

ASUS AAM6310EV

ADSL Ethernet Modem/Router

Uživatelská příručka



OBSAH

1	INSTALACE	2
1.1	VLASTNOSTI VÝROBKU	2
1.2	OBSAH BALENÍ	3
1.3	POPIS LED DIOD A KONEKTORŮ MODEMU/ROUTERU	4
1.4	ZAPOJENÍ ADSL MODEMU/ROUTERU	5
1.5	KONFIGURACE POČÍTAČE	7
1.5.1	Windows XP	7
1.5.2	Windows 95, 98	9
1.5.3	Windows NT 4.0 Workstation	10
1.5.4	Windows 2000	11
1.5.5	Windows ME	12
1.5.6	Přidělení statického internetového nastavení	12
1.5.7	Konfigurace počítače připojeného přes USB port	13
1.6	PŘÍSTUP K WEBOVÉ KONFIGURACI	18
2	KONFIGURACE PŘES WEBOVÉ ROZHRAŇÍ	19
2.1	HOME	19
2.1.1	Home	19
2.1.2	WAN Configuration	24
2.1.3	LAN Configuration	26
2.1.4	ADSL	30
2.1.5	Diagnostics	32
2.2	CONFIGURE	33
2.2.1	IP Route	34
2.2.2	DHCP Mode	38
2.2.3	DHCP Server	41
2.2.4	DHCP Relay	47
2.3	SERVICES	49
2.3.1	NAT	49
2.3.2	RIP	54
2.3.3	IP Filter	58
2.3.4	Firewall	66
2.3.5	DNS Relay	69
2.4	ADMIN	72
2.4.1	User Config - Uživatelská konfigurace	72
2.4.2	Commit & Reboot	73
2.4.3	Image Upgrade	75
2.4.4	Alarm	77
2.4.5	Port Settings	78

1 INSTALACE

1.1 VLASTNOSTI VÝROBKU

ADSL/Ethernet modem/router poskytuje „trvalé“, rychlé připojení k Internetu. Technologie ADSL je schopna přenášet data po standardních telefonních linkách více než 100krát rychleji než běžné analogové modemy bez přerušení telefonního provozu.

Kterým standardům ADSL vyhovuje

Technologie DMT (Discrete multi-tone) byla přijata ANSI, ETSI a ITU.

Podpora ATM

ATM AAL5

Vícenásobné permanentní virtuální okruhy (PVCs – Permanent Virtual Circuits)

RFC 1483 Bridging a routing

RFC 2364 PPP po ATM

RFC 2516 PPP po Ethernetu

Podpora networkingu

IEEE802.1d Transparentní bridging

DHCP Server, DNS Relay a IGMP

RIP-1, RIP-2 a statické směrování

NAT a firewall

Správa

Konfigurace přes webové rozhraní

Firmware s možností upgradu

Fyzické rozhraní

Jeden port RJ-45 pro 10/100 ethernetové připojení

Jeden port RJ-11 pro připojení linky ADSL

Jeden port USB (volitelně)

Rozměry

Výška: 27,2 mm

Šířka: 132 mm

Hloubka: 108 mm

Hmotnost: 260g

Z hlediska provozu elektronických zařízení vyhovuje

FCC Class 15 Class B

FCC část 68

UL – 1950

CE

1.2 OBSAH BALENÍ

Ujistěte se, že balení obsahuje všechny následující položky:

- ADSL Ethernet modem/router
- Síťový adaptér 15 V AC
- Telefonní kabel (konektory RJ-11)
- Síťový kabel (konektory RJ-45)
- USB kabel
- Rozbočovač (Splitter)
- CD s instalačními postupy, manuály a USB ovladačem
- Rychlo-instalační příručku
- Dokumenty (Potvrzení o shodě, ...)

Budou-li některé položky poškozené nebo chybět, kontaktujte Vašeho prodejce.

1.3 POPIS LED DIOD A KONEKTORŮ MODEMU/ROUTERU

Přední panel (LED diody):



Signalizace LED při normálním provozu:

Název	Barva	Stav	Popis
POWER	zelená	svítí	Zařízení je zapnuto
		nesvítí	Zařízení je vypnuto
STATUS	zelená	svítí	Modem navázal spojení s poskytovatelem
		bliká	Modem navazuje spojení s poskytovatelem
		nesvítí	Spojení není aktivní
LINE (WAN)	zelená	Bliká	Přenos dat mezi modemem a poskytovatelem
		nebliká	Nejsou přenášena žádná data (po ADSL)
PC (LAN)	zelená	svítí	Modem je propojen s PC nebo sítí
		bliká	Probíhá přenos dat mezi modemem a PC nebo sítí
		nesvítí	Modem není propojen s PC ani sítí
USB	zelená	svítí	Modem připojen k PC přes USB port
		bliká	Probíhá přenos dat po USB mezi modemem a PC
		nesvítí	Připojení přes USB je neaktivní nebo není nainstalován USB driver

Zadní panel (konektory):



LINE – pro připojení ADSL linky z rozbočovače (splitteru)

RESET-DEFAULT - tlačítko pro uvedení modemu/routeru zpět do továrního nastavení

CONSOLE – konektor sloužící pouze pro účely výrobce

LAN – pro připojení Ethernet kabelem k síťové kartě počítače nebo na Switch nebo HUB

USB – pro připojení k počítači pomocí USB portu

POWER – pro připojení napájecího zdroje

1.4 ZAPOJENÍ ADSL MODEMU/ROUTERU

Požadavky:

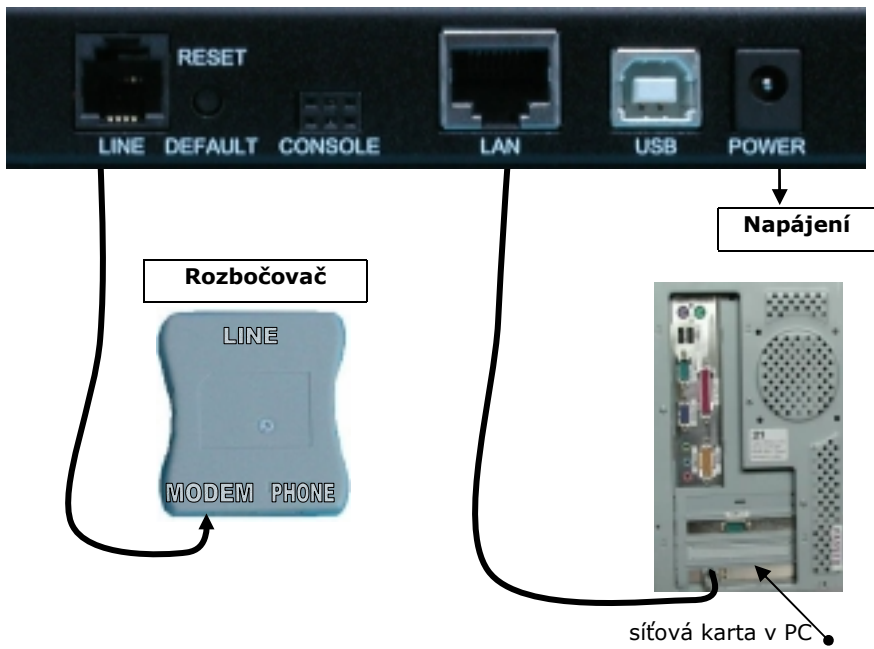
- Musíte mít korektně nainstalovanou síťovou kartu ve Vašem počítači.
- Správně nastaven protokol TCP/IP (viz. kapitola 1.5).
- Připojte správně kabely.

Postup zapojení ADSL Modemu/Routeru:

Ethernetovým kabelem (modrý 8-žilový kabel o délce 2 metry) propojte ASUS modem/router (zdířka „LAN“ na zadní straně) se síťovou kartou vašeho počítače.

Zdířku „LINE“ na zadní straně routeru propojte telefonním kabelem (bílý 4-vodičový plochý kabel) se zdířkou „MODEM“ na rozbočovači.

Napájecí zdroj zasuňte do elektrické zásuvky (230V, 50Hz) a konektor zdroje připojte do zdířky „POWER“ na ASUS modemu/routeru.



Celkové schéma zapojení:



1.5 KONFIGURACE POČÍTAČE

V této části najdete pokyny jak nastavit Vaše počítače, aby spolupracovaly s ADSL/Ethernet routrem. Seznamte se s níže uvedeným nastavením a potom přejděte k některé z dalších částí, kde je uveden podrobný návod na konfiguraci pro každý operační systém.

Než začnete

Standardně ADSL/Ethernet 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 s příslušným ovladačem.

Postupujte podle instrukcí odpovídajících instalovanému operačnímu systému.

1.5.1 Windows XP

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

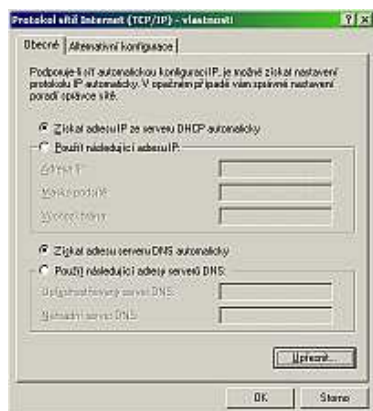
1. Klikněte na tlačítko Start systému Windows a potom na **Ovládací panel**.
2. Poklepejte na ikonu Síťová připojení.
3. V oddíle „LAN nebo vysokorychlostní Internet“ klikněte pravým tlačítkem na ikonu odpovídající vaší síťové kartě a vyberte **Vlastnosti**. Viz. obrázek napravo. (tato ikona je často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

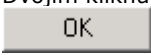


4. Přesvědčte se, že je zaškrtnuto políčko vedle protokolu TCP/IP a klikněte na tlačítko Vlastnosti.



5. Zde zvolte možnosti **Získat IP adresu ze serveru DHCP automaticky** a **Získat adresu serveru DNS automaticky**.



6. Dvojitým kliknutím na tlačítko  potvrďte a uložte provedené změny.
Budete vyzváni k restartování Windows.
7. Klikněte na **Ano**.



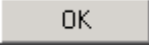
Postup nastavení TCP/IP protokolu je v ostatních OS obdobný, jen v ostatních OS Windows se mohou lišit okna Vlastnosti TCP/IP protokolu.

1.5.2 Windows 95, 98

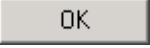
Nejprve zkontrolujte, jestli je instalován IP protokol a pokud není, nainstalujte jej:

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 , čímž se vrátíte do dialogu síť a zde opět klikněte na .

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

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

V dalších krocích nastavíme počítač, aby akceptoval IP informace z ADSL/Ethernet modemu/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. Dvojitým kliknutím na  potvrďte a uložte provedené změny.

Budete vyzváni k restartování Windows.

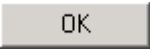
14. Klikněte na **Ano**.

1.5.3 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.

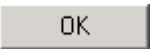
Pod záložkou Protokoly najdete seznam instalovaných síťových protokolů. Obsahuje-li položku TCP/IP, potom byl již protokol nainstalován. Můžete pokračovat od bodu 9.

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

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 , budete-li vyzváni k restartu počítače.

Nyní nastavíme počítač, aby akceptoval IP informace z ADSL/Ethernet modemu/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. Dvojitým kliknutím na tlačítko  potvrďte a uložte provedené změny a zavřete Ovládací panel.
-

1.5.4 Windows 2000

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

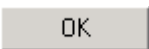
1. Klikněte na tlačítko Start systému Windows, ukažte na **Nastavení** a klikněte na **Ovládací panel**.
2. Poklepejte na ikonu Síťová a telefonická připojení.
3. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na ikonu Připojení k místní síti a vyberte **Vlastnosti**.

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.

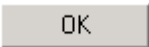
4. Není-li mezi instalovanými komponentami protokol TCP/IP, klikněte **Nainstalovat...**
5. V dialogu Vybrat typ síťové součásti vyberte **Protokol** a klikněte na **Přidat...**

6. Zvolte **Protokol sítě Internet (TCP/IP)** a poté klikněte na .

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

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

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

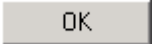
8. V Ovládacím panelu poklepejte na ikonu Síťová a telefonická připojení.
9. V okně Síťová a telefonická připojení klikněte pravým tlačítkem na ikonu Připojení k místní síti a vyberte **Vlastnosti**.
10. Ve vlastnostech Připojení k místní síti vyberte **Protokol sítě Internet (TCP/IP)** a opět klikněte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

1.5.5 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 .

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

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

Nyní nakonfigurujeme počítač, aby akceptoval IP informace z ADSL/Ethernet modemu/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  potvrďte a uložte provedené změny a zavřete Ovládací panel.

1.5.6 Přidělení statického internetového nastavení

V některých případech možná nebudete chtít, aby IP adresy přiděloval ADSL modem/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/Ethernet modemu/routeru. Ve výchozím stavu má modem/router pro tento port nastavenou adresu 10.0.0.138. (Tuto hodnotu můžete změnit, případně ji může změnit Váš ISP. Viz Konfigurace LAN a USB portů, odstavce 2.1.3).
- 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 запиšte 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/Ethernet modemu/routeru. Pokud přidělujete ručně IP informace všem PC ve Vaší síti, můžete postupovat podle pokynů v části Konfigurace LAN a USB portů (odstavec 2.1.3) a nastavit IP adresy těchto portů na patřičné hodnoty.

1.5.7 Konfigurace počítače připojeného přes USB port

Je-li ADSL/Ethernet modem/router vybaven USB portem pro připojení k počítači se stejným typem portu, musíte na tomto počítači instalovat vhodný USB ovladač, který zajistí ethernetovou komunikaci přes USB rozhraní mezi ním a modemem/routerem.

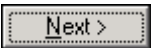
Konfigurace počítače s USB se skládá ze dvou kroků:

- V prvním kroku nainstalujete USB ovladač na PC (pro OS Windows 98SE/ME/2000/XP).
- Ve druhém kroku nastavíte konfiguraci IP vlastností.

1. krok - Instalace USB ovladače. Postupujte podle následujících pokynů:

1. Ujistěte se, že USB kabel není připojen k počítači ani k ADSL modemu/routeru. Instalační program Vás k připojení kabelu vyzve ve vhodnou chvíli sám.
2. Instalační CD s ovladači vložte do počítače s USB portem, ke kterému budete chtít připojit modem/router.
3. Automaticky se spustí instalační průvodce. Pokud tomu tak nebude, v adresáři pro USB ovladač (driver) vyhledejte soubor *setup.exe* a poklepejte na něj. Tím se spustí instalace. Zobrazí se uvítací dialog.

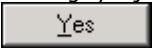


4. Klikněte na tlačítko , čímž se začne instalační proces kopírováním souborů.



Zatímco program hledá hardware USB portu, zobrazí se dialog Instalátoru ADSL. Po několika vteřinách se objeví další dialog, který Vás vyzve k připojení kabelu.

The DSL Installer is searching for installed hardware. If your modem is not yet plugged in to your computer, please plug it in now.

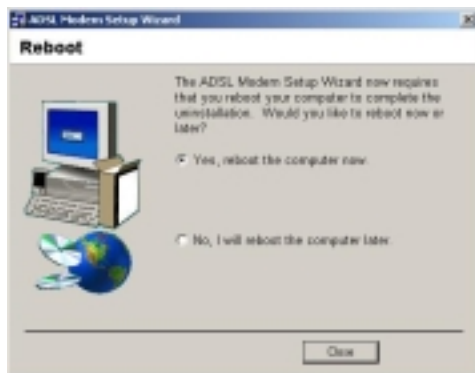
5. Připojte kabel k počítači a modemu/routeru. USB kabel, který je součástí dodávky má na jednom konci plochý konektor (Typ A) a čtverhanný konektor (Typ B) na konci opačném. Plochý konektor patří na stranu PC a druhý konektor se připojuje do modemu/routeru. Po připojení kabelu se krátce zobrazí zpráva, že systém našel nový hardware.
6. Zobrazí-li se dialog týkající se digitálního podpisu společnosti Microsoft, klikněte na .



7. Dokončete instalaci kliknutím na tlačítko .



Ve Windows 98SE/ME pro dokončení instalace je nutné restartovat počítač. Budete k tomu vyzváni následujícím oknem.



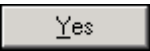
Po novém startu počítače se ujistěte, že v nabídce Start systému Windows přibyla položka Instalátor GlobeSpan:

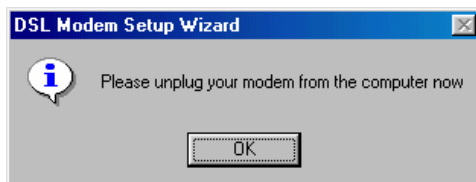
8. Klikněte na tlačítko Start, ukažte na **Programy – DSL Modem** a klikněte na **DSL Status**. Měl by se zobrazit dialog Instalátoru DSL Modemu. Tento krok slouží pouze k ověření.



Odinstalace ovladače:

Před odinstalováním ovladače, neodpojujte USB kabel ze zařízení

1. Klikněte na tlačítko Start, ukažte na **Programy – DSL Modem** a klikněte na **Uninstall**.
2. Klikněte na  pro odebrání ovladače
3. Po zobrazení níže uvedeného okna, odpojte USB kabel ze zařízení a klikněte na OK.



4. Označte **Yes, reboot the computer now** a klikněte na **Close** pro dokončení odebrání ovladače.



2. krok - Konfigurace IP vlastností na PC s USB.

Když byla dokončena instalace USB ovladače, musíte ještě PC nastavit tak, aby jej jeho IP vlastnosti přiřadily do téže podsítě jako USB port modemu/routeru. Můžete to udělat jedním ze dvou způsobů:

- Modem/Router byl nakonfigurován tak, aby počítači s USB portem přidělil vhodnou IP Adresu. Budete-li chtít toto automatické přidělování IP adresy (DHCP server) používat, musíte nastavit PC s USB, 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:
 - o V okně Síťová a telefonická připojení vyberte ikonu symbolizující nové USB připojení (ne to se síťovou kartou!). Když si zobrazíte vlastnosti

tohoto připojení, měl by se zobrazit dialog s podobným obsahem:
Připojit pomocí: GlobeSpan USB IAD LAN Modem #n.

- o USB port modemu/routeru je nastaven s IP adresou 10.0.0.139 a maskou 255.255.255.0.

Tudíž Váš počítač musí být nakonfigurován takto:

IP adresa: 10.0.0.n, kde n je číslo od 2 do 254 (vyjma 139)

Maska podsítě: 255.255.255.0

Výchozí brána: 10.0.0.139

1.6 PŘÍSTUP K WEBOVÉ KONFIGURACI

Tento ADSL modem/router umožňuje provádět nastavování pomocí webového rozhraní za využití jakéhokoliv webového prohlížeče např. Microsoft Internet Exploreru.

1. Spustíte Internetový prohlížeč.
2. Do řádku pro vkládání webových adres zadejte IP adresu modemu/routeru (10.0.0.138).
3. Zadejte přihlašovací jméno (**adsl**) a heslo (**adsl1234**) pro přístup do webového konfiguračního rozhraní modemu/routeru. (viz. obrázek)



2 KONFIGURACE PŘES WEBOVÉ ROZHRANÍ

2.1 HOME

Popis systému

Software Configuration Manager je na ADSL/Ethernet modemu/routeru již předinstalován. Dovoluje Vám konfigurovat toto zařízení tak, aby pro vaši síť zajistilo připojení k Internetu a některé další služby. Pomocí Configuration Manageru můžete měnit nastavení připojení k Internetu, monitorovat výkonnost DSL spojení a konfigurovat rozhraní a protokoly, jimiž modem/router komunikuje s Vaší sítí a Vaším poskytovatelem připojení (Internet Service Provider – ISP).

Configuration Manager Vám dále umožňuje nastavit pro Vaši síť řadu dalších služeb, např. DHCP pro centrální přidělování IP adres v rámci celé Vaší sítě, NAT, která zajistí, aby všechny počítače v síti mohly využívat jedinou veřejnou IP adresu, ochranu typu firewall a jiné.

2.1.1 Home

Home

Configure

Services

Admin

Home | WAN Config | LAN Config | ADSL | Diagnostics

Device		ADSL			
S/W Version:	138309B-CR-CzechTelecom-eu01	Operational Status:		Startup Handshake	
Up Time:	0:36:27	ADSL Version:		V1.4.2	
Time:	Thu Jan 01 00:36:27 1970	Standard:		0x0	
Time Zone:	GMT	Up		Down	
Daylight Saving Time:	OFF	Speed	Latency	Speed	Latency
		0 Kbps	-	0 Kbps	-

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoA	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	8/48	

LAN Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	10.0.0.138	255.255.255.0	-	Auto	Auto	
usb-0	-	10.0.0.139	255.255.255.0	-	-	-	

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	inside						
ppp-0	outside						
usb-0	inside						

Funkční uspořádání

Funkce Configuration Manageru jsou uspořádány do jednotlivých kategorií. Přístup k určité kategorii funkcí získáte kliknutím na patřičnou záložku v horní části každé stránky. Každá ze záložek uvádí dostupné funkce v horizontální nabídce nahoře na stránce. Příslušné možnosti konfigurace zobrazíte kliknutím na odpovídající položku z nabídky.

Pro každou funkci se zobrazuje samostatná stránka. Po kliknutí na novou záložku se standardně zobrazuje funkce uvedená jako první zleva.

Často používaná tlačítka

Submit

Ukládá do dočasné paměti systému změny, které jste provedli na aktuální stránce. Návod na trvalé uložení provedených změn najdete v odstavci 2.4.2.

Refresh

Obnoví obsah aktuální stránky s novým nastavením nebo čerstvými statistickými údaji.

Clear

Na stránkách, kde se zobrazují kumulované statistické hodnoty, toto tlačítko obnoví výchozí hodnoty.

Help

Zobrazí nápovědu pro aktuální téma v novém okně prohlížeče. Nápověda je dostupná z kterékoli stránky hlavních témat.

Domovská stránka a tabulka parametrů systému

Domovská stránka se zobrazí, když spustíte program. Je to jedna z pěti možností dostupných ze záložky Home. Tabulka parametrů systému představuje jeho aktuální konfiguraci. Všimněte si, že některé z hodnot jsou zároveň odkazy na stránky, kde se hodnota nastavuje.

Následující tabulka popisuje jednotlivé části tabulky parametrů, kde je to žádoucí, odkazuje na další témata manuálu.

Nadpis tabulky	Popis
Device (zařízení)	Poskytuje základní informace o hardwaru zařízení a verzi firmwaru, dobu provozu zařízení (od posledního nahrání firmwaru) a přednastaveném režimu provozu.
DSL	Zobrazuje provozní stav a výkonové statistiky DSL připojení. Po kliknutí na DSL v nadpisu lze zobrazit další údaje, viz odstavce 2.1.4.

WAN Interfaces	Zobrazuje názvy a různá nastavení rozhraní, která komunikují s Vaším ISP prostřednictvím DSL, např. rozhraní PPP, EOA nebo IPoA. Ačkoli máte pouze jeden fyzický DSL port, softwarově lze konfigurovat více rozhraní, která jej budou využívat. Kliknutím na jméno rozhraní se dostanete na konfigurační jeho stránku nebo zobrazíte Podrobný přehled funkcí, který nabízí podobné možnosti. Pro každé rozhraní by se mělo zobrazit jméno ve sloupci „Interface“, jako např. ppp-0. Po kliknutí na toto jméno si můžete prohlédnout nebo upravit nastavení ATM VC, které toto rozhraní používá.
LAN Interfaces	Zobrazuje názvy a různá nastavení rozhraní zařízení, které komunikuje přímo s Vaší sítí. Obsahuje většinou alespoň jedno rozhraní typu Ethernet nazvané <i>eth-0</i> a může obsahovat i jedno USB rozhraní s názvem <i>usb-0</i>. Po kliknutí na název rozhraní se zobrazí konfigurační stránka lokální sítě – viz odst. 2.1.3.
Service Summary (přehled služeb)	Zobrazuje libovolnou z následujících služeb, které ADSL/Ethernet modem/router plní v rámci správy Vaší sítě: • Překlad privátních IP adres na Vámi přidělenou veřejnou IP Adresu (NAT). • Nastavení pravidel filtrování, která zajistí přijmutí nebo odmítnutí příchozích či odchozích dat (IP Filter) • Umožňuje komunikaci router - router (RIP). • Umožňuje dynamické přidělování IP adresy buď Vaším ISP pro počítače ve Vaší síti (DHCP relay), nebo serverem, který je součástí zařízení (DHCP server) a přiděluje IP adresy do Vaší sítě, popř. jiným počítačem v síti, na němž běží DHCP server, který přiděluje IP adresu zařízení přes jeho LAN port (DHCP client). • Předávání zpráv založené na protokolu Internet Group management Protocol (IGMP – nelze konfigurovat).

Změna systémových informací

Zařízení si zaznamenává údaje o datu a času, které využívá pro výpočty a různé reporty týkající se výkonu.



Změna nastavení data anebo času zařízení nemá žádný vliv na nastavení stejných parametrů na Vašich PC.

Provedení změny data a času v zařízení:

1. V dolní části domovské stránky klikněte na tlačítko **Modify**.
V novém okně prohlížeče se zobrazí stránka modifikace systému.
2. Z rozbalovacího seznamu vyberte volbu new date and time.

3. Do příslušného pole zadejte zkratku Vašeho časového pásma.
4. Zadejte host name (tzn. jméno zařízení) a název domény (tj. název sítě, do níž je zařízení připojeno).
5. Klikněte na tlačítko **Submit**. Zobrazí se stránka potvrzující provedené změny.
6. Klikněte na tlačítko **Close** a vrátíte se na stránku parametrů systému.
7. Klikněte na záložku Admin a z nabídky funkcí vyberte **Commit & Reboot** (provést a znovu natáhnout systém).
8. Po kliknutí na tlačítko **Commit** se změny uloží trvale do paměti.

Bezpečnostní protokoly CHAP/PAP

Ve Vašem zařízení je implementována autodetekce bezpečnostních protokolů CHAP / PAP, proto není nutné jakkoliv měnit jejich nastavení. Budete-li potřebovat se přesvědčit, jaký protokol je aktuálně nastaven, zjistíte to následujícím způsobem:

1. Na záložce **Home** klikněte na odkaz **ppp-0** ve sloupci Interface.

WAN Interfaces							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoA	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	8/48	

2. V následujícím okně **Point-to-Point (PPP) Configuration** klikněte na , abyste se dostali do podrobného seznamu nastavení, kde je vidět, jaký protokol je aktuálně nastaven.

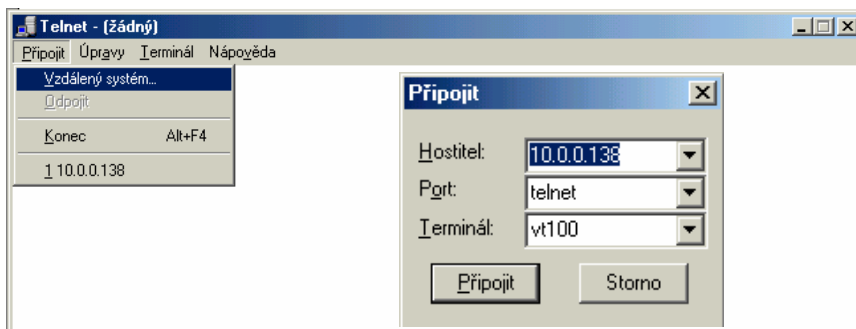
PPP Interface - Detail

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	PPPoA
Use DHCP:	Disable
Use DNS:	Enable
Default Route:	Enable
Oper. Status:	Link Down
Last Fail Cause:	VC down
PPP IP Status	
WAN IP Address:	0.0.0.0
Gateway IP Address:	0.0.0.0
DNS:	0.0.0.0
SDNS:	0.0.0.0
Security Information	
Security Protocol:	CHAP
Login Name:	adsl

Close
Refresh
Help

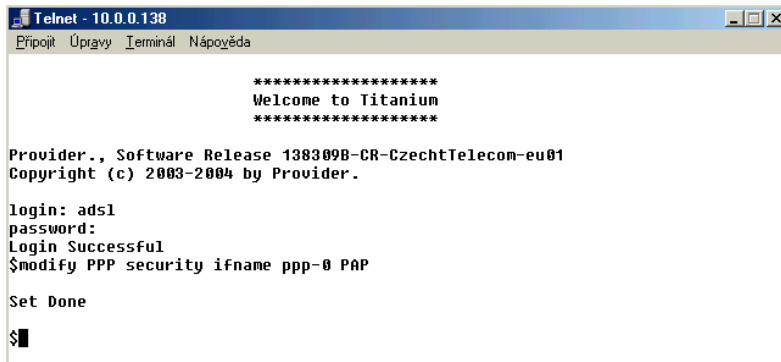
Budete-li potřebovat změnit protokol ručně, lze to provést pomocí Telnetu (je součástí OS Windows) dle následujícího návodu:

- 1) Spustíte si službu Telnet, kterou připojíte na IP adresu routeru.



- 2) Po vložení uživatelského jména a hesla (např.: adsl / adsl1234) vložte příkaz pro změnu protokolu CHAP/PAP.

- Změna protokolu na PAP:



- Změna protokolu na CHAP:

```

Telnet - 10.0.0.138
Připojit Úpravy Terminál Nápověda

*****
Welcome to Titanium
*****

Provider., Software Release 138309B-CR-CzechTelecom-eu01
Copyright (c) 2003-2004 by Provider.

login: adsl
password:
Login Successful
$modify PPP security ifname ppp-0 CHAP

Set Done

$

```

2.1.2 WAN Configuration

Home
Configure
Services
Admin

Home | WAN Config | LAN Config | ADSL | Diagnostics

Quick Configuration

Use this page to quickly configure the system.

ATM Config		Option Function	
ATM Interface:	0	IGMP:	Disabled
Encapsulation:	PPPoA VC-Max	NAT:	Enabled
VPI:	0	Default Route:	Enabled
VCI:	48	Gateway IP Address:	
IP Address:		PPP	
Subnet Mask:		Username:	adsl
QoS Type:	UBR	Password:	****
PCR:	2000	Status:	Start
		Use DNS:	☒ Enable ☐ Disable
		DNS	
		Primary DNS Server:	
		Secondary DNS Server:	

Submit
Delete
Cancel
Help

Rychlá konfigurace

Stránka Rychlá konfigurace obsahuje nastavení, která budete potřebovat upravit, až budete připravovat nový ADSL/Ethernet modem/router pro uvedení do provozu. Některé údaje a nastavení Vám bude muset sdělit Váš ISP.

Pokud se Vám stránka pro rychlou konfiguraci nezobrazila, klikněte na záložku Home a poté na **WAN Config**. Následující tabulka poskytuje stručné vysvětlení jednotlivých parametrů. Některá z těchto nastavení jsou podrobněji vysvětlena v jiných tématech napovědy, k nimž je níže uveden odkaz.

- **ATM Interface:** Vyberte ATM rozhraní, které budete chtít používat (obvyčně atm-0). Systém lze konfigurovat pro více ATM rozhraní, pokud využíváte více různých služeb Vašeho ISP.
- **Operational Mode.** Tento parametr povoluje nebo zakazuje internetové a směrovací funkce zařízení. Je-li nastaven na hodnotu „No“, zařízení nemůže plnit funkci zprostředkovatele připojení Vaší sítě k Internetu.
- **Encapsulation:** Tento parametr určuje typ datového spojení pro komunikaci s Vaším ISP.
- **VPI and VCI:** Tyto parametry udávají unikátní datovou cestu, kterou používá modem pro komunikaci s Vaším ISP.
- **Bridge:** Tento parametr povoluje nebo znemožňuje funkci mostu mezi Vaším zařízením a Vaším ISP. Váš ISP může v parametrech nastavení komunikace uvádět pro tuto funkci označení jako nař. „RFC 1483“ nebo „Ethernet over ATM“.
- **IGMP:** Povoluje nebo zakazuje Internet Group Management Protocol, který někteří ISP využívají pro dálkovou konfiguraci Vašeho zařízení.
- **IP Address and Subnet Mask:** Jestliže Vám ISP přidělil veřejnou IP adresu, запиšte ji včetně masky podsítě do příslušných políček. (Pozn.: Při určitých konfiguracích se veřejná IP adresa zadává na Vašem PC a ne na ADSL/Ethernet modemu/routeru. Tento případ konzultujte s Vaším ISP).
- **Default Route:** Toto nastavení, pokud je povoleno, udává, že výše uvedená IP adresa je výchozím směrem (cestou) pro Vaši lokální síť. Kdykoli se některý z počítačů ve Vaší síti pokusí o přístup k Internetu, budou data odesílána přes toto WAN rozhraní.
- **Gateway IP Address:** Jedná se o IP adresu serveru ISP, na níž je směrováno připojení k Internetu z Vaší sítě.
- **Username and Password:** Zadejte uživatelské jméno a heslo pro přihlášení do sítě ISP. (Pozn.: Nejedná se o uživatelské jméno a heslo, jakým se přihlašujete do programu Configuration Manager routeru).
- **Use DNS:** Pro aktivaci služby DNS forwarding klikněte na *Enable*. Jedná se o službu, která zajišťuje předávání DNS jmen serverů získaných připojením PPP od Vašeho ISP počítačům ve Vaší lokální síti. Tuto volbu lze použít jen pokud zařízení zároveň plní funkci DHCP serveru pro počítače ve Vaší síti. Zvolíte-li *Disable*, budete muset nastavit DNS adresy na každém PC ručně (viz odstavec 2.3.5)
- **Primary/Secondary DNS:** Vložte primární a sekundární IP adresu provozovanou Vaším ISP (viz odstavec 2.3.5).

Pokud jste dokončili zadávání dat anebo výběr z nabízených možností, klikněte na tlačítko **Submit**.

Potom vyberte záložku Admin, vyberte funkci **Commit & Reboot** a klikněte na tlačítko **Commit**, aby se změny uložily trvale.

Můžete také kliknout na tlačítko **Delete**, tím všechny změny v nastavení provedené na stránce Quick Configuration zruší a obnoví se výchozí hodnoty.

2.1.3 LAN Configuration

Home | WAN Config | LAN Config | ADSL | Diagnostics

LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration				
LAN IP Address:	10	0	0	138
LAN Network Mask:	255	255	255	0
IGMP:	☐ Enable ☒ Disable			

USB Configuration				
USB IP Address:	10	0	0	139
USB Network Mask:	255	255	255	0
IGMP:	☐ Enable ☒ Disable			

Submit **Cancel** **Refresh** **Help**

Konfigurace LAN a USB portů

Tento odstavec popisuje, jak se konfiguruje rozhraní na ADSL/Ethernet modemu/routeru, které budou komunikovat s Vaší LAN a počítačem s USB portem.

Připojení přes Ethernet a (nebo) přes USB

Budete-li chtít ADSL/Ethernet modem/router využívat pro více PC z Vaší lokální sítě, musíte je připojit prostřednictvím ethernetového rozbočovače (HUBu) k LAN portu na modem/routeru. Připojujete-li k ADSL/Ethernet modem/routeru jen jeden počítač, můžete jej připojit dvěma způsoby:

- PC můžete připojit přímo do LAN portu modem/routeru.
- Využívá-li PC port USB, můžete jej připojit přímo do USB portu modem/routeru s názvem *usb-0*. Tímto způsobem lze ovšem připojit jen jediný počítač.

Oba porty také můžete využívat současně a připojit lokální síť do LAN portu a jeden samostatný počítač do portu USB.

Každému použitému portu je nutné přidělit jedinečnou IP adresu.

Nastavení IP adresy síťového portu

IP adresa identifikuje LAN port (eth-0) jako uzel Vaší sítě, což znamená, že jeho IP adresa musí spadat do stejné podsítě, jako ostatní PC v síti.



Uzlem sítě je kterýkoliv port v síti, např. LAN port modem/routeru, síťová karta Vašeho počítače apod.

Výchozí nastavení můžete samozřejmě změnit a použít jednu ze skupiny IP adres Vaší sítě.

Jestliže ve Vaší síti používáte dynamické přidělování IP adres DHCP serverem (jiným než v ADSL/Ethernet modem/routeru), můžete modem/router nastavit tak, aby přijal IP adresu přidělenou mu tímto serverem. Podobně, jestliže Váš ISP provozuje službu DHCP pro Vaši síť, můžete nastavit modem/router tak, aby akceptoval IP adresu z DHCP serveru ISP. V tomto režimu se ADSL/Ethernet modem/router chová jako DHCP klient Vašeho DHCP serveru (nebo ISP).



Samotný ADSL/Ethernet modem/router může vykonávat funkci DHCP serveru pro počítače ve Vaší síti. Tento režim je popsán v odstavci Konfigurace DHCP serveru (2.2.3). Nemůže však přidělovat IP adresu svému vlastnímu síťovému portu.

Podle následujících kroků můžete upravit IP adresu síťového portu modemu/routeru nebo jej nastavit jako klienta DHCP:

1. Není-li již zobrazena stránka LAN Configuration, klikněte na záložku LAN v seznamu funkcí. Pak se tato stránka zobrazí. Tabulka síťové konfigurace uvádí následující nastavení:

- **System Mode:** Jedná se předem nastavený režim práce, např. Routing nebo Bridging. Toto nastavení uživatel nemůže změnit.
- **Get LAN Address:** Tento parametr udává, jaký způsobem má síťový port modemu/routeru získat IP adresu:
 - o *Manual* (ručně) znamená, že budete IP adresu zadávat ručně do příslušných políček
 - o *External DHCP Server* znamená, že bude IP adresa přidělena z DHCP serveru ISP dynamicky, vždy když se k ISP připojíte.
 - o *Internal DHCP* vyjadřuje, že budete používat vlastní DHCP server ve Vaší síti, který IP adresu portu přidělí.

Zvolíte-li interní nebo externí DHCP server, bude síťový port modemu/routeru klientem tohoto serveru.

Uvědomte si, že veřejná IP adresa přidělená Vám Vaším ISP není IP adresou Vaší sítě. IP adresa ze skupiny veřejných adres identifikuje WAN (ADSL) port vašeho ADSL/Ethernet modemu/routeru v Internetu.

- **LAN IP Address and Network Mask:** IP adresa a maska pro síťový port.
- **Use DHCP:** Povoluje získávat IP adresu dynamicky ze serveru Vašeho ISP (vzdáleného) nebo ze serveru ve Vaší síti (lokálního). Využijete-li některou z těchto možností, stává se LAN port klientem DHCP jednoho ze serverů. Pokud tuto možnost zakážete, bude modem/router používat dříve zadanou statickou IP adresu trvale.

2. Zadejte do příslušných políček IP adresu a masku a pro parametr Use DHCP zvolte Disabled, popř. povolte vzdálený nebo lokální DHCP server. Při nastavování mějte na paměti:

- **Ruční zadání statické adresy:** Používáte-li ve Vaší síti směrovací služby jako je DHCP a NAT, budete zřejmě používat pevnou IP adresu a masku. Tak bude zajištěno, že budou všechny počítače používat pevné IP adresy při komunikaci s modemem/routrem.

Přidělená IP adresa musí být součástí stejné podsítě, v níž se nacházejí počítače, které mají se síťovým portem modemu/routeru komunikovat (tzn., že část adresy udávající ID sítě a maska podsítě musí být stejná, jako na ostatních PC).

Jestliže změníte IP adresu sítě, budete muset aktualizovat nastavení DHCP, aby adresy, které bude DHCP server dynamicky přidělovat

Vaším počítačem, byly ze stejné podsítě. V odstavci 2.2.3 najdete pokyny jak změnit rozsah dynamicky přidělovaných adres.

- **Povolení DHCP:** Nastavíte-li, aby byl LAN port klientem místního nebo externího DHCP serveru, budou políčka pro síťovou masku nedostupná. Pole pro IP adresu však lze i nyní editovat. Adresa, kterou zde uvedete, se bude používat jako požadavek na DHCP server. Tomu se říká „Konfigurovaná IP adresa“ (Configured IP Address) v programu. Je-li konfigurovaná IP adresa na DHCP serveru nedostupná, přidělí server síťovému portu adresu jinou. I v takovém případě se v tomto poli zobrazuje zadaná (konfigurovaná) IP adresa.

Popis služby DHCP (jak je implementována ve vlastním DHCP serveru modemu/routeru) najdete v odstavci 2.2.2.

3. Klikněte na tlačítko **Submit**.

- Pokud jste změnili IP adresu modemu/routeru z PC, které připojeno ke modemu/routeru síť Ethernet, připojení se ukončí.
- Když změníte IP adresu prostřednictvím PC připojeným přes USB port, objeví se stránka s žádostí o potvrzení změny a připojení zůstane aktivní.
- Pokud jste povolili službu DHCP, vyvolá ADSL/Ethernet modem/router žádost o IP adresu z DHCP serveru. Je-li mu přidělena jiná IP adresa než před tím, současné připojení se přeruší.

4. Je-li to nutné, překonfigurujte počítače, aby je jejich IP adresy zařadily do stejné podsítě, jejíž součástí je síťový port modemu/routeru. Viz Konfigurace TCP/IP na Vašich počítačích (odstavec 1.5).
5. Přihlaste se do programu Configuration Manager zadáním nové IP adresy do adresního řádku vašeho webového prohlížeče.
6. Funguje-li nové nastavení správně, klikněte na záložku Admin a vyberte funkci **Commit & Reboot**.
7. Klikněte na tlačítko **Commit**, aby se změny trvale uložily do paměti.

Nastavení IP adresy USB portu

1. Není-li právě zobrazena stránka LAN Configuration, klikněte na záložku LAN.
Pokud není pod tabulkou LAN Configuration zobrazena tabulka USB Configuration, potom Váš systém nepodporuje USB. V takovém případě se obraťte na Vašeho ISP se žádostí o pomoc.
2. V tabulce USB Configuration zadejte IP adresu a síťovou masku USB portu.

IP adresa musí zařadit USB port do stejné podsítě, jejíž součástí je i počítač připojený přes rozhraní USB. USB počítač a USB port mohou ležet ve stejné podsíti jako síťový port modemu/routeru a k němu připojená PC.

Příklad: LAN port má přidělenou adresu 10.0.0.138 a USB port 10.0.0.139,

potom počítač připojený ke kterémukoli portu musí mít IP adresu z rozsahu 10.0.0.1– 10.0.0.254

3. Klikněte na tlačítko **Submit**.

- Pokud jste změnili IP adresu USB portu z počítače, který je připojen přes USB, spojení se ukončí.
- Jestliže využíváte právě Ethernetové rozhraní, objeví se stránka s výzvou na potvrzení provedených změn a spojení zůstane aktivní.

4. Je-li třeba, překonfigurujte svůj počítač, aby jeho IP adresa odpovídala podsíti, jejíž součástí je USB port modemu/routeru. Viz Konfigurace TCP/IP na Vašem počítači (odstavec 1.5).

5. Spusťte internetový prohlížeč a přihlaste se do programu tím, že do adresního řádku zadáte novou IP adresu USB portu.

6. Funguje-li nastavení správně, přihlaste se do programu Configuration Manager, záložku Admin a klikněte na **Commit and Reboot**.

7. Stiskněte tlačítko **Commit**, aby se změny uložily trvale do paměti.

2.1.4 ADSL

Home | WAN Config | LAN Config | **ADSL** | Diagnostics

ADSL Status

This page displays ADSL Status Information

Refresh Rate: 10 Seconds

Counters	Local		Remote	
	Intrld	Fast	Intrld	Fast
FEC:	0	0	0	0
CRC:	0	0	0	0
NCD:	0	0	0	0
OCD:	0	0	-	-
HEC:	0	0	0	0
SEF:	0	0	0	0
LOS:	0	0	0	0

Failures	Local		Remote	
	NCD	SEF	LOS	LCD
NCD:	0	0	0	0
SEF:	0	0	0	0
LOS:	0	0	0	0
LCD:	0	0	0	0

ADSL Status

Operational Status: Startup Handshake **Loop Stop**

Last Failed Status: 0x0

Startup Progress: 0xA0

Clear ADSL Param Stats Refresh Help

Prohlížení parametrů DSL

Parametry konfigurace a výkonové statistiky DSL spojení ADSL/Ethernet modemu/routeru si můžete zobrazit. Není-li právě zobrazena stránka DSL Status, klikněte na záložku WAN. Stránka DSL se poté zobrazí.

DSL Status

Stránka DSL Status obsahuje aktuální informace o výkonu DSL spojení. Obsah stránky je obnovován v závislosti na nastavení Refresh, z jehož rozbalovacího seznamu si můžete vybrat hodnotu, která vám bude vyhovovat.

V tabulce DSL Status najdete barevnou signalizaci DSL spojení: **červená** – spojení je nečinné, **oranžová** – navazuje se spojení, **zelená** – spojení je aktivní.

DSL spojení můžete přerušit kliknutím na tlačítko **Loop Stop**. Nový start linky provedete kliknutím na **Loop Start**.

I když normálně nebudete potřebovat sledovat ostatní parametry, při odstraňování poruch spojení nebo problémech s výkonem Vám mohou pomoci.

Kliknutím na tlačítko **Clear** se všechny čítače vynulují a kliknutím na **Refresh** se stránka znovu načte s aktuálními hodnotami.

Parametry DSL

Na stránce DSL Status můžete kliknout na tlačítko **DSL Param** a zobrazit údaje o konfiguraci DSL připojení. Tyto údaje nelze měnit.

- Tabulka DSL parametrů obsahuje hodnoty nastavení zadané výrobcem nebo Vaším ISP.
- V tabulce Config Data se objevují různé typy chyb zjištěných na DSL spojení.

DSL Statistics

Na stránce DSL Status můžete kliknout na tlačítko **Stats** a zobrazit provozní statistiky DSL spojení.

Stránka DSL Status obsahuje chybová data vztahující se k posledním 15 minutám provozu, aktuálnímu dni a dni předcházejícímu.

V dolní části stránky je umístěna tabulka, která uvádí podrobné statistické údaje. Kliknutím na patřičný odkaz si můžete zobrazit podrobné údaje v 15 minutových intervalech za posledních 24 hodin. Když např. kliknete na 1-4, zobrazí se šestnáct intervalů (po 15 minutách), což znamená poslední 4 hodiny.

2.1.5 Diagnostics

Home | WAN Config | LAN Config | ADSL | Diagnostics

Diagnostics

This page is used for performing diagnostics on the system.

ATM VC:

Testing Connectivity to modem		
Testing Ethernet connection	UNKNOWN	Help
Testing ADSL line for sync	UNKNOWN	Help
Testing Ethernet connection to ATM	UNKNOWN	Help

Testing Telco Connectivity		
Testing ATM OAM segment ping	UNKNOWN	Help
Testing ATM OAM end to end ping	UNKNOWN	Help

Testing ISP Connectivity		
Testing PPPoE server connectivity	UNKNOWN	Help
Testing PPPoE server session	UNKNOWN	Help
Testing authentication with server	UNKNOWN	Help
Validating assigned IP address 0.0.0.0	UNKNOWN	Help

Testing Internet Connectivity		
Ping default gateway 0.0.0.0	UNKNOWN	Help
Ping Primary Domain Name Server	UNKNOWN	Help
Query DNS for www.yahoo.com	UNKNOWN	Help
Ping www.yahoo.com	UNKNOWN	Help

Použití diagnostiky

Diagnostické funkce mohou provádět řadu testů Vašeho systému a to jak softwarové, tak hardwarové části spojení. Tyto funkce využijete v případě, že budete společně s ISP odstraňovat nějaký problém v připojení.

Při spuštění diagnostického programu postupujte následovně:

1. Není-li zobrazena stránka diagnostiky, klikněte na záložku Home a z nabídky vyberte **Diagnostics**.
2. Z rozbalovacího seznamu virtuálních okruhů zvolte název aktuálního ATM rozhraní, které je pro Vás systém definováno. (ve většině případů se bude jednat o výchozí atm-0).
3. Klikněte na tlačítko  .

Diagnostický program provede sérii testů, která ověří, jestli je připojení modemu/routeru funkční. Tyto testy zaberou jen několik vteřin. Program ohlásí, zda test prošel úspěšně, neúspěšně nebo byl vynechán. Test může být vynechán, pokud diagnostický program zjistí, že příslušné rozhraní nebylo konfigurováno a tedy není co testovat.

V pravém rohu výstupní tabulky lze kliknout na **Help** zobrazit si ke každému testu vysvětlení. Při rozboru výsledku testů diagnostiky je vhodné spolupracovat s poskytovatelem připojení.

2.2 CONFIGURE

Konfigurace IP tras

Pro odesílání dat v síti a do Internetu si můžete definovat specifické trasy (IP Routes). V této části jsou popisovány základní směrovací koncepty a najdete zde návod na vytváření tras.

Pozn.: Většina uživatelů definování IP tras pravděpodobně nebude potřebovat.

2.2.1 IP Route

[Home](#) [Configure](#) [Services](#) [Admin](#)

IP Route | DHCP Mode | DHCP Server | DHCP Relay

IP Route Table

This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
10.0.0.0	255.255.255.0	10.0.0.138	eth-0	Direct	Dynamic	
10.0.0.138	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	
10.0.0.139	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	

[Add](#) [Refresh](#) [Help](#)

Stručný popis směrování v IP sítích

Základní úloha modemu/routeru: Když obdrží data adresovaná pro konkrétní místo určení, kterému dalšímu zařízení je má odeslat? Když definujete IP trasy, vytváříte jakási pravidla, podle nichž se počítač (modem/router) rozhoduje.

Přirovnání IP tras k funkci telefonních ústředen

IP směrování je obdobou úkolu, který řeší telefonní ústředna při přepojování hovorů.

Když vytáčíte dálkový hovor, jste nejprve připojení k ústředně místního telefonního operátora. Všechny Vaše odchozí hovory jdou nejprve do této ústředny. Jestliže tedy právě vytáčený hovor směřuje mimo lokální telefonní uzel, ústředna otevře spojení k nadřazené ústředně, která zajišťuje dálkové hovory. Tato ústředna si „přečte“ směrové telefonní číslo, které jste vytočili a spojí Vás s ústřednou, která obsluhuje příslušný telefonní uzel. Tato další ústředna se podívá na první trojici čísel za číslem telefonního uzlu a spojí Vás s menší lokální ústřednou, která obhospodařuje telefonní stanice s tímto prefixem. Ta se podívá na poslední skupinu číslic voleného čísla a spojí Vás s osobou nebo firmou, kterou voláte.

Podobně, když Váš počítač zahájí internetovou komunikaci, iniciuje např. spojení s webovým serverem, odesílá data, jejichž součástí je IP adresa cílového počítače (=telefonní číslo). Všechny odesílané požadavky jdou nejprve na modem/router Vašeho ISP (=první ústředna). Modem/router si přečte z cílové adresy část, která představuje identifikaci cílové sítě (= číslo telefonního uzlu) a podle něj rozhodne, ke kterému dalšímu modemu/routeru požadavek odešle. Po několika podobných krocích požadavek dorazí ke modemu/routeru cílové sítě, jenž si zjistí z IP adresy identifikaci cílového počítače (= lokální účastnické číslo) a požadavek mu předá.

V obou případech byly požadavky odeslány nejprve stejné ústředně, případně modemu/routeru, které sloužily jako brána k dalším nadřazeným nebo podřízeným zařízením. Žádné jednotlivé zařízení neznalo celou konečnou trasu, ale vždy bylo schopné z určité části cílové adresy, ať se jednalo o telefonní číslo nebo IP adresu, rozhodnout, na které další zařízení má požadavek předat.

Hop a brána

Pokaždé, když jsou data v Internetu předána z jedné adresy na druhou, hovoříme o jednom „hopu“. Hop může představovat přesunutí z jednoho portu na druhý na tomtéž zařízení, přenos na jiné zařízení v rámci jedné sítě nebo přenos na zařízení, které se nachází v některé úplně jiné síti.

Jsou-li přenášena data jedním hopen z jedné sítě do druhé, používají tzv. bránu (Gateway). Brána je IP adresa, která zprostředkovává přístup do jiné sítě, podobně jako telefonní ústředna je branou do určité skupiny telefonních čísel. Když například počítač ve Vaší síti vznesе požadavek na připojení k webovému serveru, na němž jsou provozovány webové stránky firmy, slouží ISP jako brána do Internetu. Jakmile Váš požadavek dosáhne cíle, jiná brána zajistí přístup k webovému serveru společnosti.

Použití IP tras k definování výchozích bran

IP trasy jsou definovány na počítačích, modemových/routerových a ostatních IP zařízeních kvůli tomu, aby bylo jasné, kam má vést další hop, neboli kterou další bránu použít pro předání dat na jejich cestě k cíli.

Není-li pro příslušný cíl definována IP trasa, odešlou se data na tzv. *výchozí bránu* (*Default gateway*). Výchozí brána plní podobnou úlohu jako nadřazená telefonní ústředna. Možná nebude schopna navázat spojení přímo s cílovým účastníkem, ale bude vědět, na jaké další zařízení požadavek odeslat, aby se data dostala efektivně k cíli. Když nemůže posoudit, které z navazujících zařízení zajistí nejvhodnější hop (protože nebyla předem definována trasa), pak další zařízení opět postoupí data na svou výchozí bránu. Nakonec některé další

nadřazené zařízení již bude schopno využít přednastavenou IP trasu a odeslat data k jejich cíli.

Budu potřebovat IP trasy?

Většina uživatelů nikoliv. V běžné domácí nebo malé podnikové síti budou existující trasy dané adresami výchozích bran pro Vaše počítače a pro ADSL/Ethernet modem/router dostatečné k zabezpečení vhodných tras pro Váš veškerý internetový provoz.

- Výchozí brána nastavená na lokálních počítačích nasměruje veškerý internetový provoz na síťový port ADSL/Ethernet modemu/routeru. Počítače ve Vaší síti budou znát jejich výchozí bránu do Internetu buď proto, že jste ji nastavili ve vlastnostech jejich TCP/IP protokolu, případně proto, že byly nastaveny pro příjem potřebných informací dynamicky pokaždé, když uplatní požadavek na připojení do Internetu. (Viz odstavec 1.5).
- Výchozí brána ADSL/Ethernet modemu/routeru směřuje veškerý internetový provoz na modem/router Vašeho ISP. Adresa výchozí brány je přidělena automaticky poskytovatelem připojení pokaždé, když modem/router začne vyjednávat nové internetové spojení. (Proces přidělení výchozí trasy je popsán v další části „Přidělování IP tras“).

Trasy budete patrně muset definovat, provozujete-li více sítí nebo podsítí, využíváte-li služeb více ISP nebo se také připojujete z domova do podnikové sítě.

Prohlížení směrovací tabulky IP

Každý počítač využívající protokol TCP/IP a každý modem/router si udržuje tabulku často používaných IP adres. Pro každou z těchto *cílových IP adres* tabulka obsahuje IP adresu prvního hopu, který budou muset data absolvovat na cestě k cíli. Tato tabulka se běžně označuje jako *směrovací tabulka*.

Není-li stránka s tabulkou IP adres právě zobrazena, klikněte na záložku Routing. Stránka IP tras se poté zobrazí.

Tabulka IP tras obsahuje pro každou trasu jeden samostatný řádek. Některé z těchto řádků byly přidány při konfiguraci zařízení, další přidal sám uživatel a ještě jiné byly doplněny automaticky v průběhu komunikace se sítí ISP.

Směrovací tabulka také může ukazovat na výchozí bránu, která směřuje internetový provoz Vašeho ISP. Výchozí bránu najdete v řádku, který obsahuje cílovou adresu 0.0.0.0.

Směrovací tabulka se skládá z následujících polí:

- **Destination** (cíl): Obsahuje IP adresu cílového počítače. Cíl může ukazovat na IP adresu specifického počítače nebo celé sítě. Může také obsahovat samé nuly, což znamená, že tento směr bude použit pro všechny cíle, pro něž není definována jiná trasa (toto je trasa daná výchozí bránou).
- **Netmask** (maska sítě): Ukazuje, která část cílové adresy představuje adresu sítě a která adresu cílového počítače.
- **NextHop** (následující hop): Udává *příští* IP adresu, kam budou odeslána data, pokud je jejich místo určení uvedeno ve sloupci Cíl.
- **Ifname** (Jméno rozhraní): Udává jméno rozhraní, kterým jsou data odesílána k následujícímu hopu.
- **Route Type** (Typ trasy): Ukazuje, je-li trasa přímá nebo nepřímá. V případě přímé trasy se zdrojový i cílový počítač nalézají v téže síti a modem/router se pokusí data doručit přímo cílovému počítači. Jde-li o nepřímou trasu, leží zdrojový počítač v jiné síti než cílový a modem/router bude odesílat data na zařízení nacházející se v jiné síti k dalšímu zpracování.
- **Route Origin** (původ trasy): Udává, jakým způsobem byla trasa definována. *Dynamics* znamená, že tato trasa byla v systému předdefinována ISP nebo výrobcem. Trasy přidané Vámi jsou označeny jako *Local*. Ostatní trasy mohou vznikat automaticky (viz Konfigurace RIP v odstavci 2.3.2) nebo definovány vzdáleně prostřednictvím různých protokolů pro správu sítě (LCL nebo ICMP).
- **Action** (akce): Obsahuje ikonu () , na kterou kliknete, když budete chtít vymazat příslušný řádek.

Přidání IP trasy

Když budete potřebovat doplnit do tabulky modemu/routeru novou trasu, postupujte podle těchto pokynů:

1. Na stránce s tabulkou IP tras klikněte na tlačítko  a zobrazí se stránka pro přidání IP trasy.
2. Zadejte cíl, síťovou masku a bránu nebo další hop pro tuto trasu (viz výše uvedený popis jednotlivých polí tabulky).

Chcete-li doplnit trasu, která má plnit funkci výchozí brány modemu/routeru, do pole Destination a Netmask zadejte 0.0.0.0. Do pole Gateway(NextHop) udejte IP adresu Vašeho ISP.

Všimněte si, že zde nemůžete zadávat jméno rozhraní, typ trasy a původ trasy. Tyto parametry se používají jen pro automaticky identifikované trasy během komunikace modem/routerů mezi sebou. V případě ručně doplňovaných tras tato pole obsahují výchozí systémové hodnoty.

3. Klikněte na tlačítko **Submit**. Zobrazí se stránka vyzývající k potvrzení provedených změn.
4. Klikněte na tlačítko **Close** a vrátíte se na stránku s tabulkou IP tras. Ta by již měla novou trasu obsahovat.
5. Zobrazte záložku Admin a vyberte funkci **Commit & Reboot**.
6. Klikněte na **Commit**, aby se změny trvale uložily do paměti.

2.2.2 DHCP Mode

The screenshot shows a web interface with a top navigation bar containing 'Home', 'Configure', 'Services', and 'Admin'. Below this is a sub-navigation bar with 'IP Route', 'DHCP Mode' (highlighted), 'DHCP Server', and 'DHCP Relay'. The main content area is titled 'Dynamic Host Configuration Protocol (DHCP) Configuration'. It contains a paragraph explaining the purpose of the page: 'Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.' Below the text is a dropdown menu labeled 'DHCP Mode:' with 'DHCP Server' selected. At the bottom are four buttons: 'Submit', 'Cancel', 'Refresh', and 'Help'.

Popis konfigurace DHCP

Pro svoji síť a ADSL/Ethernet modem/router můžete použít protokol DHCP (Dynamic Host Configuration Protocol). V této části je uveden přehled protokolu DHCP a pokyny pro jeho implementaci v síti.

Viz Konfigurace DHCP Serveru (odstavec 2.2.3) a Konfigurace DHCP Relay (odst. 2.2.4), kde najdete specifické instrukce pro nastavení těchto služeb.

Co je to DHCP?

DHCP je protokol, který umožňuje správci sítě centrálně rozdělovat a přiřazovat IP informace počítačům v síti.

Jestliže v síti zavedete DHCP, povolíte tím zařízením – jako je ADSL/Ethernet modem/router nebo modem/router umístěný u Vašeho ISP – aby každému

počítači, který se připojí do sítě, přidělil dočasnou IP adresu. Zařízení, které tuto funkci vykonává se nazývá *DHCP Server*, zatímco příjemce IP adresy je označován jako *DHCP klient*.



Možná jste již každému počítači v síti IP adresu přidělili, možná jste nastavili, že mají získávat IP adresu dynamicky (automaticky). Pokud jste zvolili druhou možnost, nastavili jste Vaše počítače pro příjem IP adres z DHCP serveru, jímž může být např. Váš ADSL/Ethernet modem/router.

DHCP server čerpá IP adresy z definovaného rozsahu a „půjčuje“ je na určitou dobu počítačům, které se přihlašují do sítě. Shromažďuje, monitoruje a přiděluje adresy podle přicházejících požadavků.

V síti, v níž je aktivována služba DHCP nejsou IP informace *pevně* nastavené, ale přidělují se *dynamicky*. Proto může být klientovi DHCP přidělena při každém přihlášení do sítě jiná IP adresa.

Proč používat DHCP?

DHCP Vám umožňuje spravovat a přidělovat IP adresy v síti z jednoho centrálního místa. Bez DHCP byste museli nastavit každému počítači IP adresu a související informace zvlášť. DHCP se běžně používá v rozsáhlých sítích a v situacích, kdy dochází k častému rozšiřování či jiné aktualizaci sítě.

DHCP režim ADSL/Ethernet modemu/routeru

Modem/router může být konfigurován jako DHCP server, relay agent nebo klient.

- Když nastavíte modem/router aby plnil funkci DHCP serveru, bude spravovat daný rozsah IP adres a přidělovat je počítačům v síti. Obsahuje-li příslušný rozsah adres tzv. privátní IP adresy, je třeba také nastavit službu Network Address Translation (překlad adres), která zajistí převod privátních adres na veřejné adresy v Internetu. Ve výchozí konfiguraci modemu/routeru jsou obě služby (DHCP i NAT) povoleny.
- Jestliže službu DHCP zajišťuje pro Vaši síť Váš ISP, musíte modem/router konfigurovat jako *DHCP Relay agenta*. Jakmile pak modem/router obdrží z některého počítače žádost o připojení na Internet, spojí se s ISP a požádá o příslušné IP informace, které pak předá žádajícímu počítači.
- Pokud již ve Vaší síti provozujete DHCP server na některém počítači nebo jiném zařízení, bude třeba, abyste síťový port modemu/routeru nastavili do režimu *DHCP klienta* pro Váš server, stejně jako tomu je u všech PC v síti.

Toto nastavení je popsáno v části Konfigurace LAN a USB portů (odstavec 2.1.3).



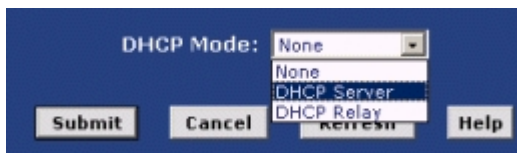
Můžete zadat nastavení pro DHCP server i DHCP relay a aktivovat kdykoli jeden z těchto režimů. Neaktivní nastavení zůstává zachováno pro příští použití.

Zapnutí a vypnutí režimu DHCP

DHCP režim byste měli nastavit až po konfiguraci DHCP relay nebo DHCP serveru. Viz část Konfigurace DHCP serveru (odstavec 2.2.3) a DHCP relay (odstavec 2.2.4), kde získáte další podrobnosti.

Při nastavování režimu DHCP postupujte následovně:

1. Pokud není právě zobrazena stránka režimu DHCP, klikněte na záložku **Configure** a vyberte funkci **DHCP Mode**.
2. Z rozbalovacího seznamu DHCP Mode vyberte **DHCP Server**, **DHCP Relay** nebo **None**.



Pokud jste vybrali **None** (nic), musí mít počítače ve Vaší síti přiděleny statické IP adresy. DHCP Server je v tomto nastavení vypnutý.

3. Klikněte na tlačítko **Submit**.
4. Zobrazte záložku **Admin** a klikněte na funkci **Commit & Reboot**.
5. Klikněte na **Commit**, aby se změny uložily trvale v paměti.

2.2.3 DHCP Server



The screenshot shows a web interface for configuring a DHCP server. At the top, there are tabs for 'Home', 'Configure', 'Services', and 'Admin'. Below these, there are links for 'IP Route', 'DHCP Mode', 'DHCP Server' (which is highlighted), and 'DHCP Relay'. The main heading is 'Dynamic Host Configuration Protocol (DHCP) Server Configuration'. A note states: 'Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.' Below this is a table with the following data:

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
10.0.0.1	10.0.0.254	-	10.0.0.138	Enabled	 

Below the table are four buttons: 'Add', 'Address Table', 'Refresh', and 'Help'.

Konfigurace DHCP Serveru

Následující část popisuje jak konfigurovat DHCP server Vašeho ADSL/Ethernet modemu/routeru.

Nejprve je třeba definovat rozsah IP adres, které bude server přidělovat Vaším počítačům, tzv. adresový pool DHCP serveru.



Než DHCP server spustíte, ujistěte se, že mají všechna PC v síti v konfiguraci TCP/IP povoleno přidělování IP adres DHCP serverem. Podrobný popis najdete v odstavci 1.5.

Návod na vytvoření adresního poolu DHCP serveru

Rozsah IP adres může obsahovat veřejné adresy, které jste si nakoupili od Vašeho ISP, zpravidla však obsahují privátní IP adresy, které si vytvoříte sami. Správci sítí si často vytvářejí privátní adresy pro použití výhradně ve vlastní síti.

Vytvořit může nejvýše dva rozsahy (pooly). V jednom poolu může ležet celkem 254 adres. Příklad: Můžete si vytvořit pouze jeden pool, který bude obsahovat adresy 192.168.1.2 až 192.168.1.255 nebo dva pooly s následujícími rozsahy:

Pool 0: 192.168.1.2 – 192.168.1.128

Pool 1: 192.168.1.129 - 192.168.1.255

Tentýž pool může být využit pro přidělování IP adres počítačům v síti (připojeným k síťovému portu modemu/routeru) i počítače připojeného přes USB port, ale jen za předpokladu, že LAN i USB porty leží v jediné podsíti. Druhý pool můžete vytvořit, nastane-li kterákoliv z následujících situací:

- Ethernetový (eth-0) a USB (usb-0) port jsou v různých podsítích.
- Vaše lokální síť je složena ze dvou podsítí.
- Máte pouze jednu podsít, ale adresy, které chcete přidělovat, netvoří jeden souvislý rozsah. (Určité adresy můžete také vyčlenit i z jednoho poolu).

DHCP server bude přidělovat adresy počítačům připojeným k určitému rozhraní jen za předpokladu, že toto rozhraní spadá do stejné podsítě jako adresový pool. Předpokládejme například, že Ethernetové a USB rozhraní mají přiděleny takové IP adresy, které je řadí do dvou rozdílných podsítí:

eth-0: IP adresa 192.168.1.1 maska 255.255.255.0

usb-0: IP adresa 192.168.2.2. maska 255.255.255.0

Při této konfiguraci můžete vytvořit následující dva pooly:

Pool 0: 192.168.1.2 až 192.168.1.11

Pool 1: 192.168.2.2 až 192.168.2.2

DHCP server bude automaticky přidělovat adresy z Poolu 0 těm počítačům, které jsou připojeny přes rozhraní ležící ve stejné posíti, tzn. eth-0. Podobně Pool 1 bude použit pro počítač připojený pře USB.

Přidání adresových poolů DHCP serveru

Pool IP adres vytvoříte podle následujících instrukcí:

1. Pokud není právě zobrazena stránka konfigurace DHCP serveru, klikněte na záložku LAN a z nabídky funkcí vyberte **DHCP Server**.

V závislosti na předem provedeném nastavení může tabulka obsahovat až dva adresní pooly, každý v jednom řádku, nebo také může být zcela prázdná.

2. Klikněte na tlačítko . Zobrazí se stránka přidání poolu (DHCP Server Pool – Add).
3. Zadejte počáteční a koncovou IP adresu, masku sítě, které jsou povinné a případně další dle potřeby:

- **Start/End IP Addresses:** Zadejte nejnižší a nejvyšší adresu poolu, maximálně 254 adres.
- **Mac Address:** Toto pole využijte jen pokud chcete přiřadit specifickou IP adresu specifickému počítači (vytváříte tím výjimku v dynamickém přidělování adres). IP adresa, kterou zde uvedete bude přidělena počítači s odpovídající Mac adresou. (MAC adresa je výrobcem přidělená identifikace hardwaru – síťové karty, která je pro každé zařízení unikátní). Jestliže sem zadáte Mac adresu, musíte zadat stejnou IP adresu do pole Start IP Address i End IP Address.
- **Net Mask:** Masku sítě udává, jaká část IP adresy z přiděleného rozsahu je adresou sítě a jaká část tvoří adresu počítače. Pomocí masky můžete rozlišit, který pool bude přidělován určité podmnožině Vašich počítačů v rámci celé sítě (této podmnožině pak říkáme *podsít*).
- **Domain Name** (jméno domény): Jméno podsítě, která zahrnuje adresy tohoto poolu.
- **Gateway Address:** Adresa výchozí brány pro počítače, kterým jsou přidělovány IP adresy jednoho poolu. Není-li její hodnota zadána, pak se počítačům přiděluje jako adresa výchozí brány adresa rozhraní (eth-0) nebo (usb-0) modemu/routeru, podle způsobu jejich připojení.
- **DNS/SDNS** (Domain Name System – doménový jmenný systém): IP adresa serveru DNS, jakou mají používat počítače, kterým je přidělena IP adresa z jednoho poolu. Systém DNS překládá Internetová jména počítačů, ta která zadáváte do Vašeho webového prohlížeče, na jejich odpovídající IP adresy. Tento server je nejčastěji umístěn u Vašeho ISP.
- **SMTP...SWINS** (volitelně): IP adresy zařízení, která plní různé služby pro počítače, které získávají svoje IP adresy z tohoto poolu (např. SMTP – Simple Mail Transfer Protocol, server zajišťující provoz elektronické pošty). Příslušné adresy Vám dodá Váš ISP.

4. Po zadání všech potřebných údajů klikněte na tlačítko **Submit**.

Krátce se zobrazí stránka signalizující, že byl adresový pool přidán úspěšně. Po několika vteřinách se na stránce DHCP Server Pool – Add nový pool objeví.

5. Klikněte na funkci **DHCP Mode**, aby se činnost DHCP serveru zahájila.

Prohlížení, úpravy a zrušení adresového poolu

Prohlízet, modifikovat nebo rušit adresové pooly lze na stránce DHCP Configuration. Zde klikněte na ikonu v příslušném řádku tabulky poolů.

- Pool IP adres zrušíte kliknutím na ikonu  a stisknutím tlačítek Submit a Commit.
- Prohlédnout detaily adresního poolu můžete po stisknutí ikony . Zobrazí se stránka, která obsahuje všechny údaje, které jste zadávali při vytváření nového poolu.

- Pool IP adres lze modifikovat kliknutím na ikonu . Tím se zobrazí stránka DHCP Server Pool – Modify. Zde můžete změnit doménové jméno přidělené poolu IP adres, pool povolit nebo zakázat. Standardně je pool povolen jakmile jej vytvoříte.

Po dokončení změn stiskněte tlačítko **Submit**. Dále použijte funkci Commit, aby se změny uložily do paměti trvale (viz odstavec 2.4.2).

Vyloučení IP adres z poolu

Jestliže existují některé IP adresy pevně přidělené určitým zařízením nebo z jakéhokoli jiného důvodu je nechcete zpřístupnit počítačům ve Vaší síti, můžete je z adresního poolu vyloučit.

Na stránce DHCP Server Configuration klikněte na ikonu  v řádku odpovídajícím poolu, který hodláte upravit. Na stránce DHCP Server Pool – Modify zadejte každou IP adresu, kterou chcete vyloučit do pole Excluded IP a

klikněte na **Add**. Po dokončení změn klikněte na tlačítko **Submit** a poté použijte funkci Commit k trvalému uložení provedených změn (viz odst. 2.4.2)

Zobrazení aktuálně přiřazených IP adres

Když Váš ADSL/Ethernet modem/router plní funkci DHCP serveru, pamatuje si, které IP adresy právě přidělil počítačům v síti. Tabulku všech aktuálních přiřazení si můžete prohlédnout na stránce DHCP Server Configuration. Na této stránce klikněte na tlačítko **Address Table**.

Adresní tabulka DHCP serveru obsahuje seznam všech IP adres, které jsou v dané chvíli propůjčeny zařízením v síti. Pro každou z těchto adres tabulka obsahuje následující informace:

- **IP Address:** Adresa z poolu, která byla použita.
- **Netmask:** Síťová maska související s propůjčenou IP adresou. Tím je identifikována síť a zařízení (počítač).
- **Mac Address:** Hardwarová adresa zařízení, kterému byla propůjčena IP adresa.
- **Pool Start:** Spodní hranice poolu (slouží k identifikaci poolu, z něhož přidělená IP adresa pochází).
- **Address Type:** Statický nebo dynamický. *Statický* ukazuje, že byla IP adresa přidělena trvale určitému zařízení. *Dynamický* znamená, že byla adresa přidělena jen dočasně, na určitou dobu.

- **Time Remaining:** Doba, po kterou bude ještě moci zařízení IP adresu používat. Standardní časový interval je 30 dnů (315360000 vteřin).

Příklad: Jak změnit IP adresu zařízení?

Potřebujete-li změnit IP routeru nebo rozmezí IP adres přidělované DHCP Serverem postupujte následovně.

1. Na záložce **Configure – DHCP Server** klikněte na  ve Vašem Adres poolu.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
10.0.0.1	10.0.0.254	-	10.0.0.130	Enabled	  

Add
Address Table
Refresh
Help

2. Tím vymažete přednastavené parametry přidělování IP adres DHCP Serverem.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
No DHCP Server Pool!					

Add
Address Table
Refresh
Help

3. Klikněte na **Add** a vložte nové, Vámi požadované parametry.

DHCP Server Pool - Add

DHCP Pool Information										
Start IP Address:	10	0	0	1						
End IP Address:	10	0	0	8						
Lease Time(sec):	3600									
Mac Address:		:		:		:		:		
Netmask:	255	255	255	0						
Domain Name:										
Gateway Address:	10	0	0	20						
DNS Address:	10	0	0	20						
SDNS Address:										
SMTP Address:										
POP3 Address:										
NNTP Address:										
WWW Address:										
IRC Address:										
WINS Address:	10	0	0	20						
SWINS Address:										

4. Klikněte na **Submit** objeví se následující okno. Potvrďte **Close**.

DHCP Server Pool Added Successfully...

Please click [here](#) to go back to the DHCP Server Pool - Add page.

5. Pool bude nyní naplněn novými parametry.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
10.0.0.1	10.0.0.8	-	10.0.0.20	Enabled	  

6. Nyní můžete změnit IP adresu routeru ze záložky **Home – LAN Config.**

The screenshot shows the 'LAN Configuration' page. At the top, there are tabs: Home, Configure, Services, and Admin. Below the tabs, there is a breadcrumb trail: Home | WAN Config | LAN Config | ADSL | Diagnostics. The main heading is 'LAN Configuration'. Below it, a text box says: 'Use this page to set the LAN configuration, which determines how your device is identified on the network.' The configuration is shown in a table:

LAN Configuration				
LAN IP Address:	10	0	0	20
LAN Network Mask:	255	255	255	0
IGMP:	☐ Enable ☒ Disable			

Dále použijte funkci Commit, aby se změny uložily do paměti trvale (viz odstavec 2.4.2).

2.2.4 DHCP Relay

The screenshot shows the 'DHCP Relay' page. At the top, there are tabs: Home, Configure, Services, and Admin. Below the tabs, there is a breadcrumb trail: IP Route | DHCP Mode | DHCP Server | DHCP Relay. The main heading is 'Dynamic Host Configuration Protocol (DHCP) Relay Configuration'. Below it, a text box says: 'As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.' The configuration is shown in a form:

DHCP Server Address:

Interfaces Running DHCP Relay	Action
No Interface Running DHCP Relay!	
eth-0	Add

At the bottom, there are buttons: Submit, Cancel, Refresh, and Help.

Konfigurace DHCP Relay

Někteří ISP poskytují pro domácí kanceláře a malé firmy službu DHCP serveru. V takovém případě můžete konfigurovat modem/router jako DHCP Relay agenta. Když některý počítač z Vaší sítě žádá o přístup na Internet, spojí se modem/router s ISP, aby pro něj získal IP adresu a související informace a ty

předá žádajícímu počítači. Chcete-li tuto funkci využít, postupujte podle následujících pokynů:

Nejprve bude třeba nakonfigurovat všechny počítače v síti pro příjem IP adres z DHCP serveru:

1. Otevřete okno Ovládací panel systému Windows a zobrazte vlastnosti síťového připojení. Ve vlastnostech protokolu TCP/IP nastavte „Získat IP adresu automaticky“ (skutečný text se může podle verze operačního systému mírně lišit). Podrobnosti viz Konfigurace TCP/IP na Vašem počítači (odstavec 1.5).

Nyní byste měli specifikovat IP adresu DHCP serveru a zvolit rozhraní Vaší sítě, pro které se bude služba DHCP Relay využívat.

2. Není-li zrovna zobrazena stránka DHCP Configuration, klikněte na záložku LAN a vyberte funkci **DHCP Relay**.
3. Do pole **DHCP Server Address** zadejte IP adresu DHCP serveru Vašeho ISP.

Pokud tuto adresu neznáte, ještě není všechno ztraceno. Požadavky na IP adresy z Vaší sítě budou směrovány na výchozí bránu, která by je měla nasměrovat ke správnému cíli.

4. Z rozbalovacího seznamu zvolte WAN rozhraní a klikněte na tlačítko .

Vaše WAN rozhraní se může jmenovat ppp-0, eoa-0 nebo ipoa-0. Nejste-li si jisti, které z uvedených rozhraní použít, požádejte o pomoc Vašeho ISP.

(Pamatujte si, že rozhraní můžete z tabulky odstranit kliknutím na ikonu  v pravém sloupci.

5. Klikněte na tlačítko . Zobrazí se stránka potvrzení Vašich změn a potom program obnoví stránku DHCP Relay Configuration.
6. Klikněte na funkci **DHCP Mode**, tím se povolí její používání.

2.3 SERVICES

2.3.1 NAT

Home Configure Services Admin

NAT | RIP | IP Filter | FireWall | DNS Relay

Network Address Translation (NAT) Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

☒ Enable ☐ Disable

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	52047

Submit Global Stats Cancel Refresh Help

Popis služby Network Address Translation – překladu adres

V této části najdete stručný výklad funkce NAT – funkce překladu adres. Tato funkce slouží k zamaskování privátních IP adres používaných ve Vaší síti a jejich nahrazení veřejnou IP adresou, kterou používáte při připojení do Internetu. Musíte jen určit pravidla, která přesně stanoví jak a kdy se mají adresy překládat.



Zatímco **privátní IP adresy** pro použití uvnitř Vaší sítě určuje její správce, **veřejné IP adresy** pro použití v Internetu je třeba získat za určitý poplatek od instituce, která se touto problematikou zabývá. V obvyklém případě zajistí veřejnou adresu pro Vaši síť Váš ISP a vy si sami definujete IP adresy pro počítače uvnitř této sítě.

Při typickém nastavení služby NAT Vám pro celou síť Váš ISP přidělí jednu veřejnou IP adresu. Vy přiřadíte každému počítači unikátní privátní IP adresu, popř. definujete adresový pool pro dynamické přidělování IP adres Vaším počítačům. Na ADSL/Ethernet modemu/routeru pak nastavíte pravidlo NAT tak, aby kdykoli bude některý z počítačů Vaší sítě komunikovat s Internetem (tzn. bude vysílat nebo přijímat *datové IP pakety*, byla jeho privátní IP adresa, která je součástí každého paketu, nahrazena veřejnou IP adresou sítě.



Datový IP paket obsahuje malou část dat sestavenou do specifického formátu, který je vhodný pro odeslání do Internetu. Tyto pakety jsou stavebními bloky veškeré Internetové komunikace. Každý paket začíná hlavičkou, jejíž součástí je IP adresa počítače, který komunikaci vyvolal (tzv. **zdrojová IP adresa**), číslo portu, s nímž si modem/router spojuje tento počítač (tzv. **číslo zdrojového portu**), IP adresu cílového počítače v Internetu (tzv. **cílovou IP adresu**) a některé další služební informace.

Je-li uplatněno toto pravidlo překladu adres, pro ostatní počítače v Internetu se zdá, že datové pakety přicházejí z počítače s Vám přidělenou veřejnou IP adresou, neboť jeho původní IP adresa byla vyměněna, (v tomto případě s adresou ADSL/Ethernet modemu/routeru).

V pravidlech NAT lze dále definovat, že se má v datových paketech zamaskovat i zdrojový port (neboli zaměnit jeho číslo za jiné), takže ostatní počítače nebudou schopny určit, z jakého portu data pocházejí. Pakety, které přicházejí jako odpověď obsahují veřejnou IP adresu jako adresu cíle a maskované číslo portu. ADSL/Ethernet modemu/routeru vrátí IP adresu i číslo portu na původní hodnoty, protože si o prováděných změnách pořizuje záznam a paket odešle původnímu počítači, který komunikaci vyvolal.

Podobná pravidla překladu adres (NAT) poskytují několik výhod:

- Eliminují nutnost pořizovat pro všechny počítače v síti veřejné IP adresy. Můžete si nastavit svoje vlastní privátní adresy bez jakýchkoli poplatků a nechat je překládat na veřejnou IP adresu jen v případě Internetové komunikace.
- Poskytují jistou míru zabezpečení Vaší sítě, protože budete mít privátní IP adresy a při přístupu na Internet je spolu s číslem zdrojového portu zamaskují.

Výše popsaná funkce se nazývá *network address port translation (NAPT)*. Můžete využít i jiné typy překladu, např. tzv. *flavors*, k jiným účelům, např. když budete chtít umožnit přístup do Vaší sítě „z venku“ nebo překládat více privátních IP adres na více veřejných.

Vypnutí a zapnutí NAT

Služba NAT je v továrním nastavení zapnutá. Vypnutí je možné provést pomocí konfiguračního menu. Nabídka **Services** položka **Disable**. Viz. obrázek níže.

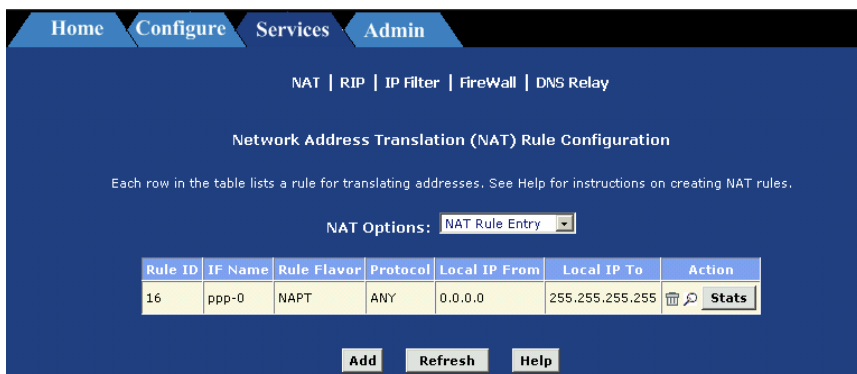


Konfigurace NAT

Konfigurace NAT se provádí pomocí nastavení pravidel NAT **NAT Options** položka **NAT Rule Entry**



V továrním nastavení je konfigurace NAT nastavena na NAPT, jak je vidět na obrázku níže. Přidání pravidel se provádí pomocí tlačítka **Add**.



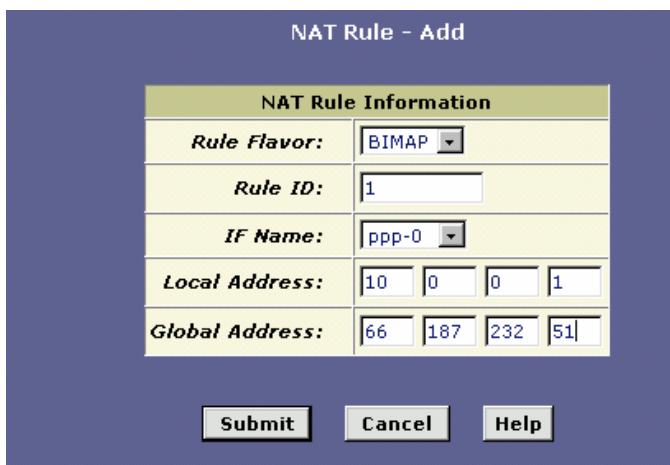
Příklady nastavení

7. Na privátní síti je umístěn Firewall který se stará o bezpečnost sítě.

IP adresa WAN	66.187.232.51
IP adresa Firewall	10.0.0.1

Zařízení nutné nastavit, tak aby doručil všechny pakety na jednu určitou adresu privátní sítě. V tomto případě je použito pravidlo **BIMAP** a doplněny **Lokální a globální IP adresy**.

Původní pravidla musí být vymazána!



2. Na privátní síti je umístěn poštovní server. Sem mají být doručovány všechny pakety související s touto službou. Ostatní pakety mají být doručovány do privátní sítě na základě NATP pravidla.

IP adresa WAN	66.187.232.51
IP adresa poštovního serveru	10.0.0.1
Port překládané služby	POP3 port 110

V tomto případě je nutné nastavit zařízení tak, aby rozlišil směrování paketu na základě čísla portu (služby). Použité pravidlo **RDR** , doplněny informace o **Lokální a Globální IP adrese a číslo portu**.

NAT Rule - Add

NAT Rule Information				
Rule Flavor:	RDR			
Rule ID:	1			
IF Name:	ppp-0			
Protocol:	ANY			
Local Address From:	10	0	0	1
Local Address To:	10	0	0	1
Global Address From:	66	187	232	51
Global Address To:	66	187	232	51
Destination Port From:	POP3 (110)			
Destination Port To:	POP3 (110)			
Local Port:	POP3 (110)			

Následně je přidáno pravidlo pro zbylou část sítě. V tomto případě je nutno zvážit konfiguraci IP Filtru z důvodu zabezpečení privátní sítě.

NAT Rule - Add

NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:	2			
IF Name:	ppp-0			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

2.3.2 RIP

The screenshot shows a web interface for configuring the Routing Information Protocol (RIP). At the top, there are tabs for Home, Configure, Services, and Admin. Below these, there are links for NAT, RIP (selected), IP Filter, FireWall, and DNS Relay. The main heading is "Routing Information Protocol (RIP) Configuration". A descriptive text states: "Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used." Below this text are two radio buttons: "Enable" (selected) and "Disable". There are two input fields: "Age(seconds):" with the value 180 and "Update Time(seconds):" with the value 30. A table with the following columns is shown: IF Name, Metric, Send Mode, Receive Mode, and Action. The table currently contains one entry: "eth-0" with Metric "1", Send Mode "NONE", and Receive Mode "NONE". Below the table is an "Add" button. At the bottom of the page are buttons for "Submit", "Cancel", "Global Stats", "Refresh", and "Help".

IF Name	Metric	Send Mode	Receive Mode	Action
No Rip Entries!				
eth-0	1	NONE	NONE	Add

Konfigurace protokolu RIP (Routing Information Protocol)

Váš ADSL/Ethernet modem/router může být konfigurován tak, aby během komunikace s ostatními modemy/routery určoval nejvhodnější trasu pro odeslání dat k jejich cíli. Směrovací zařízení si předávají podobné informace s použitím celé řady IP protokolů. Tato část se bude zabývat konfigurací Vašeho modemu/routeru pro použití jednoho z těchto protokolů, který dostal název RIP – Routing Information Protocol.

Popis protokolu RIP

RIP je jedním ze sady IP protokolů, který dovoluje sdílet informace ze směrovacích tabulek mezi více směrovacími zařízeními v lokální síti, síti Vašeho ISP nebo vzdálených sítích spojených s tou Vaší pomocí linky ADSL. Obecně řečeno, RIP se používá ke komunikaci mezi autonomními sítěmi. Autonomní síť se rozumí taková síť, jejíž počítače jsou spravovány jednou správním institucí. Proto může být autonomní síť jednotlivá síť nebo také skupina sítí, která však musí být pod jednou správou. Příkladem autonomní sítě může být síť rozvětvené organizace, která obsahuje zařízení připojující se do ní ze vzdálených míst, např. zaměstnanci pracující doma.

Při aplikaci protokolu RIP odesílá každé zařízení svoji směrovací tabulku svému nejbližšímu sousedu každých 30 vteřin. Toto sousední zařízení zase předává routovací informaci svému sousedu atd., dokud všechna zařízení autonomní síť nemají kompletní sadu tras.

Kdy byste měli konfigurovat RIP?

Ve většině malých sítí není vůbec třeba protokol RIP používat. V podobných sítích existuje jen jeden modem/router a jedna trasa k ISP. V takových případech není třeba trasy sdílet, protože všechny vedou na jedinou bránu ISP.

RIP budete muset konfigurovat, pokud pro Vaši síť platí některý z následujících případů:

- Ve Vaší, např. domácí, síti je kromě ADSL/Ethernet modemu/routeru instalován další modem/router (jeho funkci může také plnit některý z počítačů). ADSL modem/router a druhé zařízení budou potřebovat zajistit vzájemnou komunikaci pomocí RIP, aby mohly sdílet směrovací tabulky.
- Vaše síť je připojena pomocí ADSL linky k jiné, vzdálené síti (např. podnikové). Aby mohly obě sítě sdílet směrovací informace, měly by být *obě* konfigurovány s protokolem RIP.
- ISP požaduje, abyste provozovali RIP kvůli komunikaci se zařízeními v jeho síti.

Konfigurace rozhraní ADSL/Ethernet modemu/routeru s protokolem RIP

Další řádky obsahují návod jak povolit používání RIP na Vašem ADSL modemu/routeru.



Aby mohl ADSL/Ethernet modem/router s ostatními zařízeními pomocí protokolu RIP, musí být RIP povolen i na těchto zařízeních. Podrobnosti viz dokumentace těchto zařízení.

1. Není-li právě zobrazena stránka RIP Configuration, klikněte na záložku **Services** a ze seznamu funkcí vyberte **RIP**.

Stránka obsahuje políčka pro povolení nebo zakázání funkce RIP a tabulku se seznamem rozhraní, v nichž se RIP právě používá. Když tuto stránku otevřete poprvé, bude tabulka pravděpodobně prázdná.

2. Je-li to nutné, upravte parametry Age (stáří) a Update Time (interval aktualizace). Jedná se o globální parametry pro všechna rozhraní, která používají RIP.

- **Age** je doba v sekundách, po kterou si tabulka RIP pamatuje údaje o každé trase, kterou se dozví od sousedních počítačů.
- **Update Time** udává, jak často bude ADSL/Ethernet modem/router vysílat svoji směrovací tabulku sousedům v síti.

3. Ve sloupci IFName vyberte jméno rozhraní, na němž chcete spustit RIP.

Pro komunikaci s ostatními zařízeními ve Vaší síti, která RIP používají, vyberte eth-0 nebo jméno příslušného virtuálního ethernetového rozhraní.

Pro komunikaci s ISP nebo vzdálenou sítí vyberte odpovídající ppp, eoa nebo jiné WAN rozhraní.

4. Zadejte metriku vybraného rozhraní.

RIP používá pro určení nejlepší trasy do cílové sítě „čítač hopů“. Počet hopů je roven součtu metrik přiřazených portům, jimiž data na cestě k cíli musí projít. Z několika alternativních tras je za nejrychlejší považována trasa s nejnižším počtem hopů.

Dejte tomu, že svému portu přiřadíte metriku 1. Až bude RIP potom vyhodnocovat trasu vedoucí přes tento port, přičte k čítači hopů jedničku. Jestliže víte, že je komunikace přes toto rozhraní pomalejší než přes jiná rozhraní Vaší sítě, můžete portu přidělit vyšší hodnotu metriky.

Můžete použít jakékoli celé číslo od 1 do 15.

5. Vyberte Send Mode a Receive Mode.

Send Mode (režim vysílání) udává verzi RIP, v jaké bude zařízení vysílat svoje směrovací informace ostatním zařízením.

Receive Mode (režim příjmu) udává verzi RIP, v níž musí být informace předávána ADSL/Ethernet modemu/routeru, aby ji přijal do své směrovací tabulky.

RIP verze 1 je originální RIP protokol. Máte-li zařízení komunikující s tímto rozhraním, která rozumějí pouze verzi 1, volte RIP1.

RIP verze 2 se používá častěji, protože podporuje IP adresy nepatřící do žádné třídy (používají se při vytváření podsítí) a některé další vlastnosti. Pokud všechna směrovací zařízení v síti podporují tuto verzi protokolu, volte RIP2.

6. Klikněte na tlačítko . V tabulce přibude nový údaj o protokolu RIP.
7. Klikněte na políčko **Enable**, čímž funkci RIP povolíte.



Pokud byste nyní protokol RIP zakázali, nastavení rozhraní zůstane k dispozici pro pozdější použití.

8. Až nastavíte nastavení RIP pro rozhraní, klikněte na tlačítko **Submit**.
Zobrazí se potvrzení provedených změn.
9. Klikněte na záložku Admin a vyberte funkci **Commit & Reboot**.
10. klikněte na **Commit**.



Existující nastavení RIP můžete zrušit kliknutím na ikonu  ve sloupci Action.

Zobrazení statistik protokolu RIP

Na stránce RIP Configuration můžete kliknutím na **Global Stats** zobrazit statistiku pokusů o odeslání a příjem dat směrovací tabulky přes rozhraní modemu/routeru s nastaveným protokolem RIP.

Tyto hodnoty můžete vynulovat tlačítkem **Clear**, případně kliknutím na tlačítko **Refresh** zobrazit nová data.

2.3.3 IP Filter

HomeConfigureServicesAdmin

NAT | RIP | IP Filter | FireWall | DNS Relay

IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level:

None

Public Default Action:

Accept

Private Default Action:

Deny

DMZ Default Action:

Accept

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-		Stats
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255		Stats
30	Private	Enable	Incoming	Accept	N/A	Disable	-		Stats
40	Private	Enable	Outgoing	Accept	ALL	Disable	-		Stats
50	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq UDP 2.Dest Port equal to 53		Stats
60	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 53		Stats
70	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 25		Stats
80	Private	Enable	Outgoing	Accept	DMZ	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 110		Stats

Konfigurace IP Filtru

Funkce IP filtru Vám umožňuje stanovit určitá pravidla, která ovlivňují předávání příchozích a odchozích dat mezi Vaší sítí a Internetem a v rámci Vaší sítě. V této části je vysvětleno, jak se pravidla IP filtru vytvářejí.

Popis IP filtrů

IP filtr Vám dovoluje kontrolovat typy dat předávaných mezi Internetem a Vaší sítí. Můžete si vytvořit pravidla IP filtru, která budou blokovat pokusy určitých počítačů Vaší sítě přistupovat k určitým typům dat nebo místům na Internetu. Rovněž můžete zablokovat snahy o přístup k počítačům Vaší sítě „zvenku“.

Když definujete pravidlo IP filtru a povolíte jeho funkci, dáváte tím pokyn ADSL/Ethernet modemu/routeru, aby přezkoumával datové pakety a určoval, jestli splňují kritéria nastavená v pravidle. Kritériem může být síťový nebo

internetový protokol, kterým je paket přenášen, směr kterým putuje (např. ze sítě do Internetu nebo naopak), IP adresa počítače, který paket odeslal, IP adresa cíle a řada dalších charakteristik datového paketu.

Jestliže paket splňuje podmínky pravidla, může být buď přijat (odeslán dál ke svému cíli) nebo odmítnut (zahozen) – v závislosti na akci specifikované v pravidle.

Prohlížení konfigurace IP filtru

Není-li právě zobrazena stránka IP Filter Configuration, klikněte na záložku Services a vyberte funkci **IP Filter**.

Konfigurační stránka IP filtru zobrazuje globální nastavení (viz „Globální nastavení IP filtru“), které můžete modifikovat a tabulku pravidel IP filtru, která obsahuje všechna právě používaná pravidla. Popis jednotlivých položek, z nichž se skládá pravidlo, viz „Vytváření pravidel IP filtru“. U již definovaných pravidel můžete použít ikony ve sloupci Action pro editaci () , zrušení () a prohlížení detailů () příslušného pravidla.

Globální nastavení IP filtru

Stránka IP Filter Configuration Vám umožňuje konfigurovat tato globální nastavení IP filtru:

- **Security Level** (úroveň zabezpečení): Stanovuje, která pravidla IP filtru budou použita. Posuzují se podle úrovně zabezpečení dané v každém z pravidel. Je-li např. zvolena úroveň *vyšoká* (high), uplatní se pouze pravidla, jejich úroveň zabezpečení je rovněž *vyšoká*. Totéž platí o úrovních *střední* (Medium) a *nížká* (Low). Je-li vybrána hodnota *None* (žádná), IP filtrování je vypnuto.
- **Private/Public/DMZ Default Action** (výchozí akce pro privátní/veřejné/DMZ): Toto nastavení určuje co se stane s paketem (bude přijat nebo odmítnut) na privátním, veřejném nebo DMZ rozhraní, když přijde paket, který *nevyhovuje* žádnému filtrovacímu pravidlu. Pro každý typ rozhraní můžete definovat jinou výchozí akci. (Typ rozhraní určuje při jeho vytváření, viz např. stránka pro konfiguraci PPP).
 - *Veřejné* rozhraní představuje typicky připojení do Internetu. PPP, EoA a IPoA jsou typickými veřejnými rozhraními. Pakety přijaté na veřejném rozhraní jsou předmětem nejpřísnějších restrikcí definovaných v softwaru. Obvykle je globálním nastavením pro veřejné rozhraní *Deny* (odmítnout), což znamená, že veškeré přístupy do Vaší sítě vyvolané externími počítači budou odmítány (zahozeny na veřejném rozhraní), kromě těch, které povolíte určitým pravidlem IP filtru.

- o *Privátním* rozhraním se modem/router připojuje do Vaší sítě, nejčastěji je to ethernetové rozhraní. Pakety přijaté na tomto rozhraní bývají předmětem méně restriktivních opatření, protože pocházejí z vnitřní sítě. Běžným globálním nastavením pro toto rozhraní je *Accept* (přijmout), aby počítače ve Vaší síti měly přístup pře ADSL/ethernet modem/router přístup na Internet.
- o Označení *DMZ* (demilitarizovaná zóna) se v internetové terminologii používá pro počítače, které mají přístupné jak z veřejného rozhraní, tak z vnitřní sítě (např. veřejný web server společnosti). Pakety přijaté na rozhraní DMZ jsou z hlediska zabezpečení posuzovány někde na mezi privátního a veřejného rozhraní. Globální nastavení pro rozhraní DMZ může být *Deny*, pak budou všechny pokusy o přístup běžně odmítány, správce sítě však může definovat pravidlo (pravidla) IP filtru, která určité typy přístupu povolí.

Vytváření pravidel IP filtru

Při tvorbě pravidla IP filtru musíte stanovit řadu kritérií, která musí být splněna, aby se pravidlo mohlo uplatnit. Pomocí následujícího návodu můžete přidat nové pravidlo IP filtru: (Určitě Vám pomohou příklady v části „Příklady pravidel IP filtru“.)

1. Na hlavní stránce IP filtru klikněte na tlačítko **Add**, aby se Vám zobrazila stránka pro přidání nového pravidla (IP Filter Rule – Add).
2. Pro každé pole zadejte nebo vyberte údaje, které mají být v pravidle použity. Následující tabulka popisuje jednotlivá pole:
 - **Rule ID** (číslo pravidla): Každému pravidlu musí být přiřazeno pořadové identifikační číslo. Pravidla jsou posuzována pro každý paket od nejnižšího po nejvyšší číslo, dokud není některé splněno. Doporučujeme označovat pravidla čísly, která jsou násobkem 5 nebo 10 (např. 10, 20, 30...), Tak mezi nimi zůstane dostatečný prostor pro případné doplnění o další pravidla.
 - **Action** (akce): Udává, co se stane s paketem, vyhovuje-li kritériím pravidla. Možnosti jsou *Accept* (přimout – odeslat k cíli) nebo *Deny* (odmítnout – zahodit paket).
 - **Direction** (směr): Udává zda se má pravidlo uplatnit na paket přicházející nebo odcházející po daném rozhraní. Přicházející (*Incoming*) se rozumí paket, který po rozhraní vstupuje do lokální sítě a odcházející (*Outgoing*) je paket, který lokální síť opouští. Můžete použít pravidla, která se uplatní na směr do sítě a zabránit tak externím počítačům v přístupu do Vaší sítě.
 - **Interface** (rozhraní): Rozhraní na zařízení, na němž se pravidlo uplatní. V části „Příklady pravidel IP filtru“ najdete doporučení jak vybrat vhodné rozhraní pro určitý typ pravidla.
 - **In Interface**: Rozhraní, z něhož musí být paket odeslán na rozhraní specifikované v předcházejícím výběru. Tato možnost je platná pouze pro pravidla definovaná pro směr ven.

- **Log Option** (možnost logování): Je-li logování povoleno (*Enabled*), bude v logu vytvořen záznam pokaždé, když bude toto pravidlo uplatněno. Záznam bude obsahovat čas kdy došlo k porušení, zdrojovou adresu počítače zodpovědného za porušení, cílovou IP adresu, použitý protokol, zdrojový a cílový port a počet porušení za posledních x minut. (Logování je velice dobrou pomůckou při hledání závad). Tyto informace lze také poslat e-mailem příslušným správcům. Viz také odstavec 2.3.4 (Konfigurace firewallu) a související témata nápovědy.
- **Security Level** (úroveň zabezpečení): Úroveň zabezpečení, jaká musí být vybrána v globálním nastavení, aby se pravidlo mohlo uplatnit. Pravidlo se uplatní jedině pokud je jeho úroveň zabezpečení shodná s hodnotou v globálním nastavení (zobrazuje se na hlavní stránce IP filtru). Jestliže je například pravidlo nastaveno na *Medium* a zároveň globální úroveň zabezpečení firewallu je *Medium*, bude pravidlo aktivní. Bude-li ale globální úroveň firewallu *High* nebo *Low*, pravidlo bude neaktivní – neuplatní se.
- **Black List Status** (černá listina): Určuje, zda má či nemá mít porušení tohoto pravidla za následek zapsání IP adresy počítače – pachatele na černou listinu, která říká ADSL modemu/routeru, že má pakety z tohoto zdroje po určitou stanovenou dobu blokovat (viz odstavec 2.3.4. „Konfigurace firewallu“).
- **Log Tag** (poznámka do logu): Popis v délce max. 16 znaků, který se má zaznamenat do logu v případě porušení tohoto pravidla. Chcete-li této možnosti využít, nezapomeňte nastavit Log Option na *Enable*.
- **Start/End Time** (čas od – do): Časový interval, v němž se má toto pravidlo použít, udává se ve vojenských jednotkách (od půlnoci k půlnoci, čtyřciferně 0001-2359) .
- **Src IP Address** (IP adresa zdroje): Kritérium IP adres pro počítač(e) odkud byly pakety odeslány. Z rozbalovacího seznamu si vyberte variantu, kdy bude pravidlo uplatněno na pakety obsahující:
 - o **any** (cokoliv): jakákoli IP adresa.
 - o **lt** (menší než): jakákoli zdrojová IP adresa, která je numericky menší než zadaná.
 - o **lteq** (menší nebo rovno): jakákoli zdrojová IP adresa, která je numericky menší nebo rovna zadané.
 - o **gt** (větší než): jakákoli zdrojová IP adresa, která je numericky větší než zadaná.
 - o **eq** (rovno): zdrojová IP adresa, která je numericky shodná se zadanou.
 - o **neq** (není rovno): jakákoli zdrojová IP adresa, která není numericky rovna zadané.
 - o **range** (rozsah): jakákoli zdrojová IP adresa, která leží v zadaném intervalu, včetně mezních hodnot.
 - o **out of range** (mimo rozsah): jakákoli zdrojová IP adresa, která leží mimo zadaný rozsah
 - o **self** (vlastní): IP adresa rozhraní ADSL/Ethernet modemu/routeru, na kterém se má toto pravidlo použít.
- **Dest IP Address** (IP adresa cíle): Kritérium IP adresy pro cílový počítač nebo počítače (tj. IP adresa počítače, jemuž byl paket poslán).

Kromě možností uvedených u pole Src IP Address, je ještě možno použít:

- o **bcast** (broadcast): udává, že se pravidlo použije na všechny pakety poslané na adresu typu broadcast pro vstupní rozhraní. (Adresa typu broadcast se používá pro odeslání paketů všem stanicím v síti nebo podsíti přes dané rozhraní). Použijete-li tuto možnost, nemusíte zadávat adresu, a proto jsou adresní políčka nedostupná.
- **Protocol:** Kritérium IP protokolu, které musí být splněno, aby se pravidlo mohlo uplatnit. Můžete zadat, že pakety musí obsahovat zvolený protokol (*eq*), nesmí obsahovat zvolený protokol (*neq*), nebo že má být pravidlo použito bez ohledu na použitý protokol (*any*). TCP, UDP a ICMP jsou běžně používané IP protokoly, ostatní lze identifikovat podle čísel 0-255, která jim jsou přiřazena institucí IANA (Internet Assigned Numbers Authority).
- **Store State:** Je-li tato volba povolena, provádí se tzv. *stateful* filtrování a pravidlo se rovněž uplatní v opačném směru v průběhu IP relace na daném rozhraní.
- **Source Port** (zdrojový port): Kritérium čísla portu pro počítač nebo počítače, odkud pakety pocházejí. Toto pole nebude přístupné pro zadávání, pokud nevyberete jako protokol TCP nebo UDP. Možné volby viz popis Src IP Address.
- **Dest Port** (cílový port): Kritérium portu pro cílový počítač nebo počítače (tj. číslo portu počítače, jemuž byl paket poslán). Toto pole bude nepřístupné pro zadávání, pokud jste nevybrali jako protokol TCP nebo UDP. Možné volby, viz popis Src IP Address.
- **TCP Flag** (příznak TCP): Udává, jestli se má pravidlo použít jen na TCP pakety se synchronním příznakem (*SYN*), nesynchronním příznakem (*NOT-SYN*) anebo na všechny TCP pakety. Pokud není vybrán jako protokol TCP, bude toto pole nepřístupné pro zadávání.
- **ICMP Type:** Udává, zda bude hodnota v poli Type v hlavičce ICMP paketu použita jako kritérium. Hodnotou kódu může být libovolné dekadické číslo z intervalu 0-255. Můžete určit, že se hodnota musí rovnat (*eq*), popř. nesmí rovnat (*neq*) zadané hodnotě. Můžete také říct, že vyberete jakoukoli (*any*) hodnotu, která umožní pravidlo použít na všechny ICMP pakety. Pole bude nepřístupné pro zadávání, pokud nebude vybrán protokol ICMP.
- **ICMP Code:** Udává, zda se má použít hodnota pole kódu v hlavičce ICMP paketu jako kritérium. Kód může nabývat libovolné dekadické hodnoty z intervalu 0-255. Můžete určit, že se hodnota musí rovnat (*eq*), popř. nesmí rovnat (*neq*) zadané hodnotě. Můžete také říct, že vyberete jakoukoli (*any*) hodnotu, která umožní pravidlo použít na všechny ICMP pakety. Pole bude nepřístupné pro zadávání, pokud nebude vybrán protokol ICMP.
- **IP Frag Pkt** (fragment IP paketu): Určuje jak bude pravidlo použito na pakety obsahující fragmenty. Můžete použít následující možnosti:
 - o **Yes:** Pravidlo se použije pouze na pakety obsahující fragmenty.
 - o **No:** Pravidlo se použije pouze na pakety neobsahující fragmenty.
 - o **Ignore:** (výchozí hodnota) Pravidlo bude použito na paket bez ohledu na to, jestli obsahuje fragmenty či ne, pokud vyhoví ostatním kritériím.

- **IP Option Pkt** (pakety s uvedenou volbou): Udává, jestli se má pravidlo použít na IP pakety, které mají v hlavičce vyplněny volby.
 - o **Yes**: Pravidlo se použije pouze na pakety, které obsahují v hlavičce volby.
 - o **No**: Pravidlo se použije pouze na pakety, které neobsahují v hlavičce volby.
 - o **Ignore**: (výchozí hodnota) Pravidlo bude použito na paket bez ohledu na to, jestli obsahuje volby hlavičky či ne, pokud vyhoví ostatním kritériím.
- **Paket Size** (velikost paketu): Určuje, jestli bude pravidlo IP filtru použito na pakety, jejichž velikost v bytech vyhovuje tomuto kritériu. (lt = menší než, gt = větší než, lteq = menší nebo rovno atd.)
- **TOD Rule Status** (časové omezení platnosti): Udává, jak bude použito nastavení Start Time/End Time.
 - o **Enable**: (výchozí hodnota) Pravidlo je účinné v zadaném časovém intervalu.
 - o **Disable**: Pravidlo je účinné pouze mimo zadaný časový interval.

3. Máte-li hotov výběr kritérií, ujistěte se, že zaškrtnuto políčko Enable v horní části stránky a pak klikněte na tlačítko **Submit**, které je naopak v dolní části stránky. Zobrazí se stránka s potvrzením provedených změn a konfigurační stránka IP filtru se zobrazí znovu, tentokrát již s novým pravidlem.

Je-li úroveň zabezpečení pravidla shodná s globálním nastavením, pak se ve sloupci Status rozsvítí zelená značka signalizující, že je pravidlo aktivní. Červená značka znamená, že je pravidlo vypnuto, nebo jeho úroveň zabezpečení neodpovídá globálnímu nastavení.

4. Přesvědčete se, že nastavení Security Level a Private/Public/DMZ Default Action v konfiguraci IP filtru má požadované hodnoty a potom stiskněte tlačítko **Submit**. Objeví se potvrzení provedených změn.
5. Zobrazte záložku Admin a klikněte na funkci **Commit & Reboot**.
6. Stiskněte tlačítko **Commit**, aby se změny uložily trvale.

Příklady pravidel IP filtru

Příklad 1. Zabrání specifickému počítači uvnitř sítě v přístupu na webové servery na Internetu:

1. Přidejte nové pravidlo pro odchozí pakety na rozhraní ppp-0 z libovolného vstupního rozhraní (bude se týkat např. eth-0 a usb-0).
2. Zadejte zdrojovou IP adresu – adresu počítače, který chcete zablokovat.
3. Zadejte protokol = *TCP* a povolte nastavení Store State.
4. Zadejte cílový port = *80*, což je dobře známé číslo portu webových serverů.
5. Povolte použití pravidla zaškrtnutím políčka v horní části stránky.

6. Kliknutím na **Submit** vytvoříte pravidlo.
7. Na stránce IP Filter Configuration nastavíte úroveň zabezpečení stejnou, jako jste vybrali pro pravidlo a nastavíte Private Default Action i Public default Action na *Accept*.
8. Klikněte na **Submit** a uložíte provedené změny.

Určený počítač nebude moci navštěvovat webové servery, bude však mít přístup např. na FTP servery v Internetu (a také všechny ostatní, které využívají jiný port než 80).

Příklad 2. Blokování přístupu na zařízení protokolem Telnet:

1. Přidejte nové pravidlo pro pakety vstupující na rozhraní ppp-0.
2. Zadejte, že pakety musí obsahovat protokol TCP a musí být určeny pro cílový port 23 používaný protokolem Telnet.
3. Povolte pravidlo zaškrtnutím políčka v horní části stránky.
4. Klikněte na **Submit**, aby se pravidlo vytvořilo a uložte je.

Zobrazení statistik IP filtru

U každého definovaného pravidla si můžete prohlédnout statistické údaje – např. na kolik z přijatých paketů bylo pravidlo aplikováno. Zobrazte stránku IP

Filter Configuration a klikněte na tlačítko **Stats** v řádku příslušného pravidla.

Můžete zde všechny hodnoty vynulovat tlačítkem **Clear** a tlačítkem

Refresh

načíst nově naakumulované údaje.

Správa relací aktuálních IP filtrů

Když spolu komunikují dva počítače pomocí protokolu IP, hovoříme o IP relaci, která je vytvořena po dobu trvání komunikace. ADSL/Ethernet modem/router umožňuje vést určitý pevný počet souběžných IP relací. Můžete si zobrazit informace o každé z nich a můžete kteroukoli zrušit (např. z bezpečnostních důvodů).

Chcete-li si zobrazit všechny právě probíhající IP relace, zobrazte si stránku IP

Filter Configuration a klikněte na tlačítko **Session**. Bude zobrazena tabulka relací, která pro každou z nich obsahuje tato pole:

- **Session Index** (index relace): Identifikační číslo přidělené systémem IP relaci (všem relacím je tato identifikace přidělena bez ohledu na to, zda na ně je použito pravidlo IP filtru či není).
- **Time to expire** (expirační doba): Počet sekund, po nichž bude relace automaticky ukončena.
- **Protocol**: Základní protokol použitý při spojení, jako je TCP, UDP, ICMP atd.
- **I/F** (interface): Rozhraní, na němž je pravidlo IP filtru aktivováno.
- **IP Address**: IP adresy, jichž se komunikace týká. První ukazuje na počítač, který komunikaci vyvolal.
- **Port**: Čísla portů, mezi nimiž probíhá komunikace.
- **In/Out Rule Index**: Počet pravidel IP filtru, která se vztahují na tuto relaci (přiřazeno při vytváření pravidla).
- **In/Out Action**: Akce (accept, deny nebo unknown) uplatněná vůči paketům přicházejícím nebo odcházejícím po rozhraní. Určuje se při tvorbě pravidla.
- **Actions**: Obsahuje ikonu () , která slouží pro zrušení relace. Když zrušíte relaci, komunikace se přeruší.

Kliknutím na tlačítko  si můžete zobrazit čerstvá data.

2.3.4 Firewall

Home Configure Services Admin

NAT | RIP | IP Filter | FireWall | DNS Relay

FireWall Configuration

This Page is used to view FireWall Configuration.

Firewall Global Configuration	
Blacklist Status:	☐ Enable ☒ Disable
Blacklist Period(min):	10
Attack Protection:	☐ Enable ☒ Disable
DOS Protection:	☐ Enable ☒ Disable
Max Half open TCP Conn.:	25
Max ICMP Conn.:	25
Max Single Host Conn.:	75
Log Destination:	☐ Email ☒ Trace
E-Mail ID of Admin 1:	
E-Mail ID of Admin 2:	
E-Mail ID of Admin 3:	

Submit Cancel Black List Refresh Help

Konfigurace firewallu

Jednou z vestavěných funkcí softwaru modemu/routeru je funkce firewallu, jejímž účelem je chránit Váš systém proti útokům typu Denial of Service (DoS) čili vyřazení z provozu a ostatním záludným přístupům do Vaší sítě. Můžete také nastavit jak mají být potenciální útoky monitorovány a kdo má být v takovém případě automaticky vyrozuměn.

Konfigurace globálních nastavení

S konfigurací globálních nastavení firewallu Vám pomohou následující pokyny:

1. Není-li právě zobrazena stránka Firewall Configuration, klikněte na záložku Services a z nabízených funkcí vyberte funkci **Firewall**.
2. Upravte potřebné hodnoty v tabulce globálního nastavení firewallu:

- **Black List Status:** Chcete-li aby modem/router udržoval a používal „černou listinu“, klikněte na *Enable*. V opačném případě volte *Disable*.
- **Black List Period (min):** Udává interval v minutách, během něhož zůstane IP adresa počítače na černé listině (tzn. veškerý provoz pocházející z tohoto počítače bude na všech rozhraních ADSL modemu/routeru blokován). Více informací viz níže v části Správa černé listiny.
- **Attack Protection** (ochrana proti útokům): Chcete-li vestavěné ochranné funkce (firewallu) proti běžným typům útoků využívat, klikněte na políčko *Enable*:
 - o IP Spoofing: Odesílání paketů přes WAN rozhraní, které obsahují jako zdrojovou adresu IP adresy vnitřní sítě.
 - o Tear Drops: Posílání paketů, které obsahují překrývající se fragmenty.
 - o Smurf and Fraggle: Odesílání paketů, které obsahují jako zdrojovou adresu WAN nebo LAN IP adresu typu broadcast.
 - o Land Attack: Posílání paketů, které obsahují stejnou zdrojovou i cílovou IP adresu.
 - o Ping of Death: Pakety nepovolené délky.
- **DoS Protection:** Chcete-li využít ochranu proti následujícím útokům, zatrhněte políčko *Enable*:
 - o SYN DoS
 - o ICMP DoS
 - o Per-host DoS protection
- **Max Half Open TCP Connection:** Nastavuje počet souběžných IP relací vyjádřený v procentech, které mohou být v napůl otevřeném stavu. V normální TCP komunikaci jsou pakety v tomto stavu jen krátce při iniciaci spojení. Stav se změní na aktivní během výměny paketů a uzavření po ukončení výměny. TCP spojení mohou využívat nejvýše tolik napůl otevřených relací, kolik je vůbec povoleno vést souběžných IP relací. V případě překročení povoleného procenta budou napůl otevřené relace uzavřeny a nahrazeny nově vznikajícími relacemi.
- **Max ICMP Connection:** Určuje procento současných IP relací, které mohou být využity pro ICMP zprávy. Je-li procento překročeno, budou starší ICMP relace nahrazovány relacemi nově vznikajícími.
- **Max Single Host Connection:** Uvádí procento současných IP relací, které vycházejí z jednoho počítače. Tato hodnota by měla brát v úvahu celkový počet počítačů v síti.
- **Log Destination:** Udává, jak budou pokusy o porušení ochranných nastavení sledovány. Záznamy takových událostí mohou být posílány po síti ke zpracování utilitě *Trace* nebo odesílány e-mailem určenému správci.
- **E-mail ID of Admin 1/2/3:** Udává e-mailové adresy správců, kam se mají posílat informace o zjištěných útocích. Adresy se zadávají ve standardním internetovém tvaru: jnovak@neco.cz.

E-mailová zpráva bude obsahovat dobu útoku, IP adresu zdrojového počítače, cílovou IP adresu, použitý protokol, zdrojový a cílový port a počet útoků během předcházejících 30 minut. Pokud byl použit

protokol ICMP, bude zpráva obsahovat místo zdrojového a cílového portu typ a kód ICMP.

3. Klikněte na tlačítko **Submit**.
4. Zobrazte záložku Admin a klikněte na funkci **Commit & Reboot**.
5. Klikněte na tlačítko **Commit**, aby se provedené změny trvale uložily.

Správa černé listiny

Pokud jsou zachyceny pakety, které porušují nastavení firewallu nebo pravidla IP filtru, lze na určitou dobu zablokovat IP adresu, z níž tyto pakety pocházejí. Použití černé listiny můžete povolit nebo zakázat pomocí výše popsaných nastavení. Zdrojový počítač bude na černé listině po dobu, kterou určíte.

Chcete-li vidět, které počítače jsou právě na černé listině, klikněte na tlačítko **Black List** v dolní části stránky Firewall Configuration. Pro každý z případů tabulka uvádí následující informace:

- **Host IP Address:** IP adresa počítače, který odeslal pakety porušující pravidla.
- **Reason** (důvod): Stručný popis typu porušení. Jestliže paket porušil pravidlo IP filtru, objeví se text, který jste zadali do pole Log Tag (viz odstavec 2.3.3 „Vytváření pravidel IP filtru“).
- **IPF Rule ID:** Porušil-li paket pravidlo IP filtru, bude toto pole obsahovat identifikační číslo tohoto pravidla.
- **Action(s):** Obsahuje ikonu , na kterou můžete kliknout a odstranit záznam ze seznamu dříve, než mu vyprší zadaná doba platnosti.

Zapnutí FireWallu

V továrním nastavení je FireWall vypnutý. Zapnutí FireWallu s max. mírou zabezpečení docílíte tím, že na záložce **Services** vyberete **FireWall** a ve **FireWall Configuration** dáte **Enable** u **Blacklist status**, **Attack Protection** a u **DOS Protection**.

Následně v **IP Filter** si nastavte u **Security Level** položku **High**

2.3.5 DNS Relay

The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Configure', 'Services', and 'Admin'. Below the navigation bar, there are links for 'NAT', 'RIP', 'IP Filter', 'FireWall', and 'DNS Relay'. The main heading is 'Domain Name Service (DNS) Configuration'. A text block states: 'This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.' Below this, there are radio buttons for 'Enable' (selected) and 'Disable'. A table with the header 'DNS Server IP Address' and 'Action' is shown, containing the text 'No DNS Entries!'. Below the table are four input fields and an 'Add' button. At the bottom, there are four buttons: 'Submit', 'Cancel', 'Refresh', and 'Help'.

Konfigurace DNS

Krátce o DNS

Servy tzv. jmenného doménového systému (Domain Name Systém) si ve svých databázích vedou záznamy o doménových jménech serverů jaká zadáváte ve webovém prohlížeči (např. „yahoo.com“) a jejich numerických IP adresách, které se používají při směrování v Internetu.

Jakmile zadá uživatel doménové jméno serveru do webového prohlížeče, musí jeho počítač nejprve odeslat žádost DNS serveru o ekvivalentní IP adresu. DNS server se pokusí vyhledat záznam ve vlastní databázi a pokud jej nemá, spojí se s DNS serverem vyšší úrovně. Poté co je příslušná adresa nalezena, odešle se žádajícímu počítači a stává se součástí odesílaných paketů po zbytek komunikace.

Přirazování DNS adres

Do konfigurace je vhodné zadat více adres DNS. Vytvoří se tak alternativa pro případ, že je hlavní DNS server mimo provoz nebo zahlcen požadavky. Poskytovatelé internetových služeb obvykle poskytují adresu primárního a sekundárního DNS serveru a mohou nabídnout i další. Počítače ve Vaší síti se adresy DNS dozvídají jedním z těchto způsobů:

- **Staticky:** Adresu DNS poskytnutou Vaším ISP můžete sdělit každému PC ve vlastnostech jeho připojení k síti, (odstavec 1.5).
- **Dynamicky z DHCP poolu:** Můžete využít funkce DHCP serveru Vašeho ADSL/Ethernet modemu/routeru a vytvořit adresový pool obsahující adresy DNS, které budou distribuovány jednotlivým počítačům.

V obou případech můžete specifikovat aktuální adresy DNS serverů Vašeho ISP nebo také můžete specifikovat pouze síťový port ADSL modemu/routeru (např. 10.0.0.138). Zvolíte-li poslední možnost, bude modem/router plnit funkci DNS Relay, jak je popsáno v následující části.



Jestliže zadáte aktuální adresu DNS přímo do PC nebo prostřednictvím DHCP, DNS Relay se používat nebude.

Konfigurace DNS Relay

Když na místo adresy DNS použijete IP adresu síťového portu modemu/routeru, bude toto zařízení plnit funkci DNS Relay zcela automaticky. Protože modem/router není DNS serverem, předá požadavek na vyhledání IP adresy z doménového jména přijatý od některého z počítačů Vaší sítě DNS serveru Vašeho ISP. Odpověď DNS serveru potom předá žádajícímu počítači. Aby mohl modem/router vykonávat funkci DNS Relay, musí si udržovat IP adresy DNS serverů, s nimiž je v kontaktu. Zjistí si je jedním nebo oběma následujícími způsoby:

- **Prostřednictvím PPP:** Používá-li zařízení ke spojení s ISP protokol PPP, dokáže adresu primárního a sekundárního DNS serveru zjistit pomocí tohoto protokolu. Má-li být použita tato metoda, je třeba zaškrtnout políčko „Use DNS“ ve vlastnostech rozhraní PPP. (Toto nastavení nelze změnit u existujícího PPP rozhraní, musíte původní zrušit a nahradit je novým s požadovanými vlastnostmi). Tento způsob má jednu výhodu, když ISP změní adresu DNS serveru, nemusíte měnit nastavení ADSL modemu/routeru, popř. obcházet všechna PC a měnit jejich konfiguraci.
- **Z konfigurace ADSL/Ethernet modemu/routeru:** Můžete využít funkce DNS modemu/routeru a zadat DNS adresu Vašeho ISP. Pokud modem/router také používá rozhraní PPP s aktivovaným parametrem „Use DNS“, pak budou zadané adresy použity vedle DNS adres zjištěných z protokolu PPP. Není-li parametr „Use DNS“ aktivován nebo se používá jiný typ protokolu, např. EoA, budou použity pouze zadané adresy jako primární a sekundární DNS.

Při konfiguraci DNS Relay postupujte následovně:

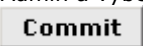
1. Počítačům v síti nastavte síťovou IP adresu ADSL modemu/routeru jako jejich adresu DNS serveru – buď statickým zadáním do každého počítače

nebo zadáním IP adresy LAN portu modemu/routeru, popř. adresy 0.0.0.0 jako Adresy DNS v poolu DHCP serveru.

2. Používáte-li připojení PPP k Vašemu ISP, nastavte je na použití DNS („Use DNS“), aby byly zjištěné adresy použity pro DNS Relay.

-- nebo--

Nepoužíváte-li PPP připojení (nebo chcete kromě zjištěných adres z PPP protokolu používat ještě ručně zadané), nastavte DNS adresy na ADSL modemu/routeru takto:

- a. Klikněte na záložku Services a ze seznamu funkcí vyberte **DNS**. Zobrazí se stránka DNS Configuration.
 - b. Do prázdného řádku запиšte adresu DNS serveru a klikněte na . Zadat smíte jen dvě adresy.
 - c. Klikněte na políčko **Enable** a potom na .
3. Klikněte na záložku Admin a vyberte funkci **Commit & Reboot**.
 4. Klikněte na tlačítko , aby se provedené změny trvale uložily.

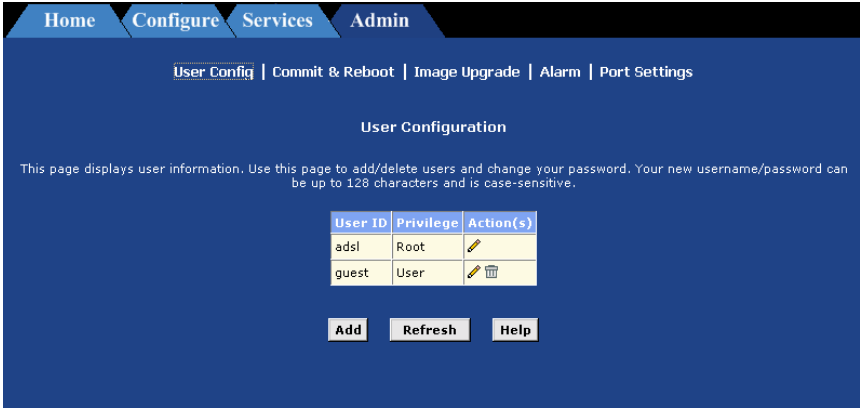


DNS adresy přidělené počítačům před aktivací funkce DNS Relay zůstávají v platnosti do nejbližšího restartu PC. DNS bude fungovat jen tehdy, když v poli IP adresy DNS na PC bude uvedena IP adresa síťového portu modemu/routeru.

Podobně, když po aktivaci funkce DNS Relay zadáte adresu DNS (jinou než IP adresu LAN portu) do DHCP poolu nebo staticky na PC, potom bude tato adresa používána namísto dotazů pře DNS Relay.

2.4 ADMIN

2.4.1 User Config - Uživatelská konfigurace



User ID	Privilege	Action(s)
adsl	Root	
guest	User	

Add **Refresh** **Help**

Změna přihlašovacího hesla

Když se poprvé přihlásíte do programu Configuration Manager, použijete k tomu výchozí uživatelské jméno a heslo (*root / root*). Systém povoluje pouze jedno uživatelské jméno a heslo. Jedině heslo si můžete změnit.



Toto uživatelské jméno a heslo nejsou přihlašovacími informacemi, které použijete při připojení k ISP.

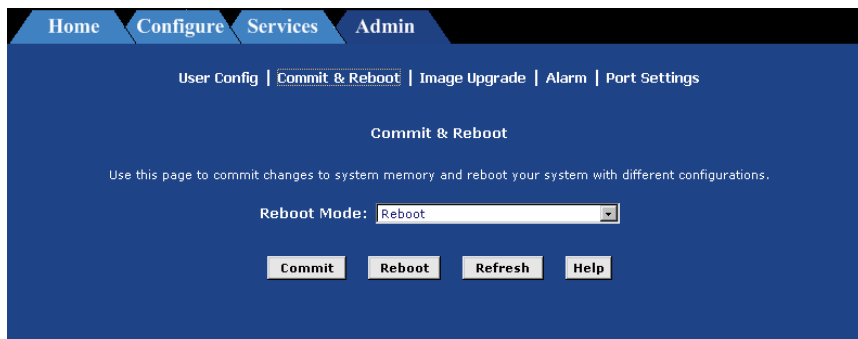
Jak změnit heslo do Configuration Manageru:

1. Není-li právě zobrazena stránka User Password Configuration, klikněte na záložku Admin. Pak se stránka standardně zobrazí.
2. Do políčka **Old Password** zadejte Vaše staré heslo.
3. Do políčka **New Password** zapište nové heslo a v políčku **Confirm New** je pro ověření zopakujte.

Heslo může obsahovat až 8 ASCII znaků. Rozlišují se malá a velká písmena, proto musíte heslo při přihlašování psát přesně tak, jako když jste prováděli jeho změnu.

4. Klikněte na **Submit**.
5. Zobrazte záložku Admin a klikněte na příkaz **Commit and Reboot**.
6. Klikněte na **Commit**, aby se změna trvale uložila.

2.4.2 Commit & Reboot



Uložení změn a nové zavedení systému

Uložení změn

Kdykoli prostřednictvím programu Configuration Manager provedete změnu systémových nastavení, ukládají se tyto změny nejprve do dočasné paměti tvořené pamětí RAM (random access memory). Tyto změny jsou účinné od okamžiku, kdy je uplatníte (stisknete tlačítko Submit), ale mohli byste je ztratit při resetu nebo vypnutí zařízení.

Změny můžete uložit trvale v paměti typu flash.



Při uplatnění změn tlačítkem **Submit** se tyto změny uloží jen do nejbližšího resetu nebo vypnutí modemu/routeru. Teprve uložení tlačítkem **Commit** zaznamená změny trvale.

Rozhodnete-li se změny trvale uložit, klikněte na záložku Admin a vyberte funkci

Commit & Reboot. Poté klikněte na tlačítko **Commit**. Nevšímejte si výběru v rozbalovacím seznamu Reboot Mode, nemá na proces uložení změn žádný vliv.

Změny jsou uloženy v permanentní paměti. Předcházející nastavení se při tom kopíruje do záložní paměti, takže je lze znovu obnovit, pokud se ukáže, že nové nastavení nefunguje podle očekávání. Následující část popisuje jak to udělat.

Nové zavedení systému zařízení

Příkaz k novému zavedení systému vydáte na stránce Commit & Reboot. Zde vyberte z rozbalovacího seznamu režim *reboot* a klikněte na tlačítko

Reboot

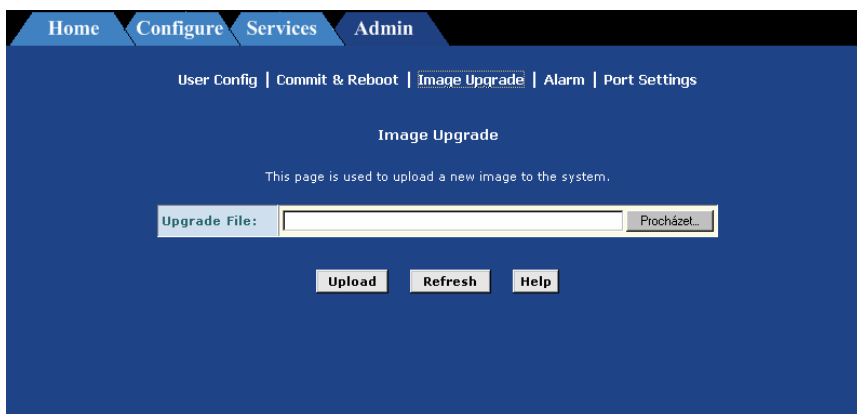
. Pro natažení systému můžete použít tři funkčně odlišných možností:

- *Reboot* (zavést poslední konfiguraci systému) zavede systém s aktuálním nastavením uloženým v permanentní paměti včetně všech změn, které jste předtím uložili.
- *Reboot from Default Configuration* (zavést systém ve výchozí konfiguraci) zavede systém ve výchozím nastavení výrobce. Tato volba vymaže všechna uživatelská nastavení.
- **Tlačítko Reset** na zadním panelu ADSL Ethernet modemu/routeru (zmáčknout 3x v rozmezí 15 sekund). Tímto postupem se rovněž obnoví výchozí nastavení výrobce. Všechny změny provedené uživatelem budou ztraceny.



POZOR! Pro aktivaci nových změn používejte funkci (tlačítko) **Commit**, v žádném případě ne funkci *Reboot from Default Configuration* nebo tlačítko **Reset** na zadním panelu ADSL/Ethernet modemu/routeru. Tímto postupem byste obnovili výchozí nastavení výrobce! Všechny změny provedené uživatelem by byly ztraceny.

2.4.3 Image Upgrade



Upgrade softwaru

Váš ISP vám může příležitostně dodat novou verzi softwaru pro ADSL/Ethernet modem/router. Celý software je obsažen v jednom souboru, kterému se říká image (obraz). Image se skládá z několika částí, z nichž každá implementuje nějakou skupinu funkcí. Při modernizaci softwaru můžete buď využít funkci, která provede kompletní upgrade softwaru, nebo jen jeho určitou část. Postupujte podle následujících pokynů:

1. Není-li právě zobrazena stránka Image Upgrade, klikněte na záložku Admin a vyberte funkci **Image Upgrade**.
2. Do pole Upgrade File zadejte jméno souboru (včetně cesty), který jste získali od ISP. Soubor také můžete vyhledat na disku svého počítače nebo CD, pomocí tlačítka **Browse...**.

Jméno souboru obsahující nový image musí být některou z následujících možností:

- TEImage.bin
- TEDsl.gsz
- TEAppl.gsz
- Filesys.bin
- TEPatch.bin

3. Klikněte na tlačítko **Upload**.

Po několika vteřinách by se měla zobrazit zpráva podobného znění (Jméno souboru se může lišit):

File: TEDsl.gsz successfully saved to flash. Please reboot for the new image to take effect.

(Soubor: TEDsl.gsz uložen do paměti flash. Zavedte, prosím, znovu systém, aby se změna projevila).

4. Vypněte napájení modemu/routeru, počkejte několik vteřin a znovu zařízení zapněte.

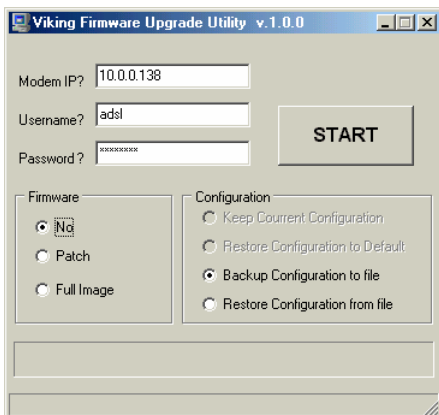
Nyní je chod modemu/routeru řízen novým softwarem. Pokud systém nefunguje správně, požádejte o pomoc Vašeho ISP.

Uložení uživatelského nastavení a jeho zálohování v PC

Chcete-li změny provedené v nastavení routeru uložit do souboru a následně z tohoto souboru obnovit při potížích poslední funkční nastavení, můžete tak učinit pomocí utility **Viking_Upgrade.exe**, kterou můžete najít na přiloženém CD v adresáři **Software**. Postup je následující:

Uložení aktuálního nastavení:

1. Vložíte CD do mechaniky a spustíte utilitku D:\Software\Viking_Upgrade.exe
2. Vyplňte IP adresu routeru, uživatelské jméno a heslo (např.: adsl / adsl1234).
3. Nastavte položky pro ukládání viz. obrázek níže a klikněte na **START**.
4. Vyberte adresář, kam budete chtít soubor TECfg.bin se zálohou Vašeho nastavení uložit.
5. Následně proběhne uložení.



Obnovení uživatelského nastavení ze souboru:

1. Vložíte CD do mechaniky a spustíte utilitku
D:\Software\Viking_Upgrade.exe
2. Vyplňte IP adresu routeru, uživatelské jméno a heslo (např.: adsl / adsl1234).
3. Nastavte položky pro obnovu nastavení viz. obrázek níže a klikněte na START.
4. Zadejte cestu k uloženému souboru TECfg.bin se zálohou nastavení.
5. Následně proběhne přehrání nastavení routeru ze zálohovaného souboru.

2.4.4 Alarm

Zobrazení systémových výstrah

Pomocí Configuration Manageru si můžete prohlédnout výstrahy zjištěné systémem. Výstrahy, někdy se též označují jako alarm nebo trap, jsou způsobeny řadou událostí v systému, např. pokusy o navázání spojení, reset, změny konfigurace apod.

Ačkoli si za normálních okolností tyto události nebudete příliš často prohlížet, někdy Vám mohou pomoci při odstraňování problémů se zařízením. (Navzdory označení, ne všechny výstrahy indikují problém s funkcí systému.)

Není-li právě zobrazena stránka Alarm, klikněte na záložku Admin a vyberte funkci **Alarm**.

Každý řádek tabulky obsahuje čas a datum výstrahy, typ výstrahy a stručný popis příčiny.

Z rozbalovací nabídky Refresh Rate si můžete vybrat, v jakém časovém intervalu bude stránka obnovována, aby zobrazovala nová data.

Celý seznam výstrah můžete vymazat kliknutím na tlačítko **Clear**. Pak se začnou shromažďovat nová data, která si můžete zobrazit stisknutím tlačítka

Refresh

2.4.5 Port Settings

The screenshot shows a web-based configuration interface for a network device. At the top, there is a navigation bar with tabs: Home, Configure, Services, and Admin. Below this, a sub-navigation bar contains links: User Config, Commit & Reboot, Image Upgrade, Alarm, and Port Settings (which is highlighted). The main content area is titled 'Port Settings' and includes a descriptive text: 'This page is used to modify various port settings across the system.' Below the text is a table with three rows, each representing a different protocol's port settings. The first row is for HTTP Port, with a range of (80, 61000-62000) and a value of 80. The second row is for Telnet Port, with a range of (23, 61000-62000) and a value of 23. The third row is for FTP Port, with a range of (21, 61000-62000) and a value of 21. At the bottom of the form, there are three buttons: Submit, Refresh, and Help.

Protocol	Port Range	Port Value
HTTP Port:	(80, 61000-62000)	80
Telnet Port:	(23, 61000-62000)	23
FTP Port:	(21, 61000-62000)	21

Submit **Refresh** **Help**

Změna nastavení portů

Popis čísel IP portů

Součástí hlavičky IP paketu je číslo cílového portu. Modemu/routeru používají toto číslo spolu s IP adresou při odesílání paketu k jeho zamýšlenému příjemci.

Například všechny datové pakety, které Váš ADSL/Ethernet modem/router přijme z Internetu, obsahují stejnou IP adresu (Vaši veřejnou IP adresu), jako určení cíle. Podle čísla cílového portu obsaženého v paketu však modem/router pozná, jestli má paket předat svému zabudovanému Web serveru nebo Telnet serveru anebo jej odeslat některému počítači ve vnitřní síti.

V Internetové komunitě byl vypracován seznam obecně používaných serverů, jako je HTTP, Telnet, e-mail a celá řada dalších a každému z nich bylo přiřazeno jedinečné číslo portu. Nejsou sice povinná, ale je vhodné je používat při vedení komunikace mezi samostatně spravovanými sítěmi.

Změna čísel portů ADSL/Ethernet modemu/routeru

V určitých případech možná budete chtít přiřadit zabudovanému http nebo Telnet serveru modemu/routeru nestandardní čísla portů. Následující situace je jedním z případů, kdy je číslo portu http nutné změnit:

Máte ve své síti Webový server, která má být viditelný z Internetu za použití pravidla NAT (rdr flavor), které přesměrovává přicházející http pakety na tento Web server. Když přicházející IP pakety obsahují jako cílovou adresu Vaši veřejnou IP adresu (která je přiřazena WAN portu modemu/routeru) a standardní číslo portu pro Web server – 80, pravidlo NAT rozpozná číslo portu a přesměruje pakety na lokální IP adresu Vašeho Web serveru.

Předpokládejme nyní, že za této situace budete chtít zajistit externí přístup k tomuto konfiguračnímu programu, aby se k němu mohl např. přihlásit Váš ISP a provádět správu vašeho systému. Přístup do programu Configuration Manager vyžaduje ve skutečnosti přístup k zabudovanému Web serveru (jinak též nazývanému HTTP server ADSL modemu/routeru). V takovém případě bude muset využít funkci pro nastavení portů a přidělit portu HTTP serveru nestandardní hodnotu. Pokud byste to neudělali, pravidlo pro překlad adres NAT by pokus Vašeho ISP o přihlášení přesměrovalo místo na HTTP server modemu/routeru na HTTP server ve vaší lokální síti.

Proto když se bude chtít technik ISP přihlásit do Vašeho programu Configuration Manager, bude muset v prohlížeči zadat IP adresu Vašeho

ADSL/Ethernet modemu/routeru následovanou dvojtečkou a nestandardním číslem portu, jak ukazuje následující příklad:

http://10.0.1.16:61000

Váš ISP může mít rovněž své důvody pro použití určitých nestandardních čísel http a Telnet portů, a proto byste s ním případné změny tohoto nastavení měli vždy konzultovat.

Při změně čísla portu postupujte následovně:

1. Není-li právě zobrazena stránka Port Setting, klikněte na záložku Admin a vyberte funkci **Port Setting**.
2. Do příslušného pole zadejte číslo portu a klikněte na tlačítko .
 - Standardní číslo portu pro HTTP server je 80, pro Telnet server 23.
 - Nestandardní čísla portů pro tyto servery můžete volit z rozmezí 61000 až 62000.
3. Klikněte na funkci **Commit & Reboot** a pak na tlačítko , aby se provedená změna uložila do permanentní paměti.
4. Na stránce Commit & Reboot klikněte na .

Uvědomte si, že nové nastavení portů začne platit až po novém natažení systému.