VMG1312-B30B

Čtyřportová brána VDSL2 s bezdrátovou technologií 802.11n

Uživatelská příručka

IP Adresa	http://10.0.0.138
Přihlašovací jméno	admin
Heslo	admin

3/2014

www.zyxel.com

ZyXEL

OBSAH

1 ZÁKLADNÍ INFORMACE 9
1.1 Popis zařízení 9
1.2 Správa zařízení 9
1.3 Několik užitečných typů pro správu zařízení 9
1.4 Typická instalace zařízení 10
1.4.1 Připojení k internetu 10
1.5 Bezdrátový přístup 11
1.5.1 Tlačítko WPS/WLAN 11
1.6 LED kontrolky 12
1.7 Tlačítko RESET 13
1.7.1 Reset modemu pomocí tlačítka 13

2 WEBOVÉ ROZHRANÍ 14
2.1 Základní informace 14
2.1.1 Jak se přihlásit k webovému rozhraní 14
2.2 Hlavní obrazovka 16
2.2.1 Titulkový pruh 16
2.2.2 Navigační panel 17
2.2.3 Hlavní okno 19

3 STAVOVÁ OBRAZOVKA 20
3.1 Základní informace 20
3.2 Informace o zařízení 20

4 TYPOVÉ PŘÍKLADY 23
4.1 Základní informace 23
4.2 Nastavení bezpečné bezdrátové sítě 23
4.2.1 Konfigurace bezdrátové sítě 23
4.2.2 Nastavení prostřednictvím WPS 24
4.2.3 Nastavení bez WPS 28

5 NASTAVENÍ SÍTĚ WAN 28
5.1 Základní informace 28
5.1.1 Co je třeba vědět o síti WAN 29
5.1.2 Než začnete 30
5.2 Nastavení WAN rozhraní – L2 interface 30
5.2.1 Rozšířená konfigurace – přidání rozhraní L2 30
5.3 Nastavení WAN služby 32
5.3.1 PPPoE 33

5.3.2 Bridge 38

6 NASTAVENÍ SÍTĚ LAN 40

6.1 Základní informace 40
6.1.1 Co je třeba vědět o síti LAN 40
6.1.2 Než začnete 41
6.2 Obrazovka LAN 41
6.3 Nastavení IP adresy 43
6.4 Seznam klientů 43
6.5 IP alias 44
6.5.1 Konfigurace IP aliasu 44
6.6 IPv6 autoconfig 45

7 BEZDRÁTOVÁ SÍŤ LAN 48

7.1 Základní informace 48
7.1.1 Co všechno lze nastavit na obrazovkách Wireless LAN 48
7.1.2 Co je třeba vědět o bezdrátových sítích 49
7.1.3 Než začnete 49
7.2 Základní nastavení přístupového bodu (AP) 50
7.2.1 Nastavení dalších bezdrátových sítí 51
7.3 Nastavení zabezpečení 51
7.3.1 Nezabezpečená síť 52
7.3.2 Šifrování WEP 52
7.3.3 Šifrování WPA(2)-PSK 53
7.3.4 Autentizace WPA(2) 53
7.4 MAC Filtr 54
7.5 Pokročilé nastavení bezdrátové sítě 55
7.6 Seznam klientů 56
7.7 Nastavení prostřednictvím WPS: zařízení ZyXEL 57

8 PŘEKLAD SÍŤOVÝCH ADRES (NAT) 59

8.1 Základní informace 59
8.1.1 Co všechno lze nastavit na obrazovkách NAT 59
8.1.2 Co je třeba vědět o překladu síťových adres (NAT) 59
8.2 Virtuální servery 60
8.3 DMZ Host 61
8.4 SIP ALG 61

9 FIREWALL 62

9.1 Základní informace 62
9.1.1 Co všechno lze nastavit na obrazovkách Firewall 62
9.1.2 Co je třeba vědět o firewallu 62

9.2 Zapnutí firewallu 63
9.3 Pravidla 64
9.4 DoS 67
9.5 MAC filtr 67

10 RODIČOVSKÁ KONTROLA 69
10.1 Časové omezení 69
10.2 Filtrování podle adres URL 70

11 STATIC IP V4 NEIGHBOR 71
11.1 Static IPv4 neighbor 71
11.2 Static IPv6 neighbor 72

12 QUALITY OF SERVICE 73
12.1 Quality of Service 73
12.2 QoS Queue 73
12.3 QoS Classification 75

13 ROUTING 77
13.1 Výchozí brána 77
13.2 Static Route 77
13.3 Policy routing 78
13.4 RIP 79

14 USB SLUŽBY 80
14.1 Sdílení souborů 80
14.2 Tiskový server 81
14.3 Media server 82

14 3G/4G BACKUP 82

15 DYNAMIC DNS 83

16 UPNP 84

17 INTERFACE GROUPING 85

18 LAN BUNDLING 86

19 IP TUNEL 87
19.1 IPv6inIPv4 87
19.2 IPv4inIPv6 88

20 CERTIFIKÁT 90

20.1 Lokální certifikát 90

21 DIAGNOSTIKA 91

21.1 Diagnostika 91

21.2 Fault management 92

22 MANAGEMENT 93

22.1 Konfigurace 93

22.1.1 Záloha 94

22.1.2 Update 94

22.1.3 Výchozí nastavení 96

22.2 Aktualizace software 97

22.3 Restart 98

22.4 Kontrola přístupu - Hesla 99

22.5 Nastavení práv 99

22.6 Vzdálená správa 100

22.7 TR-069 Client 101

22.8 SNMP Agent 102

22.9 System log 102

22.10 Nastavení času 104

23 PROBLÉMY A JEJICH ŘEŠENÍ 105

23.1 Napájení, kabelové připojení, LED kontrolky 105

23.2 Přístup a přihlášení k zařízení 106

23.3 Přístup k internetu 107

1 ZÁKLADNÍ INFORMACE

1.1 Popis zařízení

VMG1312-B30B je router ADSL2+/VDSL2 se snadnou instalací. VMG1312-B30B (dále jen „zařízení ZyXEL“) je navíc kompletním bezpečnostním řešením s robustním firewallem a filtrováním dat.

Jednotlivá písmena v názvu přístroje mají tento význam:

- „VMG“ VDSL Media Gateway.
- „B“ označuje výrobce chipsetu Broadcomm.
- Modely, jejichž modelové číslo končí číslem „30“, pracují na digitálních linkách ISDN nebo T-ISDN.

Používejte pouze firmware určený pro dané zařízení ZyXEL (informace o typu zařízení jsou uvedeny na štítku na spodní straně zařízení).

Všechny ukázky dialogových oken v této příručce pochází od modelu VMG1312-B30B.

Plný seznam všech funkcí najdete v produktové specifikaci.

1.2 Správa zařízení

Ke správě zařízení lze použít jednu z těchto čtyř metod:

- Webové rozhraní. Metoda vhodná pro každodenní správu zařízení. K jejímu užití stačí podporovaný webový prohlížeč.
- Příkazový řádek (CLI). Metoda vhodná pro zkušené uživatele nebo při řešení problémů.
- FTP přístup je určen pro aktualizaci firmwaru nebo obnovu konfigurace.
- Protokol TR-069 umožňuje dálkovou konfiguraci zařízení.

1.3 Několik užitečných typů pro správu zařízení

Níže uvádíme několik tipů pro správu zařízení.

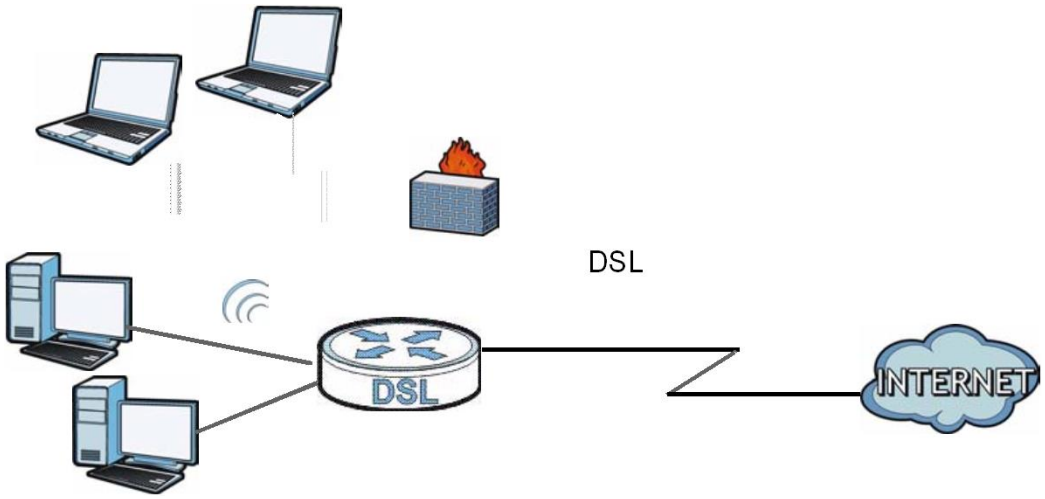
- Změňte výchozí heslo. Zvolte heslo, které nelze snadno uhodnout a které využívá kombinaci různých typů znaků (např. písmena a číslice).
- Heslo si zapište a uložte na bezpečném místě.

- Pravidelně zálohujte konfiguraci zařízení a seznamte se s postupem pro její obnovu. Obnova konfigurace je užitečná, když zařízení začne z nějakého důvodu pracovat nespolehlivě. V této situaci můžete buď provést resetování všech hodnot na tovární nastavení, nebo obnovit předchozí konfiguraci. Druhá možnost je často výhodnější, protože nemusíte zařízení znovu celé nastavovat.

1.4 Typická instalace zařízení

1.4.1 Připojení k internetu

Zařízení umožňuje sdílený přístup k internetu. Na obrázku níže je zařízení ZyXEL připojeno k telefonní lince prostřednictvím portu DSL (nebo je připojeno ke splitteru, který je připojen k telefonní lince). Počítače jsou připojeny k portům LAN zařízení, případně jsou připojeny bezdrátově.



Přístup k internetu bude bezpečnější, když využijete firewall a filtrování dat – funkce, které jsou součástí zařízení. Když je firewall aktivní, všechna příchozí data jsou blokována, pokud jste je předtím sami nevyžádali. Tím je zajištěna větší bezpečnost připojení k internetu.

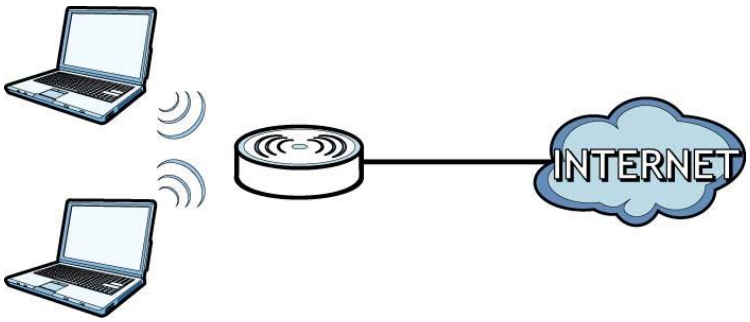
Filtrování dat slouží k blokování přístupu k určitým serverům a webovým stránkám a také k některým aplikacím, jako např. MSN nebo Yahoo Messenger. Lze také nastavit pravidla založená na IP/MAC adresách a to jak pro příchozí, tak odchozí provoz.

Technologie QoS optimalizuje provoz bezdrátové sítě, protože dokáže přidělit vhodnou prioritu různým zařízením a typům dat. Například je možné nastavit vyšší prioritu pro internetové telefonování (VoIP) nebo data řídicích pracovníků.

1.5 Bezdrátový přístup

Zařízení ZyXEL pracuje jako přístupový bod (AP) pro bezdrátové klienty (např. počítač, PDA nebo iPad).

Bezdrátovou síť je možné nastavit přes webové rozhraní nebo prostřednictvím tlačítka WPS.



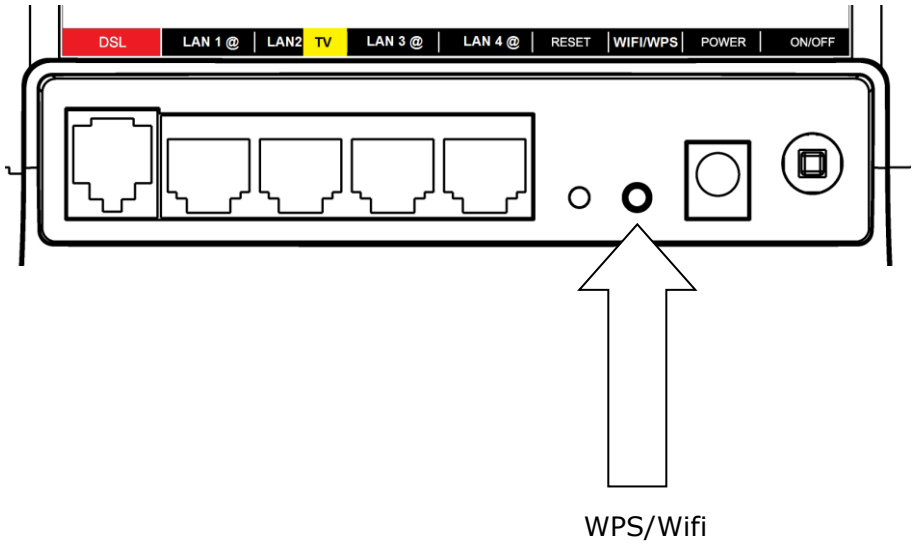
1.5.1 Tlačítko WPS/WLAN

Ve výchozím nastavení je bezdrátová síť vypnutá. Zapnete ji tlačítkem **WPS/WLAN** na zadním panelu zařízení. Bezdrátová síť je aktivní, když LED kontrolka **WPS/WLAN** svítí zeleně.

Tlačítko **WPS/WLAN** rovněž slouží k snadnému nastavení přihlašovacích údajů mezi zařízením a bezdrátovým klientem (který musí podporovat technologii WPS).

Jak připojit bezdrátového klienta s využitím WPS:

1. Kontrolka **POWER** musí trvale svítit a neblikat.
2. Stiskněte tlačítko **WPS/WLAN** na pět sekund.



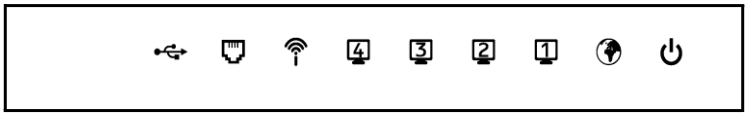
WPS/Wifi

3 Stiskněte tlačítko WPS na bezdrátovém klientu (klient musí být v dosahu signálu). V okamžiku, kdy tlačítko stisknete, musí svítit LED kontrolka **WPS/WLAN** na zařízení ZyXEL.

4 Úspěšné nastavení je potvrzeno zelenou LED kontrolkou **WPS/WLAN**.

1.6 LED kontrolky

Na obrázku níže naleznete popis LED kontrolek.



Tabulka 1 Popis LED kontrolek

LED	Barva	Stav	Popis
POWER	Zelená	Svítí	Zařízení je zapnuté a připravené k provozu.
		Bliká	Probíhá automatický provozní test při spuštění.
	Červená	Svítí	Automatický provozní test byl neúspěšný nebo došlo k jiné chybě.
		Nesvítí	Zařízení je vypnuté.
LAN1-4	Zelená	Svítí	K portu LAN je připojen počítač nebo jiné síťové zařízení.
		Bliká	Probíhá příjem nebo odesílání dat na síti LAN.
		Nesvítí	Zařízení nezjistilo připojení Ethernet k síti LAN.
WPS/WLAN	Zelená	Svítí	Bezdrátová síť je aktivní.
		Bliká	Zařízení komunikuje s bezdrátovými klienty.
	Oranžová	Bliká	Probíhá proces připojení prostřednictvím WPS.
		Nesvítí	Bezdrátová síť je vypnutá.

LED	Barva	Stav	Popis
DSL	Zelená	Svítí	Linka DSL je připojena.
		Bliká	Zařízení provádí inicializaci linky DSL.
		Nesvítí	Linka DSL není připojena.
INTERNET	Zelená	Svítí	Zařízení zjistilo IP připojení, ale neprobíhá přenos dat. Zařízení má přidělenou WAN IP adresu (statickou nebo přidělenou serverem DHCP), inicializační fáze PPP je dokončena, DSL linka je připojena.
		Bliká	Probíhá přenos dat.
	Červená	Svítí	Připojení PPP selhalo. Mezi možné příčiny patří nedostupný server DHCP, PPPoE neodpovídá nebo nebyla provedena autentizace.
		Nesvítí	Zařízení nezjistil IP připojení.
USB	Zelená	Svítí	USB Zařízení je připojené a funkční. (v případě 3G/4G modemu je sestaveno připojení do sítě)
		Bliká	Probíhá přenos dat (v případě 3G/4G modemu se sestavuje spojení).

1.7 Tlačítko RESET

Tlačítko RESET na zadní straně zařízení slouží k nastavení všech konfiguračních parametrů zařízení na tovární hodnoty. Tlačítko užijte např. v případě, když zapomenete přístupové heslo a nemůžete se přihlásit k webovému rozhraní. Po resetování na tovární nastavení bude přihlašovací heslo opět „admin“.

1.7.1 Reset modemu pomocí tlačítka

1. Kontrolka **POWER** musí trvale svítit a neblikat.
2. Stiskněte tlačítko **RESET** a držte ho deset sekund (dokud kontrolka **POWER** nezačne blikat). Proběhne nastavení parametrů na tovární hodnoty a zařízení se znovu spustí.

2 WEBOVÉ ROZHRANÍ

2.1 Základní informace

Webové rozhraní pracuje na bázi HTML a představuje snadný způsob, jak konfigurovat a spravovat zařízení. Doporučené rozlišení obrazovky pro webové rozhraní je 1024 x 768 pixelů. Podporované prohlížeče jsou Internet Explorer 6.0 a vyšší, Netscape Navigator, Mozilla Firefox a Google Chrome.

Aby webové rozhraní pracovalo správně, je třeba v prohlížeči provést toto nastavení:

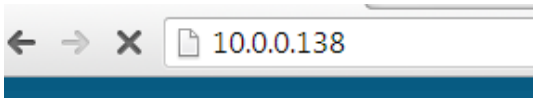
- Povolit vyskakovací okna.
- Povolit JavaScript.
- Povolit Javu.

2.1.1 Jak se přihlásit k webovému rozhraní

1 Zařízení musí být správně připojeno (viz příručka k rychlé instalaci).

2 Otevřete webový prohlížeč.

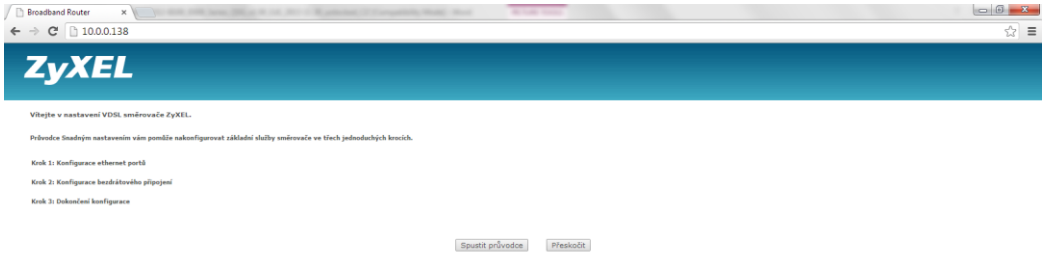
3 Do adresového pruhu zadejte adresu „10.0.0.138“.



4 Objeví se dialogová obrazovka k vložení hesla. Zadejte administrátorské heslo (výchozí heslo je admin) a klikněte na **Login** (přihlásit). Když kliknete na tlačítko **Cancel** (zrušit), vrátíte se zpět na výchozí uživatelské heslo. Pokud jste heslo změnili, zadejte nové heslo a klikněte na **Login** (přihlásit).



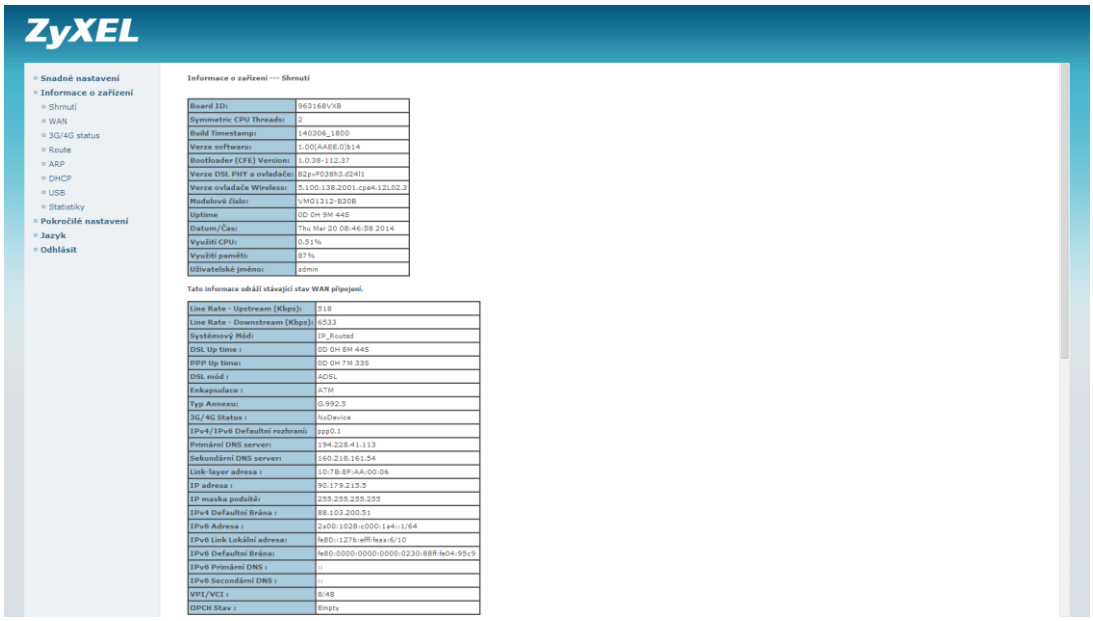
5 Objeví se průvodce nastavením zařízení. Této kapitole se věnuje příručka k rychlé instalaci. Klikněte tedy na tlačítko **Přeskočit** a objeví se **Stavová obrazovka,** kde zvolte možnost **Pokročilé Nastavení**.



Poznámka:

Z bezpečnostních důvodů budete automaticky odhlášeni, pokud během pěti minut (výchozí nastavení) nezaznamená webový konfigurátor žádnou aktivitu. Pokud se to stane, můžete se znovu přihlásit.

2.2 Hlavní obrazovka



Hlavní obrazovka se dělí do čtyř hlavních částí:

- titulkový pruh (nahoře)
- navigační panel (levý panel s volbami)
- hlavní okno (hlavní okno, kde se zobrazí zvolená volba)
- stavový pruh (informuje o stavu stránky GUI, např. „připraven“ „načítám“ atd.)

2.2.1 Titulkový pruh

V titulkovém pruhu naleznete logo výrobce.

2.2.2 Navigační panel

V navigačním panelu můžete vybírat jednotlivá okna s konfiguračními parametry. V tabulce uvádíme přehled všech konfiguračních obrazovek.

Položka	Karta	Funkce
Snadné nastavení		Spustí průvodce snadným nastavením, pro bližší informace čtěte „příručku k rychlé instalaci“
Informace o zařízení		Obecné informace o zařízení a stavu sítě. Na obrazovce naleznete přístup k informacím o WAN, 3G/4G, Routě, ARP, DHCP, USB a statistiky LAN, WAN, xTM a xDSL
Jazyk		Nastavení jazyka GUI. K dispozici je Angličtina a Čeština
Odhlásit		Odhlášení z webového rozhraní
Pokročilé Nastavení		
Layer 2 rozhraní	ATM Interface	Nastavení rozhraní pro ADSL/2/2+ WAN
	PTM Interface	Nastavení rozhraní pro VDSL2
	ETH Interface	Nastavení rozhraní pro Ethernet WAN
WAN služby	WAN služby	Konfigurace WAN služeb a jejich parametrů na jednotlivých rozhraních
	WAN DNS	Konfigurace serverů DNS a jejich parametrů
Povolit Ipv6		Povolit nebo zakázat použití protokolu Ipv6
Bezdrátové připojení	Základní	Základní nastavení sítě, název SSID, základní parametry, skrytí SSID
	Zabezpečení	Na této obrazovce lze nastavit parametry zabezpečení jako je heslo, typ šifry apod.
	MAC Filtr	Zde nastavíte seznam povolených nebo zakázaných MAC adres pro danou síť
	Pokročilé	Pokročilé nastavení bezdrátové sítě jako je šířka pásma, Wifi kanál nebo úroveň vyzařování AP
	Station info	Seznam připojených klientských zařízení
LAN		Nastavení sítě LAN, IP adresace, DHCP
	Ipv6 autoconfig	Nastavení parametrů pro autokonfigurace Ipv6. Údaje získáte od poskytovatele Internetu
NAT	Virtuální servery	Virtuální Server umožňuje adresovat příchozí data z WAN strany (identifikované protokolem a číslem externího portu) na Interní server s privátní IP adresou na LAN straně.
	DMZ Host	Nastavení parametrů DMZ host
	SIP ALG	Zapnutí / vypnutí aplikační brány SIP ALG

Položka	Karta	Funkce
Firewall	Obecné	Zapnutí / vypnutí firewallu a SPI (stavová kontrola paketů).
	Pravidla	Na obrazovce můžete nastavit pravidla pro filtrování provozu na základě IP adresy nebo portu služby.
	DoS	Nastavení ochrany před útokem Denial of Service
	MAC Filtr	Konfigurace pravidel založených na filtrování příchozích a odchozích dat pomocí MAC adres (pouze pro připojení v režimu Bridže).
Rodičovská kontrola	Časová omezení	Nastavení časových restrikcí pro omezení přístupu k internetu
	URL Filtr	Nastavení povolených nebo zakázaných stránek
Static Ipv4 neighbor		Nastavení položky statický Ipv4 neighbor
	Static Ipv6 neighbor	Nastavení položky statický Ipv6 neighbor
Quality of Service		Zapnutí funkcí QoS pro nastavení priority určitých typů dat a nastavení výchozí hodnoty.
	QoS Queue	Konfigurace jednotlivých front QoS
	QoS Classification	Konfigurace klasifikačních pravidel QoS
Routing	Výchozí brána	Volba použité výchozí brány
	Static route	Nastavení statické routy
	Policy routing	Nastavení routovacích pravidel
	RIP	Nastavení RIP verze k jednotlivých rozhraním
USB Služby	Sdílení souborů	Konfigurace sdílení souborů z připojené USB paměti
	Tiskový server	Nastavení parametrů tiskového serveru
	Media server	Nastavení Media serveru, standardu DLNA, pro sdílení dat z připojené USB paměti
3G/4G backup		Aktivace a nastavení záložního připojení přes mobilní sítě
Dynamic DNS		Nastavení DDNS pro usnadnění přístupu k zařízení z jiného místa na internetu
UPnP		Zapnutí a vypnutí UPnP.
Interface grouping		Seskupování umožňuje začlenění jednoho a více LAN portů do jedné skupiny s jedním a více WAN rozhraními
LAN bundling		Nastavení variant portů s/bez služby IPTv

Položka	Karta	Funkce
IP Tunel	IPv6inIPv4	Nastavení IP Tunelu
	IPv4inIPv6	Nastavení IP Tunelů
Certifikát	Lokální	Na této stránce můžete Přidat, Zobrazit nebo Odstranit lokální certifikáty. Lokální certifikáty jsou používány peery k ověření vaší identity.
Diagnostika	Diagnostika	Obecná diagnostika zařízení: WAN, LAN, Wifi, přistup k Internetu
	Fault management	Nastavení pravidel fault managementu
Management	Konfigurace	Zde můžete zálohovat a obnovit konfigurace, popř. Vrátit konfiguraci do továrního nastavení
	Aktualizace software	Nahrání nového/jiného firmware zařízení
	Restart	Obrazovka s tlačítkem pro restart zařízení
	Kontrola přístupu	Pod položkou „hesla“ lze upravovat a spravovat hesla a uživatele zařízení
	Nastavení práv	Zde je možné upravovat k jednotlivým uživatelům jejich přístupová práva
	Vzdálená správa	Konfigurace a nastavení atributů vzdálené správy zařízení
	TR-069 Klient	Aktivace/deaktivace správy zařízení přes TR-069
	SNMP Agent	Simple Network Management Protocol (SNMP) umožňuje provádět konfigurace, sběr dat a diagnostiku pro toto zařízení
	System log	Tato stránka vám umožní zobrazení Systémových logů a konfiguraci jejich konfiguraci
	Nastavení Času	Nastavení a konfigurace NTP serverů, změny letního/zimního času

2.2.3 Hlavní okno

V hlavním okně jsou uvedeny různé provozní údaje a nacházejí se zde konfigurační políčka.

Ihned po přihlášení se objeví stavová obrazovka. Více informací o stavové obrazovka naleznete v kapitole „Stavová obrazovka“.

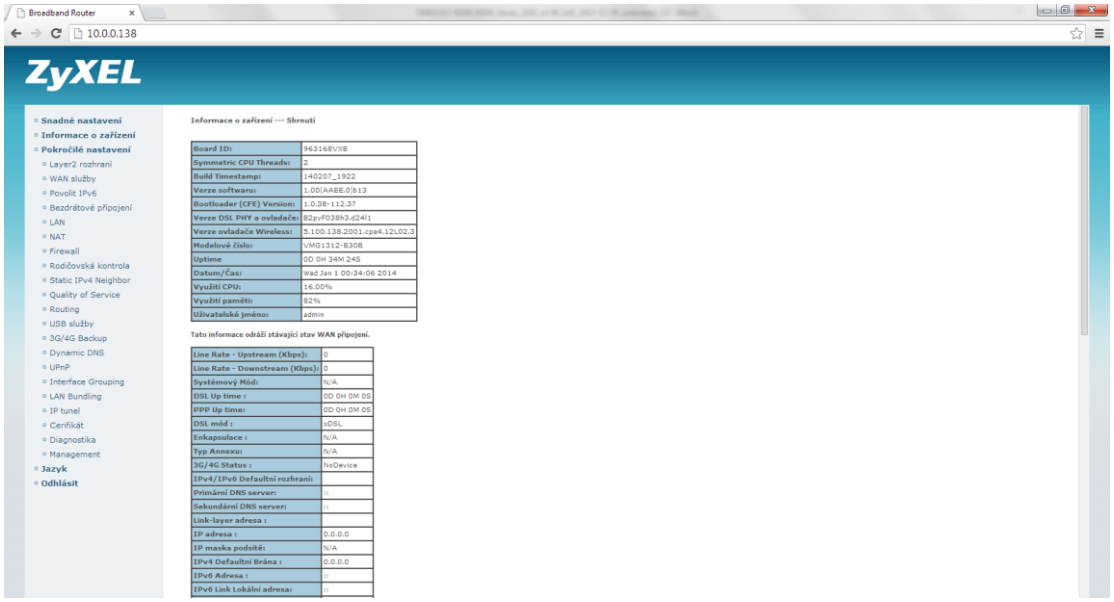
3 STAVOVÁ OBRAZOVKA

3.1 Základní informace

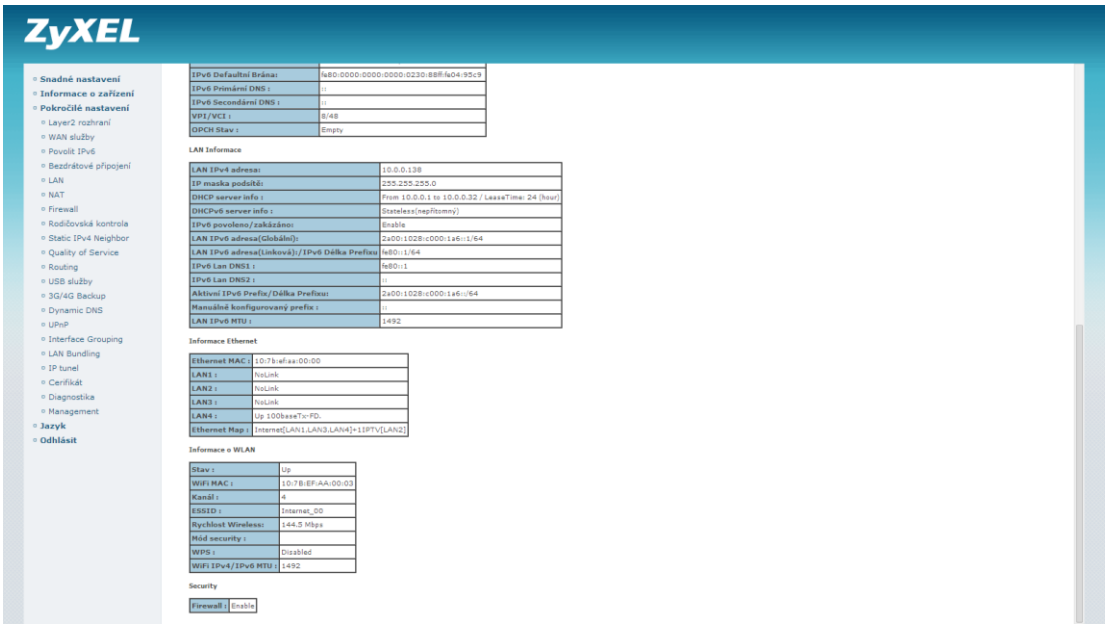
Na stavové obrazovce zjistíte aktuální stav zařízení, stav systému a stav rozhraní zařízení (LAN a WAN). Na stavové obrazovce jsou uvedeny také všechny údaje týkající se DHCP a statistické údaje o provozu zařízení.

3.2 Informace o zařízení

Stavovou obrazovku otevřete kliknutím na odkaz **Informace o zařízení**.



Stavová obrazovka 2. část



V tabulce níže naleznete popis k jednotlivým položkám nabídky Informace o zařízení.

Položka	**Popis**
Shrnutí	Komplexní přehled stavu zařízení a všech rozhraní
WAN	Informace o stavu WAN rozhraní
3G/4G status	Stav záložního mobilního připojení
Route	Přehled a nastavení routovacích pravidel
ARP	Kompletní ARP tabulka klientů
DHCP	Seznam klientů DHCP serveru a jejich stav
USB	Stav a typ připojených USB pamětí
Statistiky	Statistiky LAN, WAN, xTM a xDSL

4 TYPOVÉ PŘÍKLADY

4.1 Základní informace

V této kapitole názorně popisujeme některé funkce zařízení.

4.2 Nastavení bezpečné bezdrátové sítě

Předpokládejme, že Tomáš chce nastavit bezdrátovou síť tak, aby se ze svého notebooku mohl připojit k internetu. V tomto příkladu pracuje zařízení ZyXEL jako přístupový bod (AP) a notebook jako bezdrátový klient. Bezdrátový klient získá přístup k internetu přes AP.



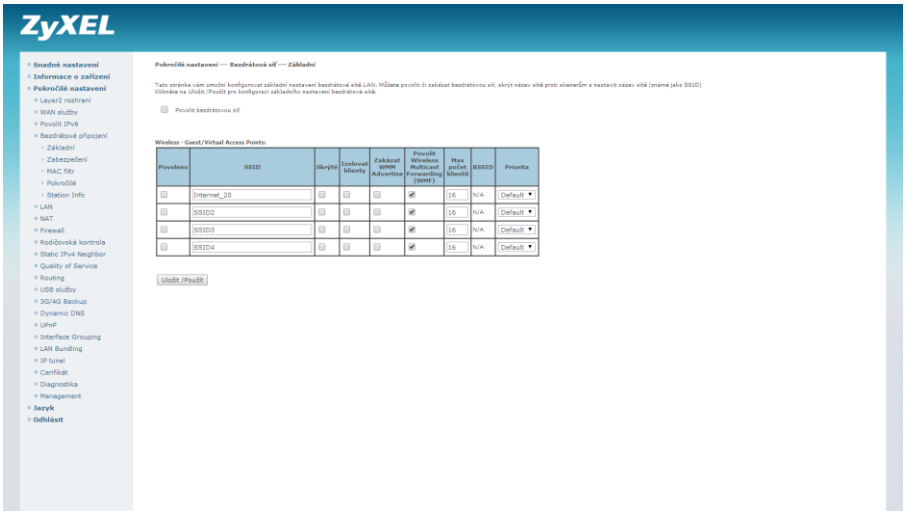
Tomáš musí konfigurovat bezdrátovou síť na rozhraní zařízení ZyXEL. Vlastní nastavení sítě může provést prostřednictvím WPS (viz kapitola „Nastavení prostřednictvím WPS“) nebo manuálně (viz kapitola „Nastavení bez WPS“).

4.2.1 Konfigurace bezdrátové sítě

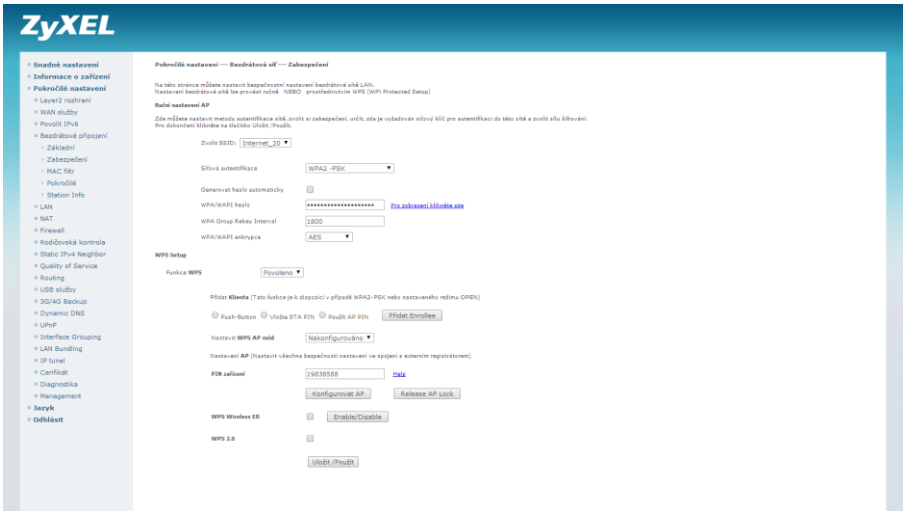
V níže uvedeném příkladu užíváme tato nastavení:

SSID (jméno sítě)	Example
Security Mode (režim zabezpečení)	WPA-PSK
Pre-Shared Key (předem sdílený klíč)	DoNotStealMyWirelessNetwork
802.11 Mode (režim 802.11)	802.11b+g+n

1 V levém menu vybereme **Pokročilé nastavení > Bezdrátové připojení** a otevřeme základní konfigurační stránku. Povolíme bezdrátovou síť a nastavíme SSID na „Example“ . Nastavení uložíme kliknutím na **Uložit/Použít**.



2 V levém menu zvolíme nabídku **Zabezpečení** . zkontrolujeme zda název sítě (Zvolit SSID) odpovídá zadanému „Example“, vybereme síťovou autentifikaci WPA-PSK a zadáme WPA/WAPI heslo „DoNotStealMyWirelessNetwork“. Můžeme nastavit funkci WPS, podle toho zda budeme nebo nebudeme používat funkci snadné konfigurace klientu.



Tomáš může nyní nastavit připojení mezi svým notebookem a zařízením ZyXEL prostřednictvím funkce WPS (viz kapitola „Nastavení prostřednictvím WPS“). Nebo se může k zařízení ZyXEL připojit pomocí ruční konfigurace svého WiFi klienta (viz kapitola „Nastavení bez WPS“).

4.2.2 Nastavení prostřednictvím WPS

V této kapitole popisujeme, jak nastavit bezdrátovou síť prostřednictvím funkce WPS. V příkladu užijeme adaptér ZyXEL NWD210N jako bezdrátového klienta.

Poznámka:

Bezdrátový klient musí podporovat WPS (např. USB adaptér s WPS nebo karta PCMCIA)

Existují dvě metody, jak přidat zařízení pomocí WPS:

- **Konfigurace pomocí tlačítka (PBC):** stačí stisknout tlačítko. Tato metoda je snazší než druhá metoda.
- **Konfigurace pomocí PIN:** Zařízení ZyXEL má své číslo PIN (identifikační kód). Tento PIN kód je třeba zadat na bezdrátovém klientovi. Tuto funkci ale nepodporují všichni WiFi klienti. Většina používá opačný postup konfigurace, PIN uvedený ve WiFi klientovi je potřeba zadat na konfigurační stránce přístupového bodu (AP).

Konfigurace pomocí tlačítka (PBC)

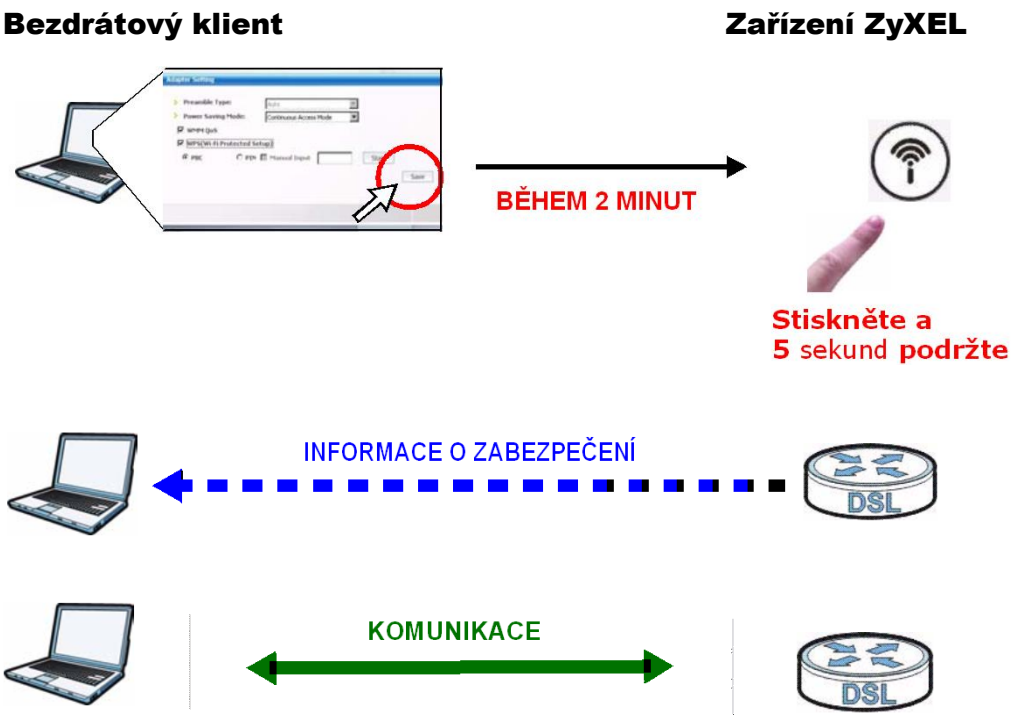
1. Zapněte zařízení ZyXEL a umístěte notebook s bezdrátovým adaptérem v dosahu signálu.
2. Nezapomeňte nainstalovat ovladač bezdrátového klienta v notebooku.
3. V utilitě bezdrátového klienta otevřete stránku s nastavením WPS. Zapněte WPS a klikněte na tlačítko WPS (tlačítko může být fyzické (na zařízení) nebo aplikační (v konfigurační utilitě klienta)).
4. Stiskněte a držte tlačítko **WPS** na zadním panelu zařízení ZyXEL po dobu delší než 5 sekund.

Poznámka: Zařízení ZyXEL má fyzické tlačítko na zadním panelu a také softwarové tlačítko WPS v konfigurační utilitě. Obě tlačítka mají tutéž funkci, můžete užít libovolné z obou tlačítek.

Poznámka: Nezáleží na tom, jestli stisknete jako první tlačítko na zařízení ZyXEL nebo v bezdrátovém klientovi. Musíte však obě tlačítka stisknout v rozmezí 2 minut.

Zařízení ZyXEL odešle bezdrátovému klientu platné konfigurační údaje. Komunikace může trvat až 2 minuty. Po skončení nastavení může bezdrátový klient bezpečně komunikovat se zařízením ZyXEL.

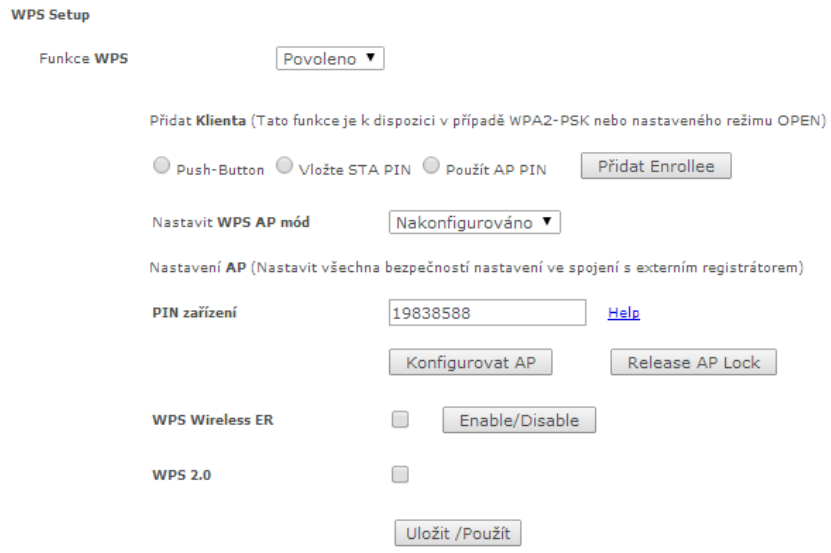
Celý postup je vyznačen na obrázku níže.



Konfigurace pomocí PIN

V této metodě je potřeba přístup k webovému konfigurátoru zařízení ZyXEL.

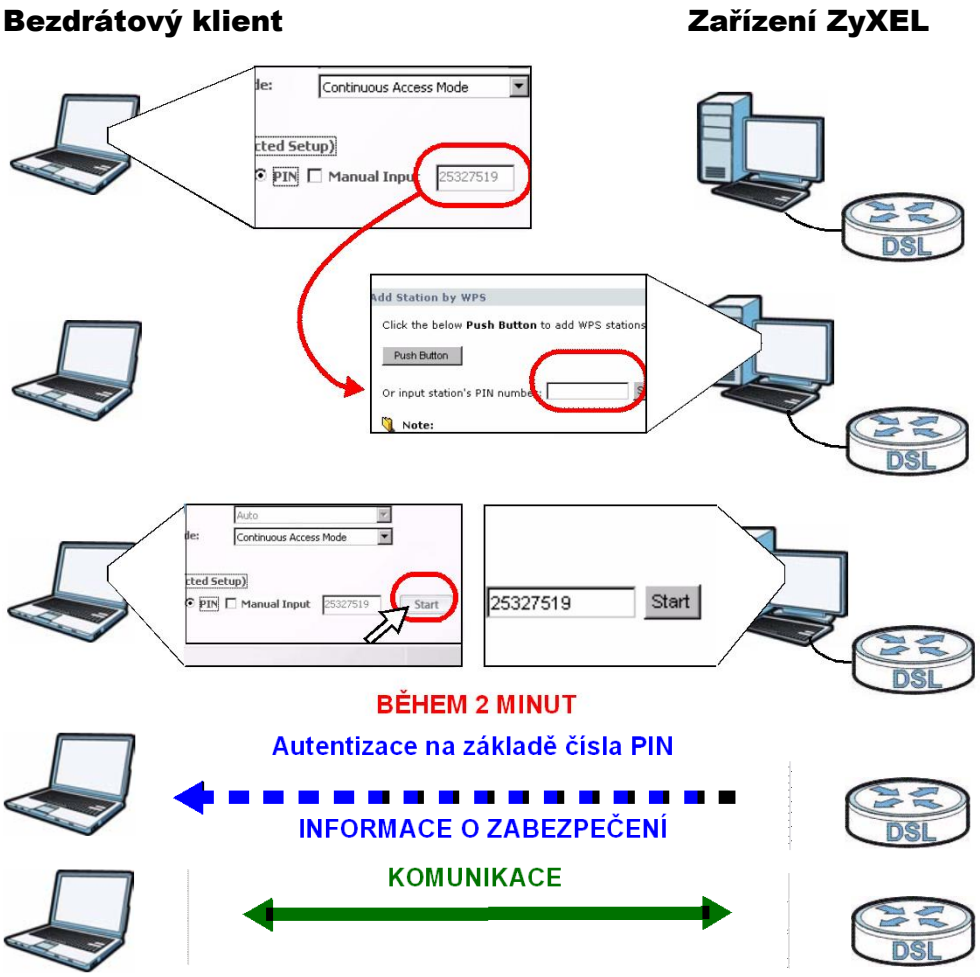
1. Spusťte konfigurační utilitu bezdrátového klienta. Otevřete kartu s nastavením WPS a zvolte metodu PIN. Klient vygeneruje PIN, který je potřeba zadat do konfigurační stránky ZyXEL.
2. Na obrazovce **Bezdrátová síť > Zabezpečení** zaškrtněte položku **WPS Wireless ER** a stiskněte tlačítko **Enable/Disable**. Vyberte položku **Vložte STA PIN**.a do odkrytého textového pole zadejte PIN vygenerovaný klientem.



3 Klikněte na tlačítko **Start** (nebo na tlačítko vedle políčka PIN) v utilitě bezdrátového klienta. Ve webovém konfigurátoru zařízení ZyXEL stiskněte tlačítko Přidat Enrollee . Obě tlačítka stiskněte v rozmezí 2 minut.

Zařízení ZyXEL odešle bezdrátovému klientu platné konfigurační údaje. Komunikace může trvat až 2 minuty. Po skončení nastavení může bezdrátový klient bezpečně komunikovat se zařízením ZyXEL.

Celý postup je vyznačen na obrázku níže.



4.2.3 Nastavení bez WPS

V utilitě bezdrátového adaptéru, která je instalována v notebooku, vyhledejte síť (SSID) s názvem „Example“ (to je jméno, které užíváme v našem příkladu). Zadejte předem sdílený klíč (Pre-shared key) „DoNotStealMyWirelessNetwork“. Notebook se připojí k zařízení ZyXEL.

Poznámka:

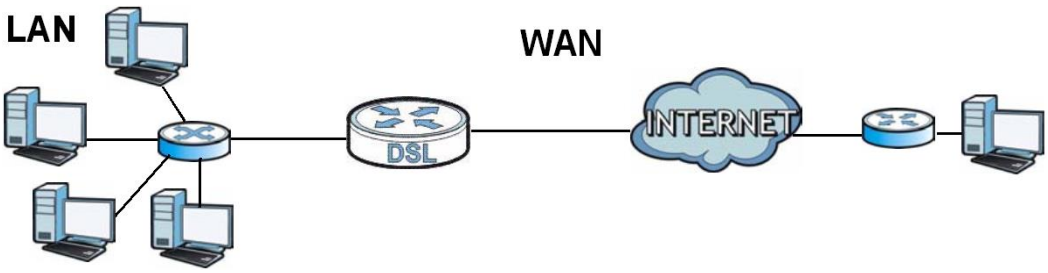
Zařízení ZyXEL podporuje standardy IEEE 802.11b/g/n. Notebook, případně bezdrátový klient, musí podporovat alespoň jeden z těchto standardů.

5 NASTAVENÍ SÍTĚ WAN

5.1 Základní informace

V této kapitole popisujeme, jak konfigurovat síť WAN a nastavit přístup k internetu na obrazovkách **Layer2 rozhraní a WAN služby**.

Připojení typu WAN (Wide Area Network) je připojení k vnější síti nebo k internetu. Propojuje tedy lokální síť (LAN) s jinými sítěmi, což je nezbytný předpoklad k tomu, aby mohly vzdálené počítače spolu komunikovat.



5.1.1 Co je třeba vědět o síti WAN

Metoda zapouzdření

Zapouzdření je mechanismus, jak zahrnout data z protokolu horní vrstvy do protokolu dolní vrstvy. Abyste se mohli připojit k internetu, musíte užít stejnou metodu zapouzdření, jakou užívá poskytovatel internetového připojení (ISP). Pokud ISP poskytuje připojení k internetu přes PPPoE (PPP over Ethernet) nebo PPPoA, musí vám sdělit také uživatelské jméno a heslo (a jméno služby) pro účely autentizace.

WAN IP adresa

WAN IP adresa je IP adresa zařízení ZyXEL na síti WAN. Přes tuto adresu komunikuje zařízení ZyXEL s vnějším světem. WAN IP adresa může být statická (pevná), nebo ji může ISP přidělovat dynamicky při každém připojení k internetu (pak je typicky po každé jiná).

Jestliže vám ISP přidělil statickou WAN IP adresu, měl by vám také přidělit masku podsítě a DNS server (a také IP adresu brány, pokud užíváte metodu zapouzdření ENET ENCAP nebo Ethernet).

Multicast

Tradičně se IP pakety přenášejí jedním ze dvou způsobů: unicast (1 odesílatel – 1 příjemce) a broadcast (1 odesílatel – každé zařízení na síti). Multicast je způsob přenosu IP paketů, který leží mezi oběma tradičními přístupy – 1 odesílatel posílá pakety určité skupině počítačů na síti, tedy ne pouze jednomu, ale ani ne všem.

IGMP

IGMP (Internet Group Multicast Protocol) je protokol síťové vrstvy, která se užívá k určení příslušnosti do skupin pro multicasting – neužívá se k přenosu uživatelských dat. Existují tři verze IGMP: v1, v2 a v3. Verze v1 je nejstarší, ale stále se hojně užívá.

5.1.2 Než začnete

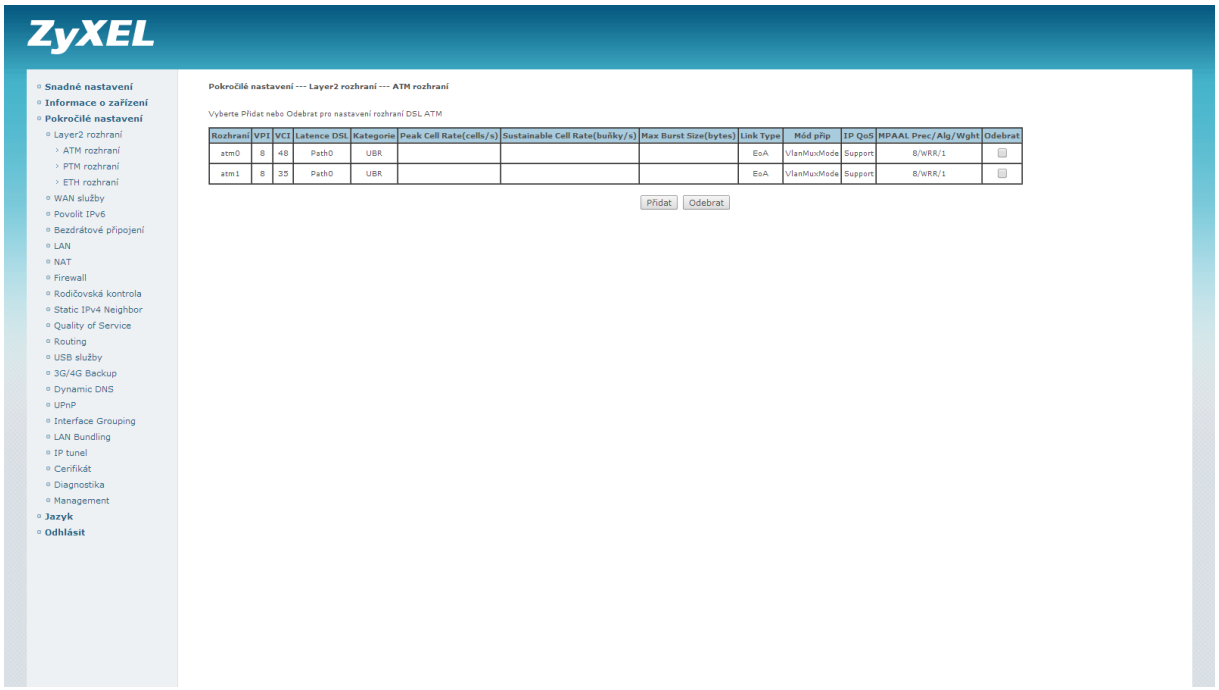
Ke konfiguraci připojení k internetu potřebujete znát metodu zapouzdření a způsob přidělení WAN IP adresy. Obě informace vám sdělí poskytovatel připojení (ISP).

5.2 Nastavení WAN rozhraní – L2 interface

L2 interface určuje fyzické rozhraní, kterým se chcete připojovat k Internetu. Například pro ADSL to je ATM rozhraní pro VDSL je to PTM rozhraní. Pokud neznáte přesné parametry pro vaše připojení ponechte nastavení tak jak jste jej dostali nastavené o poskytovatele Internetu a další úpravy WAN rozhraní provádějte na obrazovce WAN služby (kapitola 5.3).

5.2.1 Rozšířená konfigurace – přidání rozhraní L2

Na konfigurační obrazovce **Pokročilé nastavení** > **Layer 2 interface** můžete L2 rozhraní přidat nebo odebrat.



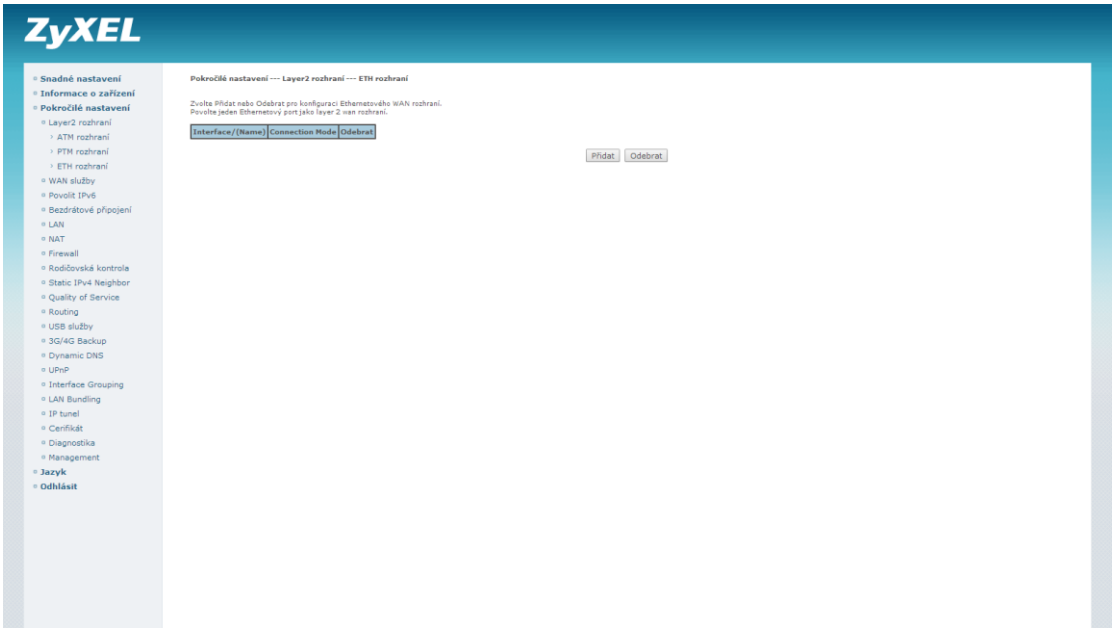
Jednotlivá rozhraní se následně přidávají nebo odebírají na:

ATM rozhraní – rozhraní standardu ADSL (resp. G.lite, G.DMT, ADSL2, ADSL2+)

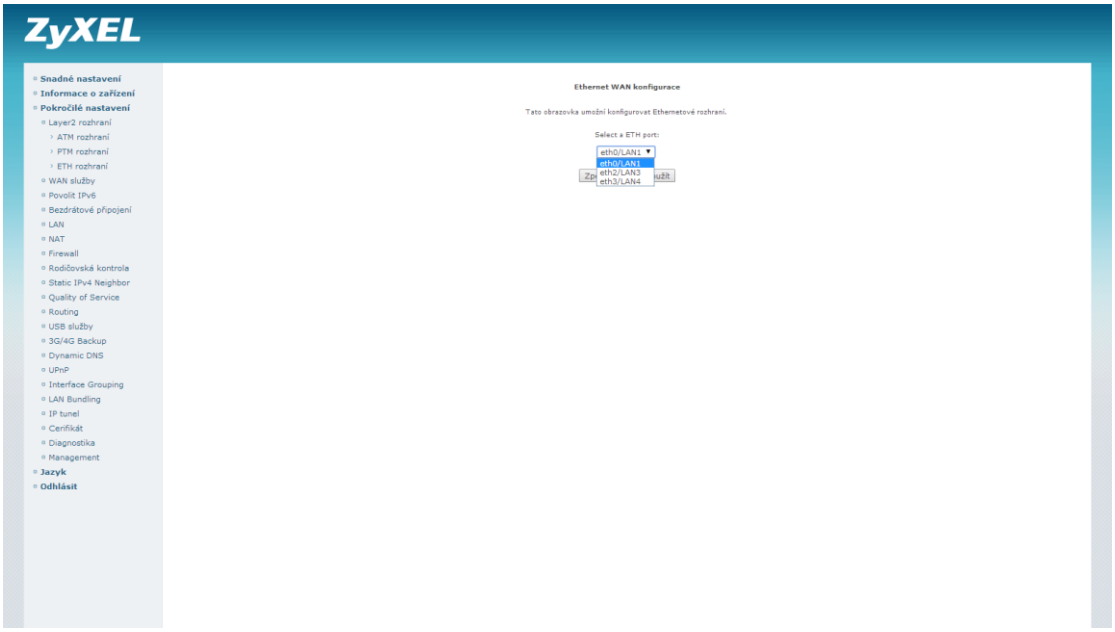
PTM rozhraní – rozhraní standardu VDSL2

ETH rozhraní – rozhraní Ethernet (jeden ehrernetový port zařízení lze nakonfigurovat jako Ethernet WAN)

Jako příklad je uvedeno přidání Ethernet rozhraní. V levém menu zvolte **ETH rozhraní** a klikněte na tlačítko **Přidat**

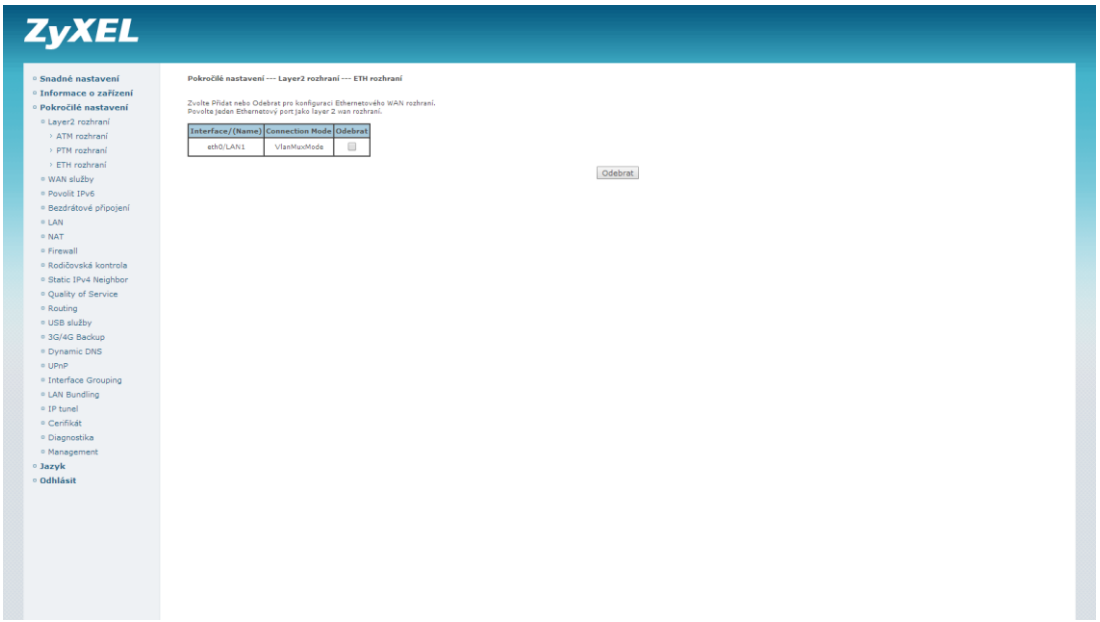


Vyberte z nabízených variant (vzhledem k ostatním nastavením doporučujeme používat pro WAN vždy Ethernet port č.1



Rozhraní je nastaveno.

Pokud budete chtít rozhraní L2 odebrat, zaškrtněte políčko “odebrat” v příslušném řádku a klikněte na tlačítko **Odebrat**



Následně můžete pro nové rozhraní nakonfigurovat službu. Nastavením WAN služby se zabývá následující kapitola.

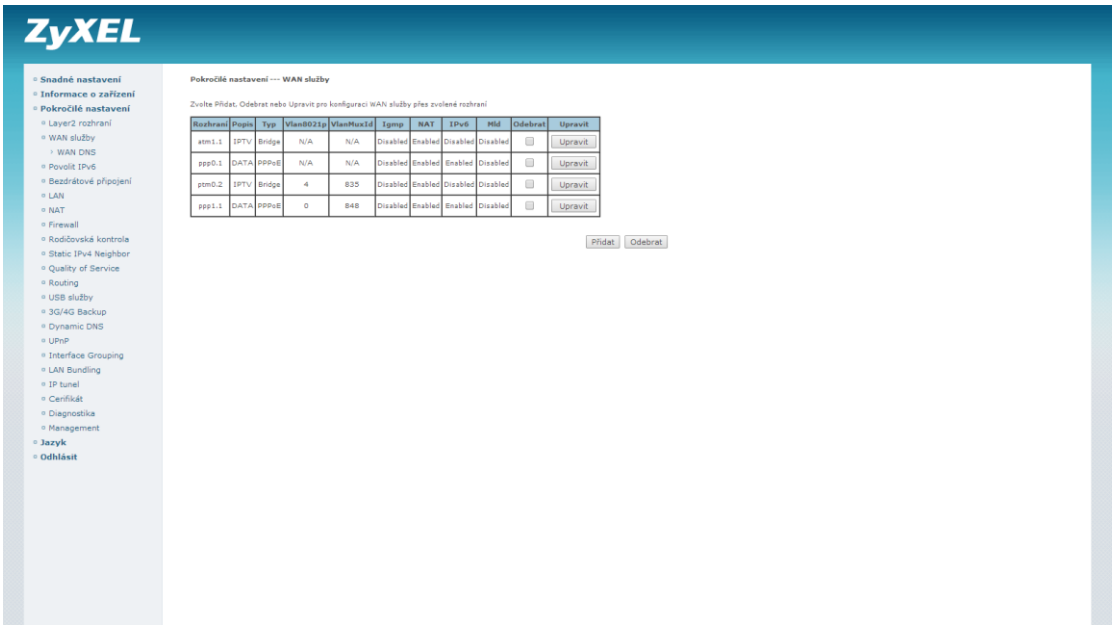
5.3 Nastavení WAN služby

Zařízení ZyXEL umožňuje konfigurovat několik různých připojení k internetu.

Na obrazovce **Pokročilé nastavení > WAN Služby** lze změnit nastavení připojení k síti WAN nebo přidat nové připojení. Podoba jednotlivých konfiguračních obrazovek se mění podle toho, jaké zapouzdření jste zvolili.

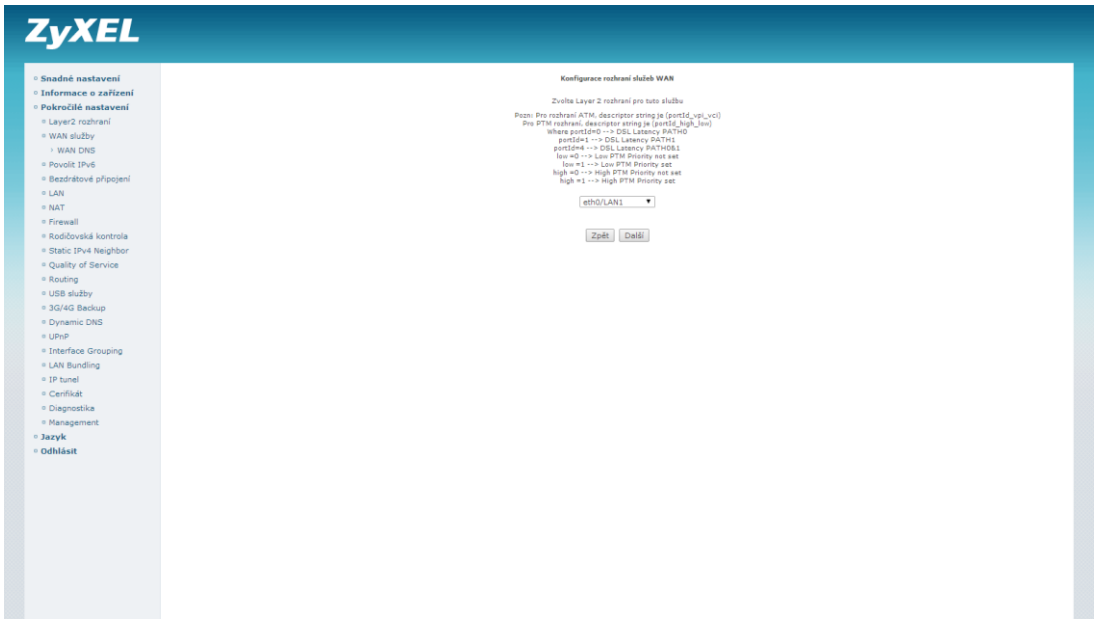
Na další konfigurační obrazovku se vždy dostanete kliknutím na tlačítko **Další**.

Na obrazovce jsou zobrazeny jako příklad již nakonfigurované služby.



V případě že chcete existující připojení odebrat označte zaškrtávací políčko u vybraného připojení a stiskněte tlačítko **Odebrat**.

Pokud chcete přidat nové připojení stiskněte tlačítko **Přidat**

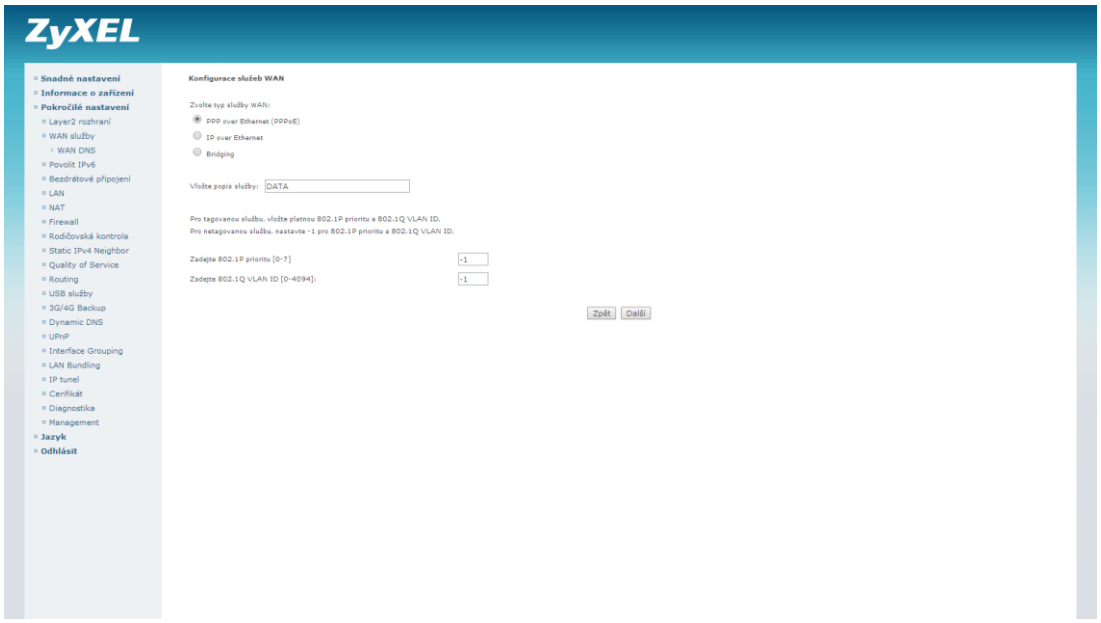


V otevřeném okně pak vyberte rozhraní L2, které chcete pro nového připojení k WAN síti využit.

Pokud budete provádět pouze úpravy v již nastaveném připojení, pomocí tlačítka **Upravit**, nebude vám volba rozhraní L2 nabídnuta.

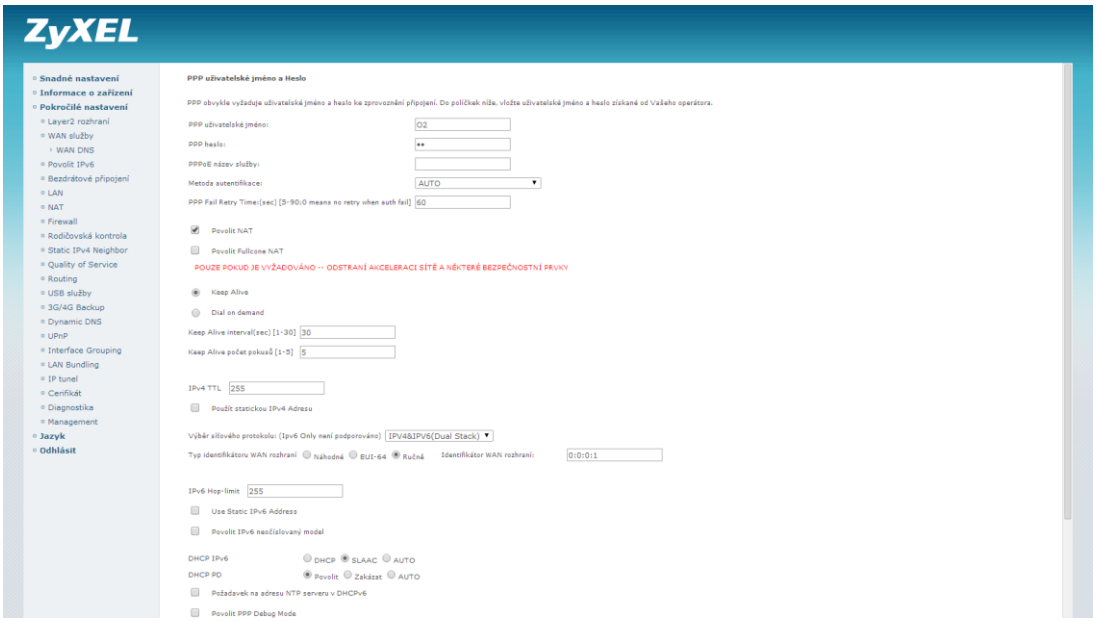
5.3.1 PPPoE

Zvolte PPPoE jako typ připojení, který chcete používat. Jedná-li se o službu využívajíci VLAN, je třeba nastavit VLAN ID a Prioritu v rámci VLAN



Položka	Popis
PPP over Ethernet (PPPoE)	Pro modem v režimu Routing s protokolem PPPoE.
IP over Ethernet	Pro modem v režimu Routing s protokolem Ethernet.
Bridging	Pro modem v režimu Bridge. Pokud je na lince PPPoE protokol provádí navázání spojení jiné zařízení.
Zadejte 802.1P prioritu [0-7]	Specifikujte prioritu provozu.
Zadejte 802.1Q VLAN ID [0-4094]	Specifikujte VLAN ID.

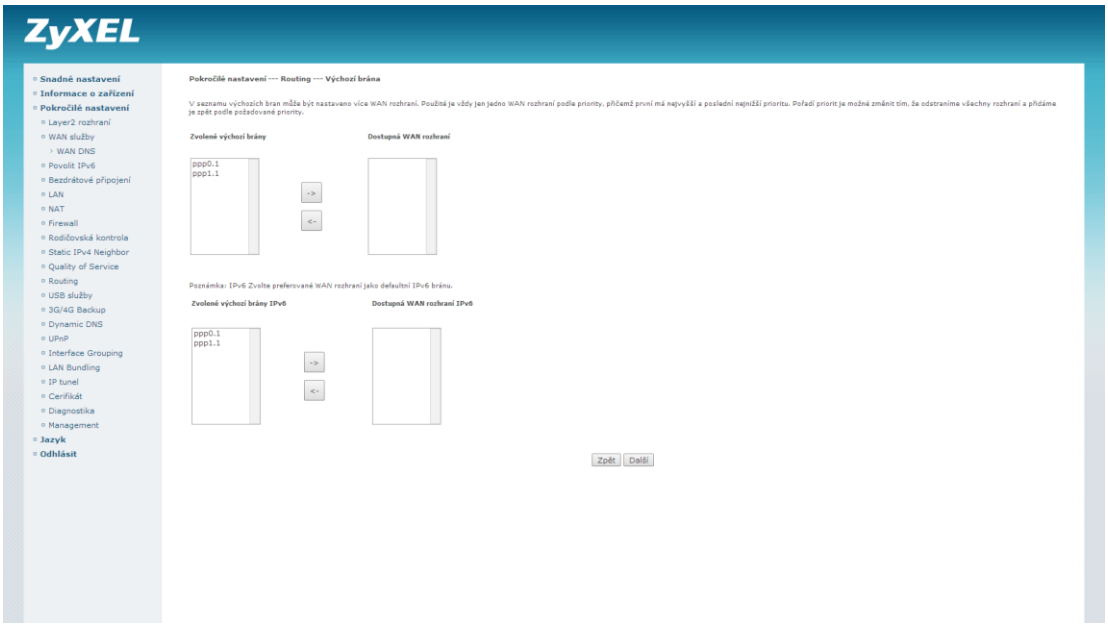
Následující údaje vyplňte dle informací získaných od Vašeho poskytovatele internetu.



Položka	Popis
PPP uživatelské jméno	Zadejte uživatelské jméno dle informací od ISP operátora.
PPP heslo	Zadejte uživatelské heslo dle informací od ISP operátora.
PPPoE název služby	Operátorem využívané označení skupiny konfiguračních procedur. Pokud není poskytovatelem určeno nezadávat.
Metoda autentifikace	Zde je možné vybrat autentifikační protokol.
PPP Fail Retry Time	Specifikuje interval pro odeslání PADI zprávy.
Povolit NAT	Umožnuje povolit službu NAT.
Povolit Fullcone NAT	Umožnuje aktivovat Fullcone NAT.
Keep Alive	PPPoE spojení bude neustále aktivní.
Dial on demand	PPPoE spojení bude ukončeno v případě, že nejsou přenášena žádná data.
Keep Alive interval	Nastavení Keep Alive intervalu.

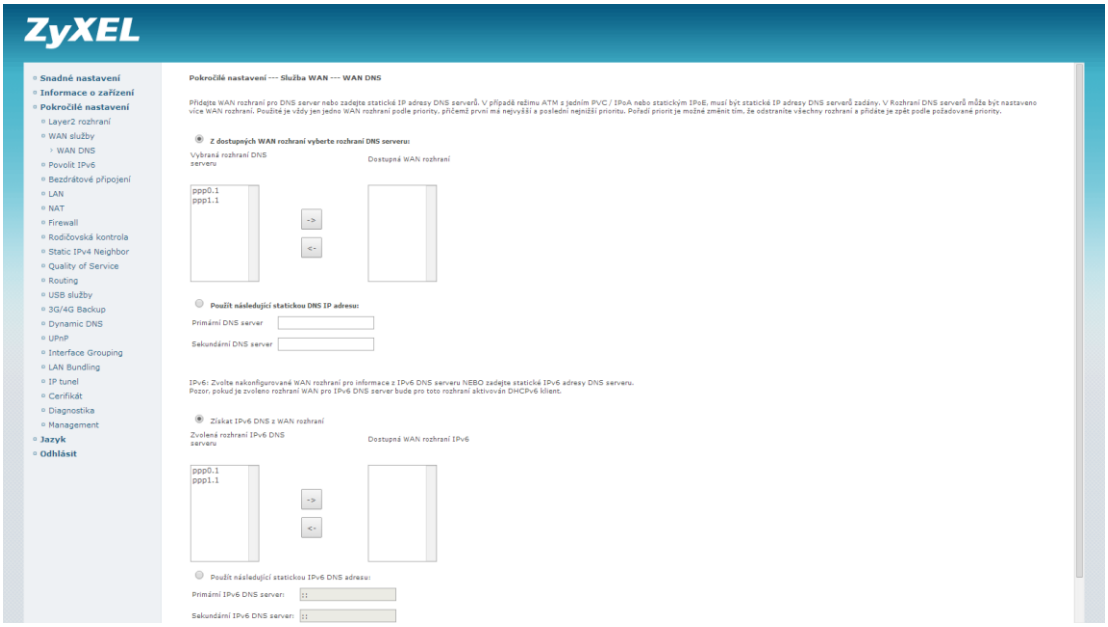
Keep Alive počet pokusů	Nastavení počtu Keep Alive pokusů.
IPv4 TTL	Nastavení maximálního počtu skoků.
Použít statickou IPv4 Adresu	Menu umožňuje nastavit statickou IPv4 adresu.
Výběr síťového protokolu	Menu umožňuje vybrat protokol IPv4 nebo Dual Stack.
Typ identifikátoru WAN	Menu umožňuje vybrat typ identifikátoru WAN rozhraní.
IPv6 Hop-limit	Nastavení maximálního počtu skoků.
Use Static IPv6 Address	Menu umožňuje nastavit statickou IPv6 adresu.
DHCP IPv6	Menu umožňuje zvolit nastavení IPv6 DHCP.
DHCP PD	Menu umožňuje zvolit nastavení DHCP Prefix Delagation.
Požadavek na adresu NTP serveru v DHCPv6	Menu umožňuje zvolit nastavení.
Povolit PPP Debug Mode	Povolit debug mode pro PPP protokol.
Bridgovat PPPoE Framy mezi porty WAN a lokálními	Povolit přenos PPPoE paketů mezi WAN a LAN rozhraním.
Povolit IGMP Multicast Proxy	Povolit IGMP Multicast Proxy.
Povolit MLD Multicast Proxy	Povolit MLD Multicast Proxy.

Zvolte rozhraní, které bude služba používat .Nepoužívaná rozhraní můžete přesunout do levého okna



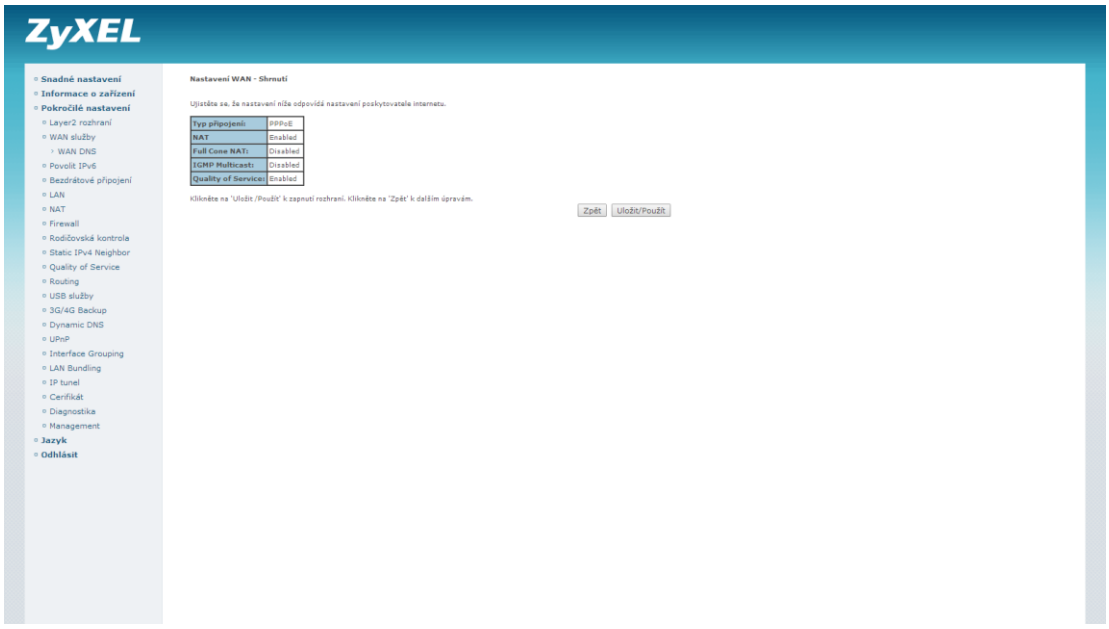
Položka	Popis
Zvolené výchozí brány	Seznam aktivních WAN rozhraní.
Dostupná WAN rozhraní	Seznam dostupných WAN rozhraní.
Zvolené výchozí brány IPv6	Seznam aktivních výchozích bran IPv6 rozhraní.
Dostupná WAN rozhraní IPv6	Seznam dostupných výchozích bran IPv6 rozhraní.

Stejným způsobem vyberte rozhraní pro funkce DNS.



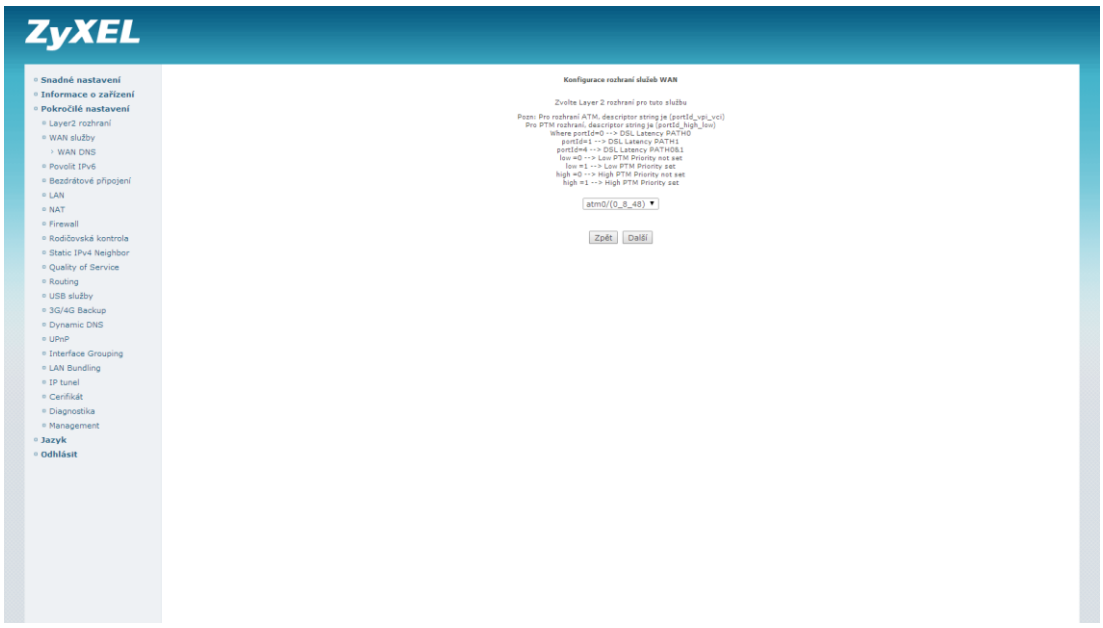
Položka	Popis
Z dostupných WAN rozhraní vyberte rozhraní DNS serveru	Menu umožnuje využít DNS servery přiřazené ISP operátorem.
Vybraná rozhraní DNS serveru	Seznam aktivních DNS rozhraní.
Dostupná WAN rozhraní	Seznam dostupných DNS rozhraní.
Použít následující statickou DNS IP adresu	Menu umožnuje využít statické nastavení DNS serverů.
Získat IPv6 DNS z WAN rozhraní	Menu umožnuje využít IPv6 DNS servery přiřazené ISP operátorem.
Zvolená rozhraní IPv6 DNS serveru	Seznam aktivních IPv6 DNS rozhraní.
Dostupná WAN rozhraní IPv6	Seznam dostupných IPv6 DNS rozhraní.
Použít následující statickou IPv6 DNS adresu	Menu umožnuje využít statické nastavení IPv6 DNS serverů.

Po dokončení Vám průvodce zobrazí sumář nastavených hodnot, pokud potřebujete některé údaje změnit, klikněte na tlačítko **Zpět,** je-li vše v pořádku, dokončíte nastavení kliknutím na tlačítko **Uložit/Použít.**

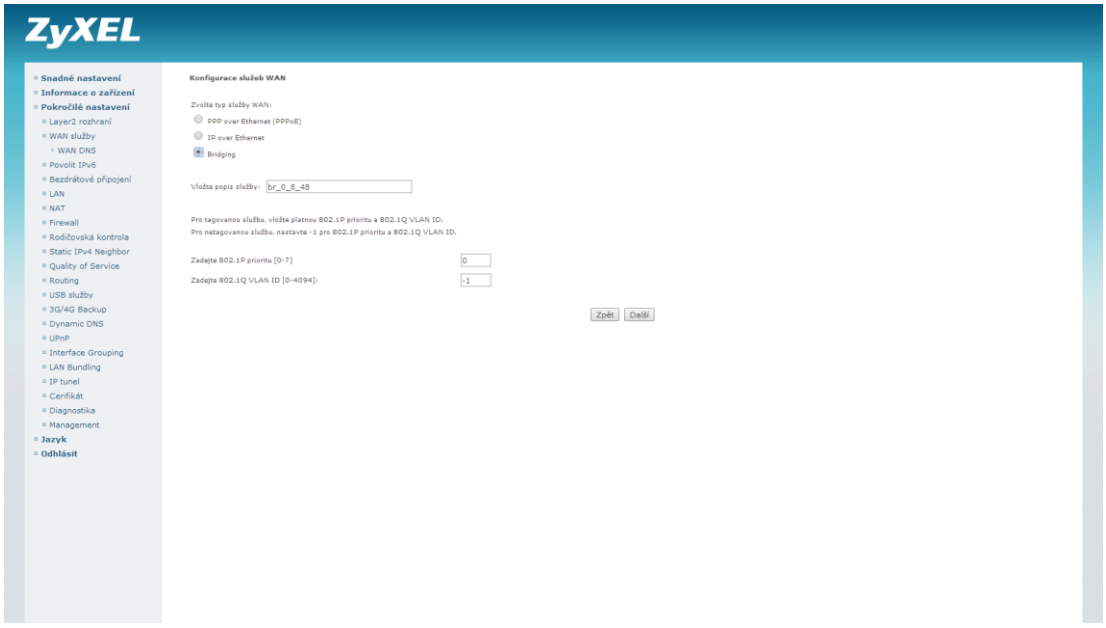


5.3.2 Bridge

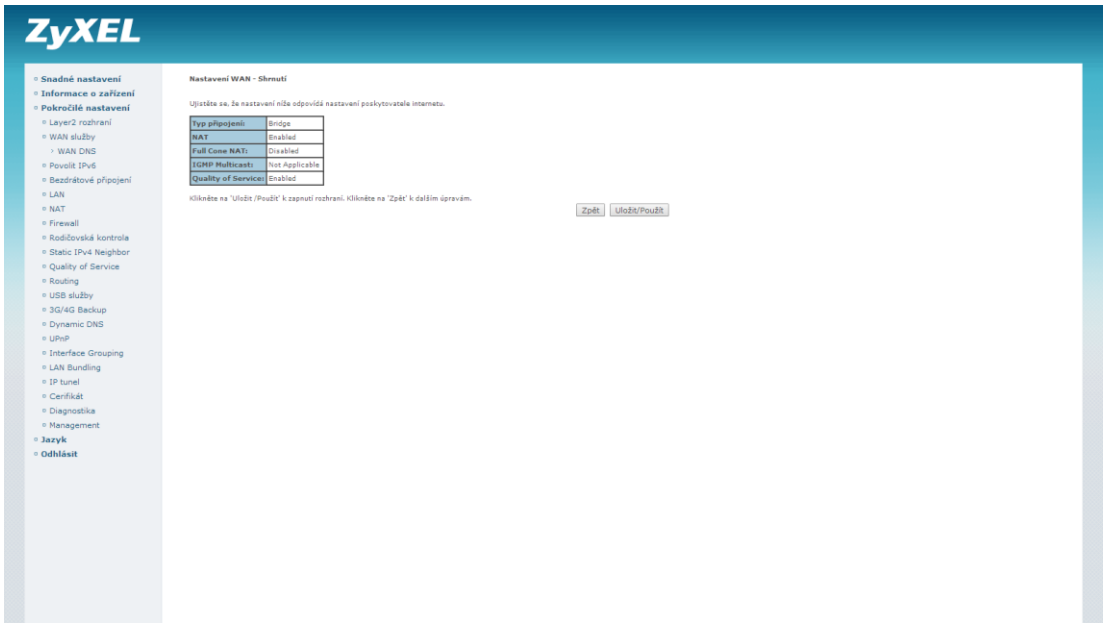
Zvolte Bridge jako typ připojení, který chcete používat a zvolte WAN rozhraní.



Nastavte údaje podle údajů od poskytovatele připojení jako v kapitole 5.3.1.



Průvodce Vám zobrazí sumář nastavených hodnot, nastavení dokončíte kliknutím na tlačítko **Uložit/Použít.**

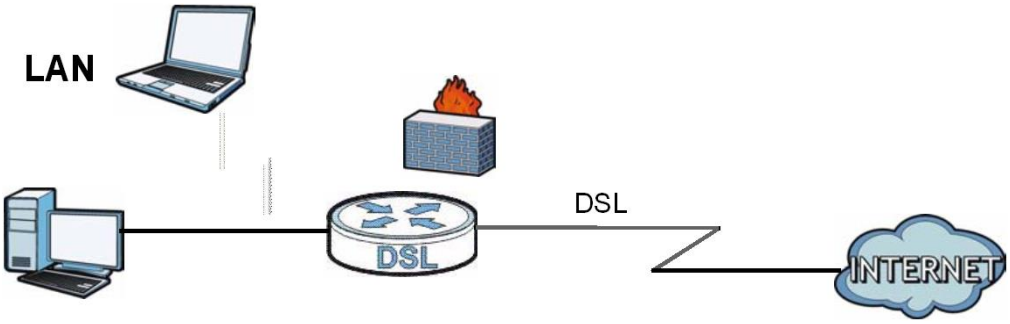

ZyXEL
Snadné nastavení
Informace o zařízení
Pokročilé nastavení
Layer2 rozhraní
WAN služby
WAN DNS
Povolit IPv6
Bezdrátové připojení
LAN
NAT
Firewall
Rodičovská kontrola
Static IPv4 Neighbor
Quality of Service
Routing
USB služby
3G/4G Backup
Dynamic DNS
UPnP
Interface Grouping
LAN Bundling
IP tunel
Certifikát
Diagnostika
Management
Jazyk
Odhlásit
Nastavení WAN - Shrnutí
Ujistěte se, že nastavení níže odpovídá nastavení poskytovatele internetu.
Typ připojení: Bridge
NAT: Enabled
Full Cone NAT: Disabled
IGMP Multicast: Not Applicable
Quality of Service: Enabled
Klikněte na 'Uložit /Použít' k zapnutí rozhraní. Klikněte na 'Zpět' k dalším úpravám.
Zpět
Uložit/Použít

6 NASTAVENÍ SÍTĚ LAN

6.1 Základní informace

LAN síť (Local Area Network) je sdílený komunikační systém, který propojuje různá síťové zařízení. Obvykle zahrnuje jednu úzce vymezenou prostorovou oblast, např. budovu nebo patro v budově.

Na obrazovce LAN můžete konfigurovat server LAN DHCP a nastavit IP adresy.



6.1.1 Co je třeba vědět o síti LAN

IP adresa

IP adresa identifikuje jednotlivá zařízení na síti. Každé síťové zařízení (počítač, server, router, tiskárna, atd.) potřebuje IP adresu, aby mohlo komunikovat s ostatními zařízeními na síti. Síťovým zařízením se také říká hostitelské zařízení nebo síťový uzel (anglicky „host“).

Maska podsítě

Maska podsítě určuje maximální počet možných síťových zařízení na síti. Maska podsítě se také užívá k rozdělení jedné sítě na několik menších podsítí.

DHCP

Server DHCP (Dynamic Host Configuration Protocol) přidělí připojenému zařízení při zapnutí IP adresu, masku podsítě, DNS a další směrovací informace.

RIP

Protokol RIP (Routing Information Protocol) umožňuje vzájemnou výměnu informací mezi routery.

Multicast

Tradičně se IP pakety přenášejí jedním ze dvou způsobů: unicast (1 odesílatel – 1 příjemce) a broadcast (1 odesílatel – každé zařízení na síti). Multicast je způsob přenosu IP paketů, který leží mezi oběma tradičními přístupy – 1 odesílatel posílá pakety určité skupině počítačů na síti, tedy ne pouze jednomu, ale ani ne všem.

IGMP

IGMP (Internet Group Multicast Protocol) je protokol síťové vrstvy, která se užívá k určení příslušnosti do skupiny pro multicasting – neužívá se k přenosu uživatelských dat. Existují tři verze IGMP: v1, v2 a v3. Verze v1 je nejstarší, ale stále se hojně užívá.

DNS

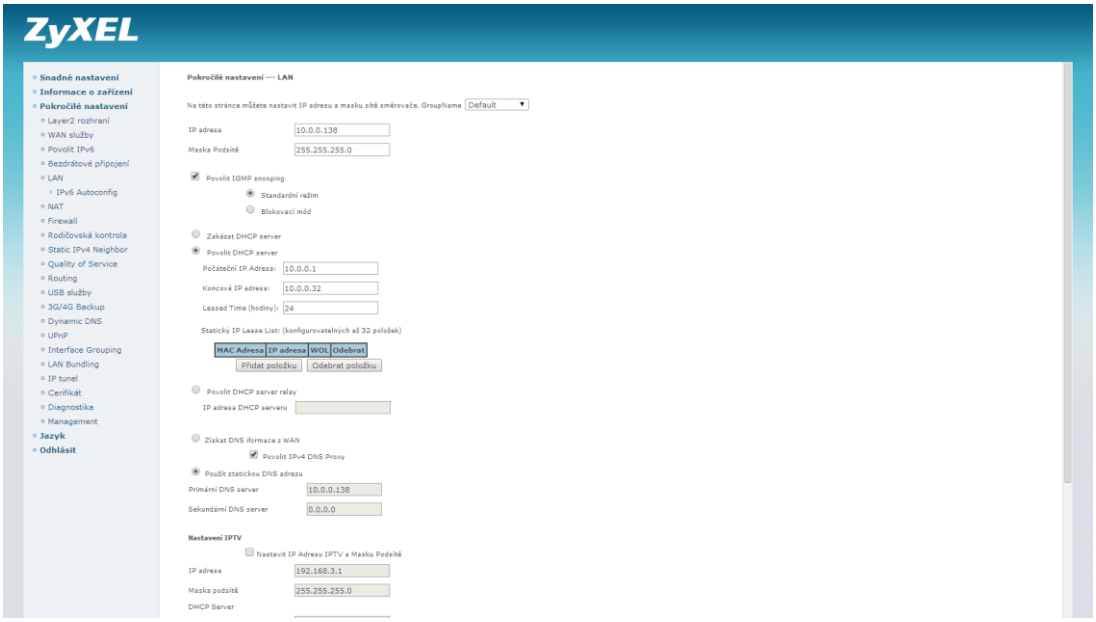
Systém DNS (Domain Name System) je hierarchický systém jmen, který přiřazuje doménové jméno IP adrese. DNS server je velmi důležité zařízení, protože ukládá informace o přiřazení doménového jména a IP adresy (bez DNS serveru by bylo k přístupu k danému zařízení potřeba znát jeho IP adresu).

6.1.2 Než začnete

Zjistěte MAC adresy síťových zařízení, které chcete přidat na seznam klientských zařízení DHCP.

6.2 Obrazovka LAN

Na obrazovce LAN můžete upravit IP adresu a masku podsítě zařízení ZyXEL nebo nastavit DHCP server včetně pevných adres a přidělovaných DNS serverů. Obrazovku otevřete kliknutím na **Pokročilé nastavení > LAN**.



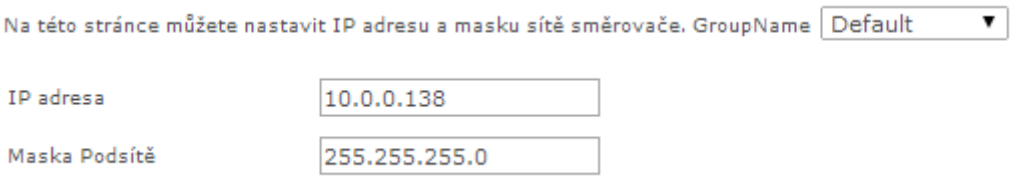
V tabulce je uveden popis všech políček na obrazovce.

Položka	Popis
Group Name	Předdefinovaná nastavení IPadres.
IP adresa	IP adresa zařízení v síti LAN. Zároveň je adresou pro GUI zařízení. Zadejte IP adresu, kterou chcete přidělit zařízení ZyXEL na lokální síti LAN. Např. 10.0.0.138 (tovární výchozí nastavení).
Maska podsítě	Zadejte masku podsítě v tečkované notaci, např. 255.255.255.0 (tovární výchozí nastavení). Zařízení ZyXEL automaticky vypočte masku podsítě podle vložené IP adresy. Vypočtenou hodnotu neměňte, pokud nemáte jiné pokyny.
Povolit IGMP snooping	Možnosti: Standardní režim, Blokovací mód. Povolením IGMP snoopingu umožníte zařízení zpracovávat multicastové streamy na všech portech (standardní režim) nebo z důvodu úspory výkonu a absence použití IPTv, IGMP pakety zakázat (blokovací mód).
Zakázat DHCP server	Zaškrtnutím zakážete funkci DHCP serveru, zařízení nebude přidělovat klientským zařízením IP adresy
Povolit DHCP server	Zaškrtnutím povolíte funkci DHCP serveru, zařízení bude přidělovat klientským zařízením IP adresy
Počáteční IP adresa	Počáteční IP adresa rozsahu, ze kterého budou přidělovány IP adresy klientským zařízením
Koncová IP adresa	Koncová IP adresa rozsahu, ze kterého budou přidělovány IP adresy klientským zařízením
Leased time (hodiny)	Doba, po kterou bude platná přidělená IP adresa pro klientské zařízení
Statický IP Lease list	zde můžete nastavit až 32 klientských zařízení, které budou mít DHCP serverem přidělenou vždy stejnou IP adresu
Povolit DHCP server relay	Menu umožňuje použít jiné zařízení jako DHCP server.

IP adresa DHCP serveru	Menu umožňuje nastavit IP adresu DHCP serveru.
Získat DNS informace z WAN	Menu umožňuje Získat DNS informace z WAN
Povolit IPv4 DNS Proxy	Menu umožňuje Povolit IPv4 DNS Proxy
Použít statickou DNS adresu	Menu umožňuje použít statickou DNS adresu
Primární DNS server	IP adresa primárního DNS serveru
Sekundární DNS server	IP adresa sekundárního DNS serveru
Nastavení IPTv	Zaškrtnutím volby můžete ručně nastavit IP adresu a masku podsítě pro službu speciální služby IPTV
IP adresa	IP adresa služby IPTV
Maska podsítě	Maska podsítě služby IPTV

6.3 Nastavení IP adresy

1. Zadejte IP adresu do políčka **IP adresa**. Adresu zadejte v tečkované notaci. Tato adresa je adresou zařízení ZyXEL na síti LAN.
2. Do políčka **Maska podsítě** zadejte masku podsítě. Pokud nemáte jiné pokyny, neměňte nastavení políčka, protože konfigurátor automaticky vypočte masku podsítě podle vložené IP adresy.
3. Klikněte na tlačítko **Uložit/Použít**. Dojde k uložení vložených hodnot.

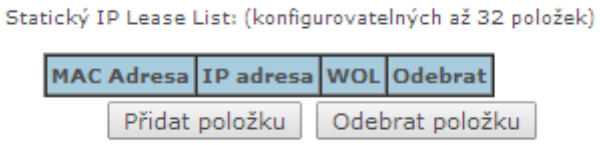


6.4 Seznam klientů

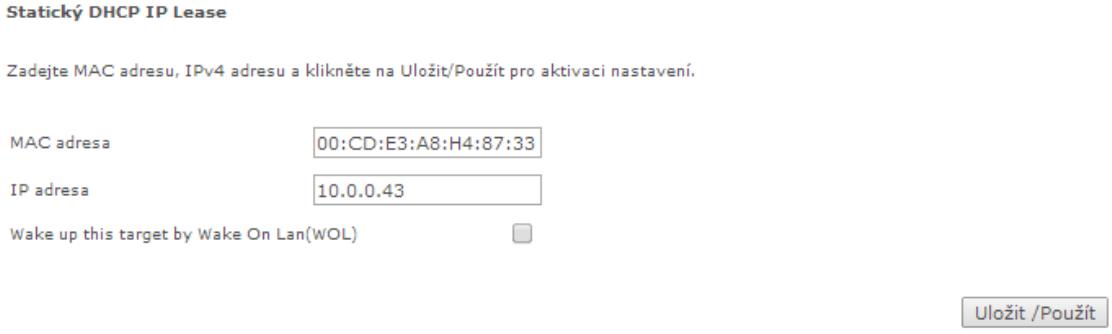
V tabulce můžete přidělit IP adresy počítačům na síti LAN na základě jejich MAC adresy. Tím nastavíte statickou položku DHCP.

Každé zařízení Ethernet má svou jedinečnou adresu MAC (Media Access Control). Adresa MAC je zařízení přidělena již v továrně a skládá se ze šesti znaků (v hexadecimální soustavě), např. 00:A0:C5:00:00:02.

Klikněte na **Přidat položku**



V otevřeném okně zadejte MAC adresu zařízení a IP adresu, kterou má zařízení z DHCP serveru získat. V případě potřeby můžete zaškrtnout položku WoL.



Pro dokončení klikněte na **Uložit/Použít**

6.5 IP alias

IP alias umožňuje rozdělit fyzickou síť na několik různých logických sítí se stejným rozhraním Ethernet.

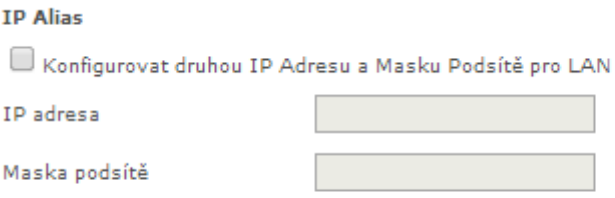
Když nastavíte IP alias, můžete také konfigurovat pravidla firewallu pro řízení přístupu mezi různými logickými sítěmi LAN

Poznámka:

Dávejte pozor, ať se logické sítě vzájemně nepřekrývají.

6.5.1 Konfigurace IP aliasu

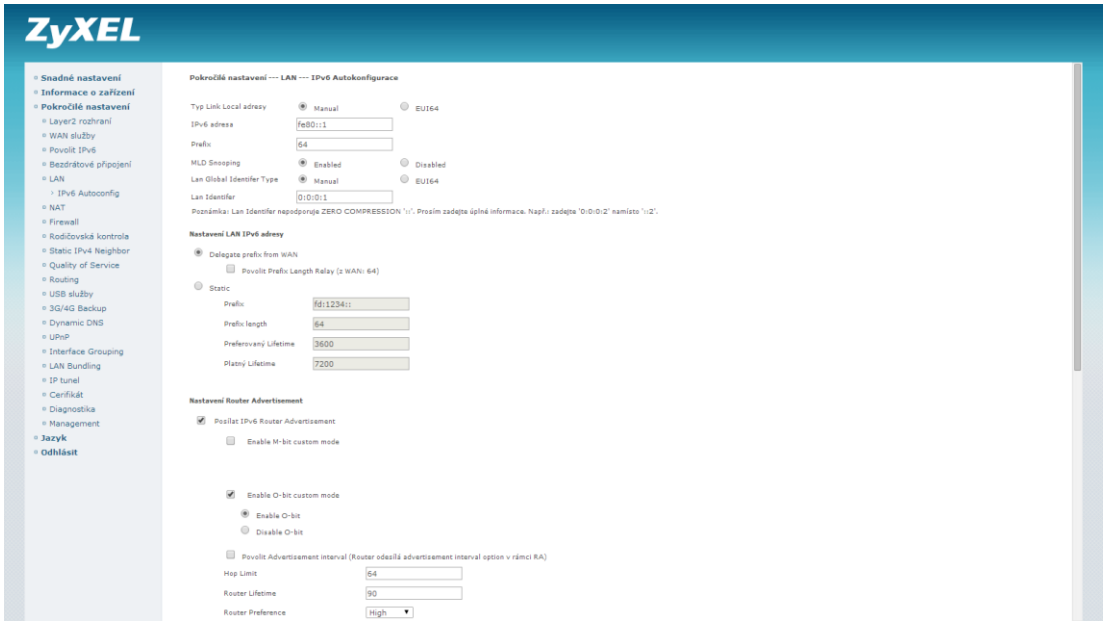
Na obrazovce můžete nastavit IP alias. Zadejte požadovanou IP adresu a Masku podsítě



6.6 IPv6 autoconfig

Kliknutím na **Pokročilé nastavení > LAN > IPv6 autoconfig** můžete nastavit konfiguraci protokolu IPv6 pro síť LAN.

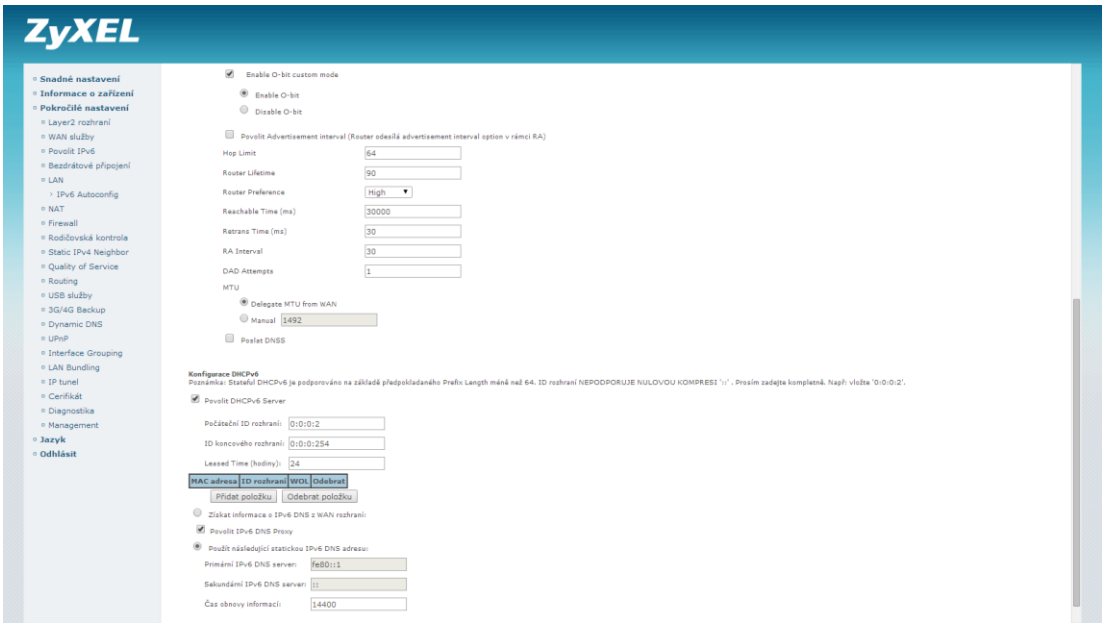
Vyplňte údaje na obrazovce podle informací získaných od Vašeho poskytovatele internetu.



V tabulce níže naleznete vysvětlení pojmů pro IPv6 autoconfig první části obrazovky

Položka	Popis
Typ link local IP adresy	způsob přidělení link local adresy.
IP adresa	IPv6 adresa směrovače.
Prefix	délka prexifu.
MLD Snooping	Multicast Listener Discovery.
LAN global identifier type	typ LAN global identifier .
Nastavení LAN IPv6 adresy	
Delegate prefix from WAN	delegovat prefix z WAN rozhraní.
Povolit prefix length relay	delegovat prefix /64 z WAN rozhraní.
Static	statické zadání IP adresy.

Prefix	statické zadání prefixu.
Prefix length	statické zadání délky prefixu.
Preferovaný lifetime	Preferovaný lifetime.
Platný lifetime	zadat platný lifetime.
Router preference	router preference.



V tabulce níže naleznete vysvětlení pojmů pro IPv6 autoconfig druhé části obrazovky

Položka	**Popis**
Enable M-bit custom mode	použít M-bit.
Enable O-bit custom mode	použít O-bit.
Povolit advertisement interval	povolit advertisement interval.
Hop limit	definovat hop limit.
Router lifetime	definovat router lifetime.
Router preference	definovat router preference.
Reachable time	definovat reachable time.
Retrans time	definovat retrans time.
RA Interval	definovat RA Interval.
DAD Attempts	definovat počet duplicate address detection.
MTU	definovat Maximum Transmission Unit.
Delegate MTU from WAN	použít MTU dle WAN rozhraní.
Manual	manuální nastavení MTU.

Konfigurace DHCPv6	
Povolit DHCPv6 server	povolit DHCPv6 server.
Počáteční ID rozhraní	zvolit počáteční ID rozhraní.
ID koncového rozhraní	zvolit ID koncového rozhraní.
Leased time	definovat leased time.
IPv6 static list	přidělení statické adresy na základě MAC adresy zařízení.
Získat informace o IPv6 DNS z WAN	získat informace o IPv6 DNS z WAN rozhraní.
Povolit IPv6 DNS Proxy	povolit IPv6 DNS Proxy.
Použít následující statickou IPv6 DNS adresu	nastavit následující statickou IPv6 DNS adresu.
Primární IPv6 DNS server	primární IPv6 DNS server.
Sekundární IPv6 DNS server	sekundární IPv6 DNS server.
Čas obnovy informací	nastavení času obnovy informací.

7 BEZDRÁTOVÁ SÍŤ LAN

7.1 Základní informace

V této kapitole popisujeme, jak nastavit bezdrátovou síť a optimalizovat její provoz. Dozvíte se např. jak:

- Zapnout a vypnout bezdrátovou síť.
- Konfigurovat jméno, bezdrátový kanál a zabezpečení sítě.
- Konfigurovat bezdrátovou síť prostřednictvím WPS (WiFi Protected Setup).
- Nastavit několik různých bezdrátových sítí.
- Omezit přístup k síti s využitím filtru na bázi MAC adres.
- A další.

7.1.1 Co všechno lze nastavit na obrazovkách Wireless LAN

V této kapitole popisujeme, co lze nastavit na obrazovkách **Pokročilé nastavení > Bezdrátové připojení**.

- Na obrazovce **Základní** můžete zapnout a vypnout bezdrátovou síť, název SSID, skrytí SSID, WMM, WMF, počty klientů a prioritu.
- Na obrazovce **Zabezpečení** nastavíte bezdrátové zabezpečení sítě a také funkce WPS.
- Na obrazovce **MAC filtr** nastavíte seznam povolených, nebo zakázaných MAC adres.
- Na obrazovce **Pokročilé** nastavíte například Wifi kanál, použitý standard připojení nebo vysílací výkon.
- Na obrazovce **Station info** vidíte seznam připojených bezdrátových klientů.

7.1.2 Co je třeba vědět o bezdrátových sítích

Základní princip

Slovo „bezdrátový“ odkazuje ke komunikaci s využitím rádiových vln. Bezdrátový síťový adaptér je zařízení, které umožňuje počítači vysílat a přijímat rádiové vlny a komunikovat s dalšími bezdrátovými zařízeními. Na stejném principu pracují i obyčejné vysílačky. Bezdrátová zařízení většinou využívají kmitočtová pásma, která jsou veřejná a nevyžadují licenci. Od obyčejné rádiové komunikace se bezdrátová zařízení liší především počtem existujících síťových standardů a metodami šifrování dat.

SSID

Každá síť musí mít své jméno; tomuto jménu se říká SSID (Service Set IDentifier, kde „service set“ v tomto kontextu znamená bezdrátová síť). Když se v určité lokalitě překrývá více sítí, je jméno sítě způsob, jak identifikovat tu správnou síť.

Filtrování podle adres MAC

Každé zařízení Ethernet má svou jedinečnou adresu MAC (Media Access Control). Adresa MAC je zařízení přidělena již v továrně a skládá se ze šesti znaků (v hexadecimální soustavě: 0-9 a až F), např. 00:A0:C5:00:00:02.

Filtrování podle adres MAC povolí přístup k bezdrátové síti jen zařízení se správnou adresou MAC.

7.1.3 Než začnete

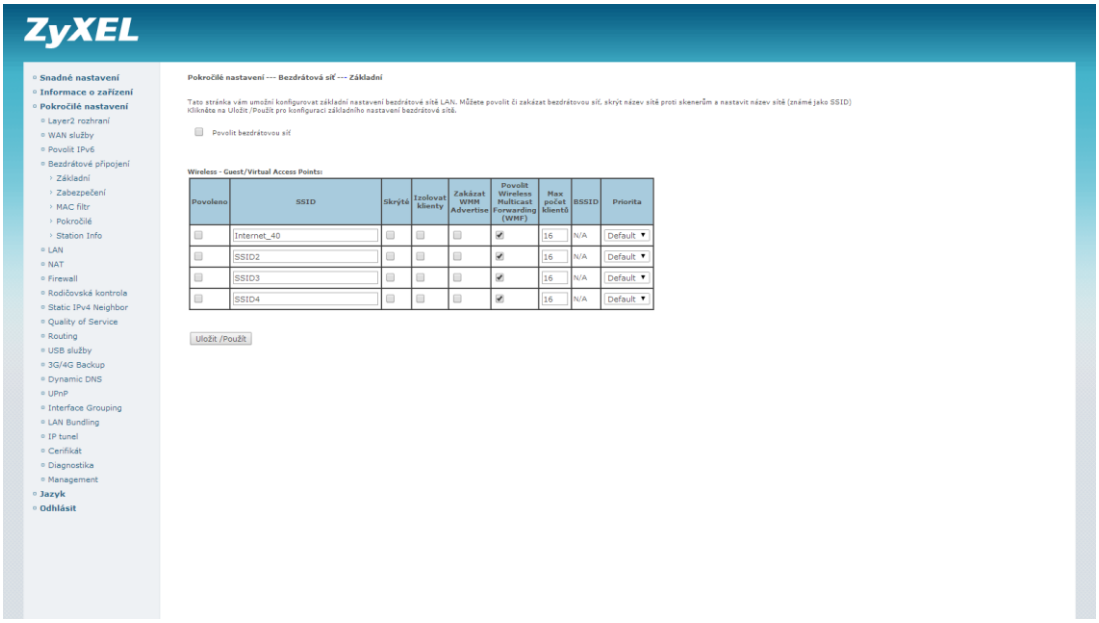
Při nastavení bezdrátové sítě byste měli znát tyto informace:

- Jaký bezdrátový standard podporují klientská zařízení, která máte (např. IEEE 802.11g)? Jaký je nejvhodnější standard?
- Jaké šifrování podporují klientská zařízení, která máte (např. WPA-PSK)? Jaké je to nejsilnější šifrování, které podporují všechna zařízení?
- Podporují klientská zařízení nastavení prostřednictvím WPS? Jestliže ano, je nastavení sítě velmi jednoduché.

  I v případě, že některá zařízení WPS nepodporují, můžete stále užít způsob WPS na zařízení, která WPS podporují, a zbytek zařízení přidat ručně.
- Chcete nastavit nějaké pokročilé volby? Jestliže např. chcete nastavit priority pro QoS, zjistěte nejprve, co přesně chcete docílit. Jestliže pokročilé volby nebudete konfigurovat, nechte je na jejich výchozím nastavení.

7.2 Základní nastavení přístupového bodu (AP)

Na obrazovce **Pokročilé nastavení > Bezdrátové připojení > Základní** nastavíte základní parametry bezdrátové sítě.



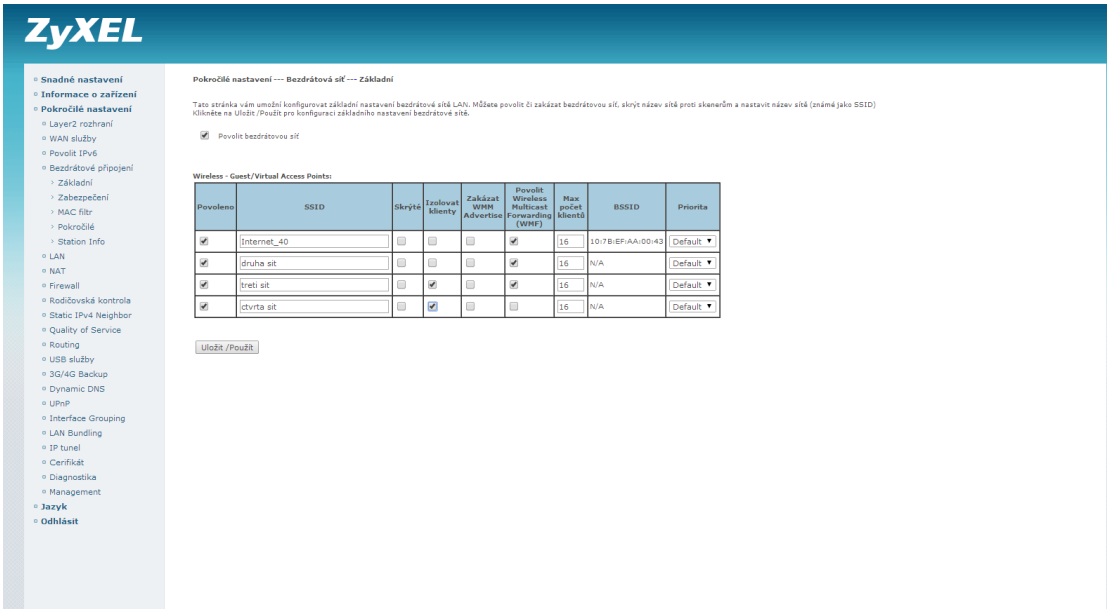
V tabulce uvádíme popis všech políček na obrazovce.

Položka	Popis
Základní	
Povolit bezdrátovou síť	Zaškrtnutím políčka aktivujete bezdrátovou síť.
SSID	SSID je identifikátor (jméno), které označuje bezdrátovou síť. K přístupovému bodu se klientské zařízení musí připojit pod tímto jménem, aby s ním mohlo komunikovat. Zadejte popisné jméno (max. 32 tisknutelných 7bitových znaků ASCII). Poznámka: Jestliže konfigurujete zařízení ZyXEL z počítače připojeného bezdrátově a změníte nastavení SSID nebo zabezpečení zařízení ZyXEL, ztratíte se zařízením po stisknutí tlačítka **Uložit/Použít** spojení. Abyste se mohli znovu přihlásit, musíte se přihlásit pod novým SSID a s platným šifrováním.
Skryté	Když zaškrtnete políčko, informace o jménu sítě se nevysílá do okolí. To znamená, že síť se neobjeví na seznamu dostupných sítí v adaptéru.

Položka	Popis
Izolovat klienty	Jednotliví bezdrátoví klienti v síti jsou od sebe bezpečně odděleni a nemají jeden k druhému přístup. Toto nastavení je obvyklé například v sítích volně přístupných veřejnosti.
Zakázat WMM advertisement	Zpřístupnění funkce Wireless MultiMedia (forma prioritizace multimediálního provozu)
Povolit Wireless Multicast Forwarding	Zaškrtnutím políčka umožníte po tomto SSID přenos video streamu.
Max počet klientů	Maximální počet bezdrátových klientů (PC, telefonů, tabletů) na tomto SSID
BSSID	Tzv. Basic Service Setting Identifikator
Priorita	Nastavení priority provozu v rámci tohoto SSID

7.2.1 Nastavení dalších bezdrátových sítí

Na obrazovce můžete také aktivovat a konfigurovat další bezdrátové sítě. Pro zabezpečení postupujte dle pokynů v kapitole „Nastavení zabezpečení“



7.3 Nastavení zabezpečení

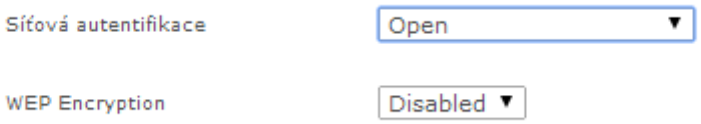
Na obrazovce **Pokročilé nastavení > Bezdrátové připojení > Zabezpečení** nastavíte zabezpečení vaší bezdrátové sítě. Mužete zde také nastavit pravidla pro WPS

Před konfiguraci zabezpečení zkontrolujte, zda název sítě (Zvolit SSID) odpovídá vámi požadovanému názvu sítě (SSID), kterou chcete konfigurovat.

7.3.1 Nezabezpečená síť

Jestliže nechcete přístup k bezdrátové síti nijak omezit (žádné šifrování dat, žádná autentizace) zvolte volbu **Open** (bez zabezpečení) v nastavení zabezpečení bezdrátového připojení.

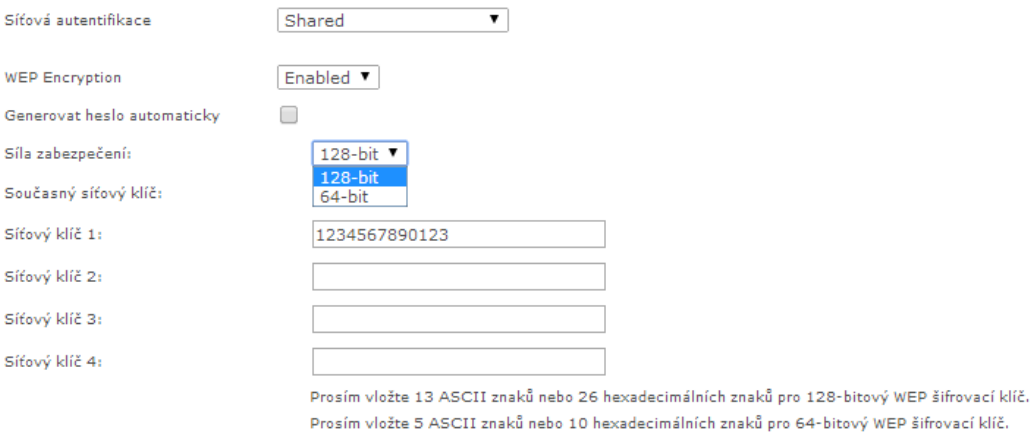
Poznámka: Uvědomte si, že bez zabezpečení se k bezdrátové síti může přihlásit každý v dosahu signálu.



7.3.2 Šifrování WEP

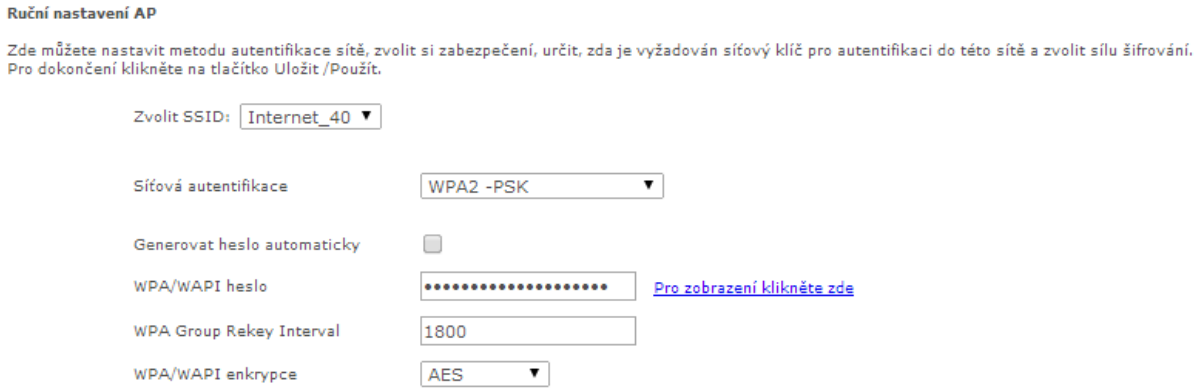
V kapitole popisujeme, jak aktivovat šifrování komunikace ve standardu WEP.

Poznámka: Metoda WEP má velmi nízkou úroveň zabezpečení. Tento způsob šifrování je možné prolomit s využitím volně dostupného softwaru. Důrazně doporučujeme, abyste zvolili silnější zabezpečení. Obecně platí, že je nejlepší užívat nejsilnější zabezpečení, které podporují všichni předpokládaní klienti. Např. dejte přednost šifrování WPA-PSK nebo WPA2-PSK nebo WPA nebo WPA2, pokud máte server RADIUS. Jestliže bezdrátoví klienti nepodporují nic silnějšího než WEP, nastavte alespoň co nejsilnější hesla. WEP šifru (64bit nebo 128 bit) zvolíte výběrem **Enabled** u položky WEP Encryption



7.3.3 Šifrování WPA(2)-PSK

V kapitole popisujeme, jak aktivovat šifrování komunikace ve standardu WPA-PSK nebo WPA2-PSK. Heslo můžete zvolit buď vlastní, nebo využít automaticky generovaného hesla.



7.3.4 Autentizace WPA(2)

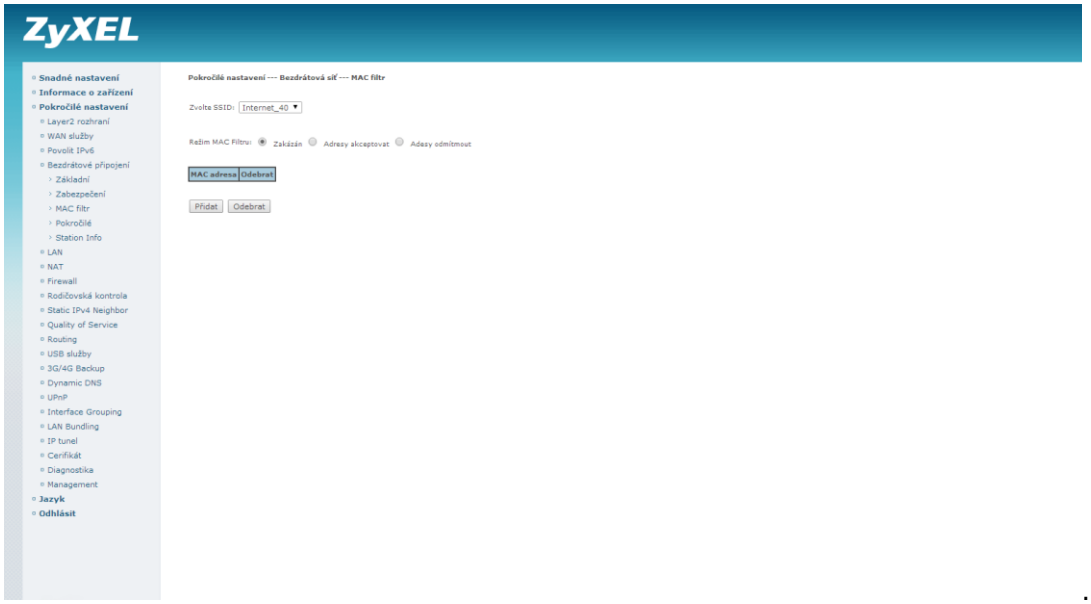
V kapitole popisujeme nastavení autentizace WPA nebo WPA2. Postupujte podle pokynů na obrazovce a dle údajů Radius serveru (IP adresa, číslo portu a klíč)



7.4 MAC Filtr

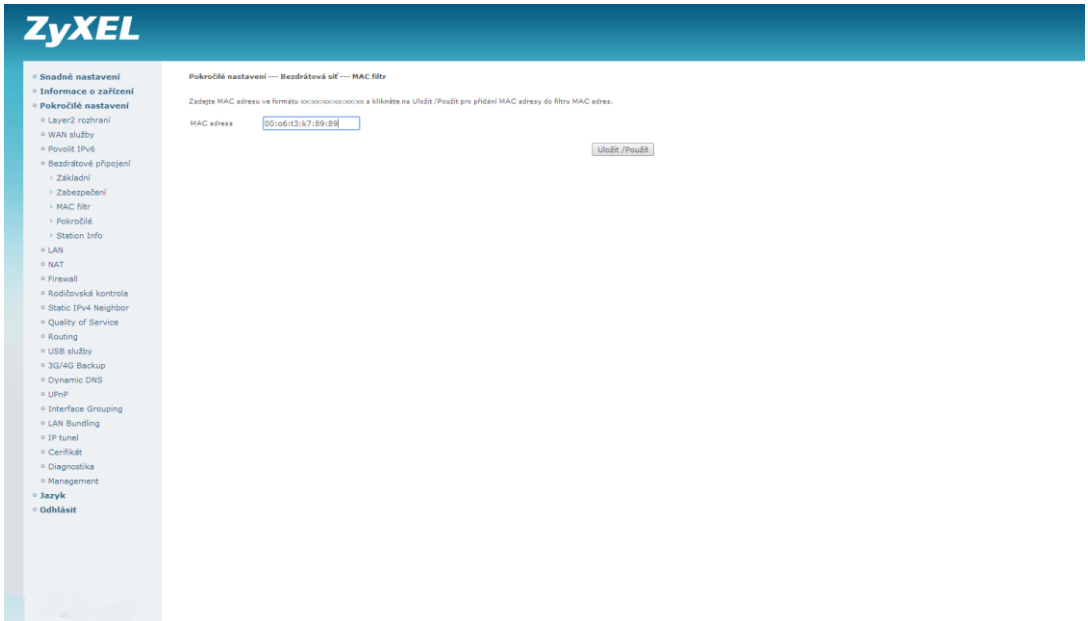
V této kapitole popisujeme, jak konfigurovat seznam MAC adres pro účely filtrování. Okno zobrazíte kliknutím na **Pokročilé nastavení > Bezdrátové připojení > Mac Filtr**

MAC filtr aktivujete zaškrtnutím políčka **Adresy akceptovat** nebo **Adresy odmítnout** podle požadované funkce MAC filtru



.

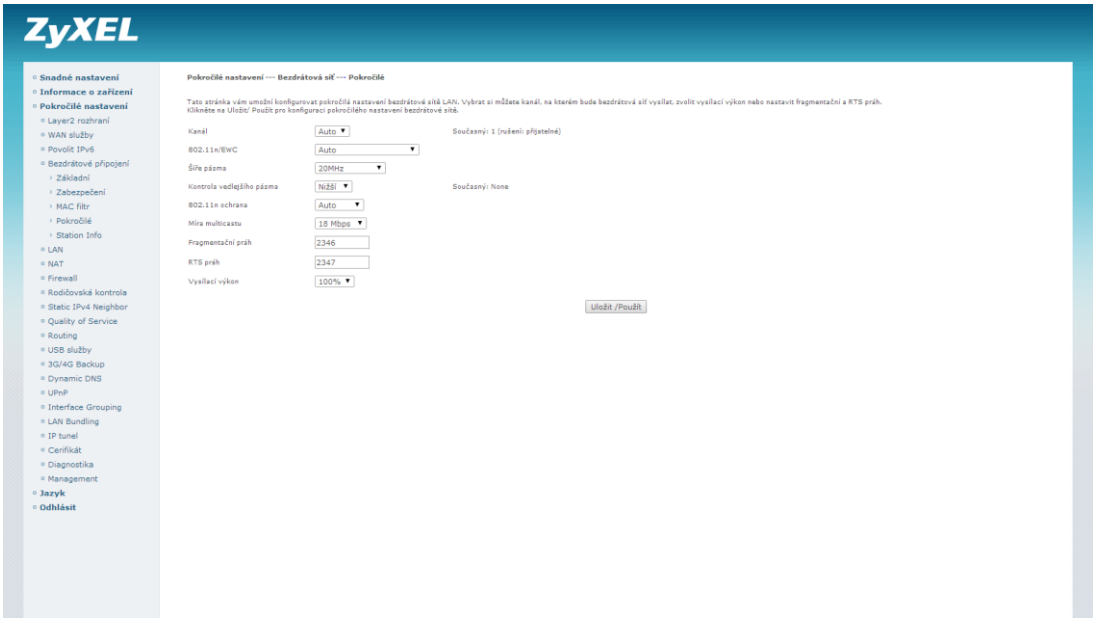
Stiskněte tlačítko **Přidat** a v otevřeném okně zadejte MAC adresu kterou chcete povolit/zakázat. Zadání uložíte kliknutím na **Uložit/Použít**



7.5 Pokročilé nastavení bezdrátové sítě

Na této obrazovce můžete nastavit pokročilé parametry. Obrazovku otevřete kliknutím na **Pokročilé nastavení > Bezdrátové připojení > Pokročilé**

.

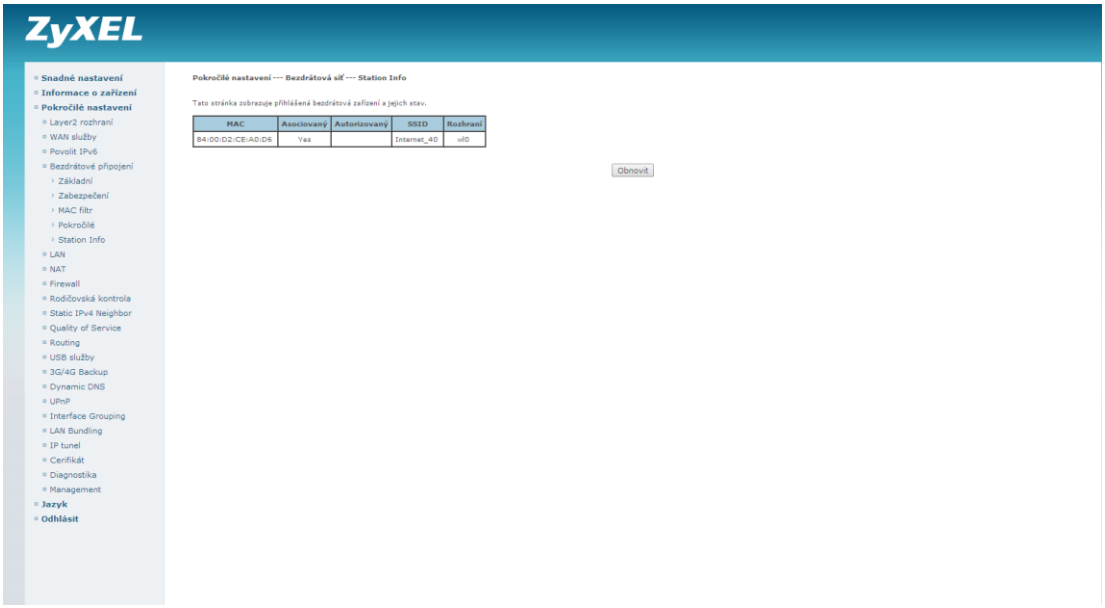


V tabulce uvádíme popis všech políček na obrazovce.

Položka	Popis
Kanál	Podle stupně zarušení jednotlivých kanálů (zobrazeno vpravo nahoře v okně) vyberte kanál 1-13
802.11n/EWC	Enhanced wireless consorcium 802.11n standard, nikoliv 802.11n „draft“
Šíře pásma	Celková šíře pásma v rámci použitého kanálu, které bude zařízení využívat.
Kontrola vedlejšího pásma	Při použití 40MHz šíře pásma bude doplňkový kanál volen z dalšího nižšího kanálu (o 3 kanály nižší než hlavní kanál).
802.11n ochrana	
Míra multicastu	Maximální rychlost multicastu šířeného přes WiFi
Fragmentační práh	Tzv „treshold“ – maximální velikost fragmentu (paketu) přenášeného přes WiFi
RTS práh	Časová hodnota trvání operace
Vysílací výkon	Zadejte výstupní výkon zařízení ZyXEL. V lokalitách s vysokou hustotou dalších přístupových bodů přispěje snížení výkonu ke snížení vzájemného rušení mezi sítěmi. Volby jsou: **100%, 75%, 50%** a **25%**.

7.6 Seznam klientů

Na obrazovce se zobrazí seznam bezdrátových klientů připojených k zařízení **Pokročilé nastavení > bezdrátové připojení > Station Info**.

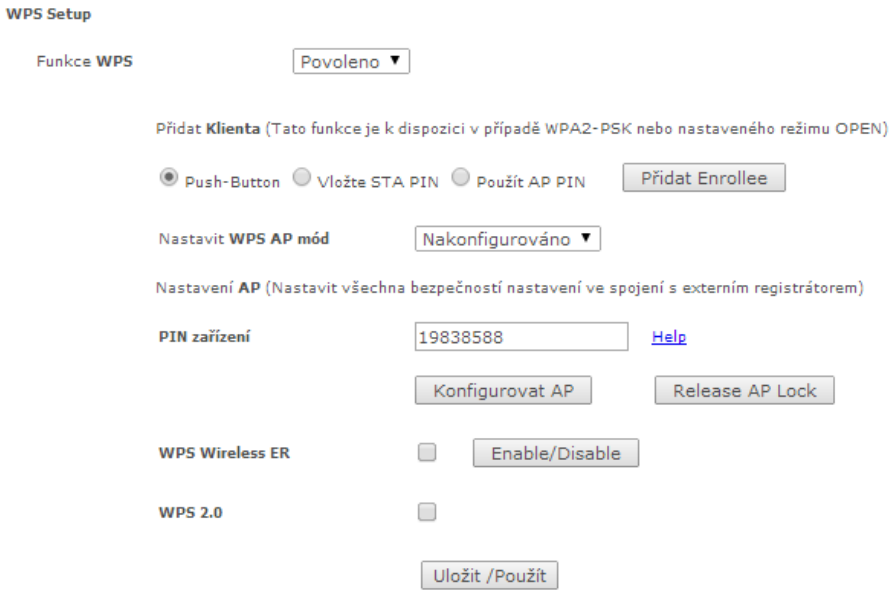


7.7 Nastavení prostřednictvím WPS: zařízení ZyXEL

Na obrazovce můžete konfigurovat bezdrátovou síť pomocí technologie WPS a zjistit stav zařízení ZyXEL ve vazbě na WPS.

Technologie WPS umožňuje rychle nastavit bezdrátovou síť se silným zabezpečením mezi dvěma stanicemi, aniž by bylo potřeba provádět manuální nastavení. WPS musí podporovat obě stanice. Další stanice lze přidat opakováním postupu.

Otevřete obrazovku **Pokročilé nastavení > Bezdrátové připojení > Zabezpečení** u položky **Funkce WPS** vyberte volbu **Povoleno** (WPS nelze povolit při šifře WEP).



Položka	Popis
Přidat Klienta	Push-Button: konfigurace pomocí stisknutí tlačítka na zařízení a poté do 2 minut na bezdrátových klientech Vložte STA PIN: Při párování bezdrátových klientů (opět do 2 minut) použijete STA PIN kód Použít AP PIN: Při párování bezdrátových klientů (opět do 2 minut) použijete AP PIN kód
Nastavit WPS AP mód	Nastavení použití WPS s AP PIN
PIN Zařízení	Zde je uvedeno číslo PIN zařízení ZyXEL. Zadejte toto číslo PIN v konfigurační utilitě zařízení, ke kterému se chcete připojit pomocí WPS. Číslo PIN není potřeba, když přidáváte zařízení pomocí Push-Button.

Konfigurovat AP	Tlačítko pro spuštění konfigurace AP z WiFi klienta pomocí metody WPS
Release AP Lock	Zrušení zamčení bezdrátové sítě po uplynutí 2 minut po stisknutí tlačítka WPS
WPS Wireless ER	Zapnutí/Vypnutí funkce WPS Wireless ER
WPS 2.0.	Použití vyššího standardu zabezpečení WPS. Pozor, některé bezdrátové klienty tento standard nepodporují.

8 PŘEKLAD SÍŤOVÝCH ADRES (NAT)

8.1 Základní informace

V kapitole popisujeme, jak konfigurovat překlad síťových adres NAT na zařízení ZyXEL (Network Address Translation – NAT, RFC 1631). NAT je funkce, která překládá jednu IP adresu na druhou (např. zdrojovou adresu odchozího paketu v lokální síti, na veřejnou IP adresu, které je přiřazená WAN rozhraní zařízení).

8.1.1 Co všechno lze nastavit na obrazovkách NAT

- Na obrazovce **Virtuální servery** Virtuální Server umožňuje adresovat příchozí data z WAN strany (identifikované protokolem a číslem externího portu) na Interní server s privátní IP adresou na LAN straně
- Na obrazovce **DMZ Host** nastavení Demilitarizované zóny zařízení. Směrovač bude přeposílat IP pakety z WAN, které nepatří žádné aplikaci v tabulce Virtuálních Serverů do počítače DMZ Host
- Na obrazovce **ALG** můžete aktivovat a deaktivovat aplikační bránu SIP ALG.

8.1.2 Co je třeba vědět o překladu síťových adres (NAT)

Vnitřní/vnější zařízení

Výrazy „vnitřní“ a „vnější“ se vztahují k zařízení ZyXEL: zařízení na stejné síti jako zařízení ZyXEL jsou vnitřní, zatímco zařízení mimo tuto síť jsou vnější (např. webové servery na internetu).

Globální/lokální adresa

Rozlišení mezi globální a lokální IP adresou zařízení se vztahuje k adrese v paketu, který prochází routerem: lokální adresa je adresa zařízení na lokální síti, zatímco globální adresa je adresa stejného zařízení v síti WAN.

NAT

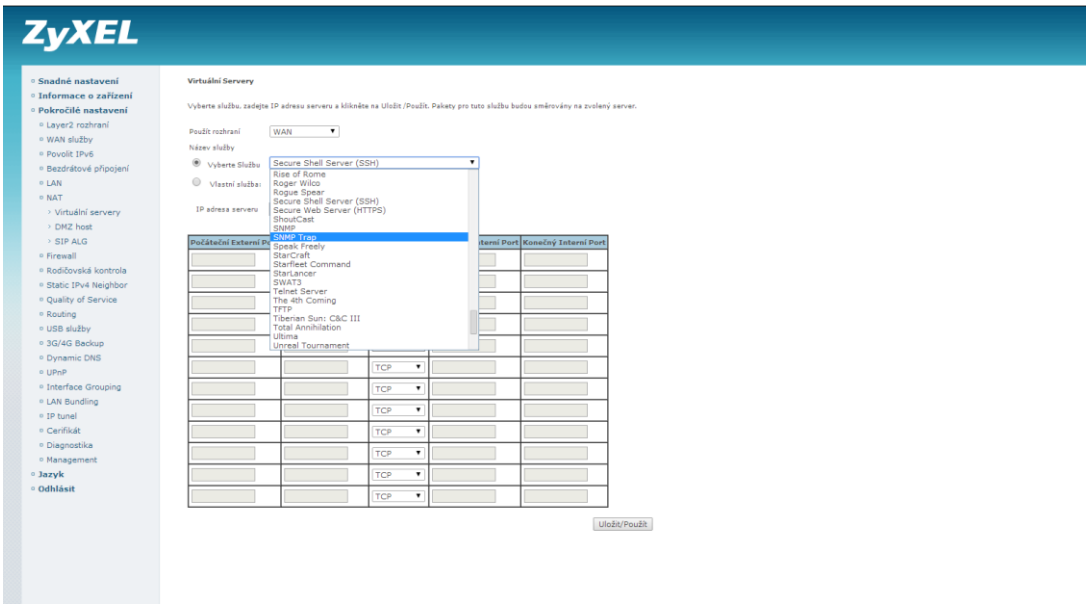
Ve své nejjednodušší podobě pracuje NAT tak, že překládá jednu IP adresu na druhou (překlad 1-1): předtím než odešle paket od určitého zařízení na síti do globální sítě WAN, změní zdrojovou IP adresu (vnitřní lokální adresa) na jinou (vnitřní globální adresa). Při zpětné komunikaci s tímto zařízením přeloží cílovou adresu (vnitřní globální adresa) zpět na vnitřní lokální adresu.

Přesměrování portů

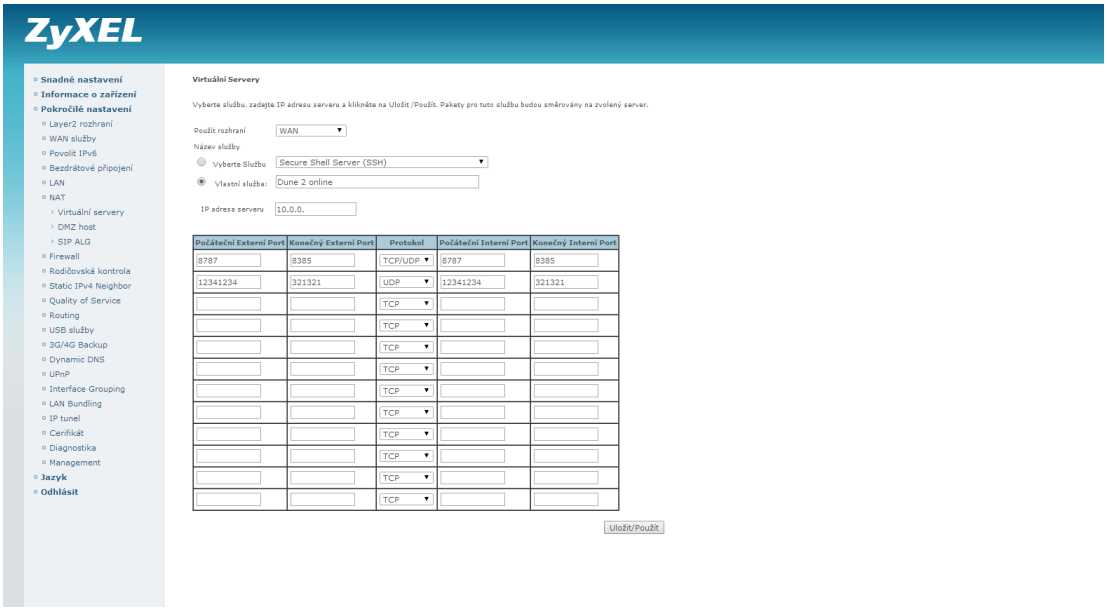
Přesměrování portů je způsob, jak umožnit počítačům na vnější síti připojit se k určitému portu na serveru, který na vnější síti není viditelný.

8.2 Virtuální servery

Virtuální Server umožňuje adresovat příchozí data z WAN strany na Interní server s privátní IP adresou na LAN straně. Číslo Interního portu je nutné pouze v případě, že je potřeba konvertovat číslo externího portu na jiné použité na serveru na LAN straně. Může být nakonfigurováno maximálně 32 záznamů. V položce IP adresa serveru zadejte IP adresu zařízení na které má být vybraný provoz směrován



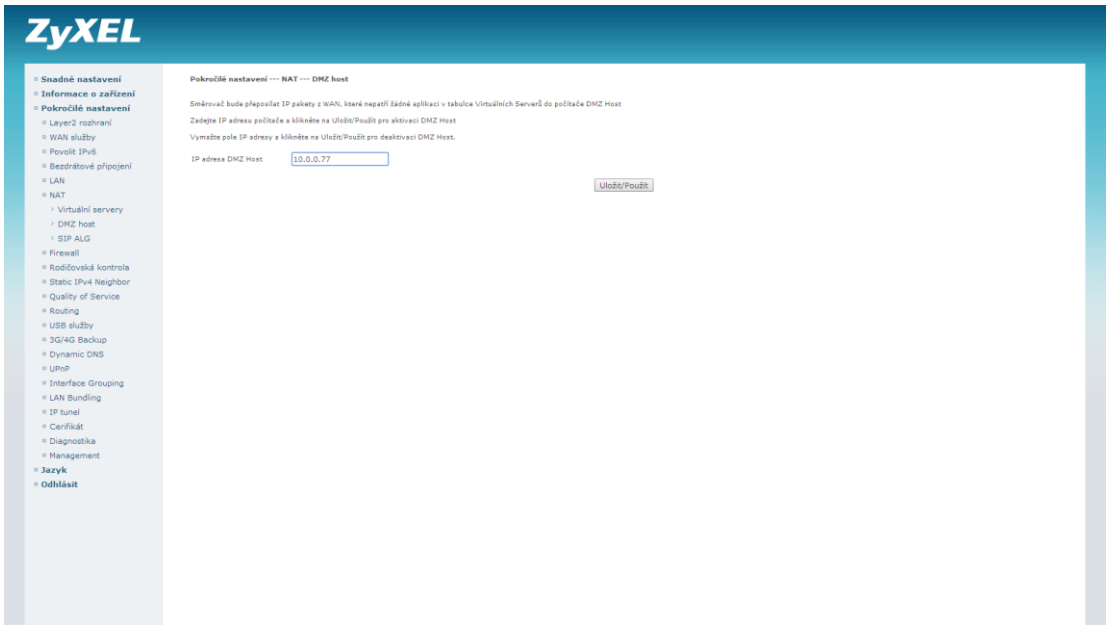
K dispozici je seznam přednastavených sad pro podporu některých aplikací (obr. výše) nebo je možné nastavit Virtuální server ručně. Zvolte možnost **Vlastní služba** a v textovém poli vyplňte název. Zadejte počáteční interní a externí porty, a konečné interní a externí porty, rovněž vyberte požadovaný protokol (UDP, TCP nebo UDP/TCP).



8.3 DMZ Host

Směrovač bude přeposílat IP pakety z WAN, které nepatří žádné aplikaci v tabulce Virtuálních Serverů do počítače DMZ Host. Zadejte IP adresu počítače a klikněte na Uložit/Použít pro aktivaci DMZ Host.

Pro deaktivaci DMZ Host vymažte pole IP adresy a klikněte na Uložit/Použít.



8.4 SIP ALG

Některé routery NAT obsahují aplikační bránu SIP ALG (SIP Application Layer Gateway). Aplikační brána SIP umožňuje průchod internetových hovorů rozhraním NAT (aplikační brána najde a přeloží IP adresy v datovém streamu). Když se zařízení ZyXEL zaregistruje u serveru SIP, přeloží brána ALG privátní IP adresu zařízení uvnitř datového streamu SIP na veřejnou IP dresu. Aplikační brána tak nahrazuje STUN nebo odchozí proxy server.

Na obrazovce **Pokročilé nastavení > NAT > SIP ALG** zapnete a vypnete aplikační bránu SIP (VoIP) ALG. .

9 FIREWALL

9.1 Základní informace

V této kapitole popisujeme, jak zapnout firewallovou ochranu na zařízení ZyXEL. Firewall chrání zařízení a síť před útoky z internetu a kontroluje přístup k zařízení. Ve výchozím nastavení provádí firewall tyto činnosti:

- povoluje průchod dat, které mají svůj zdroj uvnitř sítě LAN, do dalších sítí;
- blokuje průchod dat, které mají svůj zdroj v jiných sítích, do lokální sítě LAN;
- blokuje útoky typu SYN Flood a skenování portů.

Ve výchozím nastavení zařízení ZyXEL blokuje útoky typu DDoS, LAND a „ping smrti“ bez ohledu na to, jestli je firewall zapnutý nebo vypnutý.

9.1.1 Co všechno lze nastavit na obrazovkách Firewall

- Na obrazovce **Obecné** můžete zapnout firewall a nastavit základní pravidlo pro všechny pakety
- Na obrazovce **Pravidla** můžete nastavit pravidla pro jednotlivé aplikace
- Na obrazovce **DoS** můžete aktivovat a deaktivovat ochranu proti DoS útokům a upravit pravidla ochrany.
- Na obrazovce **MAC filter** můžete nastavit filtrovací pravidla na základě MAC adres. Lze použít pouze v případě kdy je zařízení nastaveno v režimu Bridže (přemostění)

9.1.2 Co je třeba vědět o firewallu

Útoky typu SYN

Tento útok zaplaví cílový systém řadou SYN paketů. Každý paket způsobí odeslání odpovědního SYN-ACK paketu. Zatímco cílový systém čeká na paket ACK, všechny dosud nezodpovězené pakety SYN-ACK začne řadit do fronty. Pakety SYN-ACK jsou z fronty smazány teprve tehdy, když systém obdrží paket ACK nebo když vnitřní časový spínač ukončí interval, kdy systém čeká na odpověď. Když je fronta plná, systém začne ignorovat všechny příchozí SYN pakety a stane se tím nedostupným pro legitimní uživatele.

DoS

Útoky typu DoS (Denial of Service, odmítnutí služby) míří na zařízení a sítě s připojením na internet. Cílem útoku není krádež dat, ale snaha omezit či zablokovat funkci síťových zdrojů. Zařízení ZyXEL je z továrny konfigurováno tak, aby automaticky detekovalo a vyřešilo všechny známé útoky DoS.

DDoS

Útok typu DDoS je distribuovaný útok DoS, který je veden větším počtem systémů. Útok se opět snaží znepřístupnit síťové služby pro legitimní uživatele.

Útok typu LAND

Tento útok spočívá v tom, že útočník odešle cílovému systému velký počet záměrně poškozených SYN paketů, které mají falešnou IP adresu stejnou jako cílový systém. Cílový systém odmítne služby legitimním uživatelům, když se snaží komunikovat sám se sebou a zpracovat falešné pakety.

Útok typu „ping smrti“

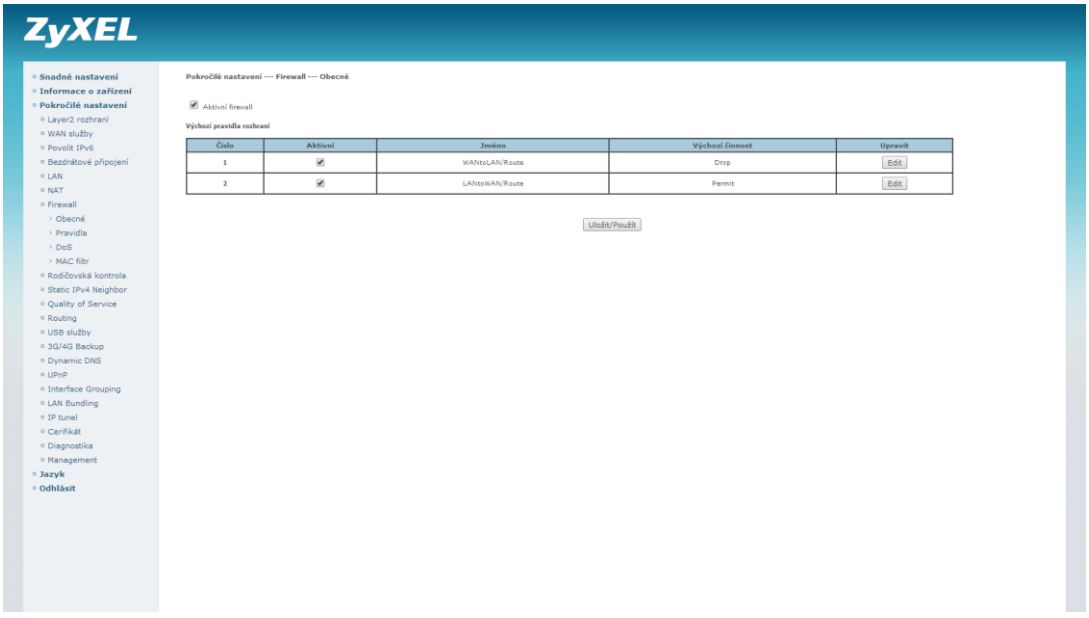
Tento útok využívá utilitu ping k vytvoření a odeslání IP paketu, který má větší velikost než 65 536 bytů, což je mezní hodnota uvažovaná ve specifikacích IP. Velký paket může způsobit zhroucení, zamrznutí nebo rebootování systému.

SPI (stavová kontrola paketů)

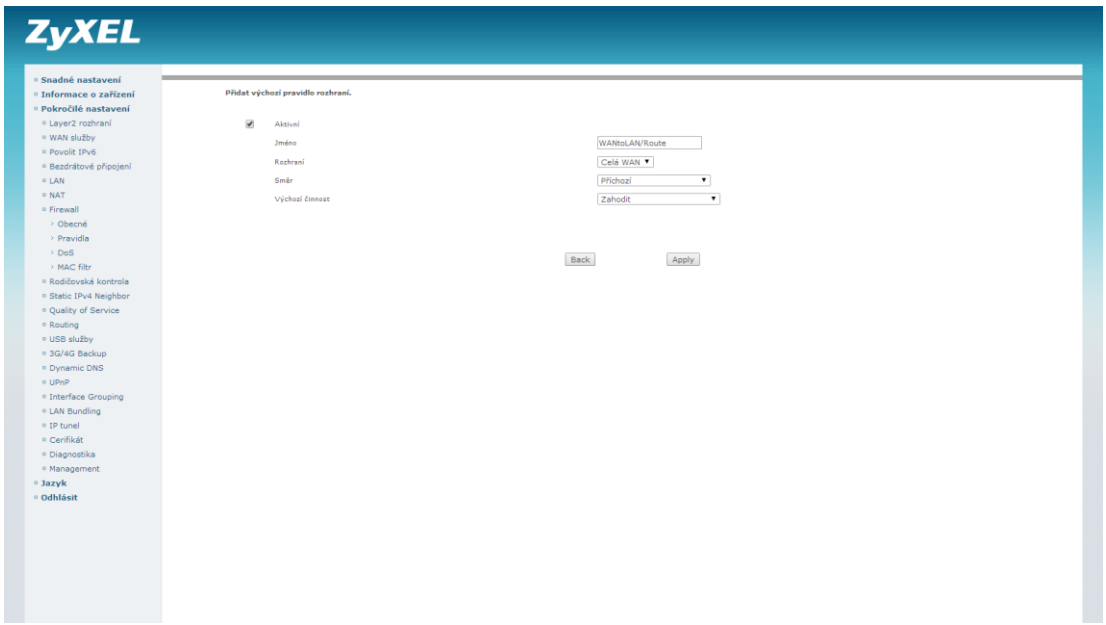
SPI sleduje připojení, které prochází firewallem, a ověřuje jeho platnost. Rozhodnutí o akci jsou založena jak na pravidlech, tak na kontextu. SPI např. povolí průchod dat ze sítě WAN do sítě LAN, pouze pokud jsou odeslána jako odpověď na žádost pocházející ze sítě LAN.

9.2 Zapnutí firewallu

Na obrazovce **Pokročilé nastavení > Firewall > Obecné** můžete zapnout firewall a upravovat jeho obecná pravidla pro příchozí a odchozí směr.



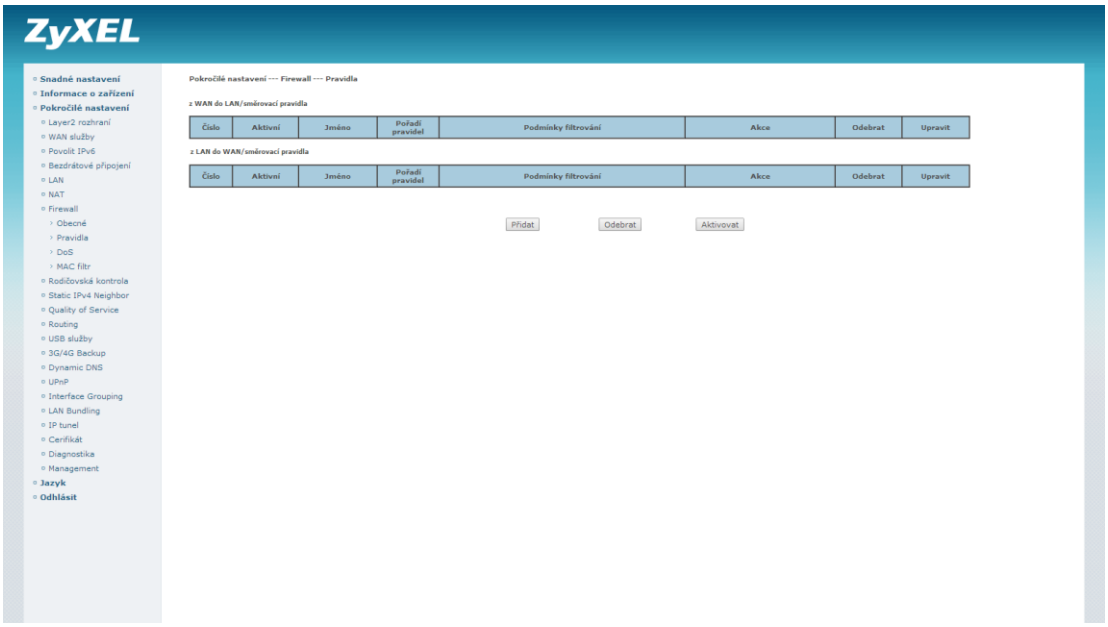
Tlačítkem Edit otevřete okno pro nastavení základních parametrů.



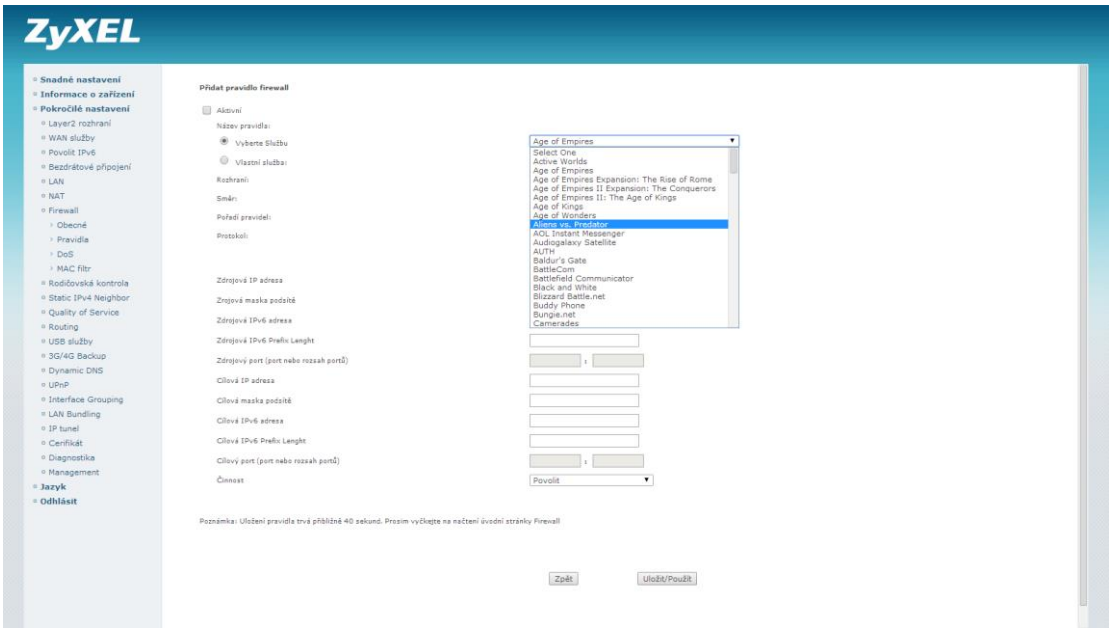
Položka	Popis
Aktivní	Zaškrtnutím tohoto políčka aktivujete výchozí pravidlo
Jméno	Libovolný název pro pravidlo
Rozhraní	Základní pravidla umožňují pouze volbu „Celá WAN“
Směr	Zvolte, pro jaký směr provozu bude pravidlo platné, zda odchozí či příchozí
Výchozí činnost	K dispozici jsou volby „zahodit“ nebo „povolit“

9.3 Pravidla

V této kapitole popisujeme vytváření pravidel pro Firewall

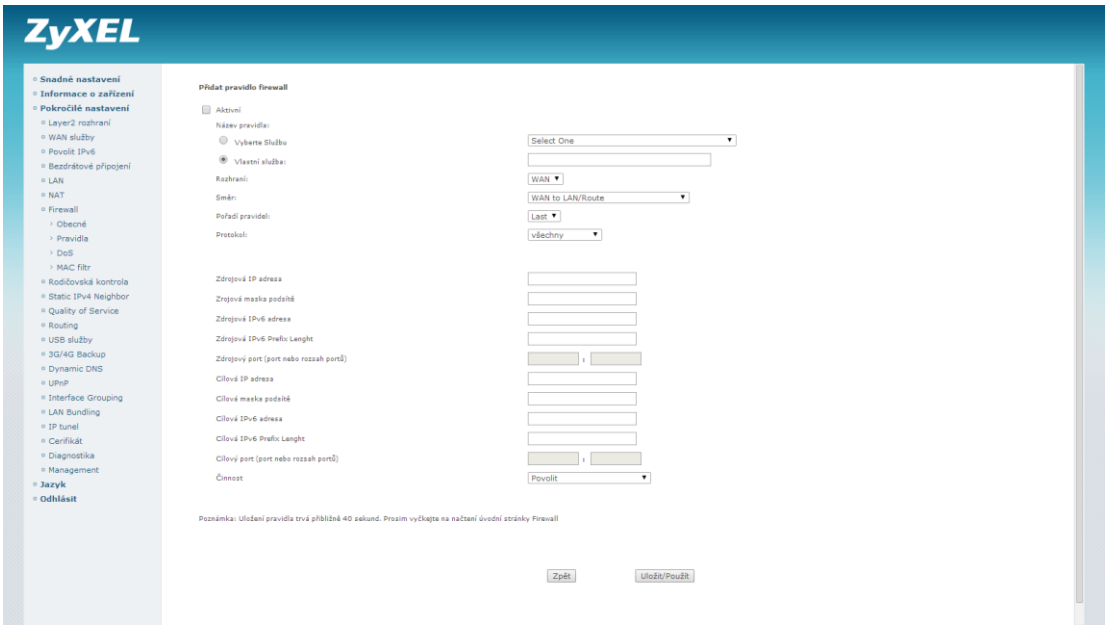


Klikněte na obrazovce **Pravidla** na tlačítko **Přidat**



Pokud je pravidlo vytvářeno za účelem konkrétní aplikace, zkuste aplikaci naléze v seznamu na této stránce. Po výběru aplikace dojde k nastavení všech součástí pravidla. Poté zaškrněte volbu **Aktivní**, zvolte typ činnosti (povolit, zahodit) a klikněte na **Uložit/Použít.**

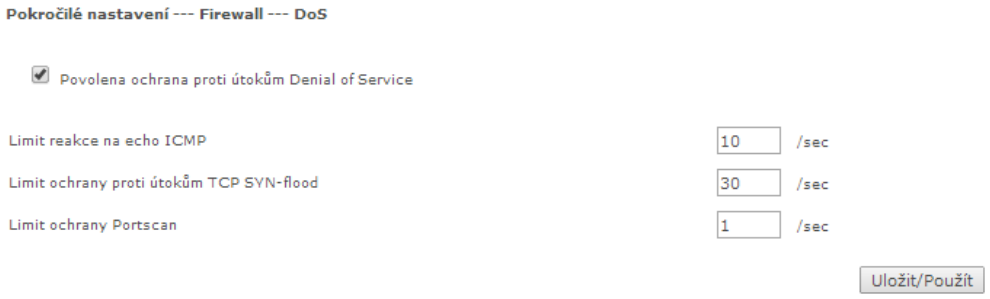
Není-li aplikace v seznamu, nebo si přejete vytvořit vlastní pravidlo, postupujte následovně.. Klikněte na volbu **Vlastní služba** a vyplňtě potřebné údaje.



Položka	Popis
Aktivní	Zaškrtnutím tohoto políčka aktivujete pravidlo
Použít službu/Vlastní služba	Libovolný název pro pravidlo v případě vlastní služby, nebo název služby (Aplikace pro pravidla) při výběru ze seznamu předdefinovaných aplikací.
Rozhraní	Je možno nastavit pravidlo pro WAN, nebo br0
Směr	Při volbě rozhraní WAN je vždy „WAN to LAN“ při volbě br0 pak „LAN to WAN“
Pořadí pravidel	V případě více nastavených pravidel lze nastavit pořadí ve kterém se budou pravidla uplatňovat.
Protokol	Nastavení protokolu. na který se bude pravidlo vztahovat. K dispozici jsou volby: všechny, TCP, UDP, TCP a UDP, ICMP, ICMPv6
Zdrojová IP adresa	IP adresa zdroje komunikace
Zdrojová maska podsítě	Maska podsítě zdroje komunikace
Zdrojová IPv6 adresa	IPv6 adresa zdroje komunikace
Zdrojový IPv6 prefix length	Zdrojové délka IPv6 prefixu
Zdrojový port (port nebo rozsah portů)	Port, nebo rozsah portů zdroje komunikace
Cílová IP adresa	IP adresa cíle komunikace
Cílová maska podsítě	Maska podsítě cíle komunikace
Cílová IPv6 adresa	IPv6 adresa cíle komunikace
Cílový prefix length	Cílová délka IPv6 prefixu
Cílový port (port nebo rozsah portů)	Port, nebo rozsah portů cíle komunikace
Činnost	K dispozici jsou volby: Povolit/Zahodit/Odmítnout

9.4 DoS

V této kapitole popisujeme nastavení ochrany proti DOS (Denial of Service) útokům.

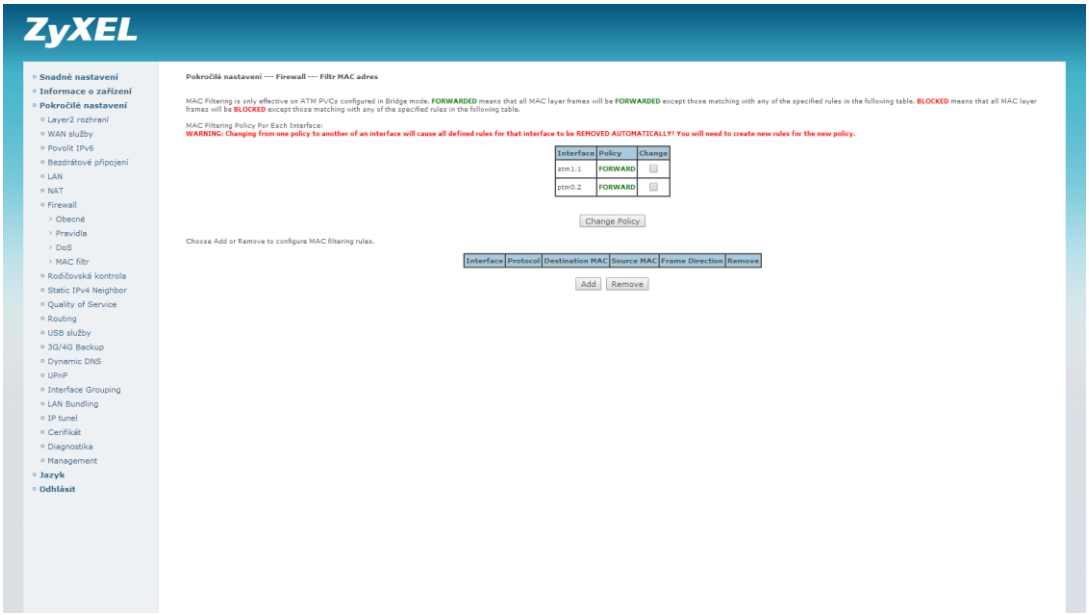


Nastavením ochranných limitů pro echo ICMP, TCP SYN-flood a Portscan omezíme počty požadavků na zařízení aby nedošlo k jeho zahlcení.

9.5 MAC filtr

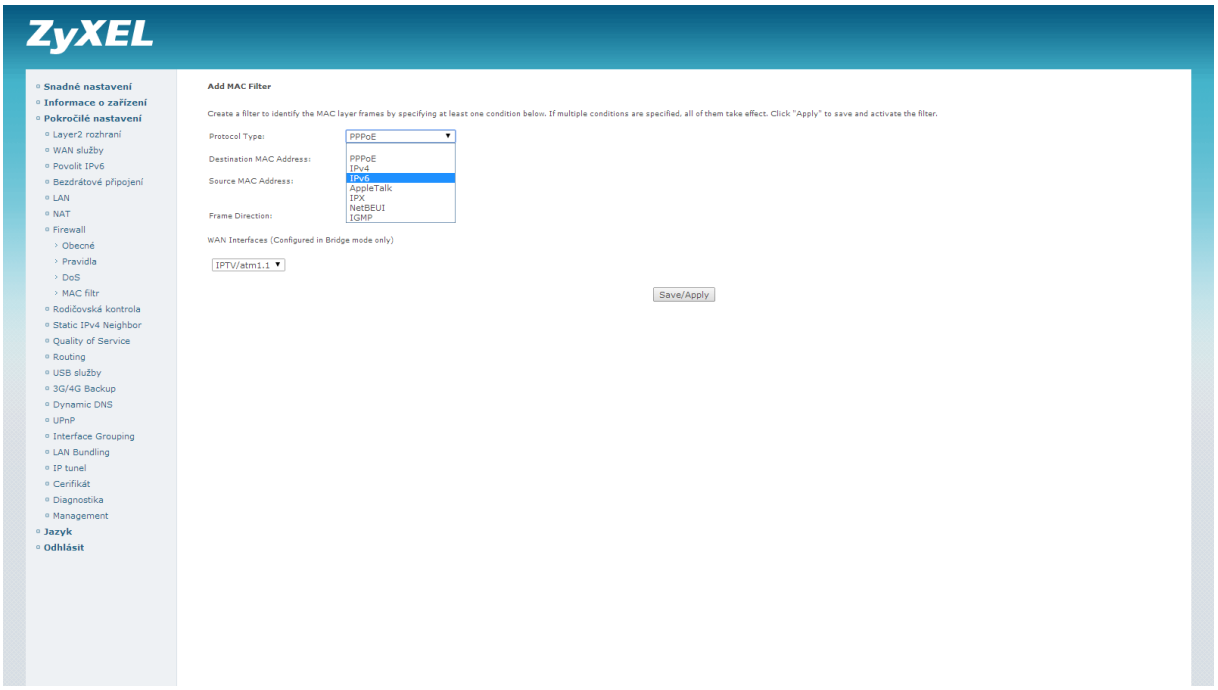
Na obrazovce můžete vytvářet pravidla pro filtrování dat na základě MAC adresy k dané oblasti (policy). Pozor, pokud chcete vytvořit novou oblast, v původní oblasti se všechna pravidla odstraní a bude třeba je znovu vytvořit.

Poznámka: MAC Filtr je možné aplikovat pouze s WAN rozhraním nastaveným do Bridže režimu



Chcete-li přidat pravidlo, klikněte na tlačítko **Add**

Vyberte požadovaný protokol, pro který budete pravidlo nastavovat.



Jako příklad jsme zvolili protokol IPv6. Zadejte cílovou a zdrojovou MAC adresu.



A následně zvolte směr provozu pro pravidlo a nastavte rozhraní (atm pro ADSL nebo PTM pro VDSL). Pravidlo uložíte kliknutím na **Save/Apply**



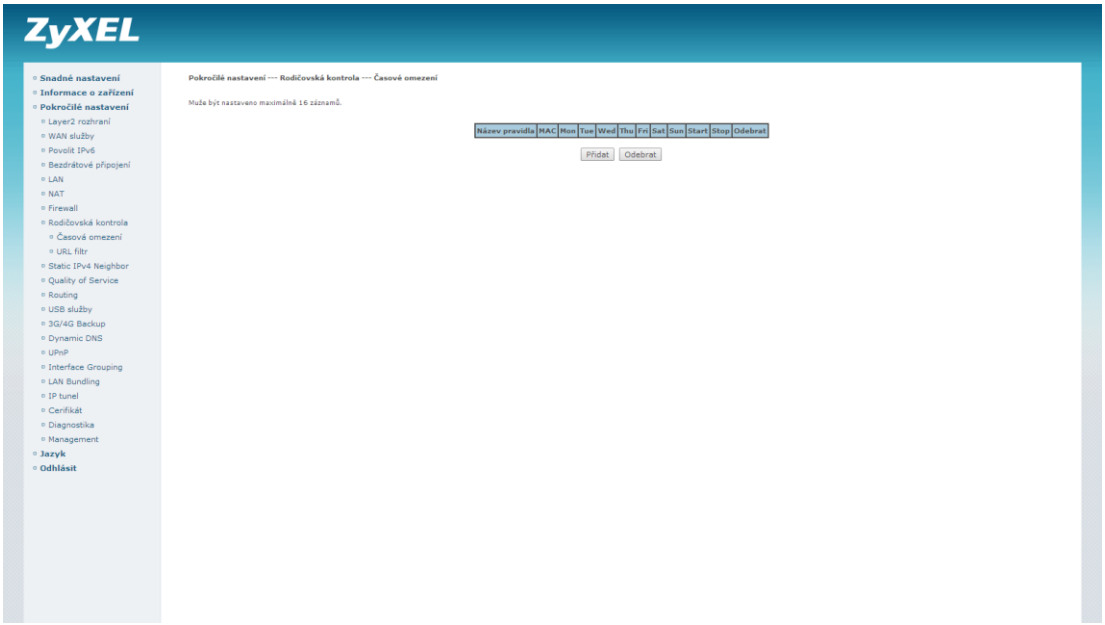
10 RODIČOVSKÁ KONTROLA

V této kapitole popisujeme dva způsoby, kterými lze zařízení zabezpečit před neúměrným užíváním Internetu a zamezit zobrazení nevhodného obsahu

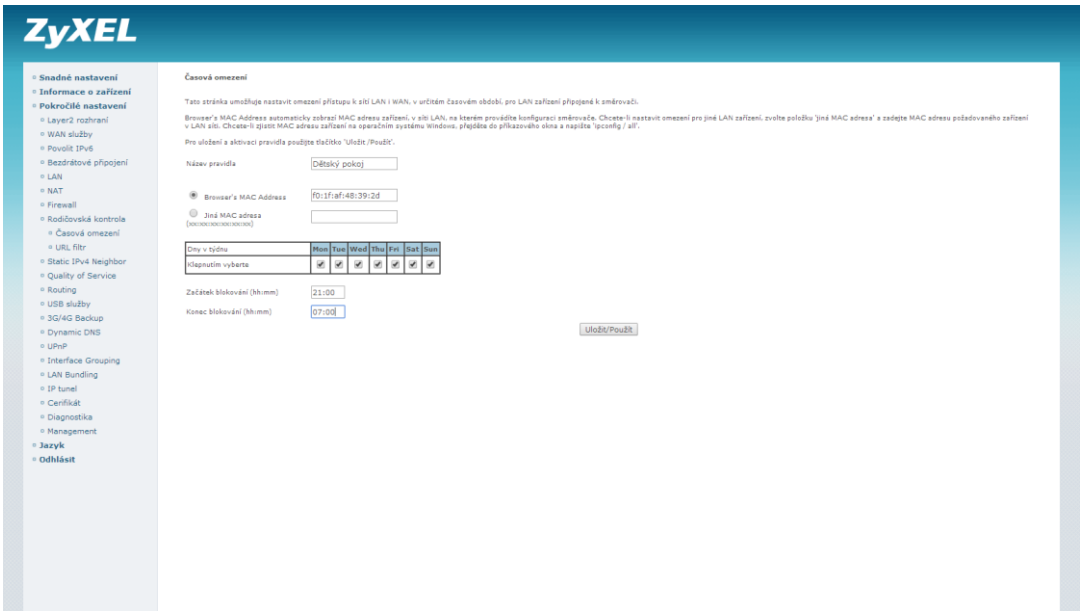
10.1 Časové omezení

Na následující obrazovce lze zapnout omezení určitých klientských zařízení po určitou dobu. (například zamezení používání počítače v dětském pokoji v nočních hodinách). Obrazovku zobrazíte kliknutím na **Pokročilé nastavení > Rodičovská kontrola > Časová omezení**

Pro přidání omezení klikněte na tlačítko **Přidat**



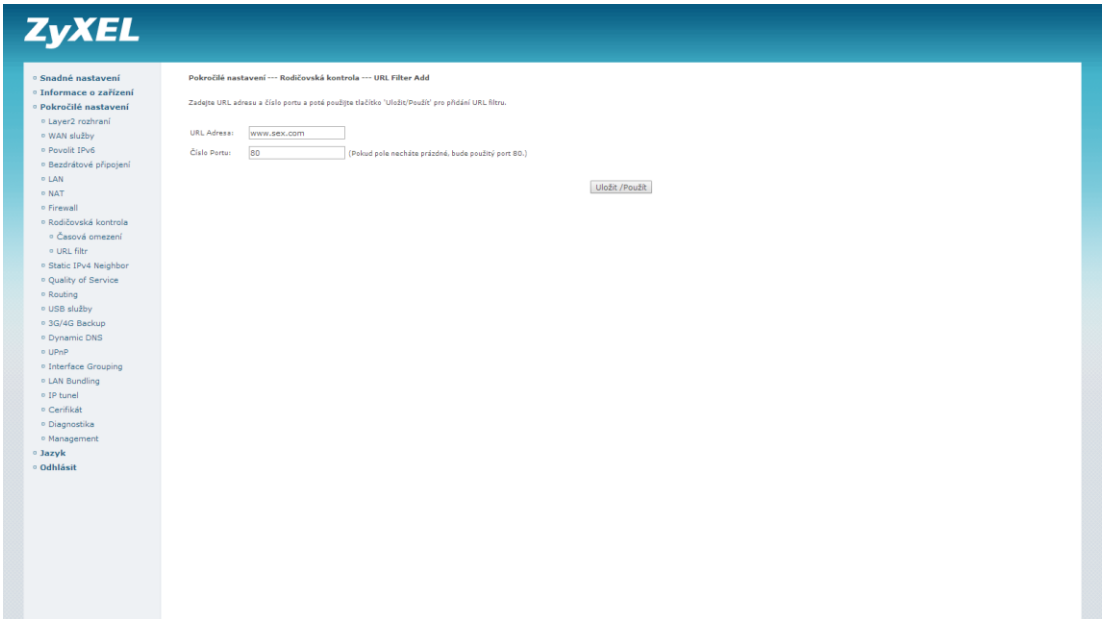
Otevře se okno pro nastavení pravidla. Zadejte **Název pravidla** a MAC adresu klientského zařízení (například počítače – pokud omezujete počátač, ze kterého pravidlo konfigurujete, je MAC adresa nabídnuta a lze ji rovnou zvolit). Dále nastavte dny v týdnu a časy, po které nebude připojení dostupné. Pravidlo nastavíte kliknutím na **Uložit/Použít**



10.2 Filtrování podle adres URL

Na obrazovce můžete blokovat nebo povolovat určité webové stránky (přes jejich URL adresu). Obrazovku otevřete kliknutím na **Pokročilé nastavení > Rodičovská kontrola > URL Filtr**. Lze vytvořit až 100 záznamů. Nejprve vyberte typ pravidla (Povolit/Zakázat) a následně klikněte na tlačítko **Přidat**

Zadejte adresu, kterou požadujete blokovat (nebo povolit) a číslo portu. Pokud nebude port definován, automaticky se nastaví na hodnotu 80.

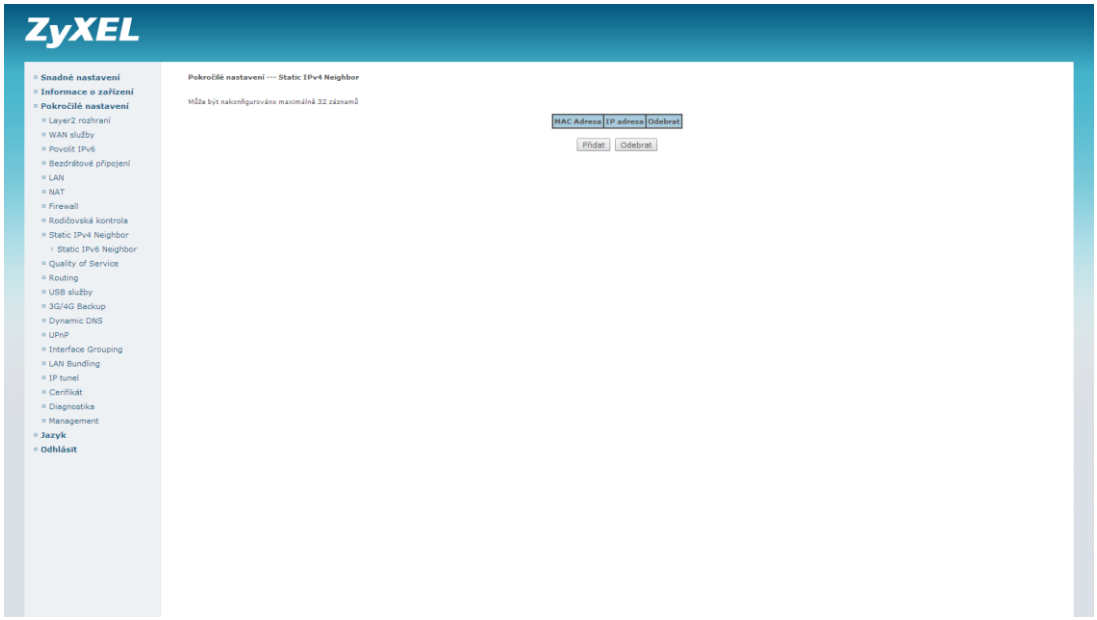


11 STATIC IPV4 NEIGHBOR

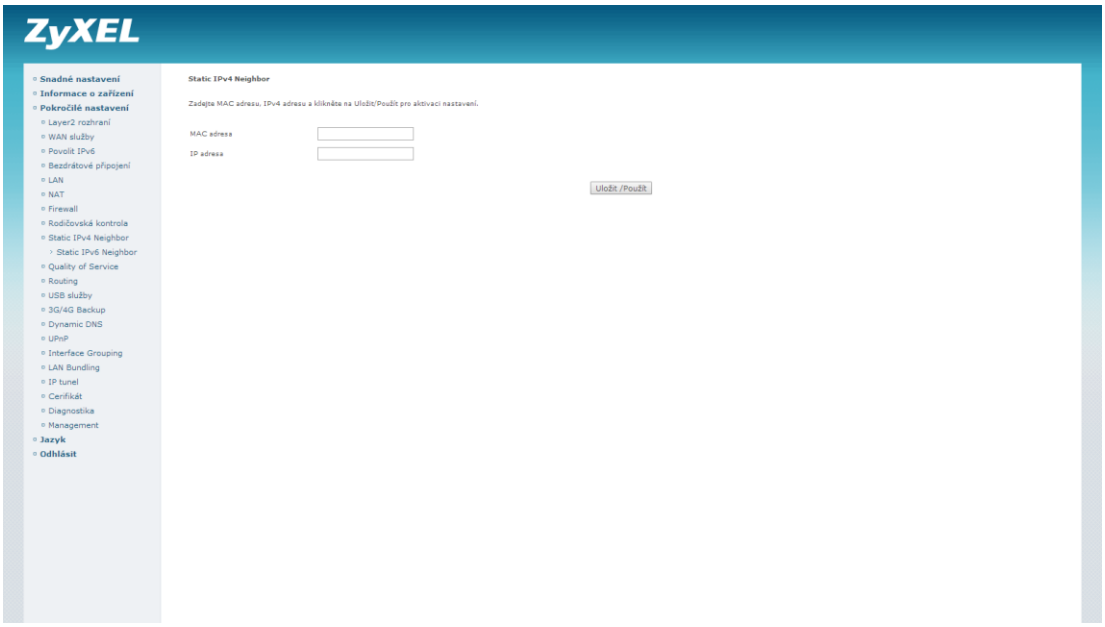
Static IPv4/IPv6 Neighbor je rozpoznání okolních zařízení v síti LAN, tedy „sousedských“ zařízení a přidělení statických údajů. Obrazovku zobrazíte kliknutím na **Pokročilé nastavení > Static IPv4 Neighbor**

11.1 Static IPv4 neighbor

Na této obrazovce nastavíte klientské zařízení, používající v síti LAN protokol IPv4. Pro nastavení klikněte na tlačítko **Přidat**



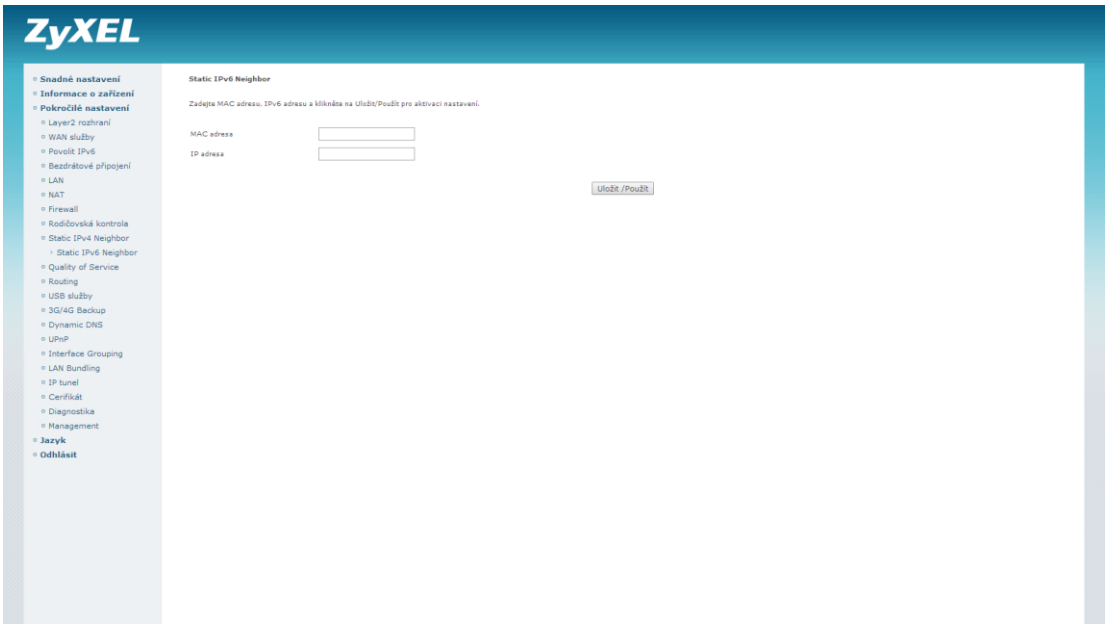
Otevře se okno, kde nastavíte MAC adresu a IP adresu klientského zařízení. Konfiguraci uložíte klinknutím na **Uložit/Použít**



11.2 Static IPv6 neighbor

Na této obrazovce nastavíte klientské zařízení komunikující přes protokol IPv6. Klikněte na **Pokročilé nastavení > Static IPv4 Neighbor > Static IPv6 Neighbor.** Pro nastavení klikněte na tlačítko **Přidat**

Otevře se okno, kde nastavíte MAC adresu a IP adresu klientského zařízení. Konfiguraci uložíte klinknutím na **Uložit/Použít**

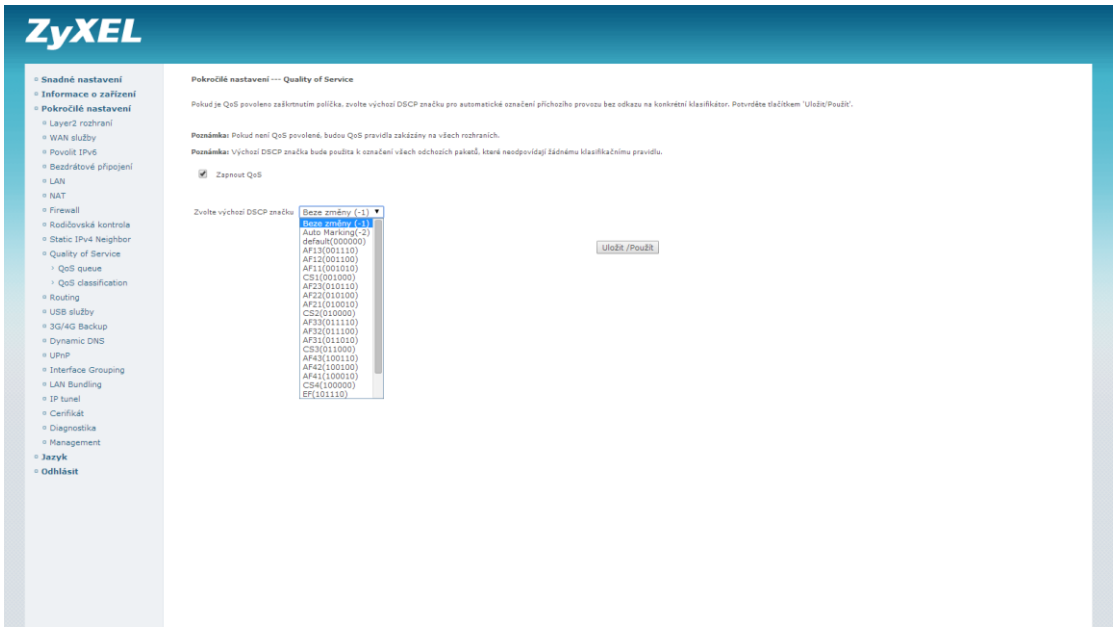


12 QUALITY OF SERVICE

Quality of Service je označení pro nastavení prioritizace provozu na základě identifikace typu provozu, protokolu nebo rozraní. Na obrazovku se dostanete kliknutím na **Pokročilé nastavení > Quality of Service.**

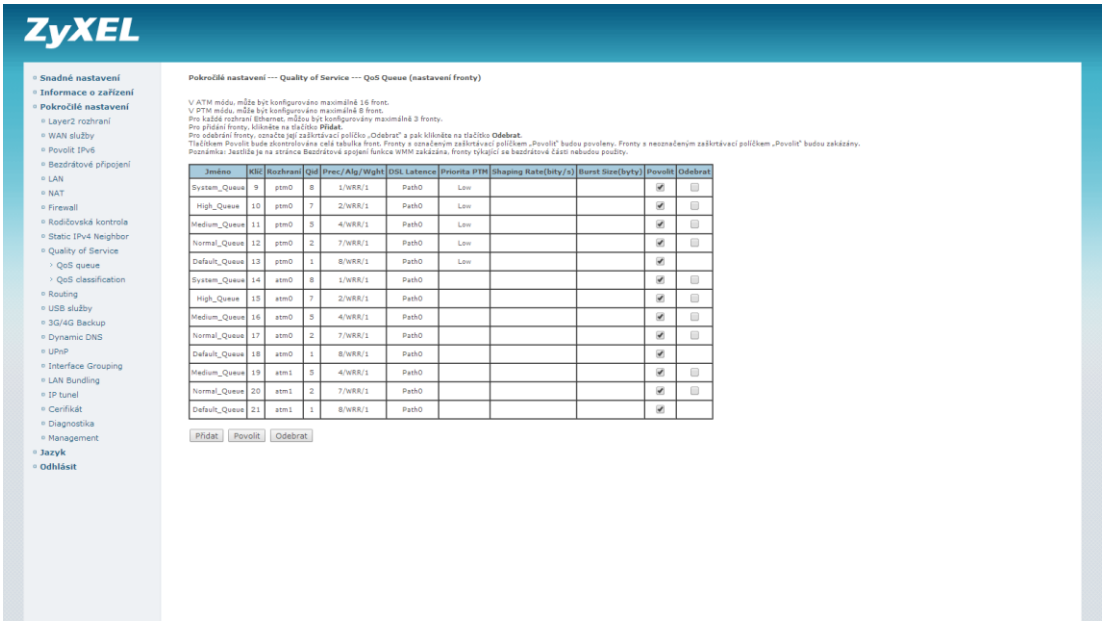
12.1 Quality of Service

QoS aktivujete zaškrtnutím políčka **Zapnout QoS** (v továrním nastavení je zaškrtnuto). Na této obrazovce je možné zvolit také obecnou prioritu pro neklasifikovaný provoz.



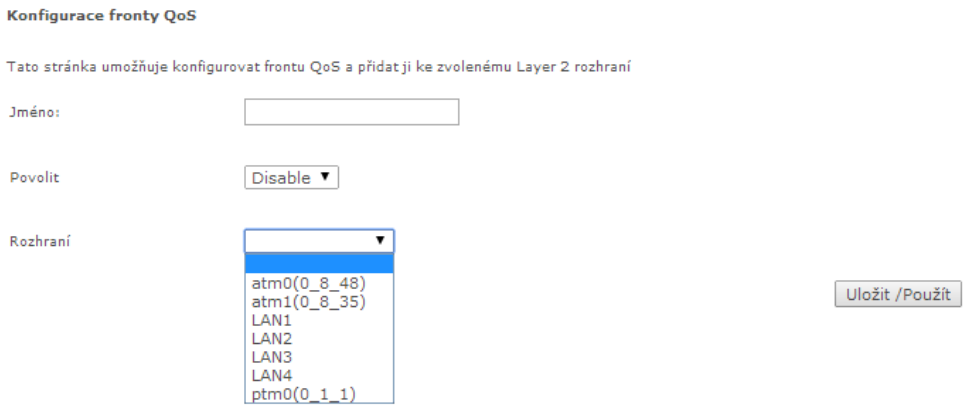
12.2 QoS Queue

Na této obrazovce vidíte seznam předdefinovaných QoS pravidel. Na obrazovce můžete zaškrtnutím příslušného plíčka QoS pravidlo povolit nebo odebrat.

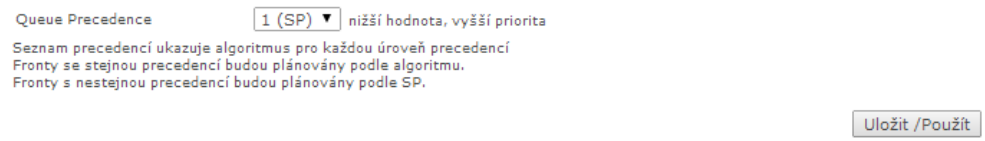


Chcete-li přidat nová pravidla, klikněte na tlačítko **Přidat.**

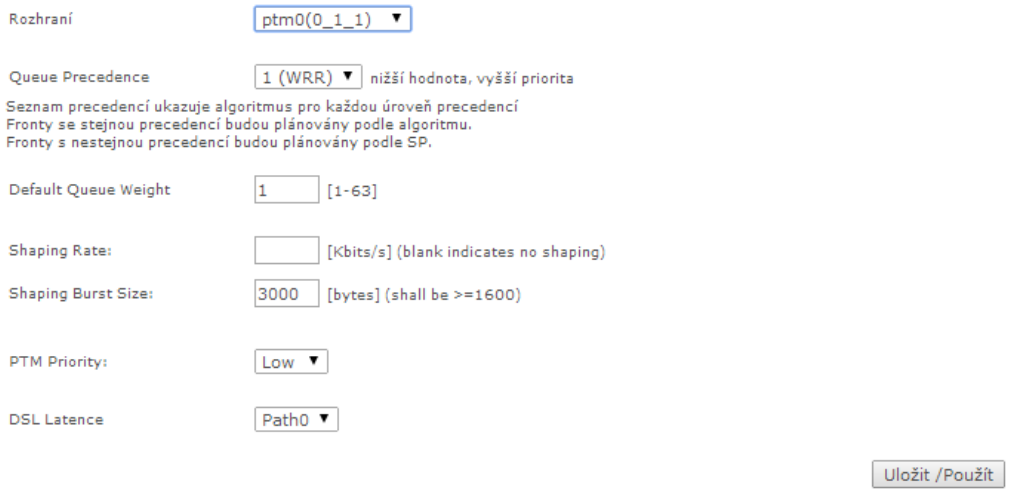
V otevřené obrazovce nastavíte údaje pro nové QoS pravidlo. Podle výběru rozhraní se zobrazí příslušné volby.



Jako přiklad zvolíme rozhraní LAN4 a vybereme hodnotu precedence. Čím nižší hodnota, tím vyšší priorita

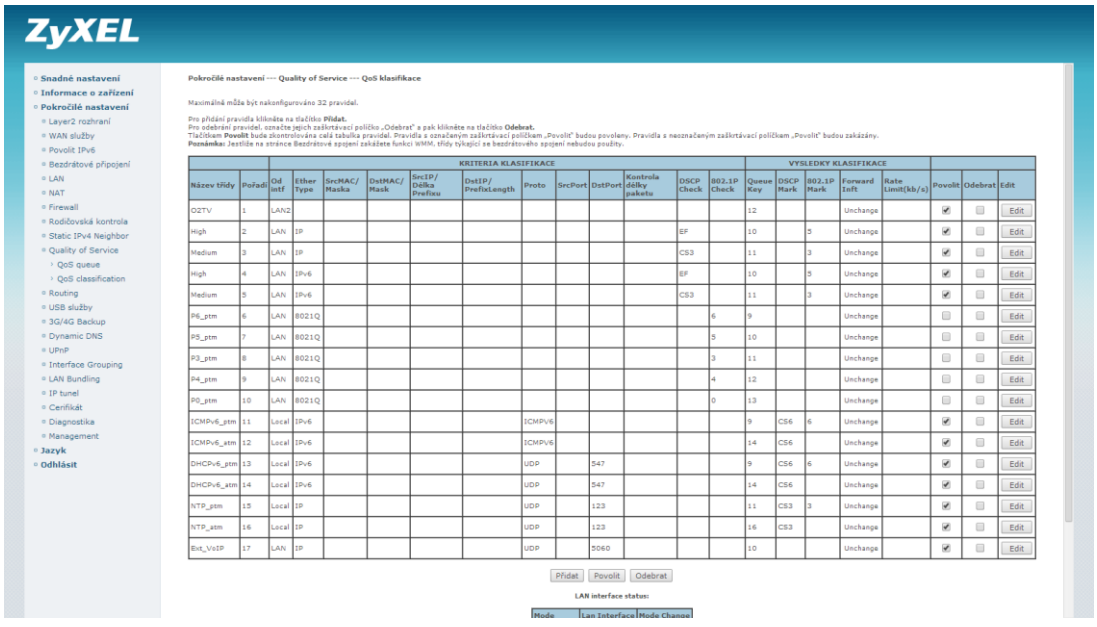


Jako další příklad vybereme rozhraní ptm0 (VDSL WAN rozhraní). Zde krom precedence nastavíme také váhu pravidla (čím nižší, tím vyšší váha neboli pořadí v důležitosti pravidla) Dále **shaping rate** (od jaké šíře pásma se začne prioritizace uplatňovat a také od jaké velikosti **Bust size,** obecnou PTM prioritu (low/mid/high) a DSL latenci. Uložíme kliknutím na **Uložit/Použít**

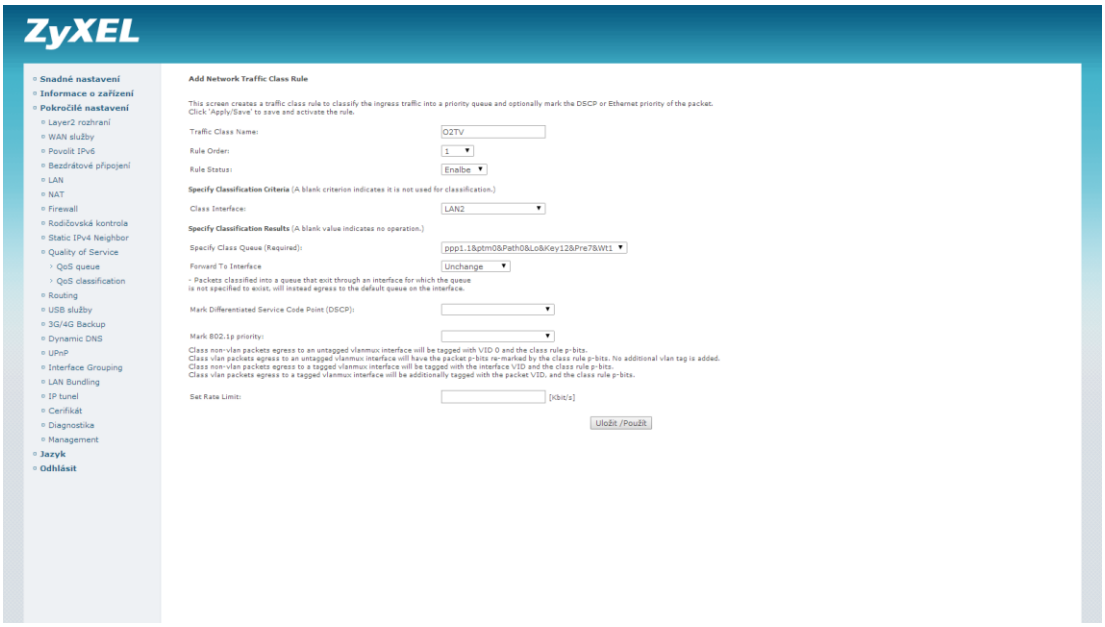


12.3 QoS Classification

Na této stránce lze vytvořená pravidla klasifikovat. Níže vidíte seznam pravidel a jejich klasifikací. Chcete-li klasifikaci změnit, klikněte na tlačítko **Edit.** Nové pravidlo vytvořte kliknutím na **Přidat.**



Po kliknutí na **Edit** se zobrazí následující obrazovka. Jako příklad jsme zvolili pravidlo O2TV.



Vysvětlení pojmů

Položka	Popis
Traffic class name	Název pravidla
Rule order	V jakém pořadí se pravidlo uplatňuje oproti ostatním (1=první, last = poslední)
Rule status	Stav pravidla. Enable = zapnout, Disable = vypnout
Class interface	Pro jaké rozhraní se pravidlo aplikuje
Specify class Qeue (required)	Specifikuje frontu a třídu pro dané pravidlo
Forward to interface	Skrz jaké rozhraní bude provoz odcházet. (není-li vyplněno, bude stejné jako zdrojové)
Mark Differentiated Service Code Point (DSCP)	Vyberte hodnotu DSCP, chcete li používat prioritizaci na bázi DSCP markingu. Pro správné fungování je potřeba, aby funkci DSCP marking podporovalo i klientské zařízení (například IP Telefon)
Mark 802.1p priority	Použijte označování paketů dle standardu 802.1p (QoS)
Set rate limit	Nastavte limit šíře pásma, která bude vyhrazena pro provoz služby, pro kterou pravidlo definujeme

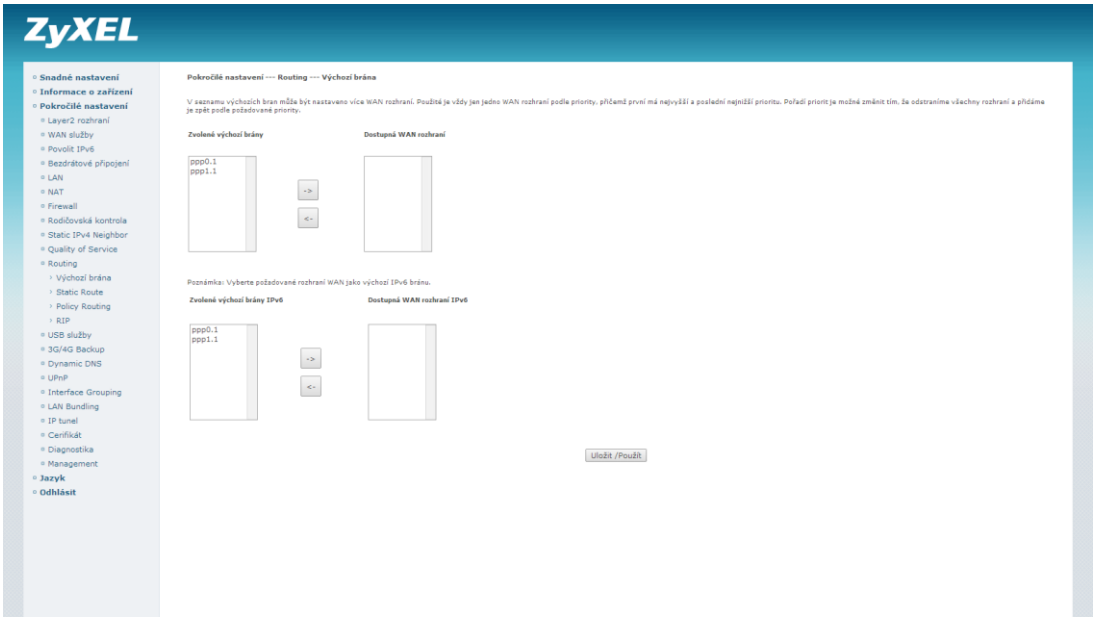
13 ROUTING

V této kapitole se věnujeme nastavení routingu (směrování provozu) zařízení.

Na obrazovku se dostaneme kliknutím na **Pokročilé nastavení > Routing**

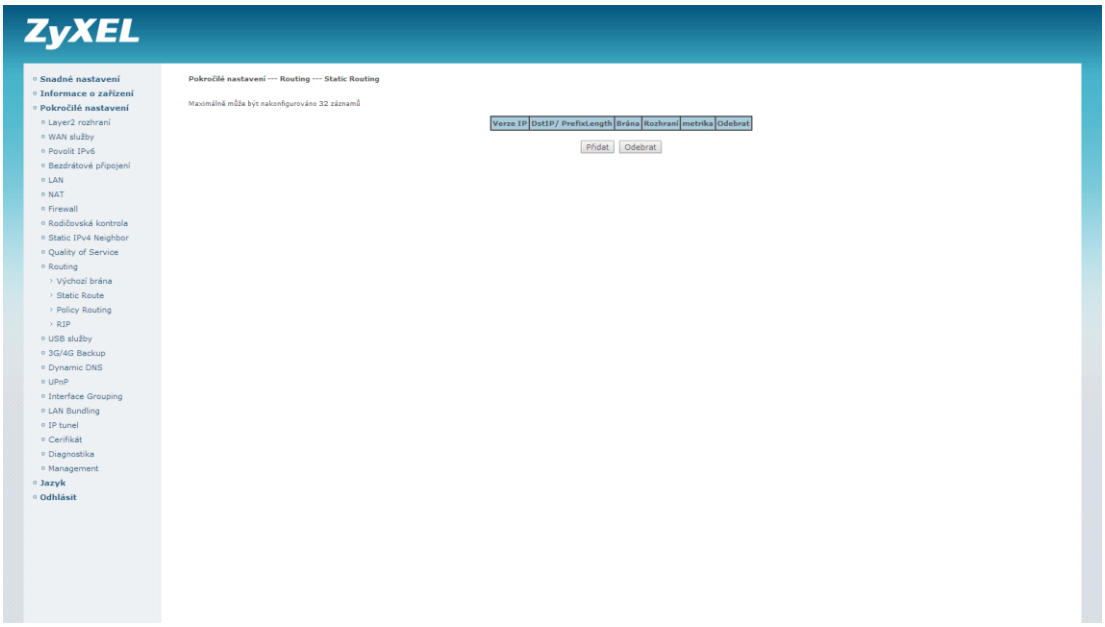
13.1 Výchozí brána

V seznamu výchozích bran může být nastaveno více WAN rozhraní. Použité je vždy jen jedno WAN rozhraní podle priority, přičemž první má nejvyšší a poslední nejnižší prioritu. Pořadí priorit je možné změnit tím, že odstraníme všechny rozhraní a přidáme je zpět podle požadované priority. Nastavení uložíte kliknutím na **Uložit/Použít.**

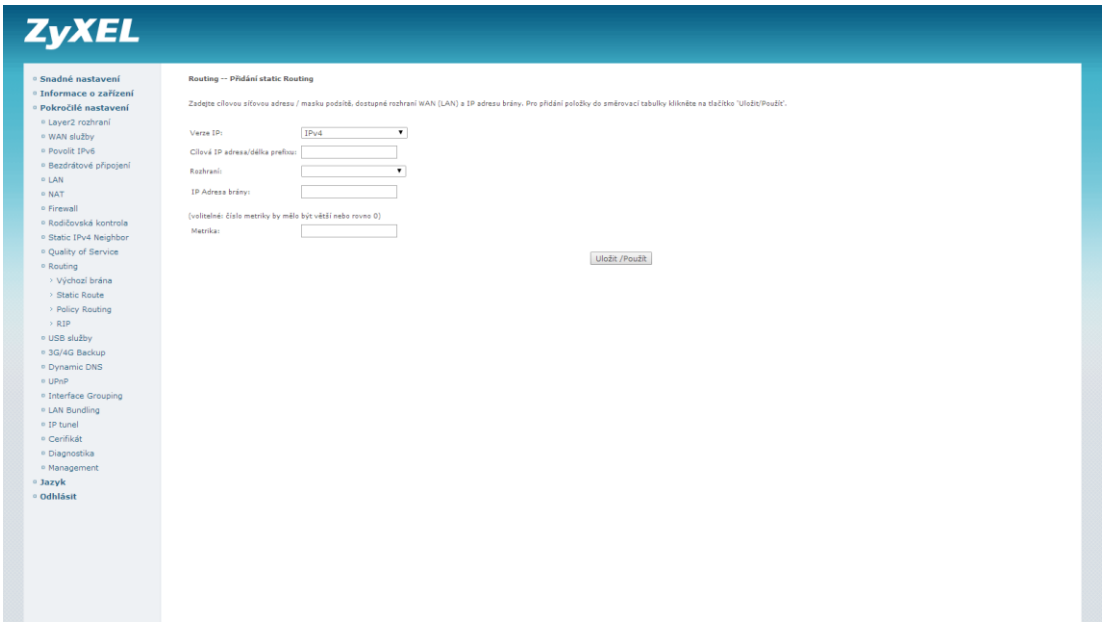


13.2 Static Route

Statická routa je definice brány, která určuje, kde se nachází cíl daného provozu**.** Nový záznam přidáte kliknutím na tlačítko **Přidat**

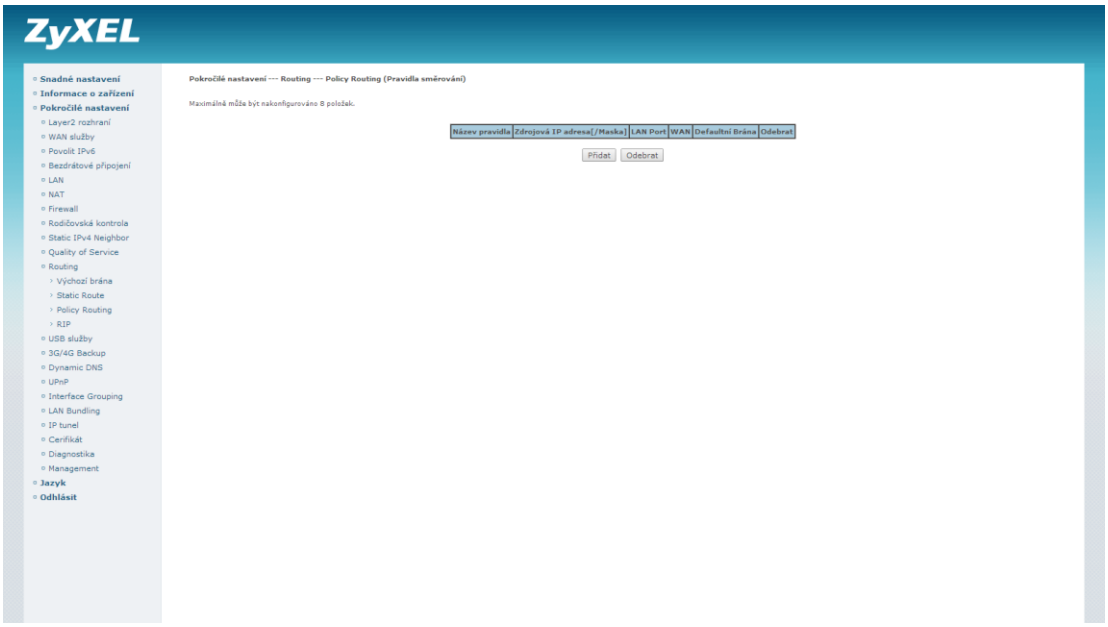


Na obrazovce definujte vlastnosti statické routy. Zvolte typ IP (IPv4 nebo IPv6), cílovou IP adresu, IP adresu brány a rozhraní, popřípadě metriku routy.

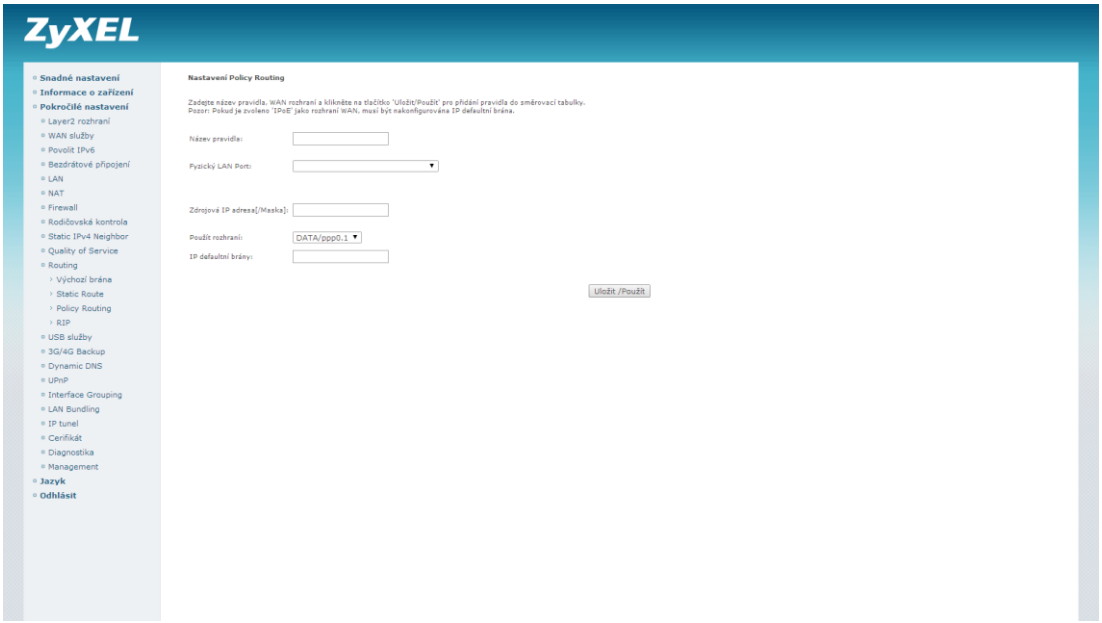


13.3 Policy routing

Policy routing definuje routovací pravidla pro zařízení s ohledem na typ provozu**.** Nový záznam přidáte kliknutím na tlačítko **Přidat**



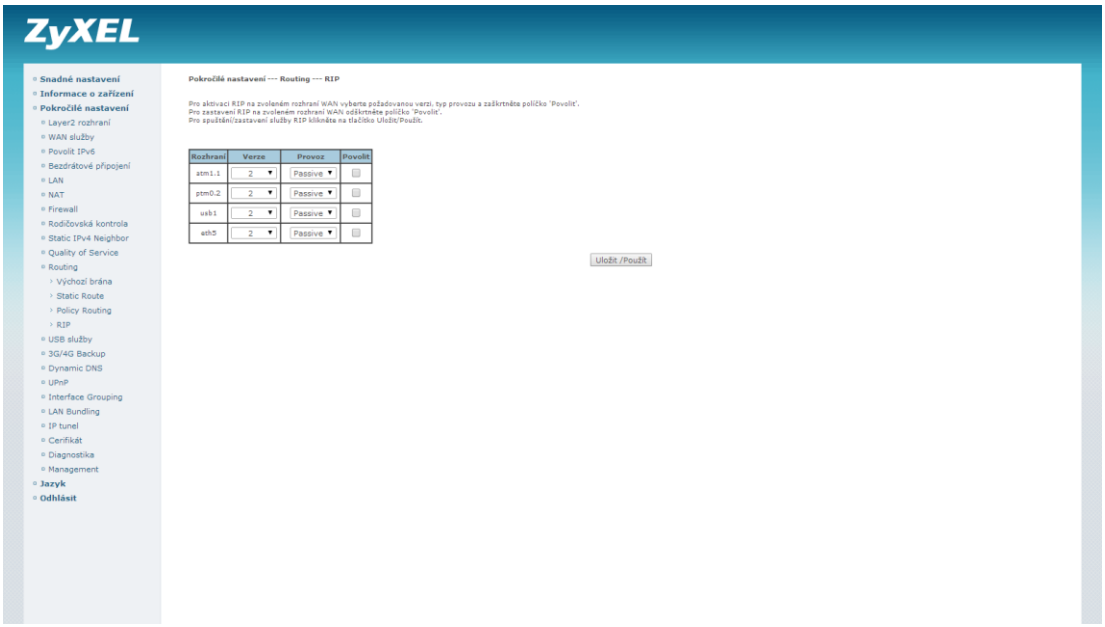
Na následující obrazovce zvolíte název pravidla, definujete LAN port pro který se bude pravidlo vztahovat, zdrojovou IP adresu/masku, IP adresu brány a použitý protokol.



13.4 RIP

Routing Information Protocol (RIP) je v informatice směrovací protokol umožňující směrovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě.

Na následující obrazovce jsou k dispozici RIP pravidla pro jednotlivá rozhraní, zde můžete definovat verzi RIP, typ provozu a zda je pro dané rozhraní RIP povolen.



14 USB SLUŽBY

V této kapitole se věnujeme nastavení USB služeb, které zařízení podporuje. Pro přístup ke konfiguraci klikněte na **Pokročilé nastavení > USB Služby**

14.1 Sdílení souborů

Zařízení podporuje funkci sdílení souborů na síti z USB disku připojeného k zařízení. Detekované USB disky jsou uvedené v tabulce připojených USB disků na obrazovce **Informace o zařízení > USB** nebo **Pokročilé nastavení > USB Služby > Sdílení souborů**.

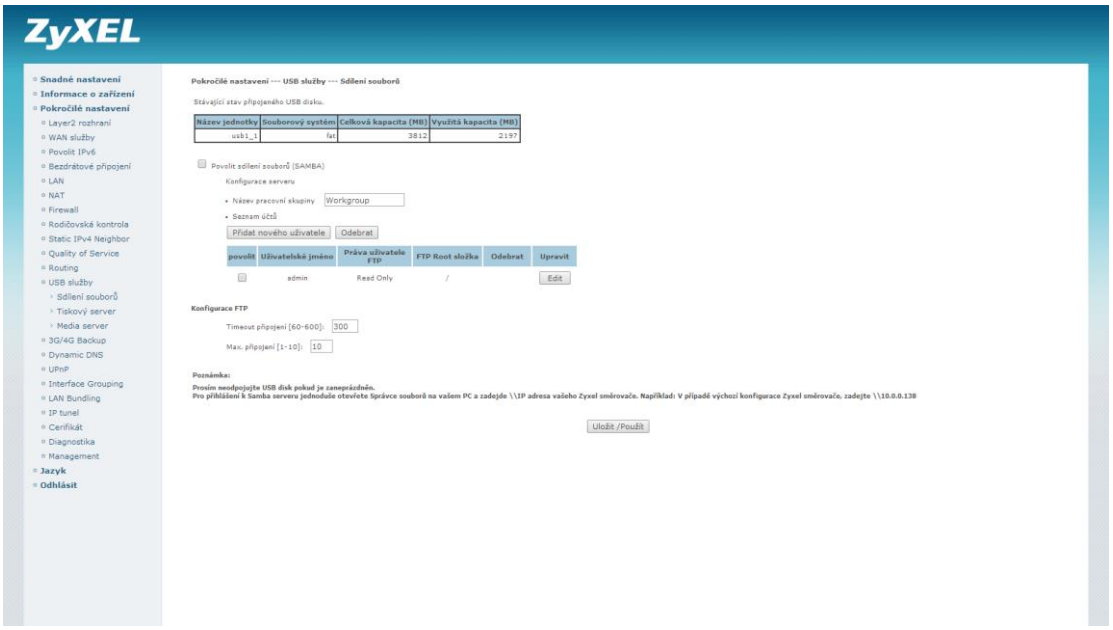
Pro aktivaci sdílení pomocí služby Samba zaškrtněte políčko **Povolit sdílení souborů (SAMBA)** a povolte nebo vytvořte uživatele (uživatelský účet) s právem přístupu na sdílené uložiště. Ve výchozí konfiguraci je přednastaven uživatel admin (odpovídá uživateli admin pro správu modemu).

Služba FTP je zprovozněná trvale a pro její využití je potřeba pouze povolit nebo vytvořit uživatele (uživatelský účet) s právem přístupu k FTP serveru. Ve výchozí konfiguraci je přednastaven uživatel admin (odpovídá uživateli admin pro správu modemu).

Pro vytvoření dalšího uživatelského účtu klikněte na tlačítko **Přidat nového uživatele** a v otevřeném okně zadejte **Uživatelské jméno** a **Heslo.** V případě že potřebujete omezit přístup pro FTP služby, nastavte požadované parametry týkající se **Práv uživatele FTP** (pouze čtení nebo čtení i zápis) a **FTP root složka** (omezení přístupu na vybraný adresář). Tyto parametry se týkají pouze FTP a nemají žádný vliv na sdílení pomocí Samba.

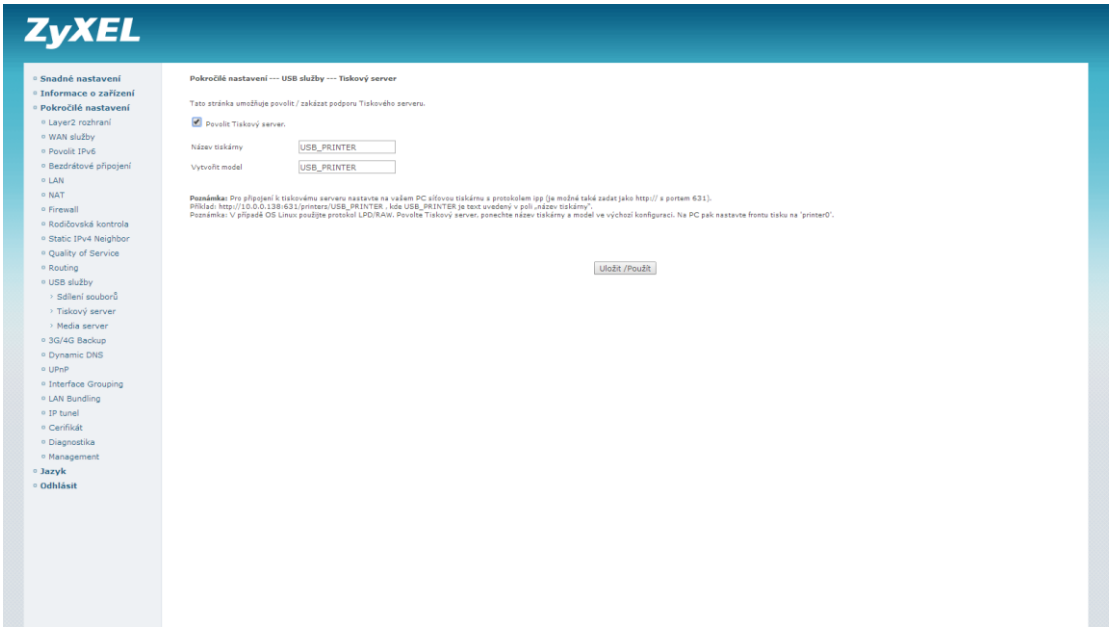
Nastavené uživatelské účty můžete povolit nebo zakázat pomocí položky Povolit, upravovat pomocí tlačítka Edit nebo smazat pomocí nabídky Odebrat

Pro uložení konfigurace klikněte na **Uložit/Použít.**



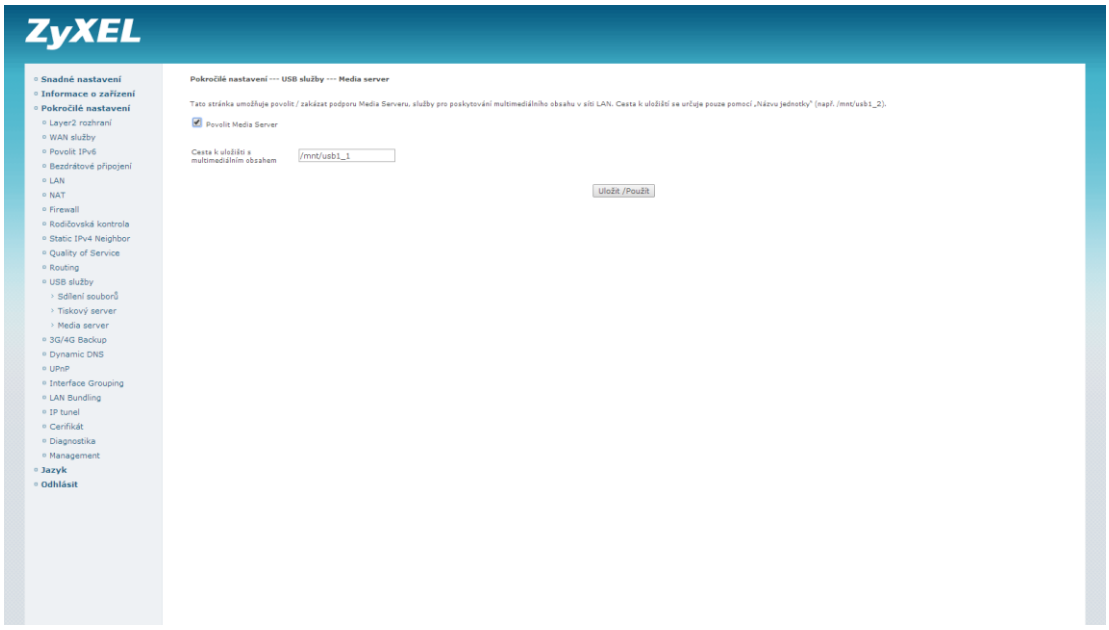
14.2 Tiskový server

Zařízení podporuje funkci tiskového serveru. Po připojení tiskárny a zaškrtnutí políčka **Povolit Tiskový server** je třeba definovat název tiskárny a definovat model (jaký název tiskárny bude zobrazován směrem do vnitřní sítě ostatním počítačům) Změny uložíte kliknutím na **Uložit/Použít.**



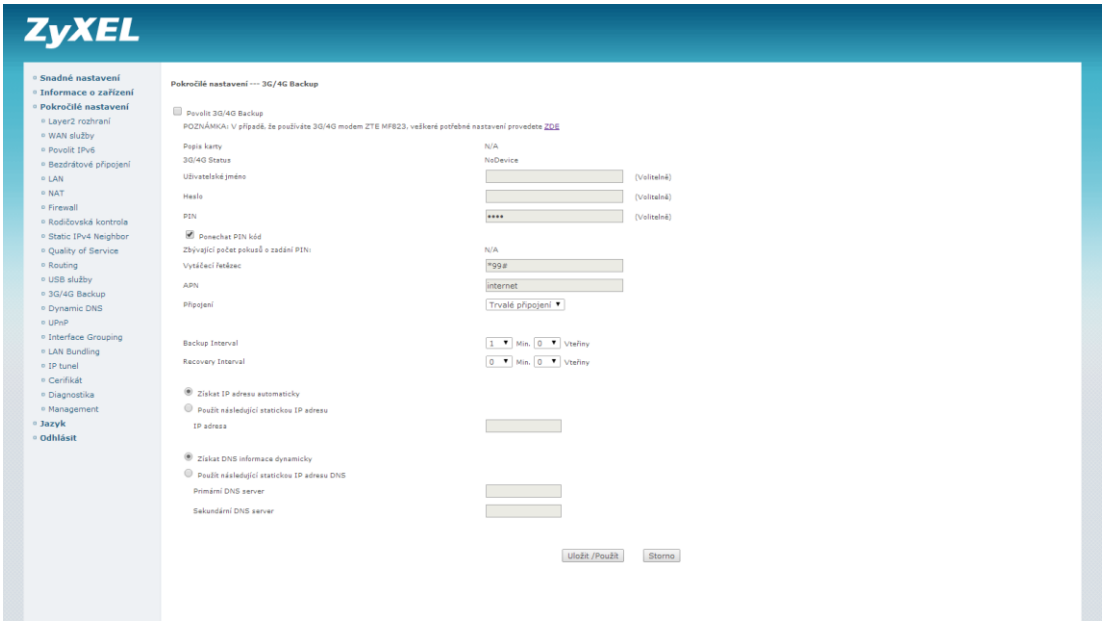
14.3 Media server

Zařízení podporuje funkci media serveru dle standardu DLNA. Multimediální soubory na USB disku je pak možno zobrazit nebo přehrávat v zařízeních s podporou DLNA (např. Smart TV nebo tablet). Aktivujete zaškrtnutím políčka **Povolit Media Server** popř. nadefinováním umístění USB disku (předdefinováno) Změny uložíte kliknutím na **Uložit/Použít.**



14 3G/4G BACKUP

Zařízení podporuje funkci záložního připojení přes mobilní sítě. Podpora standardů je odvislá od použitého 3G/4G modemu. Na obrazovku se dostanete kliknutím na **Pokročilé nastavení > 3G/4G backup.** Funkci aktivujete zaškrtnutím políčka **Povolit 3G/4G backup.**

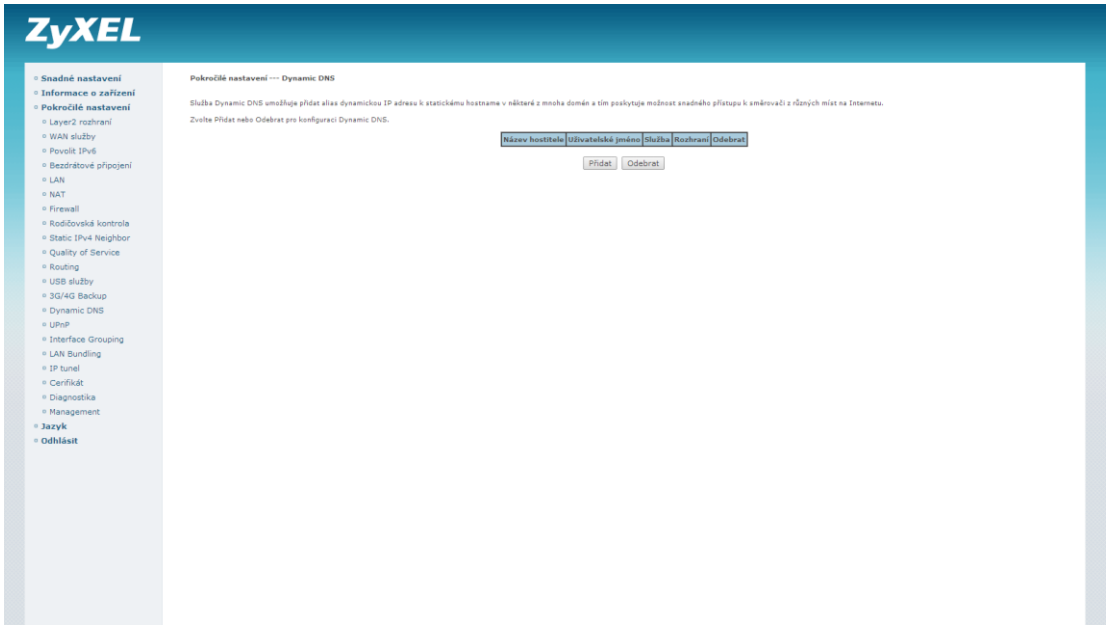


Vysvětlení pojmů

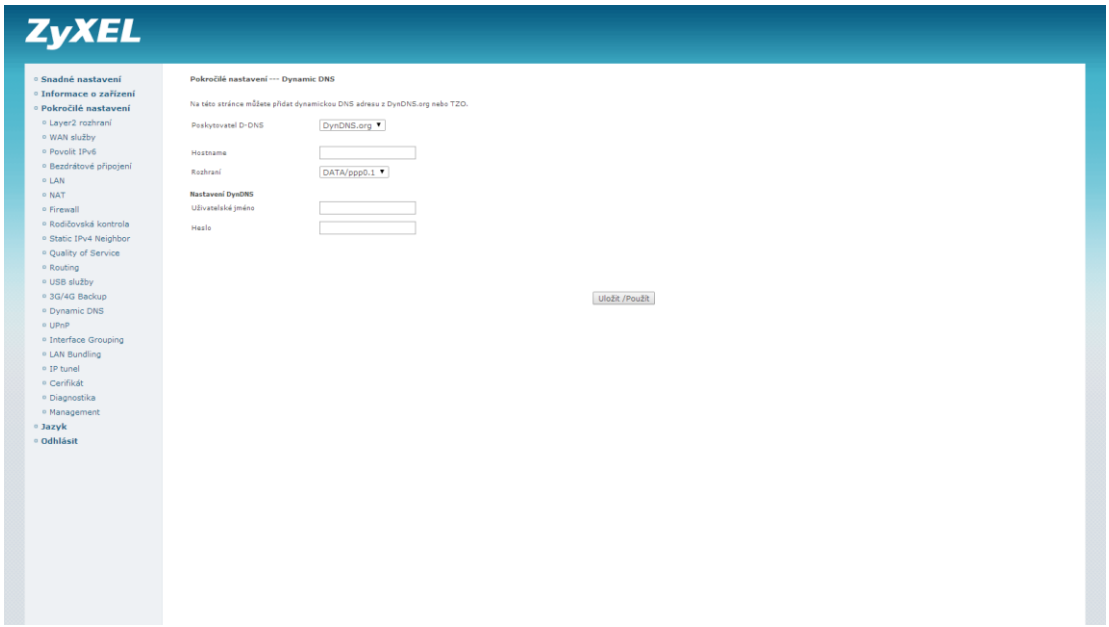
Položka	Popis
Popis karty	Název výrobce modemu a typ modemu
3G/4G status	Stav připojení (down, connected, dialing)
Uživatelské jméno	Pro GPRS a vyšší se nevyplňuje
Heslo	Pro GPRS a vyšší se nevyplňuje
PIN	Vyplňte PIN Vaší SIM karty
Ponechat PIN	Je-li políčko zaškrtnuté, bude PIN na kartě aktivní a je potřeba ho vyplnit
Vytáčecí řetězec	Ekvivalent telefonního čísla pro vytáčení, pro CZ je *99#
APN	Access Point Name = název mobilního přístupového bodu, získáte od vašeho poskytovatele internetu
Připojení	Trvalé (Nailed up) ke spojení dojde automaticky při výpadku DSL nebo ETH WAN nebo na požádání (On demand) kdy je potřeba ručně spojení vytočit
Backup interval	Po jaké době výpadku WAN/DSL se spojení naváže
Recovery interval	Po jaké době po zprovoznění WAN/DSL se mobilní připojení odpojí
IP adresa	IP adresa modemu, doporučujeme ponechat dynamické
DNS informace	Použité DNS Servery, doporučujeme ponechat dynamické přidělení

15 DYNAMIC DNS

Služba Dynamic DNS umožňuje přidat alias dynamickou IP adresu k statickému hostname v některé z mnoha domén a tím poskytuje možnost snadného přístupu k směrovači z různých míst na Internet. Na obrazovku se dostanete kliknutím na **Pokročilé nastavení > Dynamic DNS.** Pro přidání klikněte na **Přidat**

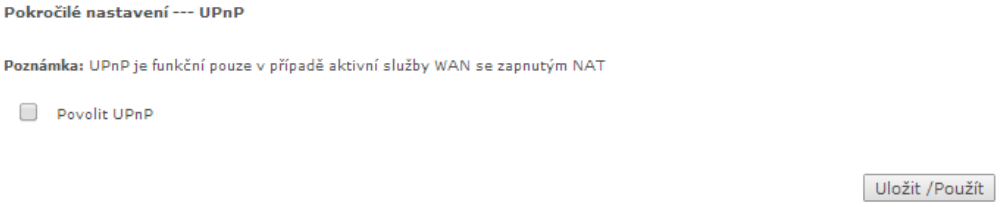


Zvolte poskytovatele D-DNS, Hostname, použité rozhraní a přihlašovací údaje od poskytovatele D-DNS. Pro uložení klikněte na **Uložit/Použít.**



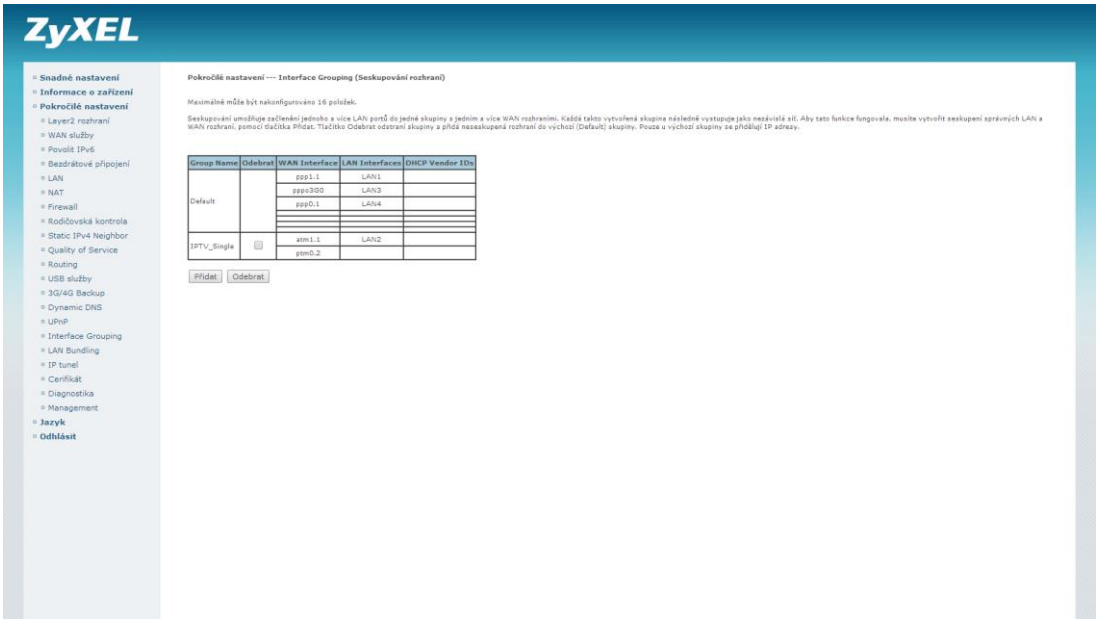
16 UPNP

Funkce UPnP (Universal Plug n‘ Play) umožňuje rychlé přidávání a správu klientských zařízení, které tuto funkci podporují. Aktivujete zaškrtnutím políčka povolit UPnP a uložte kliknutím na **Uložit/Použít.**

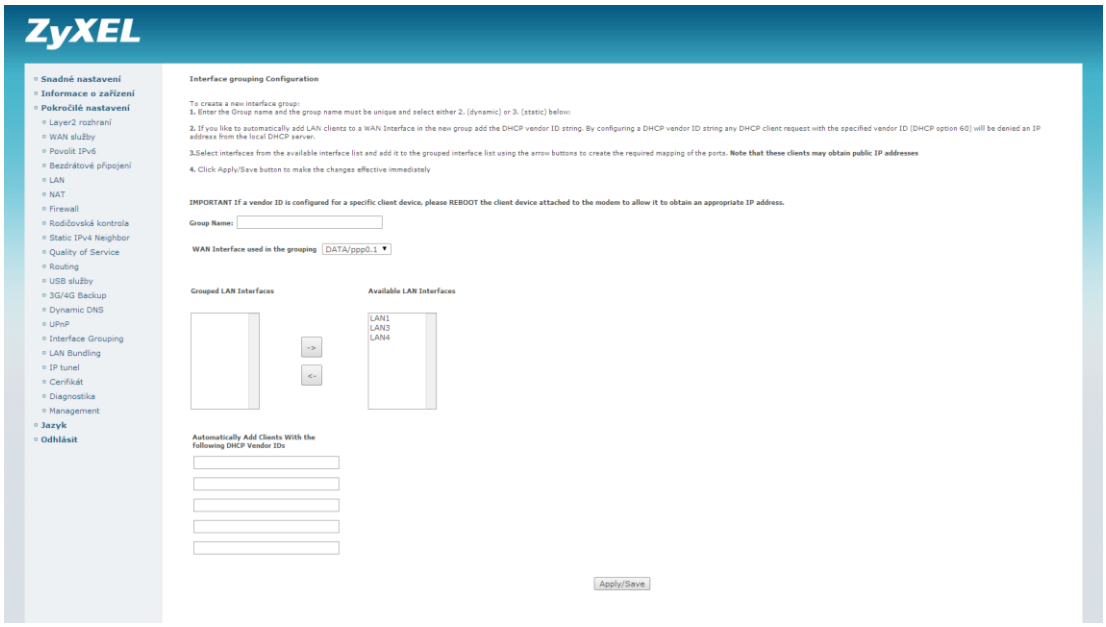


17 INTERFACE GROUPING

Seskupování umožňuje začlenění jednoho a více LAN portů do jedné skupiny s jedním a více WAN rozhraními. Každá takto vytvořená skupina následně vystupuje jako nezávislá síť. Aby tato funkce fungovala, musíte vytvořit seskupení správných LAN a WAN rozhraní, pomocí tlačítka Přidat. Tlačítko Odebrat odstraní skupiny a přidá neseskupená rozhraní do výchozí (Default) skupiny. Na obrazovku se dostanete kliknutím na **Pokročilé nastavení > Interface grouping**

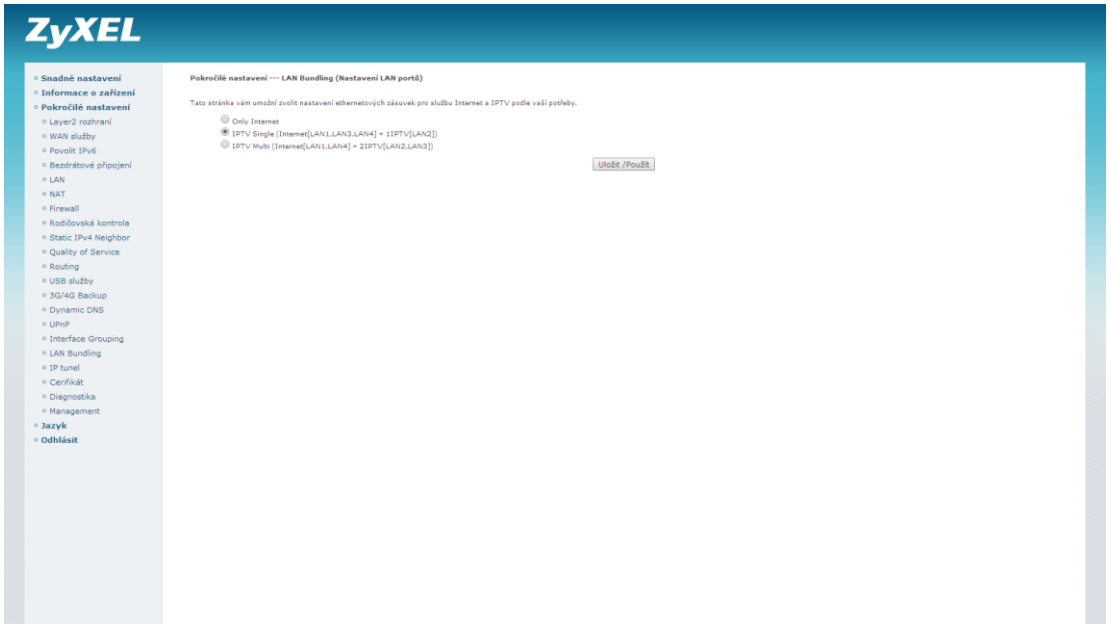


Pro aktivaci nového seskupení klikněte na tlačítko **Přidat** a postupujte podle pokynů na obrazovce.



18 LAN BUNDLING

Funkce LAN bundling umožňuje použít jedno z předdefinovaných nastavení LAN portů. Pro přístup na stránku klikněte na **Pokročilé nastavení > LAN Bundling.** Vyberte požadované nastavení a klikněte na **Uložit/Použít.**

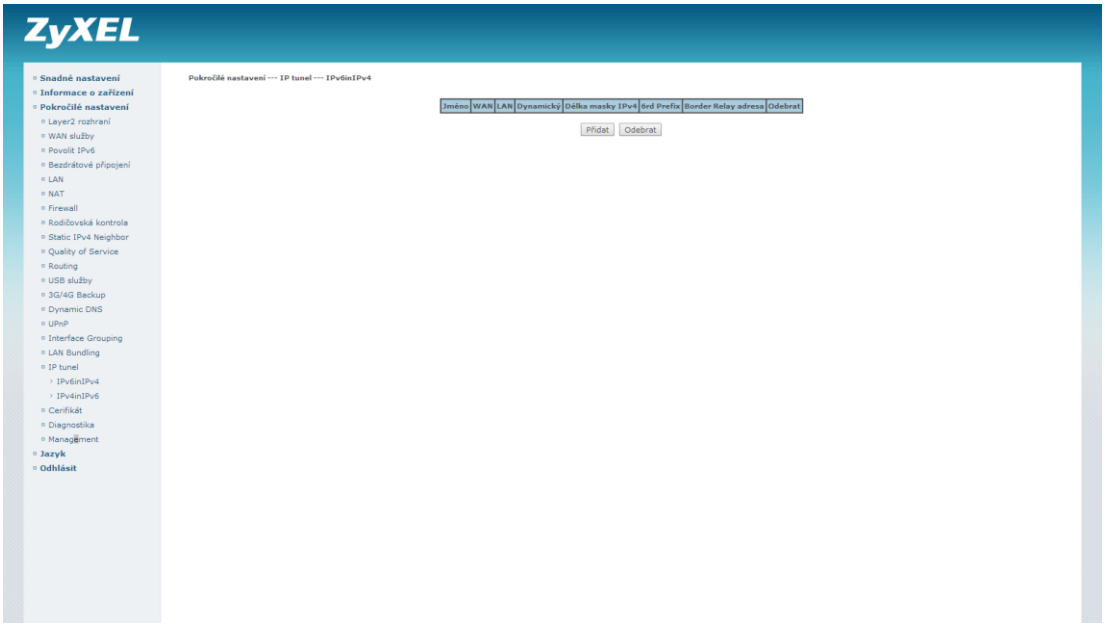


19 IP TUNEL

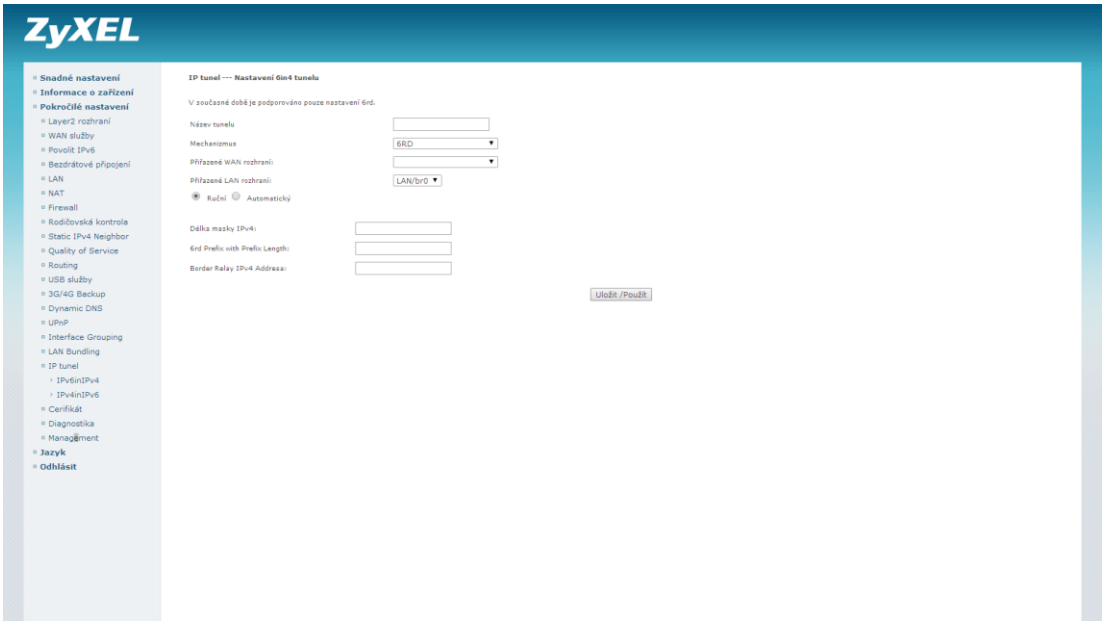
V této kapitole se věnujeme nastavení IP Tunellingu. IP Tunel je internetový protokol komunikačního kanálu mezi dvěma sítěmi. Používá se k přenosu protokolu jiné sítě zapouzdřením jejich paketů. Pro přístup na stránku klikněte na **Pokročilé nastavení > IP Tunel**

19.1 IPv6inIPv4

Konfigurace 6v4 tunelování pro zapouzdření IPv6 provozu pomocí sestaveného IPv4 spojení.. Pro přidání IP Tunelu klikněte na **Přidat.**



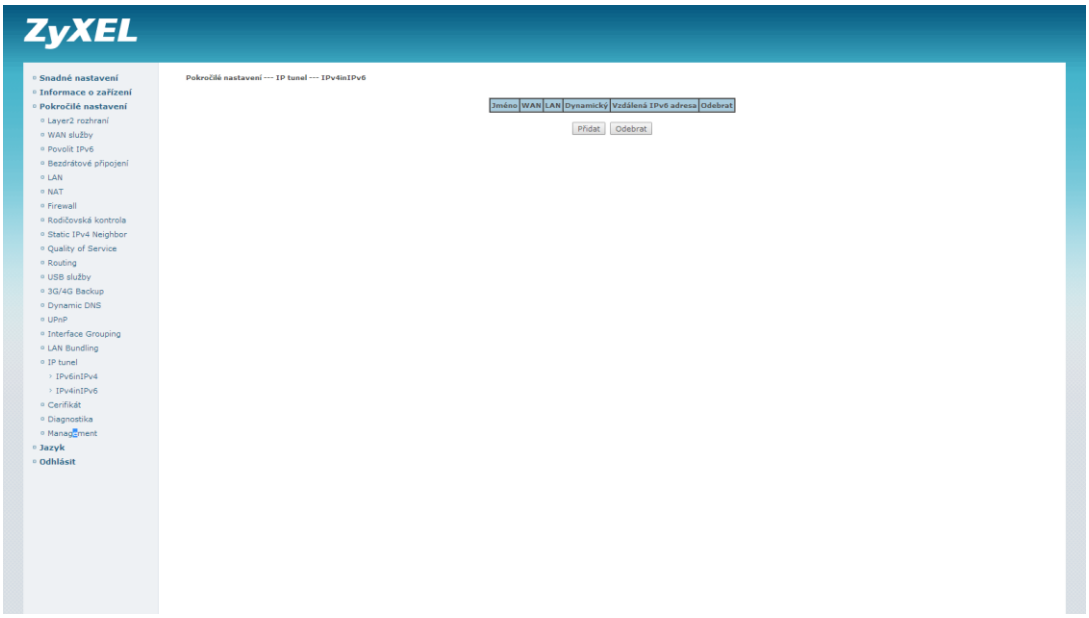
Nastavení nového IP tunelu



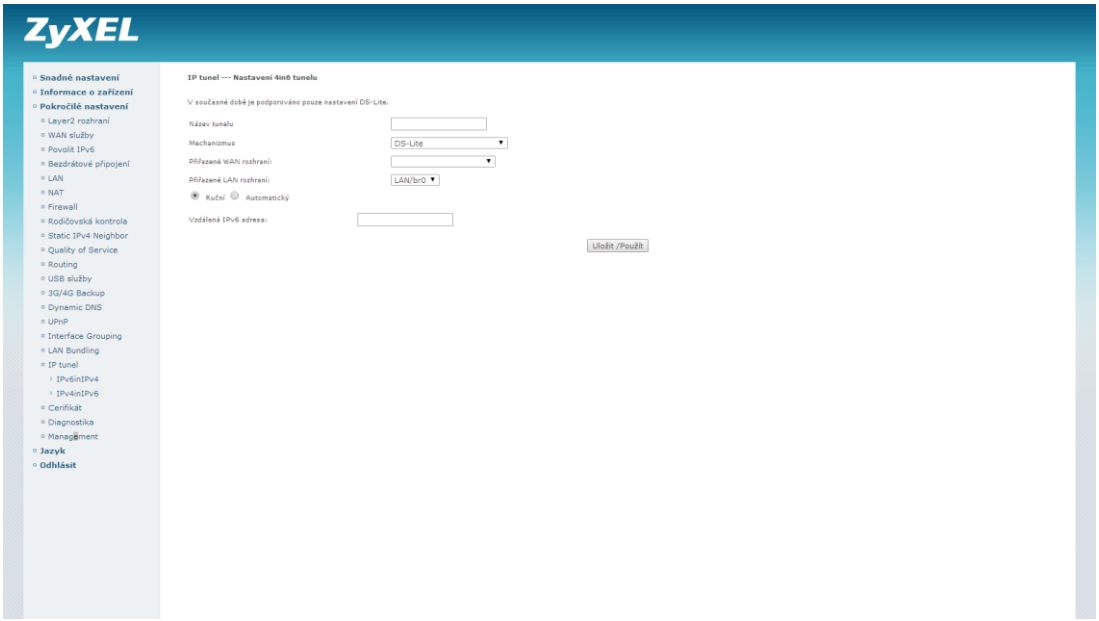
Položka	Popis
V současné době je podporováno pouze nastavení 6rd.	
Název tunelu	Vaše vlastní označení názvu tunelu
Mechanizmus	Mechanizmus tunelu (k dispozici je pouze 6rd.)
Přiřazená WAN rozhraní	WAN rozhraní, přes které bude komunikace IP tunelem probíhat
Přiřazená LAN rozhraní	LAN rozhraní, přes které bude komunikace IP tunelem probíhat
Ruční/Automaticky	Zaškrtnutím volby „Automaticky“ se tunel pokusí nastavit dle přiřazených rozhraní a mechanizmu, zaškrtnutím volby „Ruční“ nastavíte parametry níže manuálně
Délka masky IPv4	Nastavte délku masky protokolu IPv4
6rd prefix with prefix length	Nastavení 6rd prefixu a jeho délky
Border relay IPv4 adress	Hraniční hodnota relay IPv4 adresy

19.2 IPv4inIPv6

Konfigurace 4v6 tunelování pro zapouzdření IPv4 provozu pomocí sestaveného IPv6 spojení.. Pro přidání IP Tunelu klikněte na **Přidat.**



Nastavení nového IP Tunelu.



V tabulce naleznete popis položek na obrazovce

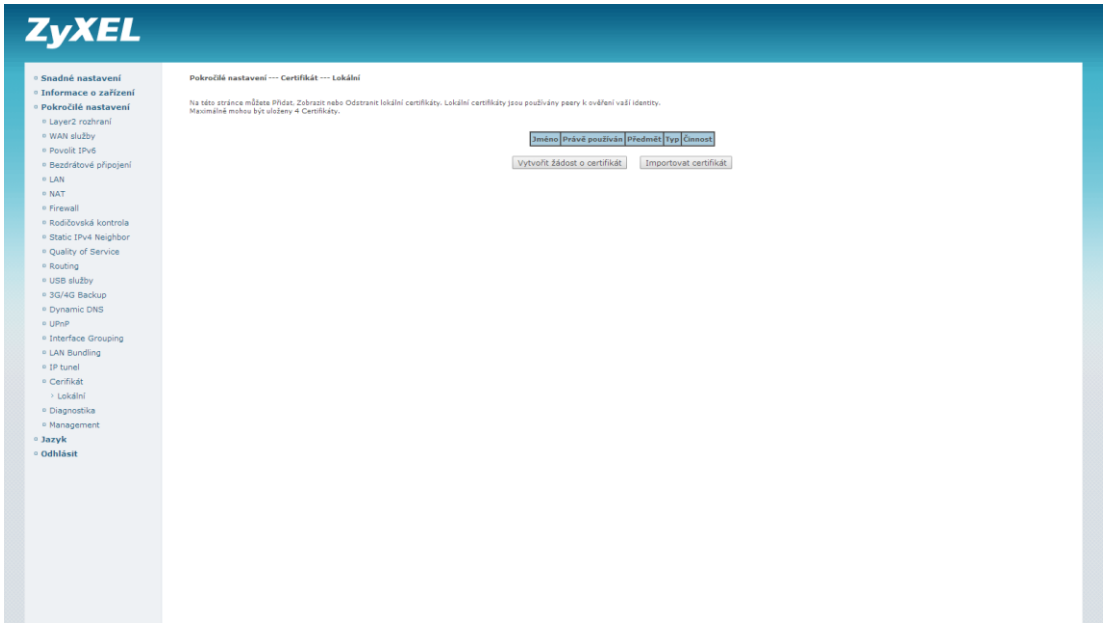
Položka	Popis
V současné době je podporováno pouze nastavení DS-Lite	
Název tunelu	Vaše vlastní označení názvu tunelu
Mechanizmus	Mechanizmus tunelu (k dispozici je pouze DS-Lite)
Přiřazená WAN rozhraní	WAN rozhraní, přes které bude komunikace IP tunelem probíhat
Přiřazená LAN rozhraní	LAN rozhraní, přes které bude komunikace IP tunelem probíhat
Ruční/Automaticky	Zaškrtnutím volby „Automaticky“ se tunel pokusí nastavit dle

	přiřazených rozhraní a mechanizmu, zaškrtnutím volby „Ruční“ nastavíte parametry níže manuálně
Vzdálená IPv6 adresa	Nastavte IPv6 adresu vzdálené sítě

20 CERTIFIKÁT

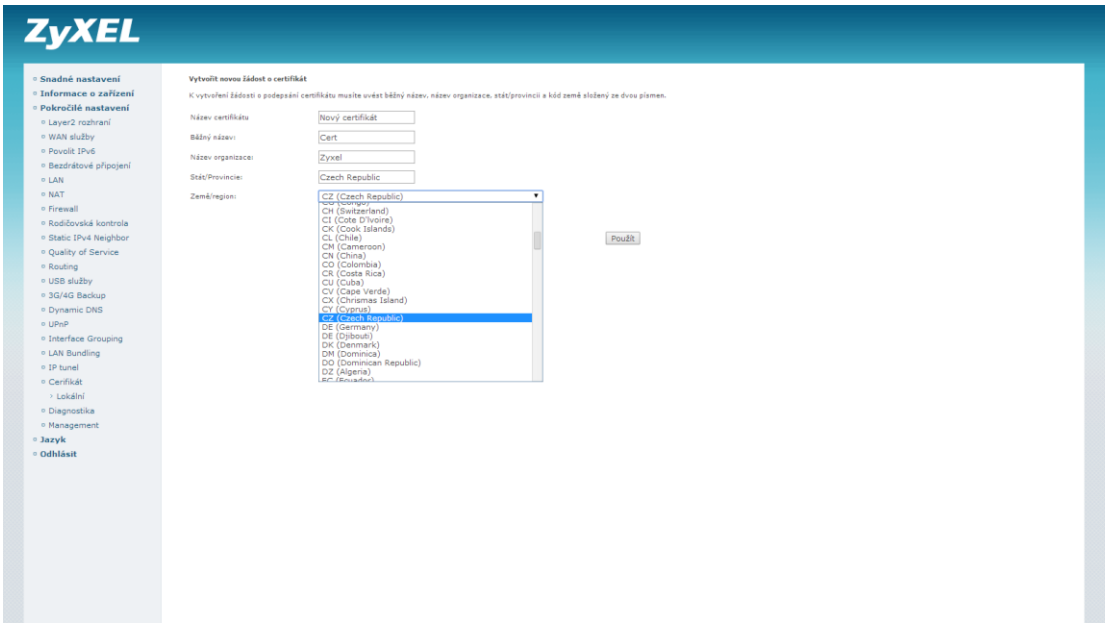
20.1 Lokální certifikát

Lokální certifikáty jsou určeny k identifikaci zařízení externími platformami jako je například TR-069, peer to peer sítě nebo cloudové služby. Na stránku se dostanete kliknutím na **Pokročilé nastavení > Certifikát > Lokální**



Chcete-li vytvořit žádost o certifikát, klikněte na tlačítko **Vytvořit žádost o certifikát**

Vyplňte příslušné kolonky dle instrukcí od poskytovatele služby certifikátu a klikněte na **Použít**

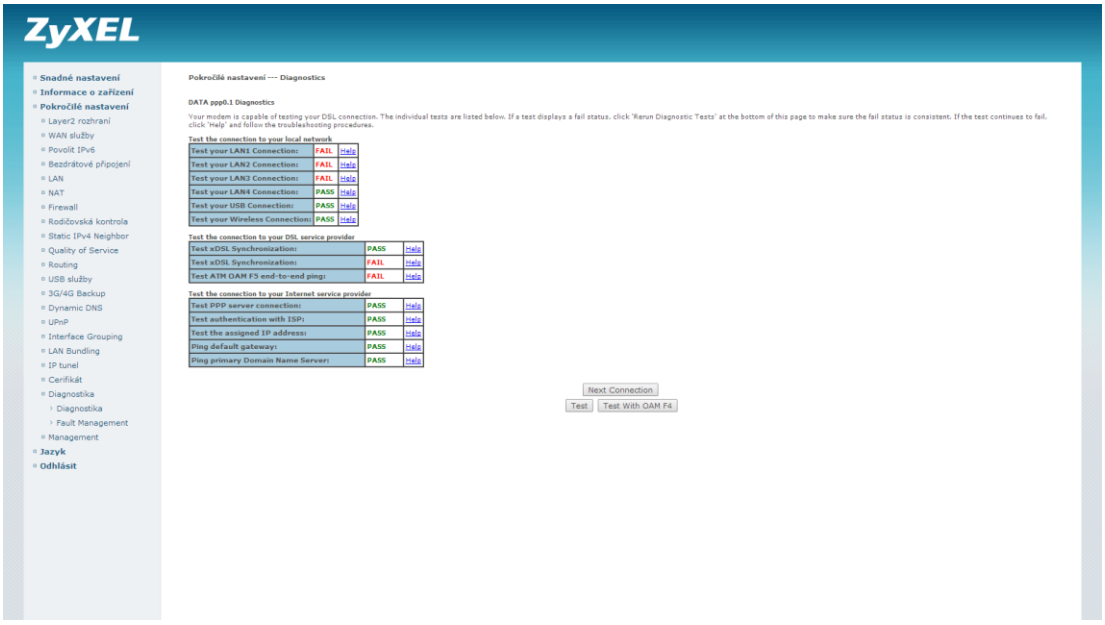


21 DIAGNOSTIKA

21.1 Diagnostika

Diagnostika analyzuje stav všech nastavených WAN profilů v zařízení. Stránku zobrazíte kliknutím na **Pokročilé nastavení > Diagnostika.**

Poznámka: Diagnostika je pouze orientační funkce. V některých případech může detekovat chybu na zařízení i v případě, kdy je zařízení funkční (např. v případě Ping primary DNS může diagnostika vyhodnotit stav jako chybu, přesto že je DNS funkční. Důvodem je zamezená odezva na PING na straně DNS serveru)

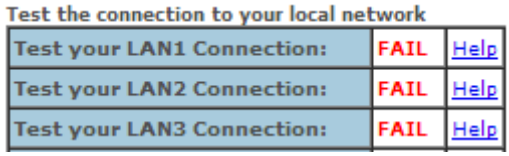


Diagnostika zkontroluje funkčnost portů LAN a USB, bezdrátového připojení, a připojení k Internetu přes xDSL nebo 4G/3G zálohu (je-li k dispozici). Pro každé nastavené připojení WAN je k dispozici samostatný test, pro test dalšího připojení klikněte na tlačítko **Next connection** a pro návrat k předchozímu připojení na tlačítko **Previous connection.**

Je-li výsledek testu „PASS“ port nebo rozhraní funguje.



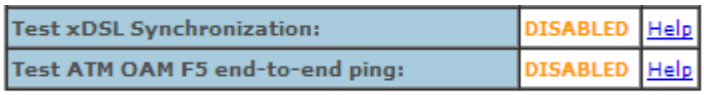
Je-li výsledek testu „FAIL“ port nebo rozhraní je odpojené. Je-li LAN port obsazen nebo rozhraní aktivní, zkontrolujte zapojení nebo klikněte na tlačítko **help** pro další instrukce.



Je-li výsledek testu „Down“, není rozhraní aktivní či zapnuté. Pokud ano, zkontrolujte nastavení nebo klikněte na **help** pro další instrukce.

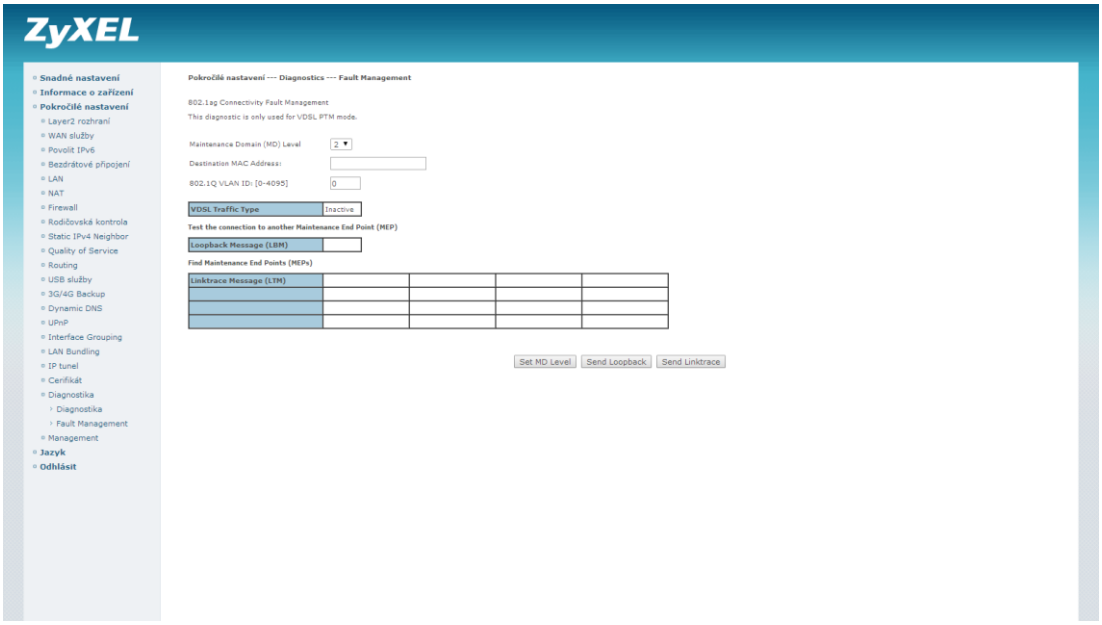


Je-li výsledek testu „DISABLED“ není test pro testovaný WAN profil dostupný.



21.2 Fault management

Fault management je set testů, který detekuje a vyhodnocuje chyby v síti. Stránku zobrazíte kliknutím na **Pokročilé nastavení > Diagnostika > Fault management.**



V tabulce naleznete popis položek na obrazovce

Položka	Popis
Maintainance domain level	Zde nastavíte Úroveň domény pro údržbu/dohled
Destination MAC adress	Nastavení cílové MAC adresy
802.1Q VLAN ID (0-4095)	ID diagnostikované VLANy
VDSL Traffic type	Typ diagnostikovaného VDSL provozu
Loopback message	Zpráva zpětné vazby
Find maintainance endpoints	
Link Trace Message (LTM)	Zpráva z trasování provozu linky

22 MANAGEMENT

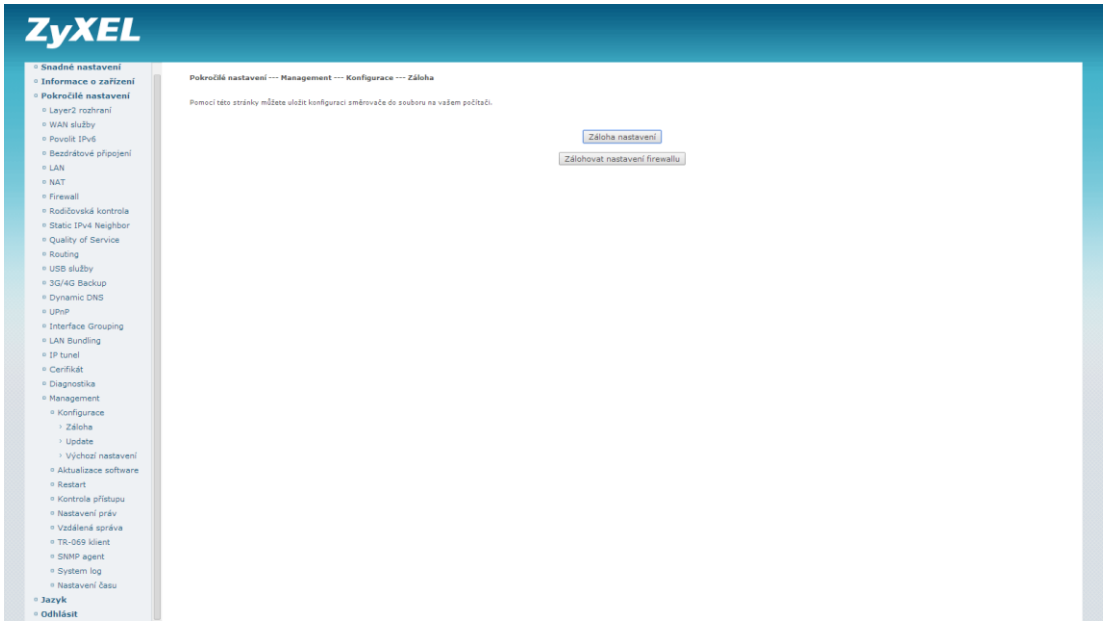
V kapitole management naleznete informace ke správě zařízení.

22.1 Konfigurace

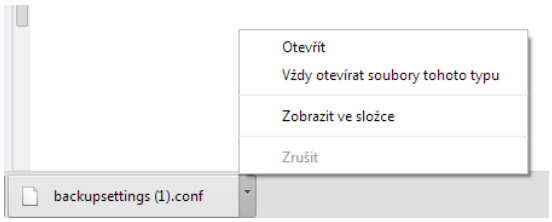
Tato nabídka vám umožní zálohovat konfiguraci zařízení, obnovit ji a nastavit všechny parametry zařízení na tovární hodnoty.

22.1.1 Záloha

Pro zálohu konfigurace zvolte v levém menu **Pokročilé nastavení > Management > Konfigurace > Záloha** a klikněte na tlačítko **Záloha nastavení** nebo **Záloha nastavení firewallu.**

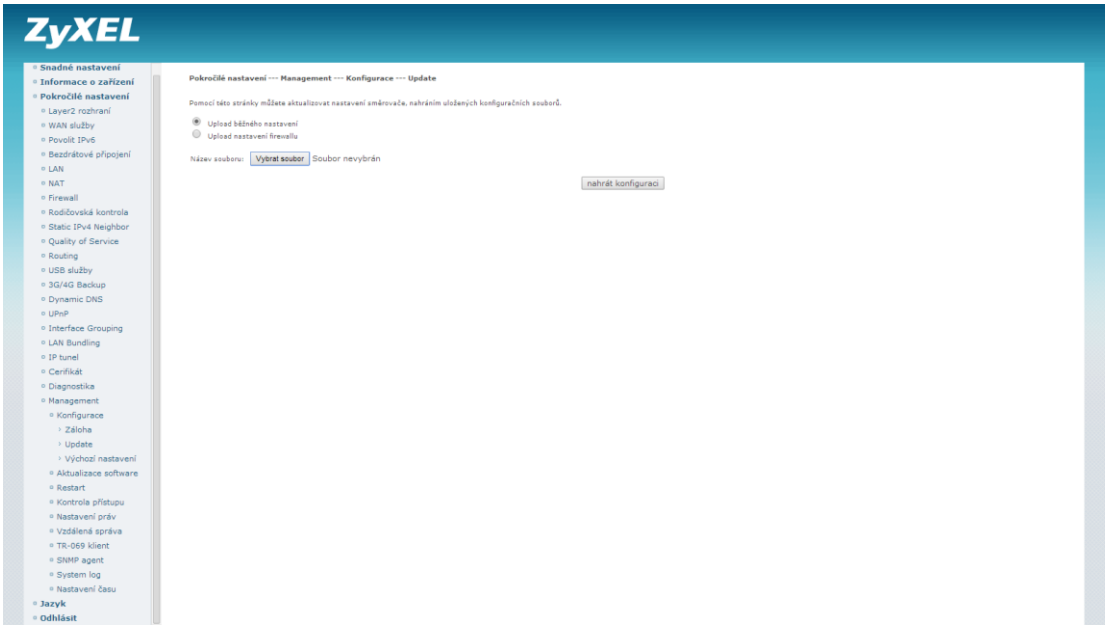


Konfigurační soubor se stáhne do cílové složky pro stahování dle nastavení Vašeho prohlížeče .

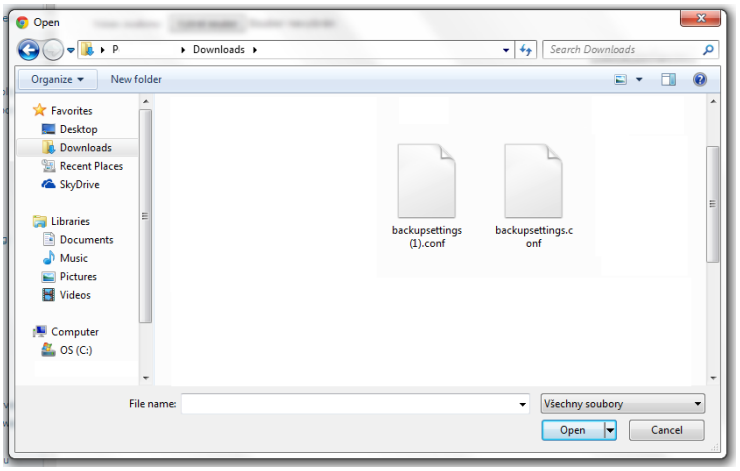


22.1.2 Update

Pro obnovení nebo update konfigurace zařízení zvolte v levém menu **Pokročilé nastavení > Management > Konfigurace > Update.**



Vyberte, zda si přejete nahrát nastavení firewallu nebo zařízení a kliknutím na **Vybrat soubor.** Zvolte požadovaný konfigurační soubor



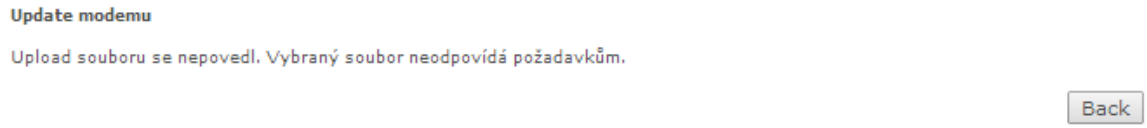
Po kliknutí na **Nahrát konfiguraci** se spustí nahrání konfiguračního souboru

Nevypínejte ani neodpojujte zařízení, když probíhá update konfigurace!

Zařízení ZyXEL se po dokončení updatu konfigurace automaticky restartuje, čímž dojde k dočasnému odpojení sítě. V některých systémech je odpojení od sítě signalizováno informační bublinou.



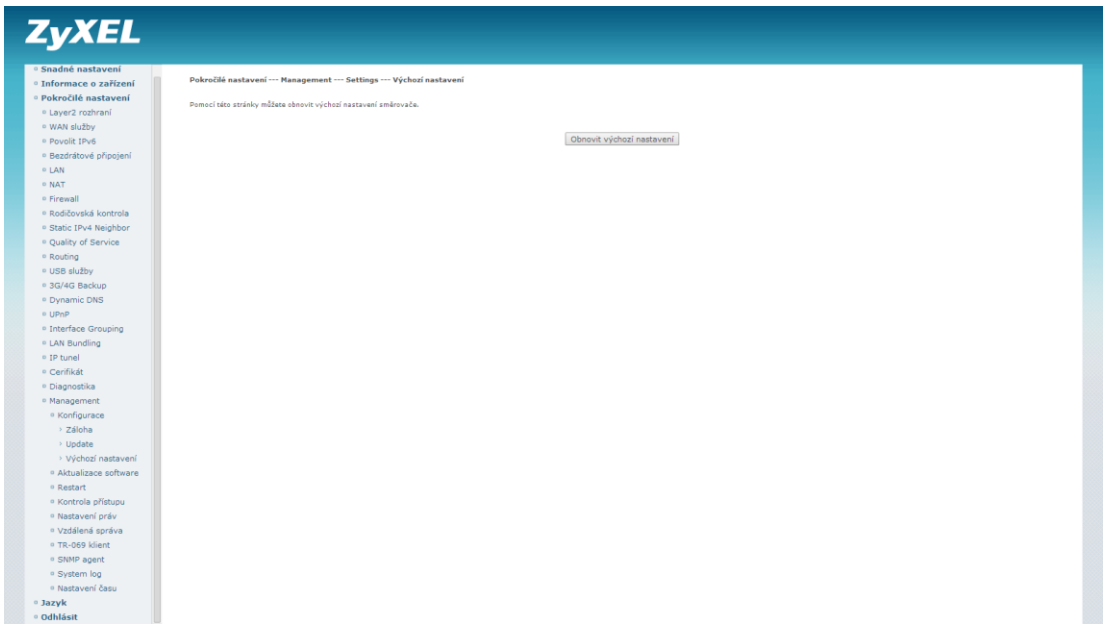
Pokud se místo restartu objeví stránka níže, byl vybrán chybný nebo poškozený konfigurační soubor.



22.1.3 Výchozí nastavení

V zařízení lze obnovit tovární konfiguraci na stránce **Pokročilé nastavení > Management > Konfigurace > Výchozí nastavení**

Klikněte na **Obnovit výchozí nastavení**



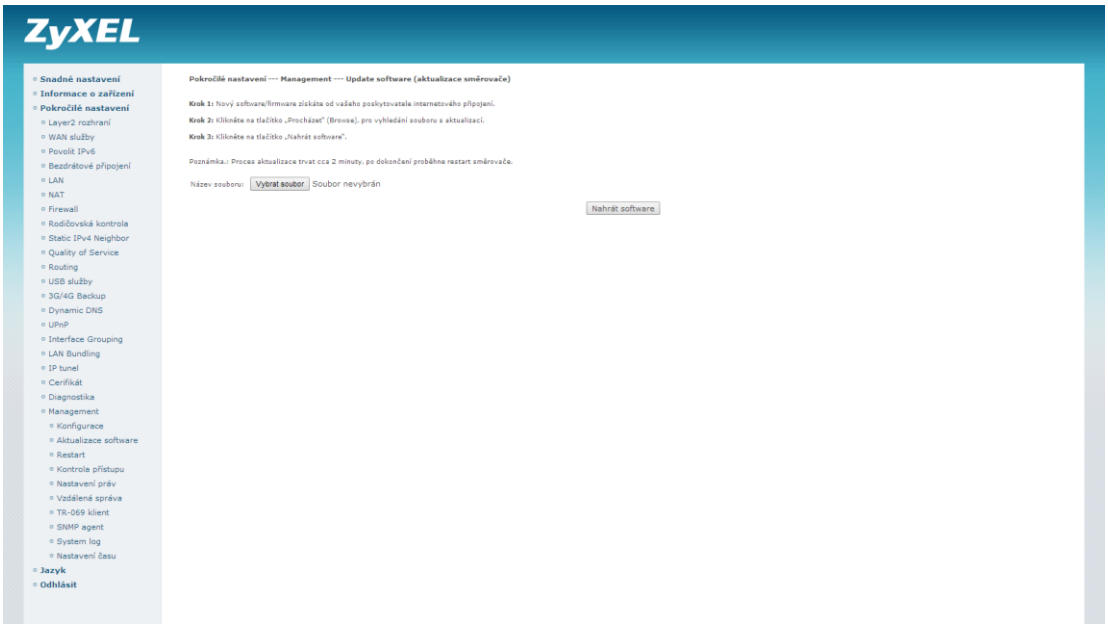
Zařízení ZyXEL se automaticky restartuje.

22.2 Aktualizace software

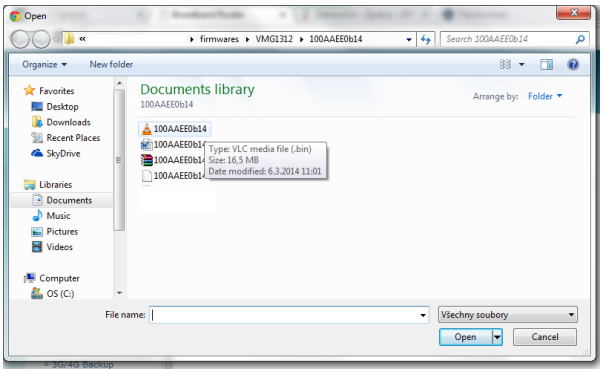
Služby různých poskytovatelů internetu můžou pro správnou funkčnost vyžadovat update softwaru (tzv. Firmware) na software schválený daným poskytovatelem. Software je ve formátu souboru *.bin.

Na obrazovku se dostanete kliknutím na **Pokročilé nastavení > Management > Aktualizace software**

Klikněte na **Vybrat soubor**



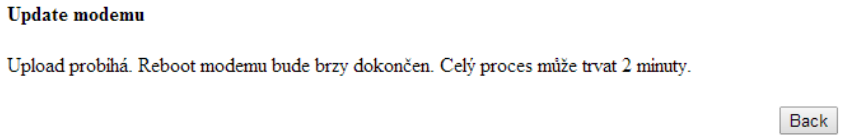
Vyberte požadovaný soubor, klikněte na **Open** (Otevřít) a následně klikněte na **Nahrát software**



Soubor se bude načítat, toto může chvíli trvat



Následně dojde k restartu zařízení



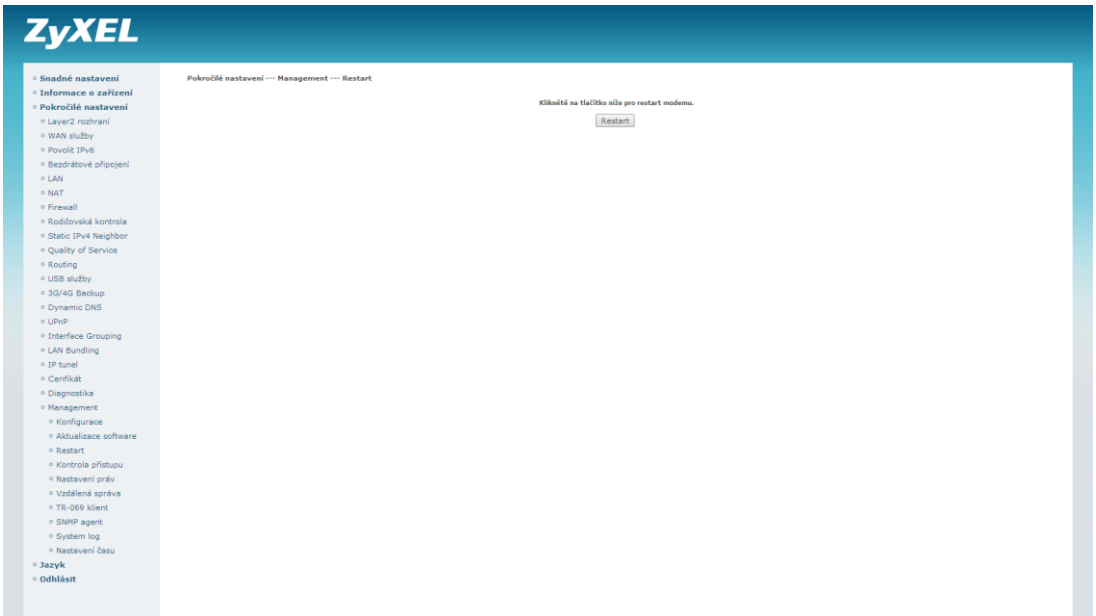
Nevypínejte zařízení, když probíhá aktualizace firmwaru!

Po dokončení aktualizace budete vyzváni k zadání hesla. Aby se nahraný software korektně uložil je vhodné resetovat zařízení do továrního nastavení, Toto provedete podržením tlačítka **RESET** na zadní straně zařízení na dobu 10 sekund. (dokud probliknou LED přístroje).

Zkontrolujte správnou verzi software na obrazovce **Informace o zařízení**

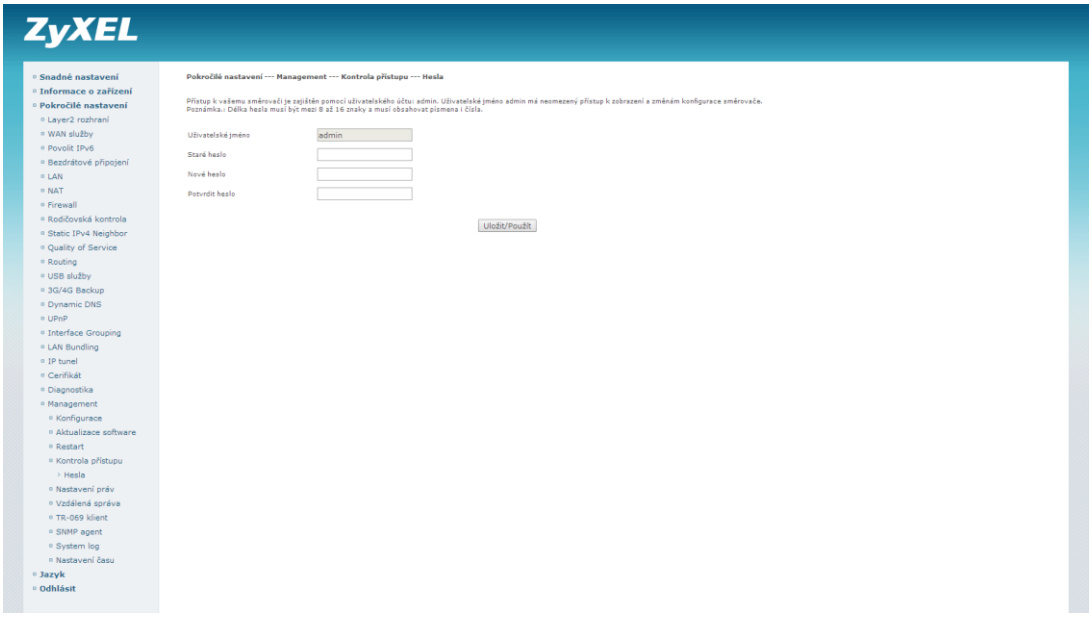
22.3 Restart

Pomocí této obrazovky můžete restartovat zařízení. Klikněte na tlačítko **Restart**



22.4 Kontrola přístupu - Hesla

Na této obrazovce můžete přenastavit heslo do Web GUI zařízení. Heslo uložíte tlačítkem **Uložit/Použít**



22.5 Nastavení práv

Na této obrazovce nastavíte konfigurační práva a heslo pro dvě definované uživatelské skupiny.

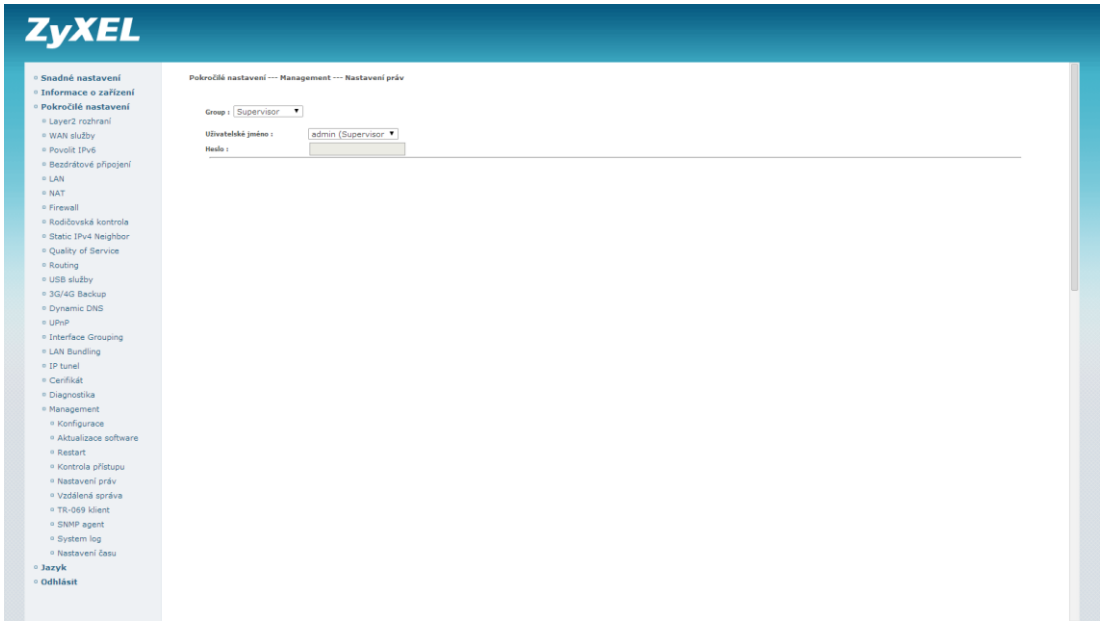
Administrátor – má přístup k základnímu nastavení zařízení

Uživatel – má přístup jen k informacím o stavu zařízení a snadnému nastavení

Poznámka: Existuje ještě třetí uživatelská skupina. U této skupiny se konfigurační práva neomezují a změna hesla s provádí v části Kontrola přístupu, jak bylo uvedeno v kapitole 22.5.

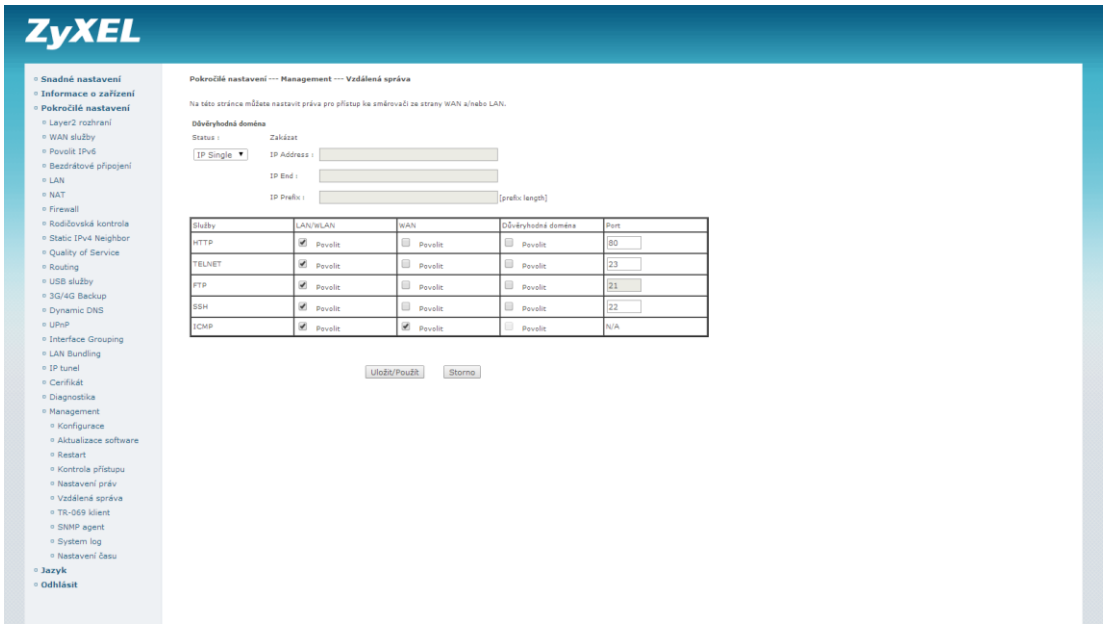
Supervisor – má přístup ke všem funkcím zařízení

Vyberte uživatele a nastavte heslo a práva



22.6 Vzdálená správa

Na této obrazovce můžete nastavit vzdálenou správu zařízení ZyXEL.

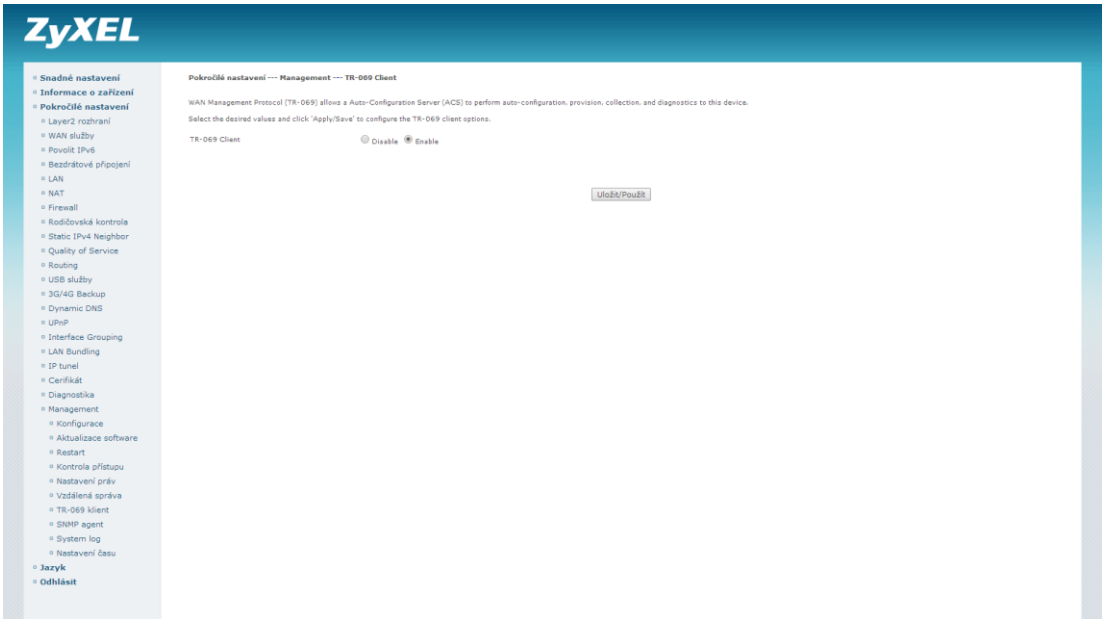


V tabulce naleznete popis položek na obrazovce

Položka	Popis
Důvěryhodná doména	
Status	stav: zakázat/povolit Pro: IP Single, IP rozsah, IP prefix
IP Address: (IP Start)	IP adresa (nebo začínající adresa v případě volby IP rozsah)
IP End:	Koncová IP adresa
IP Prefix:	Číslo IP prefixu
Tabulka (způsoby vzdálené správy)	
HTTP	Standardní webové rozhraní
FTP	File Transfer Protocol (protokol přenosu dat)
Telnet	Správa přes Telnet
SSH	Správa přes síťový protokol „Secure Shell“
ICMP	Internet Control Message Protocoll

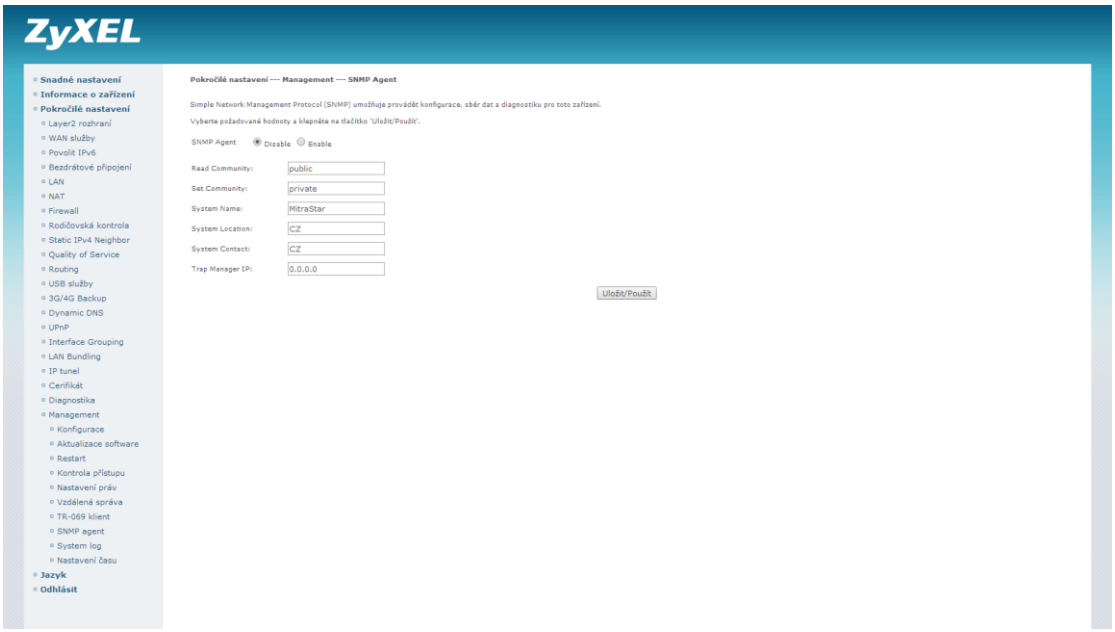
22.7 TR-069 Client

TR-069 je vzdálená správa, konfigurace a dohled zařízení přes ACS server. Je-li tato položka v továrním nastavení označena **Enable**, nedoporučujeme položku deaktivovat (**Disable**) aby nedošlo ke ztrátě správy zařízení poskytovatelem internetu.



22.8 SNMP Agent

Simple Network Management Protocoll Agent umožňuje nastavit zařízení jako tzv. Master Agent (nebo AgentX) které následně definuje ostatním zařízením (tzv. SubAgentům) způsob, jakým přijímají a zpracovávají SNMP příkazy.



V tabulce naleznete popis položek na obrazovce

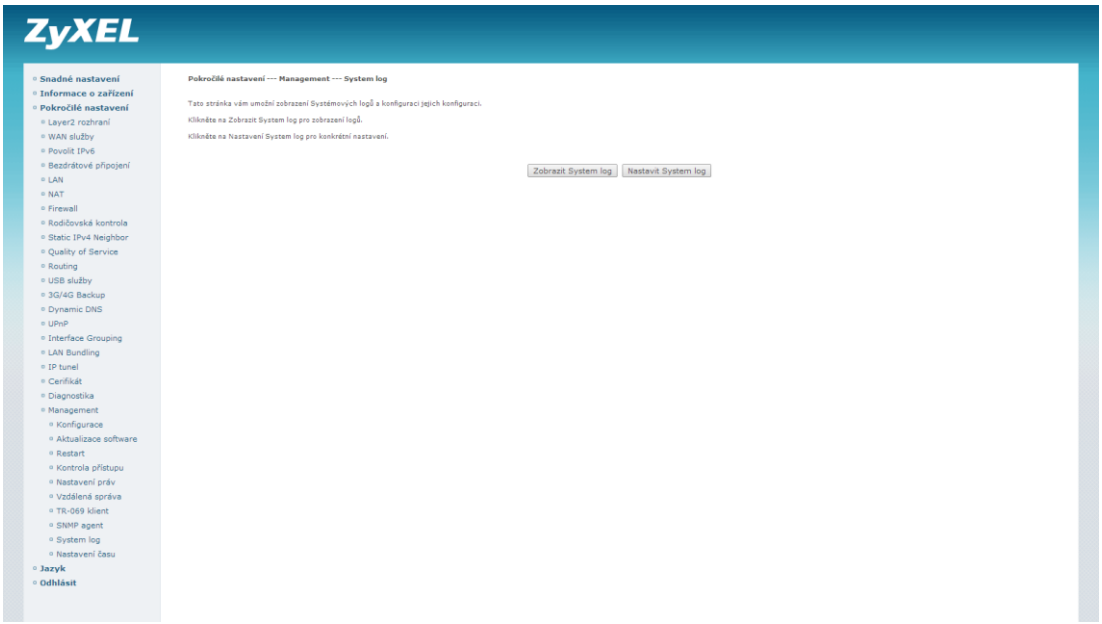
Položka	Popis
SNMP Agent	Volby: Enable/Disable
Read Community	Nastavení skupiny „read“
Set Community	Nastavení skupiny „set“
System Name	Název systému
System location	Umístění systému
System contact	Kontaktní síťový údaj systému
Trap manager IP	Nastavení IP adresy Trap Manager

22.9 System log

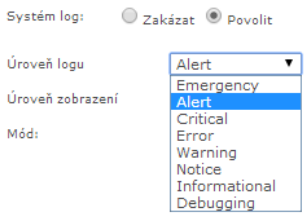
Pokud je logovací režim povolen, systém začne logovat všechny vybrané události. Logovány budou všechny události vybrané úrovně logu. Zobrazeny budou všechny události vybrané úrovně zobrazení. Je-li vybraný Mód „Vzdálený“ nebo „Oba“, události budou odeslány na specifikovanou IP adresu a UDP port vzdáleného syslog

serveru. Je-li vybraný Mód „Lokální“ nebo „Oba“, události budou zaznamenány v lokální paměti.

Pro zobrazení logu klikněte na **Zobrazit system log**

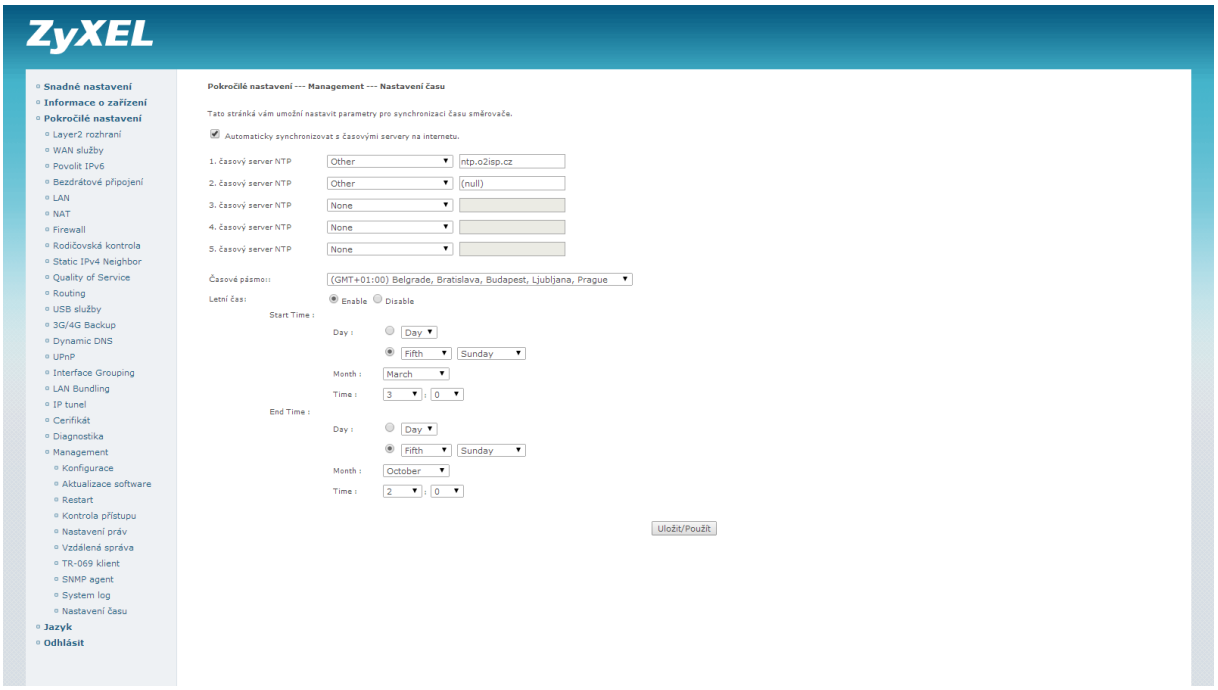


Chcete-li zapnout systém log nebo nastavit detailní parametry logu klikněte na **Nastavit system log** . Na obrazovce můžete nastavit, jaké události se budou logovat a zobrazovat podle nastavené úrovně logu. Pro uložení klikněte na **Uložit/Použít**



22.10 Nastavení času

Na této stránce nastavíte NTP servery (časové servery) a vlastnosti systémového času jako je zimní/letní čas nebo časové pásmo. Pro uložení nastavení klikněte na **Uložit/Použít**



23 PROBLÉMY A JEJICH ŘEŠENÍ

V této kapitole uvádíme několik základních tipů, jak řešit provozní problémy. Problémy pro přehlednost dělíme do tří skupin:

- Napájení, kabelové připojení, LED kontrolky.
- Přístup a přihlášení k zařízení.
- Přístup k internetu.

23.1 Napájení, kabelové připojení, LED kontrolky

Zařízení se nezapnulo. Nesvítí žádné LED kontrolky.

1. Zkontrolujte, zda je zařízení skutečně zapnuté.
2. Užívejte pouze napájecí adaptér a šňůru dodanou se zařízením.
3. Zkontrolujte, zda je napájecí adaptér připojen k funkčnímu zdroji elektrické energie.
4. Zkuste zařízení vypnout a znovu zapnout.
5. Jestliže problém přetrvá, kontaktujte prodejce.

Jedna z LED kontrolek se nechová, jak by měla.

1. Seznamte se s funkcí kontrolek (viz kapitola 1.6).
2. Zkontrolujte kabelové propojení.
3. Ověřte, zda nejsou kabely nějak poškozené. Poškozené kabely vyměňte.
4. Zkuste zařízení vypnout a znovu zapnout.
5. Jestliže problém přetrvá, kontaktujte prodejce.

23.2 Přístup a přihlášení k zařízení

Zapomněl/a jsem IP adresu zařízení.

1. Výchozí IP adresa je **10.0.0.138**.
2. Jestliže jste výchozí IP adresu změnili, můžete ji získat tak, že vyhledáte IP adresu výchozí brány v počítači. Ve většině počítačů Windows klikněte na **Start > Run** (spustit) a zadejte příkaz **cmd** následovaný příkazem **ipconfig**.
   V některých případech je adresa výchozí brány (**Default Gateway**) adresou zařízení ZyXEL. Zkuste ji zadat do prohlížeče.
3. Pokud tento postup není úspěšný, resetujte zařízení na výchozí tovární hodnoty.

Zapomněl/a jsem heslo.

1. Výchozí administrátorské heslo je **admin**.
2. Pokud je heslo jiné, resetujte zařízení na výchozí tovární hodnoty.

Nemohu zobrazit okno **Login** pro přihlášení k zařízení.

1. Musíte mít správnou IP adresu zařízení.

   Výchozí IP adresa je **10.0.0.138**.

   Jestliže jste IP adresu změnili, užijte novou IP adresu.

   Jestliže jste IP adresu změnili a zapomněli, postupujte podle pokynů v prvním odstavci na této stránce.
2. Zkontrolujte připojení kabelů a správnou činnost LED kontrolek. Viz také příručka k rychlé instalaci.
3. Internetový prohlížeč nesmí blokovat vyskakovací okna a musí povolovat JavaScript a Javu.
4. Resetujte zařízení na tovární hodnoty a zkuste získat přístup přes výchozí IP adresu.
5. Jestliže problém přetrvá, kontaktujte správce sítě nebo prodejce. Případně vyzkoušejte níže uvedené odborné tipy, které vyžadují jistou zkušenost v IT.

   Odborné tipy

   Zkuste k zařízení ZyXEL získat přístup prostřednictvím jiné služby, např. Telnetu. Jestliže se přístup podaří, zkontrolujte nastavení dálkové správy a pravidla firewallu a zjistěte, proč zařízení nereaguje na komunikaci přes HTTP.

   Jestliže je počítač připojen bezdrátově, zkuste použít počítač, který je připojen k portu **ETHERNET**.

Mohu zobrazit okno **Login**, ale nedaří se mi přihlásit.

1. Dávejte pozor, ať heslo zadáte správně. Výchozí administrátorské heslo je **admin**. Heslo rozlišuje malá a velká písmena: zkontrolujte tedy, zda nemáte zapnutá velká písmena (CAPS LOCK).
2. K webovému konfigurátoru se nelze připojit, když někdo jiný současně využívá Telnet k přístupu k zařízení. Nejprve se musí uživatel s přístupem přes Telnet odhlásit.
3. Zkuste zařízení vypnout a znovu zapnout.
4. Jestliže problém přetrvá, resetujte zařízení na tovární nastavení.

Nemohu se přihlásit přes Telnet.

Postupujte podle pokynů v této kapitole v odstavci „Nemohu zobrazit okno **Login** k přihlášení k zařízení“, ale ignorujte pokyny ohledně prohlížeče.

Nedaří se mi uploadovat/downloadovat konfigurační soubor přes FTP. Nedaří se mi aktualizovat firmware přes FTP.

Postupujte podle pokynů v této kapitole v odstavci „Nemohu zobrazit okno **Login** k přihlášení k zařízení“, ale ignorujte pokyny ohledně prohlížeče.

23.3 Přístup k internetu

Nemohu se připojit k internetu.

1. Zkontrolujte zapojení kabelů a správnou činnost LED kontrolek. Viz také příručka k rychlé instalaci.
2. Dávejte pozor, ať přihlašovací údaje sdělené poskytovatelem připojení k internetu zadáte správně. Údaje rozlišují malá a velká písmena: zkontrolujte tedy, zda nemáte zapnutá velká písmena (CAPS LOCK).
3. Jestli se pokoušíte připojit bezdrátově, zkontrolujte, zda souhlasí nastavení mezi klientem a přístupovým bodem.
4. Jestli se pokoušíte připojit bezdrátově, zkontrolujte, zda je bezdrátová síť zapnutá a je zvolen správný kanál na obrazovce **Bezdrátové připojení > Pokročilé nastavení**.
5. Odpojte všechny připojené kabely a znovu je připojte podle pokynů v příručce k rychlé instalaci.
6. Jestliže problém přetrvá, kontaktujte svého poskytovatele.

Připojení k internetu pracovalo správně, ale teď pracovat přestalo.

1. Zkontrolujte zapojení kabelů a správnou činnost LED kontrolek. Viz také příručka k rychlé instalaci.
2. Zkuste zařízení vypnout a znovu zapnout.
3. Jestliže problém přetrvá, kontaktujte svého poskytovatele.

Připojení k internetu je pomalé nebo nespolehlivé.

1. Datové trasy mohou být obsazené velkým množstvím přenášených dat. Sledujte kontrolky LED (viz kapitola 1.6). Jestliže zařízení odesílá nebo přijímá velké množství dat, zkuste zavřít některé programy, které komunikují přes internet (zvlášť to platí pro peer to peer aplikace).
2. Pokud využíváte bezdrátovou síť, zkontrolujte sílu signálu. Jestliže je signál slabý, zkuste počítač přesunout blíže k zařízení. Zkontrolujte také, zda nějaká jiná zařízení neruší příjem signálu (např. mikrovlnná trouba, další bezdrátová síť, atd.).
3. Zkuste zařízení vypnout a znovu zapnout.
4. Jestliže problém přetrvá, kontaktujte správce sítě nebo prodejce. Případně vyzkoušejte níže uvedené odborné tipy, které vyžadují jistou zkušenost v IT.

   Odborné tipy

   Zkontrolujte nastavení QoS. Jestliže je QoS vypnuté, zkuste ho zapnout. Jestliže je zapnuté, můžete experimentovat s nastavením priorit určitých aplikací.