP

Pole	Překlad	Popis / Význam
Enable SNMP Agent	Aktivovat SNMP agenta	Výchozí nastavení je vypnuto
Enable SNMP Traps	Zapnout SNMP zprávy	Výchozí nastavení je vypnuto
Name	Jméno	Jméno routeru, přidělené administrátorem
Location	Umístění	Fyzické umístění routeru
Contact	Kontakt	Kontaktní osoba nebo informace o routeru
Vendor OID	ID dodavatele	Identifikace dodavatele podsystému správy sítě. ID je ve formátu SMP stromu. Například Texas Instruments má přidělen podstrom 1.3.6.1.4.1.294
Community	Komunita	SNMP definuje komunitu jako vztah mezi agentem a jedním nebo více SNMP manažery. Jestliže textová část názvu souhlasí s názvem komunity, známé přijímanou SNMP entitou, je vysílací SNMP entita považována za člena komunity a je jí přidělena jistá úroveň přístupu: pouze čtení (*read-only*) nebo čtení+zápis (*read-write*). Profil komunity je dán složením přístupového práva komunity a projektu spravovaného MIB. Profil komunity definuje povolené operace, které mohou být s objektem prováděny. V případě RG jsou výchozí název komunity *public* a přístupové právo *read-only* uloženy v konfiguračním souboru. Jsou povoleny operace GET a GETNEXT pro všechny objekty s právy READ-ONLY a READ-WRITE vůči MIB. Přes webové rozhraní lze pro RG definovat tři názvy komunity. V budoucích verzích se počítá s podporou SNMPv2c a SNMPv3

Community Name	Název komunity	Je možno definovat tři komunity, včetně přednastavené *public*.
Community Access Right	Přístupová práva komunity	Dvě úrovně: • **ReadOnly** (pouze čtení) – povoleny operace GET a GETNEXT vůči všem objektům v MIB • **ReadWrite** (čtení i zápis) – povoleny GET, GETNEXT a k objektům s možností zápisu (*read-writable*) i operace SET
Trap	Zpráva	Trap je oznámení o události. RG podporuje čtyři standardní trapy: • WarmStart Trap • LinkUp Trap • LinkDown Trap • Authentication Failure Trap
Trap Destination IP	Cílová adresa trapu	Lze nastavit tři různé adresy
Trap Community		Název komunity trapu
Trap Version	Verze trapu	• SNMP v1 • SNMP v2c

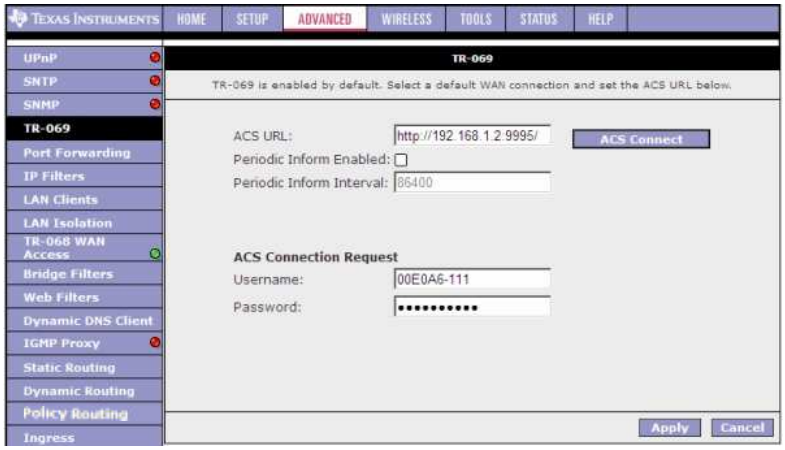
4.3.4. ADVANCED – TR-069

TR-069 je protokol, definující jednotný rámec pro zabezpečenou správu CPE (koncové zařízení na straně zákazníka) autokonfiguračním serverem (ACS) ze strany WAN.

TR-069 zahrnuje především:

- Automatickou bezpečnou konfiguraci a zajištění dynamických služeb (firewall, antispam…)
- Správu softwaru / firmwaru
- Sledování stavu a výkonu
- Diagnostiku

Na následujícím obrázku je výchozí stránka nastavení protokolu TR-069. Přístup je přes odkaz TR-069 v levém sloupci ze stránky **Advanced**. Na stránce TR-069 se nastavují parametry připojení; koncový uživatel by zde **neměl** zasahovat.



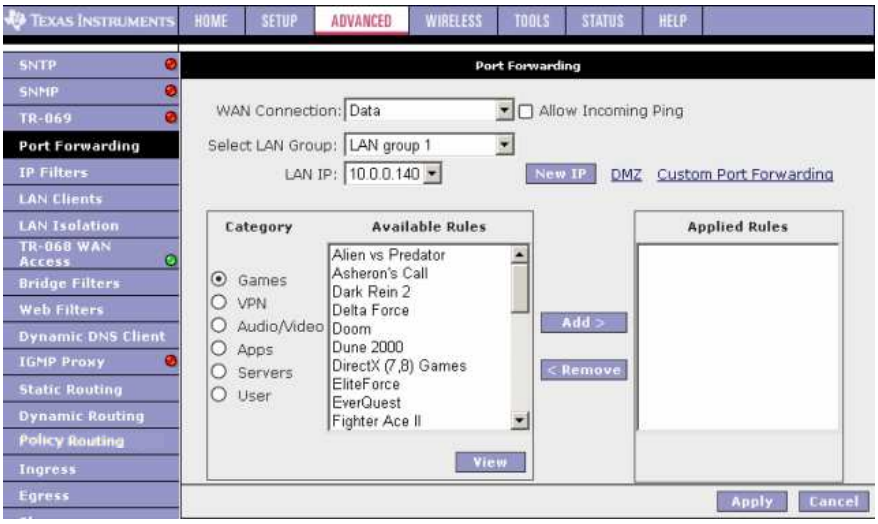
Tabulka 3 Parametry nastavení TR-069

Pole	Překlad	Popis / Význam
ACS URL	URL adresa autokonfiguračního serveru (ACS)	Podle informací od poskytovatele služby (ISP)
Periodic Inform Interval Enabled	Periodicky se přihlašovat k ACS	Je-li zapnuto, je potřeba vyplnit ještě **Periodic Inform** Interval
Periodic Inform Interval	Perioda dotazů u ACS (sekundy)	Doporučená hodnota je 86400 sekund, tj. jednou denně
ACS Connect	Připojit se k ACS	Ruční připojení (mimo interval Periodic Inform)

4.3.5. ADVANCED – Port Forwarding

Směrování portů: Směrování portů (někdy se označuje jako Virtual Servers) je nezbytné, protože překladač adres (NAT) směruje pouze provoz z internetu na specifický port pouze tehdy, je-li toto namapování zaneseno v jeho směrovací tabulce. To však přináší problémy v případě, že chcete zdroje LAN zpřístupnit internetovým klientům, například při hraní síťových her nebo hostování síťových aplikací.

Směrování portů je tedy důležité při hraní některých her, chatování, videokonferencích a dalších aplikacích. Rovněž budete potřebovat konfigurovat směrování portů, pokud zamýšlíte provozovat web server nebo mail server, jenž má být přístupný z vnější sítě.



Tabulka 4 Parametry pro přesměrování portů

Pole	Překlad	Popis / Význam
WAN Connection		Vyberte WAN připojení, pro které má přesměrování platit
Select LAN Group	Zvolte skupinu LAN	
LAN IP	IP adresa hostitele v LAN	
Allow Incoming Ping	Povolit příchozí Ping (ICMP)	Povolení odpovědi na příchozí požadavek Ping z internetu
DMZ	Demilitarizovaná zóna	Více informací je v kapitole „**Chyba! Nenalezen zdroj odkazů.**“
Custom Port Forwarding	Vlastní definice přesměrování	Odkaz na stránku nastavení vlastních pravidel pro přesměrování. Více informací je v kapitole „Chyba! Nenalezen zdroj odkazů.“

Category	Kategorie	Výběr z předdefinovaných nebo uživatelem definovaných kategorií
Available Rules	Dostupná pravidla	Seznam pravidel ve zvolené kategorii
Applied Rules	Aktivovaná pravidla	Seznam zvolených platných pravidel ve zvolené kategorii

Předdefinovaná pravidlo pro jednu skupinu LAN lze aktivovat následujícím postupem:

1. Zvolte **WAN Connection**, **LAN Group** a **LAN IP**.
2. Pokud se požadovaná LAN IP nenachází v rozbalovacím seznamu, můžete ji přidat na stránce **LAN Client** – zde klikněte na **New IP** (nová IP).
3. Vyberte kategorii a pravidlo (aplikaci) a kliknutím na **Add** (přidat) je přidáte do boxu platných pravidel **Applied Rules**.

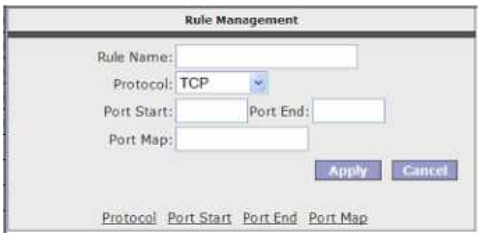
   Poznámka – Výpis pravidel spojených s daným pravidlem (aplikací) zobrazíte tlačítkem **View** (zobrazit) – přesunete se na stránku **Rule Management**

Směrování portů – zobrazení nastavení existujícího pravidla

4. Pokud se požadované pravidlo v seznamu nenachází, můžete ho vytvořit sami v kategorii **User** (uživatelský). Přepněte na **User**, potom klikněte na **New**.

   Poznámka – Tlačítka **New**, **View** a **Delete** (Nový, Zobrazit , Smazat) jsou zobrazeny pouze při volbě kategorie User. Všechny uživatelem definovaná pravidla se pak nacházejí v této kategorii.

5. Na stránce **Rule Management** je možno vytvářet nová pravidla. Zadejte název (**Name**), protokol, rozmezí portů (**Port Start / End**) a číslo portu, na nějž má být tento port namapován (**Port Map**), pokračujte **Apply**.
6. Vytvořené pravidlo se přidá do seznamu kategorie **User**. Můžete jej dále upravovat nebo smazat.
7. Podle potřeby přidejte další filtry.
8. Údaje formuláře odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
9. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
10. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).



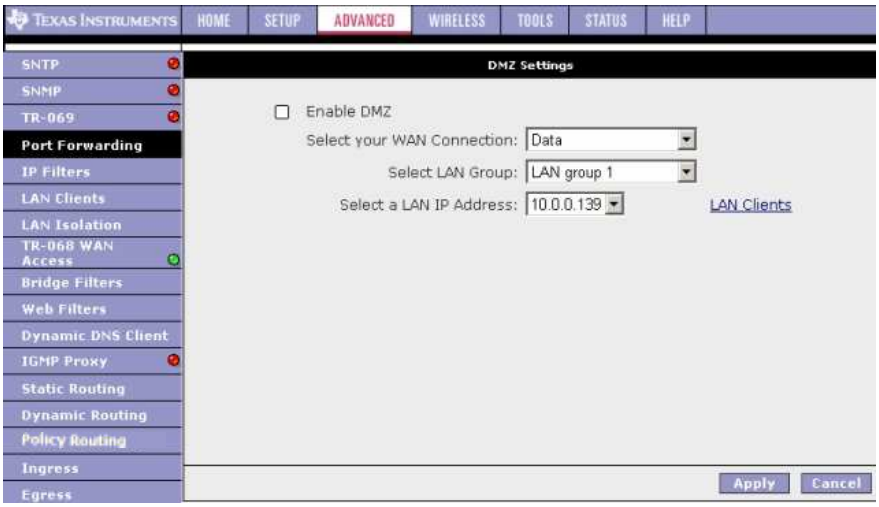
Poznámka – Odkaz **Custom Port Forwarding** lze použít také použít pro přidání programu k existujícímu seznamu.

4.3.5.1. Nastavení DMZ

DMZ (Demilitarized Zone): Je-li určitá adresa v LAN síti nastavená jako DMZ (demilitarizovaná zóna), potom je otevřena pro veškerý provoz vůči WAN (kromě dat, pro něž je nastaveno přesměrování portů). Výchozí nastavení je DMZ vypnuta. Aktivací DMZ vytváříte oblast nezabezpečenou firewallem routeru.

Postup při nastavení:

1. Na stránce **Port Forwarding** klikněte na **DMZ**. Načte se stránka **DMZ Settings**



2. Zaškrtněte **Enable DMZ**.
3. Zvolte WAN připojení, skupinu LAN, a IP adresu klienta v LAN
   DMZ lze konfigurovat pro každou LAN skupinu zvlášť.
   Poznámka – Odkaz LAN Clients vede na stejnojmennou stránku nastavení.
4. Údaje formuláře odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
5. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
6. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

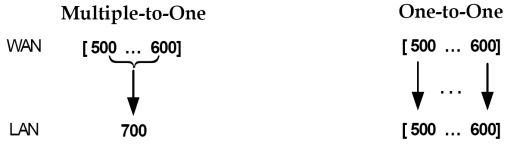
Tabulka 5 Parametry nastavení DMZ

Pole	Překlad	Popis / Význam
Enable DMZ	Aktivovat DMZ	Výchozí nastavení je vypnuto
Select your WAN Connection	Zvolte WAN připojení	WAN připojení, pro něž má DMZ platit
Select LAN Group	Vyberte skupinu LAN	LAN skupina, v níž se má DMZ nacházet
Select a LAN IP Address	Vyberte LAN IP adresu	Tato adresa se stane DMZ, tj. bude vystavena nechráněnému přístupu z internetu se všemi riziky.
LAN Clients		Odkaz na stránku **LAN Clients**. Více informací v kapitole „**Chyba! Nenalezen zdroj odkazů.**“

4.3.5.2. Custom Port Forwarding

Na této stránce můžete vytvořit až 15 nových přesměrování pro vlastní speciální potřebu (např. vytvoření vlastní NAT)

Tabuka 6 Parametry pro uživatelské přesměrování portů

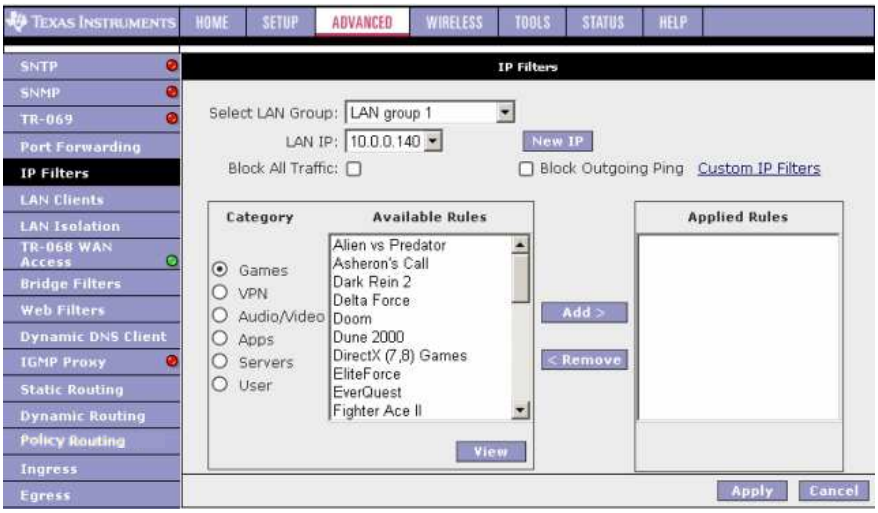
Pole	Překlad	Popis / Význam
Connection		Vyberte WAN připojení, pro nějž má nové pravidlo platit
Enable	Zapnuto	Po přidání pravidla tlačítkem **Apply** se zaškrtne automaticky
Application		Název aplikace, která bude přesměrování využívat
Protocol		Tři protokoly: • *TCP* • *UDP* • *TCP a UDP*
Source IP Address	IP adresa zdroje	Hodnota *0.0.0.0* zastupuje všechny adresy
Source Netmask	Maska zdroje	*255.255.255.255* zastupuje všechny masky
Destination IP Address	IP adresa cíle	
Destination Netmask	Maska cíle	Maska podsítě, v níž se nachází cíl. Přednastavená hodnota je *255.255.255.255*
Destination Port Start	Počáteční číslo portu cíle	Dolní mez intervalu portů, který má být pro tuto aplikaci otevřen
Destination Port End	Koncové číslo portu cíle	Horní mez intervalu portů, který má být pro tuto aplikaci otevřen
Destination Port Map	Port cíle, na něž má být provoz přesměrován	Jsou dva druhy mapování: • One-to-one (jeden na jeden) • Multiple-to-one (pásmo Start-End na jeden port) 

Poznámka – při zadávání IP adres, masek a portů je možno použít hvězdičku * (zastupuje libovolné číslo)

4.3.6. ADVANCED – IP Filters

Filtrování IP adres umožňuje určitým aplikacím nebo službám zablokovat přístup a to na základě IP adresy počítače. Na stránce IP Filters můžete pro určité IP adresy blokovat např. přístup na web nebo i veškerý odchozí provoz.

K dispozici je předdefinovaná databáze IP filtrů, ze které je možno přiřazovat jednotlivé filtry jednomu nebo více členům určité LAN skupiny. Nastavení předdefinovaných filtrů je možno prohlížet; dále lze vytvářet, upravovat a mazat filtry vlastní.



Tabulka 7 Přehled parametrů IP filtru

Pole	Překlad	Popis / Význam
Select LAN Group	Zvolte skupinu LAN	Skupina LAN, pro níž má filtr platit
LAN IP		IP adresa v dané skupině LAN, pro níž má filtr platit
Block All Traffic	Blokovat veškerý provoz	Blokování veškerého síťového provozu
Block Outgoing Ping	Blokovat odchozí Ping	Může se hodit v případě, že se v LAN počítači nachází virus, který zahlcuje síť stálým rozesíláním pingů (Ping-of-Death Denial Of Service)
Custom IP Filters	Vlastní IP filtry	Odkaz na stránku **Custom IP Filters**. (viz „8.1 Vlastní nastavení IP filtru“)
Available Rules	Dostupná pravidla	Seznam předdefinovaných a uživatelských pravidel podle kategorií
Applied Rules	Aktivní pravidla	Seznam aktivovaných pravidel podle kategorií

Postup při aktivaci předdefinovaného filtru:

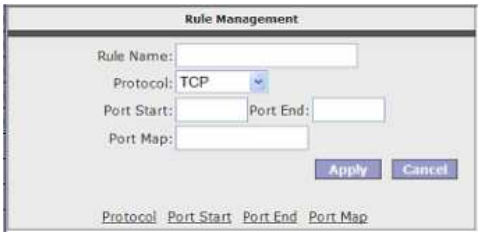
1. Na stránce **IP Filters** zvolte **LAN Group** a **LAN IP**.

   Pokud požadovaná LAN IP se v rozbalovacím seznamu nenachází, můžete ji přidat na stránce **LAN Client** – zde klikněte na **New IP** (nová IP).
2. Vyberte požadovaný filtr v dané kategorii. Kliknutím na **View** si můžete prohlédnout jeho nastavení. Tlačítkem **Add** přesunete vybraný filtr do boxu **Applied Rules**.
3. Pokud žádné z předdefinovaných filtrů nevyhovuje Vašim potřebám, můžete si vytvořit vlastní – přepněte na **User** (obr. 14) a potom **New**.

   Poznámka – Výpis pravidel spojených s daným pravidlem (aplikací) zobrazíte tlačítkem **View** (zobrazit) – přesunete se na stránku **Rule Management**
4. Pokud se požadované pravidlo v seznamu nenachází, můžete ho vytvořit sami v kategorii **User** (uživatelský). Přepněte na **User**, potom klikněte na **New**.

   Poznámka – Tlačítka **New**, **View** a **Delete** (Nový, Zobrazit , Smazat) jsou zobrazeny pouze při volbě kategorie User. Všechny uživatelem definovaná pravidla se pak nacházejí v této kategorii.

5. Na stránce **Rule Management** je možno vytvářet nová pravidla. Zadejte název (**Name**), protokol, rozmezí portů (**Port Start / End**) a číslo portu, na nějž má být tento port namapován (**Port Map**), pokračujte **Apply**.
6. Vytvořené pravidlo se přidá do seznamu kategorie **User**. Můžete jej dále upravovat nebo smazat.
7. Podle potřeby přidejte další filtry.
8. Údaje formuláře odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
9. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
10. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

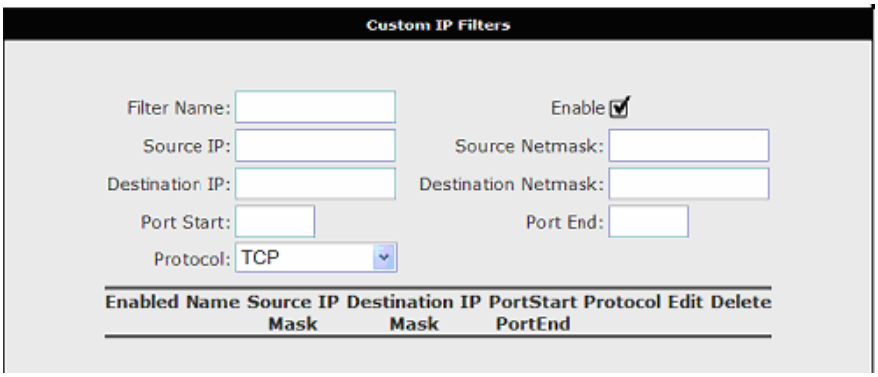


Poznámka – Odkaz **Custom IP Filters** lze použít také použít pro přidání programu k existujícímu seznamu (viz dále).

4.3.6.1. Custom IP Filters

Na stránce **Custom IP Filters** můžete definovat až 20 vlastních filtrů. Blokování probíhá na základě:

- IP adresa a maska podsítě cíle nebo zdroje
- TCP portu (možno zadat jako pásmo)
- Protokolu
  - TCP
  - UDP
  - TCP i UDP
  - ICMP
  - Any (Všechny)



Tabulka 8 Parametry nastavení IP filtru

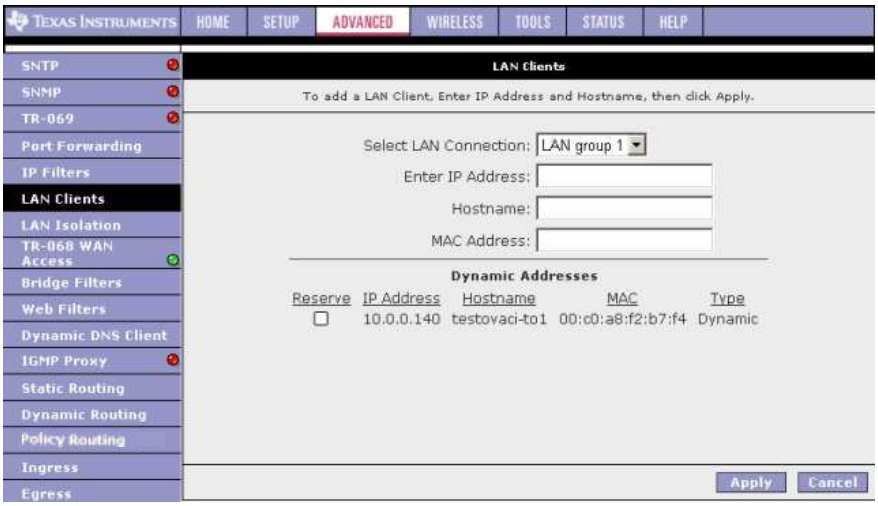
Pole	Překlad	Popis / Význam
Filter Name	Název filtru	Zvolený název
Enable	Zapnuto	Po přidání filtru tlačítkem **Apply** se automaticky zaškrtne
Source IP	IP adresa zdroje	IP adresa, jejíž odchozí provoz má být blokován
Source Netmask	Maska zdroje	Maska podsítě, v níž se nachází zdroj
Destination IP Address	IP adresa cíle	Provoz směřující k tomuto cíli bude blokován. Hodnota *0.0.0.0* zastupuje všechny adresy
Destination Netmask	Maska cíle	Maska podsítě, v níž se nachází cíl. Hodnota *255.255.255.255* zastupuje všechny masky.
Port Start	Počáteční číslo portu cíle	Dolní mez intervalu portů, který má být blokován
Port End	Koncové číslo portu cíle	Horní mez intervalu portů, který má být blokován
Protocol		Možnosti: *TCP, UDP, TCP a UDP, ICMP, Všechny (Any)*

4.3.7. ADVANCED – LAN Clients

Na této stránce se nachází přehled všech hostitelů v LAN. Hostitel může být veden jako *dynamický* (jeho adresa byla pronajata DHCP serverem routeru), nebo *statický* (ručně nastavená IP).

Zde můžete přidat *statickou* IP adresu (součást podsítě LAN). Existující adresu spadající do intervalu DHCP serveru je možno smazat a uvolnit ji tak pro další použití.

Poznámka – Klienti s dynamickou IP adresou budou zobrazeni pouze při aktivním DHCP serveru.



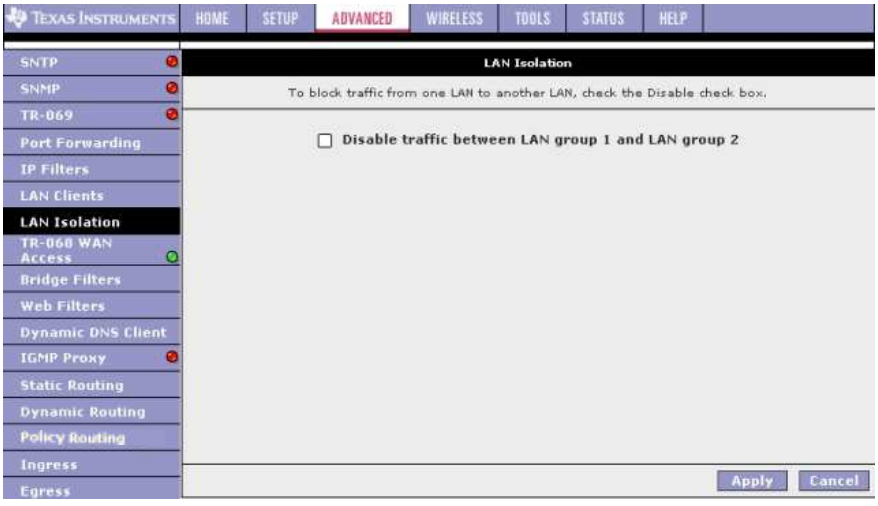
Postup při přidávání klienta LAN:

1. Na stránce **LAN Clients** zvolte **LAN Connection**, zadejte **IP** adresu, **Hostname** a **MAC** adresu.
2. Klikněte na **Apply**.
   IP adresa je umístěna a zobrazena v seznamu LAN klientů jako *dynamická* (viz obrázek)
3. Adresu můžete změnit z dynamické na statickou kliknutím na **Reserve**, potom **Apply**.
   Jak je vidět z dalšího obrázku, adresa se změnila na *Static*, Můžete ji smazat kliknutím na **Delete**.
4. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
5. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
6. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Poznámka – Pravidlo firewallu, přiřazené k určité dynamické adrese, po vypršení doby pronájmu přestane platit

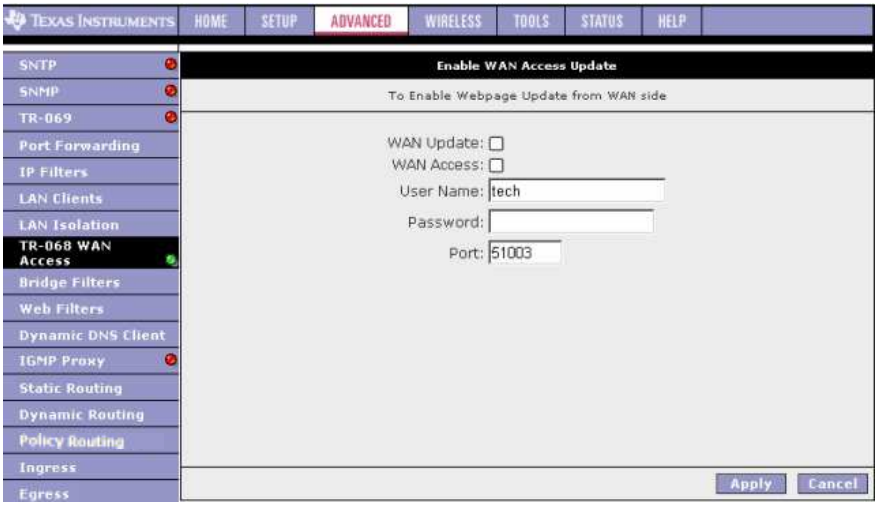
4.3.8. ADVANCED – LAN Isolation

Na této stránce můžete blokovat vzájemný provoz mezi jednotlivými skupinami LAN. LAN skupiny je možno definovat podle potřeby (zahrnují WLAN, USB, ethernet, SSID1 až 3). Takto můžete vytvořit chráněnou privátní část LAN (např. s důležitými daty).



4.3.9. ADVANCED – TR-068 WAN Access (Vzdálený přístup)

Na této stránce (**TR-068 WAN Access**) můžete dočasně povolit přístup k nastavení routeru ze strany WAN (např. technikům). Od okamžiku povolení vzdálené správy je očekáváno její přihlášení do 20 minut, jinak povolení (účet) vyprší. Po úspěšném přihlášení vzdáleného správce vyprší účet po 20 minutách nečinnosti.



Tabulka 10 Parametry pro povolení vzdálené správy (TR-098 WAN Access)

Pole	Překlad	Popis / význam
WAN Update		Zaškrtněte, chcete-li vytvořit účet s právy čtení i zápisu
WAN Access		Vytvoří účet s právy pouze číst
User Name	Uživatelské jméno	Přihlašovací jméno vzdáleného uživatele
Password	Heslo	
Port		Číslo portu, na kterém má probíhat přihlášení

Postup při vytvoření účtu vzdáleného správce:

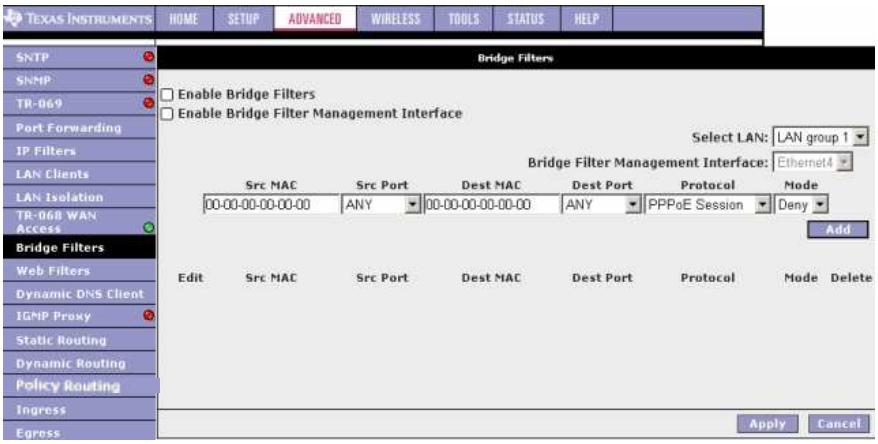
1. Zaškrtněte **WAN Update**, má-li mít vzdálený správce právo měnit konfiguraci.
2. Zaškrtněte pouze **WAN Access**, má-li mít vzdálený správce právo jen prohlížení.
3. Zadejte zvolené přihlašovací jméno a heslo (**User Name** a **Password**)
4. Zadejte zvolený port pro přihlášení (například 51003)
5. Údaje odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
6. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
7. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
8. Vzdálený správce potom přihlašuje tak, že do svého adresového řádku zadá URL (příklad):

   http(s)://10.10.10.5:51003
   Syntaxe: http(s)://<**WAN IP adresa routeru**>:<**Číslo portu**>

4.3.10. ADVANCED – Bridge Filters

Filtr v režimu přemostění (bridge) testuje každý datový rámec (MAC adresu zdroje a cíle, typ rámce, fyzický port). Posloupnost testování odpovídá pořadí zadaných pravidel. Je-li nalezena shoda, uplatní se příslušná filtrační funkce (povolení nebo odepření). Filtr dokáže testovat rámce pouze z těch portů, které jsou fyzicky součástí mostu. Lze definovat až 20 pravidel

Jednotlivé filtry lze zapínat, přidávat, měnit nebo mazat na stránce **Bridge Filters**



Postup:

1. Filtr zapnete zaškrtnutím **Enable Bridge Filters**.
2. Pravidlo filtru přidáte zadáním MAC adresy a portu zdroje (**Src MAC, Port**), cíle (**Dest MAC, Port**), protokolu a typu filtrace (**Deny/Allow** = zakázat/povolit), poté klikněte na **Add**.
3. Tlačítkem **Edit**, resp. **Delete** můžete editovat, resp. smazat stávající pravidlo.
4. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
5. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
6. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Poznámka – V tabulce filtrů se nacházejí čtyři skrytá pravidla, která zajišťují, abyste si omylem nezablokovali a neodřízli přístup k routeru. Tato pravidla se týkají určité kombinace MAC adresy a portu zdroje a cíle a protokolu.

Tabulka 11 Parametry nastavení filtru přemostění

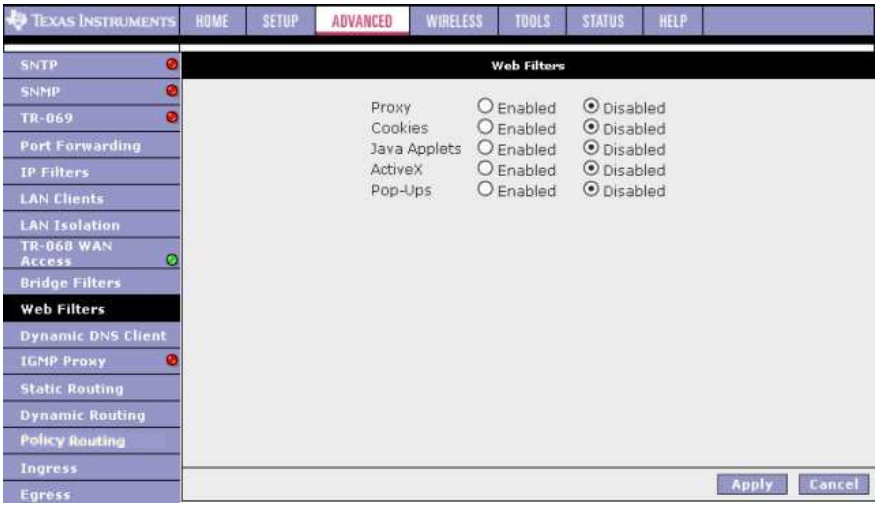
Pole	Překlad	Popis
Enable Bridge filters	Zapnout filtr přemostění	
Enable Bridge Filter Management Interface	Zapnout filtraci z rozhraní, k němuž je připojen administrátor	Tato funkce zajišťuje, že si nezablokujete přístup ke správě RG. Je nutno nastavit ještě další dvě položky.
Select LAN	Vyberte LAN skupinu	LAN skupina, v níž se nachází administrátor
Bridge Filter Management Interface		Rozhraní, přes které má být připojen administrátor. Podle zvolené skupiny LAN mohou být možnosti: *Ethernet, USN a WLAN*
Src MAC	MAC adresa zdroje	Musí být ve formátu xx-xx-xx-xx-xx-xx, 00-00-00-00-00-00 znamená libovolná. Místo nul je možno nechat prázdný znak
Src Port	Port zdroje	Možnosti: *Any* (libovolný), *Ethernet*, *USB*, *WLAN* nebo *WAN Bridge Connection Port* (přemosťovací port při částečném přemostění). Pokud není zobrazena ani jedna z možností, zkontrolujte DSL připojení.

Dest MAC	MAC adresa cíle	
Dest Port	Port cíle	Možnosti: *Any* (libovolný), *Ethernet*, *USB* a *WLAN*
Protocol		Možnosti: *PPPoE Session*, *PPPoE Discovery*, *IPX – Ethernet II, RARP, IPv6, IPv4* a *Any* (všechny)
Mode		Deny / Allow = zakázat / povolit

4.3.11. ADVANCED – Web filtr

Zde je možno filtrovat určité web stránky na základě hodnocení jejich obsahu.

Poznámka – Tato funkce z důvodu paměťové náročnosti není instalována ve všech typech RG



Dostupné filtry (výchozí nastavení je vypnuto)

- Proxy server
- Cookies
- Java applets
- Prvky ActiveX
- Pop-ups (vyskakovací okna)

Příslušný filtr zapnete přepnutím na **Enable**, nakonec klikněte na **Apply**.

4.3.12. ADVANCED – Dynamic DNS Klient

Pokaždé, když se RG připojí k internetu (ISP), může obdržet jinou IP adresu. Pokud chcete, aby vaše síť byla zároveň přístupná pro vnější uživatele, museli byste neustále sledovat aktuální přidělenou IP adresu. Řešením je registrovat se u DNS serveru jako dynamický klient (DDNS). DNS server potom Vaši proměnnou IP adresu namapuje na stále stejné registrované jméno (hostname). Tato funkce se nastavuje na stránce **Dynamic DNS Klient.**

Postup:

1. Na stránce **Dynamic DNS Client** vyplňte:
   - Connection (připojení)
   - DDNS server
   - DDNS klient
   - User Name
   - Password
   - Domain Name
2. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
3. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
4. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Tabulka 12 Parametry nastavení dynamického DNS klienta

Pole	Překlad	Popis / Význam
Connection		Zvolte WAN připojení, přes nějž má probíhat přístup
DDNS Server	Dynamický DNS server	Vyberte ze seznamu DDNS, u něhož jste registrováni. Podle typu se může jednat o placenou službu.
DDNS Client		Zapíná / vypíná funkci DDNS
User Name	Jméno	Přiděluje DDNS
Password	Heslo	Přiděluje DDNS
Domain Name	Doménové jméno	Registrované u DDNS

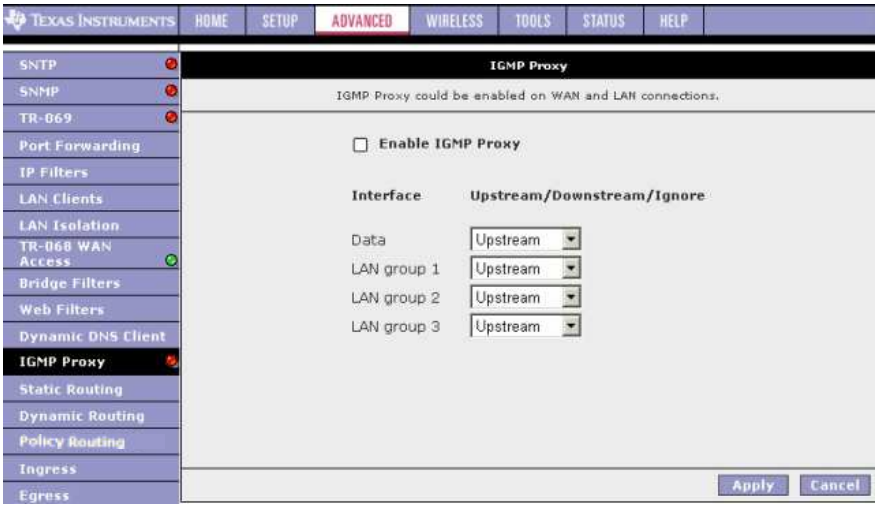
4.3.13. ADVANCED – IGMP Proxy

Multicasting je omezenou formou broadcastingu. Datagramy jsou vyslány jednosměrným protokolem UDP pouze skupině klientů, nazvané **Host Group** (na rozdíl od broadcast., který vysílá pro celou síť). Host group je skupina jednoho nebo více členů, každý je identifikován vlastní IP adresou. Vlastnosti Host Group:

- Kdokoliv se může z vlastní vůle připojit nebo odhlásit
- Umístění člena není omezeno
- Počet členů skupiny není omezen
- Jeden člen může být členem více skupin Host Group

Multicasting je přirozeným řešením v případech, kdy je třeba rozeslat stejná data pro jedno nebo více zařízení. Například pro multimediální aplikace je zvláště výhodné – velký objem dat a poměrná benevolence vůči výpadkům (protokol UDP nezaručuje doručení). Proti zasílání dat každému adresátu zvlášť, multicasting snižuje zatížení sítě.

IP hostitel rozesílá informace o svém členství v určité Host Group okolním routerů pomocí protokolu IGMP (Internet group management protocol). Podobně routery používají IGMP k mapování svého okolí a zjišťování členství svých hostitelů. RG obsahuje IGMP proxy server. Je-li zapnut, RG funguje vůči LAN jako proxy (zjišťuje a přebírá požadavky na členství klientů v multicast skupinách) nebo jako multicast router, rozesílající multicast pakety do skupin nacházejících se ve WAN.



Na stránce IGMP Proxy můžete nastavit multicasting u dostupných WAN a LAN připojení. Příslušné WAN nebo LAN rozhraní můžete konfigurovat jako:

- Upstream (směrem k serveru) – rozhraní, přes které jsou IGMP požadavky klientů zasílány k multicast routeru
- Downstream (od serveru ke klientovi) – rozhraní, přes které jsou data od multicast routeru rozesílány ke klientům v multicast skupině.
- Ignore – požadavky IGMP a multicast data jsou ignorovány.

Máte dvě možnosti:

- Jedno nebo více rozhraní WAN konfigurovat pro upstream
- Jedno nebo více rozhraní LAN konfigurovat pro upstream.

Poznámka – Před zapnutím IGMP proxy je nutno mít konfigurované aspoň jedno WAN připojení

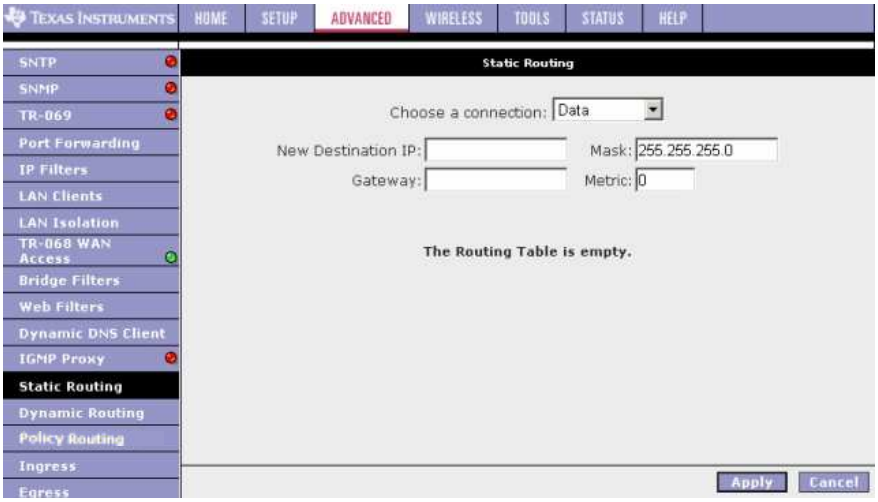
Tabulka 13 Parametry nastavení IGMP proxy

Pole	Překlad	Popis / Význam
Enable IGMP Proxy	Zapnout IGMP proxy	
Interface	Rozhraní	Jsou tři možnosti konfigurace pro každé WAN/LAN rozhraní: • Upstream – směrem od klienta k serveru • Downstream – od serveru ke klientovi • Ignore – neprůchozí.

4.3.14. ADVANCED – Static Routing

Pokud má router obsluhovat více než jednu síť, je potřeba nastavit statické směrování mezi sítěmi. Statické směrování umožňuje uživatelům z jedné IP domény přístup k internetu přes router nacházející se v jiné doméně. V tabulce Static Route je definovaná cesta, kterou musí informace projít, aby dosáhla požadovaného hosta nebo síť, která poskytuje přístup na internet.

Zde je možno definovat směrování pro určité podsítě v LAN / WAN. Směrovací tabulka se zadává ručně. Max. počet řádků tabulky je 16.

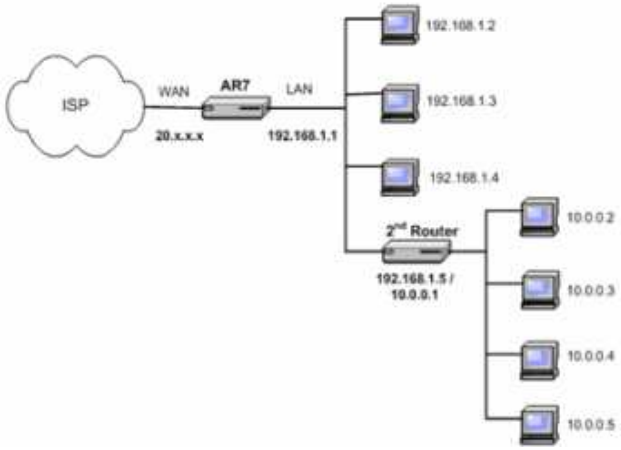


Tabulka 14 Parametry statické směrovací tabulky

Pole	Překlad	Popis / Význam
Select a Connection	Vyberte připojení	
New Destination IP	IP adresa nového cíle	IP adresa podsítě. (Můžete zadat také adresu každé stanice v podsíti)
Mask	Maska	Maska cílové podsítě
Gateway	Brána	Adresa další stanice, přes kterou má jít provoz směrem k cílové podsíti
Metric		Určuje počet skoků (hops) mezi uzly sítě na trase paketu. Přednastavená hodnota je 0, což znamená, že cílová podsíť je přímo jeden skok od místní LAN.

Příklad:

Předpokládejme, že máte síť jako na následujícím obrázku. Ve Vaší LAN se nachází router (192.168.1.1) a tři stanice (192.168.1.x). K LAN je přes druhý router (192.168.1.5 / 10.0.0.1) připojena další podsíť se čtyřmi stanicemi (10.0.0.x). Tyto čtyři stanice by normálně byly nepřístupné, zpřístupní se až zapsáním do směrovací tabulky v RG. Můžete přidat každou stanici zvlášť, snadnější je však zadat naráz celou podsíť. Postup je popsán dále.

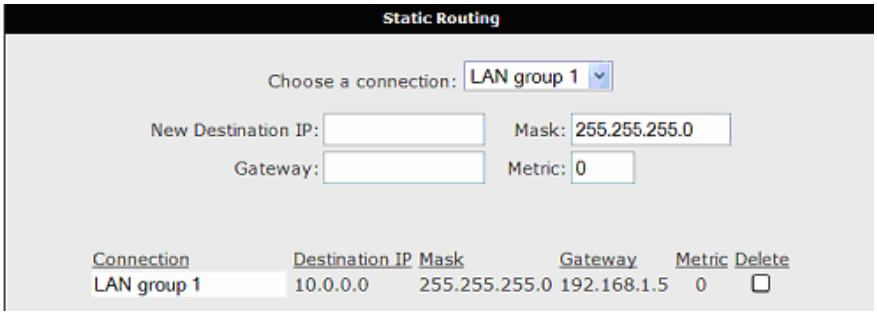


Statické směrování – LAN s podsítí

Nastavení směrovací tabulky:

1. Z rozbalovacího menu **Choose a connection** vyberte LAN spojení *LAN Group 1*.
2. Zadejte parametry (hodnoty pro příklad z obrázku):
   - **New Destination IP** – adresa nového cíle: *10.0.0.0* (adresa podsítě – končí nulou)
   - **Mask**: *255.255.255.0* (maska podsítě)
   - **Gateway**: *192.168.1.5* (adresa druhého routeru ze strany první LAN)
   - **Metric**: *0*

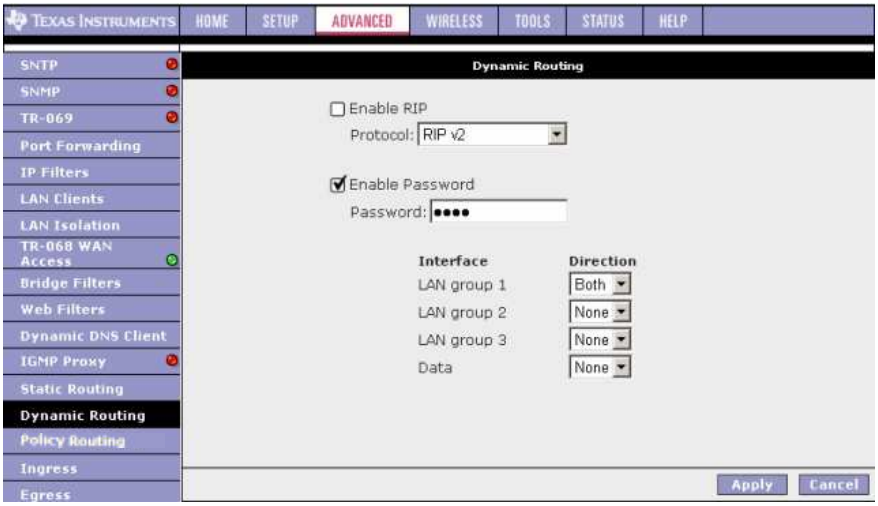
   Tím se sděluje RG, že byla přidána nová síť s adresou *10.0.0.0* a maskou *255.255.255.0*, která je přístupná přes stanici *192.168.1.5*. Metrika *0* znamená, že přidaná síť je o jednu úroveň dále od první LAN.
3. Uložíte tlačítkem **Apply**
4. Do směrovací tabulky byla přidána nová podsíť, která získala přístup k WAN.



   Můžete zadat až 16 řádků. Tlačítkem **Delete** smažete řádky se zaškrtnutým políčkem.
5. Údaje odešlete tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
6. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
7. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

4.3.15. ADVANCED – Dynamic Routing

Funkce dynamického směrování umožňuje RG dynamicky měnit směrování mezi podsítěmi LAN a WAN. K předávání a šíření informací mezi jednotlivými routery v síti slouží protokol RIP (Routing information protocol). Jeho přenos je podporován všemi rozhraními LAN i WAN. Router se zapnutým RIP v pravidelných intervalech (30 sekund) rozesílá své vlastní směrovací tabulky a naopak přijímá směrovací tabulky od okolních routerů a podle nich aktualizuje svou vlastní. Dynamické routování se nastavuje na stránce **Dynamic Routing.**



Tabulka 15 Parametry nastavení dynamického směrování

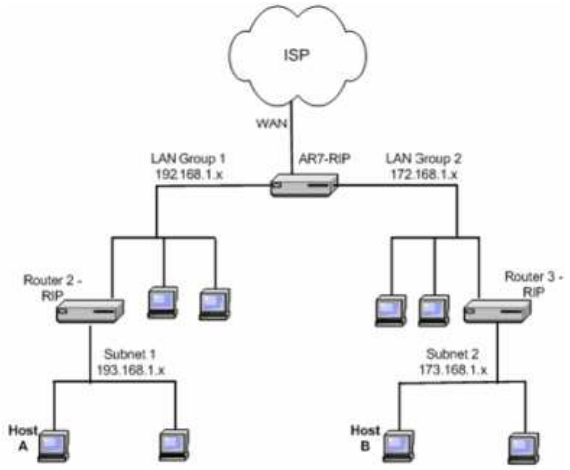
Pole	Překlad	Popis / Význam
Enable RIP	Zapnout RIP	
Protocol		Jsou k dispozici tři protokoly: RIV v1 (na bázi UDP) RIP v2 (multicast protokol) RIP kompatibilní s v1 Poznámka: Routery používající RIPv1 nebo RIPv1-kompatibilní mohou spolu komunikovat, RIPv1 s RIPv2 nikoliv

Enable Password	Zapnout heslo	Max. délka je 16 znaků
Direction	Směr toku aktualizací	Router se zapnutým RIP normálně svými daty „poučuje“ okolní routery. Parametr Direction je možné nastavit rozhraní, od kterých se „učí“, podle kterých si opravuje vlastní směrovací tabulky. Tím určujete směr šíření směrovacích dat v síti. Například volbou *In only* (pouze dovnitř) chráníte ostatní routery v privátní LAN před přepsáním jejich tabulek tabulkou routeru na straně WAN. Jsou k dispozici čtyři možnosti směrování toku přes rozhraní: • **Both** (oba) – příjem aktualizací a jejich rozesílání dalším routerům, připojených k tomuto rozhraní • **In** (dovnitř) – příjem aktualizací povolen, rozesílání zastaveno • **Out** – pouze odesílání vlastních směrovacích dat • **None** – žádné odesílání a ignorování příchozích

Příklad:

Pro demonstraci uvažujme rozšířenou variantu sítě uvedené v předchozí kapitole (statické směrování). Na následujícím obrázku je vidět její struktura: dvě skupiny LAN (*192.168.1.x* a *172.168.1.x*), každá s dalším routerem a jeho podsítí. Chce-li hostitel A v podsíti 1 (192.168.1.x) hovořit s hostitelem B v podsíti 2 (*173.168.1.x*), má dvě možnosti:

- Podobně jako v předchozí kapitole je možné přidat obě podsítě do statické směrovací tabulky (potřeba dva záznamy)
- Na všech routerech aktivovat dynamické směrování. Tuto funkci je třeba zapnout u všech routerů v síti a musejí komunikovat na stejném (nebo vzájemně kompatibilním) RIP protokolu. Postup nastavení je popsán dále.



Dynamické směrování – LAN s podsítěmi

Konfigurace dynamického směrování – postup:

1. Zaškrtněte **Enable RIP**.
2. Pro testovací účely zvolte např. protokol ***RIP v2***
   Stejný protokol musí být nastaven i pro ostatní routery v síti
3. Zaškrtněte **Enable Password** a zadejte zvolené heslo
   Heslo není povinné, je pro zvýšení bezpečnosti.
4. Pro rozhraní LAN 1 a LAN 2 ponechte položku **Direction** nastavenou **Both** (oba směry)
   Všimněte si, že není třeba zadávat adresu ani masku připojené podsítě. Routery s RIP si potřebné údaje zjistí a rozešlou automaticky.
   Podobně bude třeba nastavit RIP u routerů 2 a 3
5. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
6. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
7. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

4.3.16. Quality of Service (QoS) – objasnění pojmů

QoS je pro telefonii a podobné přenosy důležitým ukazatelem. Umožňuje administrátorům sítě konfigurovat jednotlivé routery tak, aby byly splněny požadavky pro přenos zvuku či videa v reálném čase.

Značky QoS se liší podle typu sítě (domény):

- **ToS sítě**: ToS bity v hlavičce IP paketu
- **VLAN**: prioritní bity v hlavičce VLAN
- **DSCP**: používá se pouze 5 bitů CoS
- **WLAN**: WLAN QoS hlavička

Celkový rámec QoS je přitom dodržen pro všechny typy sítí. Kontinuita a předávání požadavků je zajištěno následujícím způsobem: pro přenos QoS požadavků je vybrána **CoS** (Class of Service – třída služby) jako zastřešující jazyk. Router/most (RG) má úplnou kontrolu nad paketem po celou dobu jeho průchodu ze vstupu na výstup. Požadavek na QoS (vyjádřen podle typu příchozí sítě ToS bity, priorit. bity apod.) je na vstupu přeložen do formátu **CoS** a naopak při výstupu paketu je přeložen do formátu srozumitelného pro odchozí síť.

CoS obsahuje 6 priorit (v sestupném pořadí)

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

Pravidla provozu:

1. **CoS1** má absolutní přednost a používá se pro spěšný provoz (expedited forwarding – EF). Priorita je dodržena až do okamžiku doručení.
2. **CoS2 – CoS5** jsou používány pro zaručené doručení (assured forwarding – AF). Pokud se jich sejde více naráz, jsou jejich fronty cyklicky obsluhovány podle váhy jejich priorit:

   CoS2 > CoS3 > CoS4 > CoS5
3. **CoS6** je značka pro přenos s minimálním vypětím (best effort – BE). Je obsloužen až když není žádná vyšší třída na řadě. Pokud na routeru/mostu (RG) není aktivováno QoS, všechen provoz bude považován za BE.

Další pojmy:

- **Ingress** (příchozí) – Pakety příchozí z LAN nebo WAN rozhraní.
- **Egress** (odchozí) – Pakety vyslané od RG k LAN nebo WAN
- **Trusted Mode** (režim důvěry) – uznává QoS (označenou podle typu sítě)
- **Untruted Mode** (režim nedůvěry) – neuznává požadavky na QoS. Výchozí nastavení.
- **Traffic Conditioning Agreement** (TCA – souhlas s podmínkami) – musí být definován pro každé rozhraní
  - Ingress mapping (převod doménových QoS značek na CoS)
  - Egress mapping (převod CoS na doménové QoS značky)
  - Výchozí volba pro všechna rozhraní je režim nedůvěry (Untrusted)
- **Shaper** (lazení provozu)

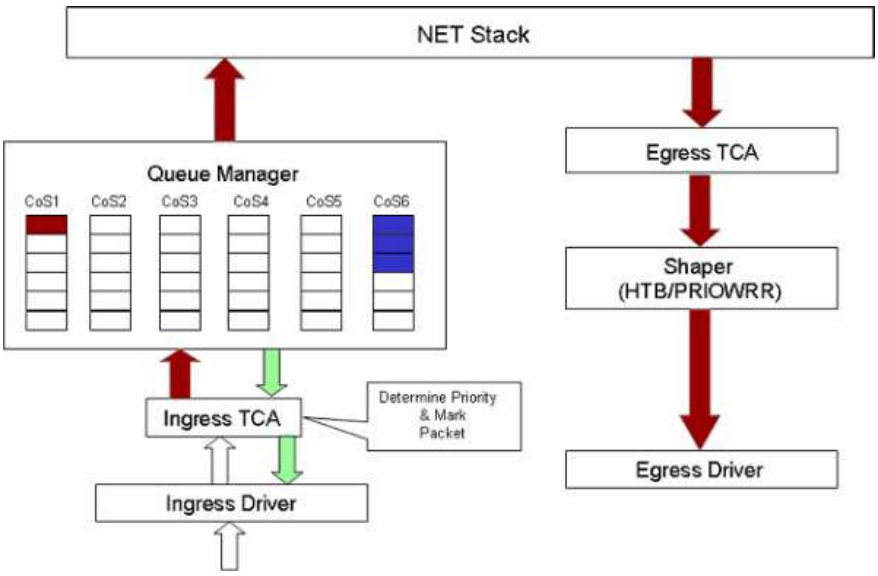


Schéma toku QoS routeru

Pro konfiguraci QoS jsou k dispozici čtyři webové stránky:

- **Ingress** – Zde se nastavuje překlad hodnocení QoS paketů příchozích z jednotlivých typů domén na jednotný CoS. Více v kapitole „Ingrees – Příchozí QoS"
- **Egress** – Zde se nastavuje zpětný překlad z formátu CoS na formát odchozí domény. Více v kapitole „Egrees – Odchozí QoS"
- **Shaper** – Na této stránce se definují pravidla a přiřazení šířky pásma pro jednotlivé třídy CoS. Více v kapitole „Shaper – Lazení provozu"
- **Policy Routing (PR)** – Politika routování se uplatní v případě konfigurace QoS pro vícenásobné WAN připojení. Dále je zde možno klasifikovat pakety na základě testování různých obsažených bytů. Více informací je v kapitolách „Policy Routing" a „Ingrees Payload Database"

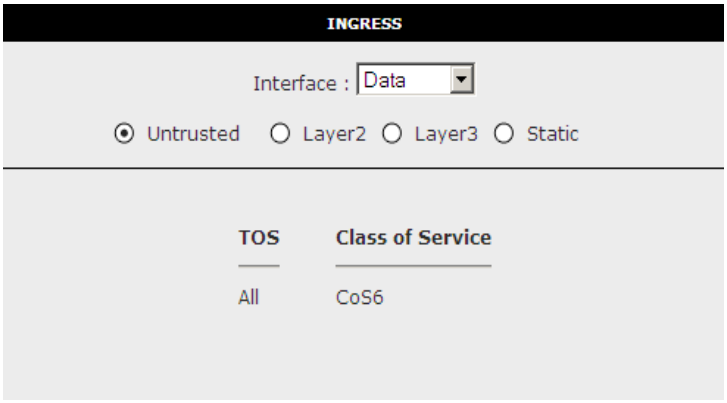
Poznámka – Koncový uživatel by neměl do stránek QoS a Policy Routing **vůbec zasahovat**; jsou určeny pouze servisním a vývojovým pracovníkům!

4.3.17. ADVANCED – Ingrees

Na stránce Ingress můžete konfigurovat QoS pro příchozí pakety hned na vstupu. Přístup je ze stránky **Advanced ⇨ Ingress**. QoS označené podle příchozí domény je převedeno na formát CoS. Jsou k dispozici čtyři režimy:

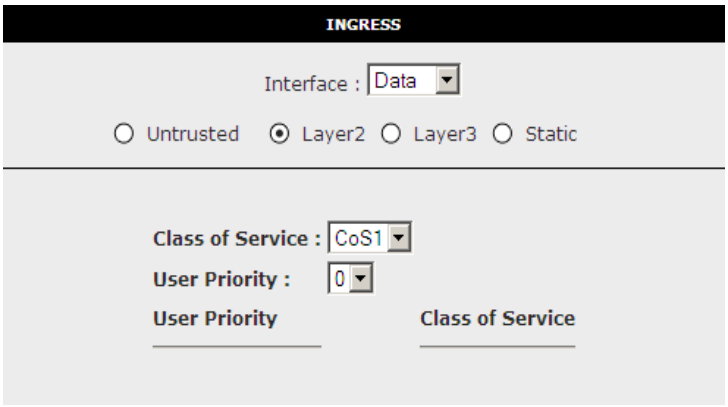
Ingress Untrusted – bez důvěry

Je to výchozí mód pro všechna rozhraní. V tomto případě je příchozí označení požadované QoS ignorováno a všechny pakety jsou označeny jako CoS6 (nejnižší priorita).



Ingress Layer 2

V režimu Layer 2 jsou do univerzálního CoS překládány značky sítě VLAN (platí pro příchozí pakety). Tento režim lze nastavit pouze pro WAN, neboť v současné verzi softwaru je síť typu VLAN podporována pouze na straně WAN.



Tabulka 16 Parametry pro Ingress – Layer 2

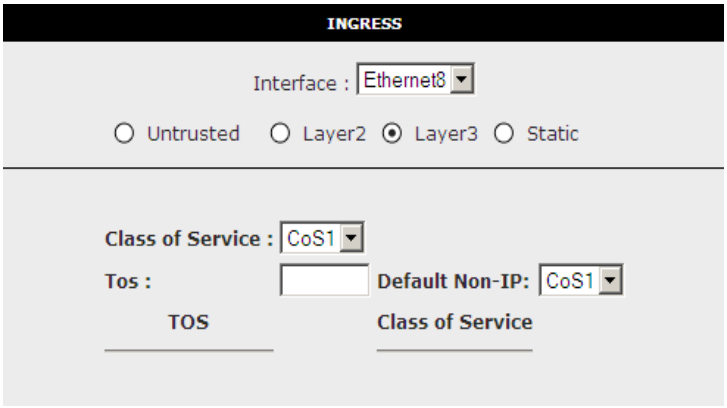
Pole	Překlad	Popis
Interface		Zvolte WAN připojení, pro které chcete konfigurovat. Síť VLAN je současnosti podporována pouze jako WAN.
Class of Service	Třída služby	V sestupném pořadí podle priority: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*
User Priority	Uživatelská priorita	Možnosti jsou: *0,1,2,3,4,5,6,7*

Postup při nastavení překladu (prioritní bity ⇨ CoS) Ingress-Layer 2:

1. V seznamu Interface zvolte *PPPoE1*.
2. V seznamu **Class of Service** zvolte *CoS1* a v seznamu **Priority Bits** zvolte *5*
   Příchozí pakety s prioritou 5 budou označeny jako CoS1 (tj. s nejvyšší prioritou, normálně vyhrazenou pro telefonii)
3. Nastavení odešlete kliknutím na **Apply**.
4. Dále zvolte CoS2 a k němu prioritu 1.
   Příchozí pakety s prioritou *1* jsou označeny jako *CoS1* (tj. s druhou nejvyšší prioritou, normálně vyhrazenou pro video a podobně)
5. Nastavení odešlete kliknutím na **Apply**.
6. Další pravidla přidáte podobným způsobem.
   Lze vytvořit až osm pravidel
   Poznámka – Prioritní bity, které nebudou přiřazeny k žádnému stupní CoS, dostanou CoS6 (nejnižší prioritu)
7. Údaje formuláře odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny..
8. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
9. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Ingress Layer 3

V režimu Layer 3 jsou do univerzálního CoS překládány značky ToS paketů příchozích z IP sítě. Lze nastavit pro přípojení LAN nebo WAN.



Tabulka 17 Parametry pro Ingress –Layer 3

Pole	Překlad	Popis
Interface		Zvolte WAN nebo LAN připojení, pro které chcete konfigurovat. Síť typu IP (Layer 3) je podporována pro obojí.
Class of Service	Třída služby	V sestupném pořadí podle priority: *CoS1*, *CoS2*, *CoS3*, *CoS4*, *CoS5*, *CoS6*
ToS	Typ služby	Typ služby může nabývat hodnot *0-255*
Default Non IP	CoS pro pakety bez IP hlavičky	Pakety bez IP hlavičky jsou např. PPP ovládací pakety a ARP pakety. Doporučená hodnota je CoS1 (nejvyšší priorita)

Postup při nastavení překladu (ToS⇨CoS) Ingress-Layer 3 (příklad pro LAN 1):

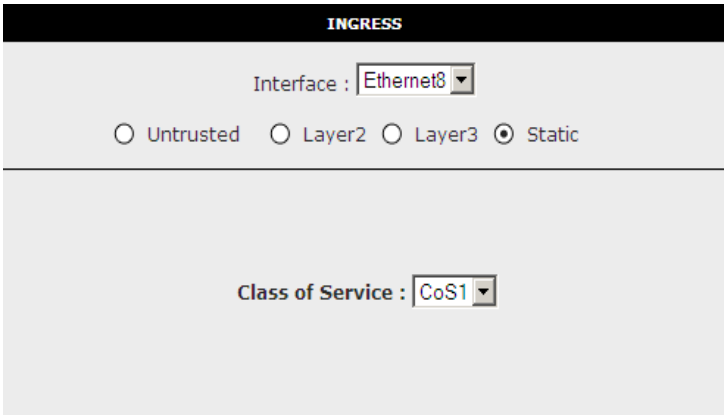
1. V seznamu Interface zvolte *LAN Group 1*.
2. V seznamu **Class of Service** zvolte *CoS1* a v seznamu **Type of Service** zvolte *22.*
3. Pakety příchozí z LAN 1 (IP – layer 3) s ToS = 22 budou označeny jako CoS1 (tj. s nejvyšší prioritou, normálně vyhrazenou pro telefonii)
4. Nastavení odešlete kliknutím na **Apply**.
5. V poli Default Non IP ponechte hodnotu CoS1.
6. Pakety příchozí z LAN 1 (IP – layer 3) bez IP hlavičky získají prioritu CoS1 (tj. nejvyšší)
7. Nastavení odešlete kliknutím na **Apply**.
8. Další pravidla přidáte podobným způsobem.
   Lze vytvořit až 255 pravidel

Poznámka – Značky ToS, které nebudou přiřazeny k žádnému stupni CoS, budou přeloženy jako CoS6 (nejnižší priorita)

9. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
10. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
11. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Ingress Static

V režimu Static je pro každý příchozí paket (z LAN nebo WAN) přiřazena konstantní hodnota CoS

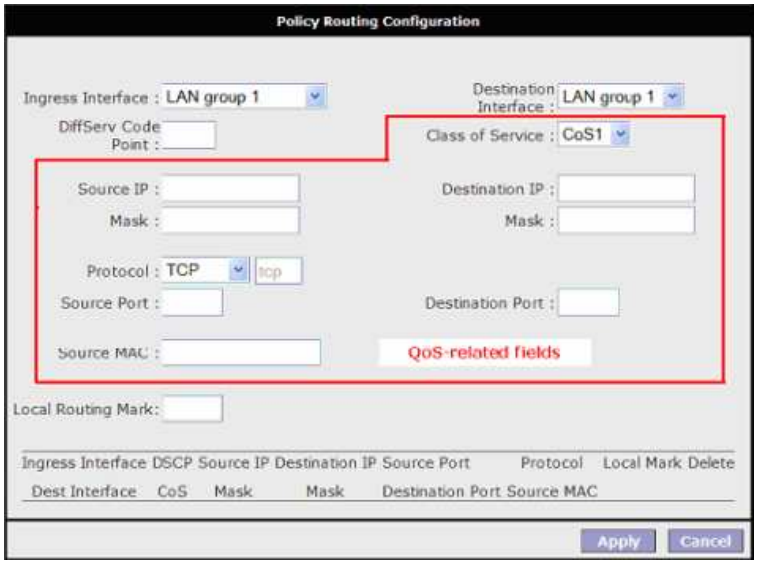


Postup při nastavení konstantní CoS Ingress-Static (příklad pro USB):

1. V seznamu Interface zvolte *USB*.
2. V seznamu **Class of Service** zvolte *CoS1*.
3. Všechen příchozí provoz z USB bude označen jako CoS1 (tj. s nejvyšší prioritou)
4. Údaje odešlete do RG tlačítkem **Apply**. Tím se provedené nastavení dočasně aktivuje. Pokud celou konfiguraci neuložíte (viz dále), budou ovšem zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
5. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
6. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).

Směrování podle vstupní QoS (Ingress Payload Database)

Na stránce **Policy Routing** lze nastavit jednak směrování provozu v závislosti na obsahu hlavičky paketu (**QoS payload database**) a jednak **Policy Routing** (směrování na základě uživatelsky definovaných pravidel). Zde rozebereme **QoS payload** databázi. Politika směrování je ve zvláštní kapitole věnované „Policy Routing".



Přenos požadavků na QoS v závislosti na směru toku lze konfigurovat na stránkách Ingress a Egress. Na stránce **Policy Routing** lze klasifikovat pakety na základě hodnoty některých bitů v hlavičce paketu.

Jedná se o parametry:

- CoS – třída služby
- IP adresa a maska zdroje
- IP adresa a maska cíle
- Protokol
- Zdrojový port
- Cílový port

- MAC adresa zdroje

Podle potřeby lze nastavit pouze jednu nebo více položek.

Tabulka 18 Parametry nastavení QoS policy routing

Pole	Překlad	Popis / Význam
Ingress Interface	Vstupní rozhraní	viz kapitola „**Chyba! Nenalezen zdroj odkazů.**“
Destination Interface	Výstupní rozhraní	viz kapitola „**Chyba! Nenalezen zdroj odkazů.**“
DiffServ Code Point		viz kapitola „**Chyba! Nenalezen zdroj odkazů.**“
Class Of Service	Třída služby	V sestupném pořadí podle priority: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*
Source IP	IP adresa zdroje	
Mask	Maska podsítě zdroje	Pokud nebylo zadáno **Source IP**, není třeba vyplňovat
Destination IP	IP adresa cíle	
Mask	Maska podsítě cíle	Pokud nebylo zadáno **Destination IP**, není třeba vyplňovat
Protocol		Možnosti jsou: *TCP, UDP, ICMP, Specify (specifikujte), none (žádný)*. Při volbě *Specify* zadejte do vedlejšího pole navíc číslo požadovaného protokolu. Spolu s touto položkou je třeba vyplnit aspoň jednu adresu IP nebo MAC Pokud bylo zadáno číslo portu (viz další řádky), je potřeba vyplnit i protokol
Source Port	Port zdroje	Nejdříve je nutno zadat protokol
Destination Port	Port cíle	Nejdříve je nutno zadat protokol
Source MAC	MAC adresa zdroje	
Local Routing Mark		viz kapitola „**Chyba! Nenalezen zdroj odkazů.**“

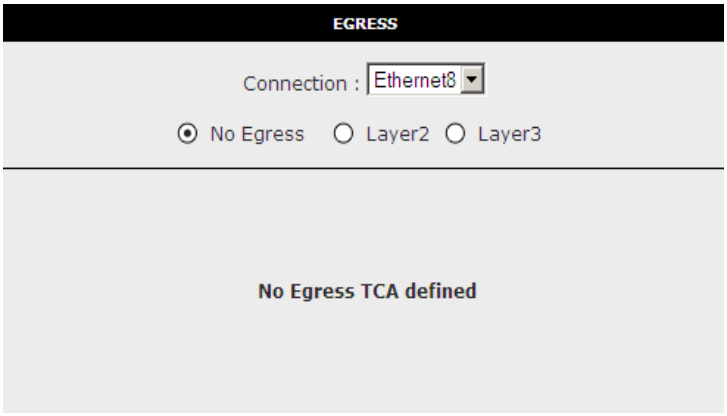
Poznámka – při zadávání IP adres, masek a portů je možno použít hvězdičku * (zastupuje libovolné číslo)

4.3.18. ADVANCED – Egress

Pro pakety odcházející z routeru je potřeba značku CoS přeložit do formátu, jemuž odchozí síť (doména) rozumí. Nastavení překladu je na stránkách Egress.

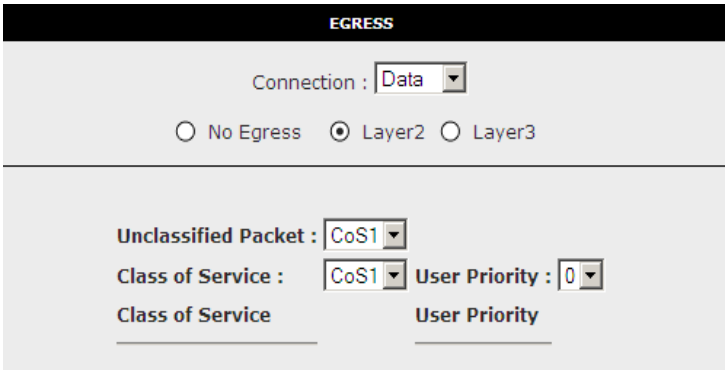
No Egress Mode

Výchozí nastavení pro odchozí provoz je *No Egress* – překlad z *CoS* se neprovádí a značky pro doménu zůstávají nedotčeny.



Egress Layer 2

V režimu Egress Layer 2 je prováděn převod značek CoS na prioritní bity – tuto značku uznávají sítě VLAN. VLAN je v současné verzi podporována pouze pro WAN rozhraní.

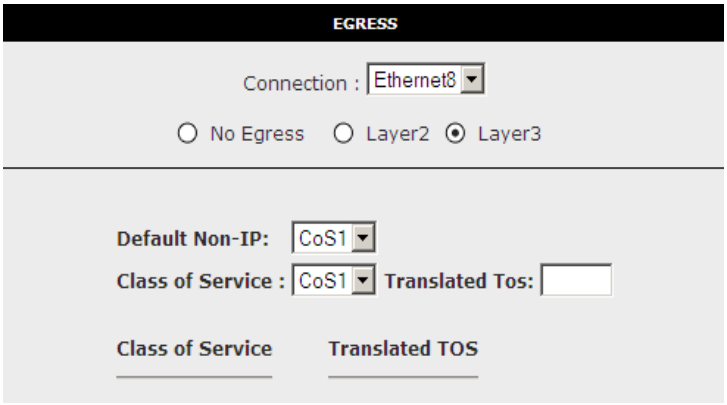


Tabulka 19 Parametry pro Egress Layer 2

Pole	Překlad	Popis / Význam
Interface	Rozhraní	Vyberte WAN rozhraní, pro nějž má konfigurace platit. VLAN jsou podporovány v současnosti pouze pro WAN
Unclassified Packet	Nezařazený paket bez CoS	Některé místně generované pakety (např. PPP control, ARP) neobsahují hodnotu CoS. V tomto případě dostanou přidělenou zde uvedenou hodnotu: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*. Doporučené nastavení je *CoS1* (max. priorita)
User Priority	Odchozí priorita	Možnosti: *0,1,2,3,4,5,6,7*
Class of Service	Třída služby	V sestupném pořadí podle priority: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*.

Egress Layer 3

Zde je možno nastavit překlad CoS do ToS; tato značka je přenášena v IP sítích.



Tabulka 20 Parametry nastavení Egress – Layer 3

Pole	Překlad	Popis / Význam
Interface	Rozhraní	Odchozí rozhraní, pro nějž má konfigurace platit
Defult Non-IP	Nezařazený paket bez CoS	Některé místně generované pakety (např. PPP control, ARP) neobsahují hodnotu CoS. V tomto případě dostanou přidělenou zde uvedenou hodnotu: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*. Doporučené nastavení je *CoS1* (max. priorita)
Translated ToS	Přeložené ToS	Nabývá hodnoty *0-255*
Class of Service	Třída služby	V sestupném pořadí podle priority: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6*.

Podpora WLAN Egress

QoS pro odchozí provoz z WLAN (WLAN Egress) je sice podporován, je však pevně kódován a nelze jej uživatelsky konfigurovat. Více informací je v následující kapitole „

Podpora QoS v sítích **WLAN**".

Podpora QoS v sítích WLAN

QoS pro provoz v sítích WLAN je sice podporován, je však pevně kódován a nelze jej konfigurovat.

V následující tabulce je uveden seznam hodnot, které příslušejí QoS v WLAN.

Tabulka 21

Vlastní priorita	CoS (Třída služeb)	Priorita WME	DSCP
0 (min. úsilí)	CoS5	0	0 (0x00)
1 (na pozadí)	CoS6	1	8 (0x20)
2 (na pozadí)	CoS6	2	16 (0x40)
3 (min. úsilí)	CoS5	3	24 (0x60)
4 (video)	CoS2	4	32 (0x80)
5 (video)	CoS2	5	40 (0xA0)
6 (hlas)	CoS1	6	48 (0xC0)
7 (hlas)	CoS1	7	56 (0xE0)

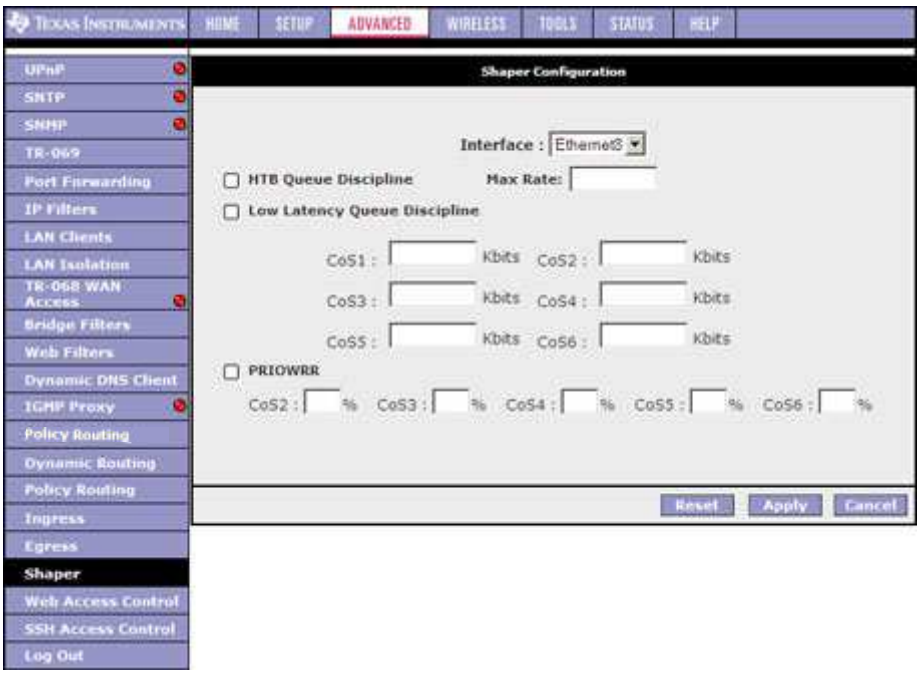
Shaper není pro WLAN podporován.

4.3.19. ADVANCED – Shaper

Blok Shaper podporuje algoritmy:

- HTB – Hierachical Token Bucket Queue Discipline
- Low Latency Queue Discipline
- PRIOWRR

Poznámka – Má-li být konfigurován shaper pro TCA, je nejdříve potřeba definovat Egress TCA.



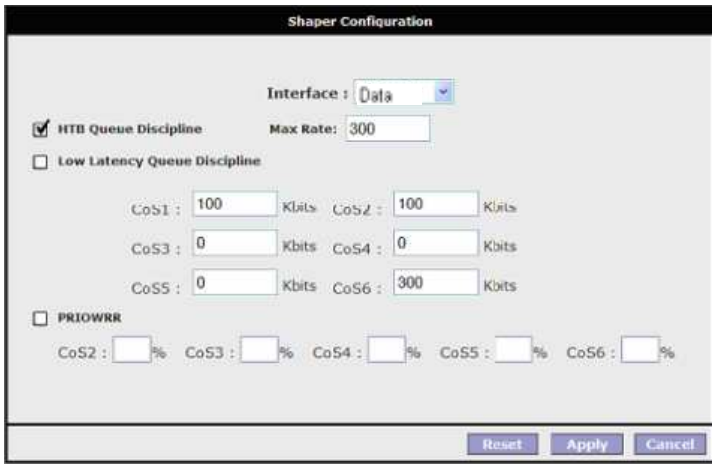
Tabuka 22 Parametry nastavení shaperu

Pole	Překlad	Popis / Význam
Interface	Rozhraní	Nelze zvolit WLAN, neboť není podporováno
Max Rate	Max rychlost odesílání	Toto pole platí pro algoritmy HTB a Low Latency... , oba algoritmy pracují na základě rychlostí
HTB Queue Discipline		HTB je algoritmus založený na rozdílných rychlostech vysílání , v závislosti na prioritě. Každému stupni CoS je přiřazena určitá rychlost odesílání. Například CoS1 je konfigurováno jako 100Kbps, takže i když shaper přijme do své fronty data rychlostí 300Kbps, bude je odesílat pouze 100Kbps.
Low Latency Queue Discipline		Tento algoritmus je podobný předchozímu, kromě toho, že rychlost pro třídu CoS1 není omezena. Ve výše uvedeném příkladu by tedy data byla odeslána plnou rychlostí 300 Kbps. Nevýhodou je, že neukázněný tok dat může zahltit celu šířku pásma
PRIOWRR		Tento algoritmus pracuje na principu priority – fronty CoS2-6 jsou cyklicky obsluhovány, každá podle své prioritní váhy. Fronta CoS1 má nejvyšší prioritu a není nijak zdržována.

Ze tří dostupných algoritmů může být aktivní pouze jeden. Příklady pro jednotlivé volby:

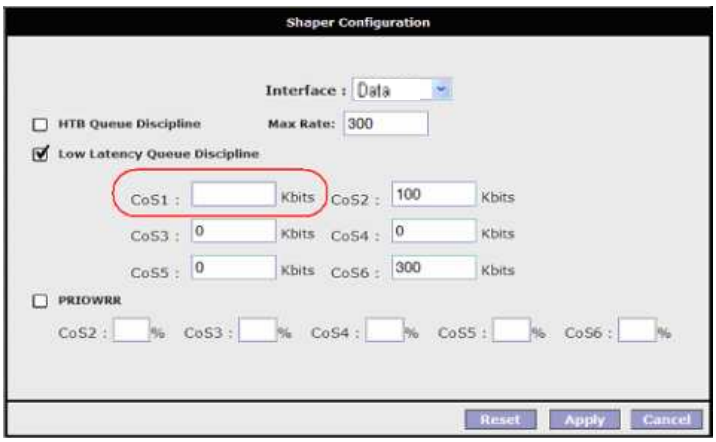
Příklad 1 : HTB

V příkladu na obrázku má připojení PPPoE1 vyhrazeno pásmo 300Kbps, z něhož 100Kbps je pro CoS1 a dalších 100Kbps pro CoS2. Pokud jsou fronty CoS1 a 2 prázdné, CoS6 má pro sebe celé pásmo 300Kbps.



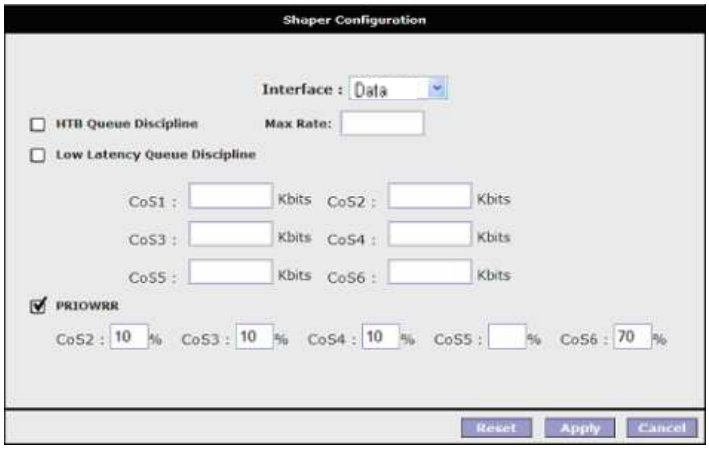
Příklad 2: Algoritmus Low Latency Queue Discipline

V tomto příkladu CoS1 nemá žádné omezení (jeho pole je neaktivní), CoS2 má vyhrazeno 100Kbps (pokud nečekají žádné CoS1). CoS6 má pro sebe celých 300Kbps, pokud nejsou žádné CoS1 ani CoS2. Je to podobné, jako předchozí příklad s algoritmem HTB, kromě toho, že CoS1 není nijak omezeno.



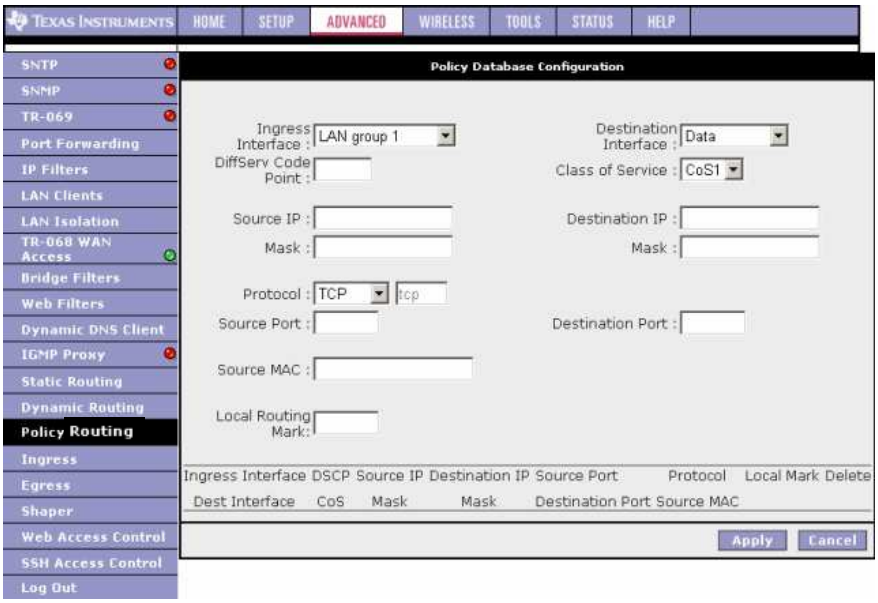
Příklad 3: PRIOWRR

Algoritmus PRIOWRR se rozhoduje na základě priority paketů a podle ní vyšle určitý počet; nepracuje s proměnnou rychlostí, proto je pole Max Rate neaktivní. Každé třídě je přiřazena určitá váha v procentech, kromě třídy CoS1, která má absolutní přednost. Pokud ve frontě nečekají žádné CoS1, CoS2 až 4 mají po 10 procentech a CoS6 70 procent. Je to podobné uspořádání jako pro Low Latency Queue, až na to, že PRIOWRR je na bázi prioritní váhy a LLQ je na bázi rychlosti vysílání.



4.3.20. ADVANCED – Policy Routing

Nastavení politiky směrování je na společné stránce s nastavením směrováním podle QoS. QoS již bylo popsáno v kapitole „**Směrování podle vstupní QoS (Ingress Payload Database)**", zde rozebereme politiku směrování (směrování podle uživatelsky nastavených pravidel – např. podle lokality cíle).



Tabulka 23 Parametry nastavení policy routing

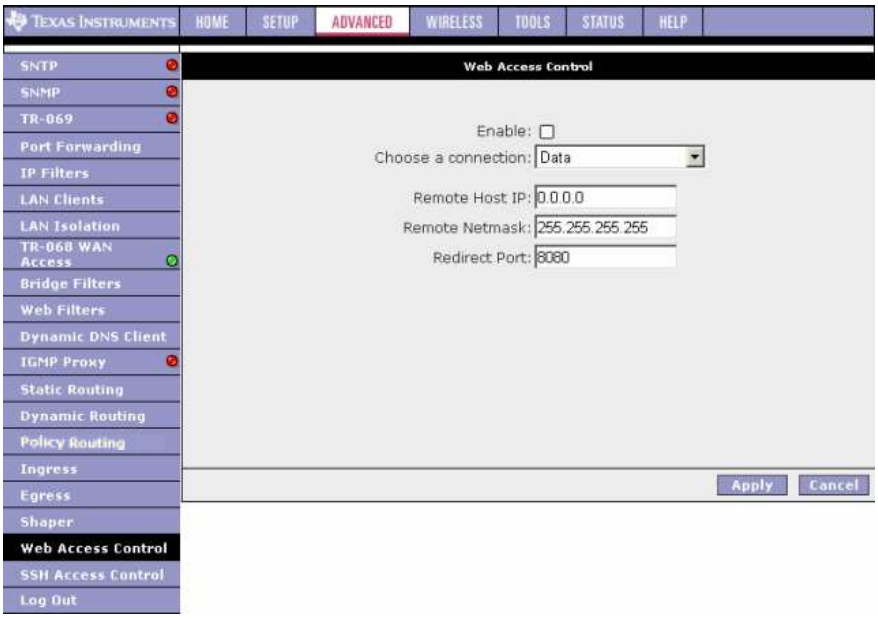
Pole	Překlad	Popis
Ingress Interface	Příchozí rozhraní	Možnosti: *LAN, WAN, Locally generated(traffic) (=místně generované), not applicable (nedostupné).* Lokálně generovaný provoz je například hlasové pakety, pakety z místních DNS, DHCP apod.
Destination Interface	Cílové rozhraní	Možnosti: *LAN...* nebo *WAN...*
DiffServ Code Point		Hodnota: *0-255*. Toto pole musí být konfigurováno spolu s minimálně jedním z **IP**, **MAC** nebo **Ingress Interface**.
Class of Service	Třída služby	Možnosti: *CoS1 - CoS6*
Source IP	IP adresa zdroje provozu	
Mask	Maska zdroje	Pokud je zadána IP, nutno vyplnit
Destination IP	IP adresa cíle	
Mask	Maska cíle	Pokud je zadána IP, nutno vyplnit
Protocol		Možnosti jsou: *TCP, UDP, ICMP, Specify (specifikujte), none (žádný)*. Při volbě *Specify* zadejte do vedlejšího pole navíc číslo požadovaného protokolu. Spolu s touto položkou je třeba vyplnit aspoň jednu adresu **IP**, **MAC** nebo **Ingress Interface** Pokud bylo zadáno číslo portu (viz další řádky), je potřeba vyplnit i protokol
Source Port	Port zdroje	Nejdříve je nutno zadat protokol
Destination Port	Port cíle	Nejdříve je nutno zadat protokol

Source MAC	MAC adresa zdroje	
Local Routing Mark		Toto pole je aktivní pouze pro volbu **Ingress Interface** = *Locally Generated* . Značky pro DNS provoz generované některými aplikacemi: • Dynamic DNS: 0xE1 • Dynamic Proxy: 0xE2 • Web Server: 0xE3 • MSNTP: 0xE4 • DHCP Server: 0xE5 • IPtables Utility: 0xE6 • PPP Deamon: 0xE7 • IP Route: 0xE8 • ATM Library: 0xE9 • NET Tools: 0xEA • RIP: 0xEB • RIP v2: 0xEC • UPNP: 0xEE • Busybox Utility: 0xEF • Configuration Manager: 0xF0 • DropBear Utility: 0xF1 • Voice: 0

Poznámka – při zadávání IP adres, masek a portů je možno použít hvězdičku * (zastupuje libovolné číslo)

4.3.21. ADVANCED – Web Access Control

Zde můžete nastavit práva pro vzdálený přístup na straně WAN.



Chcete-li například získat přístup ke své domácí RG ze vzdáleného počítače v kanceláři, postupujte následujícím způsobem:

1. Zaškrtněte **Enable**.
2. Položku výběru připojení **Choose a Connection** ponechte nastavenou na WAN.
3. Do pole **Remote Host IP** zadejte IP adresu vzdáleného počítače, ze kterého se budete připojovat (např. 10.10.10.1).
4. Zadejte masku podsítě **Remote Netmask.**
5. Zadejte číslo portu, kterým se budete připojovat **Redirect Port** (např. 80)
6. Údaje odešlete kliknutím na **Apply**.
   Zadaná WAN adresa byla přidána do seznamu **IP Access List.**
   Pokud celou konfiguraci neuložíte (viz dále), budou zadané údaje při nejbližším vypnutí / rebootování RG ztraceny.
7. Změny trvale uložíte v oddíle **Tools** (horní tlačítková lišta) – **System Commands**.
8. Na stránce **System Commands** klikněte na **Save All** (Uložit vše).
9. Pro přístup k RG ze vzdáleného počítače (10.10.10.1) zadejte do adresového řádku v prohlížeči URL (příklad):
   http://10.10.20.5:80 nebo *https://10.10.20.5:80*
   Syntaxe: http(s)://<**WAN IP adresa RG**>:<**port**>

Tabulka 24 Parametry nastavení vzdáleného přístupu

Pole	Překlad	Popis / Význam
Enable	Zapnout	
Choose a connection	Zvolte připojení	WAN připojení, přes které má probíhat vzdálený přístup
Remote Host IP	IP adresa vzdáleného počítače	
Remote Netmask	Maska podsítě	
Redirect Port	Připojit přes port	Zde můžete zvolit jiné číslo portu než obecně užívaný IP port 80. Toto číslo pak zadáváte v rámci cílové adresy, uvnitř RG je pak namapováno zpět na port 80.

4.3.22. ADVANCED – SSH Access Control

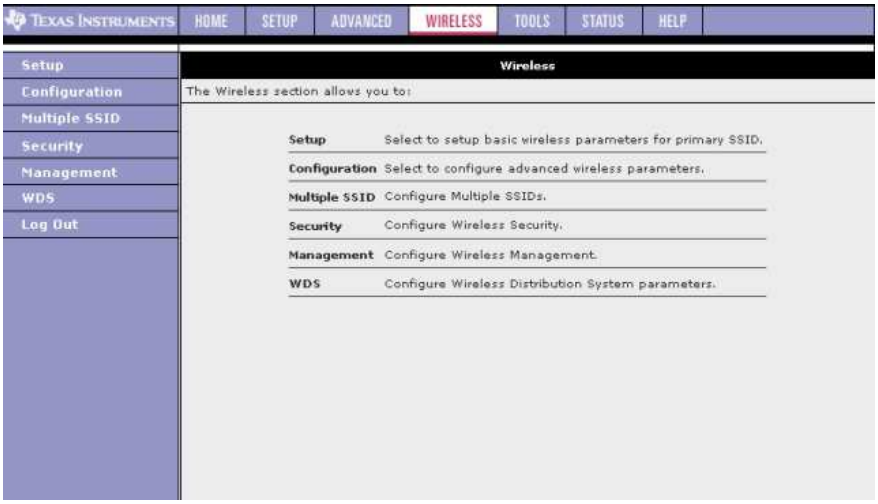
Zde můžete založit účet pro vzdáleného správce, přistupujícího zabezpečeným telnetem (protokol SSH).

Konfigurace SSH přístupu je velmi podobná jako v předchozí kapitole (Web Access Control).

4.4. WIRELESS

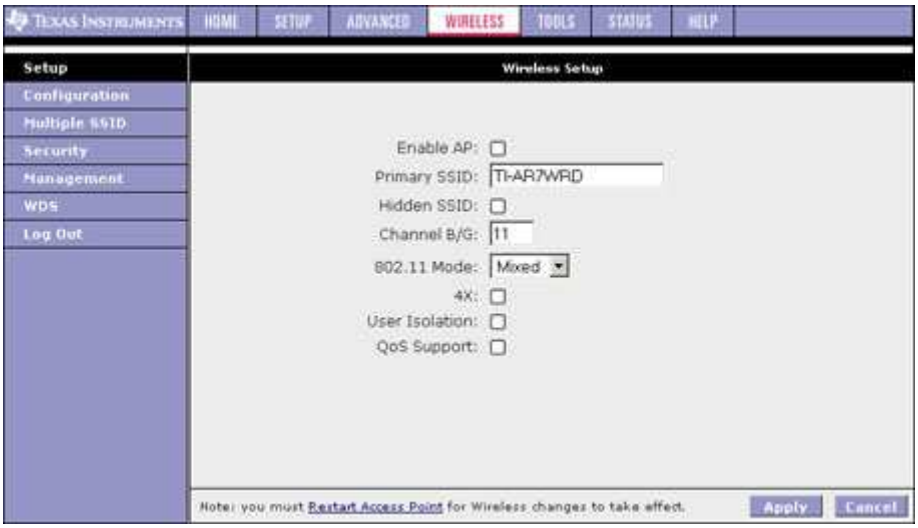
Po kliknutí na **Wireless** v horní tlačítkové liště se zobrazí hlavní stránka konfigurace bezdrátového připojení **Wireless**. V levém sloupci se nacházejí odkazy na jednotlivé oddíly:

- Setup
- Configuration
- Multiple SSID – vícenásobné SSID
- Security - zabezpečení
- Management - správa
- WDS
- Log Out - odhlášení



4.4.1. WIRELESS – Setup

Zde se nastavují základní parametry bezdrátového přístupového bodu (AP).



Tabulka 1 Parametry nastavení přístupového bodu (AP)

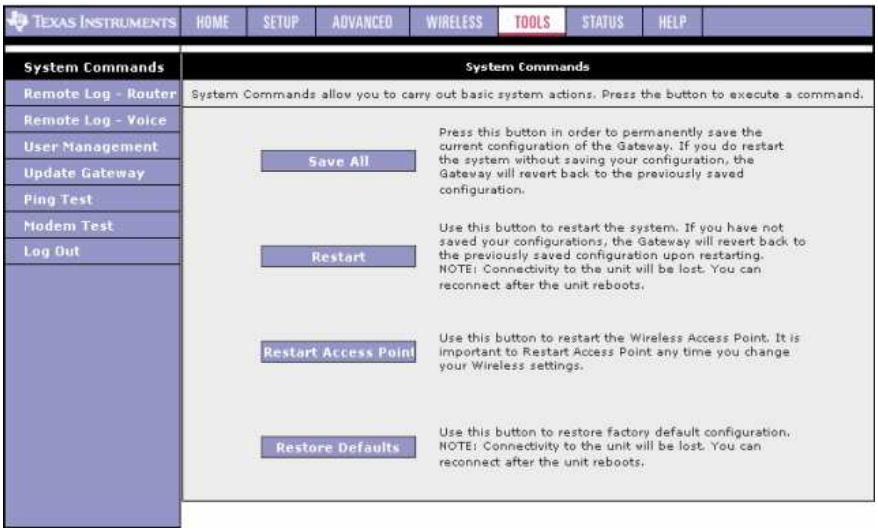
Pole	Překlad	Popis
Enable AP	Zapnout bezdrátový přístupový bod	Defaultně je AP vypnut.
Primary SSID	Primární SSID	Primární SSID jediným SSID, který je přístupovým bodem rozesílán v rámci beaconu. Přednastavený SSID je *default*, můžete ho změnit podle libosti. Max. délka je 32 znaků
Hidden SSID	Skrytý SSID	Enabled = identifikátor není rozesílán jako součást beaconu, takže WLAN zůstane cizím stanicím skryta.

VLAN ID		Platí pro primární SSID. Výchozí nastavení: vícenásobné SSID je vypnuto a VLAN pro primární SSID je 0. Pokud zapnete vícenásobné SSID, budete vyzváni ke změně VLAN ID primární SSID. Hodnota může být v rozsahu 0-4095. Více informací v kapitole „**Chyba! Nenalezen zdroj odkazů.**“
Channel B/G	Kanál B/G	Kanál, na kterém přístupový bod a stanice komunikují. Počet kanálů závisí na vysílacím pásmu. Pro FCC na 2.4 GHz je výchozí kanál 11.
802.11 Mode		Jsou k dispozici následující režimy: • **Mixed mode** (smíšený) – Jsou podporovány oba 802.11g / b. • **11b only Mode** (pouze 11b) • **11b+ Mode** – podobný jako 11b, navíc je zahrnuta PBCC modulace 22Mbps (patent TI) • **11g only Mode** – (pouze 11g).
4x		Zapnutí funkce 4x – patent TI, lze použít pouze, jsou-li připojené bezdrátové stanice také výrobkem TI
User Isolation	Vzájemná zolace stanic	Po zaškrtnutí bude zamezeno přímé komunikaci mezi jednotlivými stanicemi.
QoS Support	Podpora QoS	Viz kapitola „ Podpora QoS v sítích WLAN

4.4.1.1. Postup uložení WLAN nastavení

Upozornění – tlačítko **Apply** slouží k odeslání údajů z formuláře do routeru. Zde zůstanou pouze do vypnutí nebo resetování routeru. Pro trvalé uložení do Flash paměti je potřeba:

1. Kliknout na **Apply.**
2. Kliknout na **Restart Access Point** v dolní části stránky, přesunete se na stránku **System Commands**

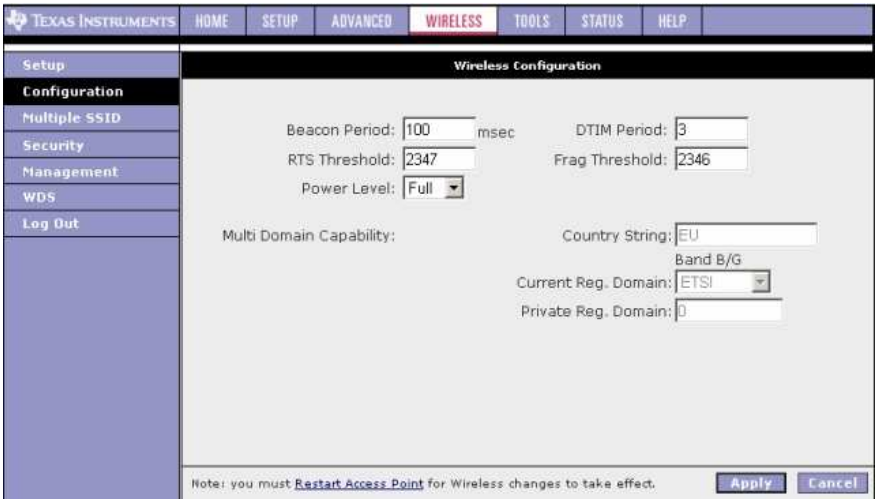


Poznámka – Odkaz na stránku **System Commands** se nachází také na stránce **Tools** (přístup přes horní tlačítkovou lištu)

3. Na stránce **System Commands** klikněte na **Save All** (Uložit vše)
4. Ještě je potřeba restartovat bezdrátový modul, aby pracoval s novou konfigurací.
5. Klikněte na **Restart Access Point**. Modul se restartuje s novým nastavením.

4.4.2. WIRELESS – Configuration

Stránka konfigurace popisuje, jak nakonfigurovat funkce bezdrátového spojení ADSL2/2+ routeru.

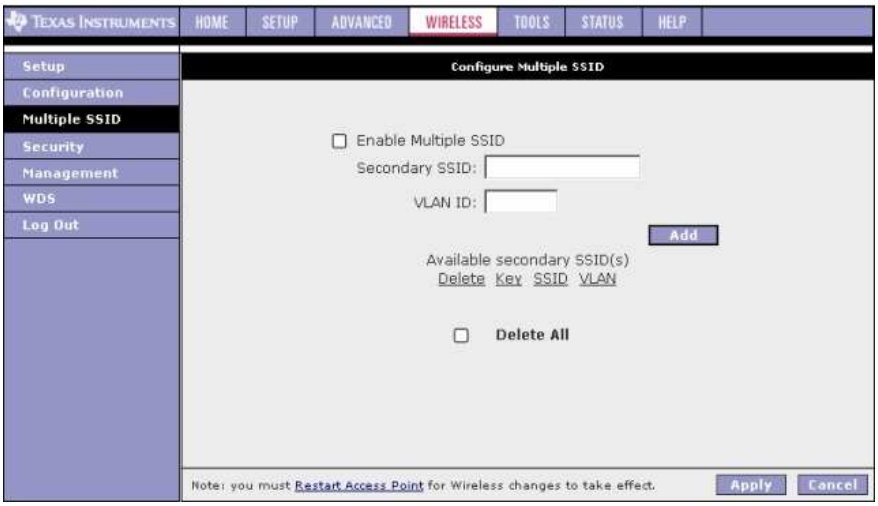


Tabulka 2 Parametry pokročilého nastavení WLAN

Pole	Popis
Beacon Period	Perioda vysílání beacon rámce, v rozsahu *0 – 65535* ms. Výchozí hodnota je *200* ms
DTIM period	DTIM (Delivery traffic identification map period) – počet period beaconu, které budou vyslány před odesláním dat určených pro stanice nacházející se v režimu nízké spotřeby. Výchozí hodnota je 2
RTS threshold	RTS (Request to send) práh – je-li počet bytů v datové jednotce MPDU (Mac protocol data unit) nižší, než RTS threshold, RTS/CTS handshake nebude spuštěn. Výchozí hodnota je 2347, je-li však zapnuta funkce 4x, bude změněna na 4096
Fragmentation Threshold	Rámce s touto a větší délkou budou fragmentovány. Výchozí hodnota je 23476, je-li však zapnuta funkce 4x, bude změněna na 4096
Power Level	Úroveň výstupního vysílacího výkonu v procentech z maxima: *full* (plný), *75%, 50%, 25%, 6%*
Multi Domain Capbility	Tuto funkci lze nastavit pouze na skryté stránce. Koncový uživatel by do ni neměl zasahovat
Country String	Tuto funkci lze nastavit pouze na skryté stránce. Koncový uživatel by do ni neměl zasahovat
Current Reg. Domain	Tuto funkci lze nastavit pouze na skryté stránce. Koncový uživatel by do ni neměl zasahovat
Private Reg. Domain	Tuto funkci lze nastavit pouze na skryté stránce. Koncový uživatel by do ni neměl zasahovat

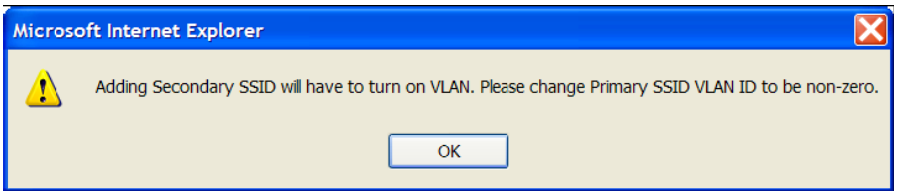
4.4.3. WIRELESS – Multiple SSID

Zde můžete vytvořit dva typy SSID (primární a sekundární) a oddělit tak jednotlivé režimy bezdrátového provozu. Funkce Multiple SSID je ve výchozí konfiguraci vypnuta.



Postup:

1. Zaškrtněte **Enable Multiple SSID**
2. Vyplňte pole:
3. Secondary SSID
4. VLAN ID
5. Odešlete kliknutím na **Add**.
6. Vyskočí upozornění „Změňte VLAN ID primární SSID na nenulovou hodnotu"



7. Potvrďte **OK**. Sekundární SSID se zobrazí ve výpisu v dolní části stránky

8. Přejděte na stránku **Wireless - Setup**, zde změňte **VLAN ID** na nenulové číslo (1-4095)
9. Pokud chcete více sekundárních SSID, postup opakujte
   Lze přidat max. 3 sekundární SSID (celkem 4 včetně primární SSID)
   SSID můžete smazat zaškrtnutím jejího políčka (**Delete All** označí všechny) a kliknutím na **Delete**.
10. Po smazání všech sekundárních SSID je QoS pro WLAN vypnuto a VLAN ID primárního SSID je nastaveno na 0
11. Uložení nastavení viz kapitola „Postup uložení WLAN nastavení".

Tabulka 3 Parametry pro vícenásobné SSID

Pole	Popis
Enable Multiple SSID	Zapíná vícenásobné SSID
Secondar SSID	Identifikátor, max. 32 znaků
VLAN ID	Hodnota 1-4095. Více v kapitole „Postup uložení WLAN nastavení“.

4.4.4. WIRELESS – Security

Můžete nastavit následující způsoby šifrování provozu:

- None (žádné)
- WEP (Wired equivalent privacy = „stejná bezpečnost, jako pro kabelové sítě“)
- 802.1x - umožní připojení stanic se standardem 802.1x
- WPA (Wi-Fi protected access – zabezpečený přístup)
- WPA2 – aktivuje se na stránce WPA

Máte-li aktivováno více SSID, můžete nastavit zabezpečení pro každé SSID zvlášť. Existuje několik omezení:

- WEP může být nastavena max. pro jedno SSID
- 802.1x může být nastavena max. pro jedno SSID
- Nelze zapnout WEP současně s 802.1x
- Pokud je zabezpečeno více než jedno SSID, metoda authentizace pro WEP nesmí být Shared (sdílená).

4.4.4.1. WIRELESS – Security – WEP

WEP (Wired Equivalent Privacy): WEP je zabezpečovací protokol pro místní bezdrátové sítě definovaný ve standardu 802.11b. WEP byl původně navržen tak, aby ve své době vzniku poskytoval stejnou úroveň bezpečnosti jako drátové sítě LAN. WEP kóduje vysílaná rádiová data.

Data jsou před odesláním zašifrována podle konstantního klíče. RG podporuje tři délky klíče:

- 64 bit
- 128 bit
- 256 bit

Přijímací stanice musí používat stejný klíč. Klíč je nutno nastavit pro každý přístupový bod (AP) i bezdrátovou kartu (NIC) ručně.

Výchoz nastavení je WEP vypnuto. Postup při aktivaci:

1. Zvolte **SSID**, které chcete šifrovat
2. Zaškrtněte **Enable WEP Wireless Security**
3. Zvolte **Authentication Type**
4. Vyberte délku klíče **Cipher** a zadejte zvolený klíč **Encryption key**.
5. Stejný klíč musí být zadán u ostatních stanic
6. Nastavení uložíte podle kapitoly „Postup uložení WLAN nastavení".

Tabulka 4 Parametry šifrování WEP

Pole	Překlad	Popis
Select SSID and its Security Level	Zvolte SSID a příslušnou úroveň zabezpečení	
Enable WEP Wireless Security	Zapnout šifrování WEP	
Authentication Type	Typ ověřování	Pokud je nastaveno zabezpečení 802.1x nebo WPA, ověřovací algoritmus je vždy *Open* (otevřený). Pro WEP jsou tři možnosti: • *Open* (otevřený, výchozí nastavení) – přístupový bod (AP) naváže spojení s každou stanicí bez ověřování její identity. • *Shared* – Před zahájením komunikace se stanicí musí být na obou stranách zadán stejný, sdílený (shared) klíč WEP • *Both* (obojí) – AP se nejprve pokusí komunikovat s WEP, při neúspěchu se spojí bez ověřování (open)
Encryption Key	Šifrovací klíč	Je možno zadat čtyři různé klíče a přepínat je přepínačem Select. Délka klíče musí odpovídat zvolené délce **Cipher**
WEP Cipher		Zvolená délka klíče

4.4.4.2. WIRELESS – Security – 802.11x

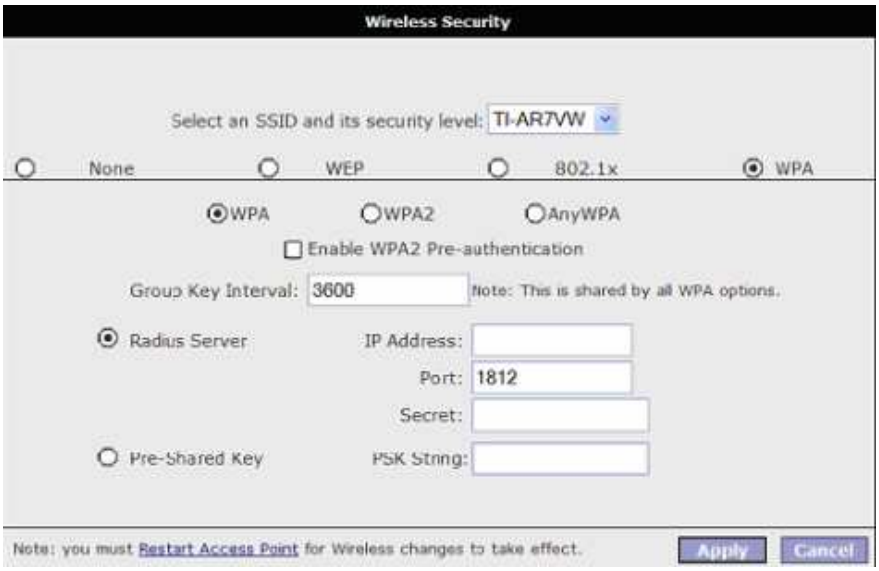
802.1x je bezpečnostní protokol pro WLAN. Ovládá přístup k portům – udržuje síťový port zavřený, dokud neproběhne ověření. 802.1x je založen na rozšířeném ověřovacím protokolu (EAP). Zprávy EAP se obvykle přenášejí protokolem RADIUS (remote authentication dial-in user service).

Tabulka 5 Parametry zabezpečení 802.1x

Pole	Překlad	Popis
Select SSID and its Security Level	Zvolte SSID a příslušnou úroveň zabezpečení	
Server IP Address		IP adresa ověřovacího RADIUS serveru
Port		Port RADIUS serveru
Secret	Klíč	Klíč, sdílený základnovou stanicí (AP) a RADIUS serverem. Max. délka je 63 znaků a číslic
Group Key Interval	Interval rozesílání skupinového klíče	Časový interval, ve kterém bude stanicím 802.1x a WEP vysílán skupinový klíč. Výchozí hodnota je *3600* sekund

4.4.4.3. WIRELESS – Security – WPA

WPA (Wi-Fi Protected Access): WPA je zabezpečovací protokol pro WLAN. Používá sofistikovanou hierarchii klíčů, ze které vždy po navázání spojení stanice se základnou vygeneruje nové klíče. Protokoly WPA, 802.1x, EAP a RADIUS se používají pro vysoký stupeň zabezpečení. Klíče mohou být nadále zadávány ručně jako u WEP (před-sdílený, pre-shared); RADIUS server však generuje klíče automaticky a zajišťuje ověřování pro celou určitou oblast (firmu). WPA používá pro šifrování protokol s dočasným klíčem (TKIP). WPA2, označovaný také jako 802.11i, používá protokol CBC-MAC (AES-CCMP).



Tabulka 6 Parametry nastavení WPA

Pole	Překlad	Popis
Select SSID and its Security Level	Zvolte SSID a příslušnou úroveň zabezpečení	
WPA		Stanice s WPA v.1 se budou moci připojit
WPA2		Stanice s WPA v.2 se budou moci připojit
Any WPA	WPA i WPA2	Stanice s WPA v.2 nebo v.1 se budou moci připojit
Enable WPA2 Pre-authentication		Povoluje předběžnou authentizaci pro WPA2. Lze nastavit pouze, je-li zvoleno **WPA2** nebo **AnyWPA**
Group Key Interval	Interval rozesílání skupinového klíče	Časový interval, ve kterém bude stanicím vysílán skupinový klíč. Výchozí hodnota je *3600* sekund
Radius Server		Je-li zapnuto, stanice WPA budou žádat o authentizaci u RADIUS serveru s použitím protokolu EAP-TLS přes 802.1x
IP Address		IP adresa ověřovacího RADIUS serveru
Port		Port RADIUS serveru
Secret	Klíč	Klíč, sdílený základnovou stanicí (AP) a RADIUS serverem. Max. délka je 63 znaků a číslic
Pre-shared Key		Pokud je zvolen, stanice WPA nežádají o ověření u RADIUS serveru, ale pro komunikaci s AP použijí tento klíč
String	Zadání pre-shared klíče	8-63 alfanumerických znaků

4.4.5. WIRELESS – Management

Na rozdíl od dat přenášených drátěným vedením vaše bezdrátové vysílání proniká i přes Vaše zdi a mohou být zachycena kýmkoliv, kdo má kompatibilní zařízení. Na stránce správy bezdrátového připojení můžete nastavit bezpečnostní prvky podle svých potřeb. Klikněte na **WIRELESS**, pak na **Management**, objeví se následující obrazovka.

4.4.5.1. WIRELESS – Management – Access List

Access List: Původní nastavení umožňuje komukoliv, jehož počítač s bezdrátovým adaptérem je konfigurován se správným jménem sítě nebo SSID, přístup k Vaší bezdrátové síti. Pro zvýšení bezpečnosti můžete omezit přístup do sítě pouze počítačům s určitou MAC adresou.

Můžete vytvořit seznam MAC adres stanic a všem členům tohoto seznamu přístup povolit nebo zakázat. Postup:

1. Klikněte na **Enable Access List**
2. Zvolte **Allow** (povolit), pokud chcete vytvořit seznam s povoleným přístupem, nebo **Ban** (zakázat) pro seznam zakázaných účastníků. Nelze aktivovat oba typy najednou.
3. Zadejte MAC adresu stanice, již chcete přidat do seznamu a odešlete tlačítkem **Apply**.
4. Stanice se zobrazí v seznamu.
5. Postupně přidejte podle potřeby další stanice
6. Uložení nastavení viz kapitola „Postup uložení WLAN nastavení".

4.4.5.2. WIRELESS–Management–Associated Stations

Na této stránce se nachází seznam všech právě připojených bezdrátových stanic. Každé stanici můžete odepřít přístup zaškrtnutím políčka **Ban Station** vedle její MAC adresy. Pokud je aktivován seznam povolených stanic (**Allowed Access**), stanice bude z tohoto seznamu vyjmuta. Je-li naopak aktivován seznam zakázaných stanic (**Banned Access**), stanice bude do tohoto seznamu přidána. Změny je potřeba uložit obvyklým způsobem – viz kapitola „Postup uložení WLAN nastavení".

4.4.6. WIRELESS – WDS

WDS (Wireless distribution system) je systém, který propojuje jednotlivé základnové stanice (BBS) do komplexní, rozlehlé sítě. Síť WDS umožňuje mobilním stanicím volně se přesouvat a stále zůstávat ve spojení s některou základnou.

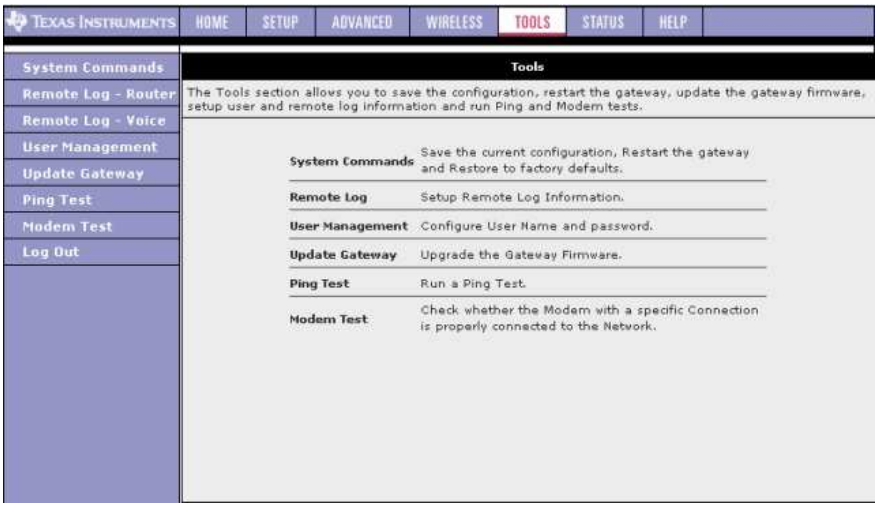
Tabulka 7 Nastavení WDS

Pole	Popis / Význam
WDS Mode	Možnosti: o *Bridge* (přemostění) – v tomto režimu je BSS zapnuta o *Repeater* (opakovač) – AP BSS je vypnuta, jakmile je navázáno spojení s vyšší vrstvou AN o *Crude* – AP BSS je stále zapnuto, vazby mezi jednotlivými AP jsou konfigurovány statickým způsobem a nejsou vzájemně udržovány o *Disabled* (vypnuto, výchozí nastavení) V režimech *Bridge* a *Repater* jsou linky spojující jednotlivé základny (AP) navazovány a udržovány prostřednictvím správcovského protokolu
WDS Name	Název sítě, max. 8 znaků. V jedné oblasti mohou existovat dvě nebo více WDS sítí.
Activate as Root	Je-li zaškrtnuto, stanice je kořenovou stanicí sítě. V jedné sítí WDS nesmí být více kořenových stanic. Nelze použít v režimu *Crude*
WDS Privacy	Používat mezi jednotlivými základnami zabezpečené spojení. Všechny základny musí mít stejné nastavení šifrování. V režimu *Crude* položka není aktivní
Secret	Šifrovací klíč, 32 alfanumerických znaků
Auto Channel Selection	V této verzi není podporováno
Auto Configuration	V této verzi není podporováno
Uplink Connection Check Box	BSS ID nadřazené stanice v hierarchii WDS. Není aktivní, pokud je zařízení konfigurováno jako Root
Downlink Connection Check Boxes	BSS ID podřízené stanice v hierarchii WDS. Lze nastavit až čtyři ID

4.5. TOOLS

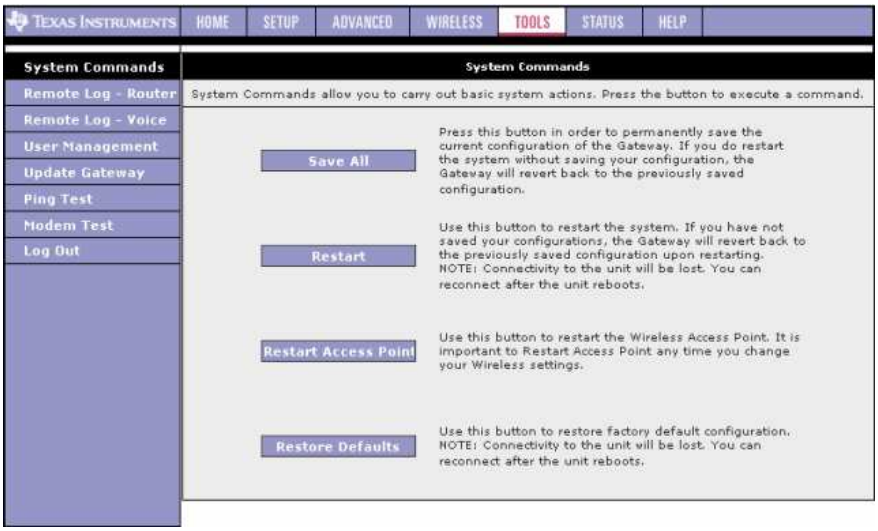
Hlavní stránka nástrojů (**Tools**) je přístupná z horní tlačítkové lišty. V levém sloupci se nacházejí odkazy k jednotlivým nástrojům, v hlavním okně je jejich stručný popis:

- o System Commands – Uložení aktuální konfigurace, restartování systému a návrat k továrním hodnotám nastavení.
- o Remote Log - Router
- o Remote Log - Voice
- o User Management – Změna uživatelského jména a hesla.
- o Update Gateway - Updatování firmware routeru.
- o Ping Test - Spouští ping test.
- o Modem Test - Ověřuje, jestli modem se specifikovaným připojením je správně připojen k síti.



4.5.1. TOOLS – System Commands

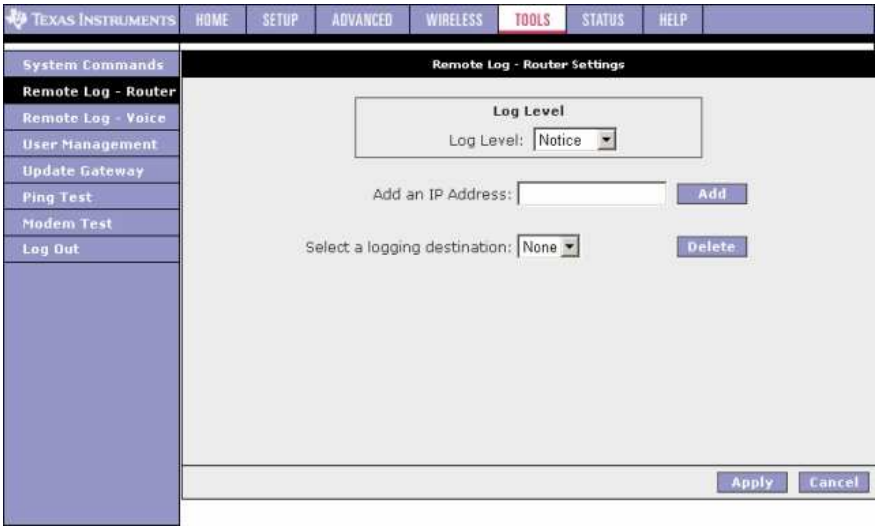
Na této stránce se dají spouštět základní systémové akce.



Pole	Překlad	Popis
Save All	Uložit vše	Uložení aktuální konfigurace do flash paměti
Restart	Restart	Po restartu bude neuložená konfigurace ztracena. Rovněž bude přerušeno spojení; je nutno se znovu přihlásit
Restart Access Point	Restartovat bezdrátový modul	Modul je nutno restartovat po každé změně nastavení, jinak se změna neprojeví
Restore Defaults	Obnovit tovární nastavení	Spojení s jednotkou bude přerušeno, nutno se znovu přihlásit.

4.5.2. TOOLS – Remote Log-Router

Funkce vzdáleného logu slouží k zasílání výpisu zpráv o událostech systému na vzdálenou adresu. Každá událost má přiřazený stupeň závažnosti, podle vlivu na chod procesu. Pro potřeby zasílání se nastavuje minimální úroveň (Log Level). Zprávy s nastavenou a vyšší závažností pak mohou být odesílány na jednu nebo více vzdálených IP (Remote Log, syslog server). K příjmu a prohlížení zpráv na PC je určena speciální aplikace, dodávaná zároveň s RB (event. lze stáhnout z internetu). Chcete-li sledovat průběh připojování (PPPoE nebo PPPoA), zadejte minimální úroveň **Log Level** = *Debugg*. K prohlížení deníku přímo v paměti RB slouží stránka „System Log".



Postup při nastavení

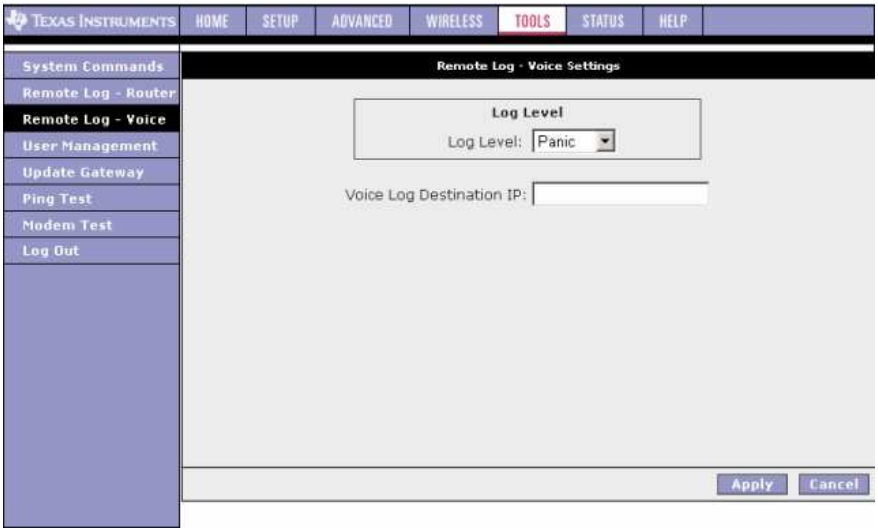
1. Zvolte požadovanou úroveň **Log Level**.
2. Budou odesílány pouze zprávy o událostech s touto a vyšší závažností.
3. Zadejte **IP Adress** vzdálené stanice (např. syslog serveru), na níž chcete zprávy zasílat, a nastavení odešlete tlačítkem **Add**.
4. Stanice se přidá do rozbalovacího seznamu výběru **Select a Logging Destination.**
5. Ze seznamu **Select a Logging Destination** zvolte požadovanou stanici. Klikněte na **Apply**.
6. Další stanice přidáte / smažete tlačítky **Add** / **Delete**.

Tabulka 2 Parametry nastavení vzdáleného logu

Pole	Překlad	Popis
Log Level	Míra závažnosti	Je definováno osm úrovní: o **Panic** – stav systému, který znemožňuje funkci RB o **Alert** (výstraha) – stav vyžadující okamžitý zásah, např. při poškození systémové databáze o **Critical** - např. chyba disku o **Error** – chyba s menší závažností, než předchozí o **Warning** (upozornění) – chyba, kterou je třeba hlásit o **Notice** (poznámka) – událost, která sama o sobě chybou není, ale může vyžadovat zvláštní opatření o **Info** – důležité zprávy z normálního chodu o **Debug** (ladění) – zprávy o chodu programu (pouze pro servisní nebo vývojové účely) Výchozí nastavení je *Notice* Na vzdálenou stanici budou zasílány pouze zprávy s nastavenou a vyšší úrovní
Add an IP Address	Přidejte IP adresu	IP adresa stanice, na níž mají být zprávy zasílány. Adresa bude uložena do seznamu a lze ji zvolit v seznamu Select… (viz dále)
Select a Loggin Destination	Zvolte cíl zasílání	Do seznamu můžete přidávat (resp. mazat) tlačítky **Add** (resp. **Delete**)

4.5.3. TOOLS – Remote Log-Voice

Zde se nastavuje výpis zpráva o provozu hlasových služeb.



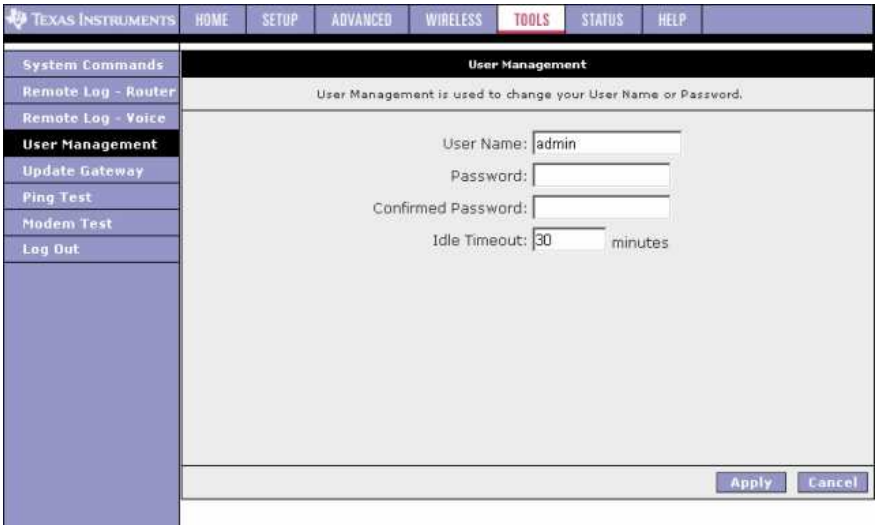
Nastaveni je podobné předešlé kapitole.

4.5.4. TOOLS – User Management

User Mangement: Na stránce User Management můžete změnit uživatelské jméno a heslo. Z bezpečnostních důvodů doporučujeme uživatelské jméno a heslo změnit z původního nastavení na jiné vlastní.

Router má své vlastní jméno a heslo. Pokud je přihlášený účastník po určitou dobu neaktivní, router se automaticky odhlásí. Budete-li při práci vyzváni o uživatelské jméno a heslo, zadejte je.

Poznámka - Pokud zapomenete uživatelské jméno nebo heslo, jediná možnost, jak se k routeru přihlásit, je resetovat celé zařízení stisknutím a podržením tlačítka **„Reset"** po dobu nejméně 10 sekund. LED indikátory zhasnou a opět se rozsvítí; tím indikují, že resetovací proces byl úspěšný.



Tabulka 4 Parametry nastavení účtu

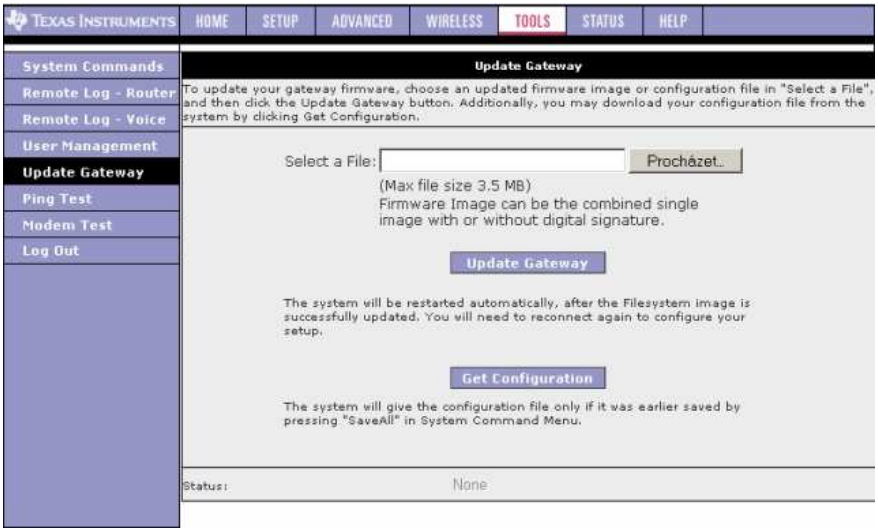
Pole	Překlad	Popis
User Name	Jméno	
Password	Heslo	Výchozí heslo je a*dmin*. Můžete zvolit jiné heslo. Zapomenete-li heslo, máte možnost restartovat RB s nastavením na tovární hodnoty – podržte tlačítko Reset na min. 10 sekund. Veškeré uživatelské nastavení bude smazáno. K přihlášení použijte potom a*dmin/admin*
Confirmed Password	Potvrzení nového hesla	
Idle Timeout	Stav nečinnosti	Lhůta pro vypršení spojení – pokud administrátor nepracuje déle než 30 minut (výchozí hodnota), bude automaticky odhlášen. Hodnotu lze změnit podle potřeby.

4.5.5. TOOLS – Update Gateway

Update Gateway: Firmware je software, jenž ovládá vlastní činnost routeru a rovněž vytváří podobu uživatelského rozhraní, jehož popis je předmětem této příručky. Firmware je uložen ve vnitřní Flash paměti routeru, verzi můžete zjistit v oddíle **STATUS ⇨ Product Information.**

Poznámka: Před upgradováním firmwaru se doporučuje uložit svou původní konfiguraci. Po dokončení upgrade se Vám bude hodit.

Proces upgradování se spouští z oddílu **TOOLS ⇨ Update Gateway**. Zobrazí se následující stránka.



Pole	Popis
Select File	Klikněte na Browse... (Procházet...) a vyhledejte soubor obsahující upgrade.
Update Gateway	Kliknutím na tlačítko upgradujete firmware/image. Po dokončení natažení se systém automaticky resetuje. Budete se muset znovu připojit a nakonfigurovat setup.
Get Configuration	Kliknutím stáhnete soubor s aktuální konfigurací systému do svého počítače. Postupujte podle instrukcí.

Poznámka - Při uploadování z počítače do routeru je důležité, abyste nijak nepřerušili činnost použitého web prohlížeče, např. zavřením jeho okna, kliknutím na nějaký odkaz nebo načtením nové stránky. Bude-li činnost prohlížeče přerušena, může to přerušit také upgradovací proces. Po ukončení uploadování se router automaticky rebootuje a restartuje. Celý proces trvá obvykle 4 až 5 minut.

Postup pro uložení aktualní konfigurace na disk (Backup):

1. Přístupte na stránku Tools – Update Gateway

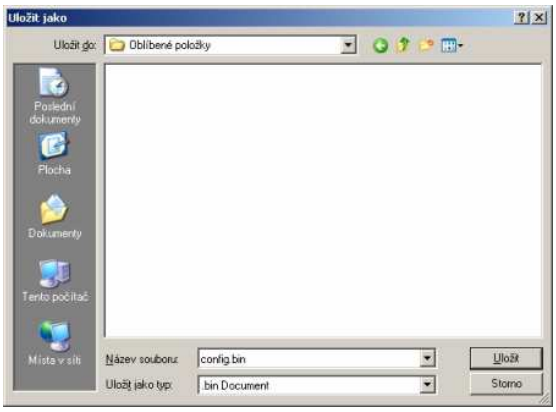
Poznámka – Pro uložení konfigurace by měly být splněny dvě podmínky:

- Již jste trvale uložili konfiguraci do paměti routeru pomocí **Tools – System Commands – Save All**.
- Používáte MS Internet Explorer ve verzi 6.x a vyšší.

2. Klikněte na **Get Configuration**. Předpokládejme, že konfigurace je trvale uložena do paměti routeru pomocí Tools – System Commands – Save All. Objeví se následující okno.

Poznámka – pokud konfigurace není trvale uložena do paměti routeru, objeví se následující okno. Všimněte si prosím informace ve spodní části okna, označené jako Status:.

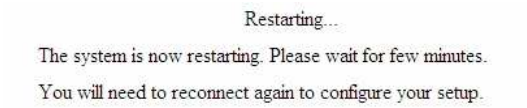
3. Klikněte na Uložit (Save) pro uložení „*config.bin*" souboru s Vaším nastavením na disk. Vyberte umístění na disku a klikněte na Uložit. Provede se uložení souboru „*config.bin*".



Postup pro obnovení konfigurace z uloženého souboru:

1. Přístupte na stránku Tools – Update Gateway
2. Klikněte na **Procházet** (Browse) a vyhledejte na disku soubor „*config.bin*" s uloženou konfiguraci.
3. Klikněte na **Update Gateway**. Objeví se následující okno s informací, že proces nakrání konfigurace byl úspěšně dokončen.

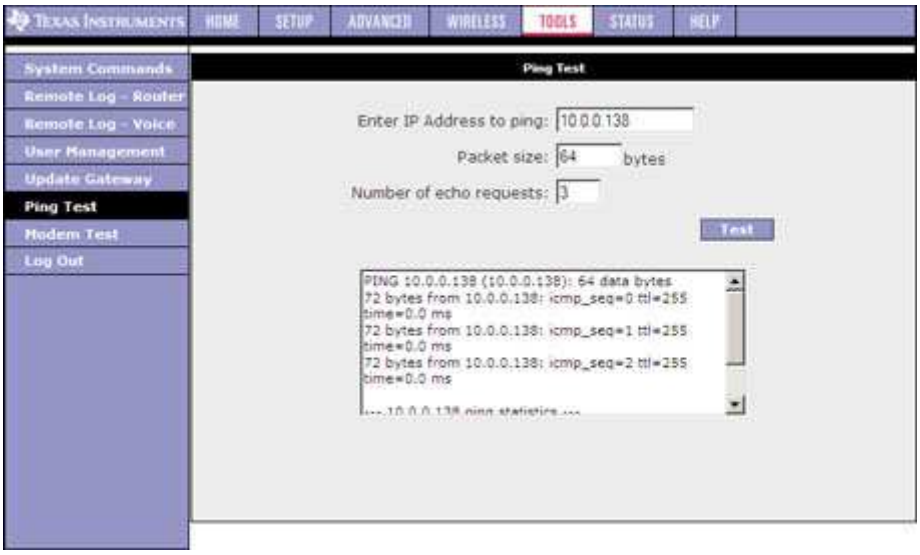
4. Klikněte na **Restart Gateway.** Router se bude restartovat. Uvidíte následující okno.



5. Proces restartu trvá cca. 1 min. Po restartu je potřeba se opět přihlasit na stránky routeru. Upozorňujeme, že nové nastavení routeru, bude již po restartu aktivované.

4.5.6. TOOLS – Ping Test

Ping test slouží ke zjišťování dostupnosti okolních i vzdálených stanic; tím je vhodný pro testování funkčnosti spojení či sítě. Pokud například na ping test odpoví některý veřejný server na straně WAN, spojení s internetem zaručeně funguje (pozor, některé servery na ping test neodpovídají).



Postup testu:

1. Přístup na stránku je Tools ⇨ Ping Test.
2. Podle potřeby změňte položky:
   - Enter the IP Address to Ping – testovaná IP adresa
   - Packet Size – délka paketu
   - Number of Echo Requests – počet odeslání
3. Klikněte na Test.
   Výsledek testu bude do několika sekund zobrazen v boxu v dolní části stránky.

Tabulka 5 Parametry ping testu

Pole	Popis
Enter IP Address to Ping	IP adresa, jejíž dostupnost chcete vyzkoušet. Výchozí nastavení je výchozí vlastní adresa RG (*10.0.0.138*).
Packet size	Délka testovacího paketu. Výchozí délka je *64* bytů
Number of Echo Requests	Počet odeslání paketu při jednom testu. Výchozí jsou *3.*

4.5.7. TOOLS – Test modemu

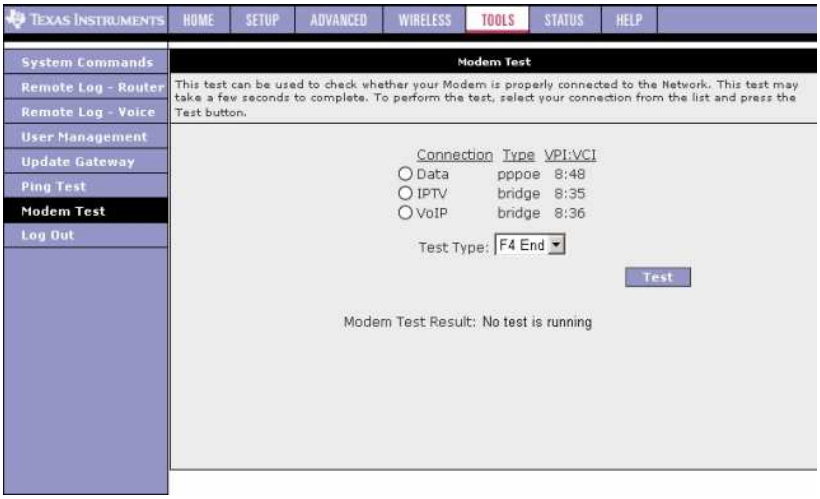
Na stránce **Modem Test** se testuje spojení s WAN. Celý test může trvat několik sekund. Nejdříve musíte mít aktivováno nejméně jedno WAN připojení a DSL linka musí být funkční, jinak test nebude fungovat. Rovněž si ověřte, že DSLAM tuto funkci podporuje, ne všechny DSLAM podporují F4 a F5. Buňky F4 a F5 jsou používány pro provoz, administrativu a údržbu (operation, administration, maintenance = OAM) v sítích ATM. Mají dva hlavní účely:

- Detekce a hlášení chybných úseků
- Testování smyček a celistvost spojů

OAM v ATM má několik úrovní:

- **F4**: Úroveň VP (virtuální cesta) – OAM prochází virtuální cestou přes síťové elementy (NE) a hlásí nedostupné nebo nezaručené cesty. Jsou vyhodnocovány jak průchody jednotlivými segmenty, tak toky mezi koncovými body sítě.
- **F5**: Úroveň VC (virtuální kanál) – OAM prochází virtuálním spojením přes síťové elementy (NE) a hlásí problémy ve funkčnosti kanálů, jako opožděně doručené buňky, ztracené buňky nebo problémy s vkládáním. Jsou vyhodnocovány jak průchody jednotlivými segmenty, tak toky mezi koncovými body sítě.

Na obrázku je testovací stránka **Modem Test**, jsou zde definována tři WAN připojení (Data, IPTV, VoIP).



Postup při testu modemu

1. Přístup ke stránce je **Tools ⇨Modem Test**.
2. Zvolte připojení (**Conection**), které chcete prověřit, a typ testu **Test Type**.
3. Klikněte na **Test**.

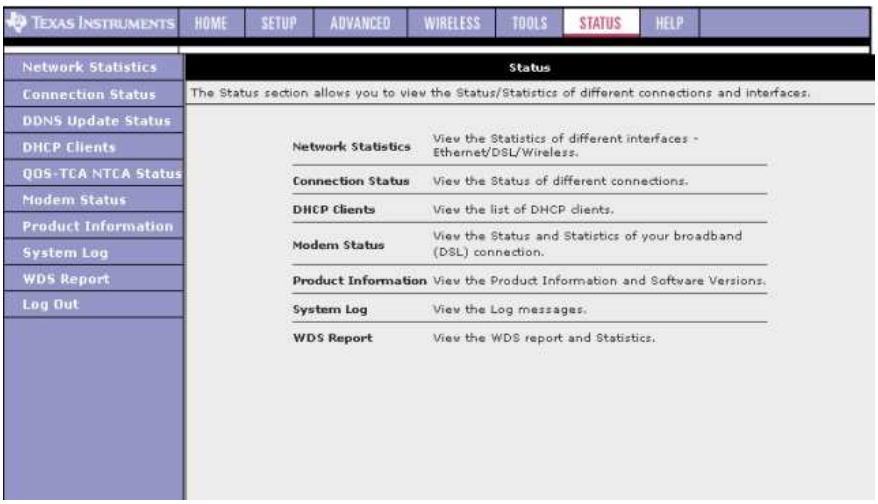
Tabulka 6 Parametry testu modemu

Pole	Popis
Connection	WAN připojení, které chcete testovat. Musí být definováno aspoň jedno WAN připojení
Type	Typ WAN připojení
VPI / VCI	Identifikátor virtuální cesty / kanálu
Test Type	Čtyři typy: **F4 End** – F4 mezi koncovými body **F4 Seg** – F4 v rámci segmentu **F5 End** – F5 mezi koncovými body **F5 Seg** – F5 v rámci segmentu

4.6. STATUS

Hlavní stránka **Status** je přístupná z horní tlačítkové lišty. V levém sloupci se nacházejí odkazy k jednotlivým výpisům, v hlavním okně se nachází jejich stručný popis:

- Network Statistics – statistické údaje z jednotlivých rozhraní
- Connection Status – stav jednotlivých připojení
- DDNS Update Status – stav aktualizace IP u DDNS
- DHCP Clients – výpis DHCP klientů
- Modem Status – stav DSL spojení modemu
- Product Information – informace o softwaru a hardwaru
- System Log – výpis událostí systém

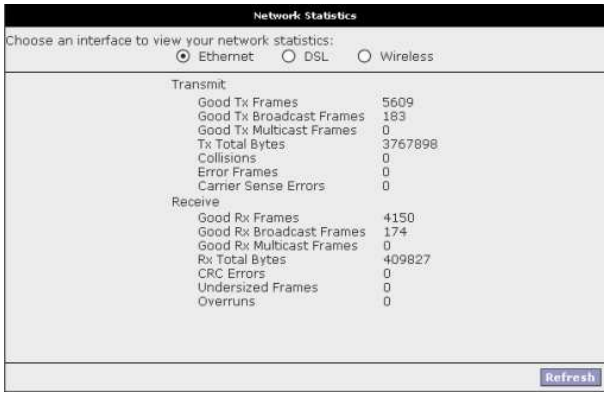


4.6.1. STATUS – Network Statistics

Na stránce **Network statistics** je možno prohlížet statistické údaje pro jednotlivé typy spojení a rozhraní. Zvolte podle potřeby Ethernet, DSL, nebo Wireless.

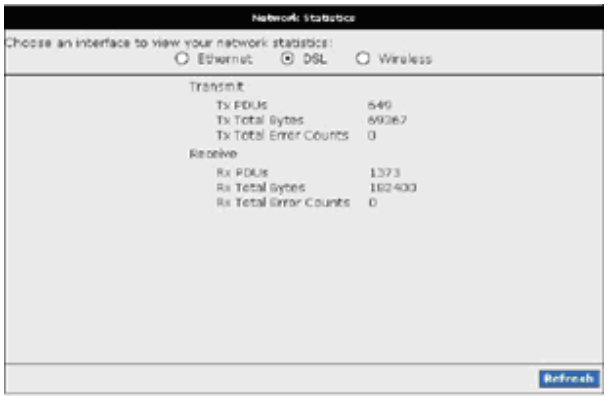
Statistika sítě - Ethernet:

Zobrazuje vyslané/přijaté rámce (Transmit/Receive Frames), chybné rámce (Error Frames), počet kolizí (Collisions) a počet CRC chyb (CRC Errors) z rozhraní Ethernet. Počitadlo provozu se po rebootování vynuluje.



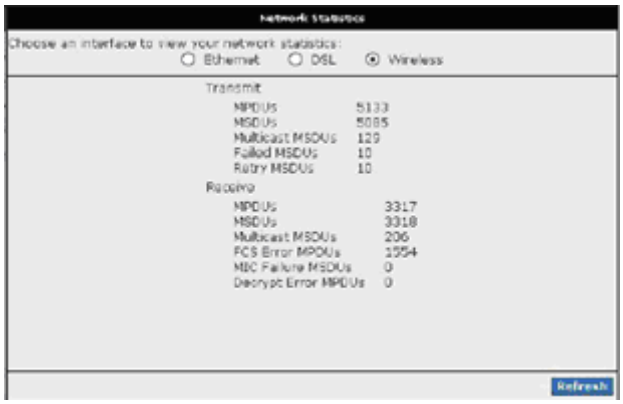
Statistika sítě - DSL:

Zobrazuje celkový počet přijatých/odeslaných bytů (Total Bytes Receive/Transmit) a počet chyb (Error Count) z rozhraní ADSL (WAN). Počitadlo provozu se při rebootování vynuluje.



Statistika sítě - Wireless:

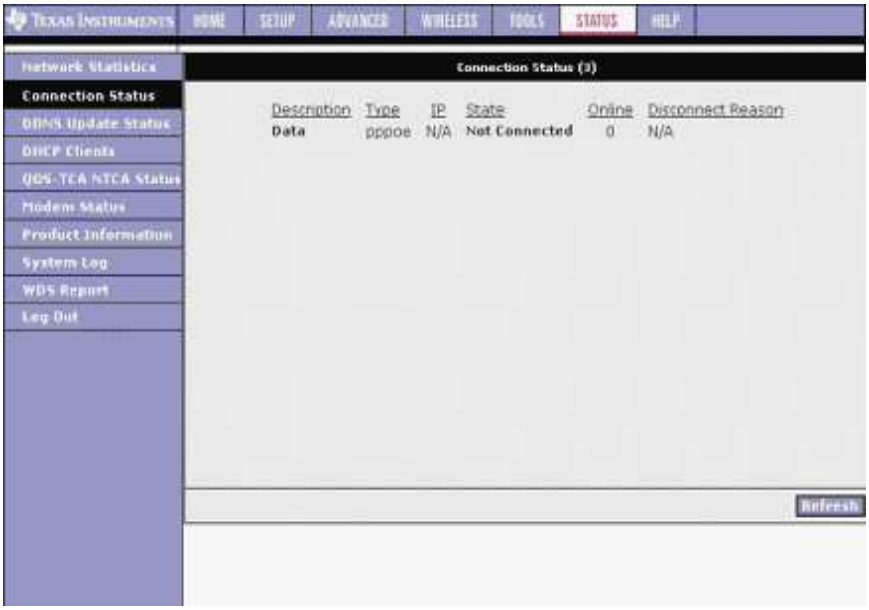
Zobrazuje informace o odeslaných/přijatých paketech (Transmit, Receive). Počitadlo provozu se při rebootování vynuluje.



Refresh: Kliknutím se znovunačte obsah okna a uvidíte případné změny údajů. Web prohlížeč by jinak setrvával v zobrazení stavu při prvním načtení.

4.6.2. STATUS – Connection Status

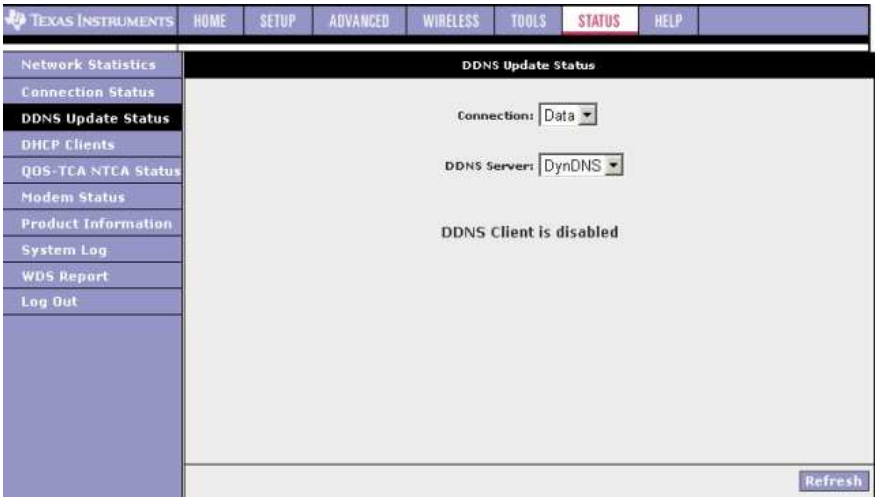
Stránka **Connection Status** zobrazuje stav existujícího připojení.



Refresh: Kliknutím se znovunačte obsah okna a uvidíte případné změny údajů. Web prohlížeč by jinak setrvával v zobrazení stavu při prvním načtení.

4.6.3. STATUS – DDNS Update Status

Na této stránce lze sledovat stav aktualizace IP u dynamického DNS serveru (pokud existuje registrace a je zapnut).



V uvedeném příkladu je DDNS vypnut (přednastavená volba). Funkce DDNS je popsána v příslušné kapitole. Aktivní DDNS klient aktualizuje svůj záznam u DDNS serveru pokaždé, když obdrží novou IP adresu.

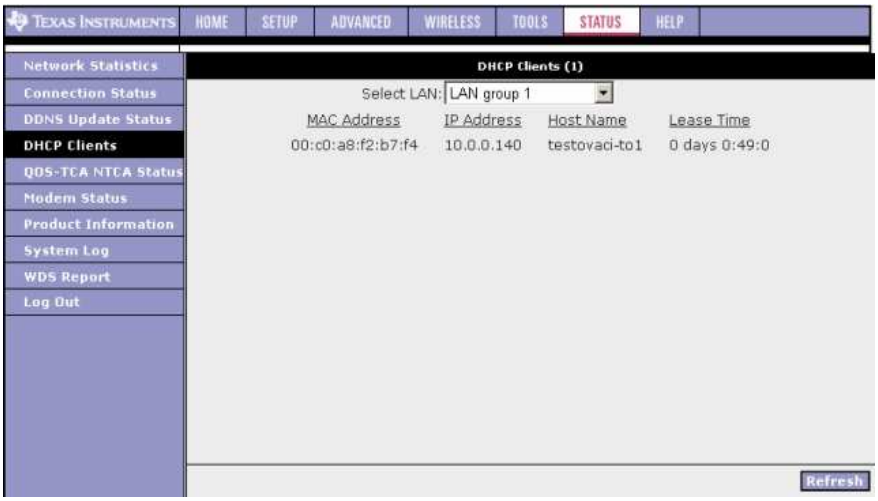
Tabulka 1 Pole stránky Status DDNS

Pole	Popis
Connection	WAN připojení, přes které má probíhat přístup
DDNS Server	Server poskytovatele služby DDNS. V současnosti RB podporuje pouze **DynDNS** a **TZO**
Status	Stav může nabývat hodnot: o **Updated** (aktualizován) – IP adresa klienta (RB) se změnila a změna byla zaslána k DDNS serveru o **No change** (beze změny) – IP adresa se od poslední návštěvy nezměnila o **Error** – Při pokusu o aktualizaci došlo k chybě
Error Description	Popis případné nastalé chyby

4.6.4. STATUS – DHCP Clients

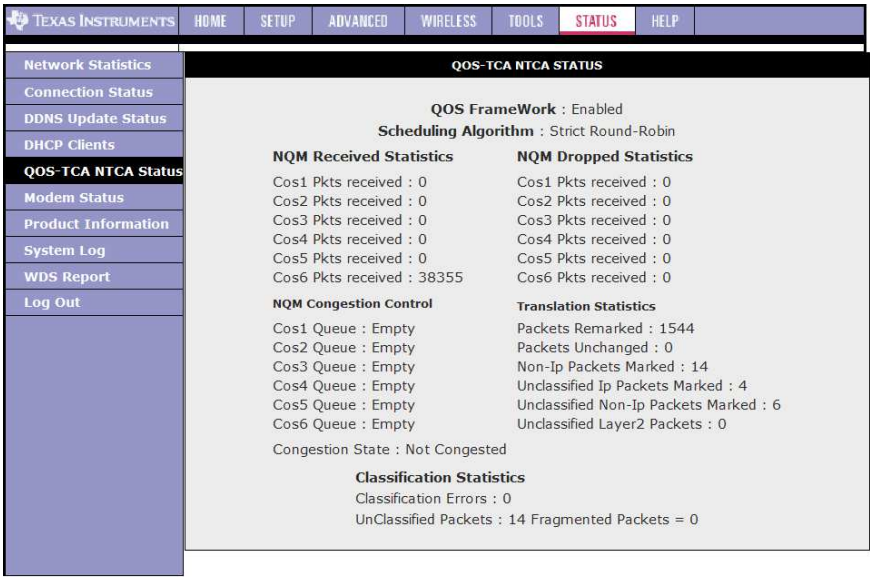
Pokud je zapnut DHCP server, je možno na této stránce sledovat výpis DHCP klientů. Vyberte skupinu LAN, kterou chcete sledovat. Zobrazí se výpis klientů; u každého klienta je zobrazeno:

- MAC adresa
- IP adresa
- Jméno klienta
- Doba pronájmu



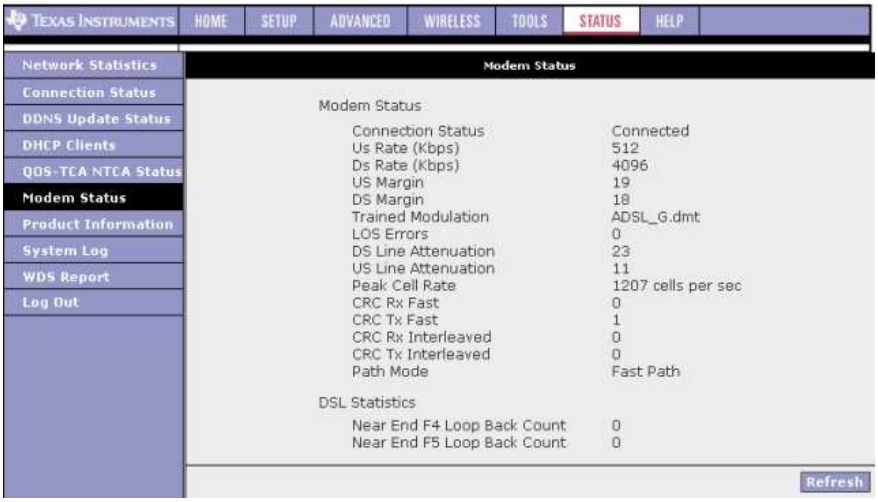
4.6.5. STATUS – QOS TCA NTCA Status

Na této stránce naleznete stav QoS TCA NTCA.



4.6.6. STATUS – Modem Status

Stránka **Modem Status** (Stav modemu) zobrazuje status fyzického připojení nebo linky. Zdrojem informací je buď router sám nebo DSLAM, uživatel je nijak nemůže měnit.

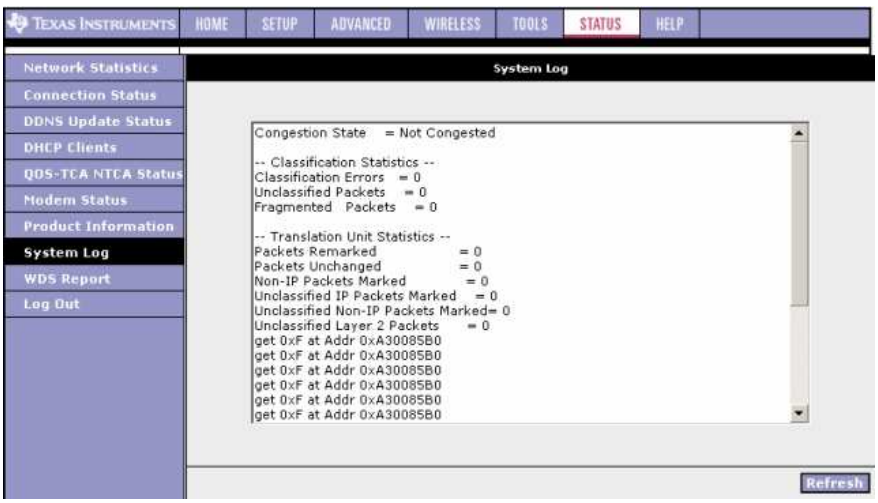


4.6.7. STATUS – Product Information

Na stránka **Product Information** (Informace o výrobku) jsou zobrazeny údaje a parametry ADSL2/2+ routeru včetně verze softwaru.

4.6.8. STATUS – System Log

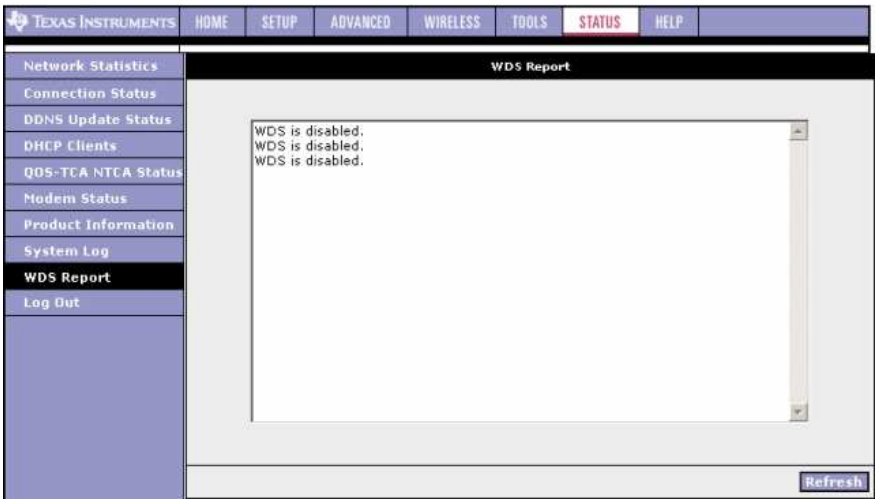
Na stránce **System Log** je přístupný výpis událostí systému. Zde jsou vypsány všechny události. Události nastavené závažnosti a vyšší jsou současně odesílány na Remote Log host (pokud je vzdálený log zapnut). Lze zobrazit posledních 32 událostí.



4.6.9. STATUS – WDS Report

Na této stránce je výpis z WDS sítě, platný pro RB = AP (access point). Zobrazují se:

- WDS konfigurace a stav
- WDS statistika
- WDS databáze



4.7. HELP

Úvodní stránka nápovědy **Help** obsahuje základní rozcestník pro jednotlivé oblasti a je kdykoliv přístupná.

PŘÍLOHA A: VÝKLAD POUŽÍVANÝCH POJMŮ

Co je to firewall ?

Firewall je zařízení, které chrání jednu síť před druhou sítí, nebrání však komunikaci mezi nimi. Firewall zahrnuje NAT router a další funkce, které se mají vypořádat s obtěžováním nebo útokem ze strany hackerů. Některé typy obtěžování nebo útoku lze rozeznat hned na vstupu. Pokud dojde k incidentu, firewall může zaznamenat zprávu (log) s detaily útoku, popřípadě informovat administrátora zasláním emailu. Administrátor s použitím záznamu o události (logu) pak může zahájit řízení s poskytovatelem služeb hackera. Při některých typech napadení může sám firewall zabránit dalšímu tím, že po určitou dobu bude zahazovat všechny další pakety přicházející z IP adresy hackera.

Co je to NAT?

NAT (Network Address Translation) – překladač síťových adres. Váš poskytovatel Vám propůjčí jednu IP adresu pro přístup na internet. Vy však můžete mít síť složenou z více počítačů, ze kterých chcete mít současně přístup na internet. Router, který disponuje NAT, převádí vaše lokální síťové adresy na jedinou adresu Vašeho poskytovatele. NAT má přehled o všech těchto spojeních a zajišťuje, že správná data se dostanou na správný počítač.

Některé programy nedokážou spolupracovat s NAT. Jedná se především o síťové hry a další speciální aplikace. Router si dokáže poradit s valnou většinou těchto problémových aplikací. NAT rovněž způsobuje problémy, pokud chcete provozovat server pro internet. V tomto případě pokračujte následujícím odstavcem o DMZ.

Co je to DMZ?

DMZ (Demilitarized Zone) – demilitarizovaná (beze zbraní) zóna. DMZ je část lokální sítě, která je více otevřená internetu. Přepokládá se, že v ní bude běžet web server nebo game server. Server umístěný v lokální síti za NAT by byl blokován. Řešením je izolovat jeden počítač do DMZ, takže bude připojen přímo k internetu (a také více zranitelný).

Počítač v DMZ zóně ve skutečnosti není k internetu (WAN) připojen přímo, ale má svou lokální adresu. Z vnějšího pohledu má adresu routeru.

DMZ byste měli používat, pokud chcete provozovat server, ke kterému má být přístup z internetu. Vnitřní programy a servery (servery tiskáren) BY NEMĚLY být připojeny k DMZ.

Co je to Gateway?

Gateway (brána). Internet je velice rozsáhlý, takže jednoduchá síť by nestačila rozumným způsobem pokrýt všechen provoz. Toto omezení lze překonat rozdělením do menších částí nebo podsítí, které již stíhají dobře komunikovat se svými stanicemi. Odpadá tak problém s obrovským množstvím stanic, na druhou stranu vzniká potřeba vzájemné komunikace mezi těmito podsítěmi.

Na rozhraní dvou podsítí se nachází zařízení zvané gateway (brána). Pokud počítač chce komunikovat s jiným počítačem v té samé podsíti, spojí se s ní poměrně jednoduchým způsobem. Pokud se však cílová stanice nachází v jiném segmentu, bez dalších infomací to nejde.

Jeden z konfiguračních parametrů každého síťového zařízení je adresa výchozí brány (Default gateway). Určuje ji administrátor sítě a síťová stanice na její adresu zasílá všechna data, jejichž příjemce se nenachází ve vlastní síti. Pokud tedy počítač vidí ostatní počítače v lokální síti, ale nemůže komunikovat s vnějškem, pravděpodobně není správně nastavená adresa výchozí brány (default gateway).

PŘÍLOHA B: ČASTÉ OTÁZKY

V této příloze jsou zodpovězeny otázky, které mohou nastat při nastavování tohoto ADSL2/2+ routeru.

Některé z odpovědí již byly zodpovězeny v textu manuálu, v kapitolách, které probírají dané téma.

1. **Jak zjistím, že spojení mezi ethernetovou kartou a ADSL2/2+ routerem funguje?**

Odp. Pro testování spojení mezi počítačem a routerem se používá ping test. Jako cílovou adresu ping testu použijte adresu routeru (výchozí je http://10.0.0.138). Více o ping testu najdete v příloze C: Řešení potíží. Nebo jinak - pokud LED dioda Ethernet Link svítí, spojení funguje.

2. **Jak zjistím, že spojení mezi ADSL2/2+ routerem a internetem funguje?**

Odp. Podobně jako v předchozím případě se používá ping test. Jako cílovou adresu ping testu tentokrát použijte nějakou URL adresu, například www.google.com. . Nebo jinak - pokud LED diody ADSL a PPP současně svítí, spojení funguje.

3. **Jak mohu zjistit nebo ověřit MAC adresu routeru nebo ethernetové karty počítače?**

Odp. Viz kapitola 3. oddíl 3.4.

4. **Co je to režim ad-hoc?**

Odp. Pokud bezdrátová síť běží v režimu ad-hoc, potom všechny fungující bezdrátové stanice mohou komunikovat navzájem mezi sebou, bez prostředníka (základnové stanice – access pointu).

5. **Co znamená režim infrastructure?**

Odp. V tomto případě veškerá komunikace v bezdrátové síti probíhá přes základnu (access point).

6. **Co je to roaming?**

Odp. Roaming je schopnost přenosného počítače komunikovat nepřetržitě při pohybu mezi více bezdrátovými sítěmi, tj. když se dostane z dosahu jedné základny, přebere ho další základna. Přenosný počítač musí však být mimo jiné nastaven na stejný kanál jako příslušná základnová stanice.

7. **Co je to ISM pásmo?**

Odp. FCC (Federální komise USA pro komunikaci) a její zahraniční partneři vyhradili radiové pásmo pro volné (bezlicenční) použití v průmyslu, vědě a medicíně (Industrial, Scientific, Medical = ISM). Použitá frekvence je kolem 2.4 MHz, měla by být celosvětově volná. Tím vznikl skutečně revoluční převrat v možnosti používání vysokorychlostního bezdrátového spojení pro uživatele celého světa.

8. **Co je to MAC adresa?**

Odp. MAC (Media Access Control Address) je jedinečná hardwarová adresa, která jednoznačně celosvětově identifikuje každé koncové síťové zařízení.

9. **Co je standard IEEE 802.11b?**

Odp. IEEE 802.11b je rozšířený standard 802.11; týká se bezdrátových LAN sítí s přenosovou rychlostí 11 Mbps v pásmu 2.4 GHz.

10. **Co je standard IEEE 802.11g?**

Odp. IEEE 802.11g je rozšířený standard 802.11; týká se bezdrátových LAN sítí s přenosovou rychlostí 54 Mbps v pásmu 2.4 GHz.

11. **Co je to NAT a k čemu se používá?**

Odp. NAT (překladač síťových adres) překládá více adres v soukromé LAN na jedinou veřejnou IP adresu (WAN port). NAT zvyšuje bezpečnost počítačů v LAN, protože jejich lokální soukromá adresa není nikdy vyslána na internet.

12. **Co mám dělat, když se nemůžu připojit na webovou stránku konfigurace toto ADSL2/2+ routeru?**

Odp. Zrušte použití proxy serveru nebo vytáčeného připojení ve svém prohlížeči.

13. **Co je to DMZ (DeMilitarizovaná zóna)?**

Odp. DMZ odkrývá jednu IP adresu (počítač) pro přístup z internetu. Některé aplikace vyžadují otevření více TCP/IP portů. Doporučuje se, aby počítač v DMZ měl statickou IP adresu.

14. **Co je to BSS ID?**

Odp. Konkrétní bezdrátová síť LAN Ad-Hoc se označuje jako Basic Service Set (BSS). Počítače v jedné BSS musí být konfigurovány se stejnou ID BSS.

15. **Co je to SSID?**

Odp. Service Set Identifier (Identifikátor sítě) je unikátní identifikátor o max. délce 32 znaků připojovaný k hlavičce paketů posílaných v bezdrátové LAN (WLAN). Slouží také jako heslo pro přípojení. SSID rozlišuje sítě jednu od druhé, proto všechny základnové a mobilní stanice, které jsou připojeny, nebo se snaží připojit do konkrétní sítě musejí použít stejné SSID. Bez správného SSID nebude umožněn přístup.

16. **Co je to WEP?**

Odp. WEP (Wired Equivalent Privacy = stejná bezpečnost jako u drátové sítě) je zabezpečovací protokol pro bezdrátové sítě, definovaný standardem 802.11b. WEP byl vyvinut tak, aby poskytoval stejnou úroveň zabezpečení jako drátová síť, tedy absolutní. WEP šifruje přenášená data klíčem.

17. **Co je to WPA?**

Odp. WPA (Wi-Fi Protected Access) je další bezpečnostní protokol, který podstaným způsobem zlepšuje ochranu přednášených dat.

18. **Jaký je maximální počet IP adres, které tento router může obsluhovat?**

Odp. Tento ADSL2/2+ router může obsluhovat maximálně 253 IP adres.

PŘÍLOHA C: ŘEŠENÍ POTÍŽÍ

Průvodce řešením problémů odpovídá na obvyklé problémy, které mohou vzniknout při nastavení, připojení routeru a nastavení PC.

1. **ADSL2/2+ router nefunguje (nesvítí žádná LED)**

Odp. Zkuste následující:

- Zkontrolujte, že síťový zdroj routeru je zapojen do zásuvky a napájecí konektor do routeru.
- Zkontrolujte, jestli máte správný originální síťový zdroj (adaptér) .
- Hlavní vypínač musí být v poloze ON .

2. **Změnili jsme LAN IP adresu na stránce LAN konfigurace a naše PC přestalo router vidět.**

Odp. Po změně LAN IP adresy routeru proveďte na svém PC následující kroky:

- Klikněte na **„Start" ⇨ „Run" (Spustit).**
- Do následujícího okna vepište **cmd**, potom klikněte na OK.
- Vyskočí okno textového režimu; vepište **ipconfig/release**, stiskněte Enter.
- Vepište **ipconfig/renew**, Enter.

3. **Bezdrátové spojení vůbec nefunguje.**

Odp. Zkuste následující.

- Zkontrolujte, zda bezdrátový adaptér jak klienta, tak routeru (access point) jsou zapnuty (enabled) a nastaveny na stejný kanál.
- Ověřte správnou konfigurace WLAN klienta (SSID, WEP).

4. **Slabý signál nebo dosah bezdrátového spojení.**

Odp. Zkuste následující:

- Nastavte automatické vyhledávání kanálů, nebo zkuste najít DSSS kanál, který není rušen ostatním provozem.
- Najděte pro základnu (router) v budově lepší místo.
- Zkontrolujte, že jak základna (router), tak klient jsou nastaveni na stejný vysílací kanál.

5. **LAN (Link/Act) LED nesvítí.**

Odp. Zkontrolujte následující:

- Kabely musejí být v pořádku a řádně připojeny (konektory).
- Kabel musí být správného typu (nekřížený).
- Ethernetový port počítače musí být nastaven pro automatické vyjednávání (auto-negotation).

6. **Nejdou načíst web stránky nastavení a konfigurace routeru (z počítače v místní LAN)**

Odp. Zkontrolujte následující :

- Hardwarové připojení k LAN portu routeru. LED musí svítit.
- Windows TCP/IP nastavení (detaily viz kapitola 3).
- Otevřete Windows příkazový řádek:

9. Windows 9x/ME: Vepište **winipcfg**, stiskněte **Enter**.
10. Windows 2000/XP: Vepište **ipconfig/all**, stiskněte **Enter**.

- Měly by vám vyjet tyto údaje:

11. **IP adresa: 10.0.0.x**
12. **Submaska: 255.255.255.0**
13. **Deault Gateway IP: 10.0.0.138**

7. **Zapomněl jsem nebo ztratil heslo administrátora:**

Odp. Jediná možnost je totálně resetovat router stisknutím a podržením tlačítka reset po dobu nejméně 10 sekund; přitom dojde k návratu k továrním nastavením.

Pokud při ukládání nastavení jste stále žádáni o heslo:

- Přejděte na webovou stránku routeru **http://10.0.0.138**
- Zadejte výchozí „username" a „password" (jméno a heslo), stiskněte **Enter**.

- Přejděte na záložku **„TOOLS"**, potom na **„User Management"**.
- Zadejte nové uživatelské jméno a heslo (heslo dvakrát pro potvrzení) do políček „Username", „Password" a „Confirm Password".
- Klikněte na **„Apply"**.

8. **Potřebuji upgradovat firmware:**

Odp. Nejnovější verzi software najdete na stránkách **www.joyce.cz**. Před zahájením vlastního upgradovacího procesu musíte:

- Stáhnout soubor firmware a uložit ho na zvoleném místě v počítači.
- Pozorně přečíst poznámky k nové verzi.
- Seznámit se s postupem uvedeným pod záložkou **TOOLS ⇨ Update Gateway**.

9. **Testování LAN cesty k routeru:**

Odp. Pro ověření správného nastavení a propojení LAN spojení z Vašeho PC k routeru můžete spustit ping test:

- Klikněte na **„Start" ⇨ „Run" (Spustit)**.
- Do otevřeného řádku napište **Ping 10.0.0.138** a klikněte **OK**.
- Pokud je cesta v pořádku, měl by se Vám zobrazit výpis v následujícím formě

  Reply from 10.0.0.138 bytes=32 time<10ms TTL=60
- Pokud je cesta není průchodná, měl by se Vám zobrazit

  Request timed out

Pokud cesta nefunguje:

- Zkontrolujte, jestli LED dioda LAN portu svítí.
- Zkontrolujte, jestli máte v pořádku kabel.
- Ověřte instalaci a nastavení Ethernetové karty
- Zkontrolujte IP adresy routeru a počítače a že se obě nacházejí ve stejné podsíti.

10. **Bezdrátové spojení počítače (Wi-Fi LAN karta) s routerem nefunguje:**

Odp. Nejdříve zkontrolujte, jestli LED dioda WL ACT na routeru svítí. Potom:

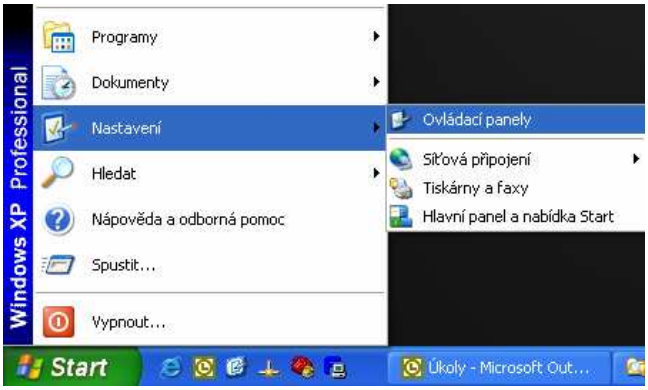
- Zkontrolujte, zda nastavení WLAN na počítači je shodné s nastavením routeru (např. SSID, číslo kanálu).
- Zkontrolujte, jestli máte na obou zařízeních nastavený shodný WEP klíč.

PŘÍLOHA D: UPNP NASTAVENÍ VE WINDOWS XP

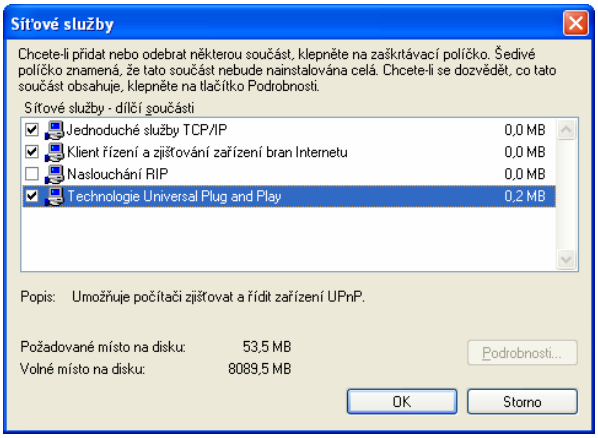
Přidání UPnP:

Jestliže pracujte v Microsoft Windows XP, doporučuje se přidat UPnP do vašeho systému, a to dle následujícího způsobu:

1. Klikněte na Start, Nastavení a poté na Ovládací panely.



2. Objeví se okno Ovládacího panelu. Klikněte na **Přidat nebo odebrat programy**.
3. Objeví se okno Přidat nebo odebrat programy. Klikněte na **Přidat/odebrat součásti systému**.
4. Objeví se okno Průvodce instalací. Vyberte **Síťové služby** v seznamu součástí a klikněte na Podrobnosti.
5. Objeví se okno Služby sítě. Vyberte **Technologie Universal Plug and Play** a klikněte na OK.



6. Klikněte na **Next**, abyste zahájili instalaci a postupujte dle pokynů Windows průvodce.

   Systém se může dotazovat na originální Windows XP CD-ROM. Vložte CD-ROM a ukažte cestu Windows na správné umístnění jednotky CD-ROM.

   Pro aktivaci vašeho nastavení je nezbytné restartovat váš systém Windows Klikněte OK pro restart vašeho systému Windows.

7. Průvodce instalací oznámí, že instalace proběhla úspěšně. Klikněte na **Dokončit** pro ukončení.

PŘÍLOHA E: SLOVNÍK

Slovník nabízí vysvětlení termínů a zkratek, které byly použity v uživatelském průvodci.

AP: Access Point: Stanice, která předává a přijímá data v WLAN (Wireless Local Area Network). Pro bezdrátové zařízení se Access point chová jako most do LAN.

ATA: Analogový telefonní adaptér

ATM: Asynchronous Transfer Mode: Metoda přenosu, ve které se data uspořádávají do 53-bytových jednotek. Ve vztahu k ostatním buňkám ATM buňky postupují asynchronně.

BC: Vysílací komunikace, ve které odesílatel doručuje každému účastníkovi v síti.

BER: Bit Error Rate: Procento bitů, které obsahuje chyby ve vztahu k celkovému počtu doručených bitů.

Bridge: Zařízení, které propojuje dvě sítě a rozhoduje, která data ze sítě by měly být odeslány.

Bridge Mode: Režim mostu se používá, když je jeden PC připojen do Ethernetu ze strany LAN nebo USB portu. Metoda přenosu přemostění IEEE 802.01D se používá pro překlenutí mezi stranou WAN (ADSL) a stranou LAN (Ethernet nebo USB), např. uchovat nebo odeslat.

CBR: Constant Bit Rate: Stálá rychlost přenosu, která je ideální pro streaming, která používáme již v průběhu stahování. Jedná se data, jako jsou audio nebo video soubory.

Cell: Jednotka přenosu v ATM, která se skládá z velikostně daného rámce. Ten obsahuje hlavičku o velikosti 5 x 8 bitů a vlastní zprávu o velikosti 48 x 8 bitů.

CHAP: Challenge Handshake Authentication Protocol: Lepší ochrana než PAP, CHAP, která používá uživatelského jména a hesla v kombinaci s náhodně vygenerovanou výzvou. Ta se ovšem musí ověřit použitím funkce jednosměrného vypočítávání adresy.

CLP: Cell Loss Priority: ATM buňky mají dvě úrovně priority, CLP0 a CLP1. CLP0 mají přednost. V případech velkého datového přetížení se mohou CLP1 chybné buňky vyřadit se seznamu, aby se pro CLP0 buňky zachoval poměr ztráty buněk.

CO: Central Office: V ústředně se na místní smyčce se domácí a kancelářské telefonní linky se spojují a jdou přes přepojovací vybavení, aby se připojily do jiných ústředen. Vzdálenost z ústředny je ovlivněna tím, zda může nebo nemůže být signál ADSL podporován danou linkou.

CPE: Customer Premises Equipment. CPE specifikuje vybavení na straně zákazníka nebo na straně LAN.

CRC: Cyclic Redundancy Checking: Metoda pro kontrolu chyb v přenosu dat mezi dvěma počítači, CRC aplikuje polynomickou funkci (16 nebo 32-bitovou) na blokaci dat. Výsledek této polynomické funkce je přidán k přenosu dat. Cílový počítač aplikuje ty samé polynomické funkce na data. Jestliže hostící a cílový počítač dostanou ten samý výsledek, přenos byl úspěšně proveden. V jiném případě odesílatel obdrží oznámení, aby znovu poslal data.

DHCP: Dynamic Host Configuration Protocol: Komunikační protokol, který umožňuje sítovým administrátorům, aby mohli zařídit a přiřadit IP adresy počítačům uvnitř sítě. DHCP poskytuje zvláštní adresy počítačům v síti, které umožňují spojení do Internetu přes Internet protokol (IP). DHCP může pronajímat IP adresy nebo poskytovat stálé statické adresy těm počítačům, které to potřebují (servery apod.).

DMZ: Demilitarized Zone: Počítač hostitel nebo síť, která se chová jako neutrální zóna mezi soukromou a veřejnou sítí. DMZ zamezuje přímý přístup do serveru nebo nějakého počítače uvnitř soukromé sítě vnějším uživatelům. Vnější uživatel posílá požadavky do DMZ a ta zahajuje relace ve veřejné síti na základě těchto požadavků. DMZ nemůže zahájit relaci v soukromé síti, může pouze odeslat paket do soukromé sítě tak, jak je požadován.

DNS: Domain Name System: Metoda umístnění a překladu jména domény do Internetového protokolu (IP), kde je jméno domény jednoduché a významné pro internetovou adresu.

DSL: Digital Subscriber Line: Technologie, která provádí širokopásmové spojení přes standardní telefonní linky.

DSLAM: Digital Subscriber Line Access Multiplexer: Používáním multiplexních technik DSLAM přijímá signály ze zákaznických DSLAM linek a umísťuje signály na vysokorychlostní hlavní přenosnou linku. DSLAM jsou obyčejně situovány v ústřednách telefonních společností.

Encapsulation: Zapouzdření jedné datové struktury uvnitř jiné. Například pakety mohou být zabaleny v rámci ATM během přenosu. FEC: Forward Error Correction: Technika opravy chyb při odesílání je metoda, ve které se zpracovávanému paketu dat přes algoritmus přidává extra chyby, která upravuje bity do paketu. Jestliže je přenášená zpráva chybná, tyto bity jsou použity na opravu chybných bitů, a to bez opětovného přenosu.

Firewall: Firewall je nástroj, který provádí jak běžnou, tak i uživatelskou bezpečnostní strategii, a to ve snaze o obranu proti vetřelcům. Firewall funguje tak, že analyzuje a pročišťuje IP pakety, které porušují pravidla definovaná ve správci firewallu. Firewall je umístněn v místě vstupu do sítě. Všechny příchozí nebo odchozí data musí projít na přezkoumání přes firewall.

FoIP: Přenos faxu internetovým protokolem (Fax over Internet Protocol)

Fragmentation: Rozbití paketu na menší pakety. To je způsobeno jak neschopností přenosového média podporovat původní velikost paketu nebo tak i neschopností přijímacího počítače obdržet paket takové velikosti. Fragmentace vznikne, když odesílatel/MTU je větší než příjemce/MRU.

FTP: File Transfer Protocol. Standardizovaný internetový protokol, který je nejjednodušší pro přenos souborů z jednoho počítače do druhého přes Internet. FTP používá pro svoji funkci Internet TCP/IP protokoly.

Full Duplex: Přenos dat se může přenášet a přijímat na stejném bázi přenosu signálu a ve stejném čase. Full Duplex linky jsou obousměrné.

G.dmt: formálně G.992.1, G.dmt je forma ADSL, kterou používá Discrete MultiTone (DMT) technologie. G.dmt ve své konstrukci obsahuje rozdělovač.

G.lite: formálně G.992.2, G.lite je standardní cesta pro instalaci ADSL služeb. G.lite umožňuje spojení o rychlosti až do 1.5 Mbps downstream a 128 kbps upstream. G.lite nepotřebuje rozdělovač na straně uživatele, protože rozdělení se provádí na vzdáleném konci (telefonní společnosti).

Gateway: Místo na síti, které je vstupem do jiné sítě. Například router je bránou, která spojuje LAN s WAN.

Half Duplex: Přenos dat se může přenášet a přijímat na stejném bázi přenosu signálu, ale už ne ve stejném čase. Half Duplex linky jsou obousměrné.

HEC: Headed Error Control: kontrola ATM chyb pomocí používání algoritmu CRC na pátém z pěti osmibitových prvků v hlavičce ATM buňky tak, aby vytvářela vlastnosti kontroly. Používáním HEC mohou být jednobitové chyby v hlavičce opraveny nebo mohou být detekovány chyby v hlavičce o velikosti více bitů.

HNP: Domácí síťový procesor

Host: V kontextu Internetového protokolu je hostující počítač ten, který má plný dvousměrný přístup do ostatních počítačů na Internetu.

IAD: Integrated Access Device: Zařízení, které multiplexuje a demultiplexuje komunikaci na CPE pro přenos do CO do a ven z jednoduché telefonní linky.

IP: Internet Protocol: Metoda pomocí níž se informace posílá z jednoho počítače do druhého přes Internet. Každý z hostujících počítačů má zvláštní IP adresy, které je odlišují od jiných počítačů na Internetu. Každý poslaný paket dat zahrnuje odesílatele, IP adresu a příjemce s jeho IP adresou.

LAN: Local Area Network: Skupina počítačů. Tato skupina počítačů sdílí zařízení jako tiskárny, harddisky, scannery a optické zařízení. Počítače v LAN běžně sdílí internetové připojení přes nějaký druh routeru, který připojuje počítače do WAN.

LLC: Logical Link Control: Zajišťuje bod rozhraní do MAC podvrstvy. V případě, že některé protokoly jsou přenášeny skrze ten samý virtuální obvod je potřeba použít LLC zabalení.

MAC Address: Media Access Control Address: Zvláštní číslo hardwaru na počítači nebo zařízení, které je identifikuje nebo má vztah k IP adrese tohoto zařízení.

MC: Multicast: Komunikace, která zahrnuje jednoho odesílatele a více specifických příjemců v síti.

MRU: Maximum Receive Unit: MRU je velikostně největší paket, který může modem přijmout. Během PPP komunikace bude protějšek PPP spojení indikovat jeho MRU a přijme jakoukoliv hodnotu až do této výše. Aktuální MTU spojení PPP bude nastaveno do menšího z následujících: MTU anebo MRU na protější straně. V případě obvyklé komunikace protějšek přijme tento MRU a nepošle paket s informacemi, který bude větší než tato hodnota.

MSS: Maximum Segment Size: Značný rozsah dat, který TCP zašle v jednoduchém, nefragmentovaném IP paketu. Jestliže je spojení vytvořeno mezi LAN klientem a hostitelem na straně sítě WAN, LAN klient a WAN hostitel budou během TCP spojení ukazovat jejich maximální segmentační velikost (Maximum Segment Size).

MTU: Maximum Transmission Unit: Největší velikost paketu, který může být odeslán modemem. Jestliže fronta v síti nějakého paketu je větší než hodnota MTU, pak se bude paket fragmentovat před přenosem. Během PPP komunikace bude protějšek PPP spojení indikovat jeho MRU a přijme jakoukoliv hodnotu až do této výše. MTU spojení PPP bude nastaveno do menšího z následujících: MTU anebo MRU na protější straně

NAPT: Network Address and Port Translation: NAPT, který je rozšířením NAT, mapuje mnoho soukromých vnitřních adres do jedné IP adresy. Vnější síť (WAN) může tuto jednu IP adresu rozpoznat, ale nemůže rozpoznat individuální zařízení IP adres, které jsou přeloženy pomocí NAPT.

NAT: Network Address Translation: Překlad IP adresy jedné sítě na odlišnou IP adresu, kterou rozpoznává jiná síť. To dává vnější (WAN) síti schopnost odlišit zařízení ve vnitřní (LAN) síti, tudíž má vnitřní síť privátní sadu IP adres přiřazenou DHCP serverem, kterou vnější síť nerozpozná.

PAP: Password Authentication Protocol: Autorizační protokol, ve kterém se autorizace provádí pomocí uživatelského jména a hesla.

PDU: Protocol Data Unit: Rám pro přenesená data přes datovou linku vrstvy 2.

Ping: Packet Internet Groper: Zařízení, které se používá na určení, zda příslušné zařízení je on-line nebo připojeno k síti, a to tak, že pošle testovací paket a vyčkává na odpověď.

PPP: Point-to-Point Protocol: Metoda přenosu a zabalení IP paketů mezi uživatelem PC a ISP. PPP je obousměrný protokol, který se přenáší přes sériové rozhraní.

Proxy: Zařízení, které uzavírá přímé spojení z vnější sítě (WAN) do vnitřní sítě (LAN). Všechny přenosy musí projít přes proxy, aby se dostaly do nebo ven z LAN. Vnitřní adresy zařízení v LAN si díky této funkci uchovávají soukromí.

PSTN: Veřejná telefonní spojovací síť.

PVC: Permanent Virtual Circuit: Software, který definuje logické spojení v síti. Virtuální okruh, který je uživateli dostupný permanentně.

RG: Resident Gateway: Univerzální označení routeru. Někdy se taky můžete setkat v textu s označením „router" nebo „ADSL2/2+ modem/router". Tyto pojmy jsou synonyma.

RIP: Routing Information Protocol: Řídící protokol, který zajišťuje, aby všichni hostitelé v příslušných sítích sdíleli ty samé informace o směrových cestách. V RIP hostitelský počítač zašle jeho celkovou směrovací tabulku do jiného hostitelského počítače každých X sekund, kde X značí dobu cyklu. Přijímací hostitelský počítač bude střídavě opakovat ten samý proces zasíláním té samé informace do jiného hostitelského počítače. Tento proces se opakuje tak dlouho, dokud všechny hostitelské počítače v dané síti nesdílí ty samé směrovací informace.

RIPv1: RIP Version 1: Jeden z prvních dynamických směrovacích protokolů, které byly použity v Internetu. RIPv1 byl vyvinut proto, aby distribuoval informace o schopnostech dosahu sítě pro to, co dnes považujeme za jednoduché topologie.

RIPv2: RIP Version 2: Sdílí ty samé základní koncepty a algoritmy jako masky podsítě, autorizaci a externí směrovací tag, další hop adresy a hromadné rozesílání dat (multicasting) jako doplněk k volnému šíření dat (broadcasting).

Router Mode: Mód směrovače: Směrovací mód se používá, když je více než jeden PC připojen do strany LAN Ethernetu a/nebo USB portu. ADSL WAN přístup má tedy možnost sdílet s vícenásobnými uzly v LAN. Překlad síťové adresy (NAT) má podporu, tudíž jedna IP adresa ze strany WAN se může sdílet mezi vícenásobnými zařízeními ze strany LAN. DHCP se používá proto, aby sloužil každému zařízení ze strany LAN a IP adresám.

RTP: Protokol pro přenos dat v reálném čase (Real-time Transport Protocol)

SIP: Protokol pro sestavení, dohled a rozpad spojení (Session Initiation Protocol)

SNAP: SubNetwork Attachment Point.

SNMP: Simple Network Management Protocol: Používá se na to, aby řídil správu sítě a monitoroval zařízení na síti. SNMP je formálně popsáno v RFC 1157.

SNR: Signal-to-Noise Ratio: SNR je výpočtový poměr užitečného signálu a šumu měřeného v decibelech. Čím je poměr větší, tím je signál kvalitnější.

Subnet Mask: Maska podsítě: Zkratka pro SUBNETwork Mask, maska podsítě je metoda používaná IP protokolem na filtrování zpráv do příslušné části sítě, zvané jako podsíť. Maska podsítě se skládá z binární šablony, která se ukládá v klientském počítači, serveru nebo routeru. Tato šablona se srovnává s příchozími IP adresami, aby se určilo, zda se má paket přijmout nebo odmítnout.

TCP: Transfer Control Protocol: Pracuje dohromady s Internetovým protokolem, rozesílá data mezi počítači přes Internet. TCP udržuje stopy paketů a zajišťuje jejich účelné směrování.

TFTP: Trivial File Transfer Protocol: Jednoduchá verze FTP protokolu, který nemá autorizační heslo nebo cílovou konstrukční kapacitu.

Trellis Code: Pokročilejší metoda FEC (Oprava chyb při odesílání - Forward Error Correction). V případě, že je tato metoda aktivována, poskytuje lepší kontrolu chyb, ale za cenu pomalejšího přenosu paketu. V opačném případě, tj. že Trellis Code je vypnut, zvýší se přenos paketů, ale se sníženou kontrolou chyb.

TTL: Time To Live: Hodnota v IP paketu, která ukazuje, zda se paket šířil sítí příliš dlouho a měl by být vyřazen. UBR: Unspecified Bit Rate: Mód přenosu, ve kterém se přenáší obvykle soubor, email apod.. UBR se může lišit od typu dat.

USB: Universal Serial Bus: Standardní rozhraní mezi počítačem a periferními zařízeními (tiskárna, externí zařízení, digitální kamery, scannery, zařízení pro síťové rozhraní, modemy atd.), které umožňují přenos o rychlosti o 12Mbps.

UDP: User Datagram Protocol: Protokol, který se používá místo TCP, a to v případě, kdy není vyžadován spolehlivý příjem. Na rozdíl od TCP, UDP nevyžaduje od příjemce úvodní komunikaci (handshake). UDP zasílá pakety v jednosměrném přenosu.

VAD: Detektor hlasové aktivity (Voice Activity Detector)

VoIP: Přenos hlasu internetovým protokolem (Voice over Internet Protocol)

VBR-nrt: Variable Bit Rate non real time: Přenos buňky s VBR-nrt závisí na jistých kritériích.

VC: Virtual Circuit: Virtuální obvod je obvod v síti, který se jeví jako fyzické přerušení cesty. Ve skutečnosti je to řízený soubor zdrojů obvodu, které umístňují specifické obvody tak, aby uspokojily požadavky na putování dat v síti.

VCI: Virtual Channel Identifier: Virtuální kanál, který se identifikuje pomocí zvláštní číselné tag, Ta se vyznačuje 16-bitovým polem v hlavičce buňky ATM. Účelem tohoto virtuálního kanálu je stanovení místa, kam by buňka měla cestovat.

VC-Mux: Virtual Circuit based Multiplexing: Ve virtuálním obvodu založeném na multiplexování je sdružený protokol sítě jasně identifikován pomocí VC (virtuálního obvodu), který je připojen ke dvěma stanicím ATM (každý protokol musí být převeden odlišnými VC).

VPI: Virtual Path Identifier: Virtuální cesta pro směrování buněk, které jsou označeny osmibitovým polem v ATM hlavičce buňky.

WAN: Wide Area Network: WAN pokrývá rozsáhlou geografickou oblast telekomunikačních sítí.

Výhradní dovozce ADSL zařízení WELL pro ČR a SR:

JOYCE ČR, s.r.o., Venhudova 6, 614 00 Brno

www.joyce.cz e-mail: support@joyce.cz

U PŘÍPADNÝCH DOTAZŮ NA TECHNICKOU PODPORU VŽDY UVÁDĚJTE:
TYP ZAŘÍZENÍ, SÉRIOVÉ ČÍSLO (S/N) A NÁZEV FIRMY, KDE JSTE ZAŘÍZENÍ ZAKOUPILI.