



Bezdrátový širokopásmový směrovač

Návod k použití

Úvod	4
Charakteristika	4
Minimální požadavky	4
Obsah balení	4
Poznámky	5
Seznámení se směrovačem	5
Zadní panel	6
Čelní panel	7
Diagram nastavení	7
Spuštění	7

Kapitola 1	
Rychlé nastavení	14
Krok 1) Časové pásmo	15
Krok 2) Typ připojení	16
1.1. Kabelový modem	16
1.2. Fixní IP-xDSL	18
1.3 PPPoE	19
1.4. PPTP	21
1.5 L2TP	23
1.6 Telstra Big Pond	25

Kapitola 2	26
Základní nastavení	27
2.1 Systém	28
2.1.1 Časové pásmo	29
2.1.2 Nastavení hesla	30
2.1.3 Dálkové nastavení	31
2.2 WAN	32
2.2.1 Bezdrátový / WiFi poskytovatel (ISP)	34
2.2.2 Dynamická IP	34
2.2.3 Statická IP adresa	34
2.2.4 PPPoE (PPP přes ethernet)	34
2.2.5 PPTP	34
2.2.6 L2TP	34
2.2.7 Telstra Big pond	34
2.2.8 DNS	35
2.2.9 DDNS	36
2.3 LAN	37
2.4. Bezdrát / WiFi Access Point	39
2.4.1 Základní nastavení	39
2.4.2 Pokročilé nastavení	41
2.4.3 Ochrana / zabezpečení	43

2.4.3.1 Pouze WEP	44
2.4.3.2 Pouze 802.1x	45
2.4.3.3 802.1 x a statický WEP	46
2.4.3.4 WPA sdílený klíč	47
2.4.3.5 WPA Radius	48
2.4.4 Kontrola přístupu	49
2.5. QoS	50
2.6 NAT	54
2.6.1 Přesměrování portu	55
2.6.2 Virtuální server	57
2.6.3 Zvláštní aplikace	59
2.6.4 Nastavení UpnP	62
2.6.5 Nastavení ALG	63
2.6.6 Statické směrování	64
2.7 Firewall	65
2.7.1 Kontrola přístupu	66
2.7.2 Blokování URL	70
2.7.3 DoS (Zamítnutí služby)	71
2.7.4 DMZ	72
Kapitola 3	73
Stav	73
3.1 Stav a informace	74
3.2 Připojení Internetu	75
3.3 Stav zařízení	76
3.4 Výpis systémových událostí	77
3.5 Výpis bezpečnostních událostí	78
3.6 Aktivní DHCP klient	79
3.7 Statistika	80
Kapitola 4	81
Nástroje	81
4.1 Konfigurace	82
4.2 Aktualizace Firmware	83
4.3 Resetování	84
Příloha A	85
Glosář/slovníček pojmů	86

Úvod

Blahopřejeme Vám k zakoupení tohoto bezdrátového širokopásmového směrovače / routeru. Toto zařízení umožňuje sdílení IP tak, aby se několik uživatelů dělilo o Internetové připojení přes ADSL nebo kabelový modem. Jednoduše nakonfigurujete Vaše nastavení připojení k Internetu ve směrovači, připojíte Váš počítač k LAN portu a můžete sdílet v síti soubory a přístup k Internetu. Jak se Vaše síť rozrůstá, můžete připojit další switch na LAN port směrovače, umožňující tak snadné rozšíření Vaší sítě o více uživatelů. Bezdrátový širokopásmový směrovač je opatřen vstupem/výstupem dle protokolu IEEE 802.11 g/b, který umožňuje vytvořit bezdrátovou WiFi síť. Bezdrátový širokopásmový směrovač poskytuje kompletní univerzální řešení pro středně velké firmy (SMB), malé kanceláře (SOHO) a moderní domácnosti. Nabízí snadno dostupnou síť a flexibilitu pro budoucí rozšiřování a zrychlování Vašeho spojení.

Charakteristika

- Vysoce výkonný přístup k Internetu (až 50M)
- Umožňuje několika uživatelům sdílet jednu Internetovou linku
- Podpora až 253 uživatelů
- Přístup k Internetu přes kabelový nebo xDSL modem
- Přístup do lokálního/privátního serveru v LAN z veřejné sítě
- Vybaven 4 LAN porty (10/100M) a jedním WAN portem (10/100M)
- Vybaven bezdrátovým Access Pointem dle IEEE 802.11 g/b
- Podpora DHCP (server/klient) pro snadné nastavení
- Podpora pokročilých vlastností jako jsou: zvláštní aplikace, DMZ, virtuální servery, kontrola přístupu, firewall.
- Umožňuje monitorovat stav směrovače (pomocí „logů“) jako je přihlášení DHCP klienta, systémové, bezpečnostní informace a stav zařízení/připojení
- Snadné použití s využitím konfigurace a správy pomocí webového prohlížeče vycházející z GUI
- Vzdálená správa umožňuje dálkovou konfiguraci a upgrade (přes Internet)

Minimální požadavky

- Jeden externí xDSL (ADSL) nebo kabelový modem s ethernetovým portem (RJ-45)
- Síťová karta (RJ45 konektor) pro všechny osobní počítače (PC)
- Počítače s prohlížečem (např. Internet Explorer 4.0 a vyšší)
-

Obsah balení

* Jeden bezdrátový širokopásmový směrovač / CD s návody k instalaci a

* Jeden uživatelský manuál / jeden el. adaptér / další příslušenství

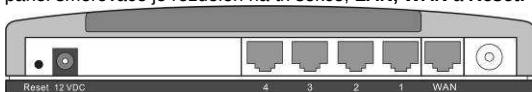
Poznámka

Funkce WAN „automatického odpojení po době nečinnosti“ nemusí pracovat korektně kvůli specifickým aktivitám některých síťových softwarových aplikací, počítačovým virům nebo útokům hackerů z Internetu. Například určitý software posílá do Internetu pakety na pozadí i přesto, že Internet nepoužíváte. Vypněte proto prosím svůj počítač, pokud jej nepoužíváte. Tuto funkci rovněž nemusí podporovat někteří poskytovatelé Internetového spojení (ISP). Proto se prosím ujistěte, že tato funkce pracuje správně, pokud tuto funkci používáte poprvé a zejména pokud poskytovatel Internetu (ISP) účtuje podle doby strávené použitím Internetu.

Seznámení se s širokopásmovým směrovačem / routerem

Zadní panel

Diagram (obr. 1.0) níže, ukazuje zadní panel širokopásmového směrovače. Zadní panel směrovače je rozdělen na tři sekce, **LAN**, **WAN** a **Reset**:



Obrázek 1.0

1) Lokální síť (LAN)

4 porty LAN širokopásmového směrovače pro připojení svých počítačů, tiskových serverů, přepínačů (switchů) atd.

2) Rozsáhlá / vnější síť (WAN)

WAN port je segment připojený k vašemu xDSL nebo kabelovému modemu a je spojen s Internetem.

3) Reset

Resetovací tlačítko umožňuje provedení jedné ze dvou věcí.

- 1) Pokud máte problémy s Vaším směrovačem, stiskněte resetovací tlačítko směrovače hrotem propisky (na méně než 4 vteřiny) a směrovač se restartuje, přičemž si zachová svou původní (nebo Vámi nastavenou) konfiguraci.
- 2) Pokud problémy přetrvávají nebo jsou problémy s nastavením vážné či jste zapomněli heslo, stiskněte resetovací tlačítko na déle než 4 vteřiny a směrovač se sám resetuje na tovární přednastavení (**upozornění:** Vaše původní konfigurace bude nahrazena standardním továrním nastavením)

Přední panel

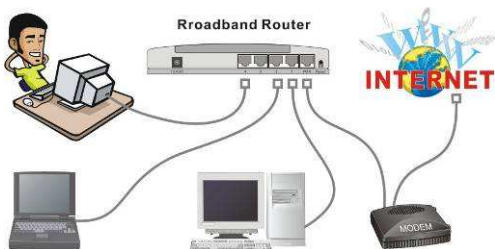
Na předním panelu směrovače jsou LED kontrolky, které Vás informují o aktuálním stavu směrovače. Níže je vysvětlení každé LED a její popis.



LED	Stav	Popis
PWR	ON	Elektrický zdroj směrovače je zapnut
WAN 10/100M	ON	WAN port 100Mbps je připojen
	Off	WAN port 10Mbps je připojen
WAN LNK/ACT	ON	WAN je připojen
	Off	WAN není připojen
	Bliká	WAN port je aktivní (ACT), data jsou odesílána
LAN 10/100M (Port 1-4)	ON	LAN port 100Mbps je připojen
	Off	LAN port 10Mbps je připojen
LAN LNK/ACT (Port 1-4)	ON	LAN je připojen
	Off	LAN bez připojení
	Bliká	LAN port je aktivní (ACT), data jsou odesílána
WLAN-G	ON	Bezdrátový LAN (WiFi) byl aktivován
	Off	Bezdrátový LAN je nečinný
	Bliká	Bezdrátový LAN je aktivní (ACT) data jsou odesílána

Diagram nastavení

Obrázek 1.2 níže ukazuje typické nastavení lokální sítě (LAN).



Obrázek 1.2

Spuštění

Dále jsou uvedeny pokyny krok za krokem, jak používat směrovač a získat připojení k Internetu.

- 1) Nastavte Vaši síť tak, jak je zobrazeno na diagramu nastavení výše (obr 1.2.).
2. Pak musíte nastavit Vaše klientské LAN PC tak, aby automaticky získal IP adresu. Všechna klientská LAN potřebují mít správnou IP adresu. Podobně jako domovní adresa i tato síťová umožňuje LAN klientům najít se vzájemně. (Pokud jste již máte nastaveno PC pro automatické získání IP, pak pokračujte krokem 3, strana 11)

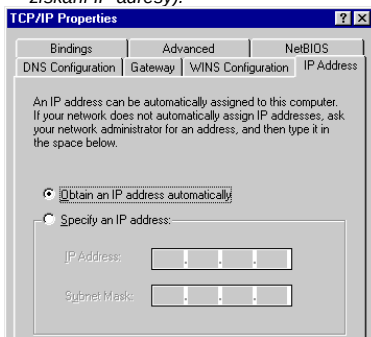
Nastavte konfiguraci PC pro automatické získání IP adresy

U širokopásmového směrovače je ve výchozím nastavení z továrny zapnut DHCP server. Znamená to, že můžete získat IP adresu automaticky, pokud je PC nastaveno pro automatické získání IP adresy. Tato sekce Vám ukáže jak konfigurovat Vaše PC tak, aby automaticky získalo IP adresu pro operační systémy Windows 95/98/Me, 2000 nebo NT. Pro jiné operační systémy (Macintosh, Sun atd.) postupujte podle návodu jejich výrobce. Dále je uveden postup jak krok za krokem konfigurovat Vaše PC pro automatické získání IP adresy pro operační systém 2a) Windows 95/98/Me, 2b) Windows XP, 2c) Windows 2000 a 2d) Windows NT.

2a) Windows 95/98/Me

1. Klikněte na tlačítko *Start* a zvolte *Settings (nastavení)*, pak klikněte na *Control Panel (kontrolní panel)*. Objeví se okno *Control Panel*.
2. Klikněte dvakrát na ikonu *Network (sítě)*. Objeví se okno *Network*.
3. Zkontrolujte Váš seznam komponentů sítě. Pokud není nainstalován TCP/IP, klikněte pro jeho instalaci na tlačítko *Add (přidat)*. Pokud je TCP/IP nainstalováno, přejděte ke kroku 6.
4. V dialogovém okně *Network Component Type (síťové komponenty)*, zvolte *Protocol (protokol)* a klikněte na tlačítko *Add (přidat)*.
5. V dialogovém okně *Select Network Protocol (Volba protokolu sítě)* zvolte *Microsoft a TCP/IP* a pak pro zahájení instalace protokolu TCP/IP klikněte na tlačítko *OK*.
6. Po instalaci TCP/IP se vraťte zpět k dialogovému oknu *Network (sítě)*. Na seznamu *Network Components (komponenty sítě)* zvolte *TCP/IP* a pak klikněte na tlačítko *Properties (vlastnosti)*.
7. Zkontrolujte všechny účty a ověřte následující nastavení:

- **Vazby/obecné:** Zkontrolujte *Client for Microsoft Networks (Klient pro síť Microsoft a File and printer sharing for Microsoft Networks (Sdílení souborů a tiskárny pro síť Microsoft))*.
- **Brána:** Všechna pole jsou prázdná.
- **Konfigurace DNS:** Zvolte *Disable DNS (neaktivní DNS)*.
- **Konfigurace WINS:** Zvolte *Disable WINS Resolution (neaktivní rozlišení WINS)*
- **IP adresa:** Zvolte *Obtain IP address automatically (automatické získání IP adresy)*.

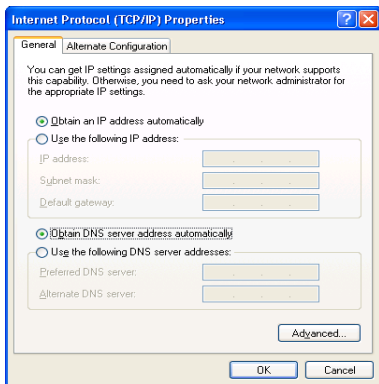


8. Restartujte počítač. Váš počítač nyní automaticky získá IP adresu z DHCP serveru širokopásmového směrovače

Upozornění: Ujistěte se prosím, že DHCP server širokopásmového směrovače je jediným dostupným DHCP ve Vaší LAN. Jakmile jste nastavili Váš počítač pro automatické získání IP adresy, postupujte prosím podle kroku 3 dále.

2b) Windows XP

1. Klikněte na tlačítko *Start* a zvolte *Settings (ovládací panel)*, pak klikněte na *Network Connections (síťová připojení)*. Objeví se okno *Network Connections*.
2. Klikněte dvakrát na ikonu *Local Area Connection (připojení k místní síti)*. Objeví se okno *Local Area Connection*.
3. Zkontrolujte seznam komponentů sítě (tlačítko „vlastnosti“). V seznamu najít protokol sítě Internet (*TCP/IP*). Zvolte jej a klikněte na tlačítko *Properties (vlastnosti)*.
4. V okně *Vlastností protokolu Internetu (TCP/IP)* zvolte *Automatické získání IP adresy ze serveru DHCP a Automatické získání adresy DNS serveru (Obtain DNS server address automatically)*



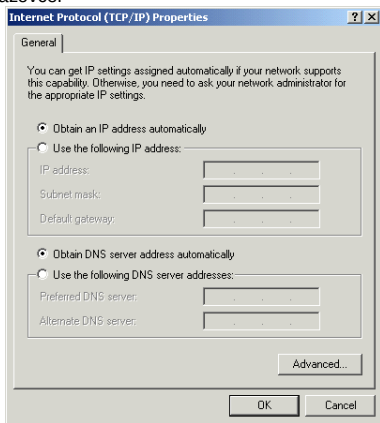
5. Klikněte na *OK* pro potvrzení nastavení. Váš počítač nyní automaticky získá IP adresu z DHCP serveru z Vašeho širokopásmového směrovače

Upozornění Ujistěte se prosím, že DHCP server širokopásmového

směrovače je jediným dostupným DHCP ve Vaší LAN. Jakmile jste zkonfigurovali svůj počítač pro automatické získání IP adresy, pokračujte prosím krokem 3 dále.

2c) Windows 2000

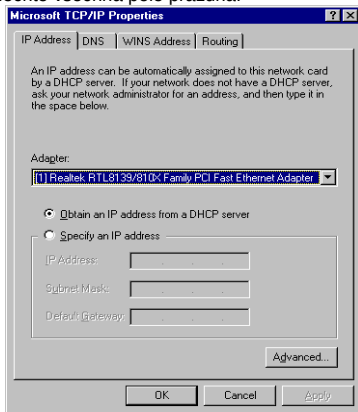
1. Klikněte na tlačítko *Start* a zvolte *Settings (nastavení)*, pak klikněte na *Control Panel (kontrolní panel)*. Objeví se okno kontrolní panel.
2. Klikněte dvakrát na ikonu *Network (sít)* a okno *Dial-up Connections (vytáčení připojení)*, klikněte dvakrát na ikonu *Local Area Connection (místní připojení)*. Objeví se okno *Local Area Connection*.
3. V okně *Local Area Connection* klikněte na tlačítko *Properties (vlastnosti)*.
4. Zkontrolujte Váš seznam Komponentů sítě. Na svém seznam by jste měli vidět *Internet Protocol (TCP/IP)*. Zvolte jej a klikněte na tlačítko *Properties (vlastnosti)*.
5. V okně vlastnosti protokolu Internetu (TCP/IP) zvolte *Obtain an IP address automatically (automaticky získat IP adresu)* a *Obtain DNS server address automatically (automaticky získat adresu DNS serveru)* jak je uvedeno na následující obrazovce.



6. Pro potvrzení nastavení klikněte na *OK*. Váš počítač nyní automaticky získá IP adresu z Vašeho DHCP serveru širokopásmového směrovače.
Upozornění: Ujistěte se prosím, že DHCP server širokopásmového směrovače je jediným dostupným DHCP ve Vaší LAN. Jakmile jste zkonfigurovali Váš počítač pro automatické získání IP adresy, pokračuje prosím krokem 3 dále.

2d) Windows NT

1. Klikněte na tlačítko *Start* a zvolte *Settings (nastavení)*, pak klikněte na *Control Panel (kontrolní panel)*. Objeví se okno kontrolní panel.
2. Klikněte dvakrát na ikonu *Network (sítě)*. Objeví se okno *Network (sítě)*. V okně *Network* zvolte *Protocol (protokol)*.
3. Zkontrolujte jestli je *TCP/IP Protocol* na Vašem seznamu *Network protocols (Protokoly sítě)*. Pokud není TCP/IP nainstalován, klikněte pro instalaci na tlačítko *Add (přidat)*. Pokud je TCP/IP nainstalováno, přejděte ke **kroku 5**.
4. V okně *Select Network Protocol (Volba protokolu sítě)*, zvolte *TCP/IP Protocol* a pro instalaci TCP/IP protokolu stiskněte tlačítko *OK*. Pro dokončení instalace budete možná potřebovat své CD Windows.
5. Jakmile nainstalujete TCP/IP vraťte se na okno *Network*. V seznamu *Network Protocols (protokol sítě)* zvolte *TCP/IP* a pak klikněte na *Properties (vlastnosti)*.
6. Zkontrolujte všechny účty a ověřte následující nastavení:
 - **IP adresa:** Zvolte *Obtain and IP address from a DHCP server (získat IP z DHCP serveru)*
 - **DNS:** Nechte všechna pole prázdná.
 - **WINS:** Nechte všechna pole prázdná.
 - **Směrování:** Nechte všechna pole prázdná.



7. Pro potvrzení nastavení klikněte na OK. Váš počítač nyní automaticky získá IP adresu z Vašeho DHCP serveru širokopásmového směrovače.

Upozornění: Ujistěte se prosím, že DHCP server širokopásmového směrovače je jediným dostupným DHCP ve Vaší LAN.

Jakmile jste na Vašem počítači zkonfigurovali automatické získání IP adresy, pokračujte prosím krokem 3 dále.

3) Jakmile jste nastavili automatické získání IP adres, DHCP server směrovače automaticky přidělí IP adresu síťovým klientům. Primárně (default) je DHCP server směrovače aktivní a k přidělení IP adresy tedy dojde automaticky.

Získání IP adresy lze ověřit dle Přílohy A na konci tohoto manuálu.

Upozornění: Ujistěte se prosím, že DHCP server širokopásmového směrovače je jediným dostupným DHCP ve Vaší síti LAN.

Pokud se v LAN nachází jiný DHCP, pak musíte vypnout jeden z DHCP serverů. (Pro odpojení serveru DHCP směrovače viz dále kapitola 2 LAN Port)

4) Jakmile Váš počítač získal IP adresu z Vašeho směrovače, zadejte IP adresu **192.168.2.1** (vlastní IP adresa směrovače) do webového prohlížeče Vašeho počítače <http://192.168.2.1> a stiskněte <enter>

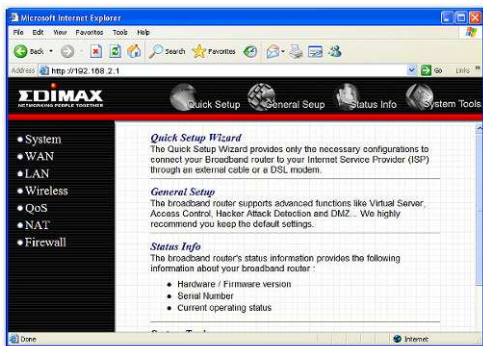
5) Objeví se obrazovka pro přihlášení. Zadejte „User Name“ (jméno uživatele) a „Password“ (heslo), pak pro přihlášení potvrďte <OK>.

Upozornění: Implicitně je jméno uživatele „**admin**“ a heslo „**1234**“.

Z důvodu ochrany doporučujeme, abyste co nejdříve heslo změnili (v hlavním nastavení/systém/heslo, viz kapitola 2)



6) Objeví se **HOME** page. Domovská stránka je rozdělena na čtyři sekce, **Quick Setup** (průvodce rychlým nastavením), **General Setup** (všeobecné nastavení), **Status Info** (stavové info) a **System Tools** (systémové nástroje).



Quick Setup Wizard (průvodce rychlým nastavením) (Kapitola 1)
Rychlé nastavení připojení Internetu pro drátové připojení. Pro bezdrátové / WiFi připojení zvolte typ WAN připojení (viz kapitola 2.2.1).

General Setup (všeobecné nastavení) (Kapitola 2)
Tato část obsahuje konfiguraci pokročilých funkcí směrovače: Mapování adres, Virtuální server, Kontrolu přístupu, Ochranu před útoky hackerů, DMZ, Speciální aplikace a další funkce pro splnění Vašich požadavků na síť.

Dále se zde konfiguruje Typ WAN připojení bezdrátové (WiFi) nebo drátové (Ethernet).

Status info (informace o stavu) (Kapitola 3)

V této části můžete vidět systémové informace širokopásmového směrovače, Internetového připojení, stav zařízení, výpis událostí v systému, výpis o bezpečnostních událostech a informaci o DHCP klientech.

System tools (systémové nástroje) (Kapitola 4)

Tato část obsahuje nástroje širokopásmového směrovače – obsahují: konfigurační nastavení, Upgrade Firmware a Resetování. Nástroje konfigurace umožňují uložení nastavení (Backup), Obnovení konfigurace z uloženého souboru, nebo Nastavení tovární (defaultní) konfigurace směrovače. Upgrade Firmware umožňuje aktualizace funkcí Vašeho směrovače. RESET umožňuje resetovat Váš směrovač v případě problémů.

7) Klikněte na **Quick Setup Wizard** (viz kapitola 1) pro spuštění nastavení konfigurace požadovaného Vaším ISP tak, abyste mohli přistupovat na Internet. Pokud nepoužíváte bezdrátového ISP pak další sekce (General Setup, Status Info a Tools) nemusíte konfigurovat a lze využít továrního nastavení.

Zvolte vždy jednu ze sekcí pokud si ji přejete konfigurovat a pokračujte v příslušné kapitole. Použijte volby z lišty nahoře vpravo webové správy (viz obr. níže) pro výběr patřičné sekce.



Kapitola 1

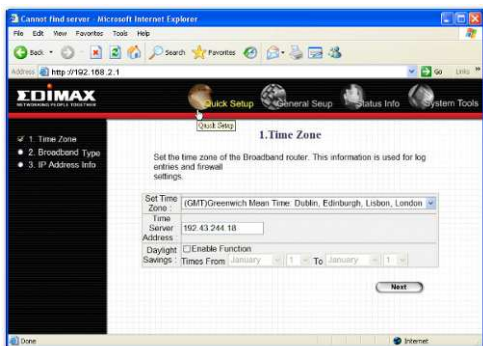
Quick Setup (průvodce rychlým nastavením)

Sekce Rychlého nastavení je vytvořena pro co nejrychlejší možnost začít používat širokopásmový směrovač. Doporučujeme zde začít pokud máte připojení k Internetu přes drát (Ethernet, např. koaxiální kabel či ADSL/telefonní linku). Stačí vyplnit pouze nezbytné informace. Pokud máte bezdrátové (WiFi) připojení je třeba změnit typ WAN viz kapitola 2.2.1 (WAN - Bezdrátový poskytovatel).

Kliknutím na **Quick Setup** na domovské stránce by se měla zobrazit obrazovka níže.

Krok 1) Time zone (časová zóna)

Časová zóna umožňuje Vašemu směrovači nastavit a synchronizovat svůj čas ve zde konfigurovaných nastaveních. Upozorňujeme, že to má vliv na i na funkce jako je ukládání/výpis událostí (Log) a nastavení Firewallu.



Parametry	Popis
Set Time Zone (Nastavení časové zóny)	Zvolte časovou zónu státu, ve kterém právě jste Směrovač nastaví svůj čas na základě Vaší volby.
Time Server Address (Adresa časového serveru)	Pokud časový server nefunguje, můžete zadat adresu časového serveru manuálně.
Enable Daylight Savings (využít lokální změny času)	Směrovač může brát v potaz také zimní/letní čas. Pokud chcete použít tuto funkci, musíte zaškrtnout oprávnění pro zpřístupnění konfigurace denního ukládání (níže).
Start Daylight Savings Time (Spuštění)	Zvolte dobu, kdy si přejete spustit podporu letního času.
End Daylight Savings Time (Konec)	Zvolte dobu, kdy si přejete ukončit podporu letního času.

Klikněte na **NEXT (další)** pro konfiguraci další strany (krok 2) - typu přípojky.

Krok 2) Typ připojení k Internetu

V této sekci volíte jeden ze čtyř typů připojení, které bude používat pro připojení prostřednictvím WAN portu (viz obr. níže). Pokud máte bezdrátové (WiFi) připojení viz kapitola 2.2.1 (WAN - Bezdrátový / WiFi poskytovatel).

Upozornění: Odlišní ISP vyžadují různé metody připojení k Internetu, ověřte si prosím u svého ISP, jaký typ připojení vyžaduje.



Menu	Popis
1.1 Cable modem (kabelový modem)	Váš ISP Vám automaticky poskytne IP adresu
1.2 Fixed-IP xDSL (Pevná IP xDSL)	Váš ISP Vám vždy poskytne IP adresu
1.3 PPPoE	Váš ISP vyžaduje použití protokolu Point-to-Point Protocol přes Ethernet standard (PPPoE)
1.4 PPTP	Váš ISP vyžaduje použití kanálu/tunelu pro připojení (protokol PPTP)
1.5 L2TP	Vaše ISP vyžaduje použití kanálu/tunelu pro připojení na druhé vrstvě (protokol L2TP).
1.6 Telstra Big Pond	Tento protokol se používá pouze pro ISP připojení v Austrálii.

Klikněte na jeden z typů WAN a pak pokračujte v příslušných odstavcích návodu (**1.1, 1.2, 1.3, 1.4, 1.5** nebo **1.6**). Pro návrat na předchozí obrazovku klikněte na **Back**.

1.1 Cable modem - Kabelový modem

Pokud Vám ISP přidělí IP adresu automaticky, zvolte kabelový modem. Někteří ISP mohou také vyžadovat upřesňující informace jako je jméno a MAC adresa (viz obrazovka níže).

Upozornění: Sekce jméno a MAC adresa je *volitelná* a můžete ji přeskočit, pokud Váš ISP nevyžaduje toto nastavení pro připojení přes Internet.



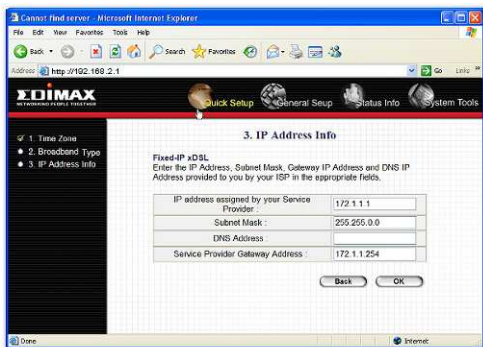
Parametry	Popis
Host Name (jméno hostitele)	Pokud Váš ISP vyžaduje jméno hostitele, zadejte jméno poskytnuté Vaším ISP, pokud ho nevyžaduje nechejte pole prázdné.
MAC Address (adresa MAC)	Váš ISP může vyžadovat konkrétní MAC adresu pro připojení na Internet. Jedná se o MAC adresu počítače, ke kterému bylo původně aktivováno (přiděleno) Vaše Internetové připojení. Vepište MAC adresu do pole nebo použijte tlačítko "Clone MAC Address" - klonování MAC adresy pro nahrazení WAN MAC adresy MAC adresou počítače ke kterému bylo aktivováno připojení (pro klonování MAC adresy byste měli použít tento počítač). Popis vyhledání MAC adresy počítače viz Příloha A. Viz slovníček pro vysvětlení termínu „MAC adresy“ na konci manuálu.

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na **<OK>**.

Gratulujeme! Dokončili jste konfiguraci připojení kabelového modemu. Nyní můžete začít používat směrovač, pokud si ale přejete využívat některé z vlastností podporovaných tímto směrovačem projděte i kapitoly 2,3,4.

1.2. Fixed-IP xDSL -Fixní xDSL

Pokud Vám ISP přidělil specifickou IP adresu pro Vaše použití zvolte fixní IP xDSL. Váš ISP by měl dodat všechny informace požadované v této sekci.



Parametry

Popis

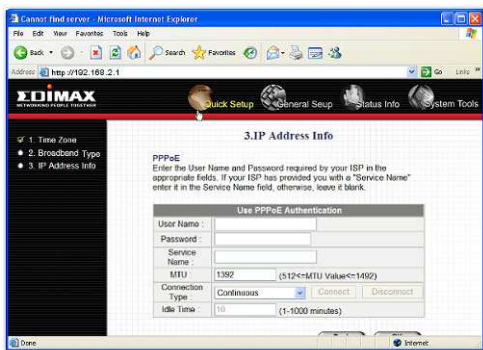
IP	Toto je IP adresa, kterou Vám ISP přidělil.
Gateway IP (portál IP)	Toto je IP adresa portálu/brány ISP
DNS	Toto je IP adresa DNS serveru ISP
Subnet Mask	Zadejte masku podsítě poskytnutou Vaší ISP (např. 255.255.255.0)

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na **<OK>**.

Gratulujeme! Dokončili jste konfiguraci připojení fixní IP xDSL. Nyní můžete začít používat směrovač, pokud si ale přejete využívat některé z vlastností, podporovaných tímto směrovačem projděte si kapitoly 2,3,4.

1.3 PPPoE

Pokud Váš ISP požaduje pro připojení k Internetu protokol PPPoE, zvolte PPPoE. Váš ISP by měl dodat informace požadované v této sekci.



Parametry	Popis
User Name (jméno uživatele)	Zadejte jméno uživatele stanovené Vaším ISP pro připojení PPPoE
Password (heslo)	Zadejte heslo stanovené Vaším ISP pro připojení PPPoE
Service Name (servisní jméno)	Je volitelné. Zadejte servisní jméno pokud ISP vyžaduje, jinak jej nechte prázdné.
MTU	Je volitelné. Můžete specifikovat maximální velikost přenosového paketu na Internet. Pokud si nepřejete nastavit maximální velikost paketu, nechejte volné.

Connection Type Pokud zvolíte „**Continuous**“ (Nepřetržitě) směrovač se vždy připojí k ISP.
(*typ připojení*) Pokud se WAN linka přeruší a pak se spojení znovu obnoví, směrovač připojení k ISP obnoví automaticky. Pokud zvolíte „**On Demand**“ (Připojit na vyžádání), směrovač se připojí k ISP pouze pokud někdo bude chtít použít Internet a připojení bude trvat při aktivitě uživatele. Směrovač odpojí připojení WAN/ k internetu, pokud doba, kdy Internet nikdo nevyužil překročí „dobu nečinnosti“ (Idle Time). Pokud zvolíte „**Manual**“, směrovač se k ISP připojí pouze pokud kliknete na „připojit“ (Connect) myši z webového rozhraní směrovače. Připojení WAN se neodpojí samo díky nečinnosti. Pokud se WAN spojení přeruší a později znovu obnoví, směrovač se k ISP již automaticky nepřipojí a bude třeba zásahu uživatele.

Idle Time Můžete specifikovat práh doby nečinnosti (v minutách)
(*doba nečinnosti*) WAN portu. Tj. dobu za kterou směrovač nepoužíváním Internetu (nebyl odeslán žádný paket z počítače) automaticky odpojí připojení s Vaším ISP (WAN připojení k Internetu).

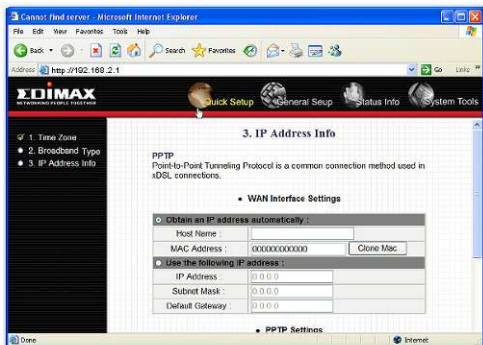
Upozornění: Tato funkce WAN automatického odpojení po určité „době nečinnosti“ nemusí pracovat korektně kvůli specifickým aktivitám některých síťových softwarových aplikací, počítačovým virům nebo útokům hackerů z Internetu. Například určitý software posílá do Internetu pakety na pozadí, přestože Internet nepoužíváte. Vypněte proto prosím svůj počítač, pokud jej nepoužíváte. Tuto funkci rovněž nemusí podporovat někteří poskytovatelé Internetového spojení (ISP). Proto se prosím ujistěte, že tato funkce pracuje správně, pokud tuto funkci používáte poprvé a zejména pokud poskytovatel Internetu (ISP) účtuje podle doby strávené použitím Internetu.

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na <OK>.

Gratulujeme! Dokončili jste konfiguraci připojení PPPoE. Nyní můžete začít používat směrovač, pokud si ale přejete využívat některé z vlastností podporovaných tímto směrovačem projděte si kapitoly 2,3,4.

1.4. PPTP

Pokud Váš ISP požaduje PPTP protokol pro připojení k Internetu, zvolte PPTP. Váš ISP by měl dodat všechny informace požadované v této sekci.



Parametry	Popis
Obtain an IP address (získání IP adresy)	Před připojením k PPTP serveru bude ISP požadovat automatické získání IP z DHCP serveru.
Use the following address (použijte následující IP adresu)	ISP Vám udělí statické IP pro připojení k PPTP IP serveru
IP Address (IP adresa)	Toto je IP adresa, kterou Vám Váš ISP poskytl pro zřízení PPTP připojení
Subnet Mask (maska podsítě)	Zadejte masku podsítě poskytnutou Vaším ISP (např. 255.255.255.0)
Gateway (Portál/brána)	Zadejte IP adresu ISP portálu/brány
User ID (uživatelské ID)	Zadejte jméno uživatele přidělené od ISP. Někdy je nazýváno „ID připojení“.

Password (heslo)	Zadejte heslo od Vašeho ISP pro připojení PPTP
PPTP Gateway (PPTP portál)	Pokud má Vaše místní síť PPTP portál/bránu, pak ji zde zadejte. Pokud PPTP portál nemáte, pak zadejte IP adresu ISP portálu
Connection ID (připojení ID)	Toto je ID přidělené ISP. Je volitelné.
BEZEQ-ISRAEL	Tuto položku zvolte, pokud používáte podporu BEZEQ v Izraeli.
Connection Type (typ připojení)	Pokud zvolíte „ Continuous “ (Nepřetržitě) směrovač se vždy připojí k ISP. Pokud se WAN linka přeruší a pak se spojení znovu obnoví, směrovač připojení k ISP obnoví automaticky. Pokud zvolíte „ On Demand “ (Připojit na vyžádání), směrovač se připojí k ISP pouze pokud někdo bude chtít použít Internet a připojení bude trvat při aktivitě uživatele. Směrovač odpojí připojení WAN/ k internetu, pokud doba, kdy Internet nikdo nevyužil překročí „dobu nečinnosti“ (Idle Time). Pokud zvolíte „ Manual “, směrovač se k ISP připojí pouze pokud kliknete na „připojit“ (Connect) myši z webového rozhraní směrovače. Připojení WAN se neodpojí samo díky nečinnosti. Pokud se WAN spojení přeruší a později znovu obnoví, směrovač se k ISP již automaticky nepřipojí a bude třeba zásahu uživatele.
Idle Time (doba nečinnosti)	Můžete specifikovat práh doby nečinnosti (v minutách) WAN portu. Tj. dobu za kterou směrovač nepoužíváním Internetu (nebyl odeslán žádný paket z počítače) automaticky odpojí připojení s Vaším ISP (WAN připojení k Internetu).

Upozornění: Tato funkce WAN automatického odpojení po určité „době nečinnosti“ nemusí pracovat korektně kvůli specifickým aktivitám některých síťových softwarových aplikací, počítačovým virům nebo útokům hackerů z Internetu. Například určitý software posílá do Internetu pakety na pozadí, přestože Internet nepoužíváte. Vypněte proto prosím svůj počítač, pokud jej nepoužíváte. Tuto funkci rovněž nemusí podporovat někteří poskytovatelé Internetového spojení (ISP). Proto se prosím ujistěte, že tato funkce pracuje správně, pokud tuto funkci používáte poprvé a

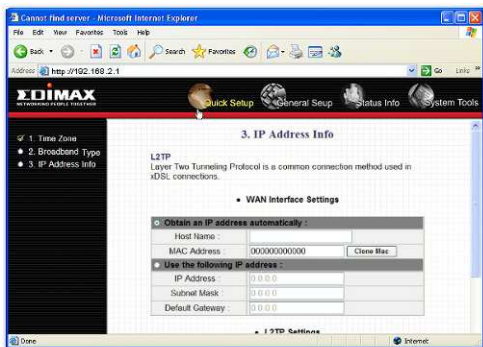
zejména pokud poskytovatel Internetu (ISP) účtuje podle doby strávené použitím Internetu.

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na <OK>.

Gratulujeme! Dokončili jste konfiguraci připojení PPTP. Nyní můžete začít používat směrovač, pokud si přejete využívat i některé z pokročilých vlastností podporovaných tímto směrovačem projděte si kapitoly 2,3,4.

1.5 L2TP

Pokud Váš ISP požaduje pro připojení k Internetu L2TP, zvolte L2TP. ISP by Vám měl dodat veškeré požadované informace.



Parametry

Popis

Obtain an IP address (získání IP adresy) Před připojením k L2TP serveru bude ISP požadovat automatické získání IP z DHCP serveru.

MAC Address (adresa MAC) Váš ISP může vyžadovat konkrétní MAC adresu pro připojení na Internet. Půjde o MAC adresu počítače, ke kterému bylo původně aktivováno (přiděleno) Vaše Internetové připojení. Vepište MAC adresu do pole nebo použijte tlačítko "**Clone MAC Address**" - **klonování MAC adresy** pro nahrazení WAN MAC adresy MAC adresou počítače, který je připojen ke směrovači/routeru (doporučujeme použít počítač k němuž bylo aktivováno připojení). Popis vyhledání MAC adresy počítače viz Příloha A na konci

manuálu.. Viz slovníček pro vysvětlení termínu „MAC adresy“ na konci manuálu.

Use the following IP (použijte následující IP adresu)	zadejte, když máte od ISP přidělenou statickou IP, která má být použita pro připojení k L2TP serveru.
IP Address (IP adresa)	Tato IP adresa je ta, kterou Vám ISP přidělilo pro vytvoření připojení L2TP.
Subnet Mask (maska podsítě)	Zadejte masku podsítě poskytnutou Vaší ISP (např. 255.255.255.0)
Gateway (portál/brána)	Zadejte IP adresu portálu/brány ISP
User ID (ID uživatele)	Zadejte jméno uživatele poskytnuté Vaším ISP
Password (heslo)	Zadejte heslo poskytnuté Vaším ISP
L2TP Gateway (Brána L2TP)	Pokud má Váš LAN L2TP portál/bránu, zadejte zde IP adresu tohoto L2TP bránu. Pokud nemáte brána L2TP, pak zadejte výše uvedenou IP adresu brányISP
MTU	Je volitelná. Můžete specifikovat maximální velikost přenosového paketu Internetu. Pokud nechcete nastavit maximální velikost, nechejte tak.
Connection Type (typ připojení)	Pokud zvolíte „Continuous“ (Nepřetržitě) směrovač se vždy připojí k ISP. Pokud se WAN linka přeruší a pak se spojení znovu obnoví, směrovač připojení k ISP obnoví automaticky. Pokud zvolíte „On Demand“ (Připojit na vyžádání), směrovač se připojí k ISP pouze pokud někdo bude chtít použít Internet a připojení bude trvat při aktivitě uživatele. Směrovač odpojí připojení WAN/ k internetu, pokud doba, kdy Internet nikdo nevyužil překročí „dobu nečinnosti“ (Idle Time). Pokud zvolíte „Manual“, směrovač se k ISP připojí pouze pokud kliknete na „připojit“ (Connect) myši z webového rozhraní směrovače. Připojení WAN se neodpojí samo díky nečinnosti. Pokud se WAN spojení

přeruší a později znovu obnoví, směrovač se k ISP již automaticky nepřipojí a bude třeba zásahu uživatele.

Idle Time (doba nečinnosti)	Můžete specifikovat práh doby nečinnosti (v minutách) WAN portu. Tj. dobu za kterou směrovač nepoužíváním Internetu (nebyl odeslán žádný paket z počítače) automaticky odpojí připojení s Vaším ISP (WAN připojení k Internetu).
--------------------------------	--

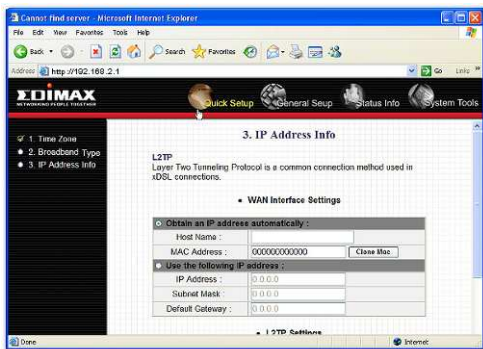
Upozornění: Tato funkce WAN automatického odpojení po určité „době nečinnosti“ nemusí pracovat korektně kvůli specifickým aktivitám některých síťových softwarových aplikací, počítačovým virům nebo útokům hackerů z Internetu. Například určitý software posílá do Internetu pakety na pozadí, přestože Internet nepoužíváte. Vypněte proto prosím svůj počítač, pokud jej nepoužíváte. Tuto funkci rovněž nemusí podporovat někteří poskytovatelé Internetového spojení (ISP). Proto se prosím ujistěte, že tato funkce pracuje správně, pokud tuto funkci používáte poprvé a zejména pokud poskytovatel Internetu (ISP) účtuje podle doby strávené použitím Internetu. Díky mnoha neovlivnitelným faktorům ze strany výrobce nemůžeme zaručit, že funkce automatického odpojení bude vždy pracovat korektně. **Doporučujeme vypínat směrovač / router vždy, když nepoužíváte připojení k Internetu.**

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na <OK>.

Gratulujeme! Dokončili jste konfiguraci připojení L2TP. Nyní můžete začít používat směrovač, pokud si přejete využívat i některé z pokročilých vlastností podporovaných tímto směrovačem projděte si kapitoly 2,3,4.

1.6. Telstra Big Pond

Protokol Telstra Big Pond zvolte, pokud Vaše ISP požaduje pro připojení k Internetu Telstra Big Pond Protokol. Vaše ISP by mělo mít všechny informace, které jsou v této sekci požadovány. Telstra Big Pond protokol je používán ISP v Austrálii.



Parametry	Popis
User Name (jméno uživatele)	Pro připojení Telstra Big Pond zadejte jméno uživatele poskytnuté Vaší ISP
Password (heslo)	Pro připojení Telstra Big Pond zadejte heslo poskytnuté Vaší ISP
User decide login server manually (rozhodnutí uživatele pro manuální přihlášení k serveru)	Zvolte zda chcete přiřadit manuálně IP přihlášením serveru Telstra Big Pond
Login Server (přihlášení serveru)	IP přihlášení serveru

Pokud jste dokončili výše uvedenou konfiguraci, klikněte na **<OK>**.
Gratulujeme! Dokončili jste konfiguraci připojení Telstra Big Pond. Nyní můžete začít používat směrovač, pokud si přejete využívat některé z vlastností podporovaných tímto směrovačem, viz kapitoly 2,3.4.

Kapitola 2

General Settings - Všeobecné nastavení

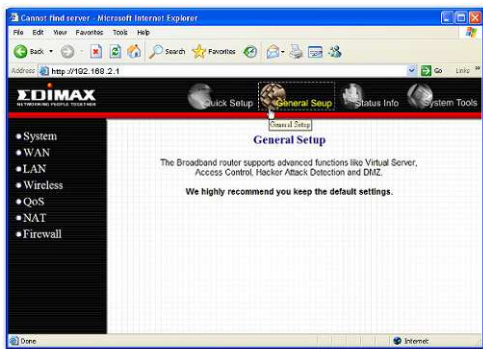
Jakmile kliknete na **General Setup** (základní nastavení) na domovské stránce, uvidíte níže uvedenou obrazovku.

Jestliže jste konfigurovali Quick Setup Wizard, NEPOTŘEBUJETE pro spuštění používání Internetu zde už nic konfigurovat (platí pro připojení „drátem“ – přes Ethernet síť).

Pouze pokud máte **bezdrátového (WiFi) poskytovatele Internetu (ISP)** je třeba změnit typ WAN připojení „WAN Type“. Nastavení najdete v sekci **2.2.1 Wireless ISP – bezdrátový (WiFi) ISP**

General Setup (*všeobecné nastavení*) obsahuje vlastnosti, které Vám umožní nakonfigurovat směrovač tak, aby splnil požadavky Vaší sítě, jako jsou: bezdrátové připojení, mapování adres, virtuální server, kontrola přístupu, ochrana proti útoku hackerů, speciální aplikace, DMZ a další.

Níže je všeobecný popis funkcí, které jsou u tohoto širokopásmového směrovače k dispozici



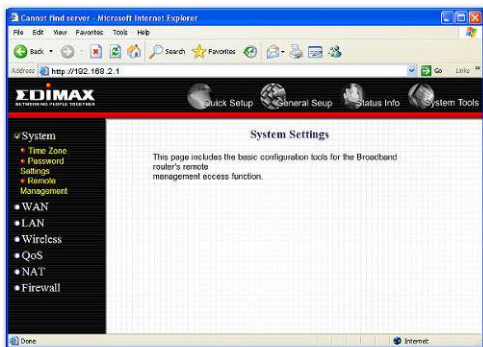
Menu	Popis
2.1 Systém	Tato sekce umožňuje nastavení časové zóny systému, heslo a správu administrátora širokopásmového směrovače.
2.2 WAN	Tato sekce Vám umožní zvolit způsob připojení k Internetu podle typu připojení poskytnutého Vaším ISP (obdoba Quick Setup – průvodcem rychlého nastavení)
2.3 LAN	Můžete specifikovat IP adresu LAN segmentu, masku podsítě, povolit/zakázat DHCP a zvolit rozsah IP Vašeho LAN

- 2.4 Wireless (bezdrát) Nastaví SSID bezdrátové/WiFi sítě, šifrovací WEP klíč, filtraci MAC adres přístupu do směrovače.
- 2.5 QoS Můžete určit pravidla užití šířky pásma (Quality of Services).
- 2.6 NAT V této sekci můžete konfigurovat mapování adres, virtuální server a funkce speciálních aplikací. To Vám umožní specifikovat, který uživatel/paket projde přes NAT směrovače.
- 2.7 Firewall Sekce Firewall Vám umožní konfigurovat kontrolu přístupu, ochranu proti hackerům a DMZ.

Zvolte jeden z pěti výše uvedených Všeobecných nastavení a pokračujte podle příslušné podsekcce manuálu

2.1 Systém

Obrazovka systému Vám umožní specifikovat časovou zónu, změnit heslo systému a určit přístupové údaje uživatele širokopásmového směrovače.



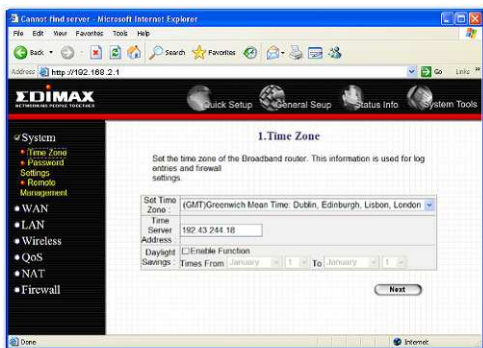
Parametry	Popis
<i>System Settings</i> (Nastavení systému)	
2.1.1 Time Zone (časová zóna)	Zvolte časovou zónu země, ve které momentálně jste. Směrovač nastaví svůj čas podle Vaší volby.

- 2.1.2 Password settings (nastavení hesla) Vám umožní zvolit heslo kvůli přístupu ke správě webové stránky směrovače / routeru
- 2.1.3 Remote Management (správa na dálku) Můžete specifikovat IP adresu hostitele, která může provést funkce správy na dálku.
-

Zvolte jeden ze tří výše uvedených nastavení systému a pokračujte podle příslušné podsektce návodu.

2.1.1 Time Zone - Časová zóna

Časová zóna umožňuje Vašemu směrovači založit svůj čas na zde provedeném nastavení. Toto ovlivní další funkce, jako je zápis událostí (Log) a nastavení Firewallu.



Parametry	Popis
-----------	-------

Set Time Zone (Nastavení časové zóny)	Zvolte časovou zónu své země, ve které právě jste. Směrovač nastaví svůj čas na základě Vaší volby.
--	---

Time Server Address (Adresa časového serveru)	Přednastavení serveru „Time Server Address“ je „192.43.244.18“
--	--

Enable Daylight Savings (využit lokální změny času)	Směrovač může brát v potaz také zimní/letní čas. Pokud chcete použít tuto funkci, musíte zaškrtnout oprávnění pro zpřístupnění konfigurace denního ukládání (níže).
--	---

Start Daylight Savings Time Zvolte dobu, kdy si přejete spustit podporu letního času.
(*Spuštění*)

End Daylight Savings Time Zvolte dobu, kdy si přejete ukončit podporu letního času.
(*Konec*)

Pro uložení výše uvedené konfigurace klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo spustit používání směrovače (s vhodným přednastavením).

2.1.2 Password Settings – Nastavení hesla

Můžete změnit heslo požadované pro přihlášení do správy systému směrovače. Implicitně je zde heslo „1234“ (toto heslo se obnoví po resetu do továrního nastavení). Prosím co nejdříve změňte heslo administrátora a uložte si je (pro případ zapomenutí) na bezpečném místě. Hesla mohou obsahovat 0 až 12 alfanumerických znaků a rozlišují se velká a malá písmena.



Parametry	Popis
Current Password (stávající heslo)	Zadejte své stávající heslo administrátora vzdálené správy pro přihlášení ke svému širokopásmovému směrovači. Upozornění: Implicitní heslo 1234 zná každý

New Password
(nové heslo)

Zadejte nové heslo

Confirmed Password
(potvrzení hesla)

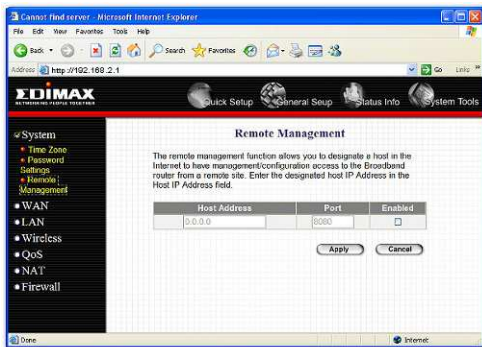
Zadejte znovu nové heslo pro jeho ověření

Upozornění: Pokud heslo zapomenete, budete muset resetovat směrovač na nastavení z výroby resetovacím tlačítkem (viz zadní panel směrovače)

Pro uložení výše uvedené konfigurace klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce **<Continue>** nebo spustit používání směrovače **<Apply>** (po restartu – nevypínat během restartu).

2.1.3 Remote Management – vzdálená správa

Funkce vzdálené správy Vám umožní určit IP adresu hostitele (z Internetu) pro konfiguraci širokopásmového směrovače na dálku. Zadejte hostitelskou IP adresu v poli „host IP address“.



Parametry

Popis

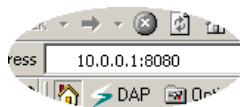
Host Address
(adresa hostitele)

Je IP adresa hostitele na Internetu, který bude mít vzdálený přístup pro správu/konfiguraci směrovače. To znamená např., že pokud jste doma a Vaše domácí IP adresa byla zadána za hostitelskou IP adresu dálkové správy pro tento směrovač (umístěný ve Vaší kanceláři), pak jste schopni konfigurovat tento směrovač z Vašeho domova. Pokud je adresa hostitele **0.0.0.0**, znamená to, že kdokoli může

mít vzdálený přístup ke konfiguraci směrovače, pokud zná heslo.

Zaškrtněte políčko **Enabled – oprávnění** pro umožnění funkce dálkové správy.

Upozornění: Pokud chcete vzdálený přístup ke správě z webu, musíte zadat WAN IP adresu směrovače (např. 10.0.0.1) ve svém webovém vyhledávači dále číslo portu 8080, např. 10.0.0.1:8080 (viz níže). Budete také potřebovat znát heslo nastavené na obrazovce Password Setting (nastavení hesla) kvůli přístupu ke správě směrovače z webu



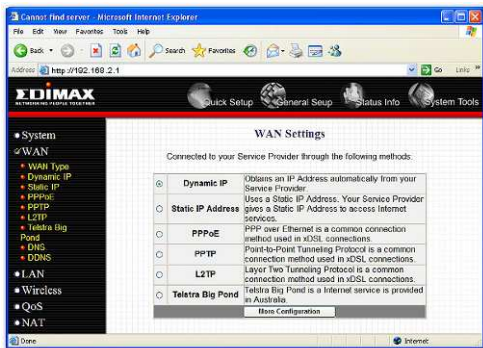
Port Číslo portu dálkové správy webového rozhraní.

Enabled Zvolte „Enabled“ pro oprávnění funkce dálkové správy.
(*oprávnění*)

Pro uložení výše uvedené konfigurace klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce (**<Continue>**) nebo spustit používání směrovače (po restartu).

2.2 WAN

Toto nastavení „WAN“ použijte pokud chcete **změnit** typ připojení k Internetu u drátového (Ethernet) ISP nebo máte **bezdrátového (WiFi) ISP** (viz 2.2.1). Specifikujete typ připojení k WAN portu, podle Vašeho ISP (drátem nebo bezdrátem). Nastavení WAN nabízí dále následující volby pro WAN port směrovače: **Dynamickou IP adresu, Statickou IP adresu, PPPoE, PPTP, L2TP, Telstra Big Pond, DNS a DDNS.**



Parametry	Popis
2.2.2 Dynamic IP address (<i>dynamická IP adresa</i>)	ISP Vám IP adresu poskytne automaticky.
2.2.3 Static IP address (<i>statická IP adresa</i>)	ISP Vám IP adresu sdělí při zřízení spojení
2.2.4 PPPoE	ISP vyžaduje připojení PPPoE.
2.2.5 PPTP	ISP požaduje pro použití Point-to-Point Tunneling Protocol (PPTP)
2.2.6 L2TP	ISP požaduje připojení L2TP.
2.2.7 Telstra Big Pond	ISP požaduje připojení Telstra Big Pond
2.2.8 DNS	Můžete specifikovat server DNS, který chcete používat
2.2.9 DDNS	Můžete specifikovat server DDNS, který chcete používat a konfigurovat jméno uživatele a heslo poskytnuté providerem služeb DDNS

Jakmile jste provedli volbu, klikněte na **<More Configuration> (další konfigurace)** ve spodní části obrazovky a pokračujte v příslušné podsekcí návodu.

2.2.1 Wireless ISP – bezdrátový (WiFi) ISP

Pro připojení k bezdrátovému přístupu k Internetu zvolte „WAN Type“, vyberte „Wireless ISP“ (implicitně je nastaveno Ethernet – drátový přístup), a tlačítkem <Apply> potvrďte a poté doplňte nastavení ISP pod novou položkou v hlavním menu „Wireless WAN Setting“ - název sítě (ESSID) a kanál (Channel). Tlačítko <Select Site Survey> zobrazí dostupné bezdrátové sítě pro lepší výběr ISP (tlačítko <Refresh> = obnovení zjišťování okolních sítí).

Pokračujte v dalším nastavení podle příslušné podsekcce návodu.

2.2.2 Dynamic IP – dynamická IP

Pokud Vám Váš ISP bude automaticky přidělovat IP adresu, zvolte Dynamic IP. Někteří ISP mohou požadovat, aby jste doplnili další doplňující informace jako jsou jméno, jméno domény a MAC adresu (další podrobnosti viz kapitola 1 „Kabelový modem“)

2.2.3 Static IP Address – statická IP adresa

Pokud Vám ISP přidělil specifickou IP adresu, zvolte Static IP. Váš ISP by měl dodat všechny informace požadované v této sekci. (další podrobnosti viz kapitola 1 „Fixní IP“).

2.2.4 PPPoE (PPP over Ethernet) – PPP přes ethernet

Pokud Váš ISP vyžaduje pro připojení k Internetu PPPoE protokol, zvolte PPPoE. Váš ISP by měl dodat všechny informace požadované v této sekci. (další podrobnosti viz kapitola 1 „PPPoE“)

2.2.5 PPTP

Pokud Váš ISP vyžaduje pro připojení k Internetu PPTP protokol, zvolte PPTP. Váš ISP by měl dodat všechny informace požadované v této sekci. (další podrobnosti viz Kapitola 1 „PPTP“)

2.2.6 L2TP

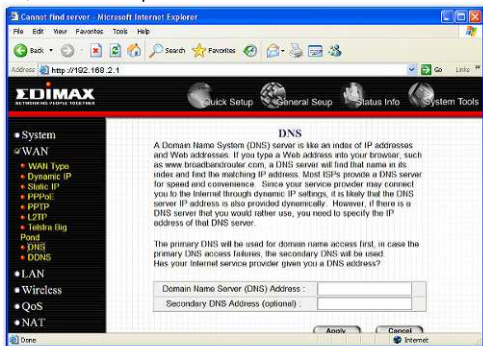
Pokud Váš ISP vyžaduje pro připojení k Internetu L2TP protokol, zvolte L2TP. ISP by měl dodat všechny informace požadované v této sekci (další podrobnosti viz kapitola 1 „L2TP“)

2.2.7 Telstra Big Pond

Pokud Váš ISP vyžaduje pro připojení k Internetu Telstra Big Pond protokol, zvolte Testra Big Pond. Vaše ISP by měla mít všechny informace požadované v této sekci. Protokol Telstra Big Pond je používán ISP v Austrálii. (další podrobnosti viz kapitola 1 „Telstra Big Pond“)

2.2.8 DNS

DNS Server (Domain Name System – systém přidělování jmen domén) je jako index IP adresy a Web adresy. Pokud zadáte ve Vašem vyhledávači Web adresu, jako je www.router.com, DNS server najde ve svém indexu toto jméno a doplní odpovídající IP adresu. Většina ISP poskytuje DNS server pro rychlost a pohodlí. Pokud Vás poskytovatel Internetu připojí k Internetu pomocí dynamického nastavení IP adresy, je to jako když je IP adresa DNS serveru poskytnuta automaticky. Nicméně, pokud máte upřednostňovaný DNS server, musíte zde specifikovat IP adresu tohoto DNS serveru.

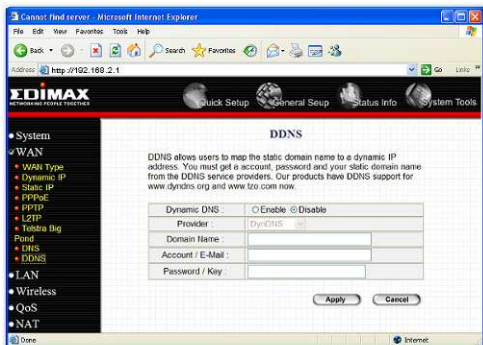


Parametry	Popis
Domain Name Server (DNS) <i>Server doménových jmen</i>	Toto je IP adresa DNS serveru, kterou jste dostali; nebo můžete specifikovat Vámi preferovanou IP adresu DNS Serveru
Secondary DNS Address (optional) <i>Druhá adresa DNS (volitelná)</i>	Je volitelná. Můžete zadat jinou IP adresu jako zálohu. Tato druhá DNS bude použita, pokud výše uvedená DNS selže.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač.

2.2:9 DDNS

DDNS Vám umožní zobrazit určité pevné jméno domény k dynamické IP adrese. Od poskytovatele DDNS musíte získat účet, heslo a statické/pevné jméno Vaší domény. Tento směrovač podporuje DynDNS, TZO a další obecné servisní služby poskytovatelů DDNS.

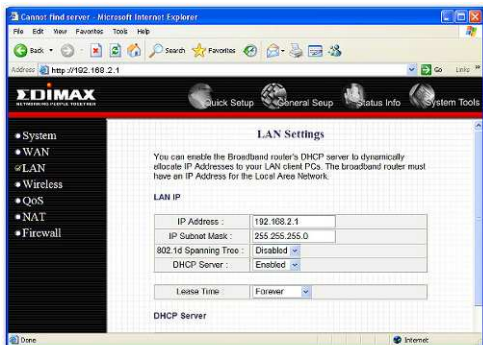


Parametry	Výchozí/Implicitní hodnota	Popis
Enable/Disable (oprávnění/zamítnutí)	Vypnutá	Opravně/vypíná funkci DDNS tohoto směrovače
Provider (poskytovatel)		Zvolte poskytovatele DDNS služeb
Domain name (název domény)		Jméno Vaší statické domény používané DDNS
Account/E-mail (Účet/e-mail)		Účet, který Vám servisní poskytovatel DDNS přidělí
Password/key (Heslo/klíč)		Heslo, nastavené pro servisní účet DDNS

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.3 LAN

Nastavení LAN portů, obr. níže, Vám umožní specifikovat soukromou/vnitřní IP adresu LAN portů Vašeho směrovače a masku podsítě Vašeho LAN segmentu.



Parametry	Implicitní hodnota	Popis
LAN IP		
IP address (IP adresa)	192.168.2.1	Toto je IP adresa LAN portu směrovače (Implicitní IP adresa brány klientů místní sítě - LAN)
IP Subnet Mask (Maska podsítě IP)	255.255.255.0	Specifikace masky podsítě Vašeho LAN segmentu
802.1d Spanning Tree (Větvění)	Neaktivní	Pokud je funkce 802.1d „Spanning Tree“ aktivována, směrovač použije tento protokol k ochraně před tvorbou smyček v síti, ke kterým u LAN může dojít a mohou znefunkčnit síť.
DHCP server	Aktivní	Můžete aktivovat nebo deaktivovat DHCP server. Při aktivaci DHCP serveru směrovač automaticky poskytne Vašemu klientskému LAN IP adresu. Pokud DHCP není aktivován, musíte ručně nastavit IP adresu Vašeho klientského LAN. Ujistěte se, že klientský

LAN je ve stejné síti a podsíti jako tento širokopásmový směrovač, pokud chcete, aby směrovač byl implicitní branou Vašeho klientského LAN.

Lease Time
(doba pronájmu)

Pokud je DHCP aktivní, poskytnete Vašemu klientskému LAN dočasnou IP adresu. V nastavení Lease Time můžete specifikovat dobu na kdy DHCP zapůjčí Vaší klientské LAN IP adresu. DHCP změní IP adresu Vaší klientské LAN, pokud vyprší časový práh doby na kdy byla IP adresa přidělena.

IP address Pool
(sdílení IP adresy)

Můžete zvolit konkrétní rozsah IP adres Vašeho DHCP serveru pro přidělení IP adres Vaším klientským LAN.

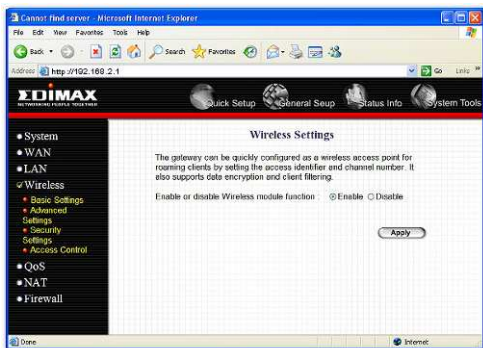
Upozornění: V továrním nastavení implicitně je rozsah IP od **192.168.2.100** do IP **192.168.2.199**. Pokud chcete aby Váš počítač měl statickou/fixní IP adresu, pak musíte zvolit IP adresu mimo rozsah této IP adresy.

Domain Name Můžete specifikovat jméno domény Vašeho LAN
(jméno domény)

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4. Wireless – bezdrát / Wi-Fi

Bezdrátové připojení vytvoří bezdrátovou síť a můžete tak všechny počítače s bezdrátovou síťovým adaptérem IEEE 802.11b nebo 802.11g připojit do Vaší vnitřní sítě. Podporuje šifrování WEP a WPA2 pro zvýšení bezpečnosti přenosu informací Vaší bezdrátové sítě.



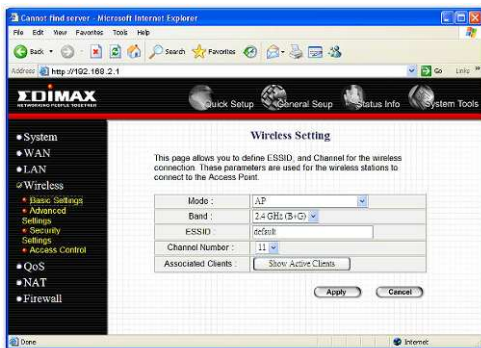
Parametry	Implicitní hodnota	Popis
Enable or disable Wireless module function (aktivace/zamítnutí bezdrátového modulu)	Zapnutý	Můžete zvolit zpřístupnění nebo vypnutí bezdrátového připojení modulu (Access Pointu) směrovače.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.1 Basic Setting – základní nastavení

Můžete nastavit parametry, které používáte pro připojení bezdrátových stanic k tomuto směrovači. Parametry zahrnují Mode (režim), ESSID, Channel Number (číslo kanálu) a Associated Client (propojeného klienta).

Setting Page - Nastavení



Parametry	Implicitní hodnota	Popis
Mode (režim)		Umožňuje nastavit spojení AP - AP, klienta (Station), přemostění, nebo WDS režim
Band (vazba)		Umožňuje nastavit fungování AP ve Wi-Fi standardu 802.11b nebo 802.11g. Můžete vybrat B+G, umožňující volbu automatické práce AP v 802.11b nebo 802.11g
ESSID	„default“	Toto je jméno bezdrátové sítě. Všechna zařízení v jedné WiFi síti LAN by měla používat stejné jméno.
Channel Number (číslo kanálu)	11	Kanál používaný bezdrátovou sítí. Všechna zařízení v jedné bezdrátové síti by měla používat stejný kanál.
Associated Clients (propojení klienti)		Klikněte na tlačítko „Show Active Clients“ (zobrazit aktivní klienty), pak se objeví „Active Wireless Client Table“ (přehled aktivních bezdrátových klientů). Můžete vidět stav všech aktivních bezdrátových stanic, které jsou připojeny k přístupovému bodu (AP).
WLAN MAC		Je MAC adresa používaná bezdrátovým rozhraním toho AP, pokud je v programu client (Station mód).

Clone MAC (klonování MAC)	Kliknutím na tlačítko „Clone MAC“ zkopírujete MAC adresu počítače, který používáte pro konfiguraci AP, místo WLAN MAC adresy.
MAC address (MAC adresa)	Pokud chcete přemostit více než jednu síť bezdrátovou sítí, musíte nastavit tento přístupový bod (AP) do „AP Bridge - Point to Point mode“, „AP Bridge - Point to MultiPoint mode“nebo „AP Bridge - WDS mode“ Musíte zadat MAC adresy ostatních AP Které jsou zapojovány, aby bylo definováno potřebné spojení mezi nimi.
Set Security (Nastavení bezpečnosti)	Klikněte na tlačítko „Set Security“, pak se objeví okno „WDS Security Settings“ (bezpečnostní nastavení WDS). Můžete nastavit bezpečnostní parametry použité pro propojení Access Pointů pokud je Váš AP nastaven v režimech „AP Bridge“. Nastavení parametrů Viz sekce 4.3 „Security Settings“ (bezpečnostní nastavení).

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.2 Advanced Settings – Pokročilá nastavení

Můžete nastavit pokročilé parametry. Parametry obsahují Authentication Type (Typ ověření), Fragment Threshold (práh fragmentace), RTS Threshold (práh RTS), Beacon Interval (interval signálu), Preamble Type (typ úvodní preamble).... **Tyto parametry byste neměli měnit, pokud nevíte bezpečně jaké následky způsobí tyto změny v nastavení směrovače.**



Parametry	Popis
------------------	--------------

Authentication Type <i>(Typ ověření přístupu)</i>	Existují dva typy ověření: „Open System“ (Otevřený systém) a „Shared Key“ (sdílený klíč). Pokud zvolíte „Open System“, může se jakákoli bezdrátová stanice spojit s tímto bezdrátovým směrovačem bez šifrování WEP. Pokud zvolíte „Shared Key“, musíte rovněž nastavit také WEP klíč na straně „Encryption“ (šifrování) a připojovaná bezdrátová stanice musí použít toto WEP šifrování při ověřování spojení s tímto bezdrátovým směrovačem. Pokud zvolíte „Auto“, bezdrátová stanice se může spojit s tímto směrovačem použitím jednoho z těchto dvou typů ověření.
---	---

Fragment Threshold <i>(práh fragmentu)</i>	„Fragment Threshold“ specifikuje maximální velikost packetu během fragmentace přenášených dat. Pokud nastavíte tuto hodnotu příliš nízkou, výsledkem může být špatný výkon.
--	---

RTS Threshold <i>(práh RTS)</i>	Pokud bude velikost packetu menší než nastavený práh RTS, bezdrátový směrovač nepoužije mechanismu RTS/CTS pro odeslání tohoto packetu.
---	---

Beacon Interval <i>(interval signálu)</i>	Časový interval, po který tento bezdrátový směrovač vysílá signál. Signál se používá pro synchronizaci bezdrátové sítě.
---	---

Data Rate (přenos dat)	„Data Rate“ je rychlost, kterou přístupový bod používá pro přenos datových paketů. Přístupový bod použije pro přenos dat nejvyšší možnou přenosovou rychlost.
Preamble Type (typ úvodu)	Dlouhá/Long Preamble může zajistit lepší kompatibilitu bezdrátového spojení; zatímco krátká /Short Preamble“ může zajistit lepší výkonnost Bezdrátové sítě.
Broadcast ESSID (vysílat ESSID)	Pokud povolíte „Broadcast ESSID“, každá bezdrátová stanice umístěná v dosahu pokrytí tímto přístupovým bodem může snadno detekovat přístupový bod. Pokud máte veřejnou bezdrátovou síť, doporučujeme tuto vlastnost aktivovat. Zamítnutí „Broadcast ESSID“ může zajistit lepší ochranu.
IAPP	Pokud zapnete „IAPP“ dovolíte přecházení/roaming bezdrátových stanic mezi oprávněnými přístupovými body IAPP v rámci stejné bezdrátové LAN.
802.11g Protection (802.11g ochrana)	Nazývá se také CTS ochrana. Doporučujeme aktivovat mechanismus ochrany. Tento mechanismus může snížit míru kolizí dat mezi bezdrátovými stanicemi 802.11b a 802.11g. Pokud je program ochrany aktivován, průchodnost AP bude nižší kvůli většímu zatížení přenosem rámců.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.3 Security – zabezpečení

Tento přístupový bod nabízí kompletní zabezpečení bezdrátového provozu, obsahuje WEP, IEEE 802.11x, IEEE 702.11x s WEP, WPA se sdíleným klíčem a WPA s RADIUSem. Prosím ujistěte se, že bezdrátové stanice (klientské zařízení) připojované ke směrovači podporují stejné bezpečnostní protokoly.

2.4.3.1 Pouze WEP

Pokud zvolíte 64-bit nebo 128-bit WEP klíč, musíte zadat WEP klíč pro šifrování dat. Klíč můžete generovat sami a zadat jej klávesnicí. Můžete zadat 4 WEP klíče a zvolit jeden z nich jako implicitní klíč. Pak může směrovač dostat jakýkoliv paket šifrovaný jedním z těchto čtyř klíčů.



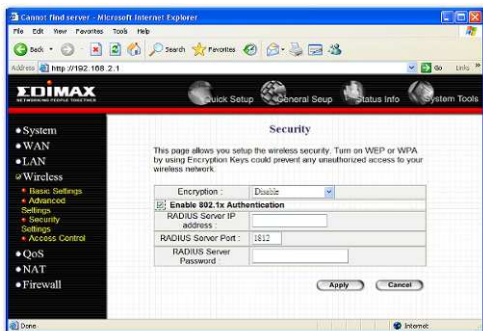
Parametry	Implicitně	Popis
Key Length (délka klíče)	64-bit	Pro šifrování můžete zvolit délku WEP klíče 64-bit nebo 128-bit. Větší délka WEP klíče zajistí vyšší úroveň ochrany, ale průchodnost bude nižší.
Key Format (formát klíče)		Pro WEP klíč můžete zvolit ASCII znaky (alfanumerický formát) nebo hexadecimální číslice (v rozsahu "A-F", "a-f" a "0-9"). Například: ASCII znaky: guest Hexadecimální číslice: 12345abcde
Default Key (implicitní klíč)		Zvolte jeden ze čtyř klíčů pro šifrování svých dat. Pouze klíč, který zvolíte jako "Default key" bude účinný.

Key 1 – Key 4 WEP klíče se používají pro šifrování dat přenášených do
(Klíč 1 – Klíč 4) bezdrátové sítě. Textové pole vyplňte podle následujících
pravidel: 64-bit WEP: jako šifrovací klíč zadejte 10místné
hodnoty (v rozsahu "A-F", "a-f" a "0-9") nebo 5místné ASCII
128-bit WEP: jako šifrovací klíč zadejte hodnotu 26 místné
(v rozsahu "A-F", "a-f" a "0-9") nebo 13místné ASCII.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.3.2 Použití pouze 802.1x

IEEE 802.1x je ověřovací protokol. Každý uživatel musí mít definován platný účet již před přístupem /přihlášením do bezdrátové sítě. Ověření loginu přihlašovaného je provedeno RADIUS serverem. V tomto režimu se ověřuje pouze platnost uživatele pomocí IEEE 802.1x, ale neprobíhá šifrování datového toku během bezdrátové komunikace.



Parametry	Popis
-----------	-------

RADIUS Server IP address	IP adresa externího RADIUS serveru. (IP adresa RADIUS serveru)
--------------------------	---

RADIUS Server Port
(port RADIUS serveru)

Port externího RADIUS serveru.

RADIUS Server Password Heslo používané externím RADIUS serverem.
(heslo RADIUS serveru)

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.3.3 802.1x WEP Static key – statický klíč WEP

IEEE 802.1x je ověřovací protokol. Každý uživatel musí mít definován platný účet již před přístupem /přihlášením do bezdrátové sítě. Ověření je provedeno RADIUS serverem. Tento režim používá také WEP protokol pro šifrování dat během bezdrátové komunikace.

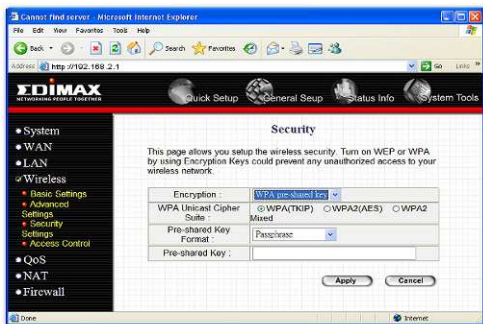


Pro nastavení WEP si prosím projděte sekci 2.4.3.1 „WEP only“. Pro nastavení 802.1x viz předchozí sekce 2.4.3.2 „802.1x“.

2.4.3.4 WPA Pre-shared key - sdílený klíč

Wi-Fi Protected Access (WPA-chráněný přístup WiFi) je pokročilé zabezpečení. Pro ověření bezdrátových klientských stanic můžete použít sdílený klíč a šifrovat data během komunikace. Používají se TKIP nebo CCMP (AES) protokoly pro častou změnu šifrovacího klíče.

Proto je šifrovací klíč jen obtížně prolomitelný hackery / neoprávněnými uživateli. Jde o vysoké zabezpečení.



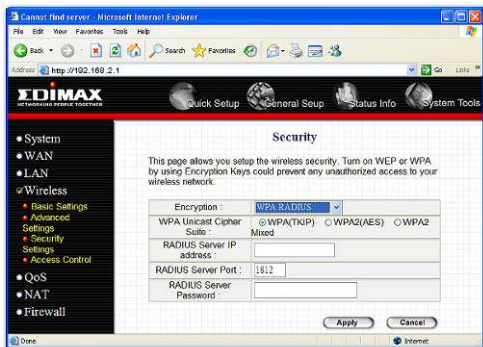
Parametry	Popis
WPA (TKIP)	TKIP může často měnit šifrovací klíč pro zvýšení ochrany bezdrátové sítě (LAN).
WPA2(AES)	Používá CCMP protokol pro častou změnu šifrovacího klíče. AES může zajistit vysokou úroveň šifrování pro zvýšení ochrany bezdrátového LAN.
WPA2 Mixed	Používá automaticky TKIP nebo AES v závislosti na stavu komunikačního spojení
Pre-shared Key Format (formát sdíleného klíče)	Jako Pre-shared Key můžete zvolit přihlašovací heslo (alfanumerický formát) nebo hexadecimální znaky v rozsahu "A-F", "a-f" a "0-9". Například: Přihlašovací heslo::iamguest Hexadecimální čísla: 12345abcde
Pre-shared Key (sdílený klíč)	Sdílený klíč se používá pro ověření a šifrování dat přenášených bezdrátovou sítí. Vyplňte textové pole podle níže uvedených pravidel. Hex WEP: zadejte 64-místnou hodnotu v Hex (v rozsahu "A-F",

„a-f“ a „0-9“) nebo nejméně 8 znaků přihlašovacího hesla pro nastavení sdíleného klíče.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.3.5 WPA Radius

Wi-Fi Protected Access (WPA-chráněný přístup WiFi) je pokročilé zabezpečení. Pro ověření přístupu bezdrátové stanice/klienta můžete používat externí RADIUS server a klíč k ustavení relace pro šifrování dat během komunikace. Používá TKIP nebo CCMP (AES) pro častou změnu šifrovacího klíče. Proto je šifrovací klíč jen obtížně prolomitelný hackery / neoprávněnými uživateli. Jde o vysoké zabezpečení.



Parametry	Popis
WPA (TKIP)	TKIP může často měnit šifrovací klíč pro zvýšení ochrany bezdrátové sítě (LAN).
WPA2(AES)	Používá CCMP protokol pro častou změnu šifrovacího klíče. AES může zajistit vysokou úroveň šifrování pro

zvýšení ochrany bezdrátového LAN.

WPA2 Mixed Používá automaticky TKIP nebo AES v závislosti na stavu komunikačního spojení.

RADIUS Server IP address IP adresa externího RADIUS serveru.
(IP adresa RADIUS serveru)

RADIUS Server Port Servisní port externího RADIUS serveru.
(Port RADIUS serveru)

RADIUS Server Password Heslo používané externím RADIUS serverem.
(heslo RADIUS serveru)

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.4.4 Access Control – kontrola přístupu

Tento bezdrátový směrovač umožňuje kontrolu MAC adres a tím brání neautorizovaným MAC adresám v přístupu do Vaší bezdrátové sítě.



Parametry

Popis

Enable wireless access control
(oprávnění kontroly bezdrátového
přístupu)

Aktivuje kontrolu bezdrátového přístupu

Add MAC address into the list
(přidání MAC adresy na seznam)

Vyplňte MAC adresu a „Comment – popis“ bezdrátové stanice, která má být přidána a pak klikněte na „Add-přidat“. Pak bude tato bezdrátová stanice přidána na „Current Access Control List - seznam povolených uživatelů“. Pokud zjistíte např. chybu před přidáním a chcete ji opravit klikněte pouze na „Clear-vymazat“ a obě pole „MAC Address“ a „Comment“ budou vymazána.

Remove MAC address from list
(vymazání MAC adresy ze
seznamu)

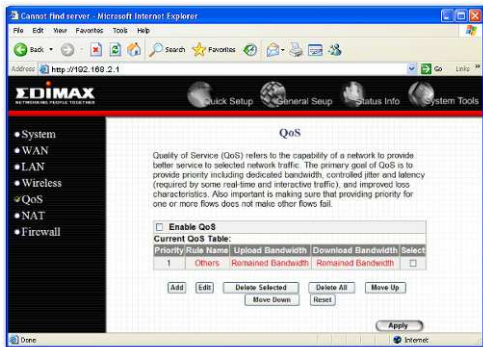
Pokud chcete z „Current Access Control List - seznamu povolených uživatelů“ odstranit některou MAC adresu, zvolte MAC adresy, které chcete odstranit a pak klikněte na „Delete Selected - vymazat výběr“. Pokud chcete odstranit z tabulky všechny MAC adresy, klikněte na „Delete All - vymazat vše“. Kliknutím na „Reset - zrušit“ vymažete stávající volbu.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.5 QoS kvalita služeb

QoS Vám umožní klasifikovat přenosy aplikací Internetu zdrojovou/cílovou IP adresou a číslem portu. Můžete označit priority pro každý typ aplikace a vyhradit pro ně šířku pásma. Pakety aplikací s vyšší prioritou se odesílají vždy jako první. Aplikace s nižší prioritou dostanou šířku pásma jakmile aplikace s vyšší prioritou dostanou dostatečnou šířku pásma. To Vám umožní získat lepší výsledky při používání služeb v reálném čase, jako jsou IP telefonování, videokonference... apod. Všechny aplikace Vámi neuvedené jsou klasifikovány jako „Others - ostatní“ Pravidlo s nižším číslem priority má vyšší priority, pravidlo s vyšším číslem priority má nižší priority. Můžete nastavovat priority pravidel jejich posouváním nahoru a dolů.

Upozornění: Pokud je celková šíře pásma aplikací vyšší priority větší než maximální šíře pásma dostupná pro WAN port, další aplikace nedostanou žádnou šíři pásma.



Parametry	Popis
-----------	-------

Enable/Disable QoS
(zapnutí/zamítnutí QoS)

Enable - aktivovat QoS, Disable - nepoužít QoS

Add a QoS rule into the table
(přidání QoS pravidla do tabulky)

Klikněte „Add - přidat“, pak zadejte formu QoS pravidla. Po vyplnění formuláře klikněte na „Apply - aplikovat“ a pravidlo bude přidáno do tabulky.

Remove QoS rules from table
(odstranění QoS pravidel z tabulky)

Pokud chcete z tabulky odstranit některá QoS pravidla, zvolte QoS pravidla, která chcete z tabulky odstranit a pak klikněte na „Delete Selected - smazat vybrané“. Pokud chcete z tabulky odstranit všechna QoS pravidla, klikněte na „Delete All - smazat vše“. Kliknutím na „Reset - zrušit“ smažete Vaše stávající volby.

Edit a QoS rule
(Upravit QoS pravidlo)

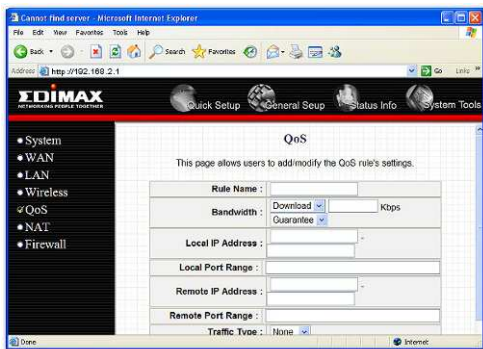
Zvolte pravidlo, které chcete upravit a klikněte na „Edit - upravit“, pak zadejte detailní formu pravidla QoS. Po upravení formy klikněte na „Apply - použít“ a pravidlo bude uloženo.

Adjust QoS Rule priority
(*nastavení priority QoS Pravidla*)

Můžete zvolit pravidlo a kliknout na „Move Up - povýšit“ pro zvýšení priority. Můžete také zvolit pravidlo a kliknout „Move Down - snížit“ pro snížení přednosti.

Edit QoS Rule – Upravení QoS pravidla:

Můžete zadat kritéria pro klasifikaci paketu, parametry v rozsahu lokálních IP, vzdálených IP, typu přenosu a protokolu. Parametry, které necháte jako prázdné, budou ignorovány. Priorita tohoto pravidla bude aplikována na pakety, které splní kritéria klasifikace daného pravidla. Můžete omezit šíři pásma použitou na pakety, které toto pravidlo splňují nebo garantovat maximální požadovanou šíři pásma pro pakety, které toto pravidlo splňují.



Parametry	Popis
-----------	-------

Rule Name
(*název pravidla*)

Název zadávaného pravidla.

Bandwidth
(*šířka pásma*)

Můžete zadat šíři pásma stahování nebo vysílání jednotkou v Kbps (1024 bitů za vteřinu). Můžete omezit maximální šíři pásma potřebnou pro toto pravidlo volbou „Maximum“. Můžete také rezervovat dostatečnou šíři pásma pro toto pravidlo zvolením „Guarantee - zaručit“

Lokální IP adresa
(*Lokální IP adresa*)

Zadejte rozsah lokálních IP adres pro pakety, na které bude toto pravidlo aplikováno. Pokud zadáte

192.168.2.3 – 192.168.2.5, znamená to 3 IP adresy:
192.168.2.3, 192.168.2.4 a 192.168.2.5

Local Port Range (rozsah lokálního portu)	Zadejte rozsah lokálních portů pro pakety, na které bude toto pravidlo aplikováno. Můžete zadat jediné číslo portu nebo zadat rozsah čísel portu zadáním prvního a posledního čísla portu. Dvě čísla jsou oddělena pomlčkou „-“, například „101-150“ znamená z čísla portu 100 k číslu portu 150 – rozsah platí pro 50 portů.
Remote IP Address (vzdálené IP adresa)	Zadejte rozsah vzdálených IP adres pro pakety, na které bude toto pravidlo aplikováno. Pokud zadáte 192.168.2.3 – 192.168.2.5, znamená to 3 IP adresy: 192.168.2.3, 192.168.2.4 a 192.168.2.5
Remote Port Range (rozsah vzdáleného portu)	Zadejte rozsah vzdálených portů pro pakety, na které bude toto pravidlo aplikováno. Můžete zadat číslo portu nebo celý rozsah čísel portu zadáním prvního a posledního čísla portu z rozsahu. Dvě čísla jsou oddělena pomlčkou, například „101-150“ znamená z čísla portu 100 k číslu portu 150 – tj. rozsah 50 čísel portů.
Traffic Type (typ přenosu)	Zvolte typ přenosu packetů, na které bude toto pravidlo použito. Uvádíme některé populární aplikace pro usnadnění konfigurace. Můžete také docílit stejných výsledků použitím jiných parametrů, například číslo portu zdroje nebo destinace, pokud dobře znáte protokol aplikace.
Protocol (protokol)	Zvolte typ protokolu pro pakety, na které bude toto pravidlo použito.
Apply (použití)	Potvrďte Apply a odejděte z formuláře.
Reset	Vymaže obsah tohoto formuláře.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.6 NAT

Network Address Translation (NAT-překlad síťových adres) umožňuje více uživatelům Vaší lokální sítě přístup na Internet přes jedinou veřejnou IP adresu nebo několik veřejných IP adres. NAT zajišťuje i základní ochranu / Firewall vůči útokům hackerů a má flexibilitu, která umožňuje zobrazení / namapování soukromých IP adres veřejným IP adresám pro klíčové služby, jako jsou webové stránky a FTP.



Parametry	Popis
2.6.1 Port Forwarding (přesměrování portu)	Můžete mít různé služby (např. email, FTP, Web atd.) využívané různými servery/klienty ve Vaší LAN. Přesměrování portu umožňuje předadresovat určitý rozsah čísel portů služeb (z Internetu/WAN portu) na jednotlivé IP adresy LAN.
2.6.2 Virtual Server (virtuální server)	Můžete mít různé služby (např. email, FTP, Web atd.) přicházející na různé servery/klienty ve Vaší LAN. Virtuální server umožňuje předadresovat částečný rozsah čísel portů služeb (z Internetu/WAN portu) na jednotlivé IP adresy LAN.
2.6.3 Special Applications (speciální aplikace)	Některé aplikace vyžadují vícenásobné připojení, Jde např.o Internetové hry, video konference, IP telefonie a další. V této sekci můžete konfigurovat směrovač tak, aby podporoval tyto typy aplikací.

2.6.4 UPnP Setting (*nastavení UPnP*)

Umožňuje aktivovat nebo deaktivovat podporu UPnP. Jakmile aktivujete funkci UPnP, všechny klientské systémy, které podporují UPnP (např. Windows XP), mohou pak automaticky detekovat v síti tento směrovač a přístup na Internet přes směrovač pak nepotřebuje žádnou konfiguraci. Funkce UPnP díky „traverzní NAT“ může pak snadno připojit aplikace, které podporují UPnP k Internetu bez jakéhokoliv problému s kompatibilitou kvůli překladu NAT portu.

2.6.5 ALG Setting (*nastavení ALG*)

Můžete zvolit speciální aplikace, které potřebují pro podporu „Application Layer Gateway – Bránu na aplikační úrovni“.

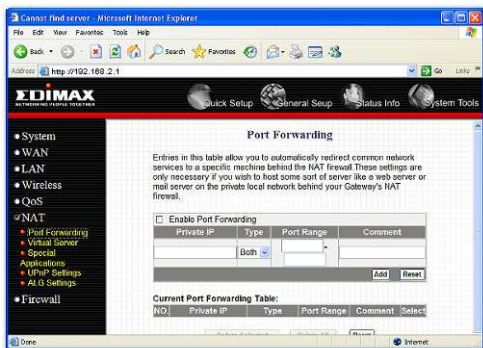
2.6.6 Static Routing (*statické směrování*)

Můžete deaktivovat NAT funkci a natavit ručně pravidla směrování.

Klikněte na jeden ze tří výběrů NAT a postupujte podle příslušné podsektce v návodu.

2.6.1 Port Forwarding – Přesměrování portu

Přesměrování portu umožňuje přeadresování určitého rozsahu čísel portů služeb (z portů Internetu/WAN) k jednotlivým LAN IP adresám. Pomůže Vám hostit některé servery za NAT, přirozeným firewallem směrovače.



Parametry

Popis

Enable Port Forwarding

(oprávnění přesměrování portu)

Zpřístupnění přesměrování portu

Private IP

(soukromá IP)

Je soukromá IP serveru za NAT firewallem.

Upozornění: Musíte přidělit Vaším klientským PC v LAN fixní/statickou IP adresu pro správné fungování přesměrování portu.

Type

(typ)

Typ protokolu, který má být přesměrován.

Můžete zvolit pouze přesměrování paketů „TCP“ nebo „UDP“ nebo zvolit „both“ - obojí pro přesměrování obou „TCP“ a „UDP“ paketů.

Port Range

(rozsah portu)

Rozsah portů, které mají být směrovány na soukromou IP.

Comment

(komentář)

Popis tohoto nastavení

Add Port Forwarding

(doplňte port přesměrování)

Vyplňte nastavení soukromé IP, typu, rozsahu portů a popisu (viz popis výše) a pak klikněte na „Add - přidat“. Poté bude toto nastavení doplněno do níže uvedené „Current Port Forwarding Table“ - tabulky nastavení přesměrování portů. Pokud potřebujete určitý typ editovat před přidáním do tabulky,

klikněte na „Clear - vymazat“ a pole budou smazána.

Remove Port Forwarding (odstranění přesměrování portů)

Pokud chcete odstranit některé nastavení přesměrování portů z „Current Port Forwarding Table“ - tabulky nastavení, vyberte nastavení směrování portů, která chcete odstranit a pak klikněte na „Delete Selected - smazat označené“. Pokud chcete z tabulky odstranit všechna nastavení směrování portu, klikněte na „Delete All - smazat vše“. Kliknutím „Reset-zrušení“ vymažete Vaši stávající volbu.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.6.2 Virtual Server – virtuální server

Funkci virtuální server použijte pokud chcete aby ve Vaší LAN různé servery/klienti obsluhovali různé typy servisních/Internetových aplikací (např. email, FTP, Web server atd.) z Internetu. Počítače používají čísla, které se nazývají čísla portů pro rozpoznání jednotlivých typů servisních/Internetových aplikací. Virtuální server umožňuje předadresovat jednotlivé čísla servisních portů (z Internetového/WAN portu) na jednotlivé soukromé / vnitřní IP adresy LAN a jejich čísla servisních portů. (viz slovník na konci pro vysvětlení „Port number“ - čísla portu)



Parametry

Popis

Enable Virtual Server (oprávnění virtuálního serveru)	Aktivuje virtuální server.
Private IP (soukromá IP)	Je IP adresa klientské/hostitelské LAN, do které budou posílány pakety určené veřejného číslu portu. Upozornění: Musíte přidělit Vaším klientským PC v LAN fixní/statickou IP adresu pro správné fungování virtuálního serveru.
Private Port (soukromý port)	Je číslo portu (výše uvedené hostitelské soukromé IP), na které budou změněné adresování paketů níže uvedeného čísla veřejného portu, když pakety vstoupí do Vaší LAN (do IP serveru/klienta místní/vnitřní sítě).
Type (typ)	Zvolte typ protokolu portu (TCP, UDP nebo oba). Pokud si nejste jisti, nechte implicitně zadány oba protokoly.
Public Port (veřejný port)	Zadejte servisní číslo portu (servisní/Internetové aplikace) z Internetu, který bude přesměrován na výše uvedenou hostitelskou soukromou IP adresu ve Vaší LAN. Upozornění: Funkce virtuálního serveru bude mít prioritu nad DMZ funkcí, pokud nastane konflikt mezi virtuálním serverem a nastavením DMZ.
Comment (komentář)	Popis tohoto nastavení.
Add Virtual Server (přidat virtuální server)	Vyplňte soukromou IP, soukromý port, veřejný port a komentář/popis nastavení, které má být přidáno a pak klikněte na „Add - přidat“. Pak bude nastavení tohoto virtuálního serveru přidáno do „Current Virtual Server Table“ tabulky aktuálního nastavení. Pokud budete chtít před jeho přidáním do tabulky ještě měnit údaje, klikněte na „Clear-vymazat“ a pole budou vymazána.
Remove Virtual Server (odstranit virtuální server)	Pokud chcete odstranit některé nastavení virtuálního serveru z tabulky nastavení „Current Virtual Server Table“, zvolte nastavení Virtual Serveru, které chcete odstranit a pak klikněte na „Delete Selected“-vymazat označené. Pokud chcete z tabulky

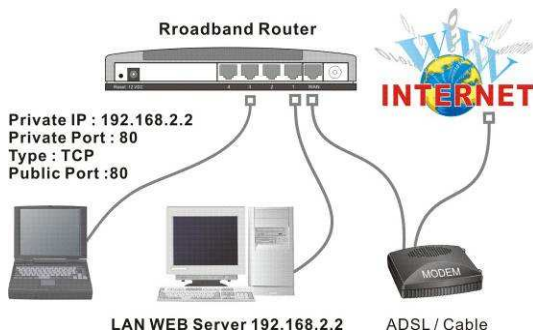
odstranit všechna nastavení virtuálního serveru, klikněte na „Delete all - smazat vše“. Kliknutím na „Reset - zrušit“ vymažete stávající volby.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

Příklad: Virtuální Server

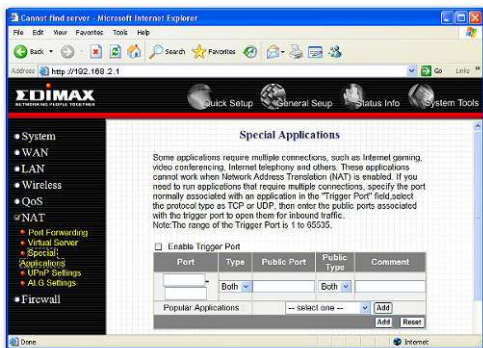
Dolní diagram ukazuje možný způsob jak používat funkci virtuálního serveru. Virtuální server použijte, pokud chcete, aby web server umístěný ve Vaší soukromé/vnitřní LAN byl přístupný uživatelům Internetu / „z venku“. Konfigurace níže znamená, že požadavek na přístup do Vašeho web serveru přicházející z Internetu bude přeložen na web server Vaší LAN (192.168.2.2).

Upozornění: Aby virtuální server pracoval správně, Internetoví/vzdálení uživatelé musí znát Vaší globální IP adresu. Pro provoz webových stránek musíte mít fixní/statickou globální/veřejnou IP adresu.



2.6.3 Speciální aplikace

Některé aplikace vyžadují vícenásobné připojení. Jedná se o Internetové hry, video konference, IP telefonování, atd. V této sekci ukážeme, jak konfigurovat směrovač tak, aby podporoval tyto typy aplikací.



Parametry

Popis

Enable Trigger Port Aktivuje speciální funkce aplikace.
(oprávnění spouštěcího portu)

Trigger Port Je odchozí (outbound) rozsah čísel portů této
(spouštěcí port)

Trigger Type Zvolte zda je protokol odchozího (spouštěcího) portu
(typ spouštění) „TCP“, „UDP“ nebo oba.

Public Port Zadejte příchozí (inbound) port nebo rozsah portů
(veřejný port) tohoto typu aplikace (např. 2300-2400, 47624)

Upozornění: Jednotlivá čísla portů jsou odděleny čárkou, (např. 47624, 5775,6541 apod.) Pro zadání rozsahu portu použijte pomlčku pro oddělení rozsahu čísel dvou portů (např. 2300-2400)

Public Type Zvolte typ protokolu odchozího portu: „TCP“, „UDP“
(veřejný typ) nebo oba.

Comment Popis tohoto nastavení.
(komentář)

Popular applications Tato sekce obsahuje nejoblíbenější aplikace,
(populární aplikace) které vyžadují vícenásobné připojení. Zvolte aplikaci ve výběru populárních aplikací.

Po jejím výběru zadejte umístění/pozici (1-10) v poli pro výběr **Copy to** a pak klikněte na **Copy to**. Tím se automaticky přiřadí potřebné veřejné porty požadované pro tuto aplikaci na určené místo (1-10), které je specifikovali.

Add Special Application
(*přidání speciální aplikace*)

Vyplňte Trigger Port, typ, veřejný port a typ a komentář nastavení, které má být přidáno a pak klikněte na „Add - přidat“. Pak bude nastavení této speciální aplikace přidáno do „Current TriggerPort“ tabulky nastavených spouštěcích portů“. Pokud chcete ještě měnit zadání, klikněte na „Clear - vymazat“ a pole budou vymazána. Pokud budete chtít přidat oblíbenou aplikaci, zvolte jednu „Popular Application“ a pak klikněte na „Add - přidat“.

Remove Special Application
(*odstranění speciální aplikace*)

Pokud chcete odstranit některá nastavení speciálních aplikací z tabulky stávajících spouštěcích portů, zvolte nastavení speciální aplikace, kterou chcete z tabulky odstranit a pak klikněte na „Delete Selected“ - vymazat označené. Pokud chcete odstranit všechna nastavení speciálních aplikací, klikněte na tlačítko „Delete all“ - smazat vše. Kliknutím na „Reset“ - zrušit vymažete stávající volbu.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

Příklad: Speciální aplikace

Pokud potřebujete spustit aplikaci, která vyžaduje vícenásobné připojení, pak specifikujte port (odchozí) obvykle přidružený k této aplikaci v poli „Trigger Port“. Pak zvolte typ protokolu (TCP nebo UDP) a zadejte veřejné porty přidružené ke spouštěcímu portu pro jejich otevření pro příchozí přenos.

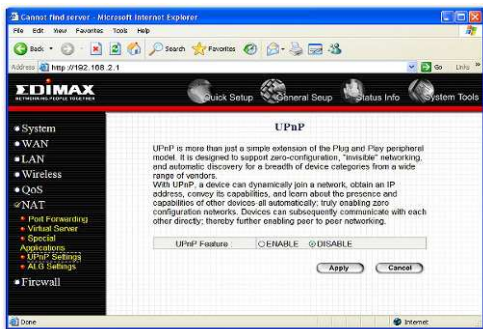
Příklad:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

Ve výše uvedeném příkladu, pokud uživatel Trigger Portu je 28800 (odchozí) pro hrací zónu MSN, pak směrovač umožní přesměrování příchozích paketů pro porty 2300-2400 a 47623 uživateli. **Upozornění:** Pouze jeden klient LAN může ve stejnou dobu použít danou speciální aplikaci.

2.6.4 Nastavení UPnP

S UPnP všechny počítače ve Vaší LAN/intranetu zaregistrují tento směrovač automaticky. Takže pro svůj počítač nepotřebujete žádnou konfiguraci a můžete přes tento směrovač ihned snadno přistupovat na Internet.



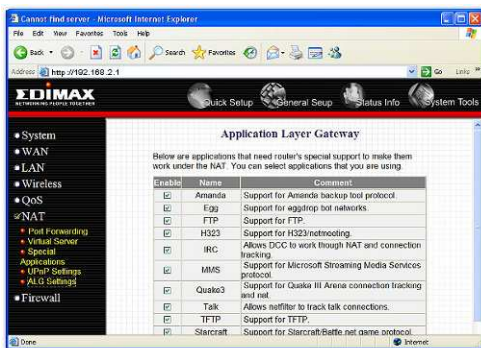
Parametry	Implicitně	Popis
UPnP Feature (funkce UPnP)	Neaktivní	Zde můžete aktivovat/deaktivovat funkci UPnP. Jakmile aktivujete funkci UPnP, Všechny klientské systémy, které podporují UPnP, jako je Windows XP, „vidí“ automaticky tento směrovač a mohou mít přístup na Internet přes tento směrovač bez jakékoliv konfigurace.

Funkce četnosti průchodů NAT(Traversal) poskytovaná UPnP může k Internetu hladce připojit aplikace, které UPnP podporuje, bez problémů kompatibility kvůli překladu NAPT portu.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.6.5 Nastavení ALG

Můžete zvolit aplikace, které potřebují podporu „Application Layer Gateway“ - bránu na aplikační úrovni síťového modelu.



Parametry

Implicita

Popis

Enable
(aktivní)

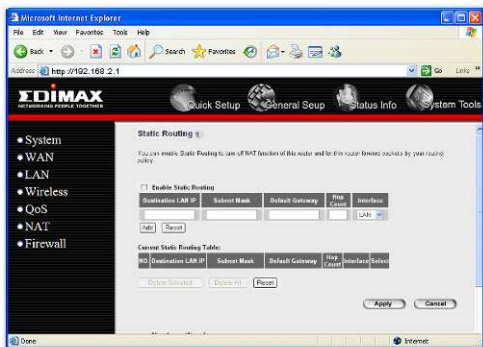
Můžete zvolit aktivaci „Application Layer Gateway“
Směrovač pak nechá tuto potřebnou aplikaci
správně projít přes NAT bránu.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.6.6 Static Routing - Statické směrování

Pokud je NAT deaktivován směrovač poskytuje statické směrování. Statickým směrováním může směrovač přenášet pakety podle Vašich pravidel směrování. Pozor v režimu statického směrování nebude pracovat funkce sdílení IP (dynamické IP).

Upozornění: Funkce DMZ firewallu nebude pracovat pokud je aktivováno statické směrování.



Parametry	Popis
Enable Static Routing (aktivní statické směrování)	Funkce statického směrování je implicitně vypnutá. Pokud chcete nastavit vlastní pravidla směrování je třeba aktivovat tuto funkci statického směrování
Destination LAN IP (IP cílové LAN)	Síťová adresa cílové LAN.
Subnet Mask (maska podsítě)	Maska podsítě cílové LAN.
Default Gateway (implicitní brána)	Nejbližší další brána na cestě k cílové LAN IP sousedního směrovače / routeru s nímž tento směrovač komunikuje cestou k cílové LAN.
Hop Count	Počet skoků (směrovačů / routerů) při průchodu

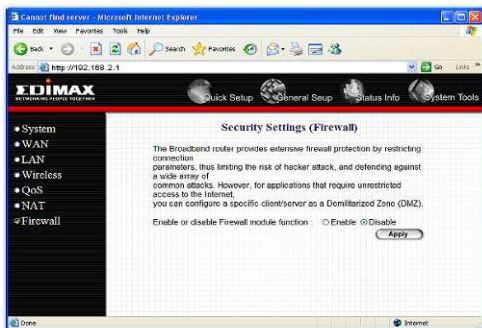
(počet skoků)	ceslou k dosažení cílové LAN.
Interface (rozhraní)	Rozhraní, které je cestou k dalšímu skoku (směrovači).
Add a Rule (zadání pravidla)	Vyplňte „Destination LAN IP“ – IP cílové LAN, masku podsítě, implicitní bránu, počet skoků a rozhraní pravidla, které má být přidáno a pak klikněte na „Add - přidat“. Pak toto pravidlo statického směrování bude přidáno do tabulky statického směrování. Pokud před přidáním budete chtít něco upravit, klikněte na „Reset-zrušit“ a tato pole budou vymazána.
Remove a Rule (odstranit pravidlo)	Pokud chcete odstranit některá pravidla směrování z tabulky statického směrování, zvolte pravidla, která chcete z tabulky odstranit a pak klikněte na „Delete Selected“- vymazat označené. Kliknutím na „Reset-zrušit“ vymažete stávající volby.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.7. Firewall

Širokopásmový směrovač poskytuje rozšířenou ochranu Firewalllem, který omezí parametry připojení. Tím se sníží riziko útoků hackerů, a zajistí ochrana vůči širokému poli Internetovým útoků. Nicméně, pro aplikace, které vyžadují volný přístup k Internetu bude třeba speciálně nakonfigurovat klienta/server jako demilitarizovaná zóna (DMZ).

Upozornění: Pro aktivaci Firewallu a jeho nastavení zvolte **Enable - aktivovat** a klikněte na **Apply - použít**.



Parametry

Popis

2.6.1 Access Control (kontrola přístupu)

Kontrola přístupu umožňuje specifikovat, který uživatel může nebo nemůže mít přístup k určitým Internetovým aplikacím.

2.6.2 URL Blocking (blokování URL)

Blokování URL umožňuje specifikovat, které URL nebudou pro uživatele přístupné.

2.6.3 DoS

Firewall širokopásmového směrovače může blokovat útoky hackerů a může zaznamenat útočné aktivity do log výpisu.

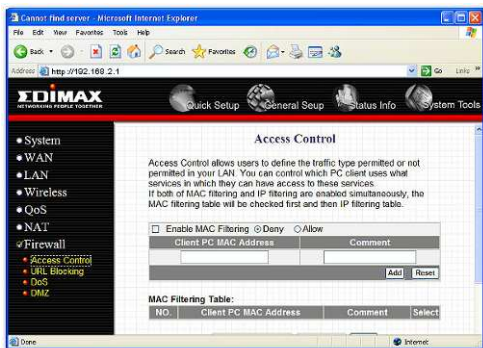
2.6.4 DMZ

Funkce DMZ umožňuje přesměrovat všechny pakety, které jdou na Vaši IP adresu WAN portu na specifickou IP adresu ve Vaší LAN.

Klikněte na jednu z částí firewallu a postupujte podle příslušné podsekcce v návodu.

2.7.1 Access Control - Kontrola přístupu

Pokud chcete omezit uživatele v přístupu z určitých Internetových aplikací/služeb (např. Internetové webové stránky, email, FTP atd.), pak to zde můžete nastavit. Kontrola přístupu umožňuje uživateli definovat typ přenosů povolený ve Vaší LAN. Můžete kontrolovat, který klientský PC může mít přístup k této službě.



Parametry

Popis

Deny
(zamítnutí)

Pokud zvolíte „Deny - odmítnout“, pak všechny počítače budou mít přístup na Internet, kromě počítačů uvedených v seznamu odmítnutých.

Allow
(povolit)

Pokud zvolíte „Allow - povolit“, pak všechny počítače budou mít zamítnut přístup k Internetu kromě počítačů na seznamu povolených.

Filter client PCs by IP
(filtrace klientských
PC podle IP)

Pro filtraci klientských počítačů podle IP vyplňte tabulku filtrovaných PC „IP Filtering Table“.

Add PC
(přidat PC)

Pro přidání pravidla kontroly přístupu podle IP adresy klikněte na „Add PC“ - přidat PC

Remove PC
(odstranit PC)

Pokud chcete odstranit některé počítače z tabulky filtrování IP, zvolte počítač, který chcete z tabulky odstranit a pak klikněte na „Delete Selected“ - vymazat označené. Pokud chcete odstranit z tabulky všechny počítače, klikněte na „Delete All“ - vymazat vše.

Filter client PC by MAC address Ověřte aktivaci filtrace MAC adres
(filtr klientského PC MAC adresou) „Enable MAC Filtering“

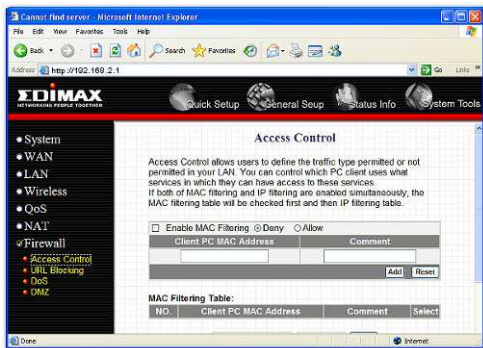
Add PC
(přidat PC)

Vyplňte „Client PC MAC Address“ - MAC adresu klientského PC“ a „Comment -popis počítače s oprávněním pro přístup k Internetu, a pak potvrďte „Add“. Pokud před přidáním budete chtít něco přepsat, klikněte na „Clear“ nebo „Reset“ pro zrušení a pole budou vymazána.

Remove PC
(odstranit PC)

Pokud chcete odstranit některá PC z tabulky „MAC Filtering Table“, zvolte v tabulce PC, které chcete odstranit a pak klikněte na „Delete Selected“ - vymazat označené. Pokud chcete volbu vymazat a provést volbu znovu, klikněte na „Reset“.

Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením)



Add PC – přidat PC

Parametry

Popis

Client PC Description
(popis klientského PC)

Popis pravidla pro tento klientský PC.

Client PC IP Addresses
(IP adresy klientského PC)

Zadejte rozsah IP adresy, na kterou chcete aplikovat toto pravidlo kontrolního přístupu. Toto je IP adresa uživatele(ů), u kterých chcete toto pravidlo kontrolního přístupu nastavit.

Upozornění: Musíte zadat svým LAN klientským PC fixní/statickou IP adresu, aby pravidlo kontroly přístupu pracovalo správně.

Client PC Service
(služby klientského PC)

Můžete klientům zablokovat přístup k některým Internetovým službám kontrolou služeb, které chcete blokovat.

Protocol
(protokol)

Umožňuje zvolit UDP, TCP nebo oba typy protokolu, které chcete blokovat.

Port Range
(rozsah portů)

Může určit až pět rozsahů portů. Směrovač zablokuje klientům přístup k Internetovým službám, které používají tento port.

Apply Changes
(použít změny)

Pro uložení nastavení klikněte „Apply Changes“.

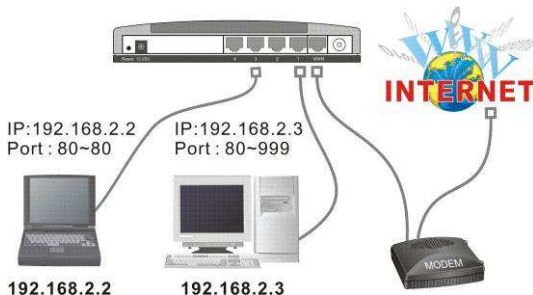
Reset

Kliknutím na „Reset“ vymažete všechna pole.

Pro uložení výše uvedených konfigurací klikněte na **<Apply Changes>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

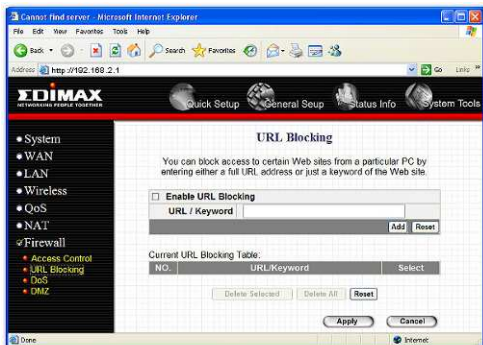
Příklad: Access Control - kontrola přístupu

V dolním příkladu LAN klient A může mít přístup pouze na webové stránky, které používají Port 80. Nicméně, LAN klient B má přístup na webové stránky a každou další službu, která používá porty mezi 80 a 999.



2.7.2 URL Blocking - Blokování URL

Můžete blokovat přístup k některým webovým stránkám z jednotlivých PC zadáním úplné URL adresy nebo klíčového slova webové stránky.

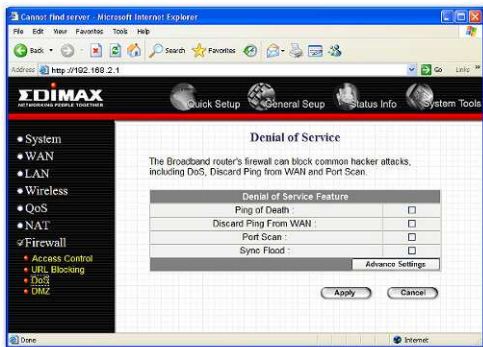


Parametry	Popis
Enable URL Blocking (oprávnění blokování URL)	Aktivuje/deaktivuje blokování URL
Add URL Keyword (zadání URL slova)	Vyplňte „URL/Keyword“ – adresu či klíčové slovo a pak klikněte na „Add“. Můžete zadat úplnou URL adresu nebo slovo z webové stránky, kterou chcete blokovat. Pokud před přidáním budete chtít ještě něco přepsat, klikněte na „Reset - zrušit“ a tato pole budou vymazána.
Remove URL Keyword (odstranit URL slova)	Pokud chcete odstranit některé položky URL z tabulky „Current URL Blocking“ stávajících blokování URL, zvolte položku URL, které chcete odstranit a pak klikněte na „Delete Selected“ - vymazat označené. Pokud chcete z tabulky odstranit všechna URL hesla, klikněte na „Delete All“ - vymazat vše. Pokud chcete vymazat výběr a znovu jej zadat, klikněte na „Reset“.

Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením)

2.7.3 DoS (Denial of Service - odmítnutí služby)

Firewall širokopásmového směrovače může blokovat běžné útoky hackerů, včetně Denial of Service (odmítnutí služby), Ping of Death, Port Scan a Sync Flood. Pokud dojde k útoku z Internetu směrovač události zaznamená a lze je vidět ve výpisu logu.



Parametry	Popis
-----------	-------

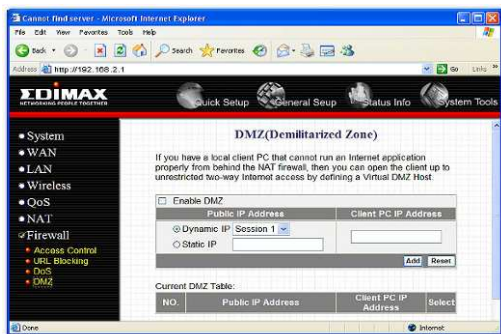
Charakteristika detektoru narušení

Ping of Death	Ochrana před útokem Ping of Death
Discard Ping From WAN	WAN port směrovače nebude odpovídat na jakékoliv požadavky Ping
Port Scan	Ochrana směrovače před scanováním portů.
Sync Flood	Ochrana směrovače před útoky Sync Flood.

Pro uložení výše uvedených konfigurací klikněte na **<Apply>** v dolní části obrazovky. Nyní můžete konfigurovat další sekce nebo začít používat směrovač (s vhodným přednastavením).

2.7.4 DMZ

Pokud máte lokální klientský počítač, který nemůže správně spustit Internetovou aplikaci (např. hry) za NAT firewallem (z LAN), pak můžete otevřít klientovi komunikaci na neomezeném oboustranném přístupu k Internetu definováním hostitelské DMZ. Funkce DMZ umožňuje přesměrovat všechny pakety přicházející na Vaši IP adresu WAN portu na specifickou IP adresu Vašeho LAN. Rozdíl mezi virtuálním serverem a funkcí DMZ je ten, že virtuální server přesměruje jen určené služby /Internetové aplikace na specifického klienta/server LAN, zatímco DMZ přesměruje všechny pakety (nezávisle na službách) přicházející na IP adresu Vašeho WAN na specifického klienta/server LAN.



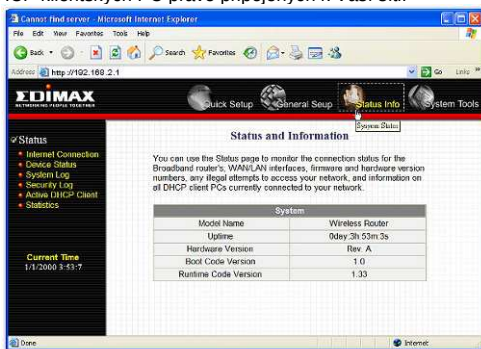
Parametry	Popis
Enable DMZ (oprávnění DMZ)	Oprávnění/zamítnutí DMZ Upozornění: Pokud nastane konflikt mezi virtuálním serverem a nastavením DMZ, pak funkce virtuálního serveru bude mít přednost před DMZ funkcí.
Public IP Address (veřejná IP adresa)	IP adresa WAN portu nebo jakákoliv jiná veřejná IP adresa, přidělená Vaším poskytovatelem (ISP)
Client PC IP Address (IP adresa klientského PC)	Zadejte IP adresu specifického hostitele ve Vaší LAN, která bude přijímat všechny pakety přicházející přímo do WAN portu/veřejné IP adresy Upozornění: Aby DMZ správně fungovalo, musíte

dát svému klientskému PC LAN fixní/statickou adresu.

Kapitola 3

Status – stav

Sekce Stav Vám umožňuje monitorovat aktuální stav Vašeho směrovače. Tuto stránku můžete používat pro monitorování: stavu připojení WAN/LAN rozhraní širokopásmového směrovače, stávajících verzí firmware a hardware, jakýchkoliv ilegálních útoků/přístupů do Vaší sítě, a seznamu všech DHCP klientských PC právě připojených k Vaší síti.



Parametry

Popis

- | | |
|--|---|
| 3.1 Status and Information
(stav a informace) | Ukazuje informace o systému směrovače. |
| 3.2 Internet Connection
(připojení Internetu) | Zobrazuje aktuální stav připojení k Internetu širokopásmového směrovače a další příslušné informace |
| 3.3 Device Status
(stav zařízení) | Zobrazuje aktuální stav nastavení širokopásmového směrovače |
| 3.4 System Log
(výpis systému) | Zobrazuje výpis systémových událostí širokopásmového směrovače |

3.5 Security Log
(bezpečnostní přihlášení)

Zobrazuje všechny pokusy o ilegální přístup do Vaší sítě.

3.6 Active DHCP Client
(aktivní DHCP klient)

Zobrazuje informace o LAN klientech, které jsou právě připojeni k DHCP serveru směrovače

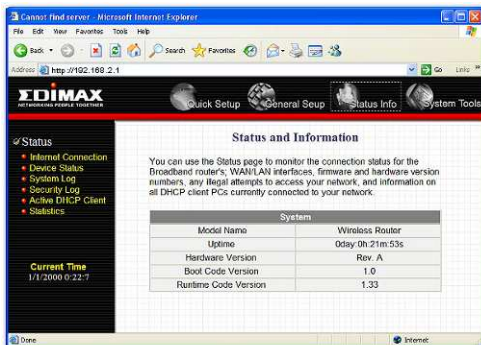
3.7 Statistics
(statistika)

Ukazuje statistiku

Zvolte jeden z výše uvedených výběrů stavu a postupujte podle příslušné podsektce v návodu.

3.1. Status and Information – stav a informace

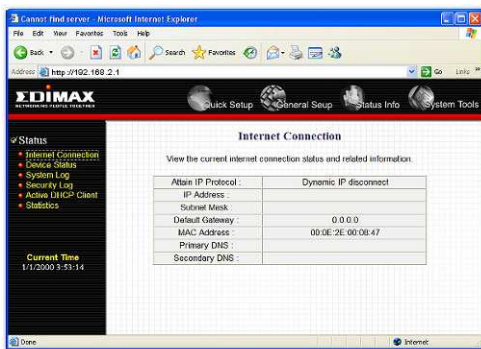
Sekce stav a informace umožňuje zobrazit informace o systému směrovače.



Parametry	Popis
Information (<i>informace</i>)	Můžete sledovat tyto informace o systému směrovače: LAN MAC adresa, WAN MAC adresa, verze Hardware, sériové číslo, verze Firmware, verze kódu doby provozu (Runtime Code)

3.2. Internet Connection – připojení Internetu

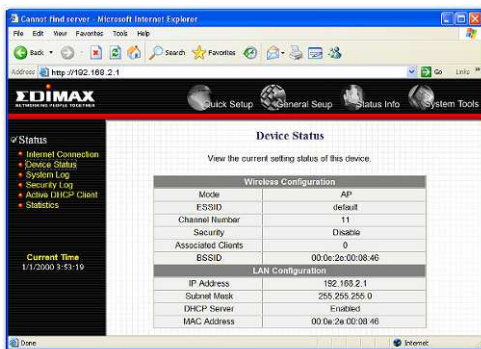
Zobrazí stav aktuálního připojení širokopásmového směrovače k Internetu a další příslušné informace.



Parametry	Popis
Internet Connection (<i>připojení Internetu</i>)	Tato strana se zobrazí, když je WAN port připojen ke kabelovému /DSL připojení. Zobrazí info o WAN portu směrovače: WAN IP adresu, masku podsítě , a ISP bráně , stejně tak i použité primární DNS a sekundární DNS .

3.3 Device Status – stav zařízení

Zobrazí stávající nastavení konfigurace širokopásmového směrovače. Zobrazuje se zde nastavení konfigurace, které jste provedli v sekci Quick Setup Wizard/General Setup (rychlé nastavení/všeobecné nastavení).



Parametry

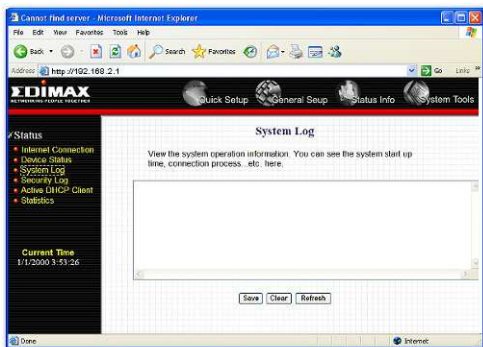
Popis

Device Status
(stav zařízení)

Tato strana zobrazuje aktuální nastavení širokopásmového směrovače. Tato strana zobrazí aktuální **IP adresu** LAN portu směrovače a **masku podsítě**. Zobrazí také zda je aktivní (Enabled) **DHCP server**.

3.4 System Log – výpis systémových událostí

Zobrazí provozní informace systému směrovače.



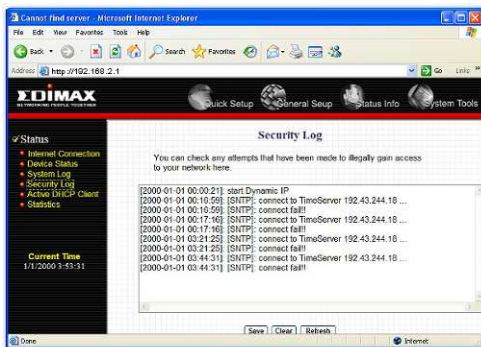
Parametry	Popis
-----------	-------

System Log
(výpis ze
systému)

Tato strana ukazuje aktuální výpis ze systému širokopásmového směrovače. Zobrazí každou událost, ke které došlo po spuštění systému. V dolní části obrazovky je volba pro uložení <Save> výpisu systému do souboru pro další zpracování nebo volba pro vymazání tohoto výpisu <Clear>, nebo může být obnoveno volbou <Refresh> pro aktualizaci situace. Při vypnutí systému dojde k vymazání výpisu, pokud jste jej neuložili do souboru.

3.5 Security Log – bezpečnostní výpis

Zobrazí všechny útoky, které proběhly pro ilegální přístup do Vaší sítě.



Parametry

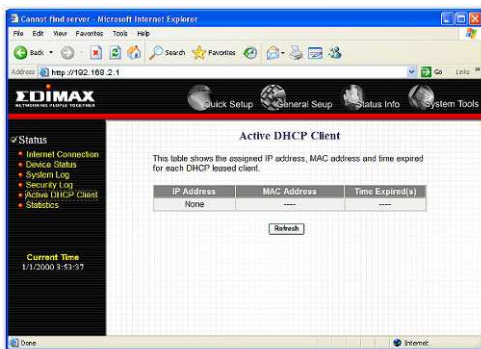
Popis

Security Log (bezpečnostní výpis)

Tato strana ukazuje aktuální bezpečnostní výpis událostí širokopásmového směrovače. Zobrazí každý pokus vniknout do sítě ke kterému došlo po spuštění systému. V dolní části obrazovky můžete výpis uložit <Save> do lokálního souboru např. pro další zpracování nebo výpis můžete vymazat stiskem tlačítka <Clear> nebo můžete obnovit/aktualizovat zobrazení výpisu pomocí tlačítka <Refresh> Při vypnutí systému dojde k vymazání výpisu, pokud jste jej neuložili do souboru.

3.6 Active DHCP Client – aktivní DHCP klient

Zobrazí informace o klientských stanicích LAN, které jsou právě spojeny s DHCP serverem širokopásmového směrovače.



Parametry

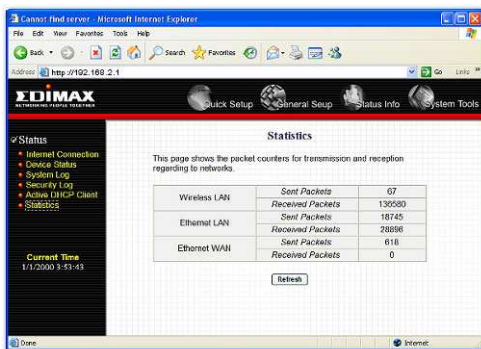
Popis

Active DHCP Client
(aktivní DHCP klient)

Tato strana zobrazí všechny klienty (LAN PC) DHCP serveru aktuálně připojené k Vaší síti. Tabulka „Active DHCP Client Table“ ukazuje **IP** adresu a **MAC** adresu a dobu jejich platnosti pro každého klienta LAN. Pro aktualizaci seznamu použijte tlačítko **Refresh - oživit**.

3.7 Statistics – statistika

Zobrazuje statistiku paketů posílaných a přijímaných WAN, LAN a bezdrátovou sítí (WiFi).



Parametry

Popis

Statistics
(statistika)

Zobrazí počítadlo odeslaných a přijatých paketů pro WAN, LAN a bezdrátovou LAN (WiFi síť).

Kapitola 4

Tool – nástroje

Tato strana obsahuje možnosti základní konfigurace, jako jsou nástroje konfigurace (uložení a obnovení nastavení konfigurace), aktualizace Firmware (poslední dostupný F/W systému viz www.edimax.com) a restart.

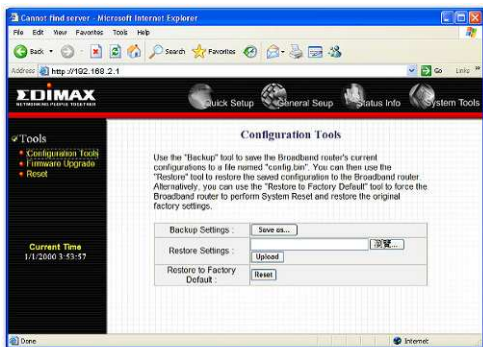


Parametry	Popis
4.1 Configuration Tool (<i>nástroje konfigurace</i>)	Můžete uložit nastavenou konfiguraci směrovače, obnovit konfiguraci pomocí uložených konfiguračních souborů, a obnovit implicitní tovární nastavení směrovače
4.2 Firmware Upgrade (<i>aktualizace firmware</i>)	Tato strana umožní aktualizovat firmware směrovače (dostupný na www.edimax.com)
4.3 Reset	Můžete resetovat systém směrovače, pokud se objeví jakýkoliv problém

Zvolte jeden ze tří výše uvedených **Tools Settings – nástrojů nastavení** a pokračujte podle příslušné podsekce v návodu.

4.1 Configuration Tool – nástroje konfigurace

Obrazovka Nástroje konfigurace umožňuje uložit (**Backup**) stávající Vámi připravené nastavení konfigurace směrovače. Soubor s uloženým nastavením konfigurace můžete využít jako pomoc, pokud by došlo k problému se směrovačem a Vy ho museli resetovat na implicitní tovární nastavení. Pomocí uloženého nastavení konfigurace (backup) můžete rychle obnovit konfiguraci směrovače volbou **Restore – opravit** (zadat cestu k uloženému souboru s backupem). Pokud problémy přetrvávají, můžete použít volbu **Restore to Factory Defaults - obnovení továrního nastavení**, tím budou změněny všechny konfigurace na své původní implicitní nastavení (tj. nastavení, když jste směrovač koupili).



Parametry

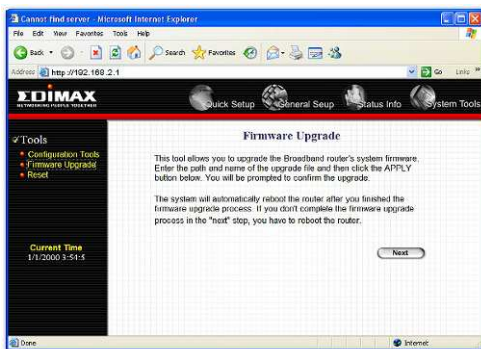
Popis

Configuration Tools (nástroje konfigurace)

Pro uložení aktuální konfigurace širokopásmového směrovače do souboru "config.bin" ve Vašem PC použijte nástroj "**Backup**" - záloha. Pak můžete použít nástroj "**Restore**" pro obnovení v souboru uložené konfiguraci širokopásmového směrovače. Alternativně můžete použít nástroj "**Restore to Factory Defaults**" - obnova na tovární nastavení provedení resetování širokopásmového směrovače a obnovit implicitní tovární nastavení.

4.2 Firmware Upgrade – aktualizace Firmware

Tato strana Vám umožňuje aktualizovat firmware směrovače.



Parametry

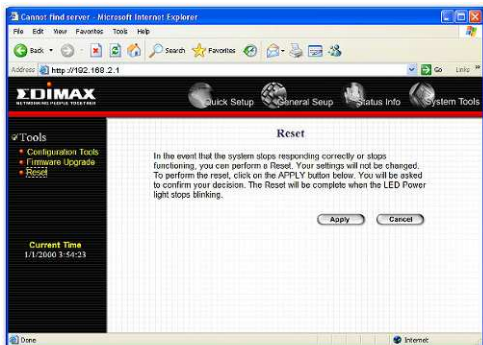
Popis

Firmware Upgrade (aktualizace firmware) Tento nástroj umožňuje aktualizovat Firmware systému směrovače. Pro aktualizaci firmware směrovače musíte stáhnout z www.edimax.com soubor s firmware na Váš lokální harddisk a zadat v příslušném poli cestu, kde je soubor uložen. Pro vyhledání firmware ve Vašem počítači můžete také využít tlačítko Browse (vyhledat).

Jakmile jste vybrali soubor s novým Firmware klikněte na **<Apply>** (v dolní části obrazovky) pro spuštění procesu aktualizace. Pozor, musíte několik minut počkat na dokončení aktualizace, během aktualizace v žádném případě nevypínejte směrovač z elektrické sítě. Jakmile jste aktualizaci dokončili, můžete začít směrovač používat.

4.3 Reset

Pokud se objeví nějaký problém, doporučujeme resetovat systém směrovače. Funkce resetování restartuje systém a obnoví korektní funkčnost.

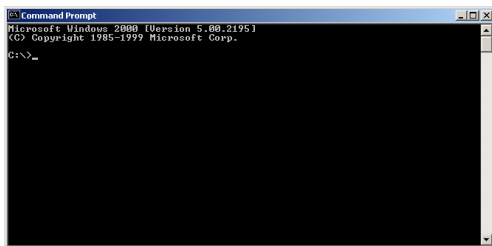


Parametry	Popis
Reset	V případech, kdy systém přestane správně reagovat nebo přestanou pracovat jeho funkce, můžete provést resetování. Vaše nastavení nebude změněno. K provedení resetování klikněte na tlačítko <APPLY>. Budete vyzváni k potvrzení Vašeho rozhodnutí. Restartování bude kompletní, jakmile přestane blikat provozní kontrolka. Jakmile je process restartování dokončen, můžete směrovač začít znovu používat.

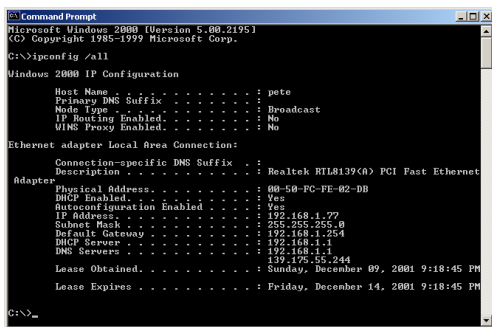
Příloha A

Jak ručně najít IP a MAC adresu svého PC?

- 1) V okně Windows otevřete program příkazový řádek (např. příkazem „cmd“ v poli „spustit“ nabídky Start).



- 2) Zadejte (s mezerou) **Ipconfig /all** a potvrďte <enter>



- IP adresa Vašeho PC je v řádku uvedeném jako **IP adresa** (zde 192.168.1.77)
- IP adresa směrovače je uvedena jako **Výchozí brána** (zde Default Gateway (192.168.1.254))
- MAC adresa Vašeho PC je **Fyzická adresa** (zde 00-50-FC-FE-02-DB)

Slovníček pojmů

Výchozí brána směrovače (Default Gateway - Router): Každé IP zařízení, které není směrovačem, potřebuje nakonfigurovat implicitní IP adresu brány. Když zařízení odesílá IP paket a pokud jeho cíl neleží v místní síti (LAN), zařízení odesílá pakety na svou Výchozí bránu a ta je pak odešle dál.

DHCP: Dynamic Host Configuration Protocol – Tento protokol poskytuje každému počítači ve Vaší domácí síti automaticky jeho IP adresu.

IP adresa DNS serveru (DNS Server IP Address): DNS znamená Domain Name Systém a umožňuje Internetovým serverům mít jméno domény (jako je www.Broadbandrouter.com) a jednu nebo více IP adres (jako je 192.34.45.8). DNS server uchovává databázi Internetových serverů a jejich příslušných jmen domén a IP adres, takže pokud zadáte jméno domény (např. „Broadbandrouter.com“) ve Vašem Internetovém prohlížeči, pak je uživatel přesměrován na správnou IP adresu (která identifikuje požadovanou doménu v síti Internetu). IP adresa DNS serveru používaná počítači ve Vaší domácí síti je umístění DNS severu, kterou Vám Váš ISP přidělil.

DSL Modem: DSL znamená Digitální účastnické vedení. DSL modem používá Vaše stávající telefonní dráty pro přenos dat vysokou rychlostí.

Ethernet: Několik standardů pro počítačové sítě. Ethernet sítě jsou připojeny speciálním kabelem s RJ45 konektory a opakovači signálu (switch), běžně dnes posílají data 10 až 100 milionu bitů za vteřinu (Mbps).

Doba nečinnosti (Idle Timeout): Doba nečinnosti je nastavena tak, že pokud nedochází k přenosu dat během přednastavené doby, připojení k Internetu se automaticky odpojí.

IP Adresa a maska podsítě (Subnet Mask): IP znamená Internet Protokol. IP adresa se skládá z řady čtyř oddělených čísel, které identifikují jednotlivého, jedinečného Internetového hostitele v IP síti. Příklad: 192.168.2.1. Je tvořena 2 částmi: síťová IP adresa, a identifikace hostitele.

IP adresa je 32-bit binární matice, která může být zastoupena čtyřmi za sebou řazenými desítkovými čísly oddělenými „.“. aaa.aaa.aaa.aaa, kde každé „aaa“ může být cokoliv od 000 do 255, nebo jako čtyři za sebou řazené binární čísla oddělené „.“: bbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, kde každé „b“ může být buď 0 nebo 1.

Síťová maska je také 32-bitová binární matice a je tvořena za sebou jdoucími 1, následovány za sebou jdoucími 0, jako je

11111111.11111111.11111111.00000000. Proto může být někdy maska sítě popsána prostě jako číslo „x“ začínající 1. Pokud jsou obě zastoupeny ve

své binární podobě, všechny bity v IP adrese, které korespondují s 1 v masce sítě jsou částí síťové IP adresy a zbylé bity odpovídají hostitelskému ID.

Například, pokud je IP adresa zařízení ve své binární formě, 11011001.10110000.10010000.00000111, a její maska sítě je, 11111111.11111111.11110000.00000000 znamená to, že síťová adresa zařízení je 11011001.10110000.10010000.00000000, a jeho hostitelské ID je 00000000.00000000.00000000.00000111. To je pohodlný a efektivní způsob pro směrování / routování IP paketů do jejich cíle.

Adresa brány ISP (ISP Gateway Address: (viz definice ISP) jde o IP adresu směrovače do Internetu umístěného u ISP (např. v kanceláři).

ISP: Internet Service Provider – poskytovatel připojení Internetu. ISP je obchodní činnost, která zajišťuje připojení k Internetu pro individuální a obchodní potřeby či celé organizace. Většinou vlastní či má pronajatý přístup k páteřnímu vedení datových toků.

LAN: Local Area Network – lokální/místní datová síť. LAN je skupina vzájemně propojených počítačů a zařízení na relativně malém prostoru (jako je dům nebo kancelář). Vaše domácí síť je považována za LAN.

MAC adresa: MAC znamená Media Access Control - řízení přístupu médií. Jde o adresu hardware zařízení připojeného k síti. MAC adresa je jedinečná identifikace zařízení s rozhraním Ethernet. Je složena ze dvou částí: 3 byty dat odpovídají ID výrobce (jedinečné pro každého výrobce), plus 3 byty, které jsou často používány jako sériové číslo výrobku.

NAT: Network Address Translation – překlad síťové adresy. Tento proces umožňuje všem počítačům např. v domácí síti používat jednu IP adresu (registrovanou a unikátní v mezinárodní síti Internet). Použitím kapacity NAT širokopásmového směrovače můžete mít přístup k Internetu z jakéhokoliv počítače ve své domácí síti aniž byste kupovali další veřejné IP adresy od svého ISP.

Paket (Packet): značí blok přenášených informací počítačovou sítí. Určité typy síťových propojení (např. bod-bod) nepodporují přenos paketů; v tomto případě se data po lince modulují (např. v směrovači nebo modemu) a přenášejí jako série bytů, znaků nebo bitů.

Port: Síťoví klienti (počítače v LAN) používají čísla portů pro rozlišení jedné síťové aplikace/protokolu od jiné. Níže je uveden seznam nejčastějších aplikací a čísel protokolu/portu:

Application/aplikace	Protocol/protokol	Port Number/číslo portu
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Protokol „bod – bod“ je původně vytvořený jako metoda bezpečného přenosu dat pro vytáčené připojení (56k). PPPoE připojení na základě Ethernetu. PPPoE pracuje ve dvou běžně rozšířených standardech: Ethernet a Point-to-Point Protocol.. Je to standardní komunikační protokol pro přenos informací přes Ethernetovou síť mezi různými výrobci.

Protocol: Protokol je sada pravidel pro interakci domluvenou mezi několika stranami, takže pokud jsou navzájem připojeni na bázi takového protokolu, interpretace jejich vztahu a komunikace je jasně definována a může být objektivní, bez zmatků nebo nedorozumění.

Směrovač (= Router): Směrovač je inteligentní síťové zařízení, které směruje pakety mezi různými sítěmi podle informace ze síťové vrstvy, jakou jsou IP adresy. Směrovače jednoduše poskytují přechod mezi různými sítěmi.

Subnet Mask (maska podsítě): Může být částí TCP/IP informace poskytnuté Vaším ISP, je nastavena čtyřmi čísly (např. 255.255.255.0) konfigurovanými jako IP adresa. Používá se pro vytvoření čísla IP adresy použité pouze v jednotlivé síti (oproti číslům platné veřejné IP adresy rozpoznatelné Internetem, která musí být přidělena mezinárodní organizací NIC).

TCP/IP, UDP: Transmission Control Protocol /Internet Protocol (TCP/IP) a Unreliable Datagram Protocol (UDP). TCP/IP je standardní protokol pro přenos dat přes Internet. TCP i UDP jsou transportními protokoly. TCP vykonává detekci chyb a regeneraci chyb, díky čemuž jsou spolehlivé. UDP na druhé straně spolehlivý není. Oba běží v nejvyšších vrstvách Internetového protokolu.

WAN: Wide Area Network – rozsáhlá počítačová síť. Síť, která spojuje počítače umístěné v geograficky oddělených místech (např. různé budovy, města, státy). Internet je také rozsáhlá počítačová síť. Jde o síť, která je směrovači připojená na veřejné telekomunikační linky.

Web-based management Graphical User Interface (GUI)- ovládání přes standardní webové rozhraní – grafické uživatelské rozhraní: Mnoho zařízení podporuje grafické uživatelské rozhraní, které je založeno na webovém vyhledávači. To znamená, že uživatel může používat obecné programy jako jsou Mozilla Firefox nebo Microsoft Internet Explorer pro řízení/konfiguraci nebo monitorování zařízení, které je takto spravováno.