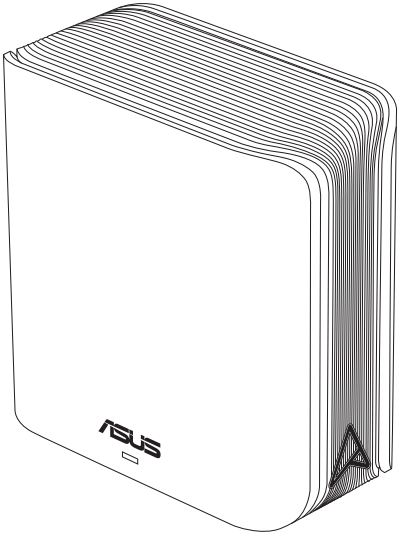
# Uživatelská příručka

# ZenWiFi BD4

## BE3600 Dvoupásmový Router



IN SEARCH OF INCREDIBLE

CZ23951

První edice

Srpen 2024

# Obsah

# Obsah

# Obsah

# 1 Seznámení s bezdrátovým směrovačem

## 1.1 Vítejte!

Děkujeme vám za zakoupení bezdrátového směrovače ASUS ZenWiFi BD4!

S kovovým odstínem v barvě monogramu A na minimalistické bílé skříni nabízí ZenWiFi BD4 vybaven duálními pásmy 2,4 GHz a 5 GHz pro bezkonkurenční souběžné bezdrátové HD streamování; server SMB, server UPnP AV a server FTP pro sdílení souborů 24/7; kapacita zpracování 300 000 relací; a technologie ASUS Green Network, která poskytuje řešení pro úsporu až 70 % energie.

## 1.2 Obsah krabice

☑ Bezdrátový směrovač ZenWiFi BD4

☑ Napájecí adaptér

☑ Záruční list

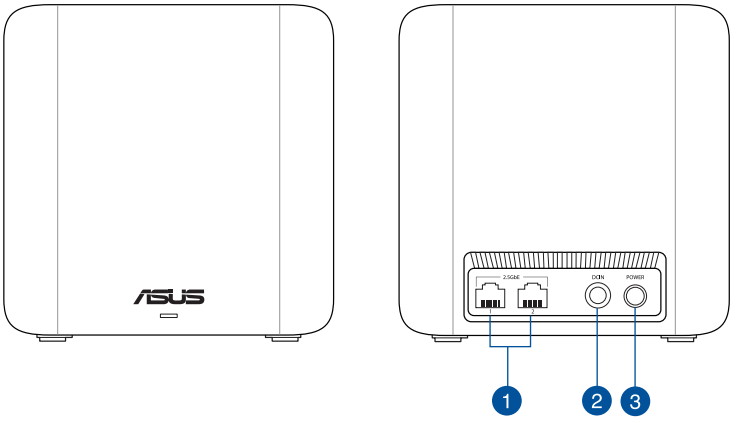
☑ Kabel RJ45

☑ Stručná příručka

**POZNÁMKY:**

- Pokud je některá z položek poškozená nebo chybí, kontaktujte společnost ASUS pro technické připomínky a podporu. Viz **Service and Support (Servis a Podpora)** na zadní straně této příručky.
- Uschovejte původní obalový materiál pro případ budoucího záručního servisu, například opravy nebo výměny.

# 1.3 Váš bezdrátový směrovač




| | |
|---|---|
| 1 | **Porty 2,5GbE (Automatická detekce WAN/LAN)**<br>K těmto portům připojte síťové kabely pro navázání 2.5GbE WAN/LAN připojení. |
| 2 | **Port vstupu stejnosměrného napájení (DCIN)**<br>K tomuto portu připojte dodaný adaptér střídavého napájení (AC) a připojte směrovač ke zdroji napájení. |
| 3 | **Tlačítko napájení**<br>Stisknutím tohoto tlačítka systém zapnete nebo vypnete. |

**POZNÁMKY**:

- Používejte pouze adaptér dodaný se zařízením. Používání jiných adaptérů může poškodit zařízení.
- **Technické údaje:**

| | | | |
|---|---|---|---|
| **Adaptér stejnosměrného napájení** | Výstup stejnosměrného napájení: +12V s proudem max. 1,5A | | |
| **Provozní teplota** | 0~40°C | Skladování | 0~70°C |
| **Provozní vlhkost** | 50~90% | Skladování | 20~90% |

## 1.4 Umístění bezdrátového směrovače

Aby byl zajištěn optimální přenos bezdrátového signálu mezi bezdrátovým směrovačem a síťovými zařízeními, zajistěte, aby byly splněny následující podmínky:

- Umístěte bezdrátový směrovač do centralizované oblasti pro maximální bezdrátové pokrytí pro síťová zařízení.
- Udržujte zařízení mimo kovové překážky a mimo přímé sluneční záření.
- Udržujte zařízení v bezpečné vzdálenosti od zařízení Wi-Fi 802.11g nebo 20 MHz, počítačových periférií 2,4 GHz, zařízení Bluetooth, bezdrátových telefonů, transformátorů, výkonných motorů, fluorescenčního osvětlení, mikrovlnných trub, chladniček a dalšího průmyslového vybavení, aby se zabránilo ztrátě signálu.
- Vždy zaktualizujte na nejnovější firmware. Nejnovější aktualizace firmwaru jsou k dispozici na webu společnosti ASUS na adrese **http://www.asus.com**.

## 1.5 Požadavky na instalaci

Chcete-li vytvořit síť, potřebujete jeden nebo dva počítače, které splňují následující požadavky na systém:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Možnost připojení k bezdrátové síti IEEE 802.11a/b/g/n/ac/ax
- Nainstalovaná služba TCP/IP
- Webový prohlížeč, například Internet Explorer, Firefox, Safari nebo Google Chrome

---

**POZNÁMKY:**

- Pokud ve vašem počítači nejsou integrovány možnosti připojení k bezdrátové síti, můžete do počítače nainstalovat adaptér IEEE 802.11a/b/g/n/ac/ax WLAN pro připojení k síti.
- Díky dvojpásmové technologii tento bezdrátový směrovač podporuje bezdrátové signály 2,4 GHz a 5 GHz současně. To vám umožňuje provádět aktivity související s Internetem, například procházení Internetu nebo čtení/psaní e-mailových zpráv prostřednictvím pásma 2,4 GHz a zároveň přenášet datové proudy se zvukovými soubory/ videosoubory o vysokém rozlišení, například filmy nebo hudbu prostřednictvím pásma 5 GHz.
- Některá zařízení standardu IEEE 802.11n, která chcete připojit k vaší síti, nemusí podporovat pásmo 5 GHz. Specifikace najdete v uživatelské příručce k příslušnému zařízení.
- Ethernetové kabely RJ-45, které budou použity k připojení síťových zařízení, nesmí přesahovat 100 metrů.

---

**DŮLEŽITÉ!**

- Některé bezdrátové adaptéry mohou mít problémy s připojením k WiFi přístupovým bodům 802.11ax.
- Pokud se s takovým problémem setkáte, zaktualizujte ovladač na nejnovější verzi. Softwarové ovladače, aktualizace a další související informace najdete na oficiální stránce podpory výrobce.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

---

# 2 Nastavení hardwaru

## 2.1 Instalace směrovače

**DŮLEŽITÉ!**

- Aby se zabránilo možným instalačním problémům, při instalaci bezdrátového směrovače použijte kabelové připojení.
- Před instalací bezdrátového směrovače ASUS proveďte následující kroky:
  - Pokud vyměňujete stávající směrovač, odpojte jej od sítě.
  - Odpojte kabely/vodiče od instalace stávajícího modemu. Pokud je modem vybaven záložní baterií, rovněž ji vyjměte.
  - Restartujte počítač (doporučeno).

**VAROVÁNÍ!**

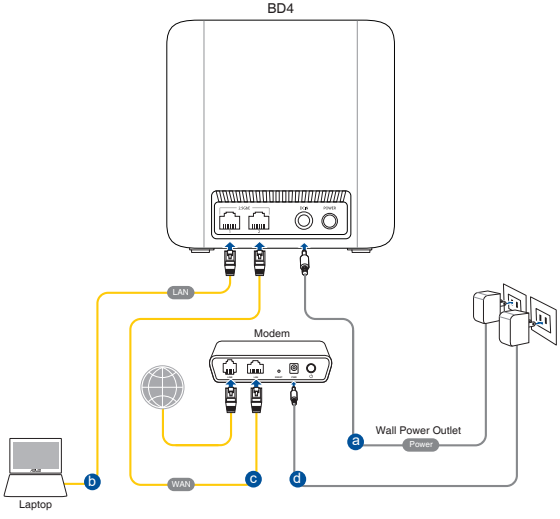
- Napájecí kabel(y) musí být připojeny do elektrické zásuvky (zásuvek) s vhodným uzemněním. Zařízení připojujte pouze k blízké zásuvce, která je snadno dostupná.
- Pokud je napájecí zdroj porouchaný, nepokoušejte se jej opravovat. Kontaktujte kvalifikovaného servisního technika nebo prodejce.
- NEPOUŽÍVEJTE poškozené napájecí kabely, doplňky ani jiné periférie.
- NEINSTALUJTE toto vybavení výše než do výšky 2 metrů.
- Počítač používejte jen při teplotě okolí 0 ˚C (32 ˚F) až 40 ˚C (104 ˚F).

## A. Pevné připojení

**POZNÁMKA:** Pro kabelové připojení můžete použít přímý nebo přechodový kabel.

### Pokyny pro instalaci bezdrátového směrovače prostřednictvím pevného připojení:

1. Připojte směrovač k elektrické zásuvce a zapněte napájení. Připojte síťový kabel od počítače k portu 2.5GbE na směrovači.

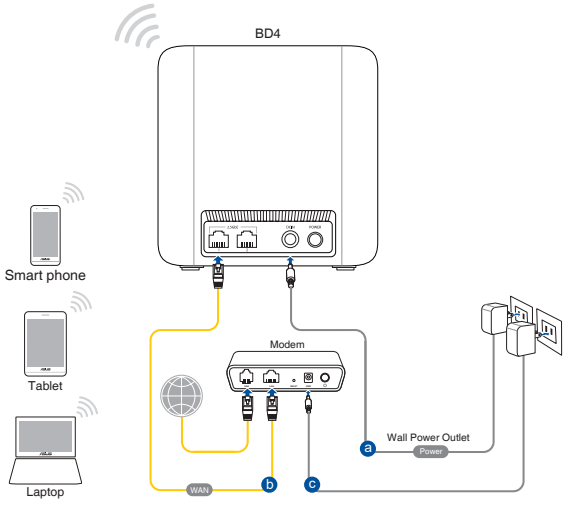



2. Po spuštění webového prohlížeče se automaticky spustí webové grafické uživatelské rozhraní. Pokud se nespustí automaticky, zadejte http://www.asusrouter.com.
3. Nastavte heslo směrovače, aby se zabránilo neoprávněnému přístupu.

## B. Bezdrátové připojení

**Pokyny pro konfiguraci bezdrátového směrovače prostřednictvím bezdrátového připojení:**

1. Připojte směrovač k elektrické zásuvce a zapněte napájení.




2. Připojte se k názvu sítě (SSID), který je uveden na štítku produktu na boční straně směrovače. Pro zvýšení zabezpečení sítě změňte na jedinečné SSID a vytvořte heslo.

| | |
|---|---|
| Název sítě Wi-Fi (SSID) : | ASUS_XX |

* **XX** označuje poslední dvě číslice adresy MAC 2,4 GHz. Je uvedeno na štítku na zadní straně přístroje směrovač.

3. Po spuštění webového prohlížeče se automaticky spustí webové grafické uživatelské rozhraní. Pokud se nespustí automaticky, zadejte http://www.asusrouter.com.
4. Nastavte heslo směrovače, aby se zabránilo neoprávněnému přístupu.

**POZNÁMKY:**

- Podrobnosti o připojení k bezdrátové síti viz uživatelská příručka k adaptéru WLAN.
- Pokyny pro konfigurování nastavení zabezpečení vaší sítě viz část **3.1.1 Setting up the wireless security settings (Konfigurování nastavení zabezpečení bezdrátového připojení)** této uživatelské příručky.

## 2.2 Rychlé nastavení Internetu (QIS) s automatickým rozpoznáním

Funkce Rychlé nastavení Internetu (QIS) vás provede rychlou konfigurací připojení k Internetu.

**POZNÁMKA**: Při prvním nastavování internetového připojení stisknutím resetovacího tlačítka na bezdrátovém směrovači obnovte jeho výchozí tovární nastavení.

**Pokyny pro použití funkce QIS s automatickým rozpoznáním:**

1. Spusťte webový prohlížeč. Budete přesměrováni na Průvodce nastavením ASUS (Rychlé nastavení internetu). Pokud ne, zadejte ručně http://www.asusrouter.com.
2. Bezdrátový směrovač automaticky rozpozná, zda je typ vaše připojení ISP **Dynamic IP (Dynamická IP)**, **PPPoE**, **PPTP**, a **L2TP**. Zadejte nezbytné informace pro váš typ připojení ISP.

   **DŮLEŽITÉ!** Získejte nezbytné informace o typu vašeho připojení k Internetu od vašeho ISP.

   **POZNÁMKY**:
   - Automatické rozpoznání vašeho typu připojení ISP je provedeno, když konfigurujete bezdrátový směrovač poprvé nebo když byla obnovena výchozí nastavení vašeho bezdrátového směrovače.
   - Pokud funkce Rychlé nastavení Internetu (QIS) nerozpoznala typ vašeho internetového připojení, klepněte na **Manual setting (Ruční nastavení)** a ručně nakonfigurujte nastavení připojení.

3. Přiřaďte název bezdrátové sítě (SSID) a bezpečnostní klíč pro bezdrátové připojení WiFi 7 Network. Po dokončení klepněte na tlačítko **Apply (Použít)**.
4. Na stránce **Login Information Setup (Nastavení přihlašovacích údajů)** změňte heslo směrovače, aby se zabránilo neoprávněnému přístupu k vašemu bezdrátovému směrovači.

**POZNÁMKY:** Uživatelské jméno a heslo pro přihlášení k bezdrátovému směrovači se liší od názvu sítě (SSID) WiFi 7 a bezpečnostního klíče. Uživatelské jméno a heslo pro přihlášení k bezdrátovému směrovači vám umožňuje přihlásit se k webovému grafickému uživatelskému rozhraní (GUI) bezdrátového směrovače a konfigurovat nastavení bezdrátového směrovače. Název sítě (SSID) WiFi 7 a bezpečnostní klíč umožňují zařízením Wi-Fi přihlašovat a připojovat se k vaší síti WiFi 7.

## 2.3 Připojení k bezdrátové síti

Po nakonfigurování bezdrátového směrovače prostřednictvím QIS můžete připojit počítač a další chytrá zařízení k vaší bezdrátové síti.

**Pokyny pro připojení k vaší síti:**

1. Klepnutím na ikonu v oznamovací oblasti v počítači zobrazíte dostupné bezdrátové sítě.
2. Vyberte bezdrátovou síť, ke které se chcete připojit, a poté klepněte na **Connect (Připojit)**.
3. Zabezpečená bezdrátová síť může vyžadovat zadání klíče zabezpečení, poté klepněte na **OK**.
4. Vyčkejte, než počítač úspěšně naváže připojení k bezdrátové síti. Zobrazí se stav připojení a ikona sítě v oznamovací oblasti zobrazuje stav .

**POZNÁMKY:**

- Další podrobnosti o konfigurování nastavení bezdrátové sítě viz další kapitoly.
- Další podrobnosti o připojení zařízení k bezdrátové síti viz uživatelská příručka k zařízení.

# 3 Konfigurování obecných a upřesňujících nastavení

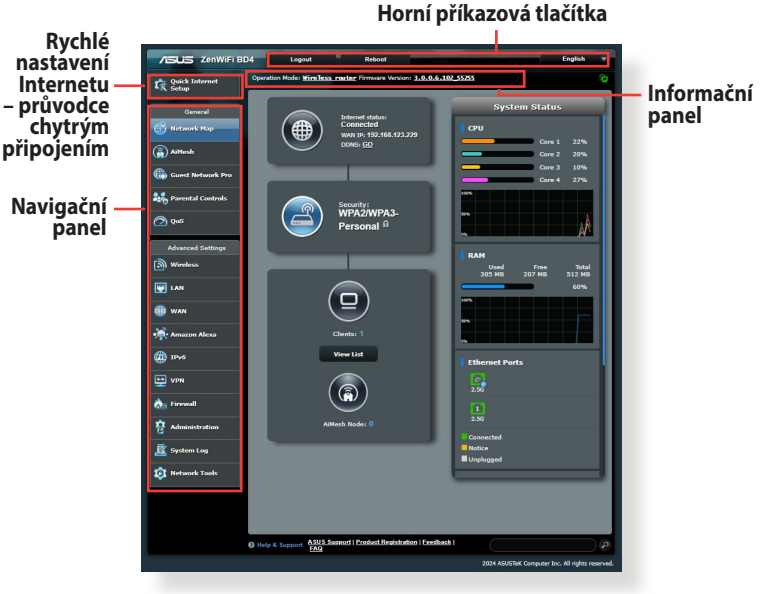
## 3.1 Přihlášení k webovému grafickému uživatelskému rozhraní (GUI)

Tento bezdrátový směrovač ASUS nabízí intuitivní webové uživatelské rozhraní, které umožňuje snadno konfigurovat různé funkce prostřednictvím webového prohlížeče, jako je Internet Explorer, Firefox, Safari nebo Google Chrome.

**POZNÁMKA:** Vlastnosti se mohou lišit v závislosti na verzi firmwaru.

**Pokyny pro přihlášení k webovému grafickému uživatelskému rozhraní (GUI):**

1. Ručně zadejte výchozí adresu IP bezdrátového směrovače do vašeho webového prohlížeče, například Internet Explorer, Firefox, Safari nebo Google Chrome: http://www.asusrouter.com.
2. Na stránce pro přihlášení, zadejte uživatelské jméno a heslo, která jste nastavili v části **2.2 Quick Internet Setup (QIS) with Autodetection (Rychlé nastavení internetu (QIS) s automatickou detekcí)**.
3. Nyní můžete ke konfigurování různých nastavení bezdrátového směrovače ASUS používat webové grafické uživatelské rozhraní (GUI).




* Obrázek je pouze orientační.

**POZNÁMKA:** Při prvním přihlášení k webovému grafickému uživatelskému rozhraní (GUI) budete automaticky přesměrováni na stránku Rychlého průvodce instalací (QIS).

### 3.1.1 Konfigurování nastavení zabezpečení bezdrátového připojení

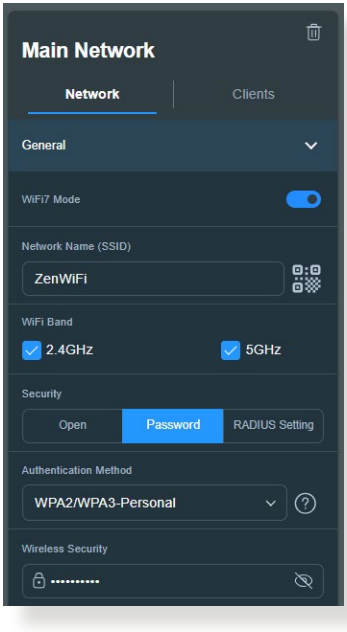
Chcete-li chránit vaši bezdrátovou síť před neoprávněným přístupem, je třeba nakonfigurovat nastavení jejího zabezpečení.

**Pokyny pro konfigurování zabezpečení bezdrátového připojení:**

1. Na navigačním panelu přejděte na **General (Obecné) > Network Map (Mapa sítě)**.
2. Vyberte síť a můžete nakonfigurovat nastavení zabezpečení bezdrátové sítě, například SSID, úroveň zabezpečení a nastavení šifrování.

**POZNÁMKY**: Můžete nakonfigurovat různá nastavení zabezpečení bezdrátového připojení pro pásma 2,4 GHz a 5 GHz.

#### Nastavení zabezpečení 2,4 GHz/5 GHz




3. Do pole **Network Name (SSID) (Název sítě (SSID))** zadejte jedinečný název vaší bezdrátové sítě.

4. V rozevíracím seznamu **WEP Encryption (Šifrování WEP)** vyberte metodu šifrování pro vaši bezdrátovou síť.

**DŮLEŽITÉ!** Standard IEEE 802.11n/ac/ax zakazuje používání vysoké prostupnosti s metodami šifrování WEP nebo WPA-TKP jako šifry unicast. Použijete-li tyto metody šifrování, vaše rychlost přenosu dat klesne na připojení IEEE 802.11g 54 Mb/s.

5. Zadejte váš zabezpečovací klíč.
6. Po dokončení klepněte na tlačítko **Apply (Použít)**.

### 3.1.2 Správa síťových klientů

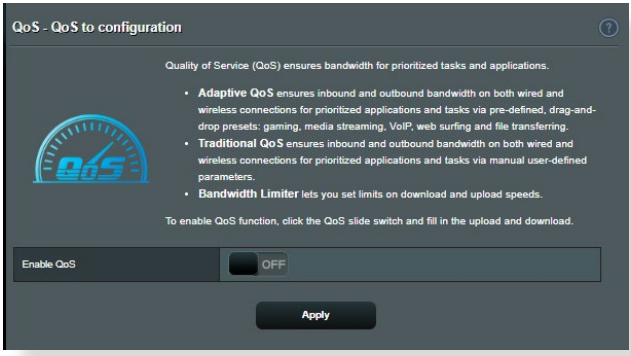

**Pokyny pro správu síťových klientů:**

1. Na navigačním panelu přejděte na **General (Obecné) > Network Map (Mapa sítě)**.
2. Výběrem ikony **Client Status (Stav klientů)** na obrazovce Network Map (Mapa sítě) zobrazte informace o vašich síťových klientech.
3. Chcete-li některému klientovi blokovat přístup k vaší síti, vyberte klienta a klepněte na **block (blokovat)**.

## 3.2 Adaptivní QoS

### 3.2.1 Správa šířky pásma QoS (Quality of Service)

Služba Quality of Service (QoS) umožňuje nastavit prioritu pásma a spravovat síťový provoz.




**Pokyny pro nastavení priority šířky pásma:**

1. Na navigačním panelu přejděte na **General (Obecné)** > **Adaptive QoS (Adaptivní QoS)** > **QoS**.
2. Klepnutím na **ON (ZAPNUTO)** aktivujte výchozí pravidlo a vyplňte políčka šířky pásma odesílání a přijímání.

   **POZNÁMKA:** Požádejte vašeho ISP o informace o šířce pásma.

3. Klepněte na **Apply (Použít)**.

   **POZNÁMKA:** Položka User Specify Rule List (Seznam pravidel určených uživatelem) je určena pro pokročilá nastavení. Chcete-li upřednostnit konkrétní síťové aplikace a síťové služby, klepněte na položku **User-defined QoS rules (Seznam pravidel určených uživatelem)** nebo **User-defined Priority (Priorita definovaná uživatelem)** v rozevíracím seznamu v pravém horním rohu.

4. Na stránce **user-defined QoS rules (Seznam pravidel určených uživatelem)** jsou k dispozici čtyři výchozí typy online služeb – procházení webu, HTTPS a přenosy souborů. Vyberte upřednostňovanou službu, vyplňte údaje **Source IP or MAC (Zdrojová IP nebo MAC)**, **Destination Port (Cílový port)**, **Protocol (Protokol)**, **Transferred (Přeneseno)** a **Priority (Priorita)** a potom klepněte na **Apply (Použít)**. Údaje budou nakonfigurovány na obrazovce pravidel QoS.

**POZNÁMKY:**

- Při zadávání zdrojové IP nebo MAC jsou k dispozici následující možnosti:

  a) Zadejte specifickou adresu IP, například „192.168.122.1".

  b) Zadejte adresy IP v rámci jedné podsítě nebo jednoho fondu IP, například „192.168.123.*" nebo „192.168.*.*"

  c) Zadejte všechny adresy IP jako „*.*.*.*" nebo ponechte pole prázdné.

  d) Formát adresy MAC je šest skupin dvou hexadecimálních číslic oddělených dvojtečkou (:), v pořadí přenášení (například 12:34:56:aa:bc:ef)

- Co se týče rozsahu zdrojových nebo cílových portů, jsou k dispozici následující množnosti:

  a) Zadejte konkrétní port, například „95".

  b) Zadejte porty v rozsahu, například „103:315", „>100" nebo „<65535".

- Sloupec **Transferred (Přeneseno)** obsahuje údaje o provozu odesílání a přijímání (odchozí a příchozí síťový provoz) pro jednu relaci. V tomto sloupci můžete nastavit limit síťového provozu (v KB) pro konkrétní službu, aby byly vygenerovány konkrétní priority pro službu přiřazenou konkrétnímu portu. Například pokud dva síťoví klienti PC 1 a PC 2 přistupují k Internetu (nastaveno jako port 80), ale PC 1 přesáhl limit síťového provozu z důvodu stahování, bude snížena priorita PC 1. Pokud nechcete nastavit omezení provozu, můžete ponechat políčko prázdné.

5. Na stránce **User-defined Priority (Priorita definovaná uživatelem)** můžete upřednostnit síťové aplikace nebo zařízení do pěti úrovní v rozevíracím seznamu **user-defined QoS rules (Seznam pravidel určených uživatelem)**. Na základě úrovně priority můžete použít následující metody odesílání datových paketů:
   - Změňte pořadí odesílaných síťových paketů, které jsou odesílány do Internetu.
   - V tabulce **Upload Bandwidth (Šířka pásma odesílání)** nastavte **Minimum Reserved Bandwidth (Minimální vyhrazená šířka pásma)** a **Maximum Bandwidth Limit (Maximální omezení šířky pásma)** pro různé síťové aplikace s různými úrovněmi priority. Procenta ukazují rychlosti šířek pásma odesílání, které jsou k dispozici pro určené síťové aplikace.

   **POZNÁMKY:**
   - Pakety nízké priority jsou zrušeny pro zajištění přenosu paketů vysoké priority.
   - V tabulce **Download Bandwidth (Šířka pásma stahování)** nastavte **Maximum Bandwidth Limit (Maximální omezení šířky pásma)** pro různé síťové aplikace v odpovídajícím pořadí. Odesílaný paket s vyšší prioritou způsobí přijímaný paket s vyšší prioritou.
   - Pokud aplikace s vysokou prioritou neodesílají žádné pakety, je pro pakety nízké priority k dispozici plná přenosová rychlost připojení k Internetu.

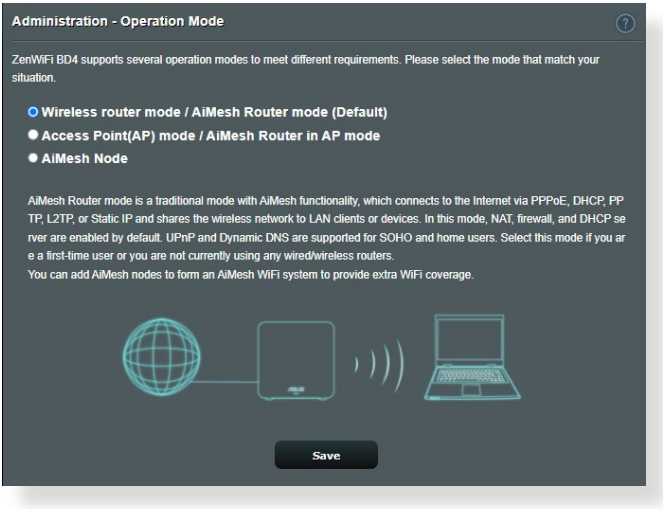
6. Nastavte paket nejvyšší priority. Pro zajištění hladkého hraní online můžete nastavit ACK, SYN a ICMP jako paket nejvyšší priority.

   **POZNÁMKA:** Nejdříve aktivujte QoS a potom nakonfigurujte limity rychlosti odesílání a stahování.

# 3.3 Správa

## 3.3.1 Provozní režim

Na stránce provozního režimu lze vybrat vhodný režim pro vaši síť.




**Pokyny pro nastavení provozního režimu:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Administration (Správa)** > **Operation Mode (Provozní režim)**.
2. Vyberte některý z těchto provozních režimů:
   - **Wireless router mode (default) (Režim bezdrátového směrovače (výchozí))**: V režimu bezdrátového směrovače se bezdrátový směrovač připojuje k Internetu a poskytuje přístup k Internetu dostupným zařízením ve své vlastní místní síti.
   - **Access Point mode (Režim přístupového bodu)**: V tomto režimu vytváří směrovač ve stávající síti novou bezdrátovou síť.
   - **AiMesh Node (Uzel AiMesh):** Jednotku ZenWiFi BD4 můžete nastavit jako uzel AiMesh a rozšířit pokrytí signálem WiFi stávajícími směrovači AiMesh.
3. Klepněte na **Save (Uložit)**.

**POZNÁMKA**: Při změně režimů se směrovač restartuje.

### 3.3.2 Systém

Na stránce **System (Systém)** lze konfigurovat nastavení bezdrátového směrovače.

**Pokyny pro provádění systémových nastavení:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Administration (Správa)** > **System (Systém)**.
2. Můžete konfigurovat následující nastavení:
   - **Change router login password (Změnit heslo pro přihlášení ke směrovači)**: Můžete změnit heslo a jméno pro přihlášení k bezdrátovému směrovači; zadejte nové jméno a heslo.
   - **WPS button behavior (Chování tlačítka WPS)**: Pomocí fyzického tlačítka WPS na bezdrátovém směrovači lze aktivovat WPS.
   - **Time Zone (Časové pásmo)**: Vyberte časové pásmo vaší sítě.
   - **NTP Server (Server NTP)**: Bezdrátový směrovač může přistupovat k serveru NTP (Network time Protocol) a synchronizovat čas.
   - **Enable Telnet (Povolit Telnet)**: Klepnutím na **Yes (Ano)** povolíte služby Telnet v síti. Klepnutím na **No (Ne)** zakážete Telnet.
   - **Authentication Method (Metoda ověřování)**: Pro zajištění přístupu ke směrovači můžete vybrat protokol HTTP, HTTPS nebo oba.
   - **Enable Web Access from WAN (Povolit přístup k síti z WAN)**: Výběrem **Yes (Ano)** povolíte zařízením mimo síť přístup k nastavení GUI bezdrátového směrovače. Výběrem možnosti **No (Ne)** zakážete přístup.
   - **Only allow specific IP (Povolit pouze specifickou adresu IP)**: Chcete-li určit adresy IP zařízení, která mají povolen přístup k nastavení GUI bezdrátového směrovače ze sítě WAN, klepněte na **Yes (Ano)**.
3. Klepněte na **Apply (Použít)**.

### 3.3.3 Upgradování firmwaru

**POZNÁMKA:** Stáhněte nejaktuálnější firmware z webu společnosti ASUS na adrese http://www.asus.com.

**Pokyny pro upgradování firmwaru:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Administration (Správa)** > **Firmware Upgrade (Upgrade firmwaru)**.
2. V poli **Firmware Version (Verze firmwaru)** klepněte na **Check (Zkontrolovat)** a vyhledejte stažený soubor.
3. Klepněte na **Upload (Odeslat)**.

**POZNÁMKY**:

- Po dokončení upgradu chvilku počkejte, než se systém restartuje.
- Dojde-li při procesu upgradování k chybě, bezdrátový směrovač přejde automaticky do nouzového nebo chybového režimu a indikátor LED napájení na předním panelu pomalu bliká. Chcete-li obnovit nebo obnovit systém, viz část **4.2 Obnova firmwaru**.

### 3.3.4 Obnovení/Uložení/Odeslání nastavení

**Pokyny pro obnovení/uložení/odeslání nastavení:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/uložit/načíst nastavení)**.
2. Vyberte úlohy, které chcete provést:
   - Chcete-li obnovit výchozí tovární nastavení, klepněte na **Restore (Obnovit)** a potom klepněte na tlačítko **OK** v potvrzovací zprávě.
   - Chcete-li uložit aktuální nastavení systému, klepněte na **Save setting (Uložit nastavení)**, přejděte na složku, do které chcete soubor uložit, a klepněte na tlačítko **Save (Uložit)**.
   - Chcete-li obnovit předchozí systémová nastavení, klepnutím na **Upload (Odeslat)** vyhledejte systémový soubor, který chcete obnovit, a potom klepněte na **Open (Otevřít)**.

**DŮLEŽITÉ!** Dojde-li k problémům, načtěte nejnovější verzi firmwaru a nakonfigurujte nová nastavení. Neobnovujte výchozí nastavení směrovače.

## 3.4 AiProtection

AiProtection provádí sledování v reálném čase a detekuje malware, spyware a nežádoucí přístup. Rovněž filtruje nežádoucí webové stránky a aplikace a umožňuje plánovat čas, ve kterém připojené zařízení může přistupovat k Internetu.

### 3.4.1 Ochrana sítě

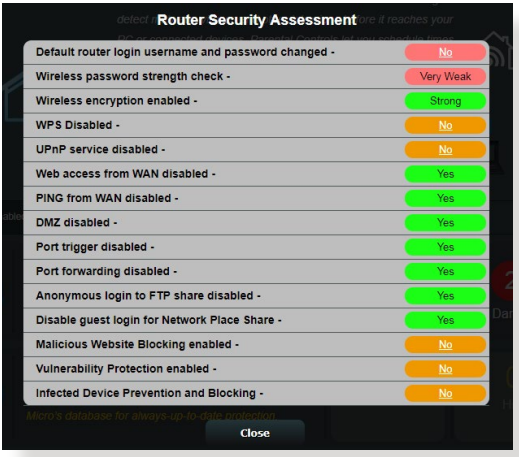
Ochrana sítě chrání síť před zneužitím a zabezpečuje vaši síť před nežádoucím přístupem.

## Konfigurování ochrany sítě

### Pokyny pro konfiguraci ochrany sítě:

1. Na navigačním panelu přejděte na **General (Obecné) > AiProtection.**
2. Na hlavní stránce **AiProtection** klepněte na **Network Protection (Ochrana sítě).**
3. Na kartě **Network Protection (Ochrana sítě)** klepněte na **Scan (Hledat).**

   Po dokončení vyhledávání nástroj zobrazí výsledky na stránce **Router Security Assessment (Vyhodnocení zabezpečení směrovače).**




**DŮLEŽITÉ!** Položky s označením **Yes (Ano)** na stránce **Router Security Assessment (Vyhodnocení zabezpečení směrovače)** jsou považovány v **bezpečném** stavu. U položek s označením **No (Ne), Weak (Slabé)** nebo **Very Weak (Velmi slabé)** se důrazně doporučuje provést příslušnou konfiguraci.

4. (Volitelně) Na stránce **Router Security Assessment (Vyhodnocení zabezpečení směrovače)** ručně nakonfigurujte položky označení **No (Ne), Weak (Slabé)** nebo **Very Weak (Velmi slabé)**. Pokyny:

   a. Klepněte na některou položku.

**POZNÁMKA:** Klepnutím na některou položku budete přesměrováni na stránku jejího nastavení.

b. Na stránce nastavení zabezpečení položky nakonfigurujte a proveďte nezbytné změny; po dokončení klepněte na **Apply (Použít).**

c. Vraťte se na stránku **Router Security Assessment (Vyhodnocení zabezpečení směrovače)** a klepnutím na **Close (Zavřít)** zavřete stránku.

5. Chcete-li, aby byla nastavení zabezpečení provedena automaticky, klepněte na **Secure Your Router (Zabezpečit směrovač).**
6. Po zobrazení zprávy s výzvou klepněte na **OK.**

### Blokování škodlivých webů

Tato funkce omezuje přístup k známým škodlivým webům v cloudové databázi, díky čemuž je ochrana vždy aktuální.

**POZNÁMKA:** Tato funkce se aktivuje automaticky při spuštění **Router Weakness Scan (Hledat slabé stránky směrovače).**

**Pokyny pro aktivaci blokování škodlivých webů:**

1. Na navigačním panelu přejděte na **General (Obecné) > AiProtection.**
2. Na hlavní stránce **AiProtection** klepněte na **Network Protection (Ochrana sítě).**
3. V podokně **Malicious Sites Blocking (Blokování škodlivých webů)** klepněte na **ON (ZAPNUTO).**

### Obousměrné IPS

Obousměrné IPS (systém prevence vniknutí) chrání váš směrovač před síťovými útoky tím, že blokuje škodlivé příchozí pakety a detekuje podezřelé odchozí pakety.

**POZNÁMKA:** Tato funkce se aktivuje automaticky při spuštění **Router Weakness Scan (Hledat slabé stránky směrovače).**

**Pokyny pro aktivaci obousměrné IPS:**

1. Na navigačním panelu přejděte na **General (Obecné) > AiProtection.**
2. Na hlavní stránce **AiProtection** klepněte na **Network Protection (Ochrana sítě).**
3. V podokně **Two-Way IPS (Obousměrné IPS)** klepněte na **ON (ZAPNUTO).**

### Prevence a blokování infikovaných zařízení

Tato funkce brání infikovaným zařízením v předávání osobních údajů nebo informací o infikování vnějším stranám.

**POZNÁMKA:** Tato funkce se aktivuje automaticky při spuštění **Router Weakness Scan (Hledat slabé stránky směrovače).**

**Pokyny pro aktivaci ochrany zabezpečení:**

1. Na navigačním panelu přejděte na **General (Obecné) > AiProtection.**
2. Na hlavní stránce **AiProtection** klepněte na **Network Protection (Ochrana sítě).**
3. V podokně **Infected Device Prevention and Blocking (Prevence a blokování infikovaných zařízení)** klepněte na **ON (ZAPNUTO).**

**Pokyny pro konfiguraci Alert Preference (Preference upozornění):**

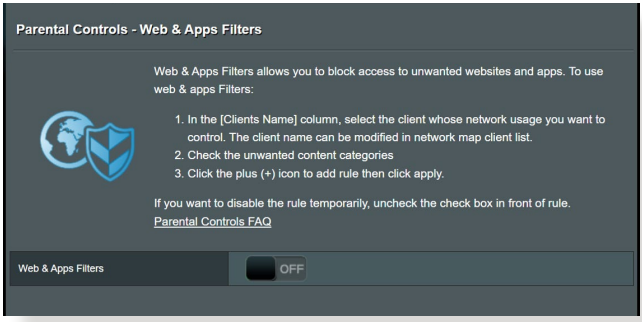
1. V podokně **Infected Device Prevention and Blocking (Prevence a blokování infikovaných zařízení)** klepněte na **Alert Preference (Preference upozornění).**
2. Vyberte nebo zadejte poskytovatele e-mailu, e-mailový účet a heslo a potom klepněte na **Apply (Použít).**

### 3.4.2 Nastavení rodičovské kontroly

Rodičovská kontrola umožňuje řídit čas přístupu k Internetu nebo nastavit časový limit používání sítě klientem.

Pokyny pro přechod na hlavní stránku rodičovské kontroly:

Na navigačním panelu přejděte na **General (Obecné) > Parental Controls (Rodičovská kontrola).**



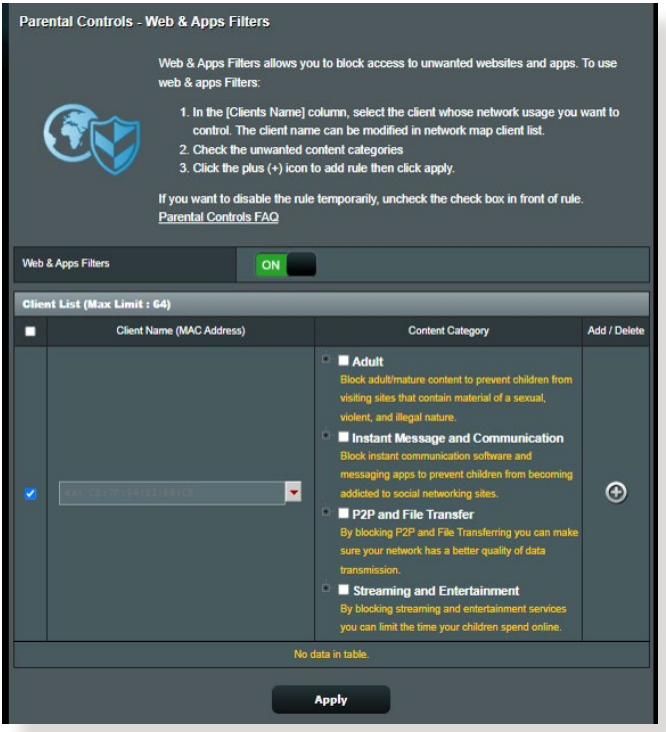

#### Filtrace webů a aplikací

Filtrace webů a aplikací je funkce nástroje P**arental Controls (Rodičovská kontrola)**, která umožňuje blokovat přístup k nežádoucím webům a aplikacím.

**Pokyny pro konfiguraci filtrace webů a aplikací:**

1. Na navigačním panelu přejděte na **General (Obecné) > Parental Controls (Rodičovská kontrola).**
2. V podokně **Web & Apps Filters (Filtraci webů a aplikací)** klepněte na **ON (ZAPNUTO).**
3. Když se zobrazí zpráva s výzvou k potvrzení podmínek licenčního ujednání s koncovým uživatelem (EULA), klepněte na **I agree (Souhlasím).**
4. Ve sloupci **Client List (Seznam klientů)** vyberte nebo zadejte název klienta z rozevíracího seznamu.
5. Ve sloupci **Content Category (Kategorie obsahu)** vyberte filtry ze čtyř hlavních kategorií: **Adult (Dospělý), Instant Message and Communication (Rychlá zpráva a komunikace), P2P and File Transfer (P2P a přenos souborů)** a **Streaming and Entertainment (Streaming a zábava).**

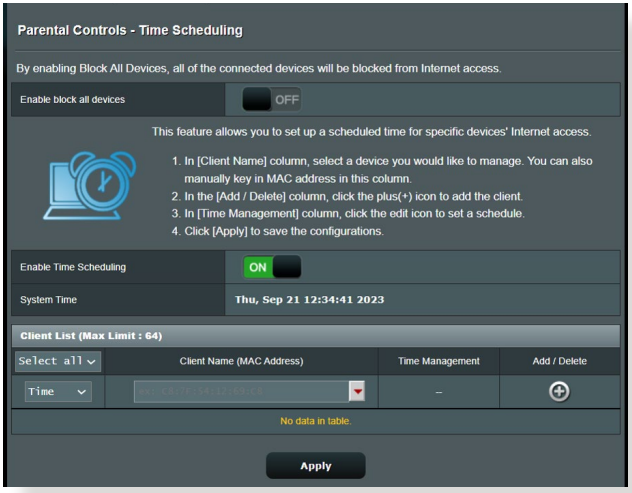
6. Klepnutím na přidejte profil klienta.
7. Klepnutím na **Apply (Použít)** uložte nastavení.



## Časové plánování

Časové plánování umožňuje nastavit časový limit používání sítě klientem.

**POZNÁMKA:** Zajistěte, aby byl čas vašeho systému synchronizován se serverem NTP**.**




### Pokyny pro konfigurování časového plánování:

1. Na navigačním panelu přejděte na **General (Obecné) > Parental Controls (Rodičovská kontrola) > Time Scheduling (Časové plánování).**
2. V podokně **Enable Time Scheduling (Aktivovat časové plánování)** klepněte na **ON (ZAPNUTO).**
3. Ve sloupci **Clients Name (Název klienta)** vyberte nebo zadejte název klienta z rozevíracího seznamu.

   **POZNÁMKA:** Rovněž můžete zadat adresu MAC klienta do sloupce **Client MAC Address (Adresa MAC klienta)**. Název klienta nesmí obsahovat žádné zvláštní znaky nebo mezery, které by mohly způsobit abnormální chování směrovače.

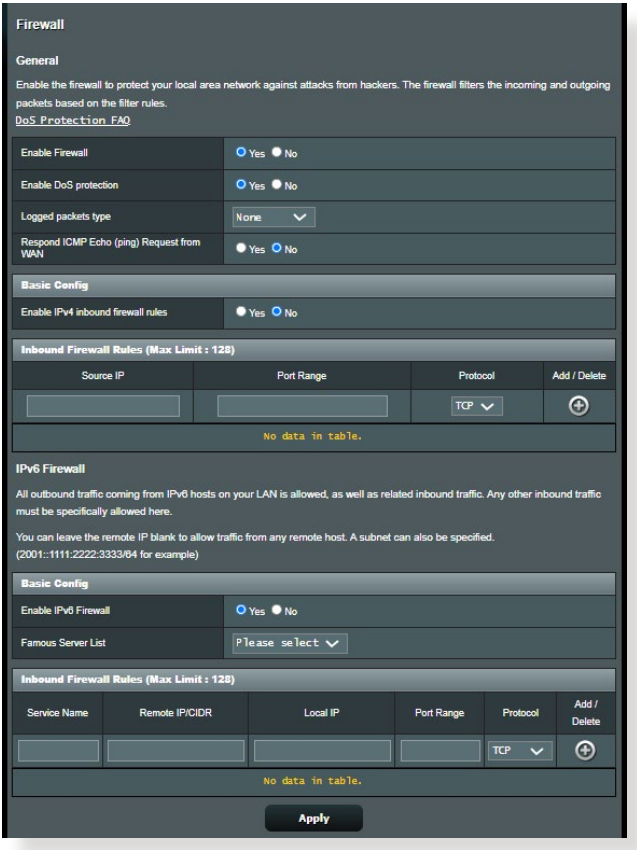
4. Klepnutím na ⊕ přidejte profil klienta.
5. Klepnutím na **Apply (Použít)** uložte nastavení.

## 3.5 Brána firewall

Tento bezdrátový směrovač může fungovat jako hardwarová brána firewall pro vaši síť.

**POZNÁMKA**: Funkce brány firewall je ve výchozí konfiguraci aktivována.

### 3.5.1 General (Obecné)




**Pokyny pro základní nastavení brány firewall:**

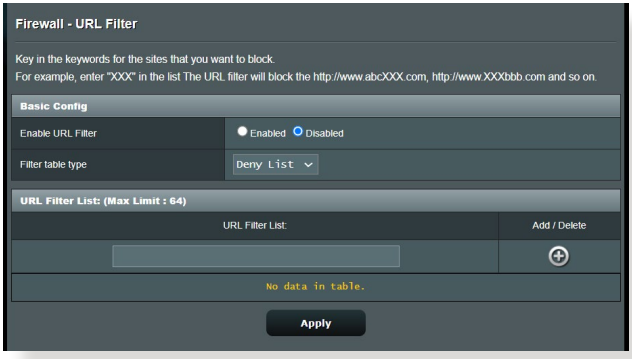
1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Firewall (Brána firewall)** > **General (Obecné)**.
2. V poli **Enable Firewall (Aktivovat bránu firewall)** vyberte **Yes (Ano)**.

3. V části **Enable DoS protection (Aktivovat ochranu DoS)** výběrem možnosti **Yes (Ano)** nastavíte ochranu sítě před útoky DoS (Denial of Service); nicméně to může omezit výkon směrovače.
4. Můžete rovněž sledovat pakety vyměněné mezi připojením LAN a WAN. V části Logged packets type (Typ sledovaných paketů) vyberte **Dropped (Zahozené)**, **Accepted (Přijaté)** nebo **Both (Oboje)**.
5. Klepněte na **Apply (Použít)**.

### 3.5.2 URL Filter (Filtr URL)

Můžete nastavit klíčová slova nebo webové adresy pro zabránění přístupu ke konkrétním adresám URL.

**POZNÁMKA**: Filtr URL vychází z dotazu DNS. Pokud síťový klient již navštívil webový server, jako například http://www.abcxxx.com, potom tento webový server nebude blokován (mezipaměť DNS v systému uchovává dříve navštívené webové servery). Chcete-li tento problém odstranit, před nastavením filtru URL vymažte mezipaměť DNS.

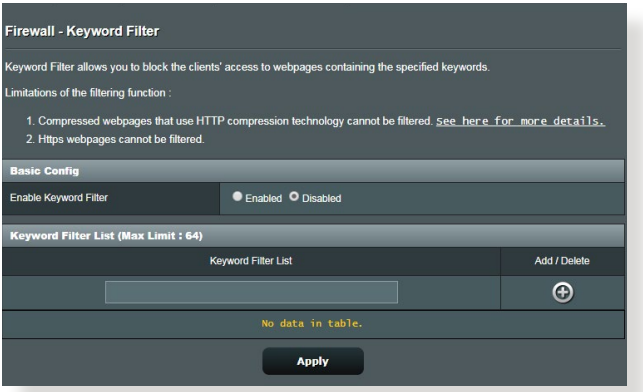



**Pokyny pro nastavení filtru URL:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Firewall (Brána firewall)** > **URL Filter (Filtr URL)**.
2. V poli Enable URL Filter (Povolit filtr URL) vyberte možnost **Enabled (Povoleno)**.
3. Zadejte adresu URL a klepněte na tlačítko .
4. Klepněte na **Apply (Použít)**.

### 3.5.3 Keyword filter (Filtr klíčových slov)

Filtr klíčových slov blokuje přístup k webovým stránkám, které obsahují určená klíčová slova.




**Pokyny pro nastavení filtru klíčových slov:**

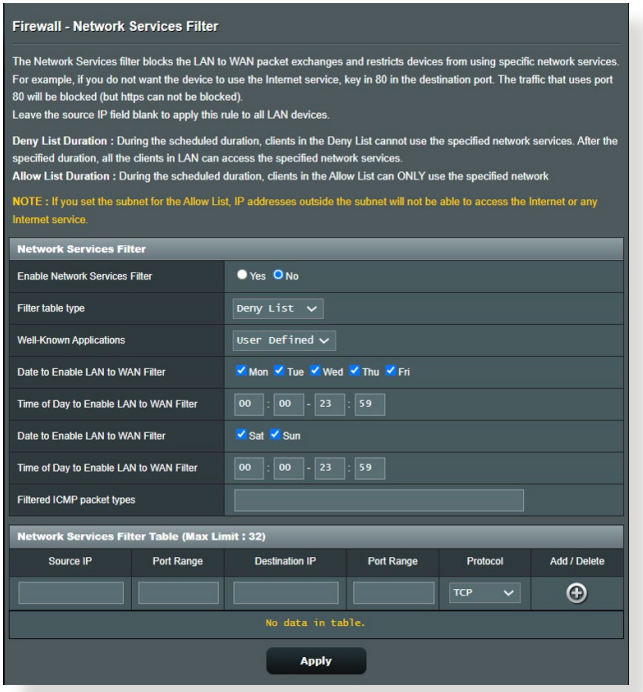
1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Firewall (Brána firewall)** > **Keyword Filter (Filtr klíčových slov)**.
2. V poli Enable Keyword Filter (Povolit filtr klíčových slov) vyberte možnost **Enabled (Povoleno)**.
3. Zadejte slovo nebo frázi a klepněte na tlačítko **Add (Přidat)**.
4. Klepněte na **Apply (Použít)**.

**POZNÁMKY:**

- Filtr klíčových slov vychází z dotazu DNS. Pokud síťový klient již navštívil webový server, jako například http://www.abcxxx.com, potom tento webový server nebude blokován (mezipaměť DNS v systému uchovává dříve navštívené webové servery). Chcete-li tento problém odstranit, před nastavením filtru klíčových slov vymažte mezipaměť DNS.
- Webové stránky s kompresí HTTP nelze filtrovat. Stránky HTTPS rovněž nelze blokovat pomocí filtru klíčových slov.

## 3.5.4 Filtr síťových služeb

Filtr síťových služeb blokuje výměnu paketů ze sítě LAN do sítě WAN a omezuje síťovým klientům přístup ke specifickým webovým službám, například Telnet nebo FTP.

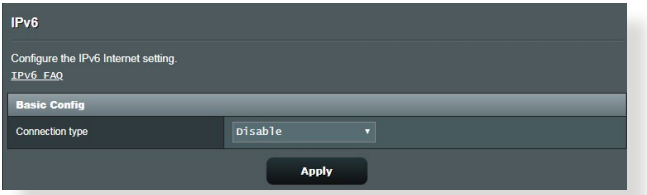



**Pokyny pro nastavení filtru síťových služeb:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Firewall (Brána firewall)** > **Network Service Filter (Filtr síťových služeb)**.
2. V poli Enable Network Services Filter (Povolit filtr síťových služeb) vyberte možnost **Yes (Ano)**.
3. Vyberte typ tabulky filtrování. **Deny (Se respinge)** blokuje specifikované síťové služby. **Allow (Se permite)** omezuje přístup pouze na specifikované síťové služby.
4. Určete den a čas aktivace filtrů.
5. Chcete-li specifikovat síťovou službu pro filtrování, zadejte údaje Source IP (Zdrojová adresa IP), Destination IP (Cílová adresa IP), Port Range (Rozsah portů) a Protocol (Protokol). Klepněte na tlačítko .
6. Klepněte na **Apply (Použít)**.

## 3.6 IPv6

Tento bezdrátový směrovač podporuje adresování IPv6, systém, který podporuje více adres IP. Tento standard dosud není velmi rozšířen. Zeptejte se vašeho ISP, zda jeho internetové služby podporují IPv6.




**Pokyny pro nastavení IPv6:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **IPv6**.
2. Vyberte příslušnou možnost **Connection type (Typ připojení)**. Možnosti konfigurace se liší v závislosti na vybraném typu připojení.
3. Zadejte nastavení IPv6 LAN a DNS.
4. Klepněte na **Apply (Použít)**.

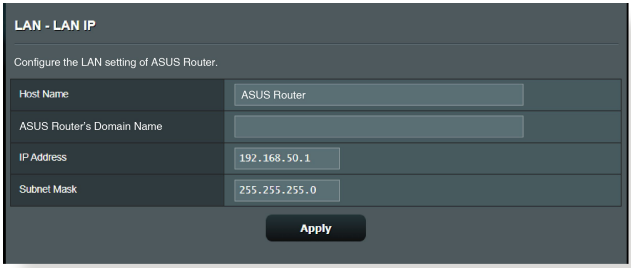
**POZNÁMKA:** Specifické informace IPv6 pro vaše internetové služby vám poskytne váš ISP.

# 3.7 LAN

## 3.7.1 LAN IP

Na obrazovce LAN IP lze upravit nastavení LAN IP bezdrátového směrovače.

**POZNÁMKA:** Jakékoli změny adresy LAN IP se projeví v nastavení DHCP.

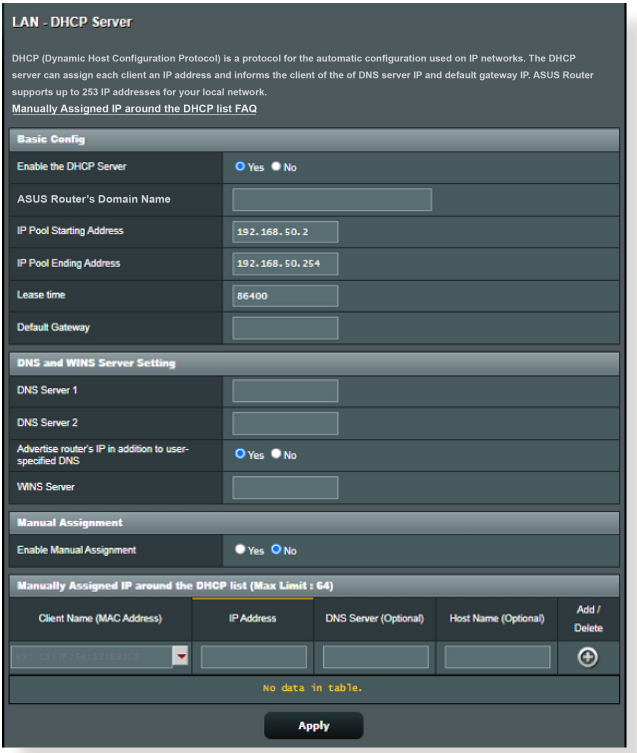



**Pokyny pro úpravy nastavení LAN IP:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **LAN** > **LAN IP**.
2. Upravte položky **IP address (Adresa IP)** a **Subnet Mask (Maska podsítě)**.
3. Po dokončení klepněte na tlačítko **Apply (Použít)**.

## 3.7.2 Server DHCP

Tento bezdrátový směrovač využívá server DHCP k automatickému přiřazování adres IP ve vaší síti. Můžete určit rozsah adres IP a dobu zapůjčení pro klienty ve vaší síti.




**Pokyny pro konfiguraci serveru DHCP:**

1. Na navigačním panelu, přejděte na **Advanced Settings (Upřesnit nastavení)** > **LAN** > **DHCP Server (Server DHCP)**.
2. V poli **Enable the DHCP Server (Povolit server DHCP)** zaškrtněte možnost **Yes (Ano)**.

3. Do textového pole **Domain Name (Název domény)** zadejte název domény bezdrátového směrovače.
4. Do pole **IP Pool Starting Address (Počáteční adresa fondu IP)** zadejte počáteční adresu IP.
5. Do pole **IP Pool Ending Address (Koncová adresa fondu IP)** zadejte koncovou adresu IP.
6. Do pole **Lease Time (Doba zapůjčení)** zadejte čas, kdy vyprší platnost adres IP a bezdrátový směrovač automaticky přiřadí nové adresy IP síťovým klientům.

**POZNÁMKY:**

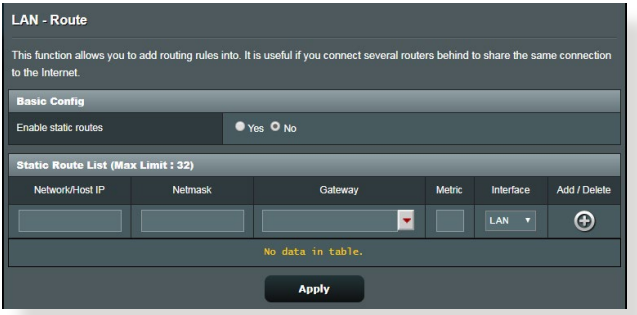
- Doporučujeme při určování rozsahu adres IP používat formát adresy IP 192.168.50.xxx (kde xxx může být libovolné číslo mezi 2 a 254).
- Počáteční adresa fondu IP nesmí být větší, než koncová adresa fondu IP.

7. Podle potřeby v části **DNS and WINS Server Settings (Nastavení DNS a WINS serveru)** zadejte adresu IP serveru DNS a serveru WINS.
8. Tento bezdrátový směrovač rovněž umožňuje ručně přiřazovat adresy IP zařízením v síti. V poli **Enable Manual Assignment (Povolit ruční přidělování)** vyberte možnost **Yes (Ano)** a přiřaďte adresu IP konkrétním adresám MAC v síti. Do seznam DHCP lze přidat až 32 adres MAC pro ruční přirazování.

### 3.7.3 Route (Trasa)

Pokud vaše síť využívá více bezdrátových směrovačů, můžete nakonfigurovat tabulku směrování pro sdílení stejné internetové služby.

**POZNÁMKA**: Bez důkladné znalosti tabulek směrování nedoporučujeme měnit výchozí nastavení směrování.

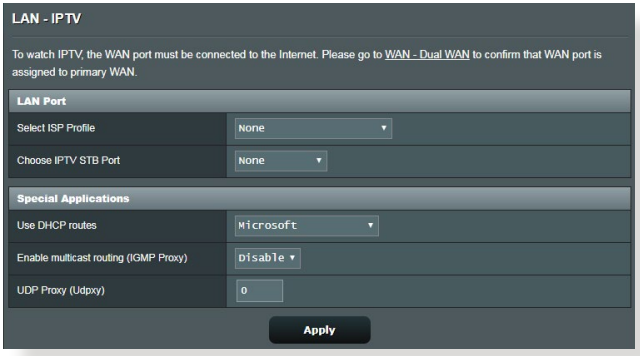



**Pokyny pro konfigurování tabulky směrování LAN:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **LAN** > **Route (Trasa)**.
2. V poli **Enable static routes (Povolit statické trasy)** vyberte možnost **Yes (Ano)**.
3. V části **Static Route List (Seznam statických tras)** zadejte síťové informace dalších přístupových bodů nebo uzlů. Klepnutím na tlačítko **Add (Přidat)** nebo **Delete (Odstranit)** přidejte nebo odstraňte zařízení ze seznamu.
4. Klepněte na **Apply (Použít)**.

## 3.7.4 IPTV

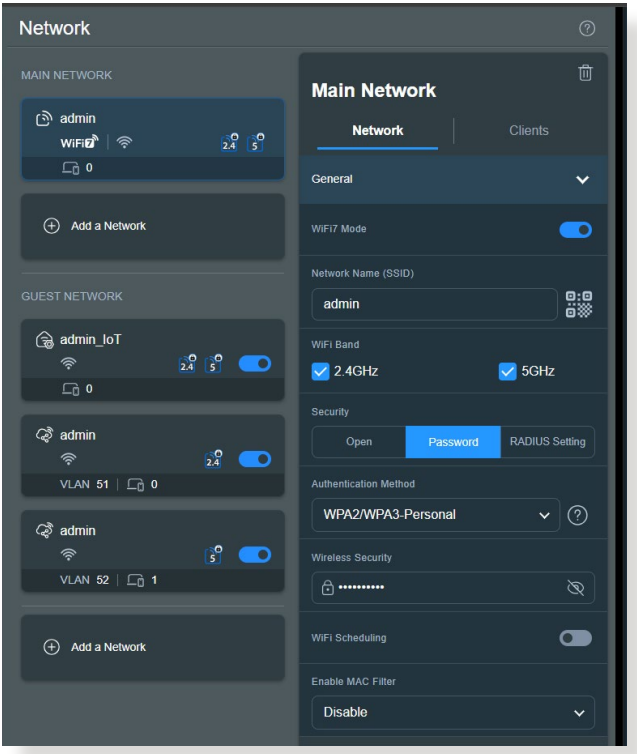
Tento bezdrátový směrovač podporuje připojení ke službám IPTV prostřednictvím ISP nebo místní sítě LAN. Na kartě IPTV jsou k dispozici konfigurační nastavení nezbytná pro nastavení IPTV, VoIP, vícesměrového vysílání a UDP pro vaši službu. Konkrétní údaje pro danou službu vám poskytne váš ISP.



# 3.8 Síť

## 3.8.1 Hlavní síť - Filtr MAC

Bezdrátový filtr MAC umožňuje kontrolovat pakety přenášené na určenou adresu MAC (Media Access Control) ve vaší bezdrátové síti.



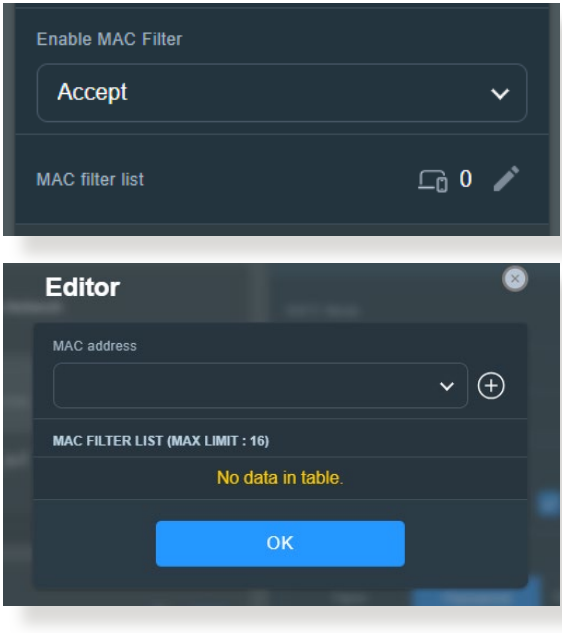

**Pokyny pro konfigurování bezdrátového filtru MAC:**

1. Na navigačním panelu přejděte na **General (Obecné) > Network (Síť) > Main Network (Hlavní síť)** a vyberte síťový název (SSID) hlavní sítě.
2. V rozevíracím seznamu **Enable Mac Filter (Povolit filtr Mac)** vyberte možnost **Accept (Přijmout)** nebo **Reject (Odmítnout)**.
   - Výběrem možnosti **Accept (Přijmout)** povolíte zařízením v seznamu filtru MAC přístup k bezdrátové síti.

- Výběrem možnosti **Reject (Odmítnout)** zabráníte zařízením v seznamu filtru MAC v přístupu k bezdrátové síti.

**POZNÁMKA:** Vyberte možnost **Disable (Zakázat)**, pokud chcete funkci **Enable MAC Filter (Povolit filtr MAC)** vypnout.

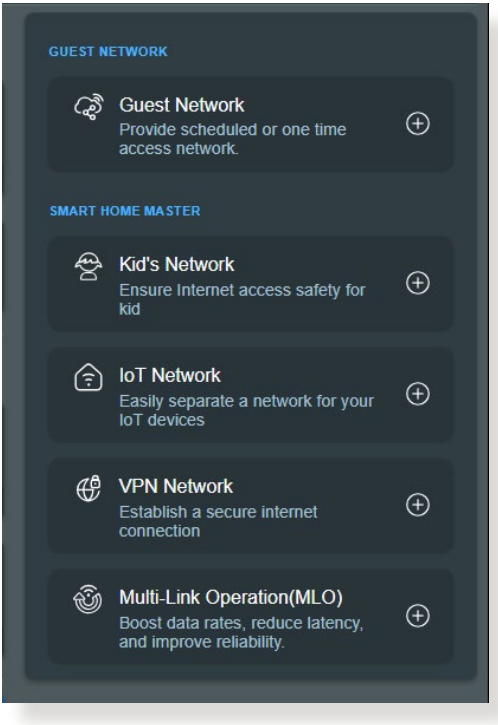
4. V seznamu filtru MAC klepněte na otevřete stránku **Editor** a poté klikněte na a zadejte MAC adresu bezdrátového zařízení.
5. Klepněte na **OK**.



## 3.8.2 Hostované sítě

### 3.8.2.1 Hostované sítě

Funkce Guest Network (Hostovaná síť) poskytuje dočasným návštěvníkům připojení k Internetu prostřednictvím přístupu k samostatným SSID nebo sítím bez přístupu k vaší privátní síti.

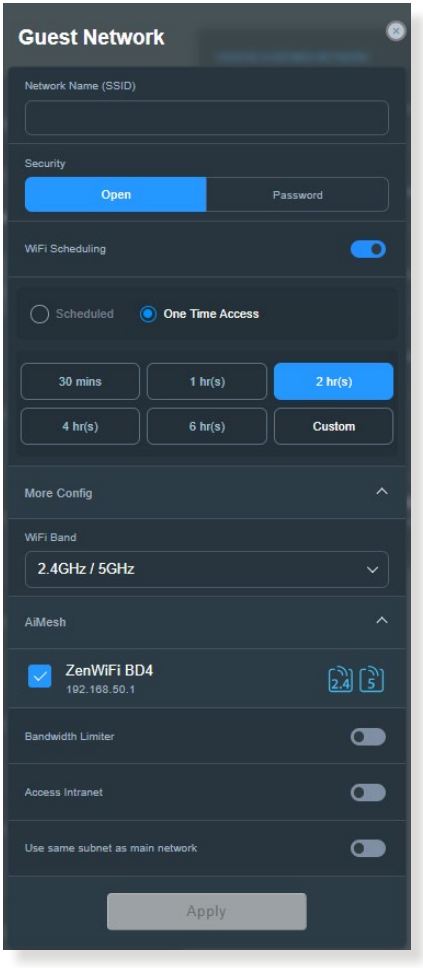



**POZNÁMKA:** ZenWiFi BD4 podporuje až tři SSID v síti pro hosty.

**Pokyny pro vytvoření hostované sítě:**

1. Na navigačním panelu přejděte na **General (Obecné)** > **Network (Síť) > Guest Network (Hostovaná síť)** > **Add a Network (Přidejte síť)**.
2. Vyberte možnost **Guest Network (Hostovaná síť)** a v poli **Network Name (Název sítě) (SSID)** přiřaďte název sítě pro dočasnou síť.
3. Vyberte metodu ověřování v části **Security (Zabezpečení)**.
4. Zadejte čas přístupu nebo zvolte možnost **Scheduled (Naplánováno)** a přidejte profil online plánu.

5. Vyberte **WiFi Band (Pásmo WiFi)** pro hostovanou síť, kterou chcete vytvořit.
6. Povolte nebo zakažte **Bandwidth Limiter (Omezovač šířky pásma)**.
7. Povolte nebo zakažte **Access Intranet (Přístup k intranetu)**.
8. Po dokončení klepněte na tlačítko **Apply (Použít)**.

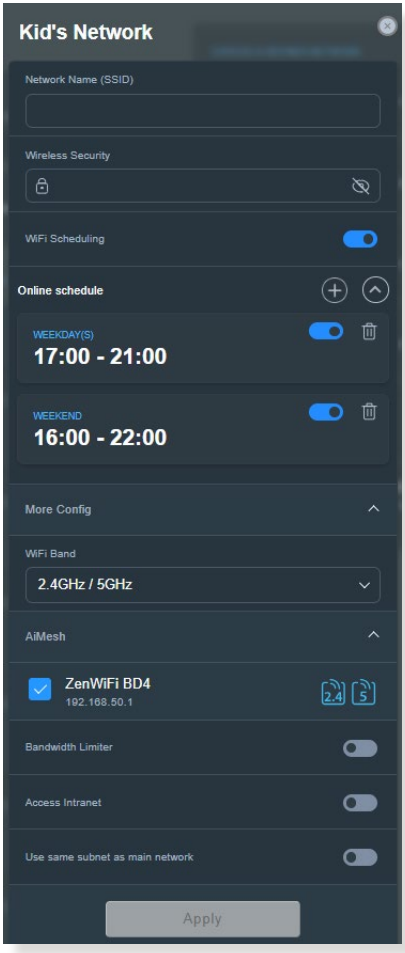


### 3.8.2.2 Smart Home Master

Smart Home Master je výkonný a uživatelsky přívětivý nástroj pro segmentaci sítě. Zjednodušuje proces vytváření a správy pokročilých schémat podsítí, jako je vytvoření vyhrazeného SSID pro zařízení vašich dětí, připojení k VPN prostřednictvím vyhrazené podsítě nebo dokonce vytvoření jednoho zabezpečeného SSID pro všechna vaše zařízení IoT.

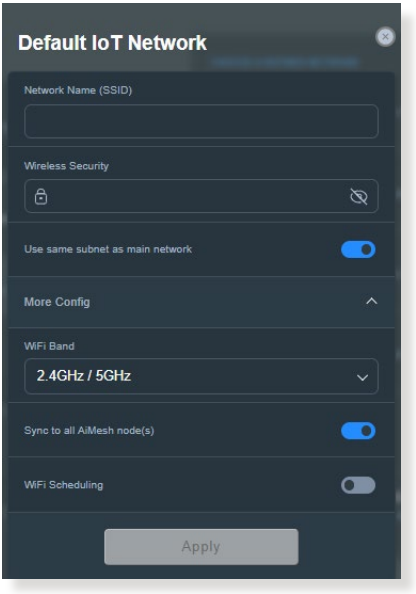
**Pokyny pro vytvoření Dětská síť:**

1. Na navigačním panelu přejděte na **General (Obecné)** > **Network (Síť) > Guest Network (Hostovaná síť)** > **Add a Network (Přidejte síť)**.
2. Vyberte možnost **Kid's Network (Dětská síť)** a přiřaďte název sítě a bezpečnostní klíč v polích **Network Name (Název sítě) (SSID)** a Zabezpečení bezdrátové sítě.
3. Přizpůsobte čas přístupu k Internetu v poli **Online schedule (Online plán)**.
4. Vyberte **WiFi Band (Pásmo WiFi)** pro dětská síť, kterou chcete vytvořit.
5. Povolte nebo zakažte **Bandwidth Limiter (Omezovač šířky pásma)**.
6. Povolte nebo zakažte **Access Intranet (Přístup k intranetu)**.
7. Po dokončení klepněte na tlačítko **Apply (Použít)**.



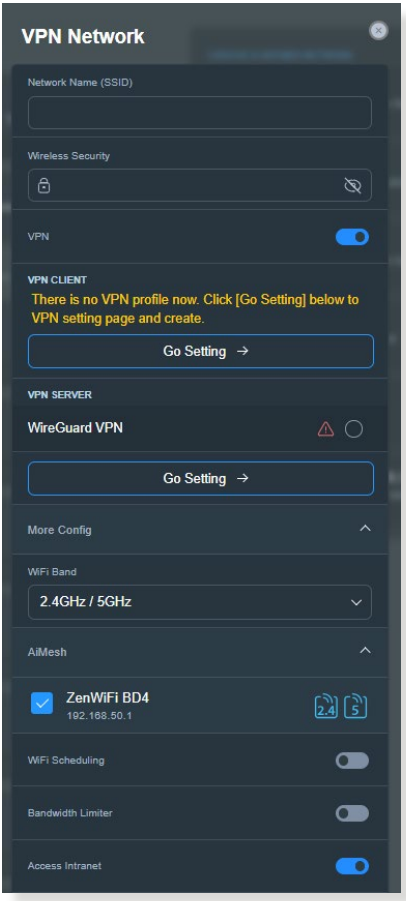

**Pokyny pro vytvoření sítě IoT:**

1. Na navigačním panelu přejděte na **General (Obecné)** > **Network (Síť) > Guest Network (Hostovaná síť)** > **Add a Network (Přidejte síť)**.
2. Vyberte možnost **IoT Network (Sítě IoT)** a přiřaďte název sítě a bezpečnostní klíč v polích **Network Name (Název sítě) (SSID)** a Zabezpečení bezdrátové sítě.
3. Vyberte **WiFi Band (Pásmo WiFi)** pro sítě IoT, kterou chcete vytvořit.
4. Přizpůsobte si dobu přístupu k internetu povolením **WiFi Scheduling (Plánování WiFi)**.
5. Po dokončení klepněte na tlačítko **Apply (Použít)**.




**Pokyny pro vytvoření sítě VPN:**

1. Na navigačním panelu přejděte na **General (Obecné)** > **Network (Síť) > Guest Network (Hostovaná síť)** > **Add a Network (Přidejte síť)**.
2. Vyberte možnost **VPN Network (Sítě VPN)** a přiřaďte název sítě a bezpečnostní klíč v polích **Network Name (Název sítě) (SSID)** a **Wireless Security (Zabezpečení bezdrátové)** sítě.
3. Pokud jste nenastavili profil VPN pro server VPN nebo klienta VPN, klikněte na možnost **Go Setting (Přejít na nastavení)** a vytvořte profil VPN.
4. Vyberte **WiFi Band (Pásmo WiFi)** pro sítě VPN, kterou chcete vytvořit.
5. Přizpůsobte si dobu přístupu k internetu povolením **WiFi Scheduling (Plánování WiFi)**.
6. Povolte nebo zakažte **Bandwidth Limiter (Omezovač šířky pásma)**.
7. Povolte nebo zakažte **Access Intranet (Přístup k intranetu)**.
8. Po dokončení klepněte na tlačítko **Apply (Použít)**.


VPN Network
Network Name (SSID)
Wireless Security
VPN
VPN CLIENT
There is no VPN profile now. Click [Go Setting] below to VPN setting page and create.
Go Setting →
VPN SERVER
WireGuard VPN
Go Setting →
More Config
WiFi Band
2.4GHz / 5GHz
AiMesh
ZenWiFi BD4
192.168.50.1
WiFi Scheduling
Bandwidth Limiter
Access Intranet

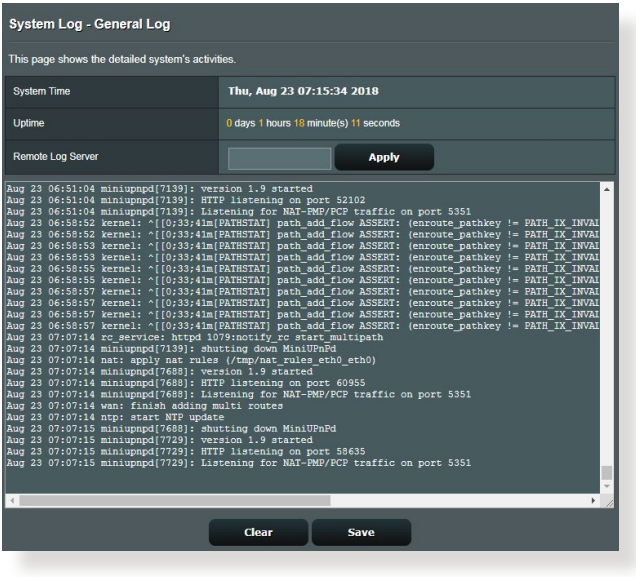
## 3.9 Systémový protokol

Systémový protokol obsahuje záznam vašich síťových aktivit.

**POZNÁMKA:** Při restartování nebo vypnutí směrovače se systémový protokol resetuje.

### Pokyny pro zobrazení systémového protokolu:

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **System Log (Systémový protokol)**.
2. Můžete zobrazit vaše síťové aktivity na následujících kartách:
   - Obecný protokol
   - Protokol bezdrátového připojení
   - Zápůjčky DHCP
   - IPv6
   - Tabulka směrování
   - Předávání portů
   - Připojení



## 3.10 Traffic Analyzer (Analizor de trafic)

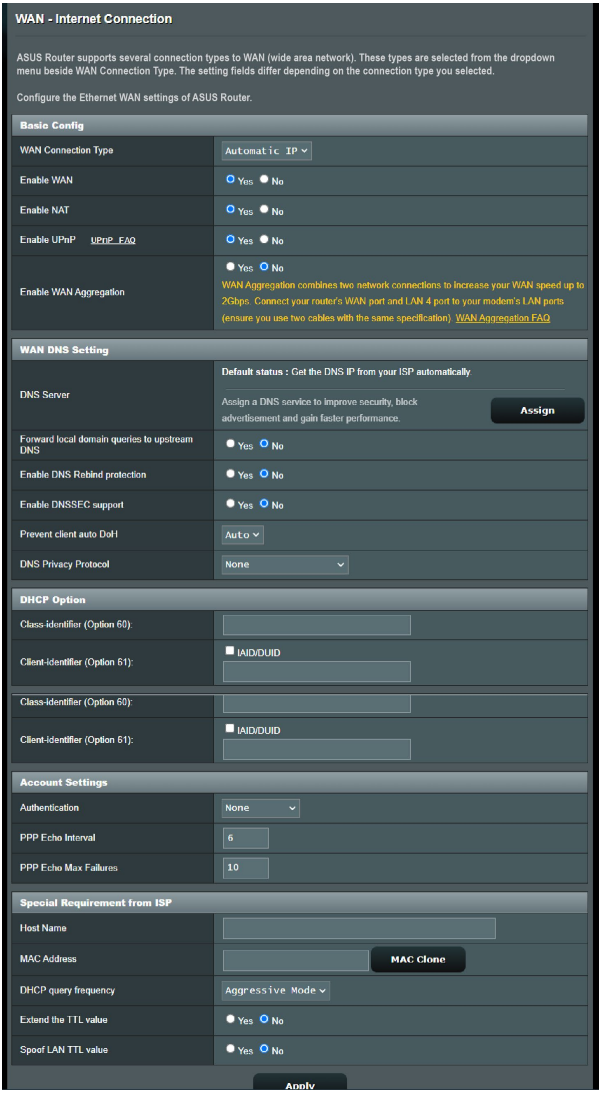
Funkce sledování provozu umožňuje vyhodnocovat využití šířky pásma a rychlost připojení k Internetu, drátových nebo bezdrátových sítí. Umožňuje každodenní sledování síťového provozu v reálném čase. Rovněž umožňuje zobrazit síťový provoz za posledních 24 hodin.


**POZNÁMKA:** Pakety z Internetu jsou rovnoměrně přenášeny do zařízení s pevným a bezdrátovým připojením.

# 3.11 WAN

## 3.11.1 Internetové připojení

Na obrazovce Internetové připojení lze konfigurovat nastavení různých typů připojení WAN.



**Pokyny pro konfigurování nastavení připojení WAN:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **Internet Connection (Internetové připojení)**.

2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **WAN Connection Type (Typ připojení WAN):** Vyberte typ poskytovatele internetových služeb. K dispozici jsou možnosti **Automatic IP (Automatická adresa IP)**, **PPPoE**, **PPTP**, **L2TP** nebo **fixed IP (Pevná adresa IP)**. Pokud směrovač nemůže získat platnou adresu IP nebo pokud neznáte typ připojení WAN, požádejte o pomoc vašeho ISP.
   - **Enable WAN (Povolit WAN)**: Výběrem možnosti **Yes (Ano)** aktivujte přístup směrovače k Internetu. Výběrem možnosti **No (Ne)** zakážete přístup k Internetu.
   - **Enable NAT (Povolit NAT)**: V systému NAT (Network Address Translation) se používá jedna veřejná adresa IP (WAN IP) k poskytování přístupu k Internetu síťovým klientům s privátní adresou IP v místní síti LAN. Privátní adresa IP každého síťového klienta je uložena do tabulky NAT a je použita ke směrování příchozích datových paketů.
   - **Enable UPnP (Povolit UPnP)**: Technologie UPnP (Universal Plug and Play) umožňuje ovládat více zařízení (směrovače, televizory, stereofonní systémy, herní konzole, mobilní telefony) prostřednictvím sítě na bázi IP s nebo bez centrálního ovládání prostřednictvím brány. Technologie UPnP umožňuje připojit počítače všech formátů a poskytuje hladký přístup k síti pro vzdálenou konfiguraci a přenos dat. S technologií UPnP je nové síťové zařízení vyhledáno automaticky. Po připojení k síti lze zařízení vzdáleně konfigurovat pro podporu P2P aplikací, interaktivních her, videokonferencí a webových nebo proxy serverů. Na rozdíl od předávání portů, které vyžaduje ruční konfiguraci nastavení portů, technologie UPnP automaticky konfiguruje směrovač tak, aby akceptoval příchozí připojení a směroval požadavky na konkrétní počítače v místní síti.

- **Enable WAN Aggregation (Povolit agregaci WAN):** Agregace WAN kombinuje dvě připojení k síti, čímž zvyšuje rychlost WAN až na 2 Gb/s. Připojte port WAN a port LAN 4 směrovače k portům LAN modemu.
- **Connect to DNS Server (Připojit k serveru DNS)**: Umožňuje tomuto serveru automaticky získávat adresu IP DNS od ISP. DNS je hostitel v Internetu, který překládá internetové názvy na číselné adresy IP.
- **Authentication (Ověřování)**: Někteří ISP mohou tuto položku specifikovat. Informujte se u vašeho ISP a případně zadejte.
- **Host Name (Název hostitele)**: Do tohoto pole můžete zadat název hostitele vašeho směrovače. Obvykle se jedná o zvláštní požadavek ISP. Pokud váš ISP přiřadil vašemu počítači název hostitele, zadejte jej zde.
- **MAC Address (Adresa MAC)**: Adresa MAC (Media Access Control) je jednoznačný identifikátor síťového zařízení. Někteří ISP sledují adresy MAC síťových zařízení, která se připojují k jejich službám, a odmítají každé nerozpoznané zařízení, které se pokusí připojit. Chcete-li zabránit problémy s připojením z důvodu nezaregistrované adresy MAC, použijte jednu z následujících možností:
  - Kontaktujte vašeho ISP a požádejte jej o registraci adresy MAC k využívané službě ISP.
  - Naklonujte nebo změňte adresu MAC bezdrátového směrovače ASUS tak, aby se shodovala s adresou MAC předchozího síťového zařízení, která byla poskytovatelem ISP registrována.

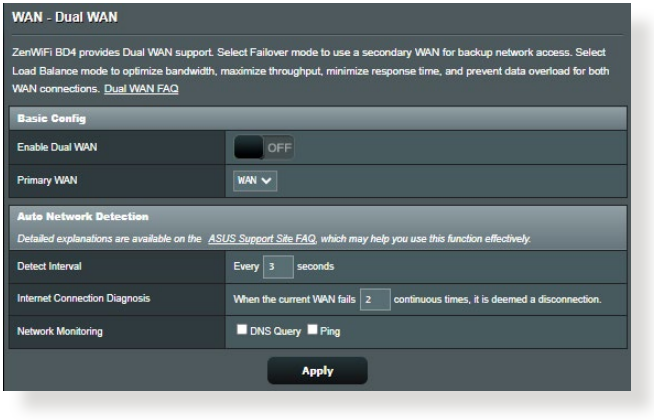
## 3.11.2 Dual WAN (Duální síť WAN)

Duální síť WAN umožňuje vybrat pro směrovač dvě připojení k internetu, primární WAN a sekundární WAN.

**Konfigurace duální sítě WAN:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení) > WAN.**
2. Přejděte k části **Dual WAN (Duální síť WAN)** a nastavte možnost **ON (Zapnuto)**.
3. Vyberte **Primary WAN (Primární WAN)** a **Secondary WAN (Sekundární WAN)**. K dispozici jsou dvě 2,5GbE WAN/LAN pro vaše možnosti.
4. Vyberte možnost **Fail Over (Záložní)** nebo **Load Balance (Vyrovnávání zatížení)**.
5. Klikněte na **Apply (Použít)**.

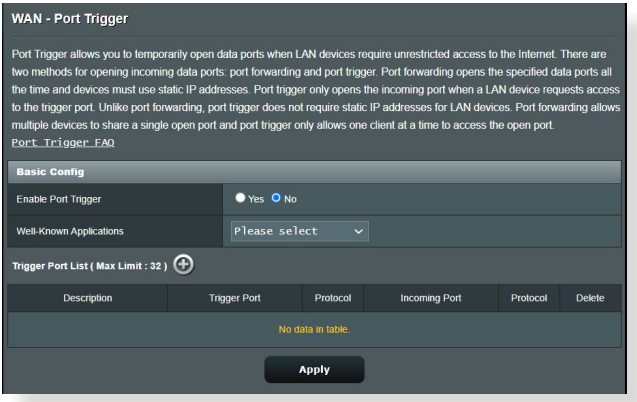
**POZNÁMKA:** Podrobná vysvětlení jsou k dispozici v části s častými otázkami na serveru odborné pomoci ASUS **https://www.asus.com/support/FAQ/1011719**.



### 3.11.3 Aktivace portů

Aktivace rozsahu portů otevírá na omezenou dobu předem určený příchozí port, kdykoli některý klient místní sítě provede odchozí připojení na některý určený port. Aktivace portů se používá v následujících situacích:

- Více místních klientů vyžaduje předávání portu pro stejnou aplikaci v různou dobu.
- Některá aplikace vyžaduje konkrétní příchozí porty, které se liší od odchozích portů.




**Pokyny pro nastavení aktivace portů:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **Port Trigger (Aktivace portů)**.
2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **Enable Port Trigger (Povolit aktivaci portů)**: Výběrem možnosti **Yes (Ano)** povolíte aktivaci portů.
   - **Well-Known Applications (Známé aplikace)**: Vyberte oblíbené hry a webové služby, které chcete přidat do seznamu aktivace portů.
   - **Description (Popis)**: Zadejte krátký název nebo popis služby.

- **Trigger Port (Aktivační port)**: Určete aktivační port pro otevření příchozího portu.
- **Protocol (Protokol)**: Vyberte protokol TCP nebo UDP.
- **Incoming Port (Příchozí port)**: Určete příchozí port pro příjem příchozích dat z Internetu.

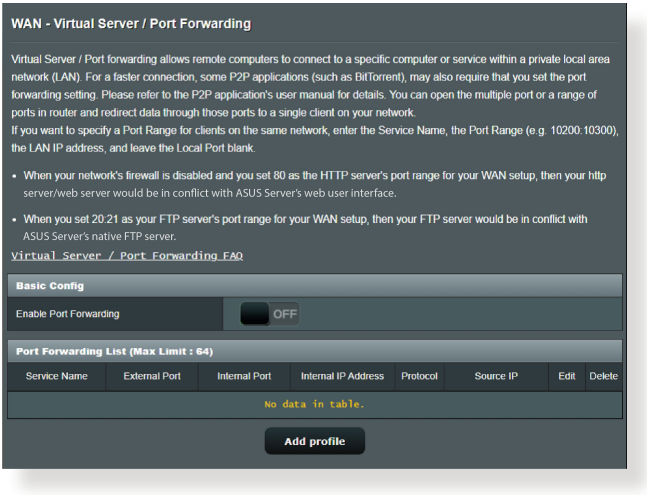
**POZNÁMKY:**

- Při připojování k serveru IRC provede klientský počítač odchozí připojení pomocí rozsahu aktivačních portů 66660 - 7000. Server IRC server odpoví ověřením uživatelského jména a vytvořením nového připojení ke klientskému počítači pomocí příchozího portu.
- Pokud je aktivace portů deaktivována, směrovač ukončí připojení, protože nemůže určit počítač, který požaduje o přístup k IRC. Když je aktivace portů aktivována, směrovač přiřadí příchozí port při přijetí příchozích dat. Tento příchozí port se po vypršení stanovené doby uzavře, protože si směrovač není jistý, kdy bude aplikace ukončena.
- Aktivace portů pouze umožňuje, aby jeden klient v síti používal konkrétní službu a specifický příchozí port současně.
- Nelze používat stejnou aplikaci pro aktivaci portu ve více počítačích současně. Směrovač předá port pro odeslání požadavku/aktivace směrovači zpět pouze poslednímu počítači.

## 3.11.4 Virtuální server/předávání portů

Předávání portů je způsob směrování síťového provozu z Internetu na konkrétní port a konkrétní rozsah portů jednoho nebo více zařízení v místní síti. Nastavením předávání portů ve směrovači umožňuje počítačům mimo síť přistupovat ke specifickým službám, které poskytuje některý počítač ve vaší síti.

**POZNÁMKA:** Když je aktivováno předávání portů, směrovač ASUS blokuje nevyžádaný příchozí provoz z Internetu a povoluje pouze odpovědi na odchozí požadavky z místní sítě LAN. Síťový klient nemá přímý přístup k Internetu a naopak.




### Pokyny pro nastavení předávání portů:

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **Virtual Server / Port Forwarding (Virtuální server / předávání portů)**.

2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **ON (ZAPNUTO)**.
   - **Enable Port Forwarding (Povolit předávání portů)**: Výběrem možnosti **ON (Zapnuto)** povolíte předávání portů.
   - **Famous Server List (Seznam slavných serverů)**: Určete typ služby, ke které chcete přistupovat.
   - **Famous Game List (Seznam slavných her)**: Zobrazí porty vyžadované pro správné fungování oblíbených online her.
   - **FTP Server Port (Port serveru FTP)**: Nepřiřazujte rozsah portů 20:21 vašemu serveru FTP, protože by došlo ke konfliktu s nativním přiřazením serveru FTP směrovače.
   - **Service Name (Název služby)**: Zadejte název služby.
   - **Port Range (Rozsah portů)**: Chcete-li určit rozsah portů pro klienty ve stejné síti, zadejte údaje Service Name (Název služby), Port Range (Rozsah portů) (například 10200:10300), LAN IP address (Adresa IP místní sítě LAN) a položku Local Port (Místní port) ponechte prázdnou. Rozsah portů akceptuje různé formáty, například Rozsah portů (300:350), individuální porty (566,789) nebo kombinaci (1015:1024,3021).

**POZNÁMKY:**

- Když je deaktivována síťová brána firewall a nastavíte 80 jako rozsah portů serveru HTTP pro nastavení WAN, dojde ke konfliktu vašeho serveru http/webového serveru s uživatelským webovým rozhraním směrovače.
- Síť využívá porty k výměně dat a každému portu je přiřazeno číslo a konkrétní úloha. Například port 80 se používá pro protokol HTTP. Konkrétní port může používat najednou pouze jedna aplikace nebo služba. Z tohoto důvodu nemohou dva počítače současně získat přístup k datům prostřednictvím stejného portu. Například nelze nastavit předávání portu 100 pro dva počítače současně.

- **Local IP (Místní adresa IP)**: Zadejte síťovou adresu IP klienta.

**POZNÁMKA**: Aby předávání portů fungovalo správně, použijte pro místního klienta statickou adresu IP. Další informace viz část **3.8 LAN**.

- **Local Port (Místní port)**: Zadejte konkrétní port pro příjem předávaných paketů. Toto pole ponechte prázdné, pokud chcete, aby byly příchozí pakety přesměrovávány na určený rozsah portů.
- **Protocol (Protokol)**: Vyberte protokol. Pokud si nejste jisti, vyberte možnost **BOTH (OBOJE)**.

**Pokyny pro kontrolu úspěšné konfigurace předávání portů:**

- Zkontrolujte, zda je nakonfigurován a spuštěn váš server nebo aplikace.
- Budete potřebovat klienta mimo vaši místní síť LAN, který má ovšem přístup k Internetu (též„internetový klient"). Tento klient nesmí být připojen ke směrovači ASUS.
- V internetovém klientovi zadejte adresu IP sítě WAN směrovače pro přístup k serveru. Pokud byl port úspěšně předán, mělo by být možné přistupovat k souborům nebo aplikacím.

**Rozdíly mezi aktivací portů a předáváním portů:**

- Předávání portů bude fungovat i bez nakonfigurování specifické adresy IP místní sítě LAN. Na rozdíl od předávání portů, které vyžaduje statickou adresu IP sítě LAN, umožňuje předávání portů předávat dynamické porty pomocí směrovače. Jsou nakonfigurovány předem stanovené rozsahy portů pro příjem příchozích připojení na omezenou dobu. Aktivace portů umožňuje více počítačům využívat aplikace, které by normálně vyžadovaly ruční předávání totožných portů na každý počítač v síti.
- Aktivace portů je bezpečnější, než předávání portů, protože příchozí porty nejsou otevřené po celou dobu. Jsou otevřeny pouze když aplikace navazuje odchozí připojení prostřednictvím aktivačního portu.

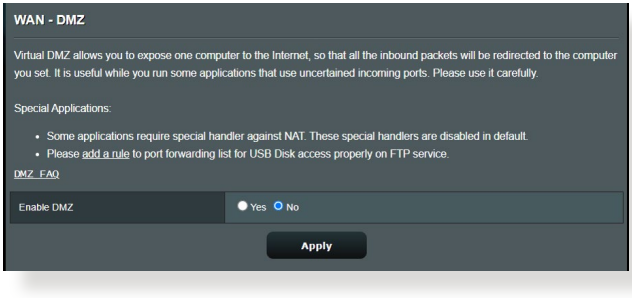
### 3.11.5 DMZ

Virtuální DMZ vystavuje jednoho klienta na Internetu a umožňuje, aby tento klient přijímal veškeré příchozí pakety směrované do vaší místní sítě LAN.

Příchozí provoz z Internetu je obvykle likvidován a směrován na konkrétního klienta pouze, pokud je v síti nakonfigurováno předávání nebo aktivace portů. V konfiguraci DMZ přijímá jeden síťový klient všechny příchozí pakety.

Nastavení DMZ v síti je vhodné, když potřebujete příchozí porty otevřené nebo chcete hostovat doménový, webový nebo e-mailový server.

**UPOZORNĚNÍ:** Otevřením všech portů klienta pro přístup z Internetu bude síť náchylná na útoky zvnějšku. Uvědomte si bezpečnostní rizika vyplývající z používání DMZ.




**Pokyny pro nastavení DMZ:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **DMZ**.
2. Nakonfigurujte následující nastavení. Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **IP address of Exposed Station (Adresa IP vystavené stanice):** Zadejte síťovou adresu IP klienta, který bude zajišťovat službu DMZ a bude vystaven v Internetu. Zajistěte, aby měl klient serveru statickou adresu IP.

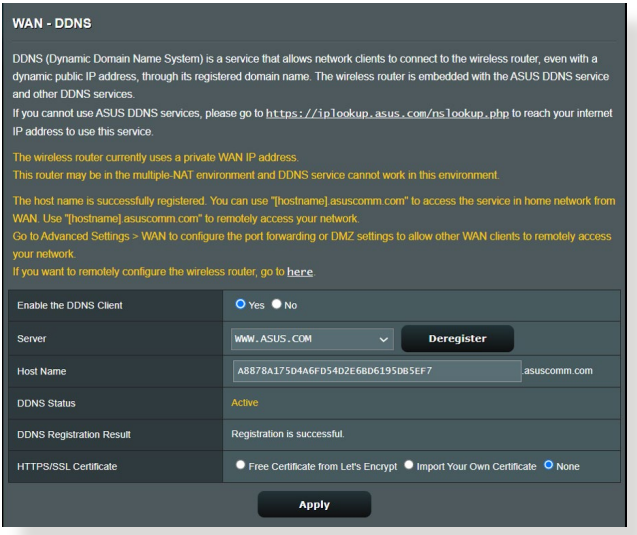
**Pokyny pro odebrání DMZ:**

1. Odstraňte síťovou adresu IP klienta z textového pole **IP Address of Exposed Station (Adresa IP vystavené stanice)**.

2. Po dokončení klepněte na tlačítko **Apply (Použít)**.

## 3.11.6 DDNS

Nastavení DDNS (Dynamic DNS) vyžaduje přístup ke směrovači z místa mimo síť prostřednictvím poskytované služby ASUS DDNS nebo jiné služby DDNS.




**Pokyny pro nastavení DDNS:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **DDNS**.
2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **Enable the DDNS Client (Povolit klienta DDNS)**: Povolte, aby mohl server DDNS přistupovat ke směrovači ASUS prostřednictvím názvu DNS, nikoli adresy IP sítě WAN.
   - **Server and Host Name (Název serveru a hostitele)**: Vyberte server ASUS DDNS nebo jiný server DDNS. Chcete-li používat server ASUS DDNS, zadejte název hostitele ve formátu xxx.asuscomm.com (xxx je váš název hostitele).

- Chcete-li používat jinou službu DDNS, klepněte na FREE TRIAL (BEZPLATNÉ VYZKOUŠENÍ) a nejdříve se zaregistrujte online. Vyplňte pole User Name or E-mail Address (Uživatelské jméno nebo e-mailová adresa) a Password or DDNS Key (Heslo nebo klíč DDNS).
- **Enable wildcard (Povolit zástupný znak)**: Povolte zástupný znak, pokud jej služba DDNS vyžaduje.

**POZNÁMKY**:

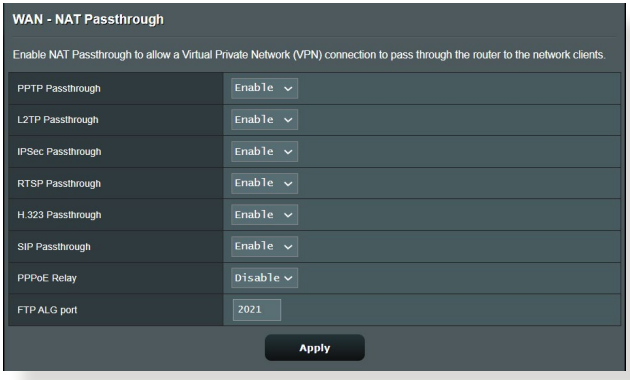
Za následujících podmínek služba DDNS nefunguje:

- Když bezdrátový směrovač používá privátní adresu IP sítě WAN (192.168.x.x, 10.x.x.x nebo 172.16.x.x), jak je uvedeno žlutým textem.
- Směrovač se pravděpodobně nachází v síti, která používá více tabulek NAT.

## 3.11.7 NAT Passthrough (Průchod NAT)

Funkce NAT Passthrough (Průchod NAT) umožňuje připojení VPN (Virtual Private Network) procházet směrovačem k síťovým klientům. Možnosti PPTP Passthrough (Průchod PPTP), L2TP Passthrough (Průchod L2TP), IPsec Passthrough (Průchod IPsec) a RTSP Passthrough (Průchod RTSP) jsou aktivovány ve výchozí konfiguraci.

Chcete-li aktivovat / deaktivovat nastavení NAT Passthrough (Průchod NAT), přejděte na **Advanced Settings (Upřesnit nastavení)** > **WAN** > **NAT Passthrough (Průchod NAT)**. Po dokončení klepněte na tlačítko **Apply (Použít)**.

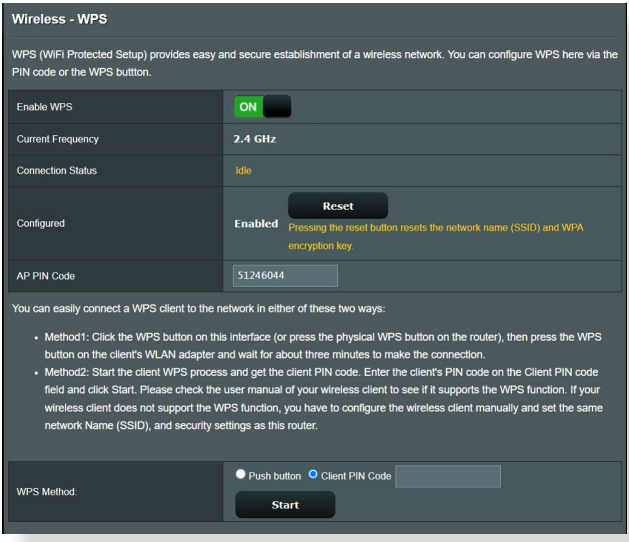


# 3.12 Bezdrátové připojení

## 3.12.1 WPS

WPS (Wi-Fi Protected Setup) je standard zabezpečení bezdrátového připojení, který umožňuje snadno připojovat zařízení k bezdrátové síti. Funkci WPS nakonfigurovat prostřednictvím kódu PIN nebo tlačítka WPS.

**POZNÁMKA**: Zkontrolujte, zda zařízení podporují standard WPS.




**Pokyny pro aktivaci standardu WPS v bezdrátové síti:**

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Wireless (Bezdrátové připojení)** > **WPS**.
2. V poli **Enable WPS (Aktivovat WPS)** přemístěte posuvník do polohy **ON (ZAP.)**.
3. Ve výchozí konfiguraci využívá standard WPS frekvenci 2,4 GHz. Chcete-li změnit frekvenci na 5 GHz, deaktivujte funkci WPS přemístěním posuvníku do polohy **OFF (VYP.)**, klepněte na položku **Switch Frequency (Změnit frekvenci)** v poli **Current Frequency (Aktuální frekvence)** a znovu přemístěte posuvník WPS do polohy **ON (ZAP.)**.

**POZNÁMKA:** Standard WPS podporuje ověřování prostřednictvím Open System (Otevřený systém), WPA-Personal (WPA-osobní) a WPA2-Personal (WPA2-podnikový). Standard WPS nepodporuje bezdrátové sítě, které využívají způsob šifrování Shared Key (Sdílený klíč), WPA-Enterprise (WPA-podnikový), WPA2-Enterprise (WPA2-podnikový) a RADIUS.

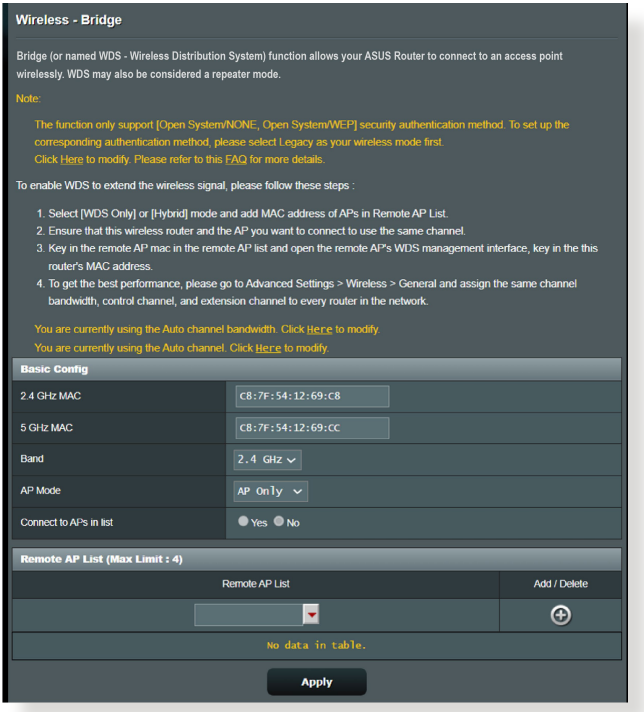
4. V poli WPS Method (Způsob WPS) vyberte možnost **Push Button (Tlačítko)** nebo **Client PIN Code (Kód PIN klienta)**. Vyberete-li možnost **Push Button (Tlačítko)**, přejděte na krok 5. Vyberete-li možnost **Client PIN Code (Kód PIN klienta)**, přejděte na krok 6.
5. Podle následujících pokynů nastavte standard WPS s použitím tlačítka WPS směrovače:
   a. Klepněte na tlačítko **Start** nebo stiskněte tlačítko WPS na zadní straně bezdrátového směrovače.
   b. Stiskněte tlačítko WPS na bezdrátovém zařízení. Obvykle je označeno logem WPS.

   **POZNÁMKA:** Vyhledejte umístění tlačítka WPS na bezdrátovém zařízení nebo v příslušné uživatelské příručce.

   c. Bezdrátový směrovač vyhledá všechna dostupná zařízení WPS. Pokud bezdrátový směrovač nenajde žádná zařízení WPS, přepne se do pohotovostního režimu.
6. Podle následujících pokynů nastavte standard WPS s použitím kódu PIN klienta:
   a. Vyhledejte kód PIN WPS v uživatelské příručce k bezdrátovému zařízení nebo na samotném zařízení.
   b. Zadejte kód PIN klienta do textového pole.
   c. Klepnutím na tlačítko **Start** přepněte bezdrátový směrovač do režimu průzkumu WPS. Indikátory LED směrovače třikrát rychle bliknou, dokud nebude konfigurování WPS dokončeno.

## 3.12.2 Most

Most nebo WDS (Wireless Distribution System) umožňuje připojit bezdrátový směrovač ASUS exkluzivně k jinému bezdrátovému přístupovému bodu, aniž by ostatní bezdrátová zařízení nebo stanice mohly přistupovat k vašemu bezdrátovému směrovači ASUS. Bezdrátový směrovač ASUS lze rovněž považovat za bezdrátový generický zesilovač, který komunikuje s jiným bezdrátovým přístupovým bodem a jinými bezdrátovými zařízeními.




Pokyny pro konfigurování bezdrátového mostu:

1. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Wireless (Bezdrátové připojení)** > **WDS**.
2. Vyberte frekvenční pásmo pro bezdrátový most.
3. V poli **AP Mode (Režim AP)** vyberte některou z následujících možností:
   - **AP Only (Pouze AP)**: Deaktivujte funkci bezdrátového mostu.
   - **WDS Only (Pouze WDS)**: Aktivuje funkci bezdrátového mostu, ale zabraňuje ostatním bezdrátovým zařízením/stanicím připojit se ke směrovači.

- **HYBRID**: Aktivuje funkci bezdrátového mostu a umožňuje ostatním bezdrátovým zařízením/stanicím připojit se ke směrovači.

**POZNÁMKA:** V režimu Hybrid mají bezdrátová zařízení připojená k bezdrátovému směrovači ASUS k dispozici pouze poloviční rychlost připojení přístupového bodu.

4. V poli **Connect to APs in list (Připojit k AP v seznamu)** klepněte na **Yes (Ano)**, chcete-li se připojit k některému přístupovému bodu v seznamu vzdálených přístupových bodů.
5. V poli **Control Channel (Řídící kanál)** vyberte provozní kanál bezdrátového mostu. Výběrem možnosti **Auto (Automaticky)** bude směrovač automaticky vybírat kanál, který je nejméně rušený.

**POZNÁMKA:** Dostupnost kanálů se liší podle země nebo regionu.

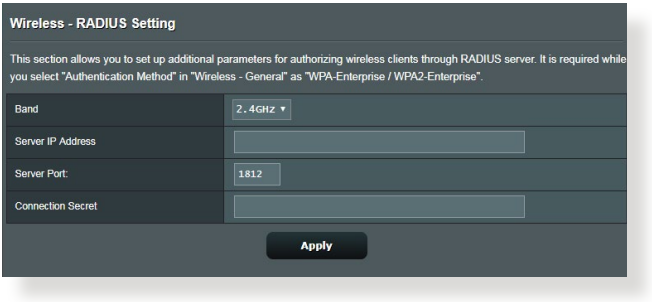
6. V **Remote AP List (Seznamu vzdálených přístupových bodů)** zadejte adresu MAC a klepnutím na tlačítko **Add (Přidat)** zadejte  adresu MAC dalších dostupných přístupových bodů.

**POZNÁMKA:** Veškeré přístupové body přidané do seznamu se musí nacházet na stejném řídícím kanálu jako bezdrátový směrovač ASUS.

7. Klepněte na **Apply (Použít)**.

### 3.12.3 Nastavení RADIUS

Nastavení RADIUS (Remote Authentication Dial In User Service) poskytuje dodatečnou vrstvu zabezpečení při výběru režimu ověřování WPA-podnikový, WPA2-podnikový nebo Radius s 802.1x.



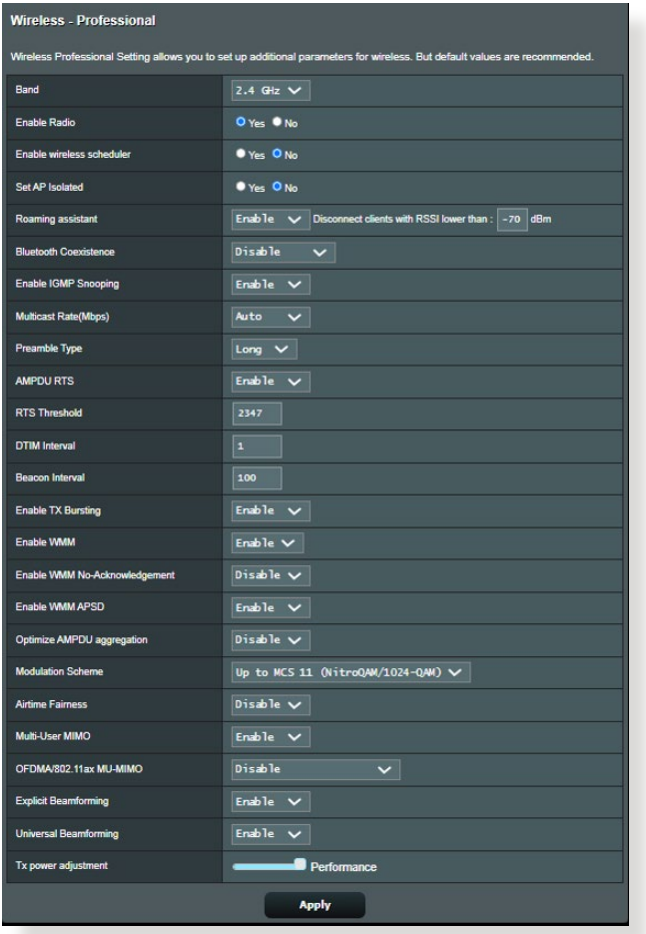

**Pokyny pro konfigurování bezdrátových nastavení RADIUS:**

1. Zkontrolujte, zda je režim ověřování bezdrátového směrovače nastaven na WPA-podnikový, WPA2-podnikový nebo Radius s 802.1x.
2. Na navigačním panelu přejděte na **Advanced Settings (Upřesnit nastavení)** > **Wireless (Bezdrátové připojení)** > **RADIUS Setting (Nastavení RADIUS)**.
3. Vyberte frekvenční pásmo.
4. Do pole **Server IP Address (Adresa IP serveru)** zadejte adresu IP serveru RADIUS.
5. Do pole **Connection Secret (Tajemství připojení)** zadejte heslo pro přístup k serveru RADIUS.
6. Klepněte na **Apply (Použít)**.

### 3.12.4 Professional (Odborník)

Na obrazovce Professional (Odborník) jsou k dispozici možnosti upřesňující konfigurace.

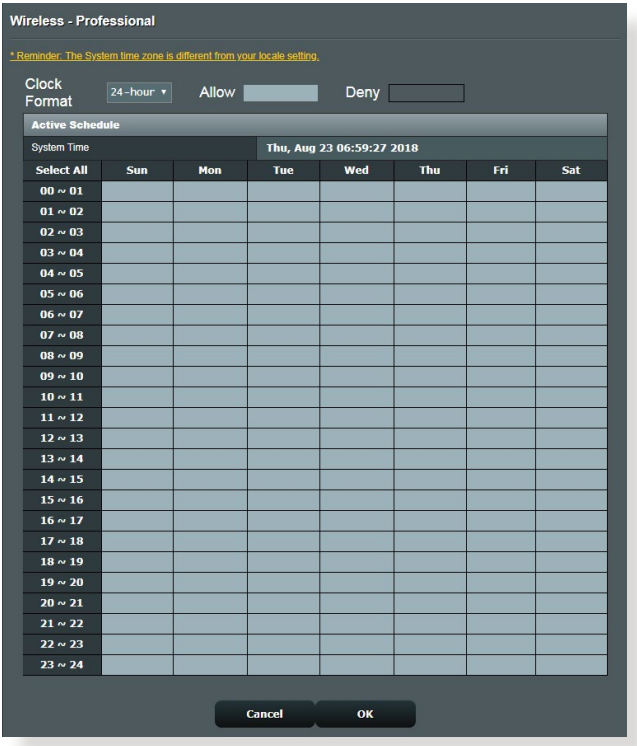
**POZNÁMKA:** Na této stránce doporučujeme použít výchozí hodnoty.




Na obrazovce **Professional Settings (Odborné nastavení)** můžete nakonfigurovat následující položky:

- **Band (Bandă)**: Vyberte frekvenční pásmo, pro které budou použita profesionální nastavení.

- **Enable Radio (Povolit rádio)**: Výběrem možnosti **Yes (Ano)** aktivujete bezdrátovou síť. Výběrem možnosti **No (Ne)** deaktivujete bezdrátovou síť.
- **Enable wireless scheduler (Activare planificator fără fir):** Puteţi alege formatul pentru afişarea ceasului, cu 24 de ore sau cu 12 ore. Culoarea din tabel indică Allow (Se permite) sau Deny (Se respinge). Faceţi clic pe fiecare cadru pentru a schimba setările pentru ora din zilele săptămânii şi faceţi clic pe **OK** când terminaţi.




- **Set AP isolated (Nastavit izolovaný AP)**: Položka Set AP isolated (Nastavit izolovaný AP) zabraňuje vzájemnou komunikaci bezdrátových zařízení ve vaší síti. Tato funkce je vhodná, pokud se k vaší síti často připojuje nebo odpojuje velké množství hostů. Výběrem možnosti **Yes (Ano)** aktivujte tuto funkci; výběrem možnosti **No (Ne)** deaktivujte tuto možnost.
- **Multicast rate (Mbps) (Rychlost vícesměrového vysílání (Mb/s))**: Vyberte rychlost vícesměrového vysílání nebo klepnutím na **Disable (Deaktivovat)** vypněte simultánní individuální přenos.

- **Preamble Type (Typ preambule)**: Typ preambule definuje dobu, po kterou směrovač provádí kontrolu CRC (Cyclic Redundancy Check). CRC je metoda určování chyb během přenášení dat. Pro frekventovanou bezdrátovou síť s vysokým síťovým provozem vyberte možnost **Short (Krátká)**. Pokud je vaše síť složena ze starších nebo zastaralých bezdrátových zařízení, vyberte možnost **Long (Dlouhá)**.
- **RTS Threshold (Práh RTS)**: Výběrem nižší prahové hodnoty RTS (Request to Send) se vylepší bezdrátová komunikace ve frekventované nebo rušené bezdrátové síti s vysokým síťovým provozem a velkým počtem bezdrátových zařízení.
- **DTIM Interval (Interval DTIM)**: Interval DTIM (Delivery Traffic Indication Message) nebo rychlost blikání dat je časový interval předtím, než je bezdrátovému zařízení v režimu spánku odeslán signálu o datovém paketu čekajícím na doručení. Výchozí hodnota jsou tři milisekundy.
- **Beacon Interval (Interval blikání)**: Interval blikání je čas mezi dvěma intervaly DTIM. Výchozí hodnota je 100 milisekund. V případě nestabilního bezdrátového připojení nebo roamingujících zařízení snižte hodnotu intervalu blikání.
- **Enable TX Bursting (Povolit shlukování TX)**: Povolení shlukování TX zvyšuje přenosovou rychlost mezi bezdrátovým směrovačem a zařízeními 802.11g.
- **Enable WMM APSD (Povolit WMM APSD)**: Povolte WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) pro vylepšení řízení spotřeby mezi bezdrátovými zařízeními. Výběrem možnosti **Disable (Zakázat)** vypněte WMM APSD.

# 4 Používání nástrojů

## 4.1 Vyhledání zařízení

Device Discovery (Vyhledání zařízení) je nástroj ASUS WLAN, který rozpoznává bezdrátový směrovač ASUS, a umožňuje konfigurovat nastavení bezdrátové sítě.

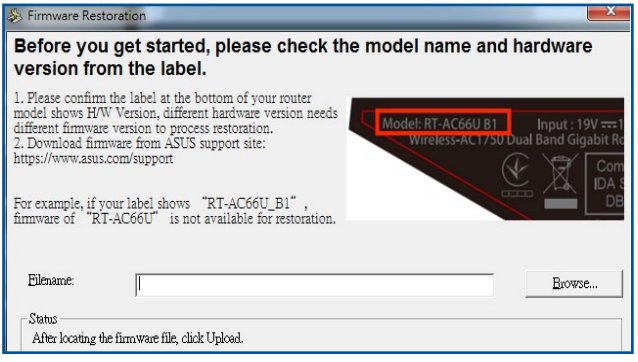
**Pokyny pro spuštění nástroje Device Discovery (Vyhledání zařízení):**

- Na pracovní ploše počítače klepněte na **Start (Zahájit)** > **All Programs (Všechny programy)** > **ASUS Utility (ASUS nástroj) > ASUS Wireless Router (ASUS Bezdrátový směrovač )** > **Device Discovery (Vyhledání zařízení)**.

**POZNÁMKA:** Když nastavíte směrovač na režim přístupového bodu, je třeba použít funkci Device Discovery (Vyhledání zařízení) pro získání adresy IP směrovače.

## 4.2 Obnova firmwaru

Funkce Firmware Restoration (Obnova firmwaru) se používá na bezdrátovém směrovači ASUS, který selhal během aktualizace firmwaru. Znovu načte určený firmware. Tento proces trvá přibližně tři až čtyři minuty.




**DŮLEŽITÉ!** Před použitím nástroje Firmware Restoration (Obnova firmwaru) spusťte záchranný režim.

**POZNÁMKA:** Tato funkce není podporována v operačním systému MAC.

**Pokyny pro spuštění záchranného režimu a použití nástroje Firmware Restoration (Obnova firmwaru):**

1. Odpojte bezdrátový směrovač od zdroje napájení.
2. Stiskněte a podržte resetovací tlačítko na zadním panelu a zároveň znovu připojte bezdrátový směrovač ke zdroji napájení. Resetovací tlačítko uvolněte, když indikátor LED napájení na předním panelu začne pomalu blikat, což znamená, že se bezdrátový směrovač nachází v záchranném režimu.
3. Nastavte statickou adresu IP v počítači a použijte následující pro nastavení TCP/IP:

   **IP address (Adresa IP):** 192.168.1.x

   **Subnet mask (Maska podsítě):** 255.255.255.0
4. Na pracovní ploše počítače klepněte na **Start** > **All Programs (Všechny programy)** > **ASUS Utility (ASUS nástroj) > Wireless Router (Bezdrátový směrovač)** > **Firmware Restoration (Obnova firmwaru)**.
5. Určete soubor firmwaru a potom klepněte na **Upload (Odeslat)**.

**POZNÁMKA:** Toto není nástroj pro upgradování firmwaru a nelze jej použít na funkčním bezdrátovém směrovači ASUS. Běžné aktualizace firmwaru musí být prováděny prostřednictvím webového rozhraní. Další podrobnosti viz **Kapitola 3: Konfigurování obecných a upřesňujících nastavení**.

# 5 Odstraňování problémů

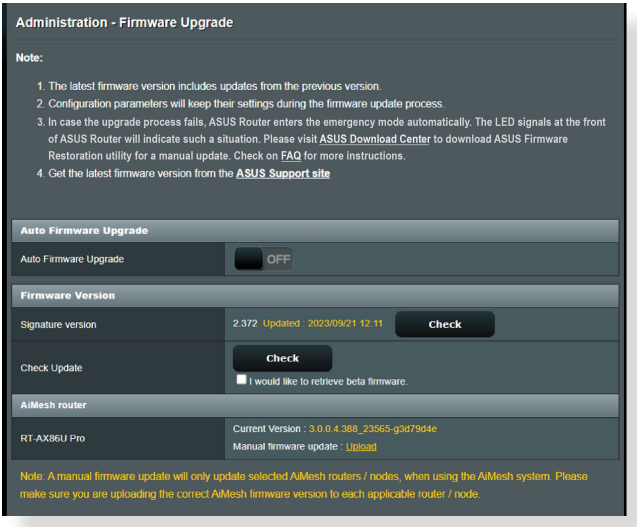
V této kapitole jsou uvedena řešení problémů, se kterými se můžete při používání směrovače setkat. Setkáte-li se s problémy, které nejsou uvedeny v této kapitole, navštivte webové stránky odborné pomoci společnosti ASUS na adrese: https://www.asus.com/support, kde najdete další informace a kontakty na technickou podporu společnosti ASUS.

## 5.1 Odstraňování nejčastějších problémů

Setkáte-li se při používání tohoto směrovače s problémy, před hledáním dalších řešení vyzkoušejte základní kroky uvedené v této části.

### Upgradujte firmware na nejnovější verzi.

1. Spusťte webové grafické uživatelské rozhraní GUI. Přejděte na **Advanced Settings (Upřesnit nastavení)** > **Administration (Správa)** > **Firmware Upgrade (Upgrade firmwaru)**. Klepnutím na **Check (Zkontrolovat)** ověřte, zda je k dispozici nejaktuálnější verze.




2. Pokud není k dispozici nejaktuálnější firmware, navštivte globální webové stránky společnosti ASUS na adrese https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/ a stáhněte nejaktuálnější firmware.

3. Na stránce **Firmware Version (Verze firmwaru)** klepněte na tlačítko **Check (Zkontrolovat)** a vyhledejte soubor firmwaru.
4. Klepnutím na tlačítko **Upload (Načíst)** upgradujte firmware.

### Restartujte síť v následujícím pořadí:

1. Vypněte modem.
2. Odpojte modem od elektrické zásuvky.
3. Vypněte směrovač a počítače.
4. Připojte modem k elektrické zásuvce.
5. Zapněte modem a počkejte 2 minuty.
6. Zapněte směrovač a počkejte 2 minuty.
7. Zapněte počítače.

### Zkontrolujte, zda se nastavení bezdrátového připojení v počítači shoduje s nastavením bezdrátového připojení ve směrovači.

- Když připojujete počítač ke směrovači bezdrátově, ověřte správnost SSID (název bezdrátové sítě), metody šifrování a hesla.

### Zkontrolujte správnost síťových nastavení.

- Každý klient v síti musí mít platnou adresu IP. Společnost ASUS doporučuje používat server DHCP bezdrátového směrovače k přidělování adres IP počítačům v síti.

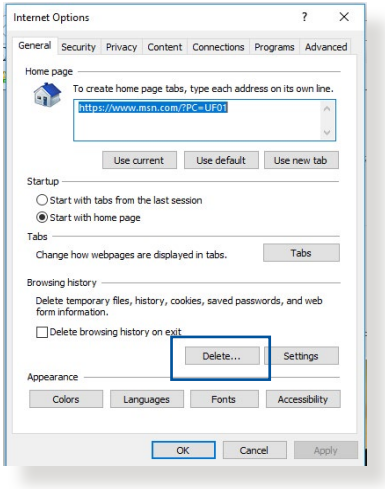
- Někteří poskytovatelé kabelových modemových služeb vyžadují používání adresy MAC počítače, který byl zaregistrován k účtu jako první. Adresu MAC můžete zobrazit ve webovém grafickém uživatelském rozhraní (GUI), **Network Map (Mapa sítě)** > stránka **Clients (Klienti)** a umístěním myši na vaše zařízení v části **Client status (Stav klienta)**.

## 5.2 Často kladené dotazy (FAQs)

### Nelze přistupovat ke grafickému uživatelskému rozhraní (GUI) směrovače prostřednictvím webového prohlížeče.

- Pokud je počítač připojen kabelem, zkontrolujte připojení ethernetového kabelu a stav indikátoru LED podle pokynů v předchozí části.
- Zkontrolujte, zda používáte správné přihlašovací údaje. Při zadávání přihlašovacích údajů zkontrolujte, zda není zapnutá funkce klávesy Caps Lock.
- Odstraňte soubory cookie a soubory ve webovém prohlížeči. V případě prohlížeče Internet Explorer postupujte podle těchto kroků:

  1. Spusťte prohlížeč Internet Explorer a potom klepněte na příkaz **Tools (Nástroje)** > **Internet Options (Možnosti Internetu)**.
  2. Na kartě **General (Obecné)** v části **Browsing history (Historie procházení)** klepněte na tlačítko **Delete… (Odstranit...)**, vyberte položku **Temporary Internet Files and website files (Dočasné soubory Internetu a soubory z webových stránek)** a **Cookies and website data (Soubory cookie a soubory z webových stránek)** a potom klepněte na tlačítko **Delete (Odstranit)**.



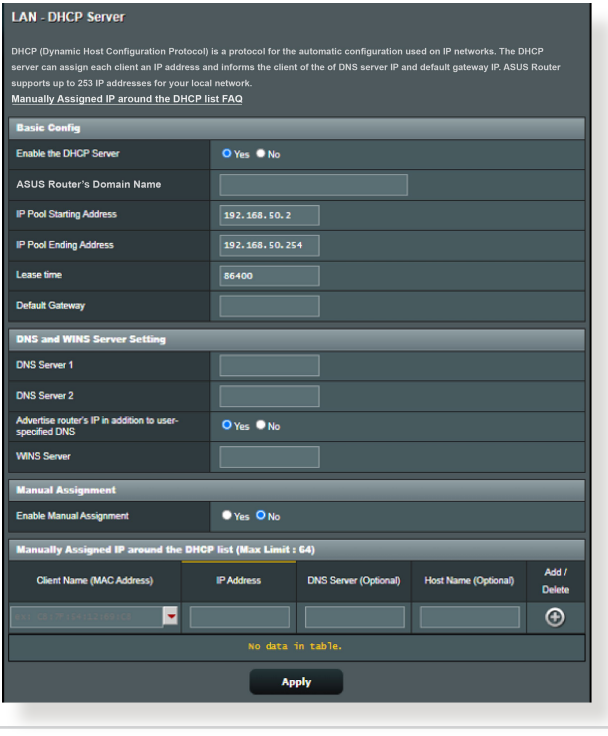

**POZNÁMKY:**

- Příkazy pro odstraňování souborů cookie a souborů se liší podle webového prohlížeče.
- Deaktivujte nastavení serveru proxy, zrušte telefonické připojení a nastavte TCP/IP na automatické získání adresy IP. Další podrobnosti viz Kapitola 1 této uživatelské příručky.
- Zkontrolujte, zda používáte ethernetové kabely kategorie CAT5e nebo CAT6.

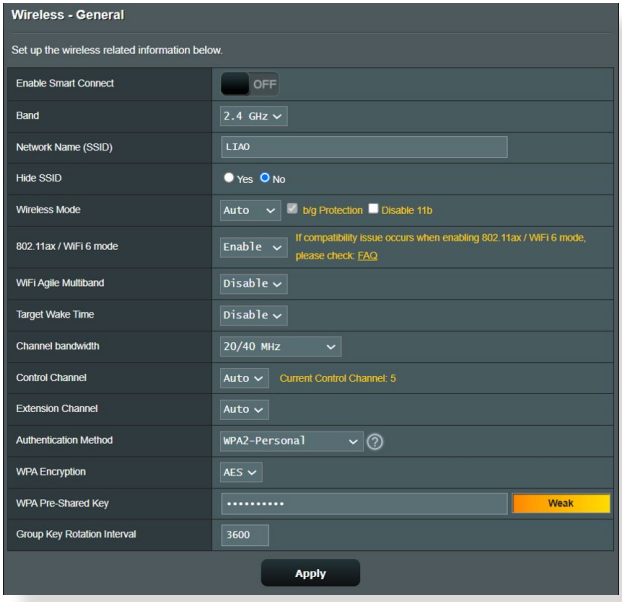
## Klient nemůže navázat bezdrátové připojení ke směrovači.

**POZNÁMKA:** Pokud máte problémy k síti 5 GHz, zkontrolujte, zda vaše bezdrátové zařízení podporuje 5 GHz nebo zda je dvoupásmové.

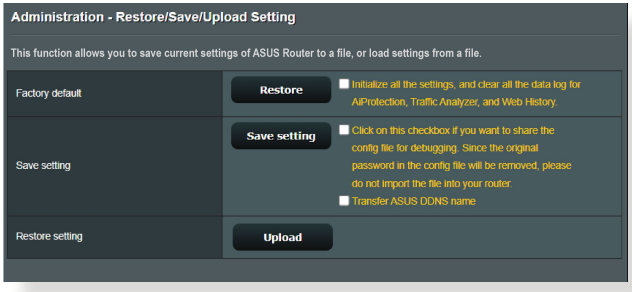
- **Mimo dosah:**
  - Umístěte směrovač blíže k bezdrátovému klientovi.
- **Server DHCP je deaktivován:**
  1. Spusťte webové grafické uživatelské rozhraní GUI. Přejděte na **General (Obecné)** > **Network Map (Mapa sítě)** > **Clients (Klienti)** a vyhledejte zařízení, které chcete připojit ke směrovači.
  2. Pokud zařízení nelze najít v části **Network Map (Mapa sítě)**, přejděte na **Advanced Settings (Upřesnit nastavení)** > **LAN** > **DHCP Server (Server DHCP)**, seznam **Basic Config (Základní konfigurace)** a vyberte možnost **Yes (Ano)** v části **Enable the DHCP Server (Povolit server DHCP)**.



- Název sítě SSID je skrytý. Pokud vaše zařízení může najít názvy sítě SSID ostatních směrovačů, ale nemůže najít název sítě SSID vašeho směrovače, přejděte na **Advanced Settings (Upřesnit nastavení)** > **Wireless (Bezdrát)** > **General (Obecné)**, vyberte **No (Ne)** v části **Hide SSID (Skrýt SSID)** a vyberte **Auto (Automaticky)** v části **Control Channel (Řídící kanál)**.



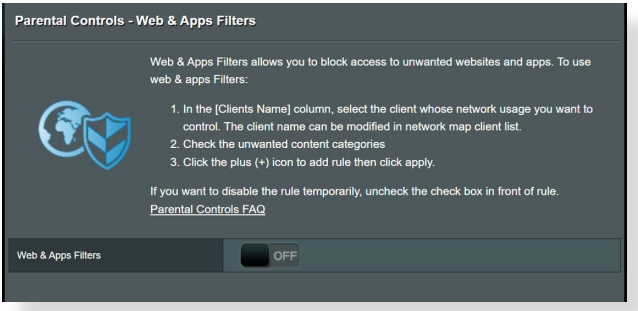

- Používáte-li adaptér bezdrátové místní sítě LAN, zkontrolujte, zda používaný bezdrátový kanál odpovídá kanálům dostupným ve vaší zemi/oblasti. Pokud ne, upravte kanál, šířku pásma kanálu a bezdrátový režim.
- Pokud se přesto nemůžete bezdrátově připojit ke směrovači, můžete obnovit výchozí tovární nastavení směrovače. V grafickém uživatelském rozhraní (GUI) klepněte na **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/Uložit/Načíst nastavení)** a klepněte na **Restore (Obnovit)**.



## Nelze přistupovat k Internetu.

- Zkontrolujte, zda se směrovač může připojit k adrese IP sítě WAN vašeho ISP. Spusťte webové grafické uživatelské rozhraní (GUI), přejděte na **General (Obecné)** > **Network Map (Mapa sítě)** a zkontrolujte **Internet status (Stav sítě Internet)**.
- Pokud se směrovač nemůže připojit k adrese IP sítě WAN vašeho ISP, zkuste restartovat síť podle pokynů v části **Restart your network in following sequence (Restartujte síť v následujícím pořadí)** v kapitole **Basic Troubleshooting (Odstraňování nejčastějších problémů)**.


- Zařízení je blokováno funkcí rodičovské kontroly. Přejděte na **General (Obecné)** > **Parental Controls (Rodičovská kontrola)** a zkontrolujte, zda je zařízení v seznamu. Pokud je zařízení uvedeno v seznamu **Client Name (Název klienta)**, odstraňte jej tlačítkem **Delete (Odstranit)** nebo upravte nastavení časové správy.



- Pokud stále nelze přistupovat k Internetu, zkuste restartovat počítač a ověřte adresu IP a adresu brány sítě.

## Zapomněli jste SSID (název sítě) nebo síťové heslo.

- Nastavte nový název SSID a šifrovací klíč prostřednictvím pevného připojení (ethernetového kabelu). Spusťte webové grafické uživatelské rozhraní (GUI), přejděte na **Network Map (Mapa sítě)**, klepněte na ikonu směrovače, zadejte nový název SSID a šifrovací klíč a potom klepněte na tlačítko **Apply (Použít)**.
- Obnovte výchozí nastavení směrovače. Spusťte grafické uživatelské rozhraní (GUI), přejděte na **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/Uložit/Načíst nastavení)** a klepněte na **Restore (Obnovit)**.

## Pokyny pro obnovení výchozích nastavení systému?

- Přejděte na **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/uložit/načíst nastavení)** a klepněte na **Restore (Obnovit)**.

## Upgrade firmwaru se nezdařil.

Spusťte záchranný režim a spusťte nástroj Firmware Restoration (Obnova firmwaru). Pokyny pro používání nástroje Firmware Restoration (Obnova firmwaru) viz část **4.2 Obnova firmwaru**.

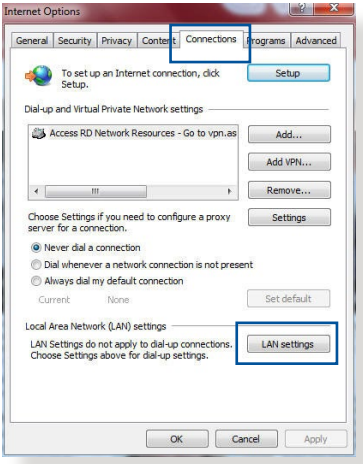
## Nelze přistupovat k webovému grafickému uživatelskému rozhraní (GUI)

Před konfigurováním bezdrátového směrovače proveďte kroky popsané v této části pro váš hostitelský počítač a síťové klienty.

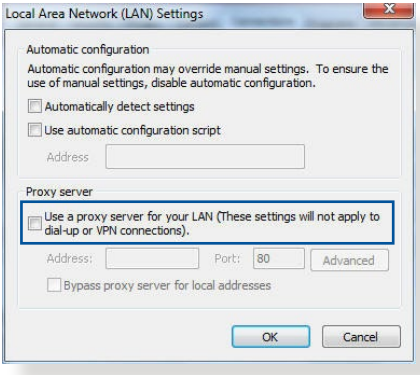
### A. Deaktivujte server proxy, je-li aktivován.

#### Windows®

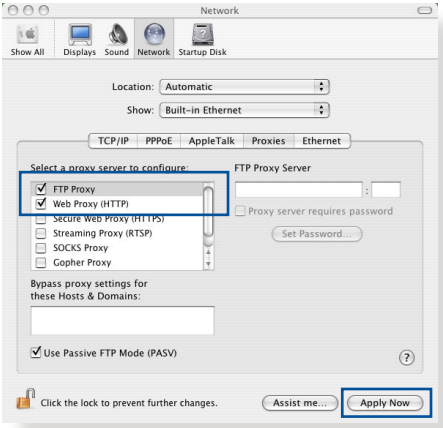
1. Klepnutím na **Start (Zahájit)** > **Internet Explorer** spusťte webový prohlížeč.
2. Klepněte na **Tools (Nástroje)** > **Internet options (Možnosti Internetu)** > **Connections (Připojení)** > **LAN settings (Nastavení místní sítě)**.




3. Na obrazovce Nastavení místní sítě (LAN) zrušte zaškrtnutí políčka **Use a proxy server for your LAN (Použít pro síť LAN server proxy)**.
4. Po dokončení klepněte na **OK**.



## MAC OS



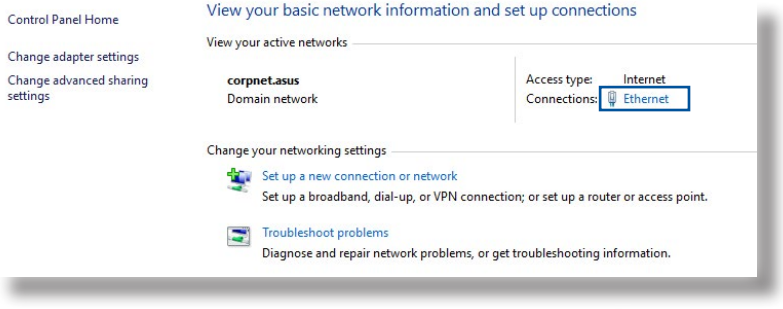

1. V prohlížeči Safari klepněte na **Safari** > **Preferences (Předvolby)** > **Advanced (Upřesnit)** > **Change Settings... (Změnit nastavení...)**.
2. Na obrazovce Network (Síť) zrušte výběr položky **FTP Proxy (FTP server proxy)** a **Web Proxy (HTTP) (Webový server proxy (HTTP))**.
3. Po dokončení klepněte na **Apply Now (Použít)**.

**POZNÁMKA:** Podrobné pokyny pro deaktivaci serveru proxy viz nápověda k prohlížeči.

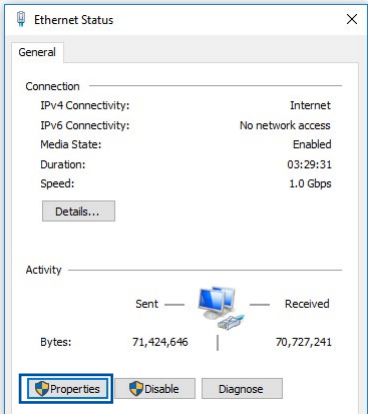
## B. Proveďte nastavení TCP/IP pro automatické získání adresy IP.

## Windows®

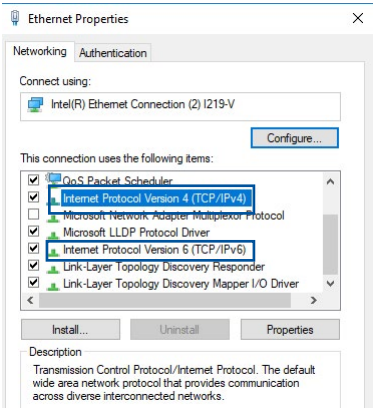
1. Klepněte na **Start (Zahájit)** > **Control Panel (Ovládací panely)** > **Network and Sharing Center (Centrum sítí a sdílení)**, potom kliknutím na síťové připojení zobrazíte jeho stavové okno.



2. Kliknutím na tlačítko **Properties (Vlastnosti)** zobrazíte okno Ethernet Properties (Vlastnosti ethernetu).



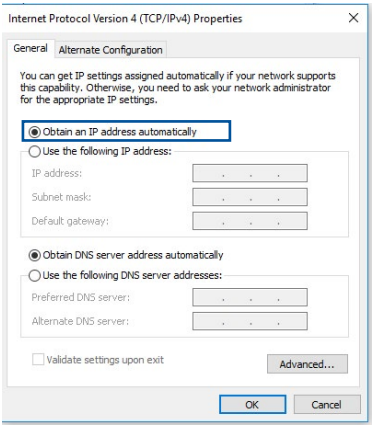

3. Vyberte **Internet Protocol Version 4 (TCP/IPv4) (Protokol Internet verze 4 (TCP/IPv4))** nebo **Internet Protocol Version 6 (TCP/IPv6) (Protokol Internet verze 6 (TCP/IPv6)** a potom klepněte na **Properties (Vlastnosti)**.




4. Zaškrtnutím položky **Obtain an IP address automatically (Získat adresu IP automaticky)** budou nastavení iPv4 IP získána automaticky.

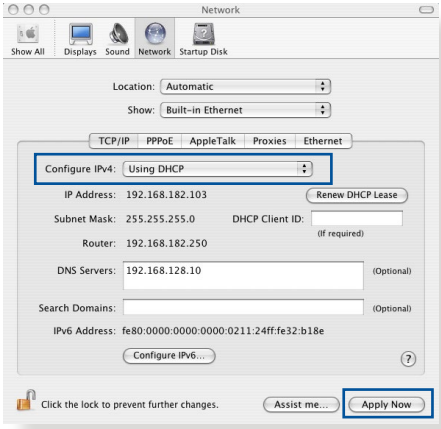
   Zaškrtnutím položky **Obtain an IPv6 address automatically (Získat adresu IPv6 automaticky)** budou nastavení iPv6 IP získána automaticky.

5. Po dokončení klepněte na **OK**.



## MAC OS

1. Klepněte na ikonu Apple v levé horní části obrazovky.
2. Klepněte na **System Preferences (Systémové preference)** > **Network (Síť)** > **Configure... (Konfigurovat...)**.
3. Na kartě **TCP/IP** vyberte **Using DHCP (Použití protokolu DHCP)** v rozevíracím seznamu **Configure IPv4 (Konfigurovat IPv4)**.



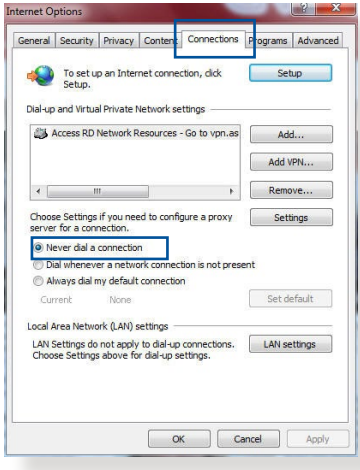

4. Po dokončení klepněte na **Apply Now (Použít)**.

**POZNÁMKA:** Podrobnosti o konfigurování nastavení TCP/IP počítače viz nápověda k operačnímu systému a podpůrné funkce.

## C. Deaktivujte telefonické připojení, je-li aktivováno.

### Windows®

1. Klepnutím na **Start (Zahájit)** > **Internet Explorer** spusťte webový prohlížeč.
2. Klepněte na **Tools (Nástroje)** > **Internet options (Možnosti Internetu)** > **Connections (Připojení)**.
3. Zaškrtěte políčko **Never dial a connection (Nikdy nevytáčet připojení)**.
4. Po dokončení klepněte na **OK**.




**POZNÁMKA:** Podrobné pokyny pro deaktivaci telefonického připojení viz nápověda k prohlížeči.

# Dodatky

## GNU General Public License

### Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

**GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

### Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

# Poznámky k bezpečnosti

Při používání tohoto produktu vždy dodržujte základní bezpečnostní opatření, mimo jiné:

**VAROVÁNÍ!**

- Napájecí kabel(y) musí být připojeny do elektrické zásuvky (zásuvek) s vhodným uzemněním. Connect the equipment only to a nearby socket outlet that is easily accessible.
- Pokud je napájecí zdroj porouchaný, nepokoušejte se jej opravovat. Kontaktujte kvalifikovaného servisního technika nebo prodejce.
- NEPOUŽÍVEJTE poškozené napájecí kabely, doplňky ani jiné periférie.
- NEINSTALUJTE toto vybavení výše než do výšky 2 metrů.
- Počítač používejte jen při teplotě okolí 0 ˚C (32 ˚F) až 40 ˚C (104 ˚F).
- Před použitím produktu si přečtěte provozní pokyny a informace o uvedeném teplotním rozsahu.
- Při používání tohoto zařízení na letištích, v nemocnicích, čerpacích stanicích a profesionálních garážích věnujte zvláštní pozornost osobní bezpečnosti.
- Rušení lékařského zařízení: Aby se snížilo riziko rušení, udržujte mezi implantovanými zdravotnickými zařízeními a produkty ASUS minimální vzdálenost alespoň 15 cm (6 palců).
- Produkty ASUS používejte v podmínkách s dobrým příjmem, aby se minimalizovala úroveň záření.
- Udržujte zařízení mimo dosah těhotných žen a spodní části břicha dospívajících.
- Tento výrobek NEPOUŽÍVEJTE, pokud nese zjevné známky poškození nebo je mokrý, poškozený či upravený. Požádejte o pomoc servis.

**VAROVÁNÍ!**

- NEPOKLÁDEJTE na nerovné ani nestabilní pracovní povrchy.
- Na výrobek NEPOKLÁDEJTE žádné předměty a zabraňte pádu předmětů na výrobek. Nevystavujte výrobek mechanickým nárazům, jako je lámání, ohýbání, propíchnutí nebo drcení.
- Tento výrobek NEDEMONTUJTE, neotevírejte, neohřívejte v mikrovlnné troubě, nespalujte, nenatírejte ani do něj nestrkejte žádné cizí předměty.
- Informace naleznete na energetickém štítku na spodní straně vašeho produktu. Ujistěte se, že napájecí adaptér je v souladu s hodnotou na něm uvedenou.
- Udržujte výrobek mimo dosah ohně a zdrojů tepla.
- NEVYSTAVUJTE ani nepoužívejte blízko tekutin, deště nebo vlhkosti. Tento výrobek NEPOUŽÍVEJTE za statických bouří.
- Výstupní okruhy PoE tohoto výrobku připojujte výhradně k sítím PoE, bez směrování do externích zařízení.
- Aby nedošlo k zásahu elektrickým proudem, odpojte napájecí kabel z elektrické zásuvky před přemístěním počítače.
- Používejte pouze příslušenství, které bylo schváleno výrobcem zařízení pro použití s tímto modelem. Použití jiných typů příslušenství může zneplatnit záruku nebo porušovat místní předpisy a zákony a může představovat bezpečnostní rizika. Informace o dostupném ověřeném příslušenství vám poskytne nejbližší prodejce.
- Používání tohoto výrobku způsobem, který není doporučen v poskytnutých pokynech, může způsobit požár nebo zranění osob.

## Servis a Podpora

Navštivte naše vícejazyčné webové stránky na adrese https://www.asus.com/support.