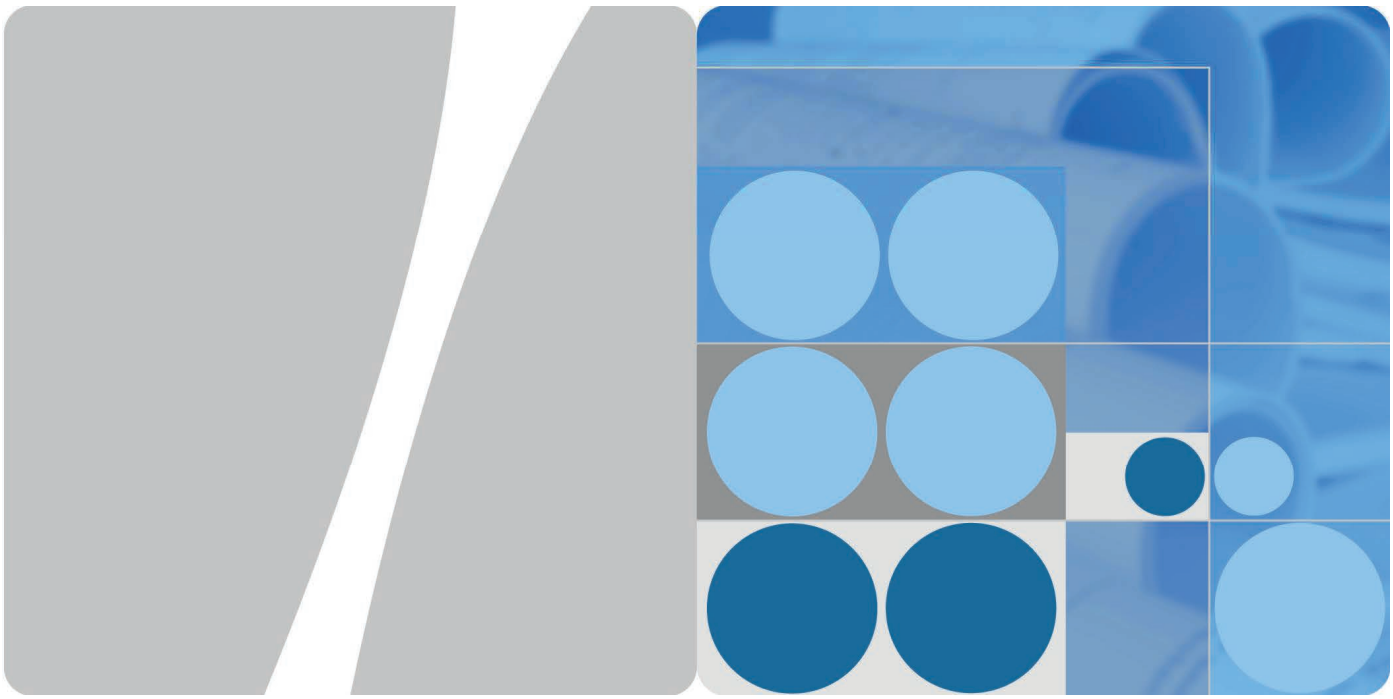


LTE outdoor modem B2338-168

Návod k obsluze

Vydání	01
Datum	1. 11. 2016

HUAWEI TECHNOLOGIES CO., LTD.

Ochranné známky a oprávnění


a ostatní symboly a nápisy Huawei jsou ochranné známky společnosti Huawei Technologies Co., Ltd.

Všechny ostatní ochranné známky a obchodní názvy uvedené v tomto dokumentu jsou majetkem příslušných vlastníků.

Poznámka

Zakoupené produkty, služby a funkce jsou stanoveny na základě smlouvy uzavřené mezi společností Huawei a zákazníkem. Žádné produkty nebo jejich části, služby a funkce popsané v tomto dokumentu nemusí být v rozsahu zakoupeného produktu nebo způsobu použití. Není-li ve smlouvě uvedeno jinak, všechny údaje, informace a doporučení v tomto dokumentu jsou poskytovány tak, jak jsou uvedeny, bez záruky nebo zastoupení jakéhokoli druhu, ať už výslovném nebo předpokládaném.

Informace obsažené v tomto dokumentu mohou být změněny bez předchozího upozornění. Pro zajištění přesnosti obsahu bylo vynaloženo maximální úsilí. Žádné výroky, informace a doporučení v tomto dokumentu však nepředstavují záruku jakéhokoli druhu, výslovnou nebo předpokládanou.

Huawei Technologies Co., Ltd.

Adresa:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 Čínská lidová republika
Webové stránky:	http://www.huawei.com
E-mail:	support@huawei.com

Obsah

Seznam obrázků

1 Webové rozhraní

Obsah této kapitoly

1.1 Přihlášení do webového rozhraní

Krok 1: Otevřete webový prohlížeč a zadejte výchozí adresu zařízení, kterou je: **https://192.168.1.1/**

Krok 2: Pro přístup do webového administračního rozhraní zadejte výchozí uživatelské jméno a heslo, která naleznete na typovém štítku vnitřní jednotky.

Zabezpečení přihlášení:

Pokud zadáte uživatelské jméno nebo heslo špatně třikrát po sobě, dojde k dočasnému uzamčení přihlášení a před dalším pokusem bude nutné pět minut vyčkat.

	Po prvním přihlášení důrazně doporučujeme heslo změnit. Změnu můžete provést v menu Personalizace > Nastavení zařízení. Změnou výchozího hesla značně snížíte riziko neautorizovaného přístupu a použití vašeho modemu.

Obrázek 1-1 Webové rozhraní – standardní

Obrázek 1-2 Webové rozhraní – nesprávné zadání uživatelského jména nebo hesla

Obrázek 1-3 Webové rozhraní – nesprávné zadání uživatelského jména nebo hesla třikrát po sobě

	Pokud používáte prohlížeč Internet Explorer 8 a máte potíže s prohlížením webových stránek i po úspěšném připojení k internetu, může být problém v nastavení prohlížeče. Doporučujeme obnovit nastavení prohlížeče na výchozí hodnoty, případně provést následující opatření. 1. Otevřete prohlížeč IE8 a stiskněte klávesu F12 (Nástroje pro vývojáře). 2. Režim prohlížeče -> Internet Explorer 8.

1.2 Funkční tlačítka

 (odpojeno)

 (připojeno)

 (opětovné připojení)

Funkční tlačítka se nacházejí v pravém horním rohu webového rozhraní.

RESTARTOVÁNÍ

Slouží k vynucenému restartování zařízení.

ODHLÁŠENÍ

Slouží k odhlášení z administračního webového rozhraní a návratu na přihlašovací stránku.

ODPOJENÍ/OPĚTOVNÉ PŘIPOJENÍ

Slouží k odpojení nebo opětovnému připojení zařízení k WAN rozhraní. Funkce opětovného připojení závisí na nastavení automatického připojení. To lze nastavit v nabídce Správa > Nastavení modemu, kde zaškrtněte možnost „Povolit automatické připojení“.

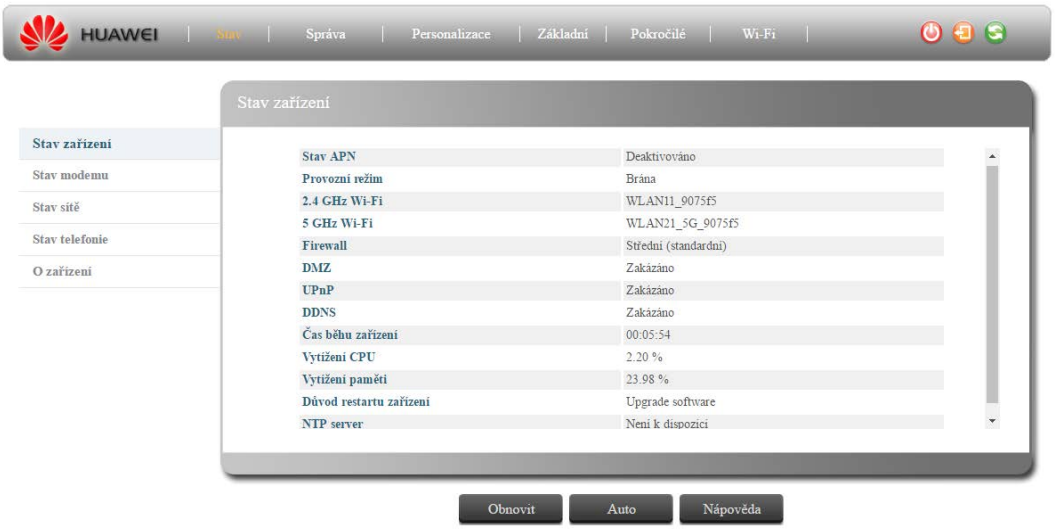
	Pokud je automatické připojení povoleno, zobrazí se ikona OPĚTOVNÉ PŘIPOJENÍ. Pokud automatické připojení není povoleno, zobrazí se po připojení zařízení ikona ODPOJENÍ, která slouží k manuálnímu odpojení. Po případném stisknutí se ikona změní na PŘIPOJENÍ.

1.3 Informace o zařízení a stavech jednotlivých funkcí

1.3.1 Stav > Stav zařízení

Tato stránka slouží pouze pro přehled o aktuálním stavu zařízení. Poskytuje například informace o času běhu zařízení nebo rozhraní WAN. Podrobnější informace o jednotlivých položkách najdete v tabulce níže.

Obrázek 1-4 Stav zařízení



Stav APN – jednoduchý režim Hodnota (aktivováno/deaktivováno) závisí na dostupnosti připojení WAN. **Stav APN Data/VoIP/DM – vícenásobný režim** Hodnota (aktivováno/deaktivováno) závisí na dostupnosti datového, VoIP nebo DM připojení.
Provozní režim Režim směrování datových paketů mezi internetovými porty. Existují tři možnosti: Brána/VPN-L2TP (tunel ve 2. nebo 3. vrstvě OSI modelu)/VPN-GRE (tunel ve 2. nebo 3. vrstvě OSI modelu)/Router. Pro nastavení přejděte do menu Správa > Nastavení WAN.
2,4 GHz Wi-Fi Wi-Fi v pásmu 2,4 GHz.
DNS server – jednoduchý režim Adresa DNS severu se získává ze sítě, pokud je k dispozici. **DNS server pro Data/VoIP/DM – vícenásobný režim** Adresa DNS severu se získává ze sítě pro provoz dat/VoIP/DM, pokud je k dispozici.

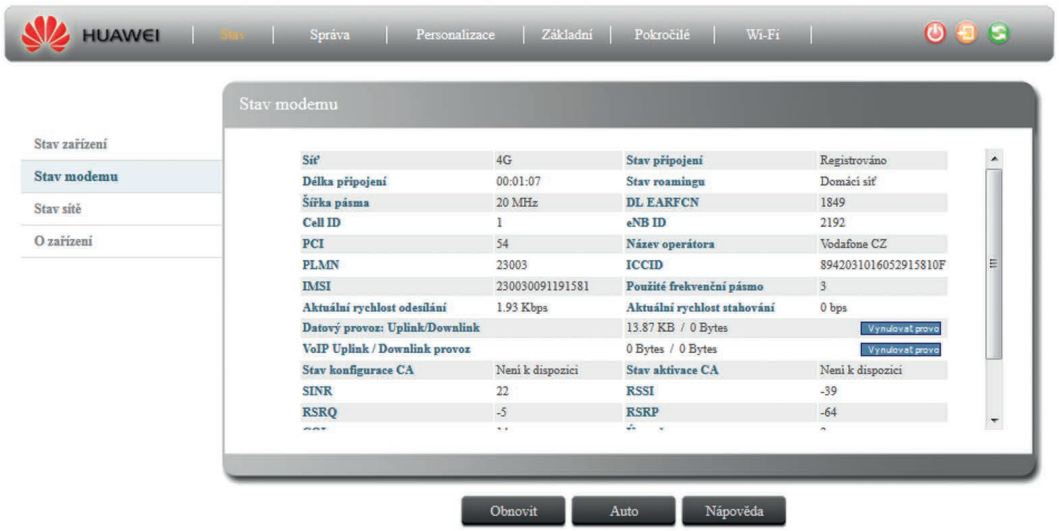
5 GHz Wi-Fi Wi-Fi v pásmu 5 GHz.
NTP server Adresa NTP (Network Time Protocol) serveru.
Firewall Zde se zobrazuje aktuální stupeň zabezpečení branou firewall. K dispozici jsou tři možnosti: Nízká/Střední/Vysoká nebo Vlastní, u které lze jednotlivé parametry brány firewall nastavit ručně. Více informací naleznete v kapitole Základní > Firewall.
DMZ Informace o stavu DMZ (zakázáno/povoleno).
UPnP Informace o stavu UPnP (zakázáno/povoleno).
DDNS Informace o stavu DDNS (zakázáno/povoleno).
Čas běhu zařízení Čas, který uběhl od uvedení zařízení do provozu ve formátu „x dnů <hodin>:<minut>:<vteřin>“.
Vytížení CPU Aktuální vytížení procesoru v procentech.
Vytížení paměti Aktuální vytížení operační paměti v procentech.
Důvod restartu zařízení Důvod, proč bylo zařízení naposledy restartováno (zvoleno zařízením, aktualizace firmware atd.).

	Kliknutím na tlačítko „**Obnovit**“ zapnete manuální aktualizaci všech údajů. Kliknutím na tlačítko „**Auto**“ zapnete automatickou aktualizaci všech údajů.

1.3.2 Stav > Stav modemu

Záložka „Stav modemu“ slouží ke zobrazení všech informací o připojení k LTE síti. Mezi tyto informace patří:

Obrázek 1-5 Stav modemu



Síť Typ sítě, ke kterému je zařízení aktuálně připojeno, např. 4G.
Stav připojení Stav připojení modemu.
Délka připojení Doba, po kterou je zařízení připojeno k vysílači nebo základní stanici.
Stav roamingu Informuje o tom, zda je zařízení připojeno k domácí nebo roamingové síti.
Šířka pásma Udává šířku frekvenčního pásma.
DL EARFCN Udává hodnotu Downlink EARFCN.
Cell ID Identifikátor základní stanice.
eNB ID Identifikátor eNB.
PCI Hodnota kontrolního indikátoru PCI.

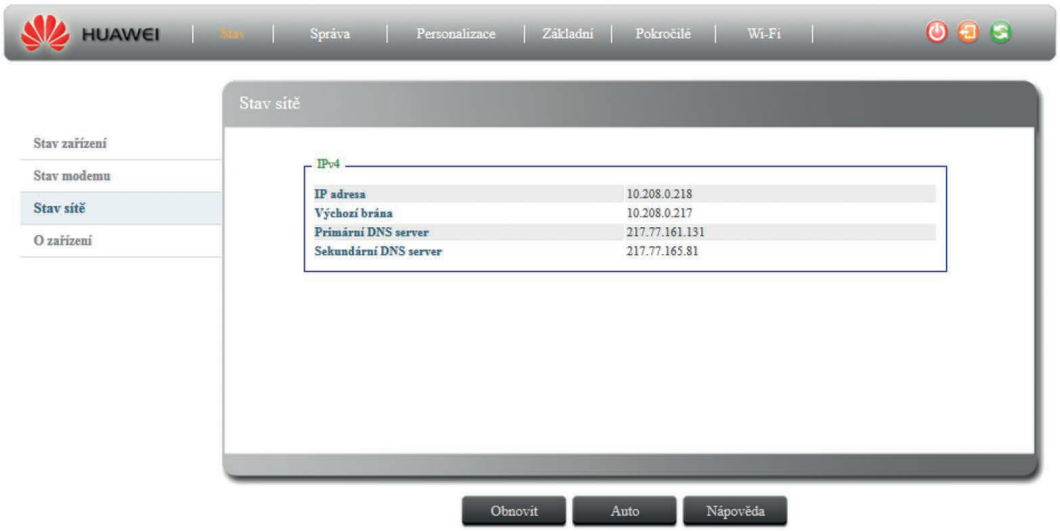
Název operátora Název operátora, k jehož síti je zařízení aktuálně připojeno.
PLMN Identifikační číslo PLMN.
ICCID Identifikační číslo obvodové karty.
IMSI Identifikační číslo vložené SIM karty.
Použité frekvenční pásmo Číslo aktuálně používaného frekvenčního pásma (dle 3GPP).
Aktuální rychlost odesílání Rychlost probíhajícího odesílání (upload).
Aktuální rychlost stahování Rychlost probíhajícího stahování (download).
Datový provoz: Uplink/Downlink Zobrazuje celkový datový provoz odesílání a stahování. Počítadlo je možné vynulovat kliknutím na tlačítko „Vynulovat provoz“ na pravé straně.
VoIP Uplink/Downlink provoz Zobrazuje celkový VoIP provoz odesílání a stahování. Počítadlo je možné vynulovat kliknutím na tlačítko „Vynulovat provoz“ na pravé straně.
Stav UL CA Informace o Uplink Carrier Aggregation.
Stav DL CA Informace o Downlink Carrier Aggregation.
SINR Hodnota odstupu signál-šum plus interference (v dB).
RSSI Hodnota síly přijatého signálu (dílčí jednotka 1 dBm). Minimum: -141.
RSRQ Kvalita přijatého referenčního signálu (dílčí jednotka 0,5 dBm). Minimum: -40.
RSRP Výkon přijatého referenčního signálu (dílčí jednotka 1 dBm). Minimum: -141.
CQI Indikátor kvality kanálu.
PIN: zbývající počet pokusů Zbývající počet pokusů pro zadání kódu PIN.

PUK: zbývající počet pokusů Zbývající počet pokusů pro zadání kódu PUK.
Stav USIM Informace o stavu SIM karty.

	Kliknutím na tlačítko „**Obnovit**“ zapnete manuální aktualizaci všech údajů. Kliknutím na tlačítko „**Auto**“ zapnete automatickou aktualizaci všech údajů.

1.3.3 Stav > Stav sítě

Obrázek 1-6 Stav sítě – data



DATA

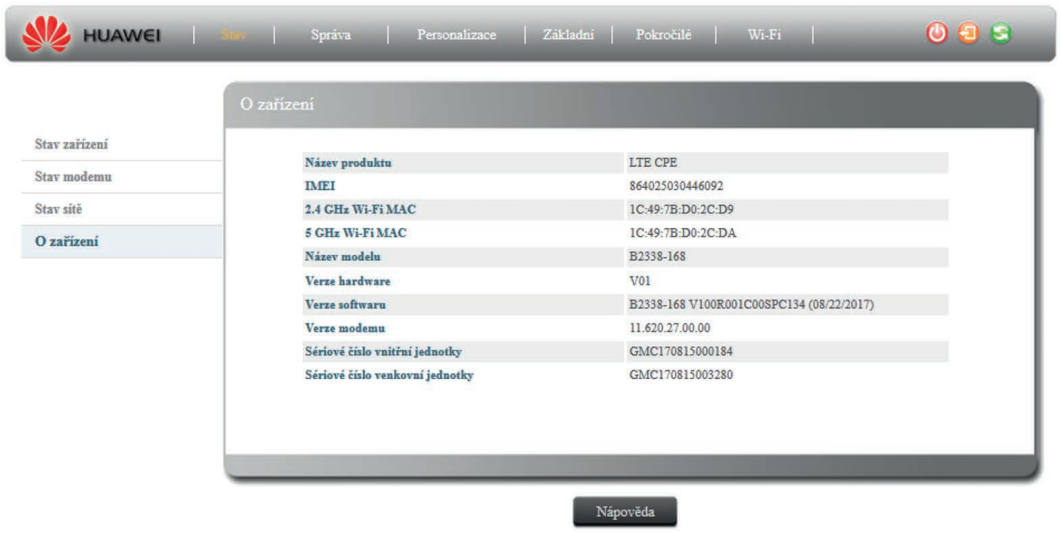
- **IPv4**
  - **IP adresa:** IP adresa získaná prostřednictvím WAN rozhraní. Pokud adresa není k dispozici, zobrazí se hodnota N/A.
  - **Primární DNS server:** Adresa DNS severu se získává ze sítě, pokud je k dispozici.
  - **Sekundární DNS server:** Adresa sekundárního DNS severu se získává ze sítě, pokud je k dispozici.

	Kliknutím na tlačítko „**Obnovit**“ zapnete manuální aktualizaci všech údajů. Kliknutím na tlačítko „**Auto**“ zapnete automatickou aktualizaci všech údajů.

1.3.4 Stav > O zařízení

V této záložce jsou uvedeny nezbytné informace o zařízení. Uvedené hodnoty jsou určeny výrobcem.

Obrázek 1-7 O zařízení



Název produktu Identifikační název přístroje.
2,4 GHz Wi-Fi MAC MAC adresa 2,4GHz Wi-Fi
5 GHz Wi-Fi MAC MAC adresa 5GHz Wi-Fi.
Název modelu Identifikační číslo typu přístroje.
Verze hardware Verze HW zařízení.
Verze softwaru Verze softwaru/firmwaru zařízení.

Sériové číslo vnitřní jednotky Sériové číslo vnitřní jednotky.
Sériové číslo venkovní jednotky Sériové číslo venkovní jednotky.

1.4 Struktura menu

Mezi dílčími nastavení přístroje lze procházet pomocí jednotlivých podmenu.

Struktura podmenu odpovídá následujícímu přehledu:

Stav	Stav zařízení
	Stav modemu
	Stav sítě
	Stav telefonie (po povolení hovorů VoIP)
	O zařízení
Správa	Rychlé nastavení
	Nastavení modemu
	Nastavení WAN
	Nastavení LAN
	Nastavení IPv6
	Nastavení telefonie
	Diagnostika
	Systémový log
Personalizace	Správa PIN
	Nastavení
	Nastavení zařízení
	Software
Základní	Firewall
	DMZ
	UPnP
	Dynamické DNS
	VPN Passthrough

Pokročilé	Filtr síťových adres MAC
	Filtr IP adres
	Přesměrování portu
	Port Triggering
	Filtrování 7. vrstvy (OSI modelu)
	URL filtrování
	ACL filtrování
	Rodičovský zámek
	Statické směrování
Wi-Fi	Základní
	Pokročilé
	WPS
	Připojený klient

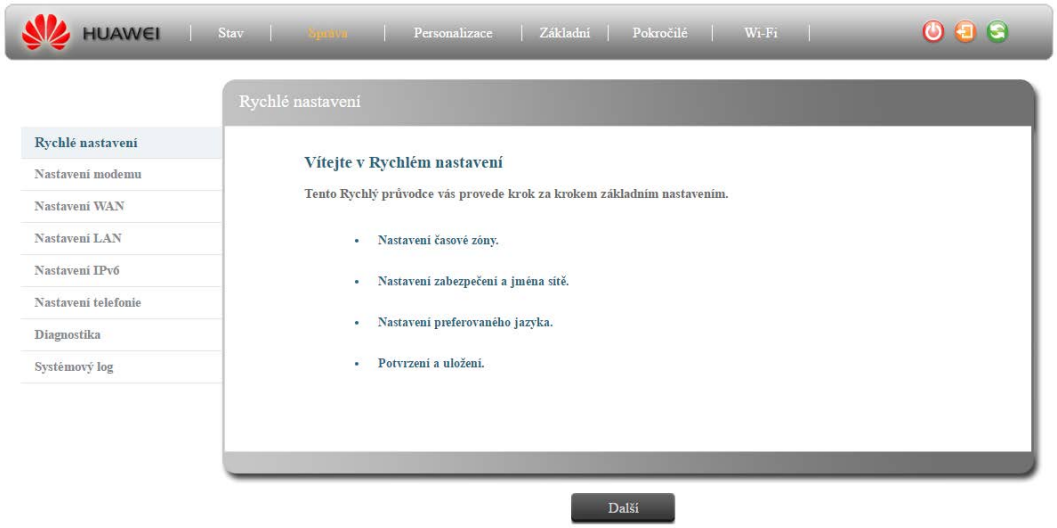
2 Referenční příručka

Obsah této kapitoly

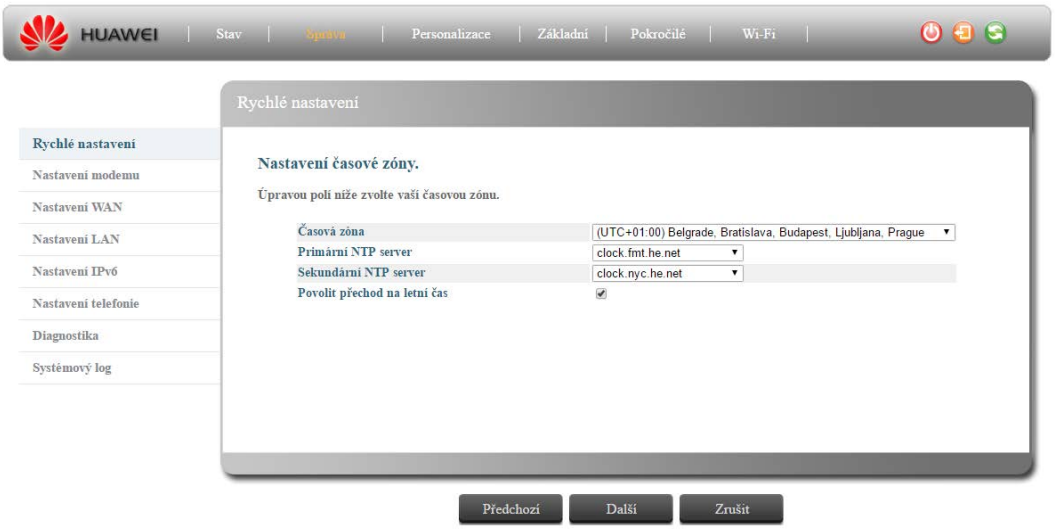
2.1 Správa

2.1.1 Správa > Rychlé nastavení

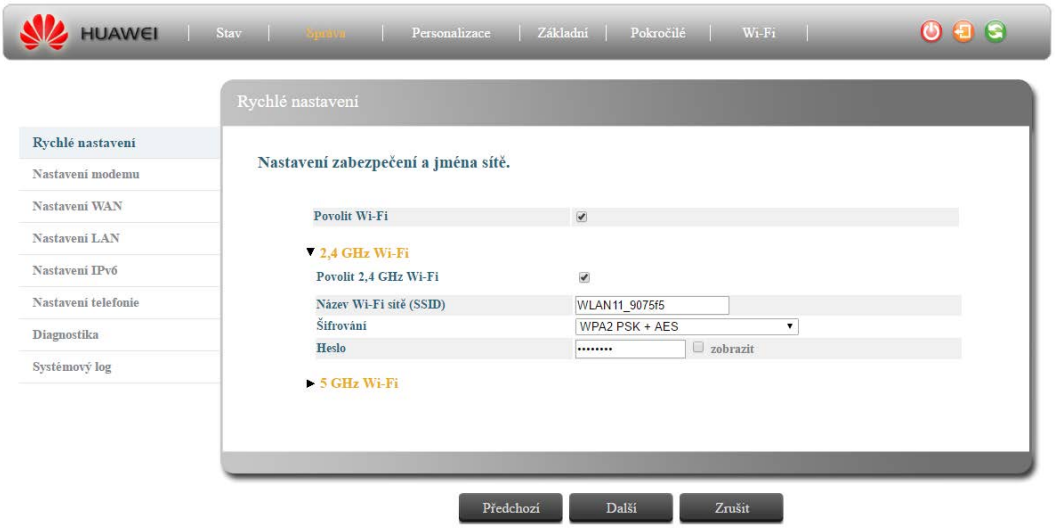
Obrázek 2-1 Rychlé nastavení



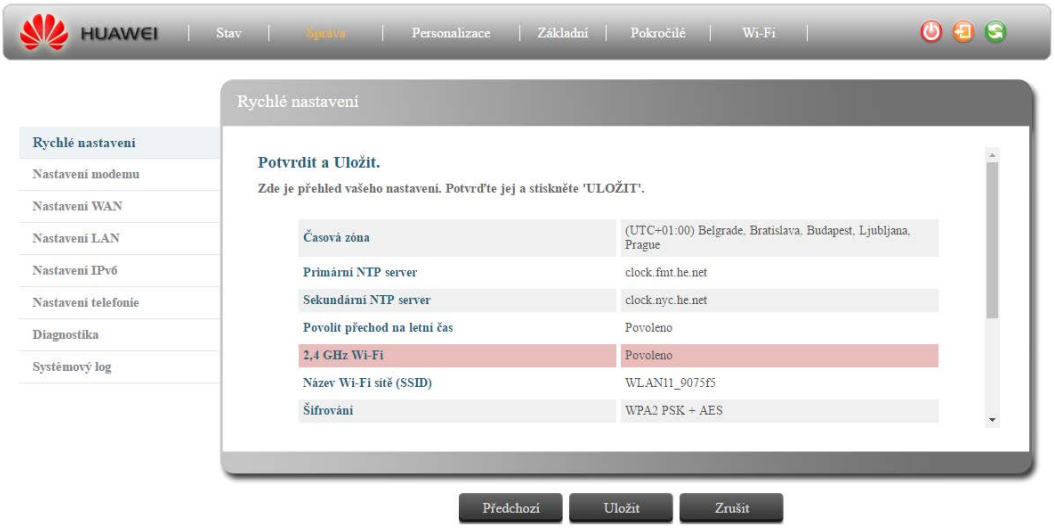
Obrázek 2-2 Rychlé nastavení – nastavení časové zóny



Obrázek 2-3 Rychlé nastavení – nastavení zabezpečení a jména sítě



Obrázek 2-4 Rychlé nastavení – přehled



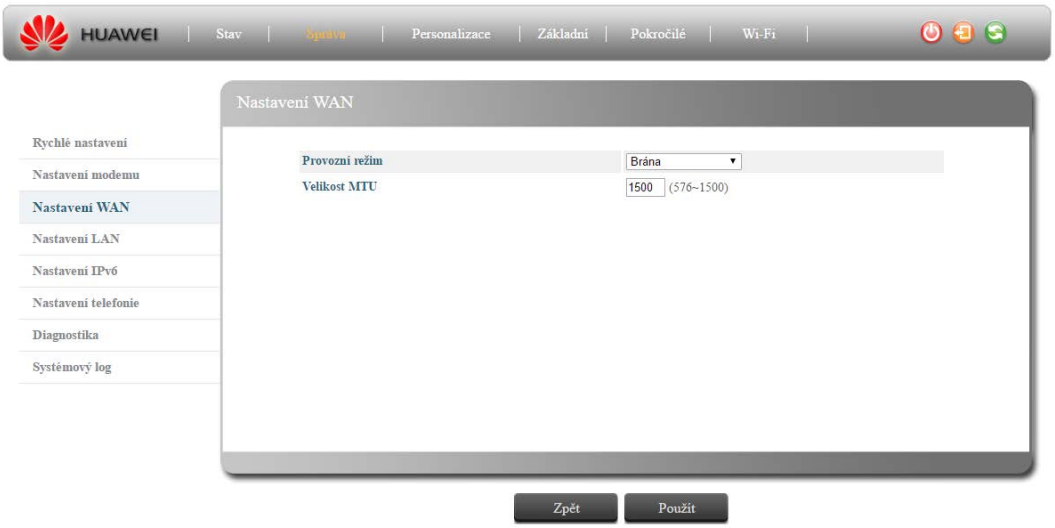
Průvodce rychlým nastavením slouží pro přehledné nastavení nejdůležitějších funkcí zařízení.

- Krok 1: Kliknutím na tlačítko „**Další**“ spustíte průvodce, jehož prvním krokem bude nastavení časové zóny.
- Krok 2: a. Vyberte ze seznamu časovou zónu místa, ve kterém se nacházíte, zadejte adresy NTP serverů a zvolte, zda ve vaší zemi platí přechod na letní čas.
  b. Zkontrolujte zadaná nastavení a pokud nenarazíte na problém, klikněte na tlačítko „**Další**“.
- Krok 3: Zadejte název sítě, typ šifrování a heslo sítě Wi-Fi v pásmu 2,4 a 5 GHz a klikněte na tlačítko „**Další**“.
- Krok 4: Ještě jednou zkontrolujte všechna nastavení a stiskněte pro uložení tlačítko „**Uložit**“.

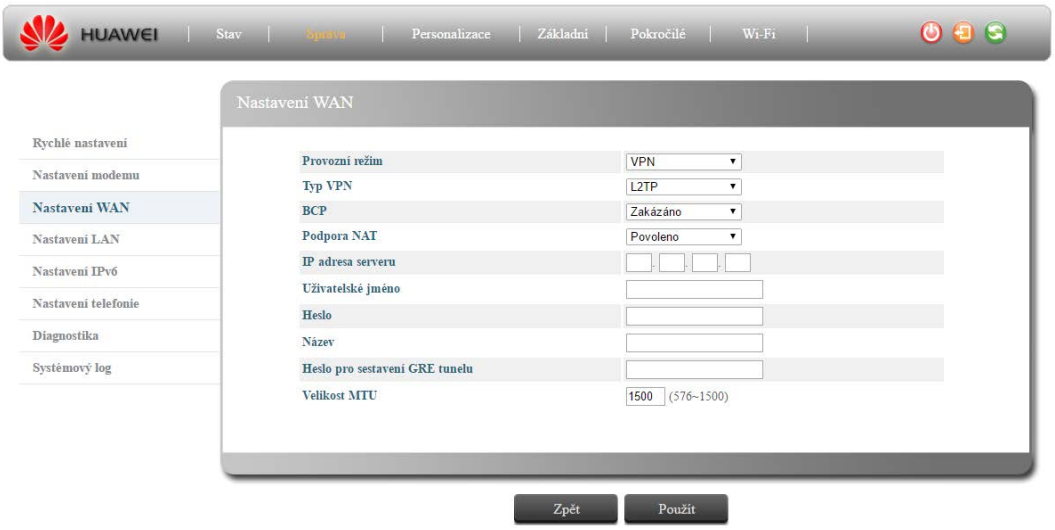
	Kliknutím na tlačítko „**Další**“ přejdete k dalšímu kroku rychlého nastavení. Kliknutím na tlačítko „**Předchozí**“ se vrátíte na předchozí stránku. Kliknutím na tlačítko „**Zrušit**“ se vrátíte na úvodní stránku. Kliknutím na tlačítko „**Uložit**“ uložíte provedené změny.

2.1.2 Správa > Nastavení WAN

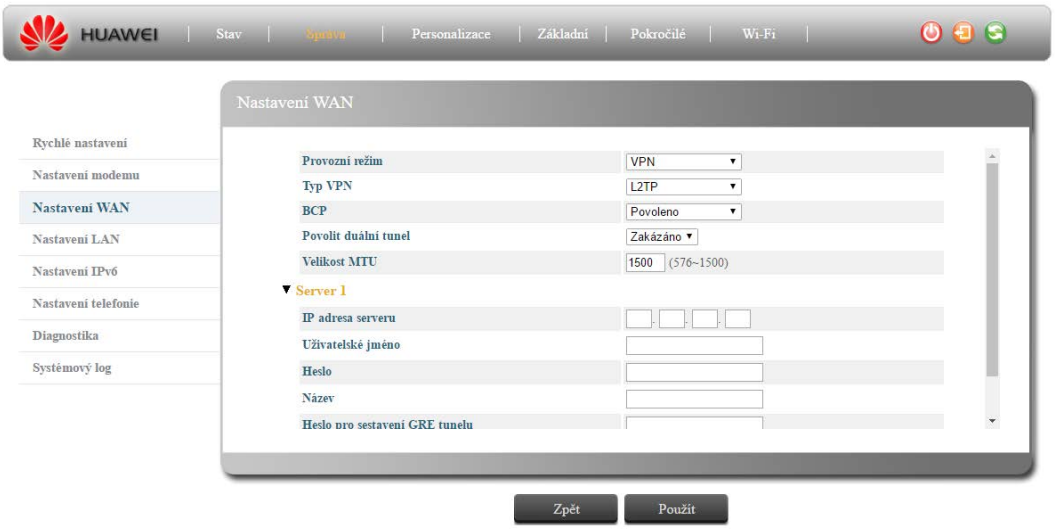
Obrázek 2-5 Brána



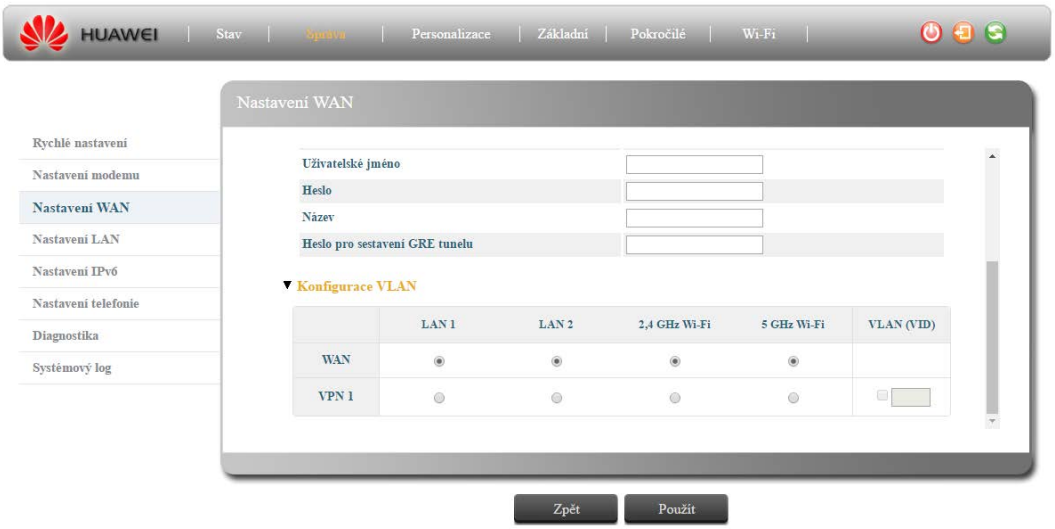
Obrázek 2-6 L2TP (BCP zakázáno)



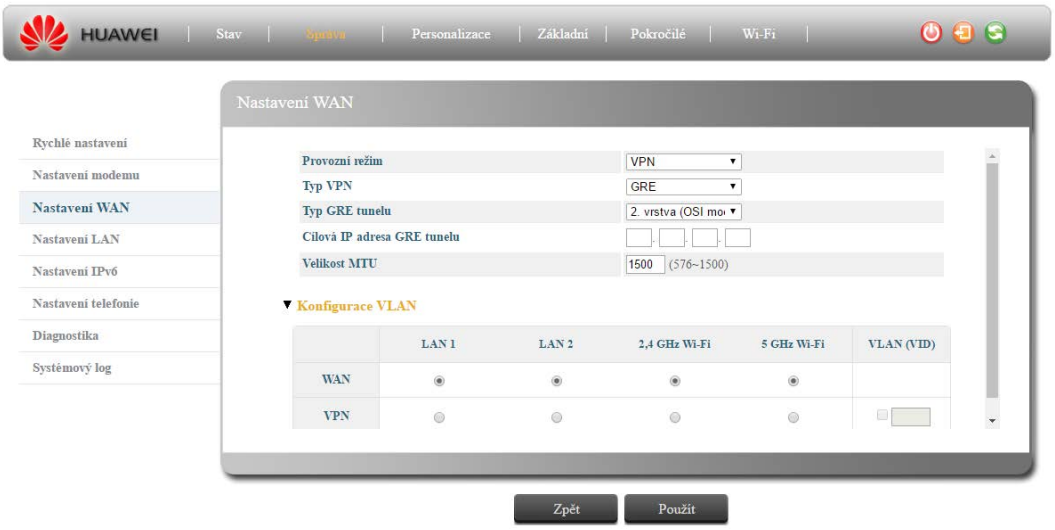
Obrázek 2-8 L2TP (BCP povoleno) – server



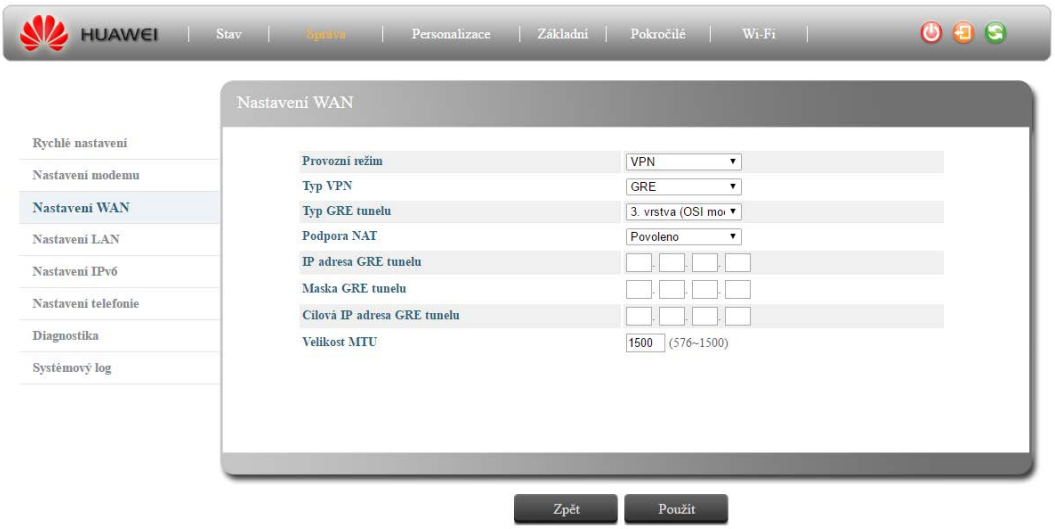
Obrázek 2-9 L2TP (BCP povoleno) – konfigurace VLAN



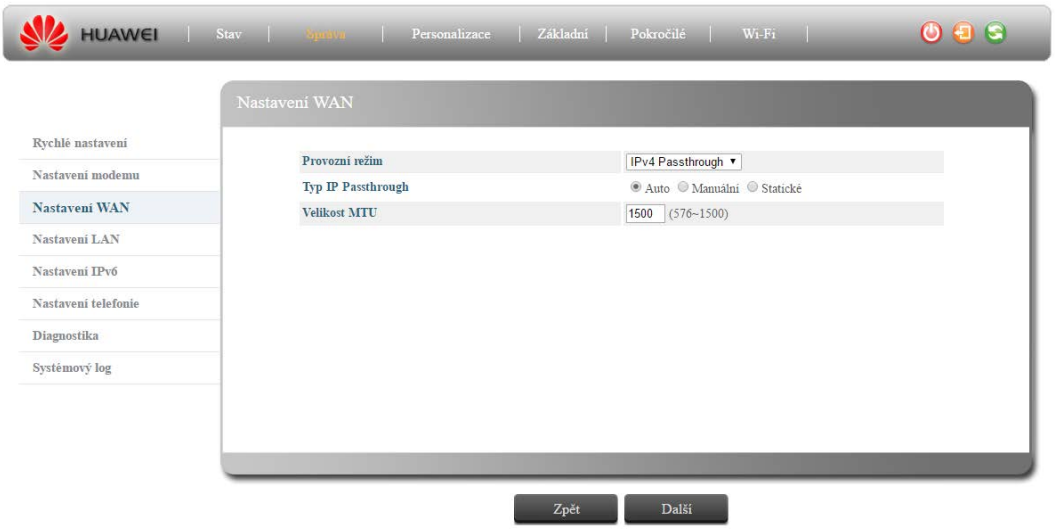
Obrázek 2-10 Nastavení WAN – GRE (2. vrstva OSI modelu)



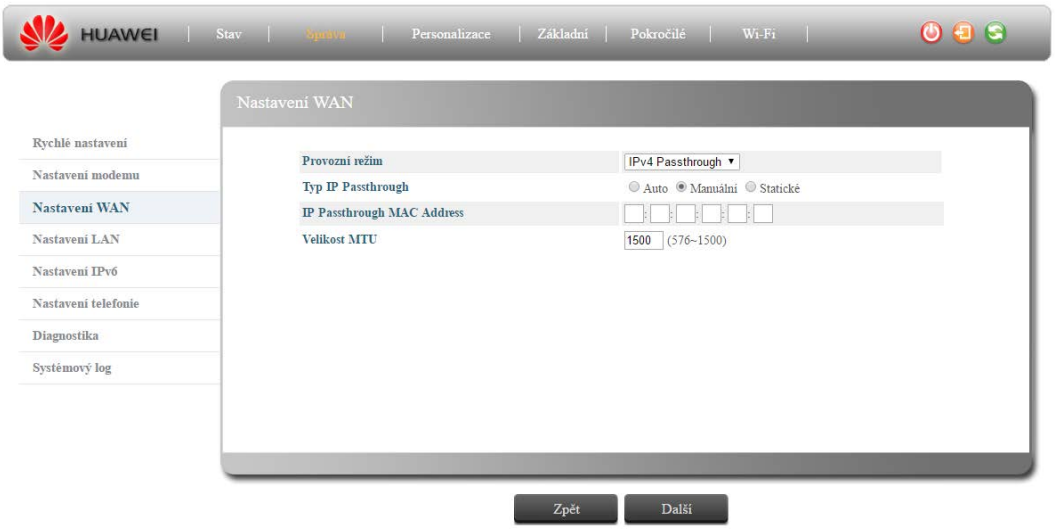
Obrázek 2-11 Nastavení WAN – GRE (3. vrstva OSI modelu)



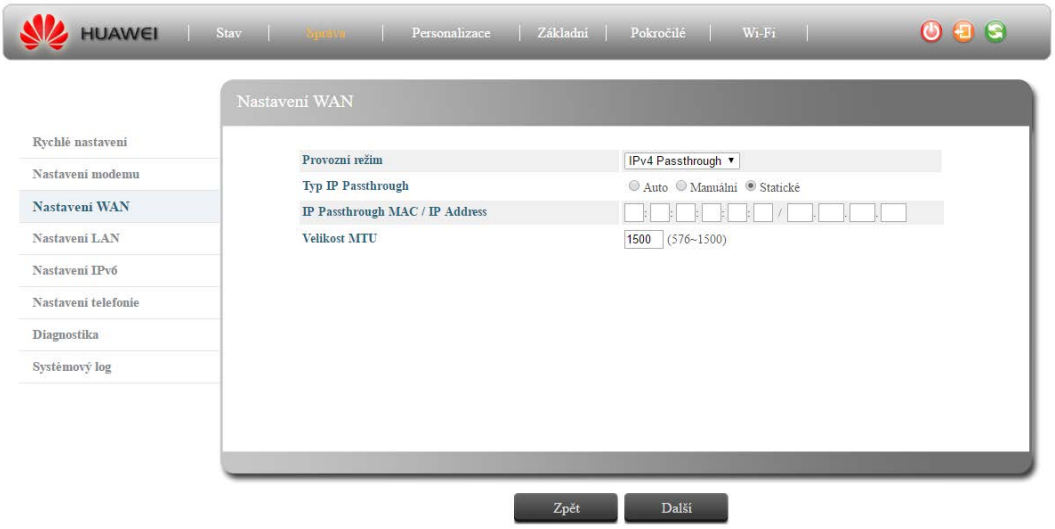
Obrázek 2-12 Nastavení WAN – IPv4 Passthrough (Auto)



Obrázek 2-13 Nastavení WAN – IPv4 Passthrough (Manuální)



Obrázek 2-14 Nastavení WAN – IPv4 Passthrough (Statické)



Provozní režim

Režim směrování datových paketů mezi internetovými a intranetovými porty.

Režim Brána

Režim získávání IP adresy zařízení, ve kterém je povolen zabezpečený překlad adres SNAT.

- **Velikost MTU:** Velikost maximální přenosové jednotky (MTU) v bajtech. Zadejte velikost přenosové jednotky (rozsah: 576–1500).

Režim VPN

- **Typ VPN:** Slouží k nastavení typu VPN. Toto zařízení podporuje L2TP a GRE.
  - **L2TP**
    - **BCP: Povoleno:** Připojení L2 VPN je možné.
      - **Povolit duální tunel:**
      - **Velikost MTU:** Zadejte velikost přenosové jednotky (rozsah: 576–1500).
    - **Server 1**
      - **IP adresa serveru:** IP adresa VPN serveru 1, ke které se chcete připojit.
      - **Uživatelské jméno:** Uživatelské jméno pro VPN účet.
      - **Heslo:** Heslo k vašemu VPN účtu.
      - **Název:** Pokud server vyžaduje název zařízení, vyplňte toto pole.
      - **Heslo pro sestavení GRE tunelu:**
    - **Server 2**
      - **IP adresa serveru:** IP adresa VPN serveru 2, ke které se chcete připojit.
      - **Uživatelské jméno:** Uživatelské jméno pro VPN účet.
      - **Heslo:** Heslo k vašemu VPN účtu.
      - **Název:** Pokud server vyžaduje název zařízení, vyplňte toto pole.
      - **Heslo pro sestavení GRE tunelu:**
    - **BCP: Zakázáno:** Připojení L3 VPN je možné.
      - **Podpora NAT**
        - **Povoleno:** Zařízení s vnitřní IP adresou může provádět překlad NAT.
        - **Zakázáno:** Zařízení s vnitřní IP adresou nemůže obejít překlad NAT.
      - **IP adresa serveru:** IP adresa VPN serveru, ke které se chcete připojit.
      - **Uživatelské jméno:** Uživatelské jméno pro VPN účet.
      - **Heslo:** Heslo k vašemu VPN účtu.
      - **Název:** Pokud server vyžaduje název zařízení, vyplňte toto pole.
      - **Heslo pro sestavení GRE tunelu:**

	Pokud zvolíte VPN s tunelem ve 3. vrstvě OSI modelu, je zapotřebí přidat příslušné pravidlo směrování v menu Pokročilé > Statické směrování.

- **GRE**
  - ♦ **Typ GRE tunelu: 2. vrstva (OSI modelu)**
    - **Cílová IP adresa GRE tunelu:** Zadejte cílovou IP adresu VPN tunelu.
    - **Velikost MTU:** Zadejte velikost přenosové jednotky (rozsah: 576–1500).
  - ♦ **Typ GRE tunelu: 3. vrstva (OSI modelu)**
    - **Podpora NAT:**
      - ■ **Povoleno:** Zařízení s vnitřní IP adresou může provádět překlad NAT.
      - ■ **Zakázáno:** Zařízení s vnitřní IP adresou nemůže obejít překlad NAT.
    - **IP adresa GRE tunelu:** Zadejte IP adresu VPN tunelu.
    - **Maska GRE tunelu:** Zadejte masku podsítě VPN tunelu.
    - **Cílová IP adresa GRE tunelu:** Zadejte cílovou IP adresu VPN tunelu.
    - **Velikost MTU:** Zadejte velikost přenosové jednotky (rozsah: 576–1500).

Konfigurace VLAN

- ➢ **WAN:** Pakety ze zařízení vycházejí prostřednictvím WAN rozhraní: WAN.
- ➢ **VLAN (1,2):** Pakety z PC připojeného k LAN vycházejí prostřednictvím WAN rozhraní: VLAN (1,2).
- ➢ **LAN1 (2):** Pakety z PC připojeného k LAN vycházejí prostřednictvím LAN rozhraní: LAN1 (2).
- ➢ **2,4 GHz Wi-Fi:** Pakety z PC připojeného k LAN vycházejí prostřednictvím LAN rozhraní: Wi-Fi v pásmu 2,4 GHz.
- ➢ **5 GHz Wi-Fi:** Pakety z PC připojeného k LAN vycházejí prostřednictvím LAN rozhraní: Wi-Fi v pásmu 5 GHz.
- ➢ **VLAN (VID):** Identifikátor virtuální LAN (Virtual ID).

Režim IPv4 Passthrough

- ➢ **Typ IP Passthrough:** Slouží k nastavení typu IP passthrough. Toto zařízení podporuje typ auto, manuální a statické.
  - **IP Passthrough MAC Address:** MAC adresa klienta.
  - **IP Passthrough IP Address:** IP adresa klienta.

Režim Router

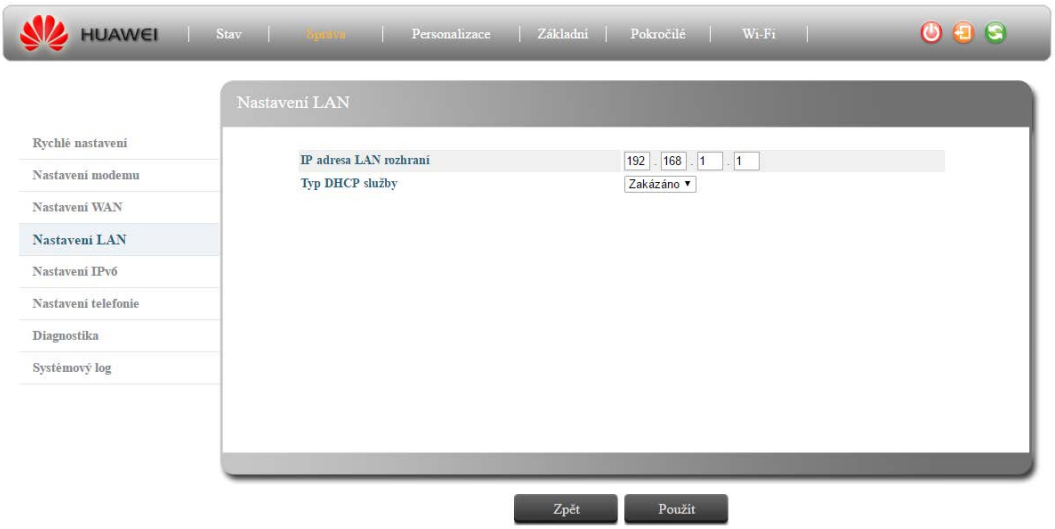
Pokud je zařízení v režimu Router, bude překlad adres SNAT zakázán a bránu firewall (tj. DMZ a přesměrování portů) nebude možné aktivovat.

- ➢ **Velikost MTU:** Velikost maximální přenosové jednotky (MTU) v bajtech. Zadejte velikost přenosové jednotky (rozsah: 576–1500).

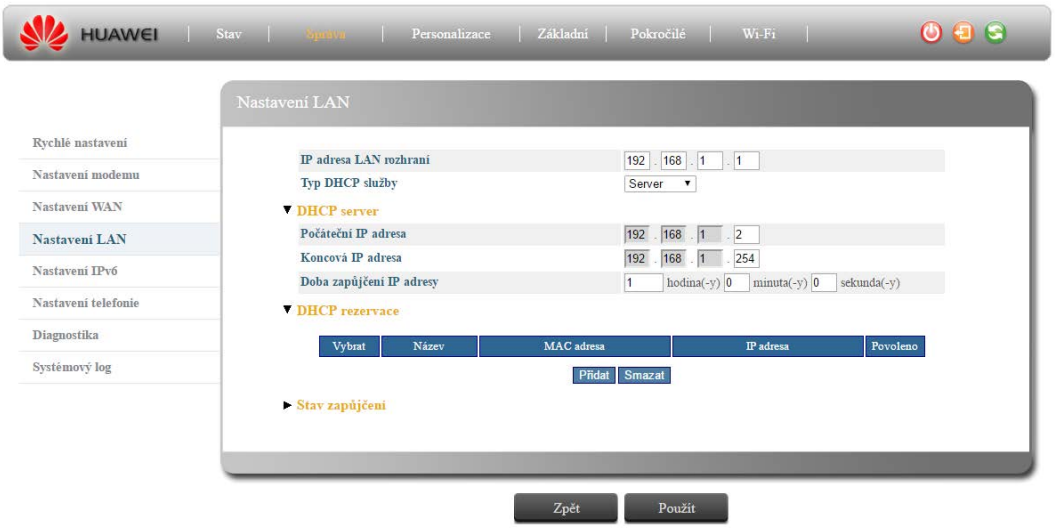
2.1.3 Správa > Nastavení LAN

Prostřednictvím této nabídky je možné změnit rozsah distribuce lokálních IP adres.

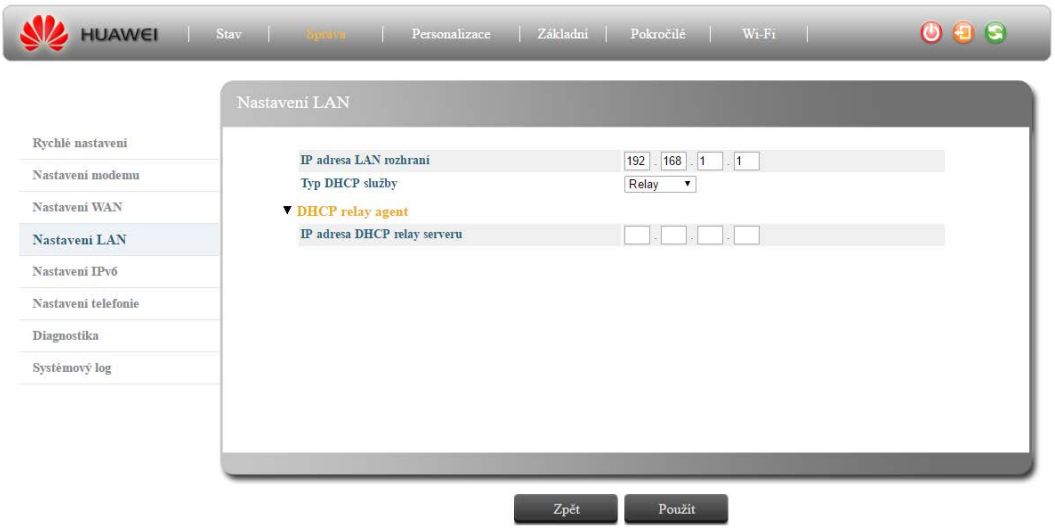
Obrázek 2-15 Nastavení LAN – zakázáno



Obrázek 2-16 Nastavení LAN – server



Obrázek 2-17 Nastavení LAN – relay



IP adresa LAN rozhraní: Zadejte požadovanou IP adresu LAN rozhraní. Výchozí hodnotou je 192.168.1.1.
Typ DHCP služby Vyberte požadovaný typ DHCP služby. Možnosti: zakázáno, server, relay. ➢ **Zakázáno:** Zařízení nebude žádným způsobem přiřazovat IP adresy k připojeným PC. IP adresu je nutné zadat manuálně, aby bylo možné přistupovat k administrátorskému rozhraní. ➢ **DHCP server:** Toto zařízení je vybaveno DHCP serverem, který je možné použít pro automatické řízení a přiřazování IP adres počítačům a zařízením připojeným k lokálním LAN rozhraním (ethernetovým nebo Wi-Fi). Dílčí nastavení parametrů dynamického přiřazování IP adres je možné provést v záložce „DHCP server“.
Typ DHCP služby: server Zvolením této možnosti z rozbalovací nabídky bude automaticky spuštěna dynamická rezervace IP adres zařízením připojených k místní síti. Pokud zvolíte možnost „Zakázáno“, bude zapotřebí IP adresy jednotlivým zařízením přidělit manuálně.
IP adresa DHCP serveru: Zadejte IP adresu DHCP serveru.
Počáteční IP adresa Zadejte dolní mez rozpětí přiřazování IP adres DHCP serverem.

Koncová IP adresa

Zadejte horní mez rozpětí přiřazování IP adres DHCP serverem.

Doba zapůjčení IP adresy

Zadejte dobu, po jejímž uplynutí bude zařízení přiřazena nová IP adresa.

DHCP rezervace

Záložka „DHCP rezervace“ obsahuje informace o rezervovaných IP adresách pro určitá zařízení. Můžete zde vytvořit pravidlo, podle kterého bude konkrétním zařízením připojeným k ethernetovým portům nebo prostřednictvím Wi-Fi přiřazována určitá, stále stejná IP adresa. Jednotlivá pravidla lze přidávat, mazat nebo upravovat.

- **Vybrat**

Zaškrtněte IP adresu, kterou si přejete smazat.

- **Název**

Zadejte název zařízení.

- **MAC adresa**

Zadejte MAC adresu zařízení.

- **IP adresa**

Vložte IP adresu, která bude zařízení se zadanou MAC adresou vždy přiřazena.

- **Povoleno**

Zaškrtněte, pokud chcete pravidlo pro danou IP adresu povolit.

Stav zapůjčení

Záložka „Stav zapůjčení“ informuje o přidělených IP adresách a jednotlivých zařízeních:

- **Název klienta**

Název PC nebo jiného zařízení připojeného k LTE modemu.

- **MAC adresa**

MAC adresa PC nebo jiného zařízení připojeného k LTE modemu.

- **IP adresa**

IP adresa přiřazená příslušnému PC nebo jinému zařízení v síti LAN.

- **Zbývající doba zapůjčení**

Doba, která zbývá před vypršením platnosti příslušné IP adresy.

- **Akce**

Blokování: Pokud chcete zablokovat některé z připojených zařízení, klikněte na tlačítko „**Blokovat**“. Dané zařízení se nadále nebude moci připojit k tomuto LTE modemu.

Odblokování: Kliknutím na tlačítko „**Odblokovat**“ zablokovanému zařízení opět umožníte se k LTE modemu připojit.

Touto funkcí můžete snadno spravovat připojená zařízení a zabránit tak nevyžádanému připojení k vaší síti LAN.

- **Stav**

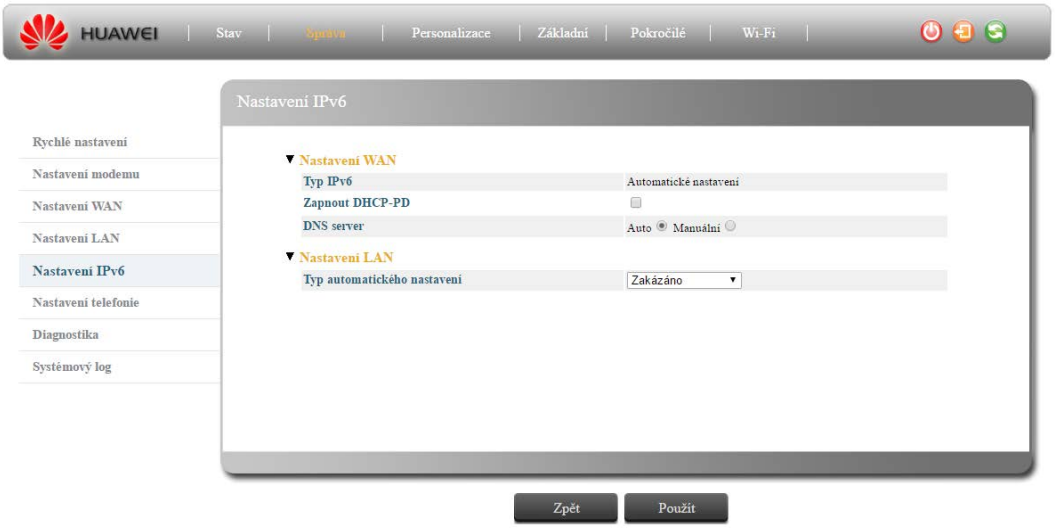
Tato položka indikuje aktuální stav připojeného zařízení.

IP adresa DHCP relay serveru:
Zařízení vyžádá IP adresu od DHCP relay serveru. Zadejte tedy IP adresu příslušného DHCP relay serveru. Pokud zadáte neplatnou IP adresu DHCP relay serveru nebo pokud daný server nebude v provozu, přiřaďte IP adresy připojeným zařízením manuálně dle postupu výše.

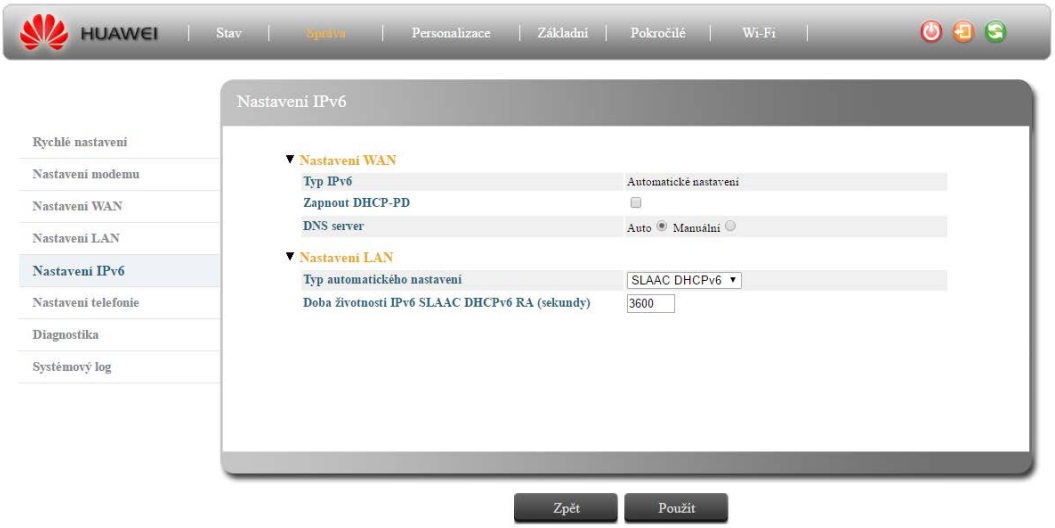
	Pomocí tlačítek „Přidat“ a „Smazat“ lze přidávat nebo mazat rezervace IP adres. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko „Zpět“ vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko „Použít“ provedené změny uložíte.

2.1.4 Správa > Nastavení IPv6

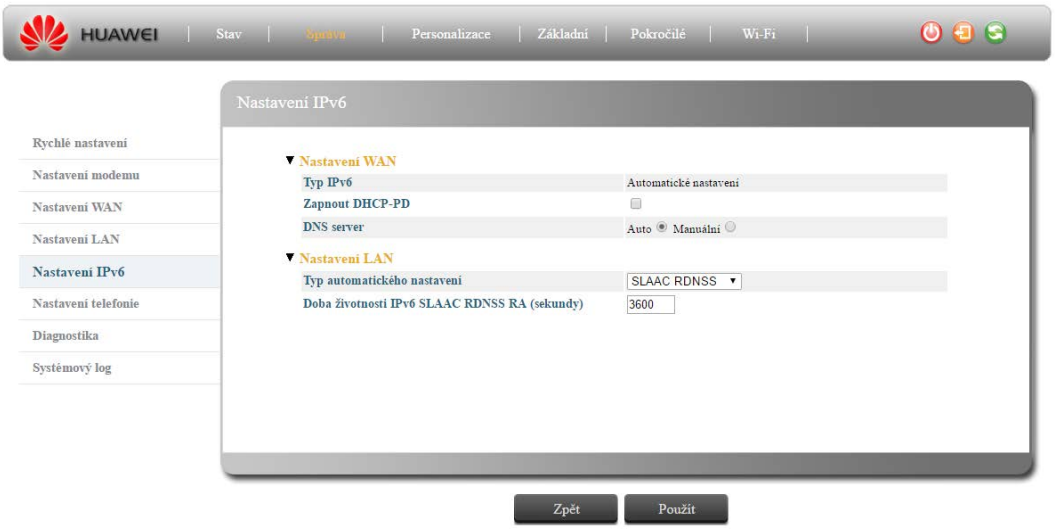
Obrázek 2-18 Nastavení IPv6 – automatické nastavení LAN zakázáno



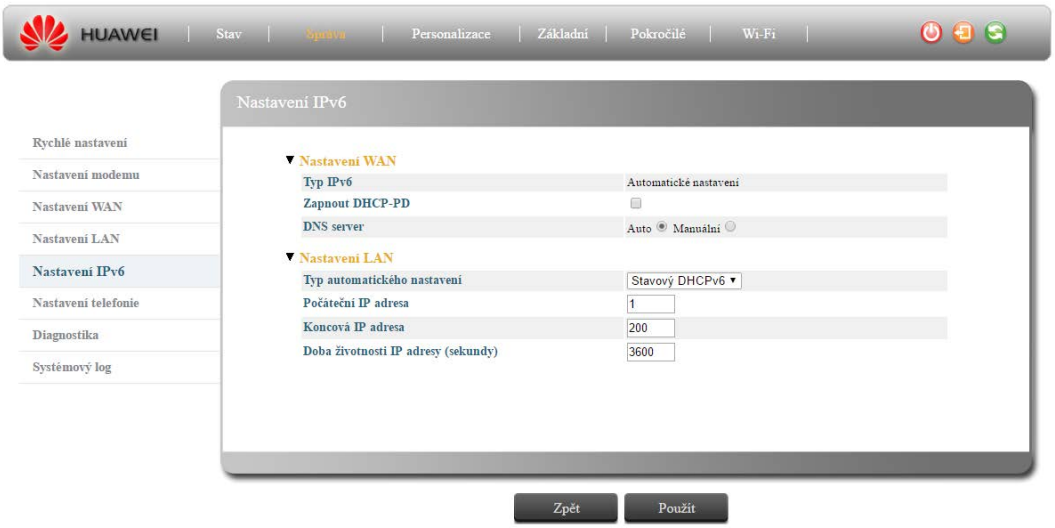
Obrázek 2-19 Nastavení IPv6 – SLAAC DHCPv6



Obrázek 2-20 Nastavení IPv6 – SLAAC RDNSS



Obrázek 2-21 Nastavení IPv6 – Stavový DHCPv6



Nastavení WAN:

- **Typ IPv6:**
  - **Automatické nastavení:** Zařízení přiřadí IPv6 adresu automaticky.
- **Zapnout DHCP-PD:** Zaškrtnutím této položky povolíte serveru DHCP-PD přiřazování prefixů připojeným klientům.

  DNS Sever: Vyberte, zda si přejete získat informace o DNS serveru automaticky nebo zadat manuálně.
  - **Primární DNS server:** Zadejte adresu IPv6 DNS serveru.
  - **Sekundární DNS server:** Zadejte adresu sekundárního IPv6 DNS serveru, pokud je k dispozici.

Nastavení LAN:

- **Typ automatického nastavení:** Zakázáno, SLAAC DHCPv6, SLAAC RDNSS, stavový DHCPv6.
  - **Zakázáno:** Přiřazování IPv6 adres LAN klientům bude vypnuto.
  - **SLAAC DHCPv6:** (bezstavové automatické nastavení DHCPv6), ohlašování směrovače (RA) přiřadí IPv6 prefix a údaje o výchozí bráně, zatímco DHCPv6 poskytne adresu DNS serveru a další síťové parametry. Tato metoda automatického přiřazování IP adres je doporučena v soukromých sítích, jelikož neposkytuje příliš vysokou úroveň zabezpečení.
    - Doba životnosti IPv6 SLAAC DHCPv6 RA (sekundy): Platnost přiřazené IP adresy vyprší po zadané době. Výchozí hodnota: 3600 sekund.
  - **SLAAC RDNSS:** (bezstavové automatické nastavení + rekurzivní DNS server), ohlašování směrovače (RA) pravidelně vysílá multicast pakety, ze kterých klient získá prefix, informace o výchozí bráně a DNS serveru. Na straně klienta se pomocí prefixu vygeneruje host ID, což bude současně IPv6 adresa zařízení.
    - Doba životnosti IPv6 SLAAC RDNSS RA (sekundy): Platnost přiřazené IP adresy vyprší po zadané době. Výchozí hodnota: 3600 sekund.
  - **Stavový DHCPv6:** Ohlašování směrovače (RA) poskytne pouze informace o výchozí bráně. Ostatní parametry, jako je IPv6 prefix, host ID a IP adresa DNS serveru, přiřadí protokol DHCPv6. Ten rovněž udržuje záznamy o všech přiřazených IPv6 adresách a seznam MAC adres a provádí jejich pravidelnou aktualizaci. Použití stavového DHCPv6 je doporučeno u veřejných sítí.
    - Počáteční IP adresa: Zadání spodní meze přiřazování IP adres. Výchozí hodnota: 1
    - Koncová IP adresa: Zadání horní meze přiřazování IP adres. Výchozí hodnota: 200
    - Doba životnosti IP adresy (sekundy): Platnost přiřazené IP adresy vyprší po zadané době. Výchozí hodnota: 3600 sekund.

	Kliknutím na tlačítko „**Obnovit**“ zapnete manuální aktualizaci všech údajů. Kliknutím na tlačítko „**Auto**“ zapnete automatickou aktualizaci všech údajů.

2.1.5 Správa > Nastavení telefonie

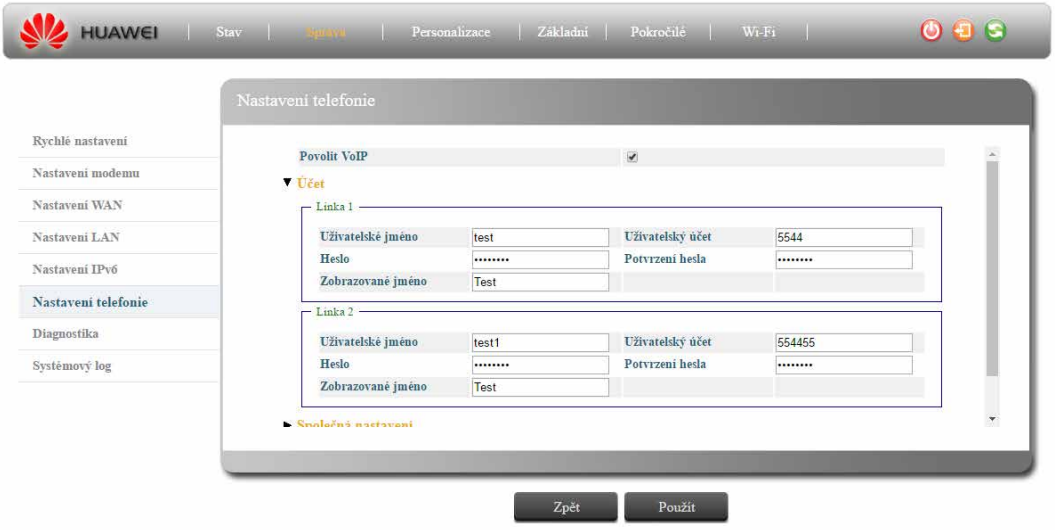
Tato kapitola popisuje nastavení parametrů pro hovory VoIP.

Voice over Internet Protocol (zkratkou VoIP) je technologie umožňující přenos telefonních hovorů prostřednictvím internetu. Standardní telefon je možné připojit do konektorů PHONE na tomto zařízení.

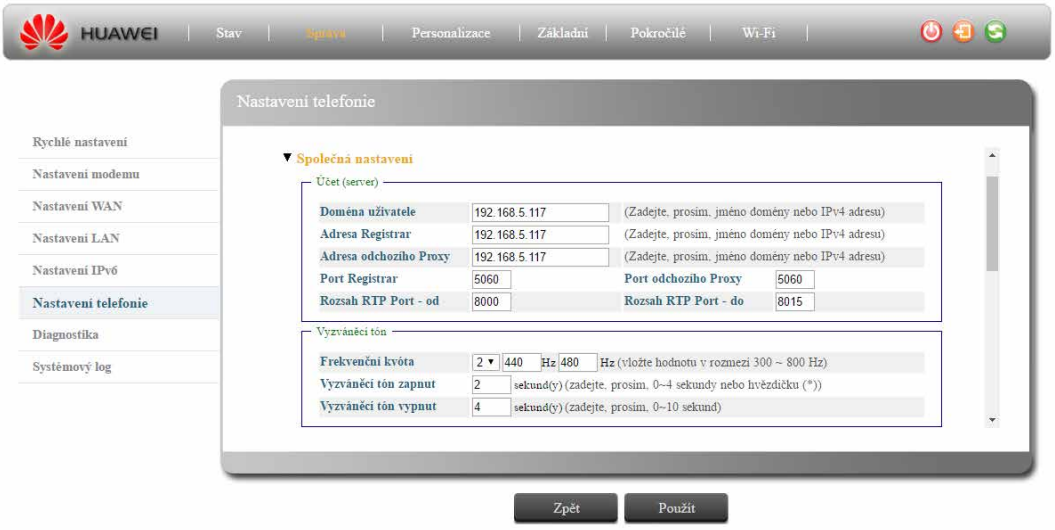
Před prvním použitím VoIP je nutné si vytvořit účet a získat přístup prostřednictvím protokolu SIP u vašeho operátora. Před nastavením popsaným níže si u vašeho operátora ověřte platnost údajů a dostupnost služby. (Provozovatel Vodafone CZ aktuálně tuto službu nepodporuje.)

	VoIP telefonie nepodporuje funkci Flash + číslo.

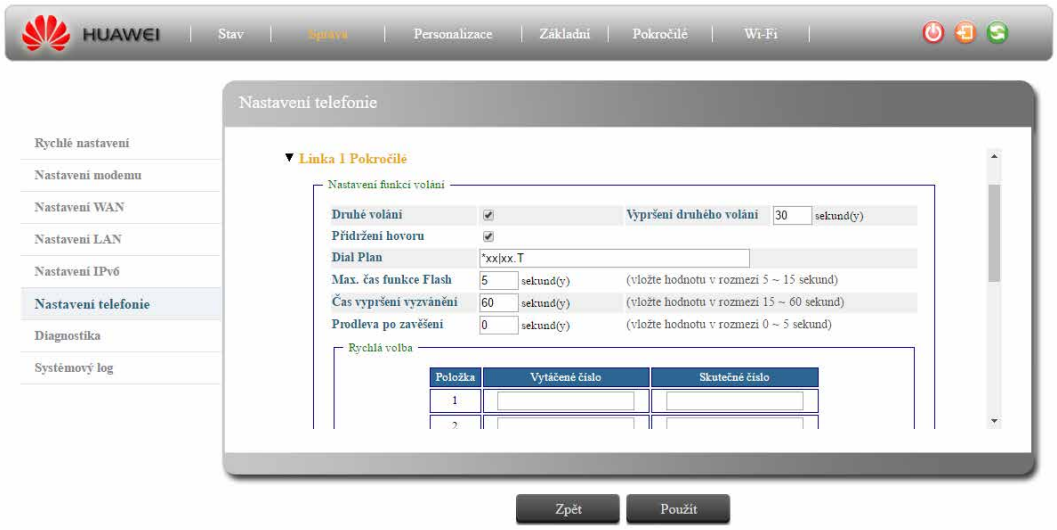
Obrázek 2-22 Nastavení telefonie – účet



Obrázek 2-23 Nastavení telefonie – parametry serveru

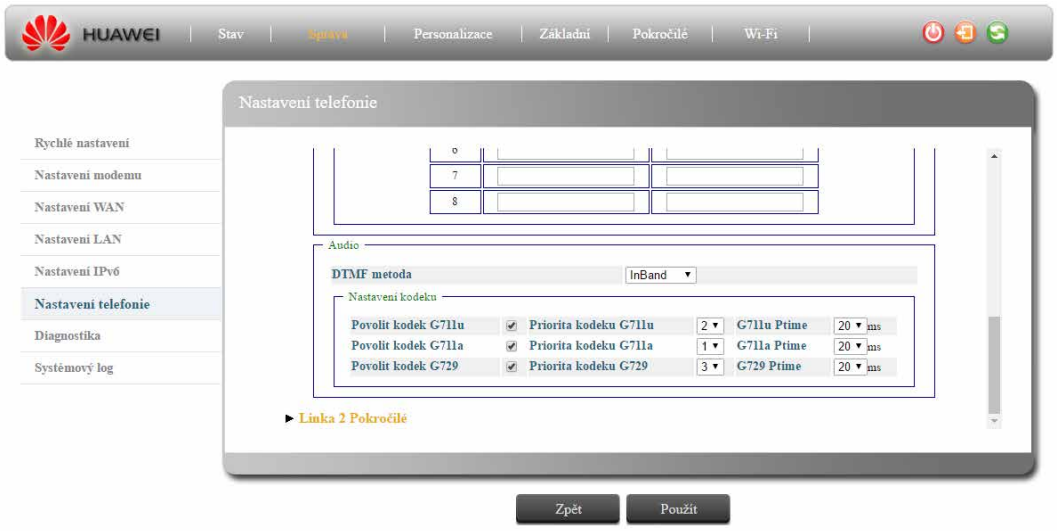


Obrázek 2-24 Nastavení telefonie – nastavení funkcí volání



Obrázek 2-25 Nastavení telefonie – rychlá volba

Obrázek 2-26 Nastavení telefonie – audio



Povolit VoIP

Zaškrtávací pole sloužící pro zapnutí nebo vypnutí VoIP telefonie.

Účet

- **Linka 1/Linka 2**
  - **Uživatelské jméno:**
    Uživatelské jméno SIP (protokol pro inicializaci relací). Jeho formát závisí na serveru SIP.
  - **Uživatelský účet**
    Uživatelský účet SIP. Jeho formát závisí na serveru SIP.
  - **Heslo**
    Heslo SIP uživatele.
  - **Potvrzení hesla**
    Zadejte opětovně heslo SIP uživatele pro ověření.
  - **Zobrazované jméno**
    Zadejte jméno, které bude zobrazeno příjemci odchozího hovoru jakožto identifikátor volajícího (pakliže tuto funkci server SIP podporuje).

Společná nastavení

- **Účet (server)**
  - **Doména uživatele**
    Doménové jméno tohoto LTE modemu.
  - **Adresa Registrar**
    IPv4 adresa serveru SIP.
  - **Adresa odchozího Proxy**
    Odchozí proxy serveru SIP se chová stejně jako běžný server proxy. Pomáhá obcházet omezení a blokace zavedené poskytovatelem připojení k internetu pomocí naslouchání neblokovaných portů a směrování požadavků mezi SIP klientem a poskytovatelem VoIP telefonie. V případě, že je vyplněna adresa Registrar i adresa odchozího Proxy, bude odchozímu serveru proxy odeslán požadavek REGISTER, který bude dále přesměrován příslušnému koncovému bodu SIP protokolu.
  - **Port Registrar**
    Číslo portu serveru SIP.
  - **Port odchozího Proxy**
    Číslo portu, na kterém bude odchozí server Proxy naslouchat.
  - **Rozsah RTP Port – od**
    Pokud tento údaj máte k dispozici, zadejte spodní mez rozsahu možných portů pro provoz RTP. V opačném případě v poli ponechte výchozí hodnotu.

- **Rozsah RTP Port – do**
  Pokud tento údaj máte k dispozici, zadejte horní mez rozsahu možných portů pro provoz RTP. V opačném případě v poli ponechte výchozí hodnotu. Pokud vám byl přidělen pouze jeden port pro provoz RTP, zadejte do polí „od“ a „do“ stejnou hodnotu.

➢ **Vyzváněcí tón**

Pomocí této záložky je možné nastavit vyzváněcí tón.

- **Frekvenční kvóta:**
  Zadejte frekvenci vyzváněcího tónu v rozsahu 300–800 Hz. Zařízení podporuje nastavení 1 či 2 frekvencí.
- **Vyzváněcí tón zapnut:**
  Zadejte dobu, po kterou bude tón vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí nepřetržité vyzvánění.
- **Vyzváněcí tón vypnut:**
  Zadejte dobu, po kterou tón nebude vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí, že vyzváněcí tón bude vždy vypnutý.

➢ **Tón druhého volání**

Pomocí této záložky je možné nastavit vyzváněcí tón druhého volání.

- **Frekvenční kvóta:**
  Zadejte frekvenci vyzváněcího tónu v rozsahu 300–800 Hz. Zařízení podporuje nastavení 1 či 2 frekvencí.
- **Tón druhého volání zapnut:**
  Zadejte dobu, po kterou bude tón vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí nepřetržité vyzvánění.
- **Tón druhého volání vypnut:**
  Zadejte dobu, po kterou tón nebude vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí, že vyzváněcí tón bude vždy vypnutý.

➢ **Tón vytáčení**

Pomocí této záložky je možné nastavit tón vytáčení.

- **Frekvenční kvóta:**
  Zadejte frekvenci tónu vytáčení v rozsahu 300–800 Hz. Zařízení podporuje nastavení 1 či 2 frekvencí.
- **Tón vytáčení zapnut:**
  Zadejte dobu, po kterou bude tón vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí nepřetržité vyzvánění.
- **Tón vytáčení vypnut:**
  Zadejte dobu, po kterou tón nebude vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí, že vyzváněcí tón bude vždy vypnutý.

- **Obsazovací tón**

  Pomocí této záložky je možné nastavit obsazovací tón.

  - **Frekvenční kvóta:**
    Zadejte frekvenci obsazovacího tónu v rozsahu 300–800 Hz. Zařízení podporuje nastavení 1 či 2 frekvencí.
  - **Obsazovací tón zapnut:**
    Zadejte dobu, po kterou bude tón vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí nepřetržité vyzvánění.
  - **Obsazovací tón vypnut:**
    Zadejte dobu, po kterou tón nebude vyzvánět. Přípustné nastavení je v rozmezí 0–4 sekundy nebo hvězdička (*), která značí, že vyzváněcí tón bude vždy vypnutý.

- **Audio**

  - **Nastavení faxu:**
    Zvolte kodek, který chcete použít pro fax (T.38/G.711a Passthrough/G.711u Passthrough).

Linka 1/Linka 2 pokročilé

- **Nastavení funkcí volání**
  - **Druhé volání**
    Zapíná nebo vypíná funkci druhého volání, která umožňuje podržet druhého volajícího na lince v případě, že již dřívější telefonní hovor probíhá. K přepínání mezi hovory slouží tlačítko FLASH.
  - **Vypršení druhého volání**
    Zadejte čas v sekundách, po jehož uplynutí bude druhý hovor zavěšen.
  - **Přidržení hovoru**
    Zapíná nebo vypíná funkci přidržení hovoru. Tato funkce umožňuje přidržet probíhající hovor stisknutím tlačítka FLASH.
  - **Dial Plan**
    Funkce Dial Plan (pravidlo vytáčení) představuje sadu pravidel pro ověření správnosti zadání telefonního čísla a jeho vytáčení.

    Zařízení podporuje dva formáty pravidel vytáčení:

    xx: symbol „“ představuje hvězdičku na klávesnici telefonu, „x“ libovolnou číslici.

    (0–9). Tento plán vytáčení je určen pro dvoumístné číslice začínající *. Symbol „|“ zastupuje logický operátor „nebo“ a umožňuje oddělování jednotlivých pravidel vytáčení.

    xx.T: Symbol „x“ představuje libovolnou číslici (0–9), „.“ libovolné množství číslice a „T“ vyjadřuje konec číslovky. Pro ukončení vytáčení není zapotřebí žádný zvláštní postup, jednoduše vyčkejte po dobu vypršení vytáčení (3 sekundy). Pokud chcete čekání na konec doby vypršení přeskočit, nastavte následující pravidlo vytáčení: xx.#. Po zadání tohoto pravidla budete moci např. telefonní číslo 1111 okamžitě vytočit zadáním 1111#.
  - **Max. čas funkce Flash**
    Zadejte maximální čas podržení tlačítka FLASH. Pokud toto tlačítko budete držet déle než určuje zadaný čas, bude stisknutí tlačítka ignorováno a nebude provedena žádná akce (čas zadejte v rozpětí 5–15 vteřin).
  - **Čas vypršení vyzvánění**
    Zadejte maximální čas vyzvánění (čas zadejte v rozpětí 15–60 vteřin).

- **Prodleva po zavěšení**
  Zadejte prodlevu po zavěšení. Prodleva vyjadřuje časový interval od položení sluchátka, po kterém bude hovor skutečně zavěšen (čas zadejte v rozpětí 0–5 vteřin).
- **Rychlá volba**
  Pomocí funkce rychlé volby lze urychlit vytáčení vybraných telefonních čísel pomocí zkratky.
  - ♦ Vytáčené číslo: Zadejte vytáčené číslo, tedy zkratku, kterou chcete pro vytočení příslušného čísla používat. Povoleny jsou pouze číslice 0–9.
  - ♦ Skutečné číslo: Zadejte skutečné číslo, které chcete po zadání klávesové zkratky vytočit. Povoleny jsou pouze číslice 0–9 a znaky # a *.

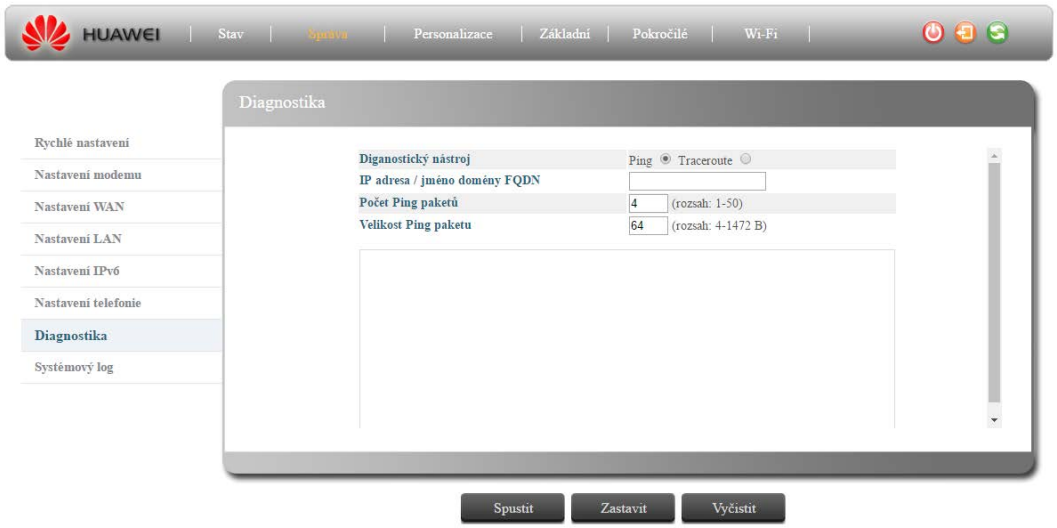
➢ **Audio**

- **DTMF metoda**
  Tato rozbalovací nabídka slouží k výběru DTMF metody. K dispozici je InBand, RFC2833 a SIPInfo.
- **Nastavení kodeku**
  Povolení kodeku: Zařízení podporuje tři audio kodeky: G711u, G711a a G729. Zaškrtnutím políčka u příslušného kodeku jeho použití povolíte/zakážete.
  - ♦ Priorita kodeku: Tyto rozbalovací nabídky slouží k určení priority použití jednotlivých kodeků.
  - ♦ Ptime: Tato položka určuje délku trvání záznamu v jednom paketu v milisekundách. Hodnota ptime určuje délku hlasového bloku v jednotlivých RTP paketech. V případě kodeků G711u/G711a jsou k dispozici čtyři možnosti: 5, 10, 20 a 30 ms; u kodeku G729 jsou k dispozici tři možnosti: 10, 20 a 30 ms.

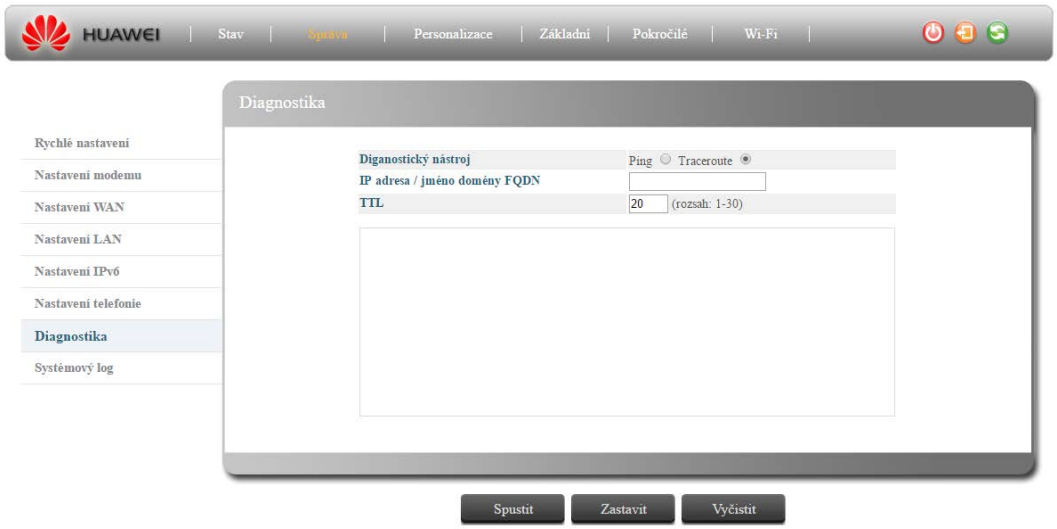
2.1.6 Správa > Diagnostika

Stránka „Diagnostika“ nabízí nástroje pro řešení potíží se síťovým připojením, jako jsou příkazy ping či traceroute.

Obrázek 2-27 Diagnostika – příkaz ping



Obrázek 2-28 Diagnostika – příkaz traceroute



Diagnostický nástroj

- **Příkaz ping**
  - **IP adresa/jméno domény FQDN:**
    Pro provedení diagnostického testu zadejte cílovou IP adresu nebo doménové jméno.
  - **Počet Ping paketů:**
    Zadejte počet testovacích paketů, které si přejete odeslat (rozsah: 1–50).
  - **Velikost Ping paketu:**
    Zadejte požadovanou velikost jednoho testovacího paketu v rozsahu 4–1472 bajtů.

Příklad	Pokud připojení k internetu nebude úspěšné, pokuste se identifikovat zdroj problému pomocí příkazu ping. Postup je následující: 1. Přejděte do menu **Správa** > **Diagnostika**. Jako diagnostický nástroj zvolte „Ping“. Na stránce se zobrazí parametry příkazu ping. 2. Zadejte cílovou IP adresu nebo doménové jméno do pole **IP adresa/jméno domény FQDN**, například www.google.com 3. Nastavte požadovaný **počet Ping paketů** a **velikost Ping paketu**. 4. Klikněte na tlačítko **Spustit**. 5. Vyčkejte, dokud nebude provedení příkazu ping dokončeno. 6. Výsledek se zobrazí v textovém poli na stránce.

Diagnostický nástroj

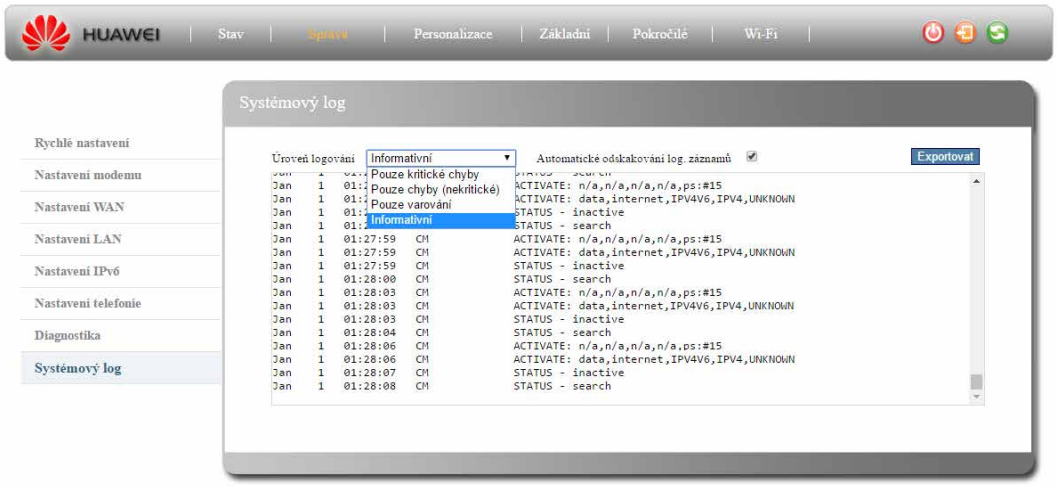
- **Příkaz traceroute**
  - **IP adresa/jméno domény FQDN:**
    Pro provedení diagnostického testu zadejte cílovou IP adresu nebo doménové jméno.
  - **TTL:**
    Hodnota „time to live“, tedy číslo, které určuje dobu platnosti datového paketu. Zadejte požadovanou hodnotu a následně zkontrolujte, jaký byl skutečný čas průchodu jednotlivými uzly k zadanému cíli (rozsah: 1–30).

Příklad	Pokud připojení k internetu nebude úspěšné, pokuste se identifikovat zdroj problému pomocí příkazu traceroute. Postup je následující: 1. Přejděte do menu **Správa** > **Diagnostika**. Jako diagnostický nástroj zvolte „Traceroute“. Na stránce se zobrazí parametry příkazu traceroute. 2. Zadejte cílovou IP adresu nebo doménové jméno do pole **IP adresa/jméno domény FQDN**, například www.google.com 3. Zadejte hodnotu **TTL**. 4. Klikněte na tlačítko **Spustit**. 5. Vyčkejte, dokud nebude provedení příkazu traceroute dokončeno. 6. Výsledek se zobrazí v textovém poli na stránce.

2.1.7 Správa > Systémový log

Systémový log slouží pro podrobnou diagnostiku technické funkcionality modemu v případě potíží. Součástí záznamů v systémovém logu v žádném případě nejsou žádné osobní nebo citlivé údaje.

Obrázek 2-29 Systémový log



Úroveň logování

K dispozici jsou čtyři přednastavené úrovně logování: Pouze kritické chyby, pouze chyby (nekritické), pouze varování a informativní, viz přehled jednotlivých záznamů v tabulce níže.

- **Automatické odskakování log. záznamů:**
  Pokud bude toto zaškrtávací pole zaškrtnuto, systémový log po každém otevření odskočí na poslední řádek, tedy na poslední záznam v logu. Pokud si přejete začínat u prvního záznamu, toto pole odškrtněte.
- **Exportovat:**
  Systémový log je možné v rámci podrobné analýzy nebo sledování chyb exportovat. Log se exportuje do souboru TXT komprimovaném v archivu TAR.

- **Systémový log**

Informativní záznamy	➢ **Systém** - Zapnutí/restartování/vypnutí ➢ **Správa připojení** - Připojení WAN - Získání WAN IP adresy ➢ **VoIP** - Zapnutí/vypnutí - Registrace k serveru SIP - Příchozí/odchozí hovor - Zahájení telefonické relace ➢ **Wi-Fi** - Zapnutí/vypnutí přístupového bodu - Klient: přiřazen/vyřazen ➢ **FOTA** - Zahájení/ukončení - Pravidelná kontrola firmwaru/výsledek aktualizace - Zahájení stahování firmwaru - Zahájení aktualizace firmwaru ➢ **TR069**

Varování	➢ **Správa připojení** - SIM karta není vložena - Ověření PIN se nezdařilo ➢ **VoIP** - Registrace SIP se nezdařila - Telefonní hovor nelze zahájit - Požadavek REGISTER se nepodařilo odeslat ➢ **Wi-Fi** - Klient: bez autorizace ➢ **FOTA** - Připojení k serveru se nezdařilo - Stažení balíčku nebo firmwaru se nezdařilo ➢ **TR069**
Nekritické chyby	➢ **FOTA** - Aktualizace firmwaru se nezdařila - Ověření firmwaru se nezdařilo ➢ **TR069**
Kritické chyby	

➢ **Provozní log**

Informativní záznamy	- Přihlášení/odhlášení uživatele - Odhlášení uživatele z důvodu vypršení relace - Změna hesla pro přihlášení do administrace - Změna IP adresy DHCP serveru - Změna stupně zabezpečení branou firewall - Blokování/odblokování DHCP klienta - Aktualizace firmwaru prostřednictvím webového rozhraní - Změna SSID sítě Wi-Fi - Změna zabezpečení sítě Wi-Fi - Uložení změn na libovolné stránce administrace - Spuštění/ukončení WPS - Spuštění/ukončení příkazu ping - Spuštění/ukončení příkazu traceroute - Export/import konfiguračního souboru

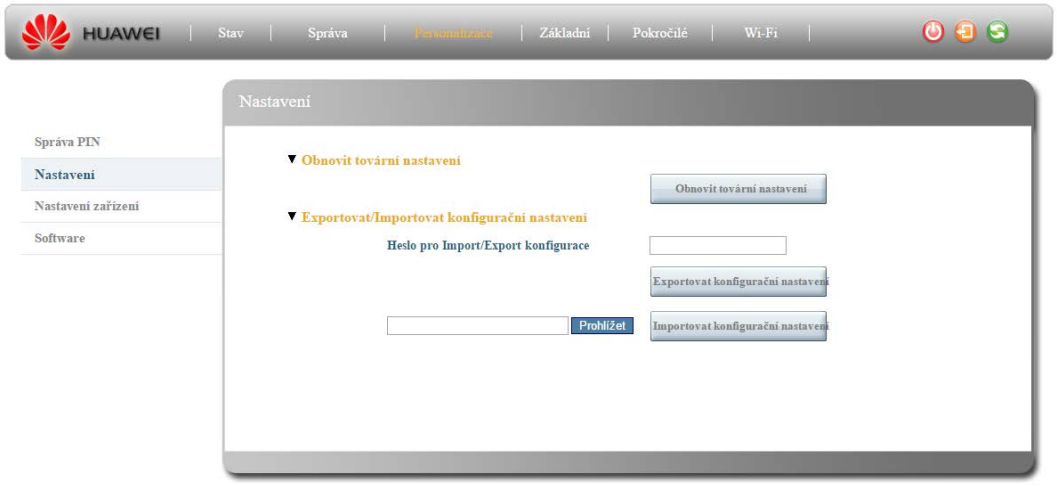
Varování	- Přihlášení do webového rozhraní se nezdařilo - Odmítnutí výzvy k aktualizaci firmwaru uživatelem - Nezdařená aktualizace firmwaru
Nekritické chyby	
Kritické chyby	

	Systémový log NELZE vyexportovat v prohlížeči Internet Explorer 8.

2.2 Personalizace

2.2.1 Personalizace > Nastavení

Obrázek 2-30 Nastavení



Obnovit tovární nastavení
Funkci obnovy továrního nastavení lze použít pro navrácení všech položek nastavení na výchozí hodnoty. Veškeré provedené změny a nastavené parametry budou ztraceny. Pokud chcete některé z nich zachovat, bude zapotřebí si současné nastavení zapamatovat a opětovně provést příslušné změny po obnovení továrního nastavení.

➢ **Obnovit tovární nastavení**
Pro obnovení továrního nastavení jednoduše klikněte na tlačítko „Obnovit tovární nastavení“. Po dokončení procesu obnovy se zařízení restartuje.

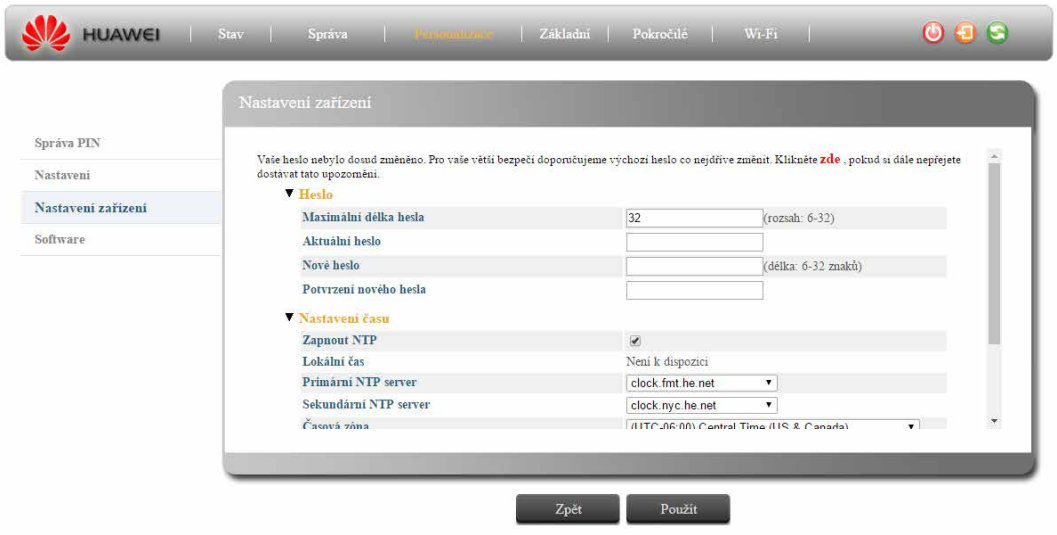
Exportovat/importovat konfigurační nastavení

- **Heslo pro Import/Export konfigurace**
  Před exportováním nebo importováním konfiguračního souboru je zapotřebí zadat heslo do tohoto pole (heslo musí obsahovat alespoň 2 velká písmena, malé písmeno, číslici, mezeru a speciální znak (`~!@#$%^&*()-_=+\|[{}];:‘“,<.>/?). Povolená délka je 6–128 znaků. Heslo pro import/export nesmí být stejné jako heslo pro přihlášení do administrace.
- **Exportovat konfigurační nastavení**
  Veškerá uživatelská nastavení budou exportována do souboru.
- **Importovat konfigurační nastavení**
  Pomocí této funkce lze importovat předem uložené konfigurační nastavení ze zadaného souboru.

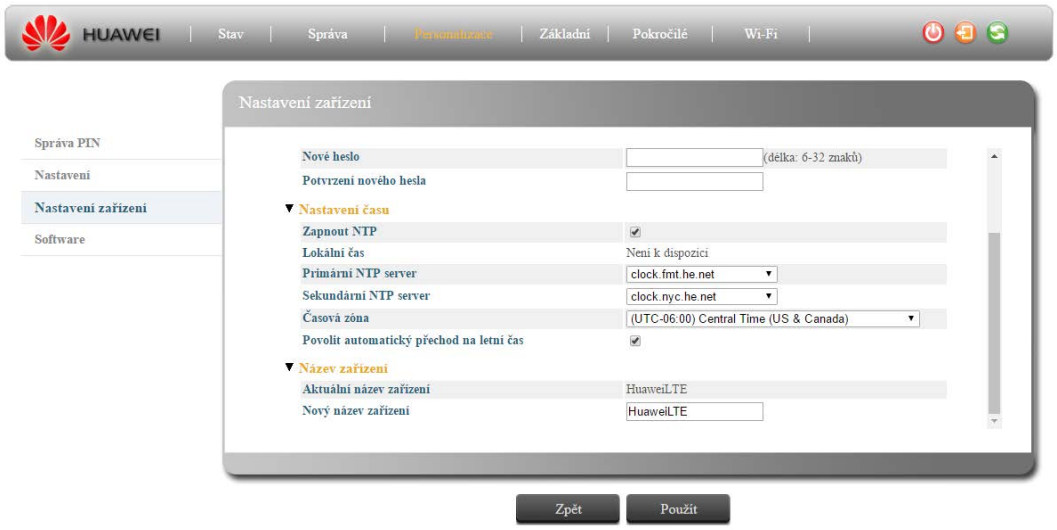
	1. Konfigurační nastavení NELZE vyexportovat v prohlížeči Internet Explorer 8. 2. Soubor s konfiguračním nastavením pro import musí mít název „conf.tar“.

2.2.2 Personalizace > Nastavení zařízení

Obrázek 2-31 Nastavení zařízení – heslo



Obrázek 2-32 Nastavení zařízení – čas a název zařízení



Heslo

Tato záložka slouží pro změnu přístupového hesla do administračního rozhraní.

- **Maximální délka hesla:**
  Zadejte maximální délku hesla v rozpětí 6–128 znaků.
- **Aktuální heslo:**
  Zadejte heslo, které v současné době používáte.
- **Nové heslo:**
  Zadejte nové heslo. Mějte na paměti, že délka nového hesla musí splňovat limit zadaný v poli „**Maximální délka hesla**“.
- **Potvrzení nového hesla:**
  Zadejte nové heslo ještě jednou pro ověření.

	Pokud do výše uvedených polí nezadáte nic, znamená to, že heslo zůstane nezměněno.

Nastavení času

Tento modem používá pro synchronizaci času protokol SNTP (Simple Network Time Protocol), jehož prostřednictvím provádí pravidelnou aktualizaci času. Udržování přesného údaje o aktuálním čase umožňuje vytváření smysluplných a vypovídajících systémových logů.

V záložce „Nastavení času“ se nachází následující položky:

- **Zapnout NTP**
  Zaškrtávací pole sloužící k zapnutí/vypnutí synchronizace s NTP serverem.
- **Lokální čas**
  Zobrazuje aktuální systémový čas.
- **Primární NTP server**
  Výběr primárního NTP serveru ze seznamu dostupných serverů.
- **Sekundární NTP server**
  Výběr sekundárního NTP serveru, ke kterému se modem připojí v případě selhání primárního serveru.
- **Časová zóna**
  SNTP server používá greenwichský střední čas (GMT, známý rovněž jako koordinovaný světový čas – UTC) založený na počítání časových zón od nultého poledníku. Aby systémový čas odpovídal místnímu času, vyberte z rozbalovacího seznamu časovou zónu, ve které se nacházíte. Výchozím nastavením je UTC - 06.00, tedy centrální čas (Spojené státy a Kanada).
- **Povolit automatický přechod na letní čas**
  Zaškrtněte toto pole v případě, že se nacházíte ve státě, který dodržuje přechod na letní čas.

Název zařízení

Tato záložka umožňuje nastavit název zařízení pro jeho jednoznačnou identifikaci v síti. Výchozí název zařízení můžete nahradit jiným, snadno zapamatovatelným názvem, jehož prostřednictvím můžete snadno přistupovat k administračnímu rozhraní. Název zařízení můžete zadat do adresního řádku prohlížeče jako webovou adresu s tečkou na konci a otevřít tím webové administrační rozhraní (např. http://huaweilte.).

V záložce „Název zařízení“ se nachází následující položky:

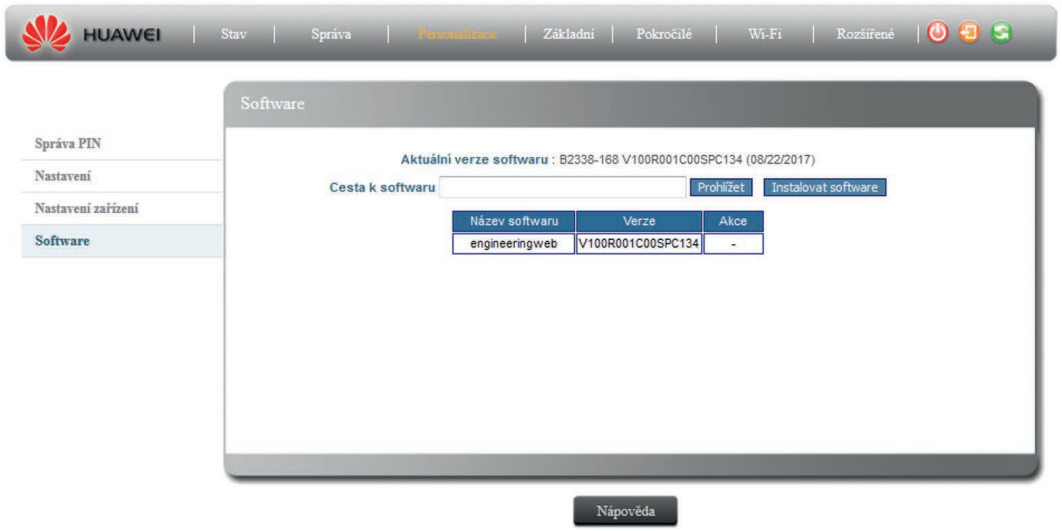
- **Aktuální název zařízení**
  Zobrazuje aktuální název zařízení.
- **Nový název zařízení**
  Pole pro zadání nového názvu zařízení (max. délka je 20 tisknutelných znaků ASCII). Nový název uložíte kliknutím na tlačítko „Použít“.

	Klient nemůže přistoupit k zařízení příkazem ping v případě, že je výchozím nastavením klienta IPv6 DNS.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.2.3 Personalizace > Software

Obrázek 2-33 Software – upgrade ze souboru



- **Upgrade ze souboru:**

  Krok 1: Klikněte na tlačítko „Prohlížet“ a zvolte aktualizační soubor IPK.

  Krok 2: Aktualizaci softwaru prostřednictvím zvoleného souboru spusťte kliknutím na tlačítko „Instalovat software“.

	Během aktualizace softwaru zařízení nevypínejte. V opačném případě hrozí poškození modemu.

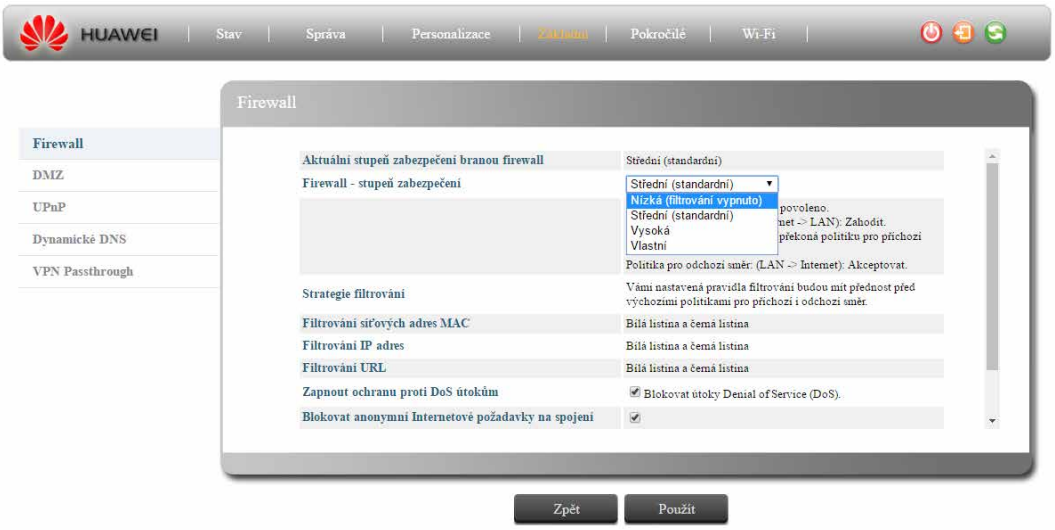
2.3 Základní

2.3.1 Základní > Firewall

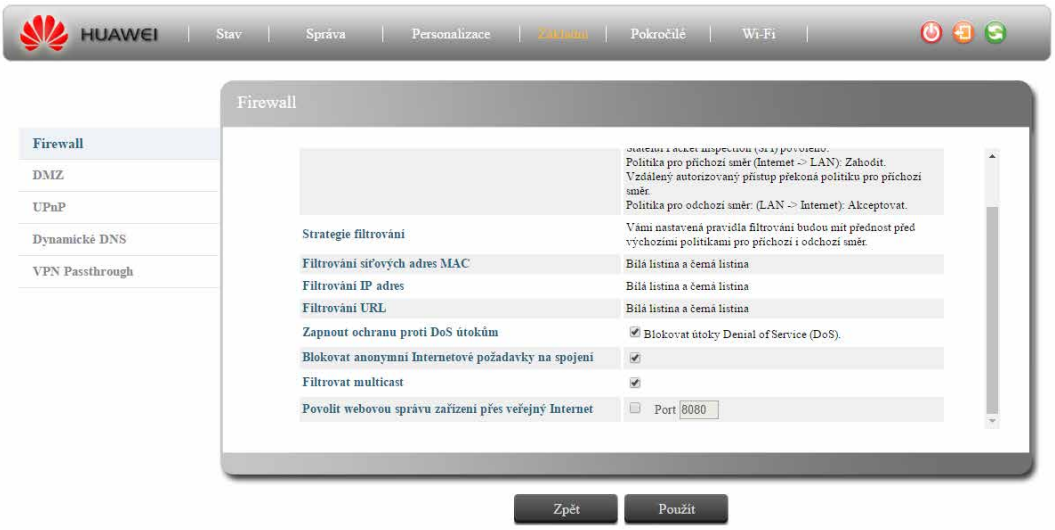
Tento modem poskytuje pokročilou ochranu prostřednictvím brány firewall, která zabraňuje neoprávněné síťové komunikaci a značně tak snižuje pravděpodobnost mnoha běžných hackerských útoků.

Tato stránka slouží ke konfiguraci a změně nastavení brány firewall. Brána firewall slouží k blokování neautorizovaného přístupu a propouštění pouze předem schváleného datového toku z internetu. Slouží také pro vzdálenou správu modemu prostřednictvím internetu autorizovaným uživatelem.

Obrázek 2-34 Firewall – 1



Obrázek 2-35 Firewall – 2



Aktuální stupeň zabezpečení branou firewall

Zobrazuje aktuální stupeň zabezpečení branou firewall.

Firewall – stupeň zabezpečení

Umožňuje změnit nastavení stupně zabezpečení branou firewall. K dispozici jsou čtyři přednastavené úrovně:

- Nízká (filtrování vypnuto)
- Střední (standardní)
- Vysoká
- Vlastní (pokud zvolíte tuto možnost, budete moci dále nastavit filtrování síťových adres MAC, IP adres a URL)

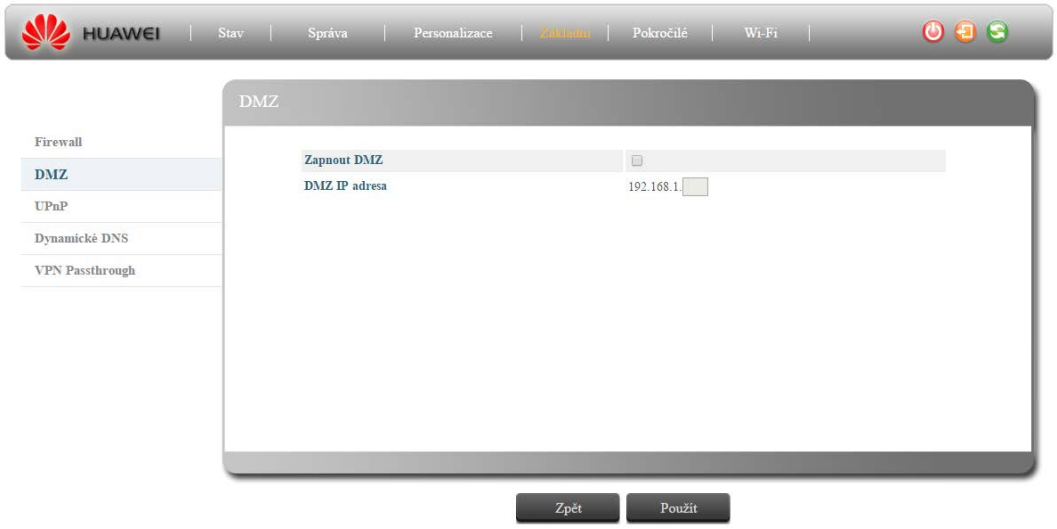
Strategie filtrování Vámi nastavení pravidla filtrování budou mít přednost před výchozími politikami pro příchozí i odchozí směr.
Filtrování síťových adres MAC Zablokuje nebo naopak autorizuje klienta podle zadané MAC adresy. Bílou a černou listinu adres upravíte prostřednictvím menu Pokročilé > Filtr síťových adres MAC.
Filtrování IP adres Zablokuje nebo naopak autorizuje klienta podle zadané IP adresy. Bílou a černou listinu adres upravíte prostřednictvím menu Pokročilé > Filtr IP adres.
Filtrování URL Zablokuje nebo naopak autorizuje přístup klienta dle zadané URL (webové) adresy. Bílou a černou listinu adres upravíte prostřednictvím menu Pokročilé > URL filtrování.
Zapnout ochranu proti DoS útokům Zaškrtnutím tohoto pole aktivujete ochranu proti útoku typu „denial of service“ (DoS).
Blokovat anonymní internetové požadavky na spojení Zaškrtnutím tohoto pole zabráníte příjmu anonymních internetových požadavků na spojení.
Filtrovat multicast Zaškrtnutím tohoto pole aktivujete filtrování multicast paketů.
Povolit webovou správu zařízení přes veřejný internet Zaškrtnutím tohoto pole povolíte vzdálený přístup k administračnímu rozhraní prostřednictvím internetu.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.3.2 Základní > DMZ

Pokud používáte aplikace, které vyžadují neomezený přístup k internetu, můžete prostřednictvím DMZ vytvořit logickou podsíť se zvláštním vztahem klient-server.

Obrázek 2-36 DMZ

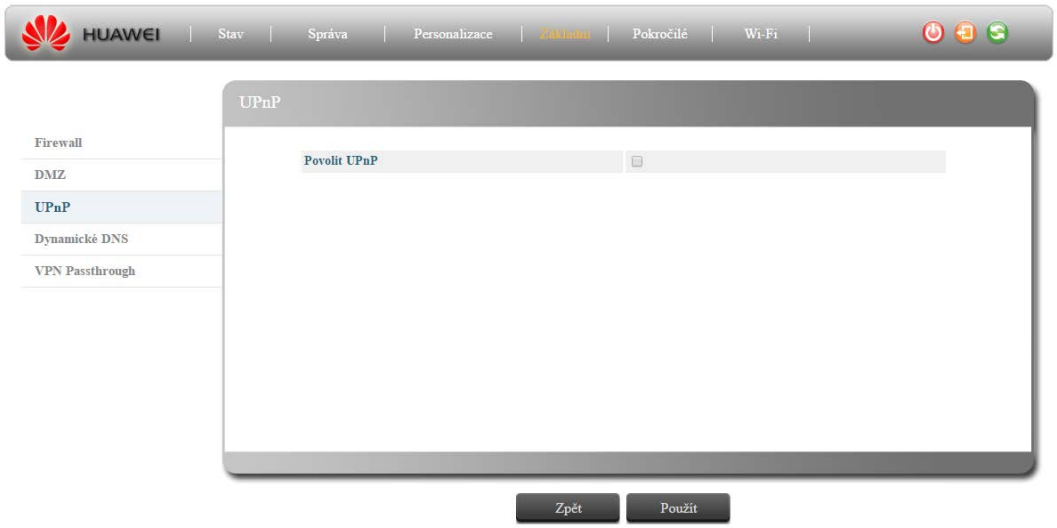


Zapnout DMZ Zaškrtnutím tohoto pole zapnete nebo vypnete DMZ.
DMZ IP adresa Zadejte požadovanou adresu logické podsítě, která bude sloužit jako „neutrální zóna“ (DMZ je zkratkou pro „demilitarizovanou zónu“) oddělená od ostatního síťového provozu. DMZ následně nasměruje síťový provoz jednotlivým zařízením na základě protokolu a čísla portu.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.3.3 Základní > UPnP

Obrázek 2-37 UPnP



UPnP

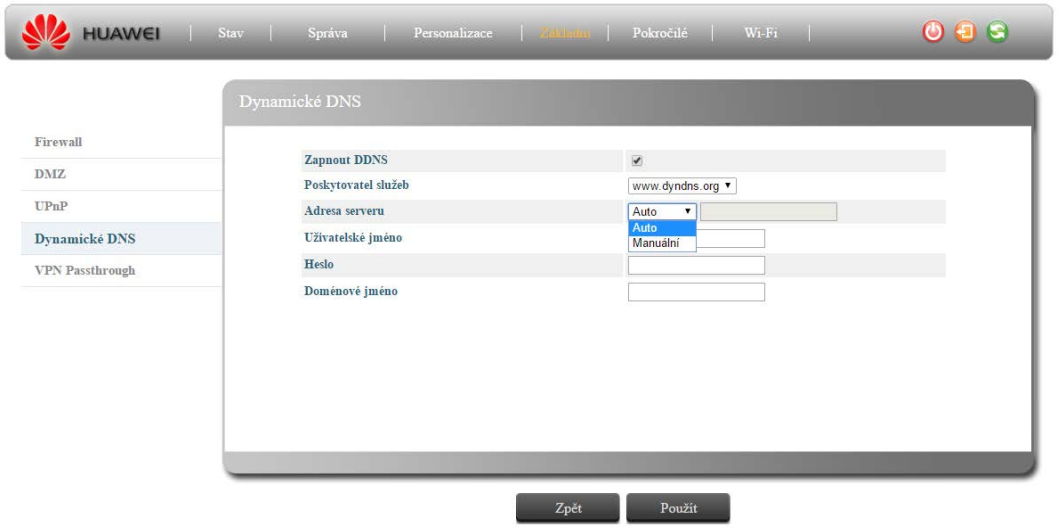
Povolit UPnP – zaškrtávací pole pro zapnutí/vypnutí sady protokolů Universal Plug and Play, která zjednodušuje připojení různých zařízení a instalaci domácí sítě. Pokud je UPnP povoleno, budou určité aplikace v systému Windows automaticky vytvářet pravidla pro směrování portů.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.3.4 Základní > Dynamické DNS

Dynamické DNS (DDNS) je označení systému, který umožňuje v reálném čase aktualizovat záznamy o internetové doméně uložené na DNS serveru. Tato stránka umožňuje zapnutí dynamického DNS a výběr poskytovatele služeb. Na stránce „Dynamické DNS“ se nachází následující nastavení:

Obrázek 2-38 Dynamické DNS

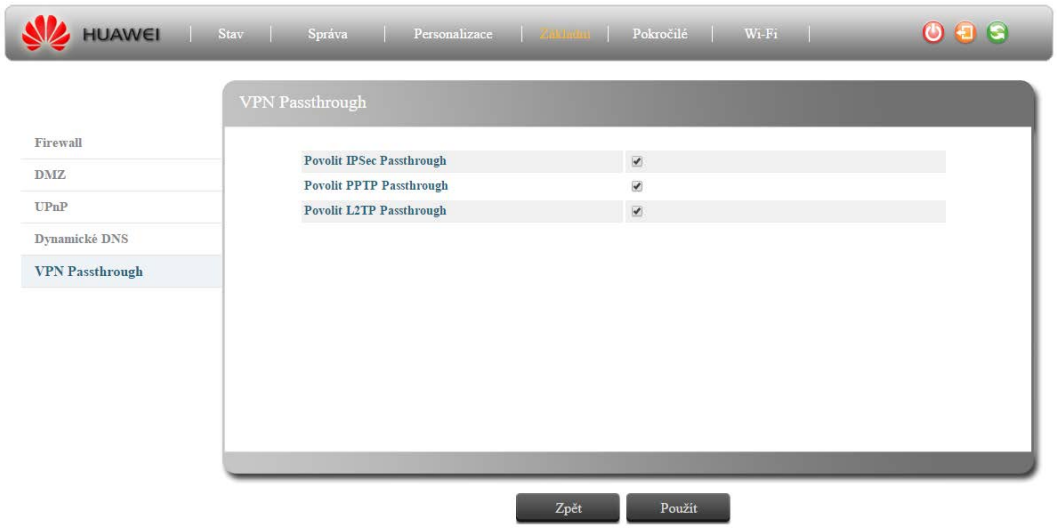


Zapnout DDNS Zaškrtněte toto pole v případě, že zařízení nemá statickou IP adresu. Doménové jméno tak zůstane přiřazeno k zařízení i v případě změny IP adresy. Po zapnutí DDNS je dále zapotřebí nastavit následující parametry: ● Uživatelské jméno ● Heslo ● Doménové jméno
Poskytovatel služeb Vyberte z rozbalovacího seznamu název poskytovatele služeb.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.3.5 Základní > VPN Passthrough

Obrázek 2-39 VPN Passthrough



Povolit IPSec Passthrough IPsec (IP security) je název bezpečnostního rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu odesílaného mezi dvěma zařízeními.
Povolit PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) je síťovým protokolem umožňujícím přenos TCP/IP paketů prostřednictvím sítě, která není na těchto protokolech založená, přiřazením adresy, kterou cizí síť rozpozná a paket správně nasměruje, i když neumí zpracovat jeho samotný obsah.
Povolit L2TP Passthrough L2TP je označením pro tunel v 2. vrstvě OSI modelu, otevřený standard s širokou kompatibilitou a podporou většiny výrobců.

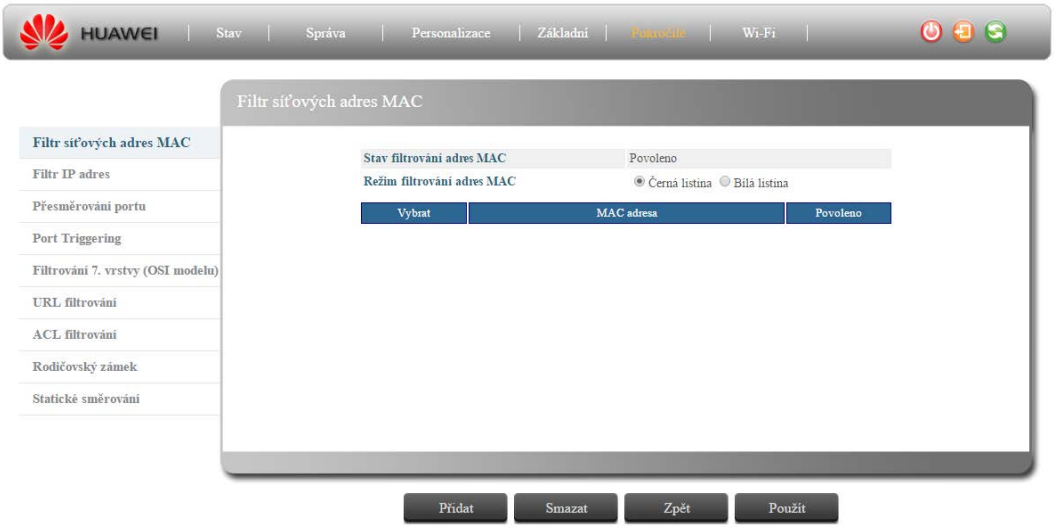
	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4 Pokročilé

2.4.1 Pokročilé > Filtr síťových adres MAC

Prostřednictvím této nabídky můžete zablokovat přístup k internetu klientům z místní sítě podle jejich MAC adresy. Na stránce se nachází seznam MAC adres, které budou bezpečnostním systémem zablokovány. Do seznamu lze přidávat adresy nebo je naopak odstraňovat či zapínat/vypínat filtrování v určitý čas. K dispozici jsou následující nastavení:

Obrázek 2-40 Filtr síťových adres MAC



Stav filtrování adres MAC

Zobrazuje aktuální stav funkce filtrování adres MAC.
Stav lze změnit prostřednictvím menu **Základní** > **Firewall** a změnou nastavení stupně zabezpečení brány firewall.

- **Nízká:** Filtrování vypnuto.
- **Střední:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování adres MAC.**
- **Vysoká:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování adres MAC**.
- **Vlastní:** Pokud je stupeň zabezpečení nastaven na „Vlastní“, můžete zvolit, zda chcete filtrování adres MAC vypnout či filtrovat podle černé nebo bílé listiny.

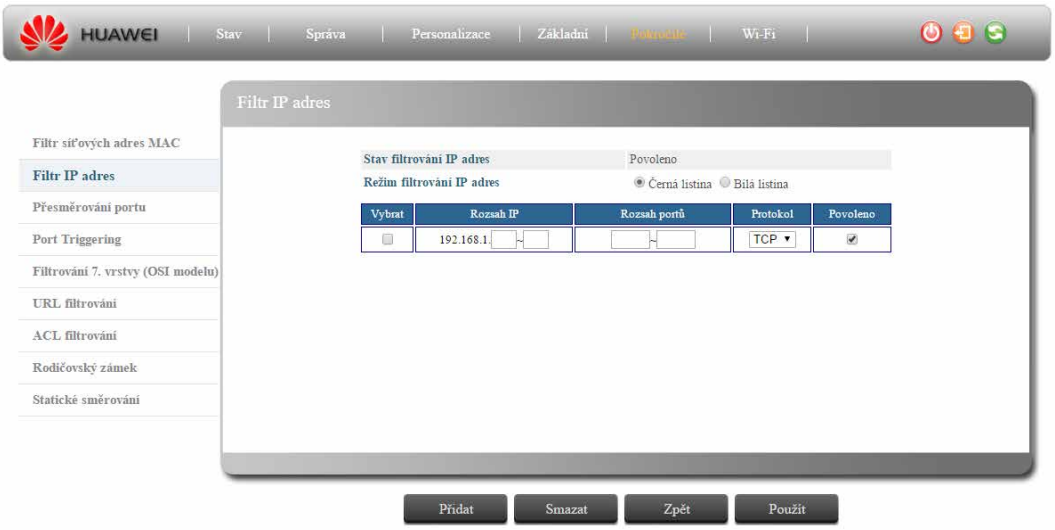
Režim filtrování adres MAC Zvolte, zda chcete adresy MAC filtrovat podle černé nebo bílé listiny. ● Černá listina: Zablokuje přístup k internetu zařízením uvedeným na černé listině. ● Bílá listina: Povolí přístup k internetu POUZE zařízením uvedeným na bílé listině.
Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
MAC adresa: Pole pro zadání MAC adresy přístroje, který chcete přidat do seznamu filtrování.
Povoleno Zaškrtnutím tohoto pole zapnete filtrování MAC adresy příslušného zařízení.

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.2 Pokročilé > Filtr IP adres

Prostřednictvím této nabídky můžete zablokovat přístup k internetu klientům z místní sítě podle jejich IP adresy a čísla TCP/UDP portu. Tento modem umožňuje nastavení až pěti filtrů IP adres. Na stránce se nachází seznam IP adres, které budou bezpečnostním systémem zablokovány. Adresy lze přidávat nebo mazat. Filtrování lze také zapnout/vypnout na určitou dobu. K dispozici jsou následující nastavení:

Obrázek 2-41 Filtr IP adres



Stav filtrování IP adres

Zobrazuje aktuální stav funkce filtrování IP adres.
Stav lze změnit prostřednictvím menu **Základní** > **Firewall** a změnou nastavení stupně zabezpečení brány firewall.

- **Nízká:** Filtrování vypnuto.
- **Střední:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování IP adres.**
- **Vysoká:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování IP adres**.
- **Vlastní:** Pokud je stupeň zabezpečení nastaven na „Vlastní“, můžete zvolit, zda chcete filtrování IP adres vypnout či filtrovat podle černé nebo bílé listiny.

Režim filtrování IP adres

Zvolte, zda chcete IP adresy filtrovat podle černé nebo bílé listiny.

- Černá listina: Zablokuje přístup k internetu zařízením uvedeným na černé listině.
- Bílá listina: Povolí přístup k internetu POUZE zařízením uvedeným na bílé listině.

Vybrat

Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.

Rozsah IP

Zadejte IP adresu zařízení nebo rozsah.

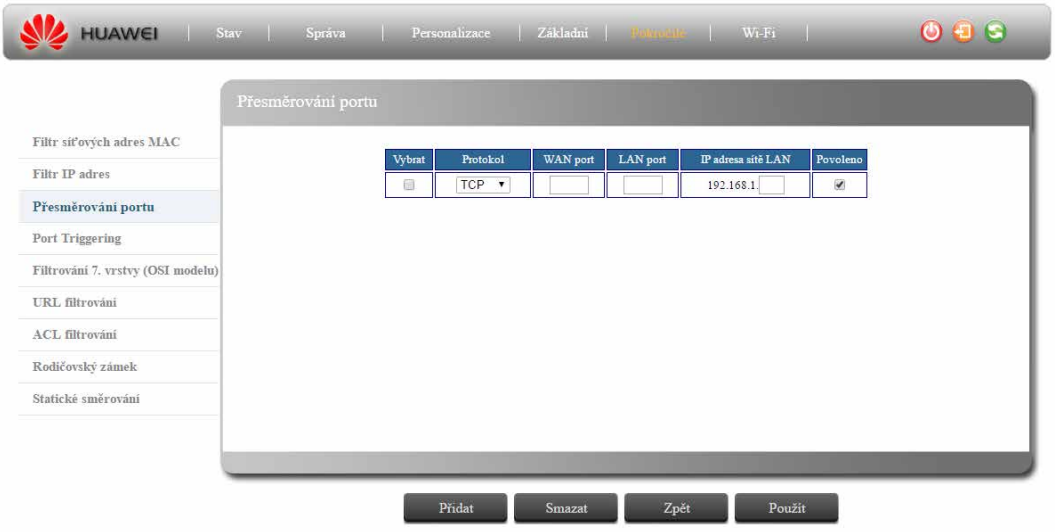
Rozsah portů Zadejte rozsah portů, které chcete filtrovat.
Protokol Zvolte protokol, který chcete filtrovat: TCP nebo UDP.
Povoleno Zaškrtnutím tohoto pole zapnete filtrování příslušné IP adresy nebo jejich rozsahu.

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.3 Pokročilé > Přesměrování portu

Přesměrování portu stanovuje zařízení v místní síti, kterému má modem poslat datové pakety. Router na základě pravidel přesměrování portu odesílá data z externí IP adresy/čísla portu na IP adresu/číslo portu v místní síti. Pravidla přesměrování portu jsou založena na jednotlivých portech. Stránka „Přesměrování portu“ slouží ke správě těchto pravidel. K dispozici jsou následující nastavení:

Obrázek 2-42 Přesměrování portu



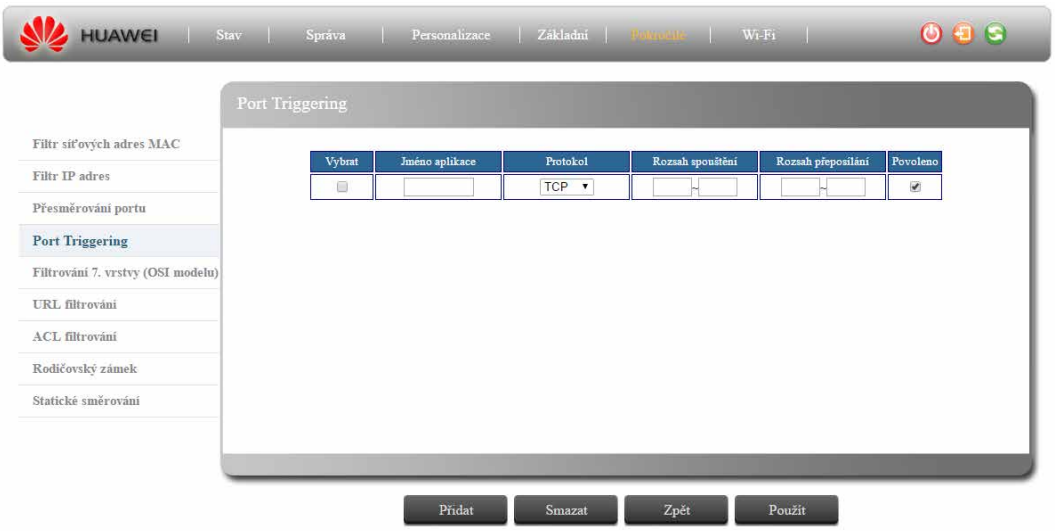
Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
Protokol Zvolte protokol pro přesměrování portu: TCP, UDP nebo BOTH (oba).
WAN port Zadejte číslo portu WAN rozhraní.
LAN port Zadejte číslo portu LAN rozhraní.
IP adresa sítě LAN Zadejte IP adresu identifikující podsíť vzdálené sítě.
Povoleno Zaškrtnutím tohoto pole zapnete přesměrování portu pro příslušnou IP adresu.

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.4 Pokročilé > Port Triggering

Port Triggering je technologie umožňující automatizaci přesměrování portu, při které odchozí spojení na předem určeném portu („triggering port“) způsobí, pokud jsou odchozí porty stále používány, že příchozí provoz na specifické příchozí porty je dynamicky přesměrován na hostitele, který započal komunikaci. To umožňuje počítačům ukrytým za NAT poskytovat služby, které obvykle vyžadují veřejnou adresu počítače. Port Triggering otevře příchozí port v případě, že zařízení v místní síti použije předem určený odchozí port nebo port z předem určeného rozsahu. Na této stránce lze nastavit až 15 pravidel pro Port Triggering. K dispozici jsou následující nastavení:

Obrázek 2-43 Port Triggering



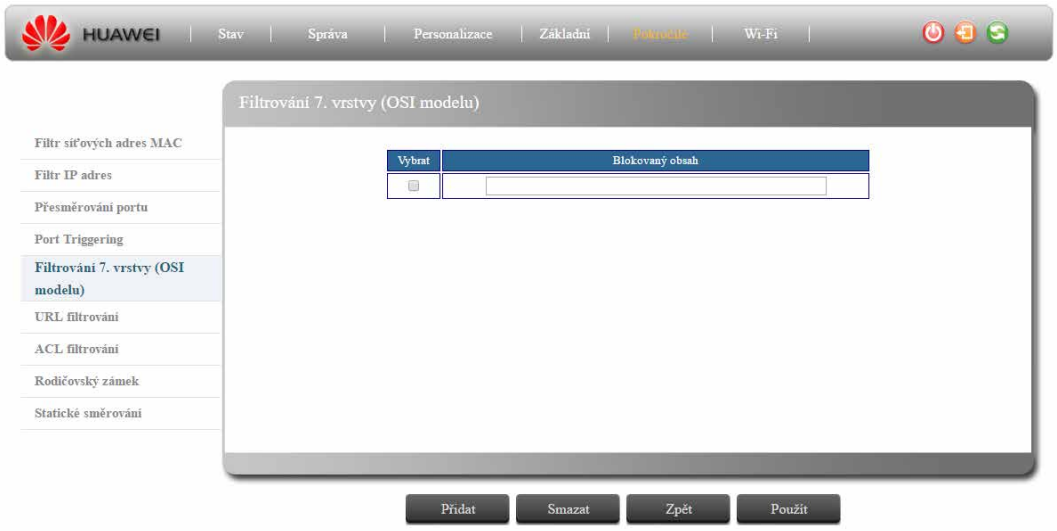
Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
Jméno aplikace Zadejte název aplikace.
Protokol Zvolte protokol pro Port Triggering: TCP, UDP nebo BOTH (oba).
Rozsah spouštění Zadejte rozsah spouštění (1–65535).

Rozsah přeposílání Zadejte rozsah přeposílání (1–65535).
Povoleno Zaškrtnutím tohoto pole zapnete Port Triggering pro příslušnou aplikaci.

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.5 Pokročilé > Filtrování 7. vrstvy (OSI modelu)

Obrázek 2-44 Filtrování 7. vrstvy (OSI modelu)

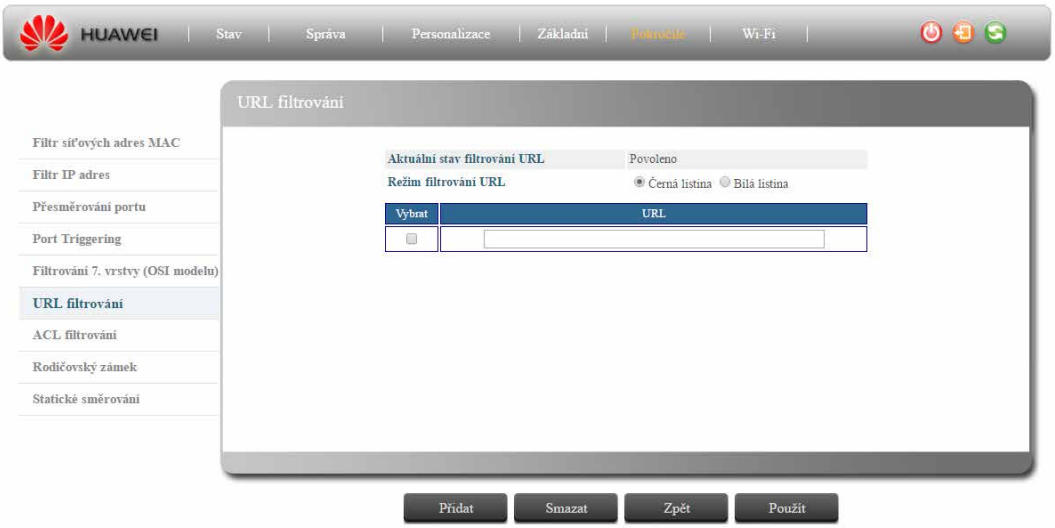


Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
Blokovaný obsah Zadejte klíčová slova, která chcete na sedmé vrstvě (OSI modelu) filtrovat. Filtr rozlišuje malá/velká písmena.

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.6 Pokročilé > URL filtrování

Obrázek 2-45 URL filtrování



Aktuální stav filtrování URL

Zobrazuje aktuální stav funkce filtrování URL.
Stav lze změnit prostřednictvím menu **Základní** > **Firewall** a změnou nastavení stupně zabezpečení brány firewall.

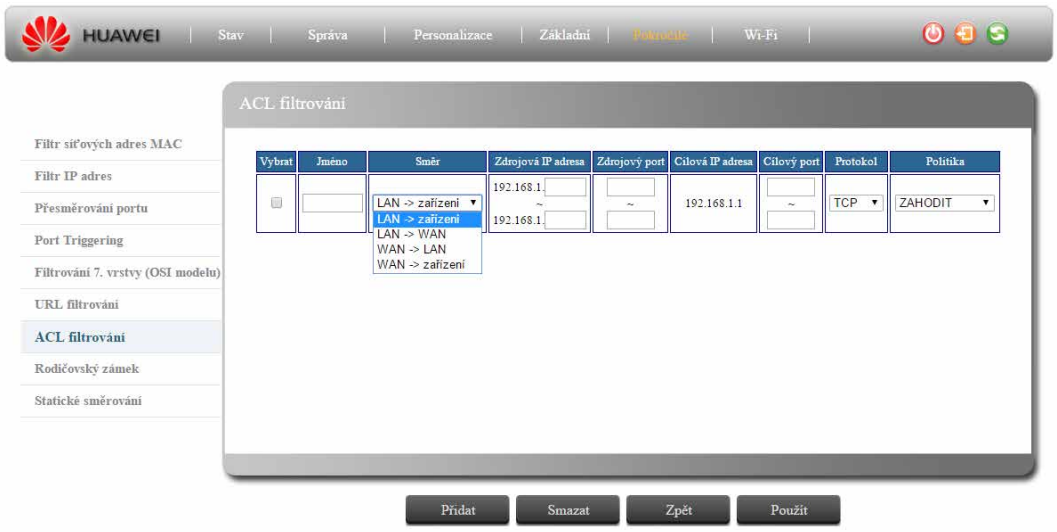
- **Nízká:** Filtrování vypnuto.
- **Střední:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování URL.**
- **Vysoká:** Filtrování je zapnuto. Můžete zvolit, zda chcete filtrovat podle černé nebo bílé listiny prostřednictvím nastavení **Režim filtrování URL**.
- **Vlastní:** Pokud je stupeň zabezpečení nastaven na „Vlastní“, můžete zvolit, zda chcete filtrování URL vypnout či filtrovat podle černé nebo bílé listiny.

Režim filtrování URL Zvolte, zda chcete adresy URL filtrovat podle černé nebo bílé listiny. ● Černá listina: Zablokuje přístup k internetu zařízením uvedeným na černé listině. ● Bílá listina: Povolí přístup k internetu POUZE zařízením uvedeným na bílé listině.
Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
URL Zadejte požadovanou adresu URL nebo klíčová slova, která chcete filtrovat. Filtr rozlišuje malá/velká písmena.

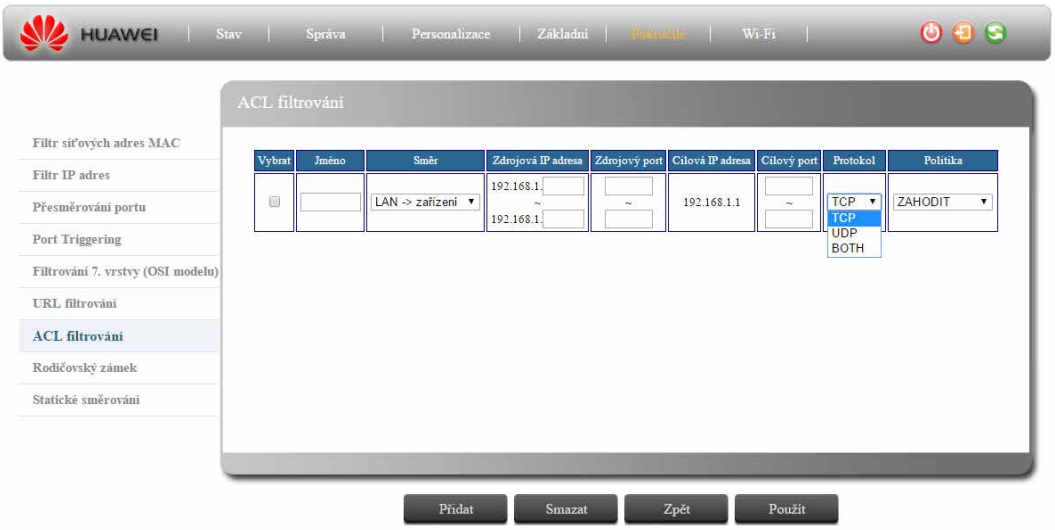
	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.7 Pokročilé > ACL filtrování

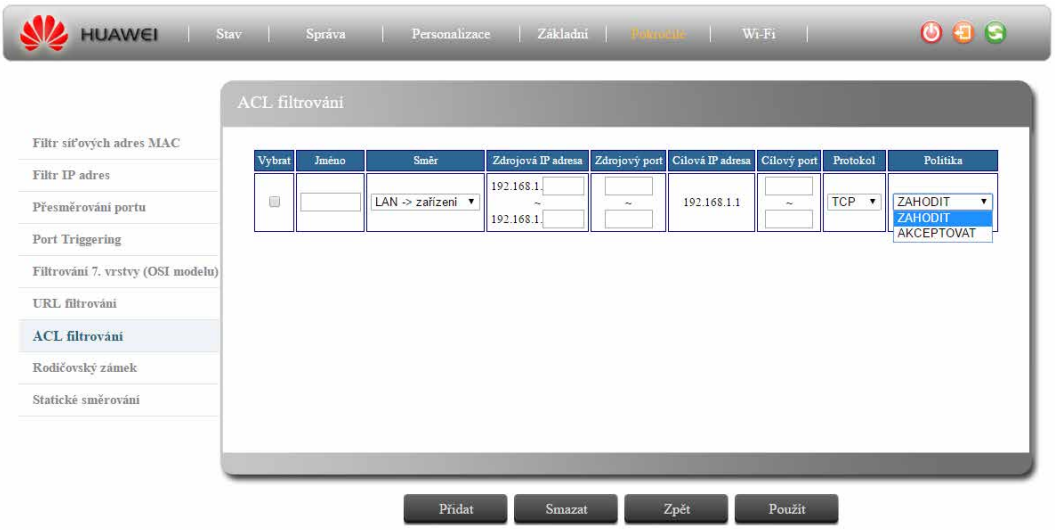
Obrázek 2-46 ACL filtrování – 1



Obrázek 2-47 ACL filtrování – 2



Obrázek 2-48 ACL filtrování – 3



Vybrat

Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.

Jméno

Zadejte jméno příslušného pravidla ACL filtrování. Jméno může být libovolné a max. 10 znaků dlouhé.

Směr

Zadejte směr filtrování

- LAN -> zařízení
- LAN -> WAN
- WAN -> LAN
- WAN -> zařízení

Zdrojová IP adresa

Zadejte spodní a horní mez rozsahu zdrojových IP adres, pro které bude pravidlo filtrování platit.

Zdrojový port

Zadejte rozsah zdrojových portů.

Cílová IP adresa

Zadejte spodní a horní mez rozsahu cílových IP adres, pro které bude pravidlo filtrování platit.

Cílový port

Zadejte rozsah cílových portů.

Protokol

Zadejte, jaký typ paketů bude filtrován:

- TCP
- UDP
- BOTH (oba)

Politika

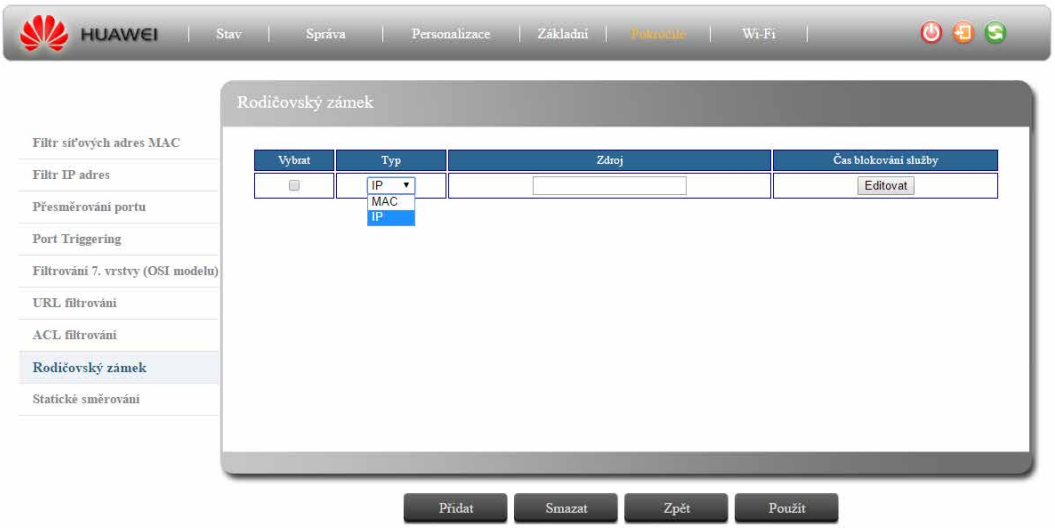
Vyberte z rozbalovacího seznamu akci, která bude při filtrování provedena:

- ZAHODIT
- AKCEPTOVAT

	Pomocí tlačítek **Přidat** a **Smazat** lze přidávat nebo mazat jednotlivá pravidla. Tuto akci následně potvrdíte kliknutím na tlačítko „Použít“. Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.4.8 Pokročilé > Rodičovský zámek

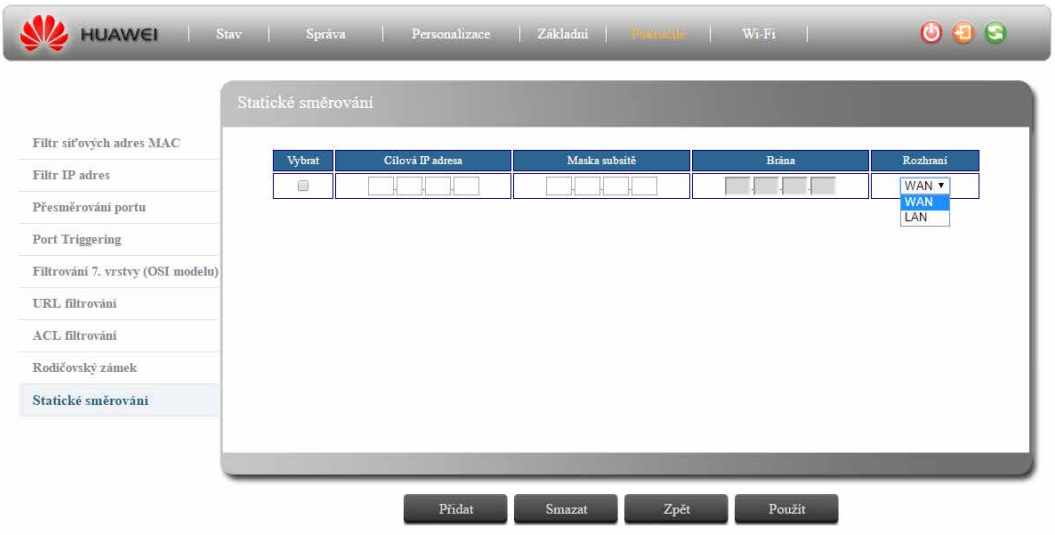
Obrázek 2-49 Rodičovský zámek



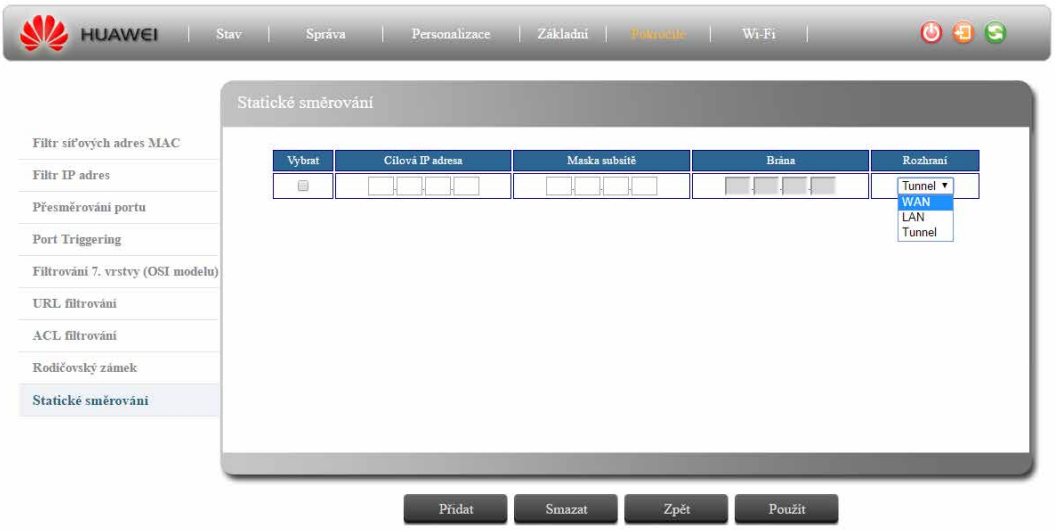
Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
Typ Zvolte typ identifikace nevhodného obsahu.
Zdroj Zadejte IP nebo MAC adresu cesty, kterou chcete blokovat.
Čas blokování služby Zvolte čas, během kterého chcete řídit odchozí datový provoz.

2.4.9 Pokročilé > Statické směrování

Obrázek 2-50 Statické směrování – režim Brána



Obrázek 2-51 Statické směrování – režim VPN



Vybrat Zaškrtnutím tohoto pole a stisknutím tlačítka „Smazat“ odstraníte příslušný záznam.
Číslo Identifikuje číslo příslušného pravidla statického směrování.
Cílová IP adresa Zadejte IP adresu požadované cesty.

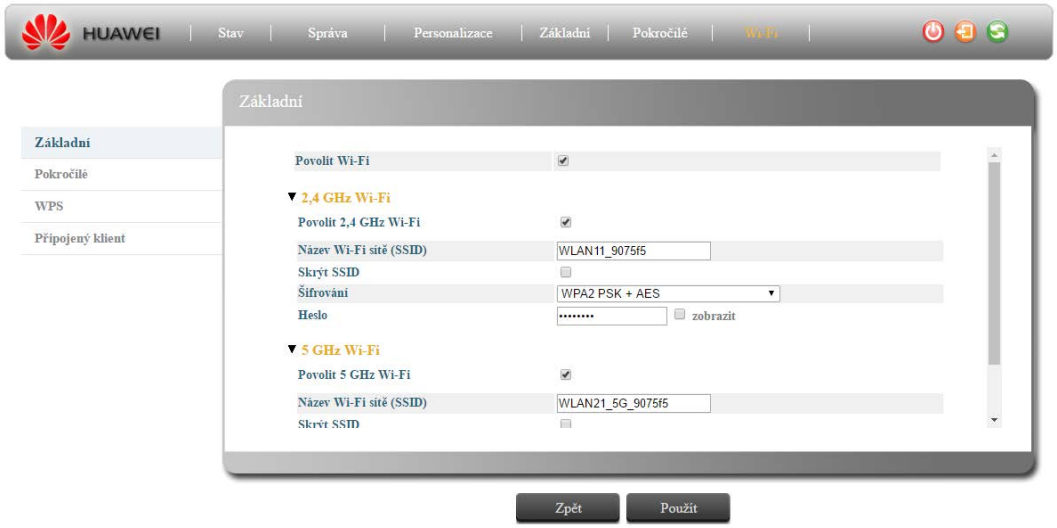
Maska subsítě Zadejte masku podsítě cílové sítě.
Brána Bránou může být směrovač (router) nebo přepínač (switch) umístěný ve stejné části sítě jako rozhraní LAN/WAN/Tunnel tohoto zařízení. Určete rozhraní pro příslušné pravidlo směrování.

	Tato funkce je k dispozici v režimech Brána, Router a VPN. Pokud je některý z těchto režimů aktivní, bude stránka „Statické směrování“ k dispozici. Pokud budete používat provozní režim VPN nebo WAN, zobrazí se v nabídce jako možné rozhraní položka „Tunnel“.

2.5 Wi-Fi

2.5.1 Wi-Fi > Základní

Obrázek 2-52 Wi-Fi – základní



Povolit Wi-Fi Zaškrtávací pole pro zapnutí/vypnutí Wi-Fi.

2,4 GHz Wi-Fi

- **Povolit 2,4 GHz Wi-Fi**
  Zaškrtávací pole pro zapnutí/vypnutí Wi-Fi v pásmu 2,4 GHz.
- **Název Wi-Fi sítě (SSID)**
  Identifikátor bezdrátové sítě (SSID). SSID rozlišuje velká/malá písmena a jeho délka je omezena na 32 alfanumerických znaků.
  Pro název sítě (SSID) lze použít následující znaky:

'	(	)	*	-	.	/	0	1	2	3	4	5	6	7	8
9	:	<	=	>	@	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
[	]	^	_	`	a	b	c	d	e	f	g	h	i	j	k
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	{
|	}	~													

- **Skrýt SSID**
  Tato funkce slouží ke skrytí SSID sítě před ostatními zařízeními a zabraňuje tak neočekávanému požadavku na připojení. Po zaškrtnutí tohoto pole bude SSID sítě skryté, pokud pole zaškrtnuté nebude, SSID bude veřejné.

- **Šifrování**
  Datový provoz mezi modemem a připojenými klienty musí být chráněný před narušením a odposloucháváním.

  Za účelem zvýšení zabezpečení sítě podporuje tento modem několik šifrovacích mechanismů. Použití jednotlivých typů šifrování se odvíjí od požadované úrovně zabezpečení sítě, dostupných technických a administrátorských zdrojů a softwarové podpory u bezdrátových klientů.

  K dispozici je několik možností. Po kliknutí se zobrazí rozbalovací seznam se všemi možnostmi. Možnost „Open System“ v kombinaci s vypnutým šifrováním představuje nulovou míru zabezpečení. Libovolný klient se bude moci okamžitě připojit k síti Wi-Fi.

  K dispozici jsou dále následující způsoby šifrování:

  - **Open WEP**
  - **Sdílený klíč**
  - **WPA2 PSK**
  - **WPA-WPA2-Mixed PSK**

5 GHz Wi-Fi

- **Povolit 5 GHz Wi-Fi**
  Zaškrtávací pole pro zapnutí/vypnutí Wi-Fi v pásmu 5 GHz.
- **Název Wi-Fi sítě (SSID)**
  Identifikátor bezdrátové sítě (SSID). SSID rozlišuje velká/malá písmena a jeho délka je omezena na 32 alfanumerických znaků.
  Pro název sítě (SSID) lze použít následující znaky:

'	(	)	*	-	.	/	0	1	2	3	4	5	6	7	8
9	:	<	=	>	@	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
[	]	^	_	`	a	b	c	d	e	f	g	h	i	j	k
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	{
|	}	~													

- **Skrýt SSID**
  Tato funkce slouží ke skrytí SSID sítě před ostatními zařízeními a zabraňuje tak neočekávanému požadavku na připojení. Po zaškrtnutí tohoto pole bude SSID sítě skryté, pokud pole zaškrtnuté nebude, SSID bude veřejné.

- **Šifrování**
  Datový provoz mezi modemem a připojenými klienty musí být chráněný před narušením a odposloucháváním.

  Za účelem zvýšení zabezpečení sítě podporuje tento modem několik šifrovacích mechanismů. Použití jednotlivých typů šifrování se odvíjí od požadované úrovně zabezpečení sítě, dostupných technických a administrátorských zdrojů a softwarové podpory u bezdrátových klientů.

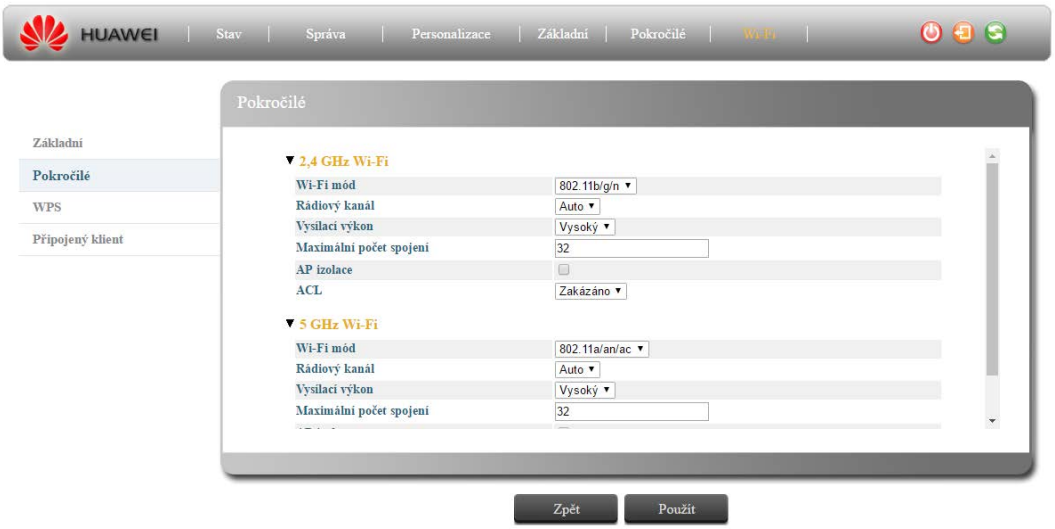
  K dispozici je několik možností. Po kliknutí se zobrazí rozbalovací seznam se všemi možnostmi. Možnost „Open System“ v kombinaci s vypnutým šifrováním představuje nulovou míru zabezpečení. Libovolný klient se bude moci okamžitě připojit k síti Wi-Fi.

  K dispozici jsou dále následující způsoby šifrování:

  - **Open WEP**
  - **Sdílený klíč**
  - **WPA2 PSK**
  - **WPA-WPA2-Mixed PSK**

2.5.2 Wi-Fi > Pokročilé

Obrázek 2-53 Wi-Fi – pokročilé



2,4 GHz Wi-Fi

- **Wi-Fi mód**
  Výběr ze standardů Wi-Fi protokolu 802.11 b/g/n.
- **Rádiový kanál**
  Rádiový kanál používaný k vzájemné komunikaci modemu a připojených klientů. Kanál musí být shodný napříč všemi připojenými zařízeními. Počet dostupných kanálů závisí na místních nařízeních.
- **Maximální počet spojení**
  Maximální počet současně připojených klientů.
- **AP izolace**
  Pokud je toto zaškrtávací pole odškrtnuto, veškerá připojená zařízení si mohou mezi sebou vzájemně odesílat diagnostický příkaz ping. Pokud je toto zaškrtávací pole zaškrtnuto, není vzájemné odesílání příkazu ping povoleno.
- **ACL**
  Tato záložka slouží pro přidání MAC adres klientů, kterým bude umožněno přistoupit k administrátorskému rozhraní.

  Krok 1: Zvolte možnost **Vypnuto**, **Povolit** nebo **Zakázat**.

  Krok 2: Kliknutím na tlačítko „Vložit“ přidejte do seznamu požadovanou MAC adresu a doplňte příslušné parametry.

5 GHz Wi-Fi

- **Wi-Fi mód**
  Výběr ze standardů Wi-Fi protokolu 802.11 a/n/ac.
- **Rádiový kanál**
  Rádiový kanál používaný k vzájemné komunikaci modemu a připojených klientů. Kanál musí být shodný napříč všemi připojenými zařízeními. Počet dostupných kanálů závisí na místních nařízeních.
- **Maximální počet spojení**
  Maximální počet současně připojených klientů.
- **AP izolace**
  Pokud je toto zaškrtávací pole odškrtnuto, veškerá připojená zařízení si mohou mezi sebou vzájemně odesílat diagnostický příkaz ping. Pokud je toto zaškrtávací pole zaškrtnuto, není vzájemné odesílání příkazu ping povoleno.
- **ACL**
  Tato záložka slouží pro přidání MAC adres klientů, kterým bude umožněno přistoupit k administrátorskému rozhraní.

  Krok 1: Zvolte možnost **Vypnuto**, **Povolit** nebo **Zakázat**.

  Krok 2: Kliknutím na tlačítko „Vložit“ přidejte do seznamu požadovanou MAC adresu a doplňte příslušné parametry.

	Kliknutím na tlačítko **Zpět** vrátíte veškeré provedené změny zpět. Kliknutím na tlačítko **Použít** provedené změny uložíte.

2.5.3 Wi-Fi > WPS

Obrázek 2-54 Wi-Fi – WPS

2,4 GHz Wi-Fi

2.4GHz Wi-Fi podporuje ŽÁDNÝ, WPA2 PSK + AES, WPA-WPA2-MIXED PSK + TKIP/AES.

- **PBC**
  Připojení a šifrování datového přenosu u libovolného zařízení je možné po stisknutí tlačítka. Mějte na paměti, že v dvouminutovém intervalu, během kterého probíhá konfigurace připojení, se do sítě mohou připojit nevyžádaná zařízení, která jsou v dosahu.
  - **Start**
    Zvolte PBC a stiskněte tlačítko „Start“. Funkce WPS bude spuštěna a zahájí pokus o připojení k dostupným klientům.
- **PIN**
  Před připojením každého zařízení prostřednictvím funkce WPS bude vyžadováno zadání kódu PIN.
  - **Kód PIN:**
    Čtyř až osmimístný kód PIN je nutné zadat na zařízení, které chcete připojit do sítě. Po zadání příslušného kódu WPS klienta se zobrazí tlačítko „Start“.
  - **Start**
    Zadejte kód PIN a stiskněte tlačítko „Start“. Funkce WPS bude spuštěna a zahájí pokus o připojení k dostupným klientům.

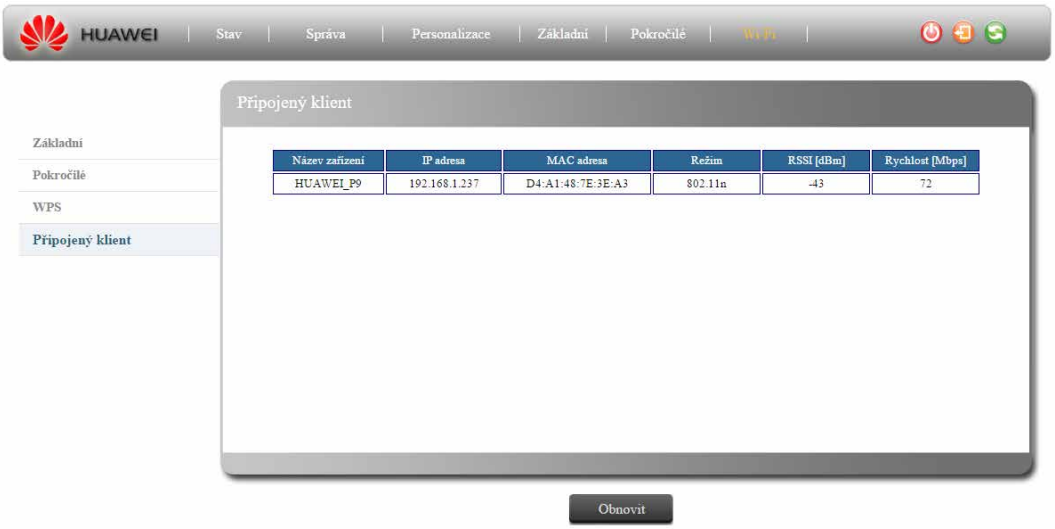
5 GHz Wi-Fi

5GHz Wi-Fi podporuje ŽÁDNÝ, WPA2 PSK + AES, WPA-WPA2-MIXED PSK + TKIP/AES.

- **PBC**
  Připojení a šifrování datového přenosu u libovolného zařízení je možné po stisknutí tlačítka. Mějte na paměti, že v dvouminutovém intervalu, během kterého probíhá konfigurace připojení, se do sítě mohou připojit nevyžádaná zařízení, která jsou v dosahu.
  - **Start**
    Zvolte PBC a stiskněte tlačítko „Start“. Funkce WPS bude spuštěna a zahájí pokus o připojení k dostupným klientům.
- **PIN**
  Před připojením každého zařízení prostřednictvím funkce WPS bude vyžadováno zadání kódu PIN.
  - **Kód PIN:**
    Čtyř až osmimístný kód PIN je nutné zadat na zařízení, které chcete připojit do sítě. Po zadání příslušného kódu WPS klienta se zobrazí tlačítko „Start“.
  - **Start**
    Zadejte kód PIN a stiskněte tlačítko „Start“. Funkce WPS bude spuštěna a zahájí pokus o připojení k dostupným klientům.

2.5.4 Wi-Fi > Připojený klient

Obrázek 2-55 Připojený klient



Název zařízení Název připojeného zařízení.
IP adresa IP adresa přidělená zařízení modemem.
MAC adresa MAC adresa klienta.
Režim Mód Wi-Fi, ve kterém je klient připojen.
RSSI [dBm] Hodnota síly přijatého signálu.
Rychlost [Mbps] Maximální podporovaná rychlost.

Příloha 1: Evropa – EU prohlášení o shodě

Společnost Huawei Technologies Co., Ltd. tímto prohlašuje, že LTE outdoor modem typu B2338-168 je ve shodě se základními požadavky a s dalšími příslušnými ustanoveními směrnice 1999/5/ES (a Nařízení vlády č. 426/2000 Sb.).

Tento LTE outdoor modem nevysílá na místech nepokrytých signálem sítě.

Výstraha: používejte výhradně příslušenství schválené výrobcem

K ověření předpokladu shody se základními požadavky směrnice R&TTE 1999/5/ES byly použity následující testovací metody.

- **EN 301 908-1 V7.1.1**
- **EN 301 908-13 V6.2.1**
- **EN 300 328 V1.9.1**
- **EN 301 893 V1.8.1**
- **EN 62311:2008, EN50385:2002**
- **EN 301 489-1 V1.9.2**
- **EN 301 489-17 V2.2.1**
- **EN 301 489-24 V1.5.1**
- **EN 300 386 V1.6.1**
- **EN 55022:2010/AC:2011, EN 55024:2010**
- **EN 60950-1:2006 + A1:2010 + A11:2009 + A12:2011 + A2:2013**
- **EN 60950-22: 2006**

Česky [Czech]	Huawei Technologies Co., Ltd. tímto prohlašuje, že tento modem B2338-168 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Toto zařízení vyhovuje limitům pro vystavení radiaci stanoveným pro nekontrolované prostředí. Toto zařízení by mělo být naistalováno a provozováno s minimálním odstupem 25 cm mezi zdrojem záření a tělem uživatele.