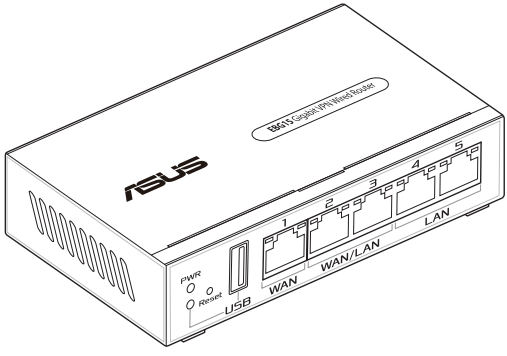
Uživatelská příručka

ASUS EBG15

Gigabitový VPN drátový router

Model: EBG15



IN SEARCH OF INCREDIBLE

CZ23348
První edice
Duben 2024

Obsah

Obsah

Obsah

1 Seznámení s EBG15

1.1 Vítejte!

Děkujeme vám za zakoupení bezdrátového směrovače ASUS EBG15!

EBG15 poskytuje rychlou, bezpečnou a škálovatelnou síť, zvýšenou stabilitu sítě prostřednictvím ethernetové konektivity a poskytuje internetové zálohování se dvěma porty WAN/LAN a jedním portem USB pro podporu operací.

1.2 Obsah krabice

☑ EBG15
☑ Napájecí adaptér
☑ Stručná příručka
☑ Kabel RJ45
☑ Nálepka s místními přihlašovacími údaji
☑ Záruční list

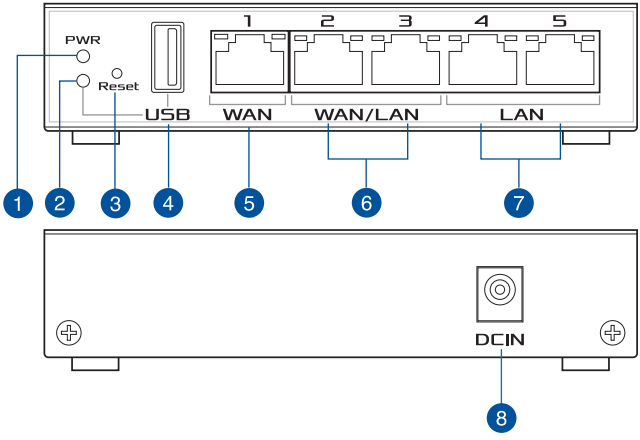
POZNÁMKY:

- 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 drátový router

1. Připojte adaptér k portu DCIN.
2. Když je váš hardware připraven, rozsvítí se indikátor LED napájen.

Popis tlačítek a portů



1	**Indikátor LED napájení** **Nesvítí**: Žádné napájení. **Svítí**: Zařízení je připraveno. **Bliká pomalu**: Záchranný režim.
2	**Kontrolka LED USB 3.2 Gen 1** **Nesvítí**: Vypnuto nebo žádné fyzické připojení. **Svítí**: Zařízení je připraveno. **Bliká pomalu**: Vysílání nebo přijímání dat.
3	**Resetovací tlačítko** Toto tlačítko slouží k resetování nebo obnovení výchozích továrních nastavení systému.
4	**Port rozhraní USB 3.2 Gen 1** Do tohoto portu vložte zařízení s rozhraním USB 3.2 Gen 1, například pevný disk USB nebo jednotku USB Flash.
5	**Port WAN (Internet)** K tomuto portu připojte síťový kabel pro navázání připojení WAN.
6	**Porty WAN / LAN** K tomuto portu připojte síťový kabel pro navázání připojení WAN / LAN.
7	**Porty LAN** Tento port slouží k připojení počítače k portu LAN síťovým kabelem.
8	**Port vstupu stejnosměrného napájení (DCIN)** K tomuto portu připojte dodaný adaptér střídavého napájení (AC) a připojte směrovač ke zdroji napájení.

Signály kontrolky LED ethernetového portu

Indikátory LED			
LED rychlosti (Zelený)		Kontrolka LED připojení/aktivity (Oranžová)	
1G	ZAPNUTO	1G/100M/10M	Bliká
100M/10M	VYPNUTO	Žádný provoz	ZAPNUTO

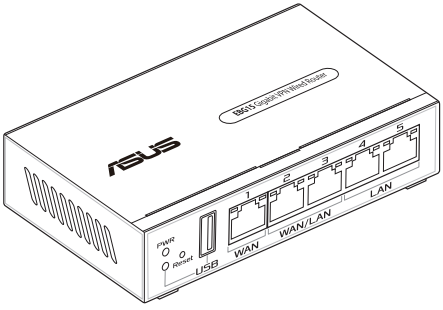
Technické údaje:

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 směrovače

Pro nejlepší síťový zážitek se ujistěte, že:

- 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 počítače, které splňují následující požadavky na systém:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Nainstalovaná služba TCP/IP
- Webový prohlížeč, například Internet Explorer, Firefox, Safari nebo Google Chrome

POZNÁMKA: Ethernetové kabely RJ-45, které budou použity k připojení síťových zařízení, nesmí přesahovat 100 metrů.

1.6 Instalace směrovače

DŮLEŽITÉ!

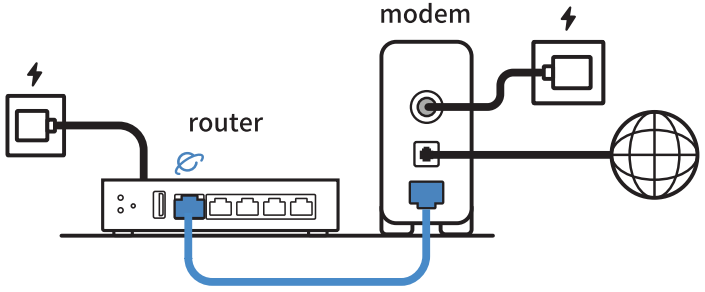
- Před instalací drátový router ASUS proveďte následující kroky:
  - Pokud vyměňujete stávající směrovač, odpojte jej od sítě.
  - Odpojte kabely/vodiče od instalace stávajícího modemu. Pokud je modem vybaven záložní baterií, rovněž ji vyjměte.
  - Restartujte počítač (doporučeno).

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).

1.6.1 Pevné připojení

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



Pokyny pro instalaci drátový router prostřednictvím pevného připojení:

1. Připojte adaptér střídavého napájení drátový router ke vstupnímu portu stejnosměrného napájení a připojte jej k elektrické zásuvce.
2. Pomocí dodaného síťového kabelu připojte počítač k portu LAN drátový router.
3. Pomocí síťového kabelu připojte počítač k portu WAN drátový router.
4. Připojte adaptér střídavého napájení modemu ke vstupnímu portu stejnosměrného napájení a připojte jej k elektrické zásuvce.

2 Nastavení hardwaru

2.1 Přihlášení k webovému grafickému uživatelskému rozhraní (GUI)

Tento ASUS drátový router je vybaven intuitivním webovým grafickým uživatelským rozhraním (GUI), které umožňuje snadno konfigurovat různé funkce prostřednictvím webového prohlížeče, například Microsoft Edge, Safari nebo Google Chrome.

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

Kabelové připojení k vaší síti:

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

1. Ručně zadejte výchozí adresu IP bezdrátového směrovače do vašeho webového prohlížeče, zadejte http://expertwifi.net.
2. Postupujte podle pokynů pro konfiguraci.

2.2 Automatická detekce sítě WAN

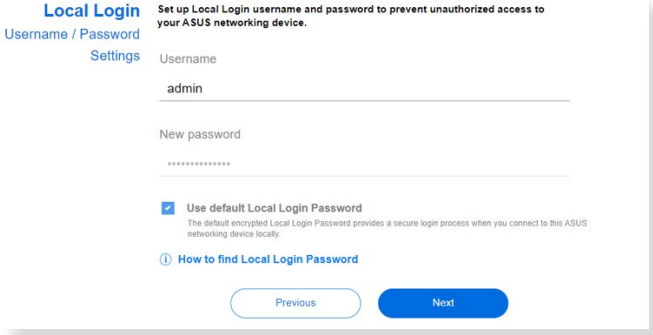
Funkce Rychlé nastavení Internetu (QIS) vás provede rychlou konfigurací připojení k Internetu.

POZNÁMKA: Při prvním nastavování internetového připojení stisknutím resetovacího tlačítka na drátový router obnovte jeho výchozí tovární nastavení.

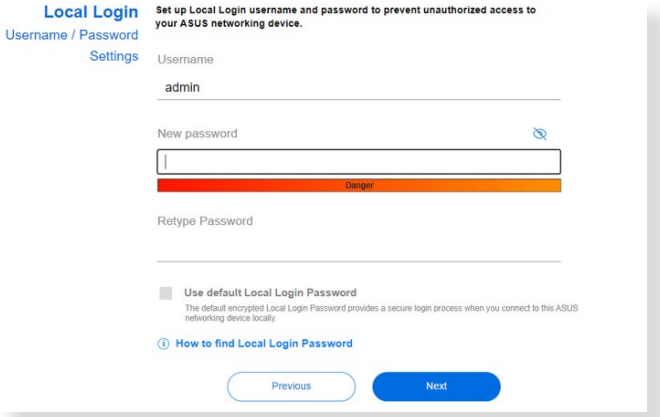
Automatická detekce sítě WAN:

1. Přihlaste se k webovému grafickému uživatelskému rozhraní (GUI) a klikněte na **Create A New Network (Vytvořit novou síť)**.

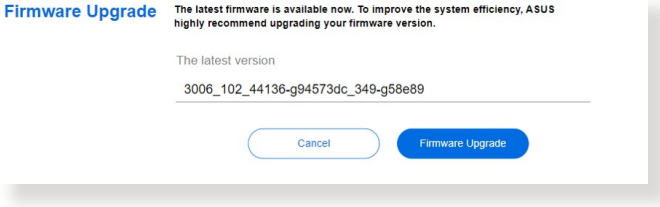
2. Kliknutím na **Next (Další)** se přihlaste pomocí výchozího uživatelského jména a hesla.



Zrušte zaškrtnutí políčka **Use default Local Login Password (Použít výchozí místní přihlašovací heslo)**, zadejte nové uživatelské jméno a heslo a klikněte na tlačítko **Next (Další)**.



3. Kliknutím na **Firmware Upgrade (Upgrade firmwaru)** zaktualizujte firmware na nejnovější verzi nebo kliknutím na **Cancel (Zrušit)** zachováte aktuální verzi.



POZNÁMKA: Tato obrazovka se zobrazí pouze v případě, že je k dispozici nová verze firmwaru.

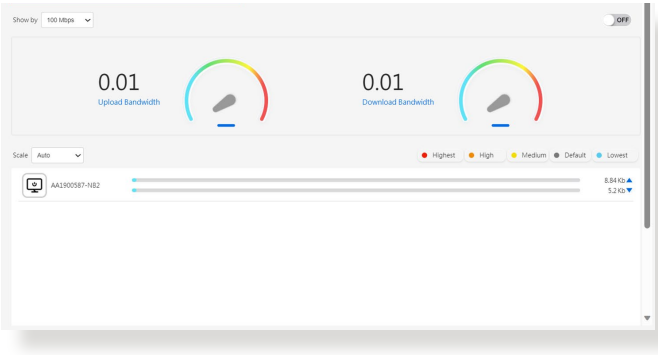
3 Konfigurování EBG15

3.1 Adaptivní QoS

3.1.1 Monitorování šířky pásma

Monitorování šířky pásma umožňuje sledovat celkové využití šířky pásma pro stahování a odesílání každého klienta.

Chcete-li používat **Bandwidth Monitor (Monitorování šířky pásma)**, přejděte na **Settings (Nastavení)** > **Adaptive QoS (Adaptivní QoS)** > **Bandwidth Monitor (Monitorování šířky pásma)**.

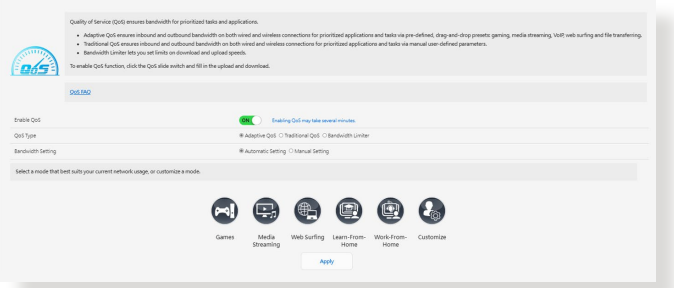


POZNÁMKA: Další informace najdete na https://www.asus.com/support/faq/1008717.

3.1.2 QoS

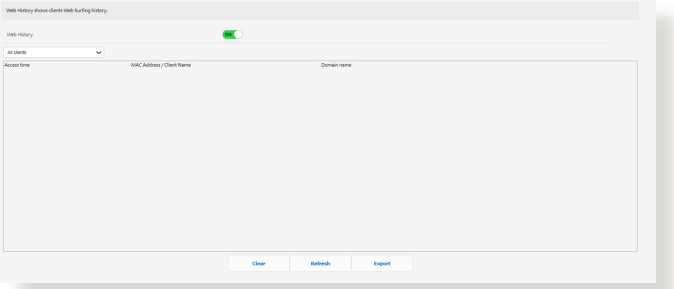
Služba QoS (Quality of Service) zajišťuje dostatečnou šířku pásma pro úlohy a aplikace, kterým stanovíte vyšší prioritu.

1. Služba **Adaptive QoS (Adaptivní QoS)** zajišťuje šířku pásma příchozích a odchozích kabelových i bezdrátových připojení především pro prioritní aplikace a úlohy prostřednictvím předdefinovaných předvoleb a předvoleb přetažení: hry, streamování médií, VoIP, procházení webu a přenos souborů.
2. **Traditional QoS** (**Tradiční QoS)** zajišťuje příchozí a odchozí šířku pásma na kabelových i bezdrátových připojeních pro prioritní aplikace a úkoly pomocí ručně definovaných parametrů.
3. **Bandwidth Limiter** (**Omezovač šířky pásma)** umožňuje nastavit limity rychlosti stahování a odesílání.



3.1.3 Historie webu

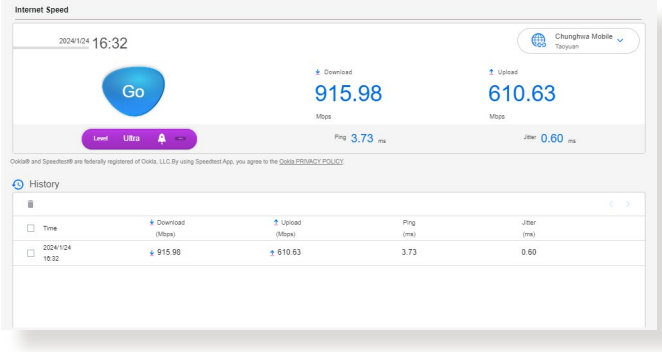
Web History (**Historie webu)** zobrazuje historii procházení webu klientů.



3.1.4 Rychlost internetu

Tuto službu poskytuje Ookla®. Detekuje rychlost stahování a odesílání z vašeho routeru do internetu.

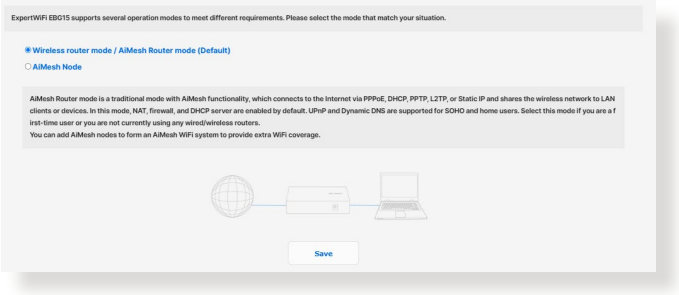
Kliknutím na **GO (PŘEJÍT)** spustíte test rychlosti internetu, jehož dokončení trvá přibližně jednu minutu.



3.2 Správa

3.2.1 Provozní režim

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



Pokyny pro nastavení provozního režimu:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Administration (Správa)** > **Operation Mode (Provozní režim)**.
2. Vyberte některý z těchto provozních režimů:
   - **Wireless router mode / AiMesh Router mode (default) (Režim bezdrátového směrovače / Režim AiMesh Router (výchozí))**: AiMesh Router je tradiční režim s funkcí AiMesh , který se připojuje k internetu přes PPPoE, DHCP, PPTP, L2TP nebo statickou IP a sdílí bezdrátovou síť s LAN klienty nebo zařízeními. V tomto režimu je ve výchozím nastavení povolen překlad adres NAT, brána firewall a server DHCP. UPnP a dynamický server DNS jsou podporovány pro uživatele SOHO a domácí uživatele.
   - **AiMesh Node (Uzel AiMesh)**: Můžete přidat uzly AiMesh a vytvořit tak AiMesh WiFi systém pro dodatečné pokrytí WiFi.
3. Klepněte na **Save (Uložit)**.

POZNÁMKA: Při změně režimů se směrovač restartuje.

3.2.2 Systém

Na stránce **System (Systém)** lze konfigurovat nastavení drátový router.

Pokyny pro provádění systémových nastavení:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Administration (Správa)** > **System (Systém)**.
2. Můžete konfigurovat následující nastavení:
   - **Změnit heslo pro přihlášení ke směrovači**: Můžete změnit heslo a jméno pro přihlášení k drátový router; zadejte nové jméno a heslo.
   - **USB Setting (Nastavení USB)**: Můžete povolit hibernaci pevného disku a změnit režim USB.
   - **Časové pásmo**: Vyberte časové pásmo vaší sítě.
   - **Server NTP**: Drátový router může přistupovat k serveru NTP (Network time Protocol) a synchronizovat čas.
   - **Network Monitoring (Sledování sítě)**: Můžete povolit dotazování DNS pro kontrolu převodu názvů hostitele a převedených IP adres nebo povolit ping a potom zkontrolovat cíl pingu.
   - **Auto Logout (Automatické odhlášení)**: Můžete nastavit dobu pro automatické odhlášení.
   - **Enable WAN down browser redirect notice (Povolit upozornění prohlížeče na přesměrování při ztrátě připojení)**: Tato funkce umožňuje prohlížeči zobrazit stránku s varováním, když směrovač není připojen k internetu. Když je funkce vypnutá, stránka s varováním se nezobrazí.
   - **Povolit Telnet**: Klepnutím na **Yes (Ano)** povolíte služby Telnet v síti. Klepnutím na **No (Ne)** zakážete Telnet.
   - **Metoda ověřování**: Pro zajištění přístupu ke směrovači můžete vybrat protokol HTTP, HTTPS nebo oba.
   - **Enable Reboot Scheduler (Povolit plán restartování)**: Když je možnost aktivní, můžete nastavit datum a čas pro restartování.
   - **Povolit přístup k síti z WAN**: Výběrem **Yes (Ano)** povolíte zařízením mimo síť přístup k nastavení GUI drátový router. Výběrem možnosti **No (Ne)** zakážete přístup.
   - **Enable Access Restrictions (Aktivovat omezení přístupu)**: Chcete-li určit adresy IP zařízení, která mají povolen přístup k nastavení GUI drátový router ze sítě WAN/LAN.

- **Service (Služba):** Tato funkce umožňuje nakonfigurovat možnosti Enable Telnet (Povolit telnet) / Enable SSH (Povolit SSH) / SSH Port / Allow Password Login (Povolit přihlášení s heslem) / Authorized Keys (Oprávněné klíče) / Idle Timeout (Časový limit nečinnosti).

3. Klepněte na **Apply (Použít)**.

3.2.3 Upgradování firmwaru

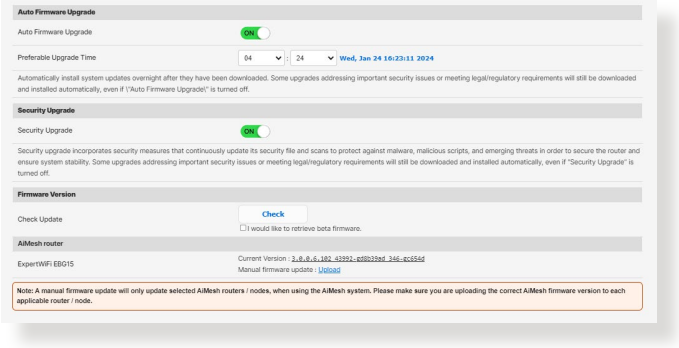
POZNÁMKA: Stáhněte nejaktuálnější firmware z webu společnosti ASUS na adrese **http://www.asus.com.**

Pokyny pro upgradování firmwaru:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Administration (Správa)** > **Firmware Upgrade (Upgrade firmwaru)**.
2. V poli **New Firmware File (Nový soubor firmwaru)** klepněte na **Browse (Procházet)** 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, drátový routerč přejde automaticky do nouzového nebo chybového režimu a indikátor LED napájení na předním panelu pomalu bliká.

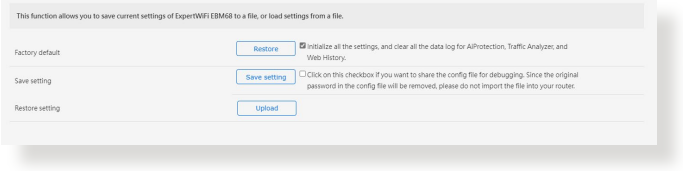


3.2.4 Obnovení/Uložení/Odeslání nastavení

Pokyny pro obnovení/uložení/odeslání drátový router nastavení:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/uložit/načíst nastavení)**.
2. Vyberte úlohy, které chcete provést:
   - **Factory default** (**Výchozí tovární nastavení)**: Inicializujte všechna nastavení a vymažte všechny datové protokoly pro AiProtection, Analyzátor provozu a Historie webu.
   - **Save setting** (**Uložit nastavení)**: Klikněte na toto zaškrtávací políčko, pokud chcete sdílet konfigurační soubor pro ladění. Neimportujte soubor do routeru, protože původní heslo v konfiguračním souboru bude odstraněno.
   - **Restore setting** (**Obnovit nastavení)**: Odešle nastavení obnovy, které chcete použít.

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



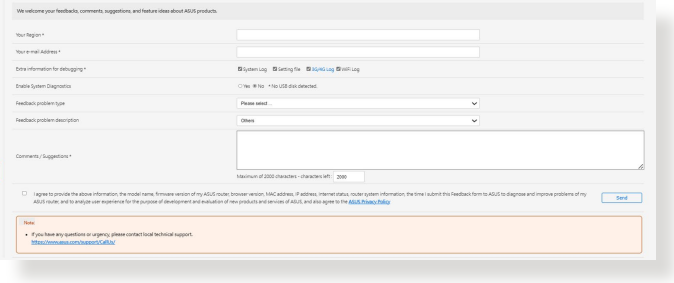
3.2.5 Zpětná vazba

Pokyny pro použití zpětné vazby:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Administration (Správa)** > **Feedback (Zpětná vazba)**.
2. Zadejte váš region, e-mailovou adresu, další informace pro ladění, komentáře a návrhy a odešlete protokol routeru zpět k řešení problémů.

DŮLEŽITÉ!

- Popište podrobně své komentáře k situaci, abyste získali rychlou odpověď.
- Přijměte Zásady ochrany osobních údajů ASUS.



3.2.6 Soukromí

1. Pro vazbu účtu, DDNS a vzdálené připojení (aplikace ASUS Router / aplikace Lyra / AiCloud / AiDisk):

Vezměte na vědomí, že prostřednictvím výše uvedených funkcí bude společnost shromažďovat vaše údaje, včetně názvu modelu vašeho produktu, verze firmwaru, stavu internetu, IP adresy, MAC adresy a názvu DDNS.

Pokud chcete zakázat sdílení vašich informací se společností ASUS prostřednictvím výše uvedených funkcí, klikněte níže na **Withdraw** (**Odvolat)**. Upozorňujeme však, že tyto vlastnosti/ funkce nemusí fungovat, pokud přestanete sdílet své informace se společností ASUS.

DŮLEŽITÉ!

- Po kliknutí na **Withdraw (Odvolat)** dojde k některým změnám, jak je uvedeno níže:
  - Název DDNS, který aktuálně používáte, nebude ve vašem routeru uložen.
  - Aplikaci ASUS Router, aplikaci Lyra, AiCloud, AiDisk lze používat pouze v případě, že je vaše zařízení ve stejné síti LAN jako router.

2. Upozornění OCHRANA OSOBNÍCH ÚDAJŮ SPOLEČNOSTI ASUS (pro upgrade firmwaru/zabezpečení):

Vezměte na vědomí, že router ASUS bude shromažďovat vaše údaje pro účely aktualizace firmwaru/zabezpečení. Pokud chcete zakázat sdílení vašich informací s routerem ASUS, klikněte níže na **Withdraw (Odvolat)**.

DŮLEŽITÉ! Kliknutím na **Withdraw (Odvolat)** zde může dojít k selhání upgradu na nejnovější firmware a získání nejaktuálnější ochrany vašeho routeru ASUS. Pro ochranu zabezpečení vašeho routeru a zajištění souladu se zákony se však aktualizace řešící důležité bezpečnostní problémy nebo splňující zákonné/regulační požadavky budou i nadále stahovat a instalovat automaticky.

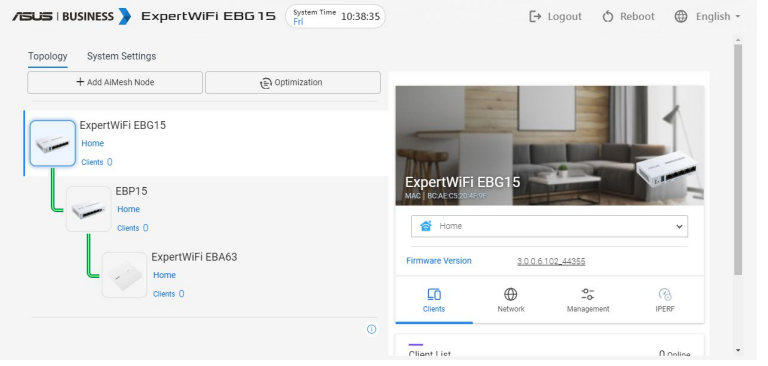
3.3 AiMesh

3.3.1 Nastavení systému ExpertWiFi AiMesh

Chcete-li vybudovat systém ExpertWiFi AiMesh, musíte nakonfigurovat jeho nastavení.

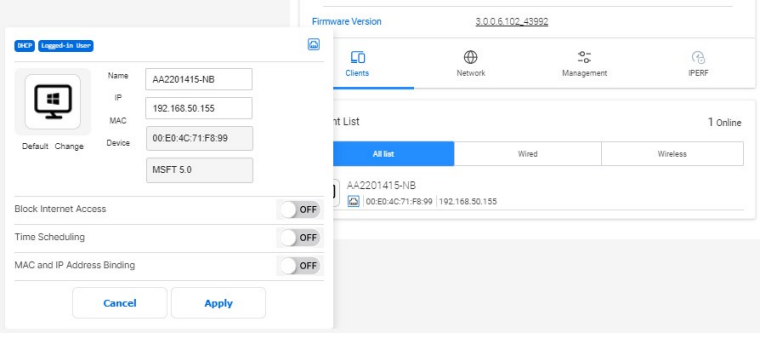
Pokyny pro nastavení systému ExpertWiFi AiMesh:

1. Z navigačního panelu přejděte na **AiMesh** > **Topology (Topologie)**.
2. Klepnutím na spodní část **Set up as AiMesh Node (Nastavit jako uzel AiMesh)** můžete přidat zařízení ExpertWiFi pod kontrolou EBG15.



3. Přejděte na **AiMesh** > **System Settings** (**Nastavení systému)** a povolte nebo zakažte **AiMesh node Ethernet auto setup (Automatické nastavení ethernetového uzlu AiMesh)**, **Ethernet Backhaul Mode (Režim Ethernet Backhaul)**, nakonfigurujte **Roaming Block List (Seznam roamingových bloků)**, **System Reset to Factory Default (Obnovení výchozího továrního nastavení systému)** nebo **System Reset (Obnovení systému)**.

3.3.2 Správa síťových klientů

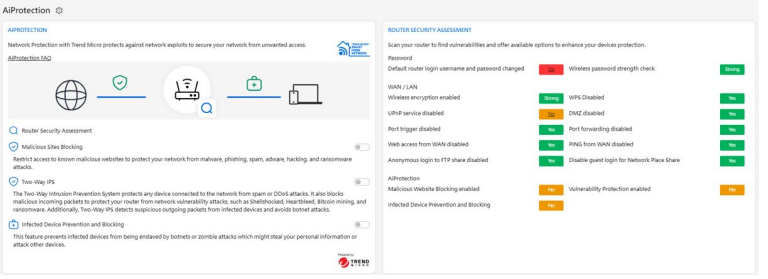


Pokyny pro správu síťových klientů:

1. Z navigačního panelu přejděte na **AiMesh** > **Topology (Topologie)**.
2. Výběrem ikony **Clients** (**Klienti)** zobrazíte informace o vašem síťovém klientovi, jako je jméno klienta, MAC a IP adresa.
3. Přemístěním posuvníku do polohy **OFF** (**VYPNUTO)** lze zablokovat přístup klienta k vaší síti, zakázat jeho časové plánování nebo deaktivovat vazbu MAC a IP.
4. Po dokončení klepněte na tlačítko **Apply (Použít)**.

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.

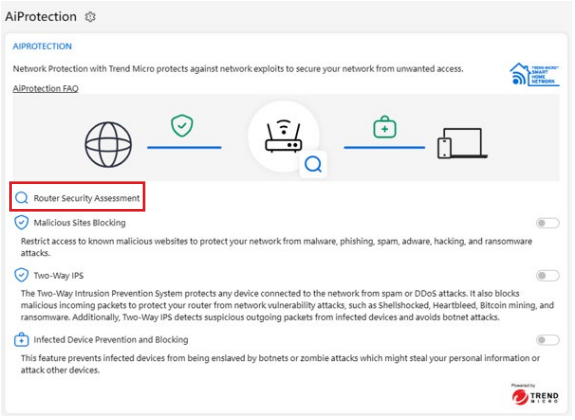


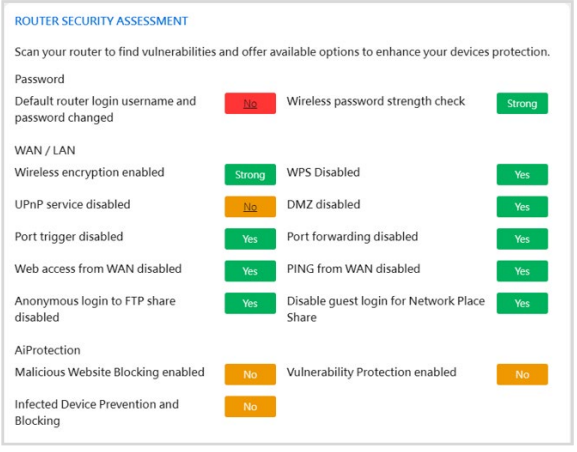
3.4.1 Ochrana sítě

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

Pokyny pro posouzení zabezpečení routeru:

1. Na navigačním panelu přejděte na **AiProtection**.
2. Kliknutím na **Router Security Assessment** (**Posouzení zabezpečení routeru)** zobrazíte výsledky posouzení zabezpečení.





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)** se důrazně doporučuje provést příslušnou konfiguraci.

3. (Volitelně) Na stránce **ROUTER SECURITY ASSESSMENT (VYHODNOCENÍ ZABEZPEČENÍ SMĚROVAČE)** ručně nakonfigurujte položky označení **No (Ne)**. 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.

4. Chcete-li, aby byla nastavení zabezpečení provedena automaticky, klepněte na **Secure Your Router (Zabezpečit směrovač).**

5. Po zobrazení zprávy s výzvou klepněte na **OK.**

Pokyny pro aktivaci ochrany sítě:

1. Na navigačním panelu přejděte na **AiProtection**.

2. Vyberte typ ochrany, kterou chcete implementovat, a přemístěte posuvník. Můžete si vybrat možností **Malicious Sites Blocking (Blokování škodlivých webů)**, **Two-Way IPS (Obousměrné IPS)** a **Infected Device Prevention and Blocking (Prevence a blokování infikovaných zařízení)**.

   #### Blokování škodlivých webů

   Tato funkce omezuje přístup ke známým škodlivým webům a chrání vaši síť před malwarem, phishingem, spamem, adwarem, hackerskými útoky a útoky ransomwaru.

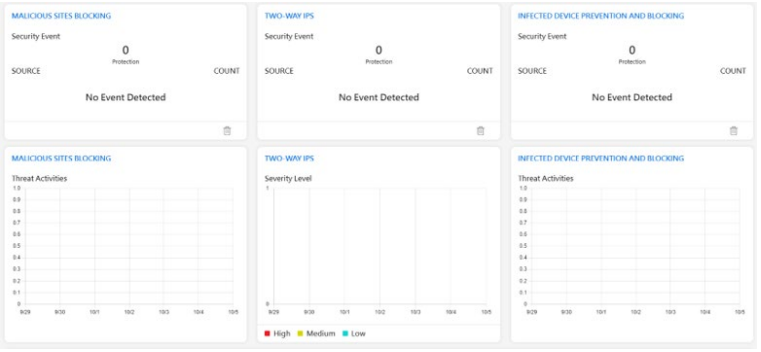
   #### Obousměrné IPS

   Obousměrné IPS (Intrusion Prevention System) chrání připojená zařízení před spamem nebo DDoS útoky. Blokuje také škodlivé příchozí pakety, aby chránil váš router před útoky na zranitelnost sítě, jako je Shellshocked , Heartbleed, těžba bitcoinů a ransomware. Obousměrné IPS navíc detekuje podezřelé odchozí pakety z infikovaných zařízení a vyhýbá se útokům botnetů.

   #### Prevence a blokování infikovaných zařízení

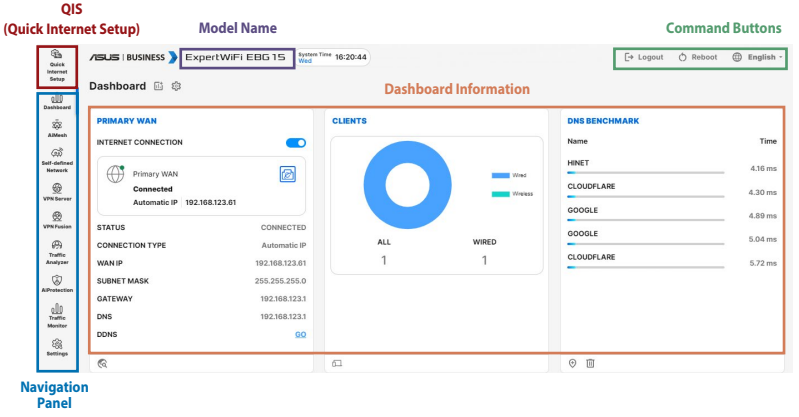
   Tato funkce zabraňuje ovládnutí infikovaných zařízení botnety nebo útoky zombie, které by mohly odcizit vaše osobní údaje nebo zaútočit na jiná zařízení.

3. Přijměte **Trend Micro End User License Agreement (Licenční ujednání společnosti Trend Micro s koncovým uživatelem)**.


MALICIOUS SITES BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
TWO-WAY IPS
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
INFECTED DEVICE PREVENTION AND BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
MALICIOUS SITES BLOCKING
Threat Activities
TWO-WAY IPS
Severity Level
High
Medium
Low
INFECTED DEVICE PREVENTION AND BLOCKING
Threat Activities

3.5 Ovládací panel

Ovládací panel umožňuje spravovat síť, jako je připojení k internetu, připojení klienta, benchmark DNS, stav systému, ethernetový port a sledování provozu.



3.6 Řízení přístupu k zařízení

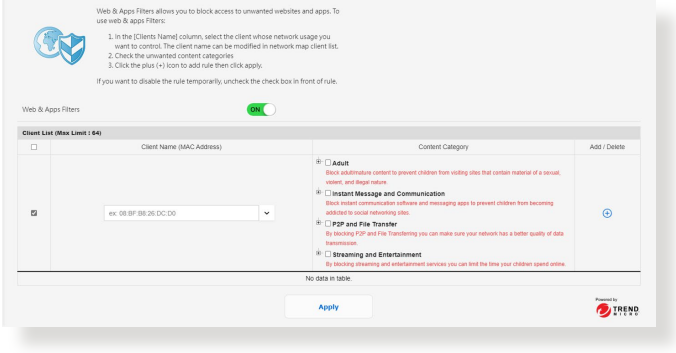
3.6.1 Filtrace webů a aplikací

Filtry webu a aplikací umožňují blokování přístupu k nežádoucím webům a aplikacím.

Pokyny pro používání filtrů webu a aplikací:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Device access control (Řízení přístupu k zařízení)** > **Web & Apps Filters (Filtrace webů a aplikací)**.
2. Posunutím posuvníku do polohy **ON** (**ZAPNUTO)** aktivujte **Web & Apps Filters (Filtrace webů a aplikací)**.
3. Ve sloupci **Client Name (Jméno klienta)** vyberte klienta, u kterého chcete řídit využití sítě. Název klienta lze upravit v seznamu klientů v mapě sítě.
4. Zaškrtněte kategorie nežádoucího obsahu.
5. Kliknutím na ⊕ přidejte pravidlo a klikněte na **Apply (Použít)**.

Pokud chcete pravidlo dočasně zakázat, zrušte zaškrtnutí pravidla.

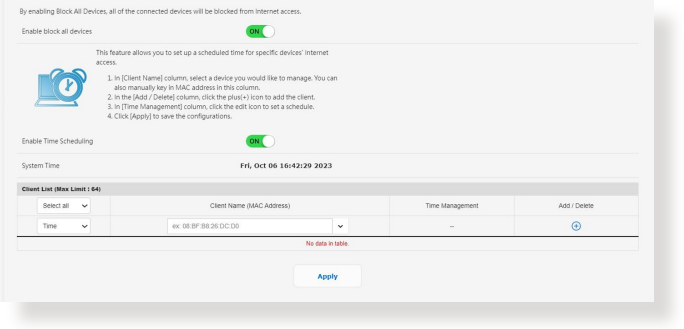


3.6.2 Časové plánování

Časové plánování vám umožňuje nastavit naplánovaný čas pro přístup konkrétních zařízení k internetu.

Pokyny pro používání časového plánování:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Device access control (Řízení přístupu k zařízení)** > **Time Scheduling (Časové plánování)**.
2. Posunutím posuvníku do polohy **ON** (**ZAPNUTO)** aktivujte **Enable Time Scheduling (Aktivovat časové plánování)**.
3. Ve sloupci **Client Name (Název klienta)** vyberte nebo zadejte název klienta z rozevíracího seznamu.
4. Kliknutím ⊕ přidejte profil klienta.
5. Kliknutím na tlačítko **Apply (Použít)** uložte nastavení.



3.7 Brána firewall

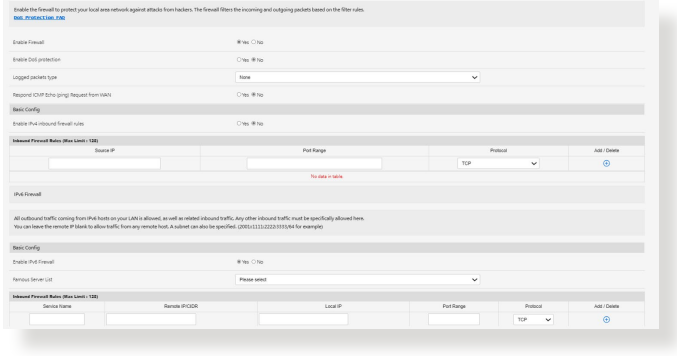
3.7.1 Obecné

Tento drátový router může fungovat jako hardwarová brána firewall pro vaši síť.

POZNÁMKA: Funkce brány firewall je ve výchozí konfiguraci aktivována.

Pokyny pro základní nastavení brány firewall:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Firewall (Brána firewall)** > **General (Obecné)**.
2. V poli **Enable Firewall (Aktivovat bránu firewall)** vyberte **Yes (Ano)**.
3. V části **Enable DoS (Aktivovat ochranu DoS)** ochranu 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)**.



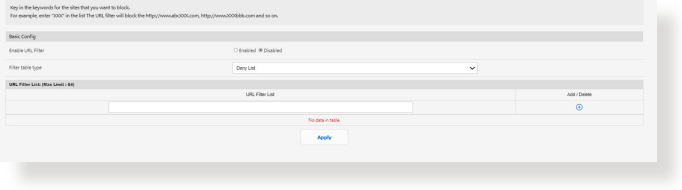
3.7.2 Filtr URL

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 **Settings (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)**.



3.7.3 Filtr klíčových slov

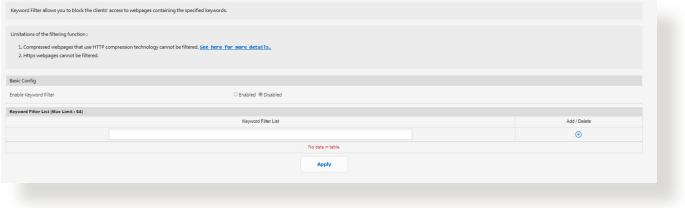
Filtr klíčových slov blokuje přístup k webovým stránkám, které obsahují určená klíčová slova.

Pokyny pro nastavení filtru klíčových slov:

1. Na navigačním panelu přejděte na **Settings (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 ⊕.
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.

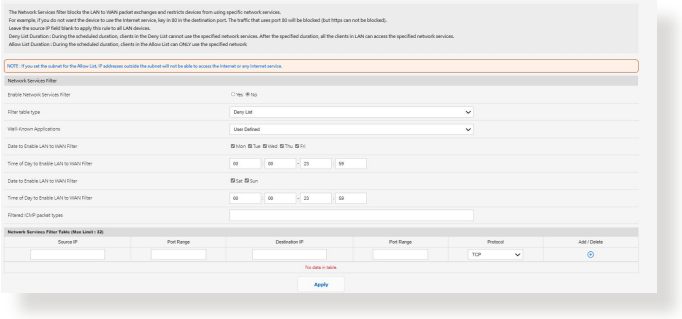


3.7.4 Filtr síťových služeb

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.

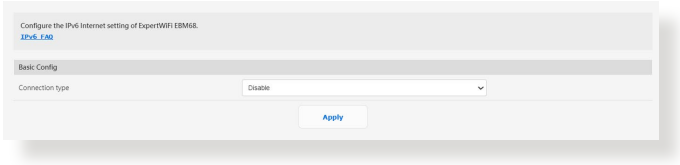
Pokyny pro nastavení filtru síťových služeb:

1. Na navigačním panelu přejděte na **Settings (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 List (Seznam odmítnutých)** blokuje specifikované síťové služby. **Allow List (Seznam povolených)** 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)**.



3.8 IPv6

Tento drátový router podporuje adresování IPv6, systém, který podporuje více adres IP. Zeptejte se vašeho ISP, zda jeho internetové služby podporují IPv6.



Pokyny pro nastavení IPv6:

1. Na navigačním panelu přejděte na **Settings (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)**.

POZNÁMKY:

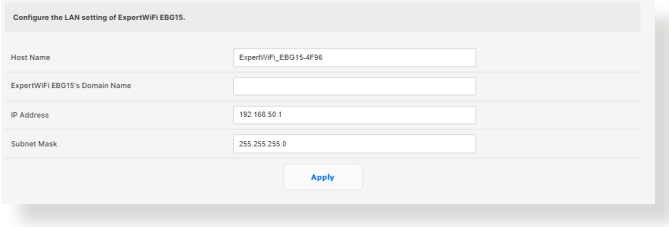
- Specifické informace IPv6 pro vaše internetové služby vám poskytne váš ISP.
- Další informace najdete na https://www.asus.com/support/FAQ/113990.

3.9 LAN

3.9.1 LAN IP

Na obrazovce LAN IP lze upravit nastavení LAN IP drátový router.

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

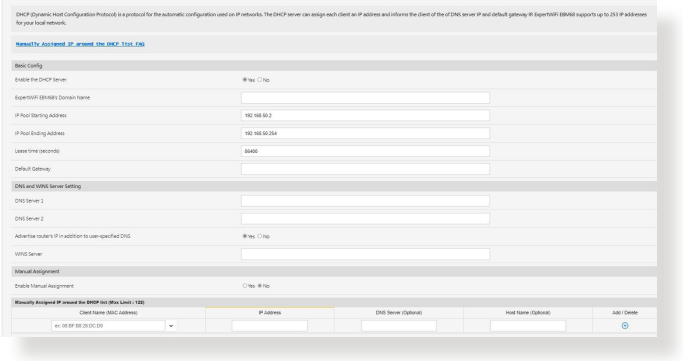


Pokyny pro úpravy nastavení LAN IP:

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

3.9.2 Server DHCP

DHCP (Dynamic Host Configuration Protocol) je protokol pro automatickou konfiguraci používaný v sítích IP. Server DHCP může přiřadit jednotlivým klientům IP adresu a informovat klienta o IP adrese serveru DNS a IP adrese výchozí brány.



Pokyny pro konfiguraci serveru DHCP:

1. Na navigačním panelu, přejděte na **Settings (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 drátový router.
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.

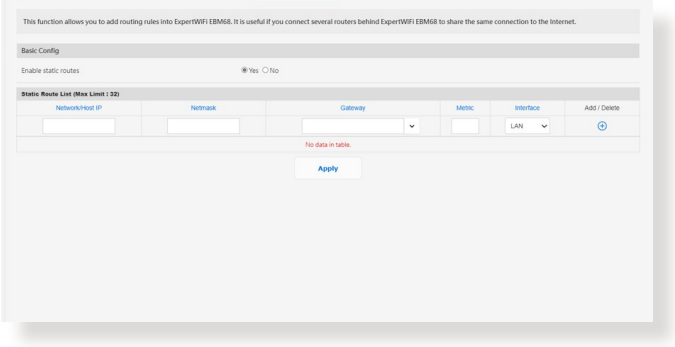
POZNÁMKY:

- Doporučujeme při určování rozsahu adres IP používat formát adresy IP 192.168.1.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 Server Settings (Nastavení DNS a serveru)** zadejte adresu IP serveru DNS a serveru WINS.
8. Tento drátový router 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.

3.9.3 Trasa

Tato funkce umožňuje přidávat pravidla směrování do routeru. To je užitečné, jestliže za zařízení EBG15 připojíte několik routerů, které sdílejí stejné připojení k Internetu.

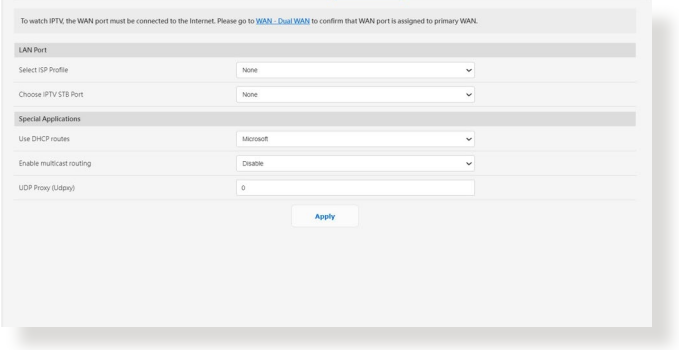


Pokyny pro konfigurování tabulky směrování LAN:

1. Na navigačním panelu přejděte na **Settings (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 ⊕ nebo ⊖ přidejte nebo odstraňte zařízení ze seznamu.
4. Klepněte na **Apply (Použít)**.

3.9.4 IPTV

Tento drátový router 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.

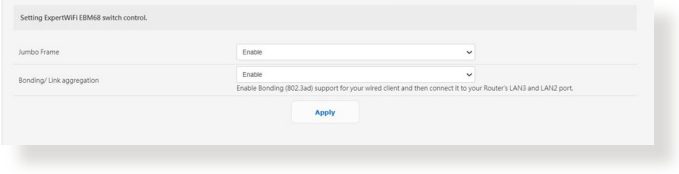


3.9.5 Ovládání přepínání

Umožňuje nastavit router pro funkci ovládání přepínačů. Můžete zkombinovat dva 1Gbps LAN porty a poskytovat až 2Gbps kabelové rychlosti prostřednictvím propojení s vaším kompatibilním NAS nebo jiným širokopásmovým síťovým zařízením.

POZNÁMKY:

- Chcete-li používat funkci Link Aggregation Control Protocol (LACP), musí zařízení podporovat protokol IEEE 802.3ad.
- Funkci agregace LAN lze provozovat spárováním portu LAN3 s portem LAN2.

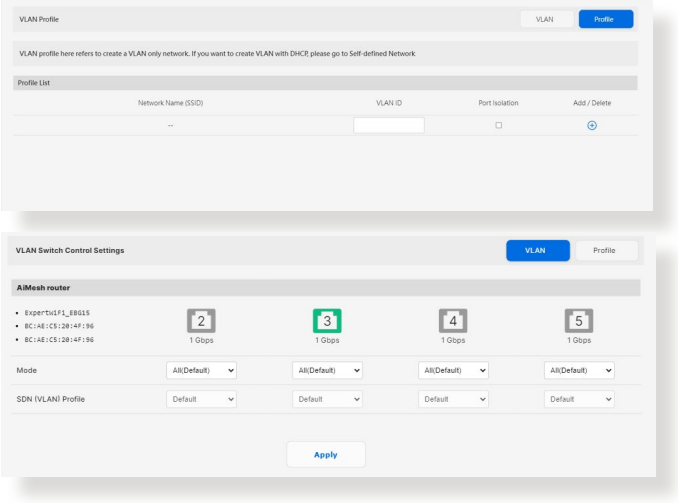


3.9.6 VLAN

VLAN (Virtual Local Area Network) je logická síť vytvořená v rámci větší fyzické sítě. VLAN vám umožňují segmentovat síť na menší, virtuální podsítě, které lze použít k izolaci provozu a zlepšení výkonu sítě.

Pokyny pro nastavení VLAN:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **LAN** > **VLAN**.
2. Klikněte na kartu **Profile** (**Profil)** a potom kliknutím na ⊕ vytvořte profil VLAN. Můžete přiřadit své vlastní VLAN ID.
3. **Port isolation** (**Izolace portů)** omezuje přístupová práva různých zařízení ve stejné VLAN . Nyní vytváříte „VLAN-only-Network“, což znamená síť s VID, ale bez DHCP.



4. Klikněte na kartu **VLAN** a vyberte port se specifickým profilem a režimem (**Trunk** / **Access**) **(Sloučení / Přístup)**.

POZNÁMKA: Můžete vybrat jeden z následujících výchozích režimů:

All (Default) (**Vše (výchozí))** umožňuje přístup všem označeným a neoznačeným paketům.

Režim **Access** (**Přístup)** umožňuje přístup k vybrané síti SDN (VLAN). Můžete si vybrat profily vytvořené pomocí Guest Network pro nebo pomocí VLAN.

Režim **Trunk (Sloužení)**:

- **Allow all tagged (Povolit vše označené):** Přístup mají pouze označené pakety.
- **With selected SDN (VLAN) (S vybranou SDN (VLAN)):** Přístup je povolen pouze vybraným SDN nebo VLAN.

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

POZNÁMKA: Další informace najdete na https://www.asus.com/support/FAQ/1049415/.

3.10 Síťové nástroje

Chcete-li použít síťové nástroje, přejděte na navigačním panelu na **Settings (Nastavení)** > **Network Tools (Síťové nástroje)**.

3.10.1 Síťová analýza

Odešle pakety ICMP ECHO_REQUEST síťovým hostitelům.

3.10.2 Netstat

Zobrazí podrobnosti sítě.

3.10.3 Wake on LAN

Funkce WOL (Wake-On-LAN) umožňuje probudit počítač z jakéhokoli zařízení v síti.

3.10.4 Pravidlo chytrého připojení

Nakonfigurujte informace, které souvisí s chytrým připojením.

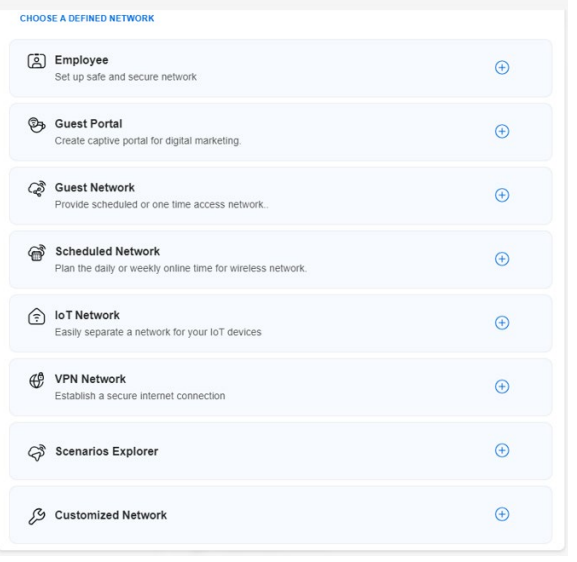
3.11 Vlastní definovaná síť

Self-Defined Network (SDN) poskytuje až pět SSID k oddělení a upřednostnění zařízení pro různé obchodní použití a síťové alternativy, vytváří síťové segmenty pro zaměstnance, portály pro hosty, sítě pro hosty, plánované sítě, sítě IoT a sítě VPN.

DŮLEŽITÉ! Chcete-li zpřístupnit funkci Wi-Fi, zajistěte integraci bezdrátového přístupového bodu (AP), jako je ExpertWiFi EBA63 nebo router, jako je ExpertWiFi EBR63 nebo ExpertWiFi EBM68, do sítě AiMesh EBG15.

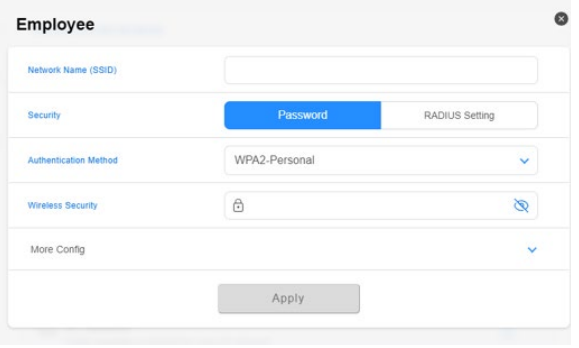
Pokyny pro vytvoření vlastní definované sítě:

1. Na navigačním panelu přejděte na **Self-Defined Network (Vlastní definovaná síť)**.
2. Vyberte definovanou síť, která vyhovuje vašemu konkrétnímu scénáři.



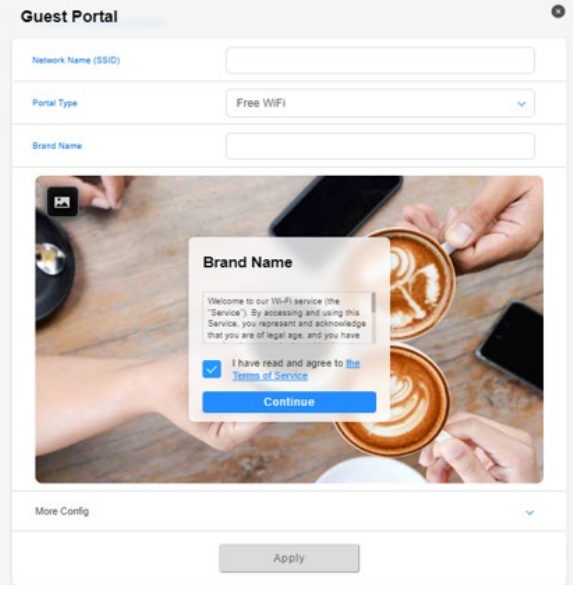
3.11.1 Zaměstnanec

Umožňuje nastavit úroveň přístupu pro různá použití pro zvýšení zabezpečení sítě. Doporučeno pro kanceláře, které přidělují oprávnění různým oddělením.



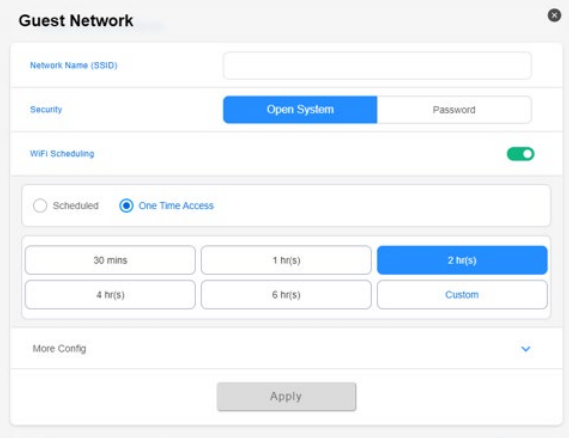
3.11.2 Portál pro hosty

Umožňuje vám vytvořit portál pro hosty pro digitální marketing. Doporučeno pro použití v restauracích, hotelech nebo pojízdných kuchyních.



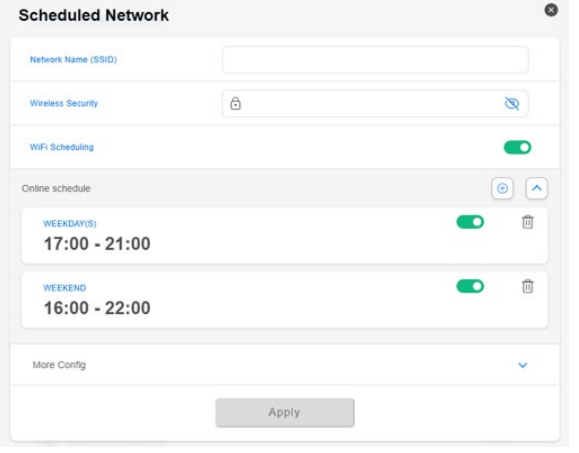
3.11.3 Síť pro hosty

Poskytuje dočasným návštěvníkům plánovaný nebo jednorázový přístup k síti. Doporučeno pro použití v nákupních centrech, tělocvičnách nebo pro návštěvníky.



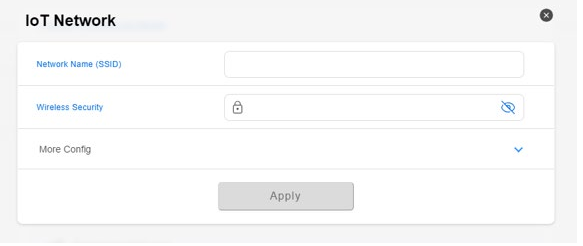
3.11.4 Plánovaná síť

Plánuje denní nebo týdenní online čas pro bezdrátovou síť. Doporučeno pro dálkové studium, použití ve třídě nebo pro děti.



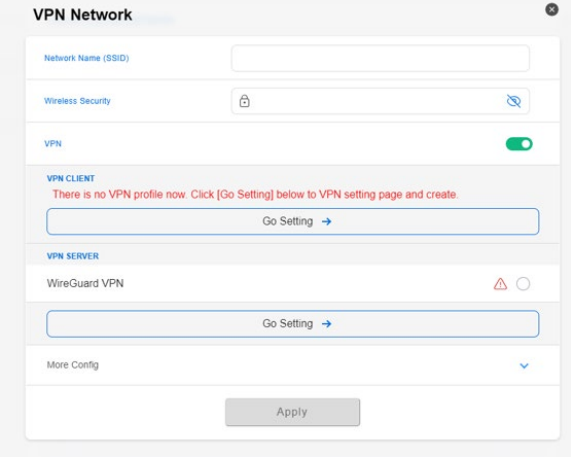
3.11.5 Síť IoT

Umožňuje snadno nastavit samostatnou síť pro zařízení IoT. Doporučeno pro použití se sledovacími zařízeními, hlasovými asistenty, osvětlením, kamerami na zvonky, chytrými zámky a senzory.



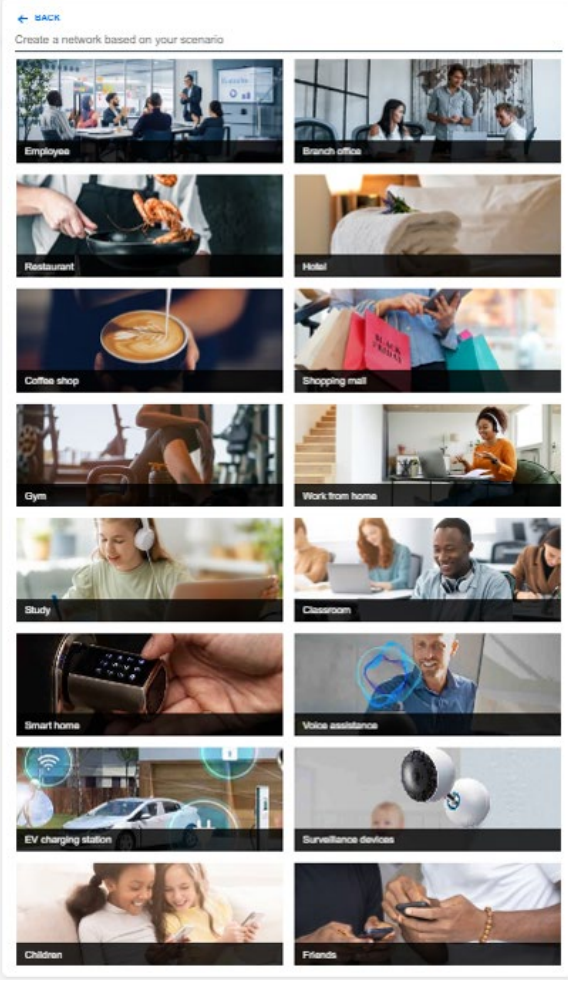
3.11.6 Síť VPN

Pomáhá vytvořit zabezpečené internetové připojení s použitím VPN.



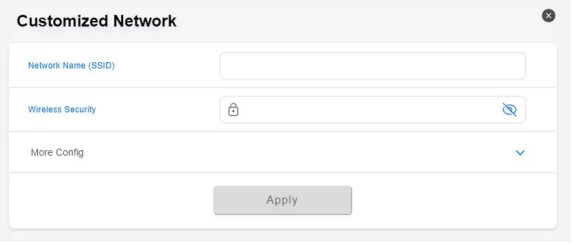
3.11.7 Nabídka situací

Pokud netušíte, jakou síť vytvořit, můžete si pro vytvoření sítě vybrat sektor, který odpovídá vaší příslušnosti.



3.11.8 Přizpůsobená síť

Umožňuje vybrat možnost přizpůsobené sítě.



3.12 Systémový protokol

Systémový protokol obsahuje záznam vašich síťových aktivit.

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

Pokyny pro zobrazení systémového protokolu:

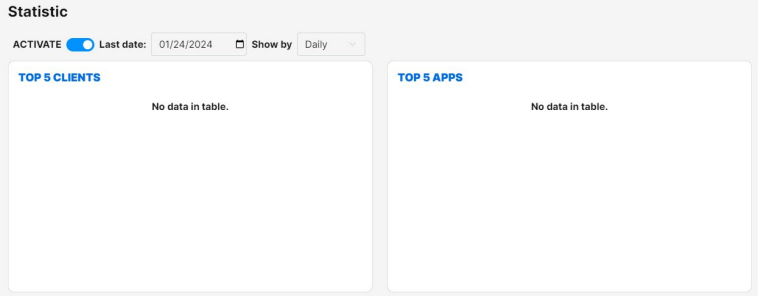
1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **System Log (Systémový protokol)**.
2. Můžete zobrazit vaše síťové aktivity na následujících kartách:
   - Obecný protokol
   - Zápůjčky DHCP
   - Předávání portů
   - Tabulka směrování
   - IPv6
   - Připojení

3.13 Sledování provozu

3.13.1 Analizor de trafic

Pokyny pro použití analyzátor provozu::

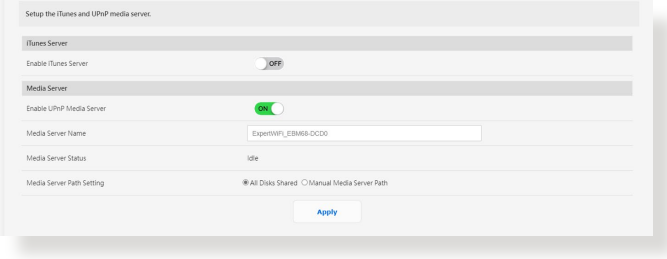
1. Zapněte **ACTIVATE (AKTIVOVAT)**.
2. Přiřaďte poslední datum k zobrazení a v rozevíracím seznamu **Show by (Zobrazit podle)** zvolte denní, týdenní nebo měsíční sledování síťového provozu.
3. Zobrazí se pět nejlepších klientů, pět nejlepších aplikací, zařízení, stav klienta a analýza aplikací.



3.14 USB Aplikace

3.14.1 Servery médií

Server médií umožňuje nastavit server iTunes a UPnP.



Chcete-li spustit stránku nastavení aplikace Media Server (Server médií), přejděte na **Settings (Nastavení)** > **USB Application (USB Aplikace)** > **Media Server (Servery médií)**.

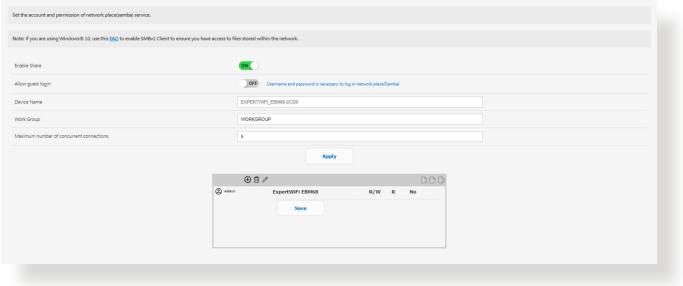
Níže je uveden popis jednotlivých polí:

- **Enable iTunes Server (Povolit server iTunes)**: Výběrem ON/OFF (ZAP./VYP.) povolte/ zakažte server iTunes.
- **Enable UPnP Media Server (Povolit mediální server UPnP)**: Výběrem ON/OFF (ZAP./VYP.) povolte/ zakažte mediální server UPnP.
- **Media Server Name** (**Název serveru médií)**: Slouží k zadání názvu serveru médií.
- **Media Server Path Setting (Nastavení umístění serveru médií):** Vyberte **All Disks Shared (Všechny disky sdílené)** nebo **Manual Media Server Path (Ruční zadání umístění serveru médií).**

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

3.14.2 Sdílené síťové místo (Samba)

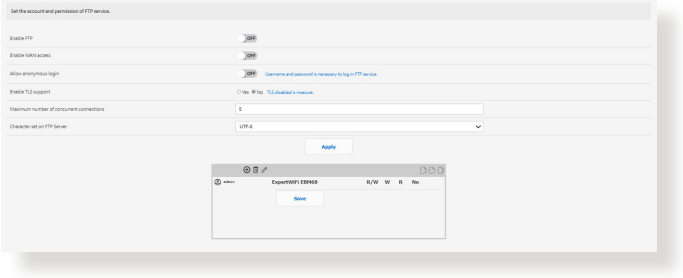
Služba sdílení místa v síti (Samba) umožňuje nastavit účet a oprávnění pro službu Samba.



Pokyny pro používání sdílení Samba, přejděte na **Settings (Nastavení)** > **USB Application (USB Aplikace)** > **Network Place (Samba) Share (Sdílené síťové místo (Samba))**.

3.14.3 Sdílení FTP

FTP Share umožňuje nastavit účty a oprávnění pro službu FTP.



Pokyny pro používání sdílení FTP, přejděte na **Settings (Nastavení)** > **USB Application (USB Aplikace)** > **FTP Share (Sdílení FTP)**.

3.14.4 Síťový tiskový server

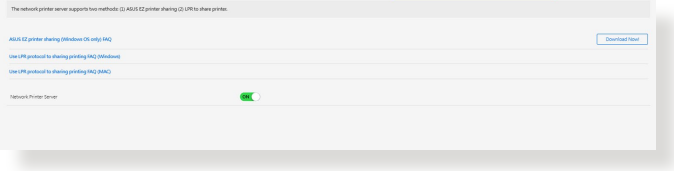
3.14.4.1 Sdílení tiskárny ASUS EZ

Nástroj ASUS EZ Printing Sharing (Sdílení tiskárny ASUS EZ) umožňuje připojit tiskárnu USB k portu USB drátový router a nakonfigurovat tiskový server. To umožňuje síťovým klientům bezdrátově tisknout a skenovat soubory.

POZNÁMKA: Funkci tiskového serveru podporuje operační systém Windows® 10 a Windows® 11.

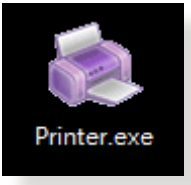
Pokyny pro nastavení režimu sdílení tiskárny EZ:

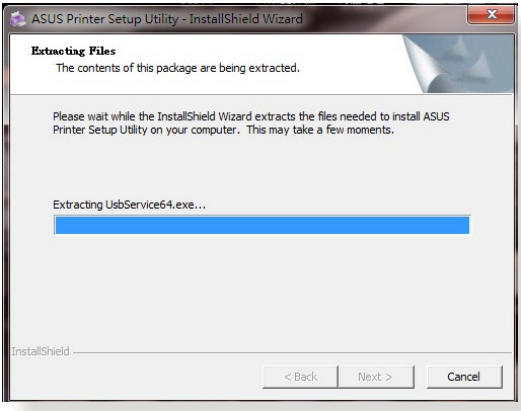
1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **USB Application (USB Aplikace)** > **Network Printer Server (Síťový tiskový server)**.
2. Klepnutím na **Download Now! (Stáhnout!)** stáhněte nástroj síťové tiskárny.



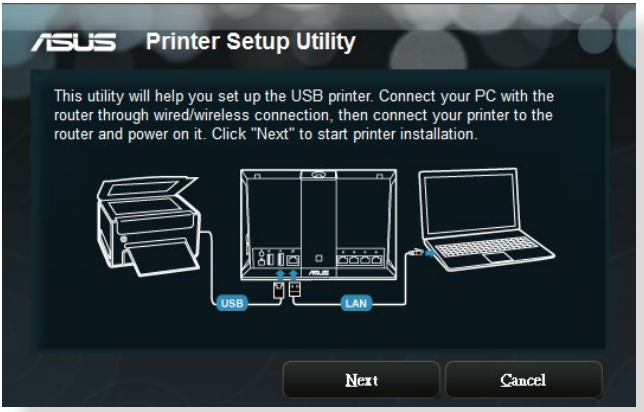
POZNÁMKA: Funkci síťové tiskárny podporují pouze operační systémy Windows® 10 a Windows® 11. Chcete-li nainstalovat tento nástroj v operačním systému Mac, vyberte **Use LPR protocol for sharing printer (Použít protokol LPR pro sdílení tiskárny)**.

3. Dekomprimujte stažený soubor a klepnutím na ikonu Printer (Tiskárna) spusťte instalační program síťové tiskárny.



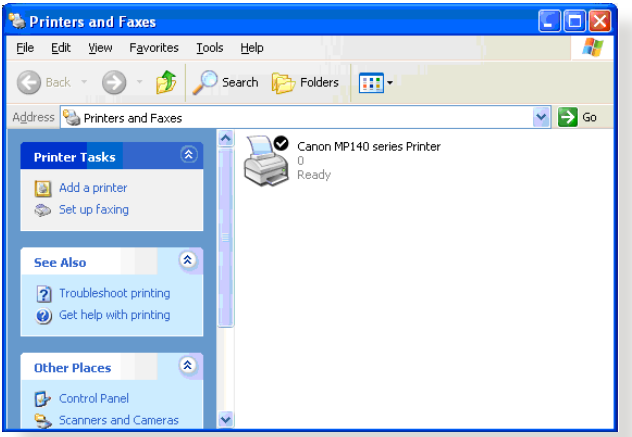


4. Nastavte heslo podle zobrazených pokynů a potom klepněte na tlačítko **Next (Další)**.



5. Počkejte několik minut na dokončení počáteční instalace. Klepněte na tlačítko **Next (Další)**.
6. Dokončete instalaci klepnutím na tlačítko **Finish (Dokončit)**.
7. Podle pokynů operačního sytému Windows® nainstalujte ovladač tiskárny.

8. Po dokončení instalace ovladače tiskárny mohou síťoví klienti používat tiskárnu.

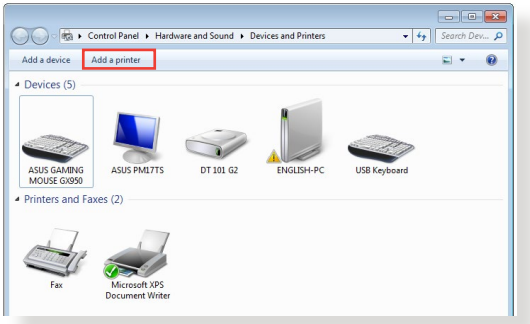


3.14.4.2 Použít protokol LPR pro sdílení tiskárny

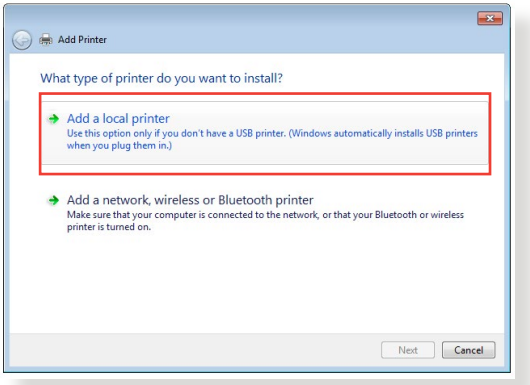
Vaši tiskárnu můžete sdílet s počítači s nainstalovanými operačními systémy Windows® a MAC pomocí LPR/LPD (Line Printer Remote/Line Printer Daemon).

Pokyny pro sdílení tiskárny LPR:

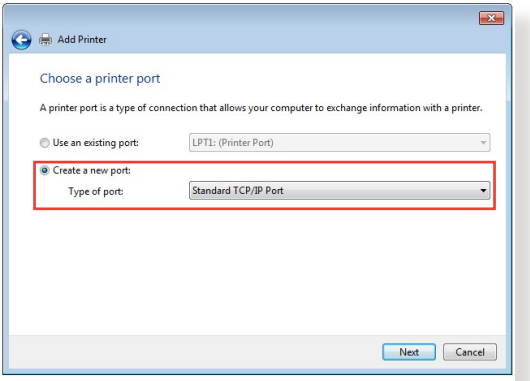
1. Na pracovní ploše operačního systému Windows® klepnutím na **Start** > **Devices and Printers (Zařízení a tiskárny)** > **Add a printer (Přidat tiskárnu)** spusťte **Add Printer Wizard (Průvodce přidáním tiskárny)**.



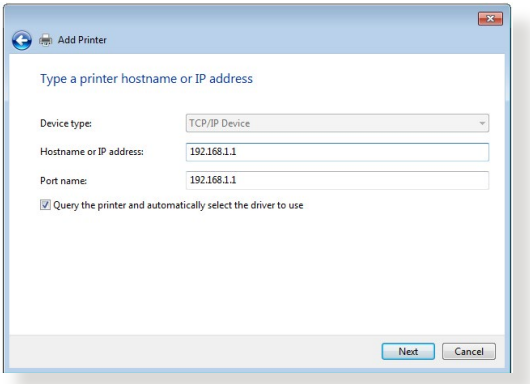
2. Vyberte položku **Add a local printer (Přidat místní tiskárnu)** a potom klepněte na tlačítko **Next (Další)**.



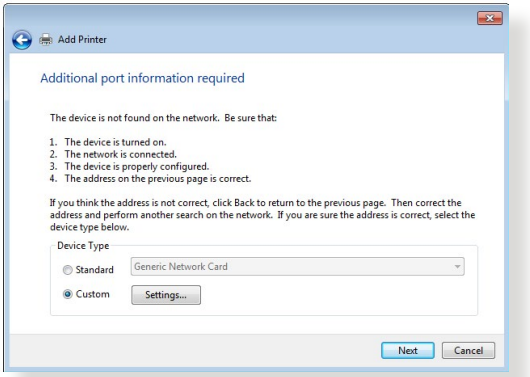
3. Vyberte možnost **Create a new port (Vytvořit nový port)** a potom nastavte položku **Type of Port (Typ portu)** na **Standard TCP/IP Port (Port standardu TCP/IP)**. Klepněte na tlačítko **New Port (Nový port)**.



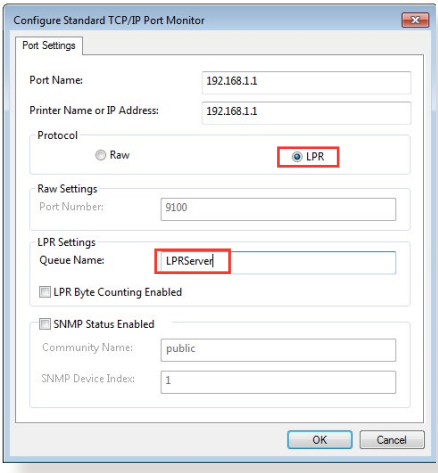
4. Do pole **Hostname or IP address (Název hostitele nebo adresa IP)** zadejte adresu IP drátový router a potom klepněte na tlačítko **Next (Další)**.



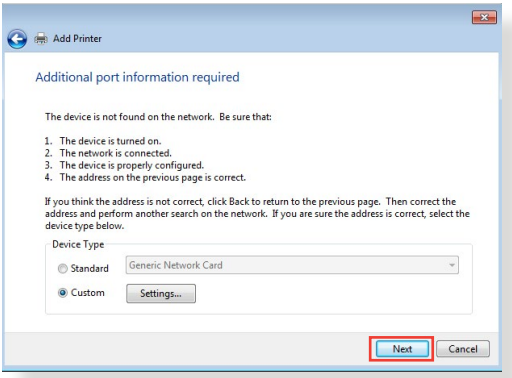
5. Vyberte položku **Custom (Vlastní)** a potom klepněte na **Settings (Nastavení)**.



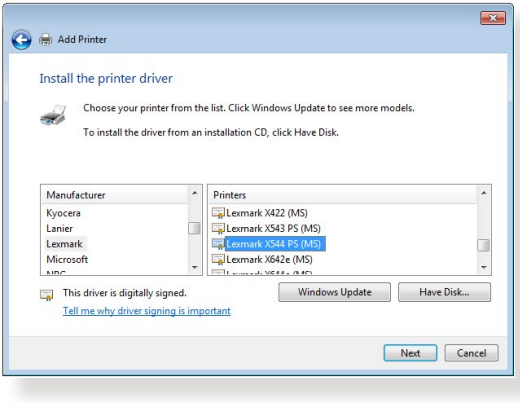
6. Nastavte položku **Protocol (Protokol)** na **LPR**. Do pole **Queue Name (Název fronty)** zadejte **LPRServer** a potom pokračujte klepnutím na tlačítko **OK**.



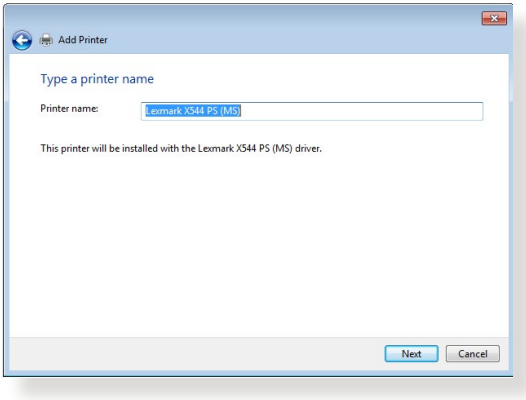
7. Klepnutím na tlačítko **Next (Další)** dokončíte nastavení portu standardu TCP/IP.



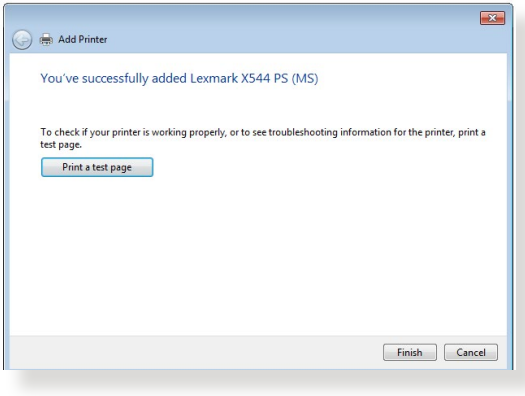
8. Nainstalujte ovladač tiskárny ze seznamu modelů výrobce. Pokud vaše tiskárna není uvedena v seznamu, klepnutím na tlačítko **Have Disk (Z diskety)** ručně nainstalujte ovladače tiskárny z disku CD-ROM nebo ze souboru.



9. Klepnutím na tlačítko **Next (Další)** použijete výchozí název tiskárny.



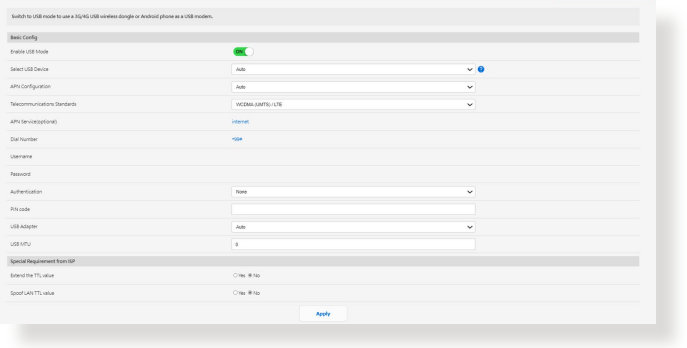
10. Klepnutím na tlačítko **Finish (Dokončit)** dokončete instalaci.



3.14.5 USB Modem

Přepne do režimu USB a použije 3G/4G USB bezdrátový klíč nebo telefon Android jako USB modem.

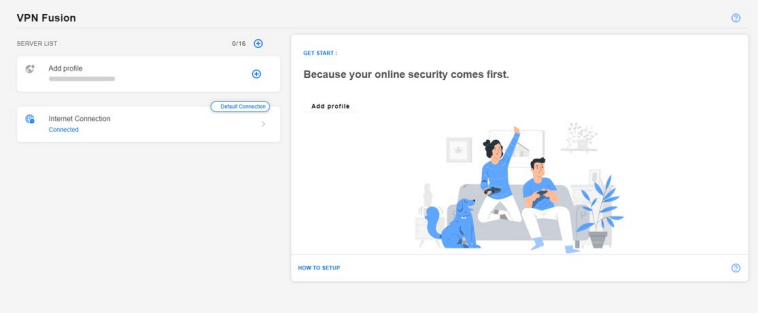
Chcete-li použít modem USB, přejděte na **Settings (Nastavení)** > **USB Application (Použití USB)** > **USB Modem**.



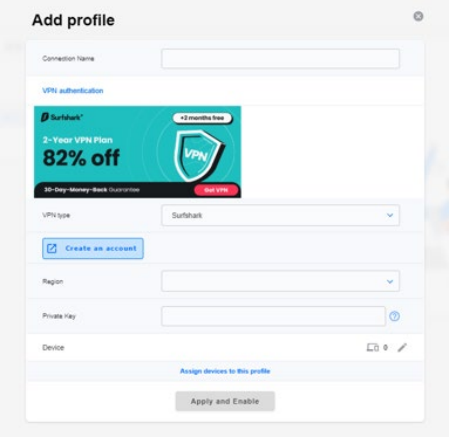
3.15 Spojení VPN

3.15.1 Vytvoření spojení VPN

Funkce VPN Fusion (Fúze VPN) umožňuje připojení k vícero serverům VPN současně a přiřazení zařízení pro připojení k různým tunelům VPN.

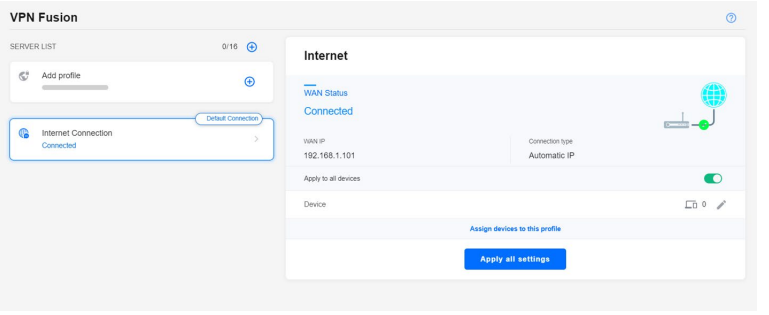


1. Z navigačního panelu přejděte na **VPN Fusion (Spojení VPN)**.
2. Kliknutím na ⊕ v poli **Add profile** (**Přidat profil)** nastavte nový tunel VPN.
3. Dokončete konfiguraci VPN včetně názvu připojení, typu VPN, oblasti, soukromého klíče a zařízení.
4. Klikněte na **Apply and Enable (Použít a aktivovat)**.



3.15.2 Internetové připojení

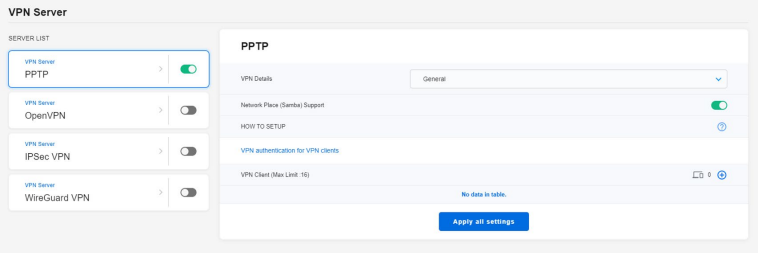
Umožňuje spravovat stav WAN připojených zařízení.



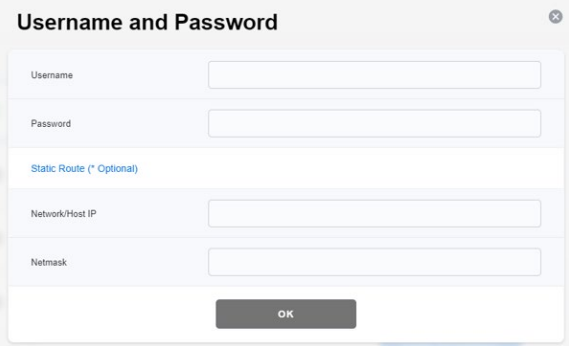
3.16 Server VPN

3.16.1 PPTP

1. Z navigačního panelu přejděte na **VPN Server (Server VPN)** > **PPTP** a posuňte posuvník doprava (ve výchozím nastavení je na levé straně vypnutý).
2. V poli **VPN Client (Max Limit: 16)** (**Klient VPN (max. limit: 16))** klikněte na ⊕ a přidejte účet.



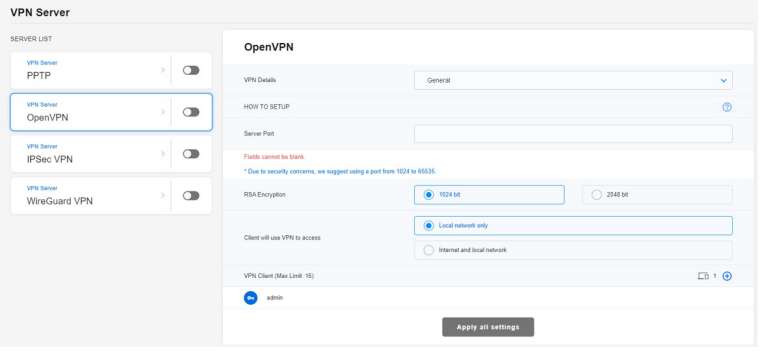
3. Zadejte vlastní [*Uživatelské jméno*] a [*Heslo*] a klikněte na **OK**.



POZNÁMKA: Nastavené *[Uživatelské jméno]* a *[Heslo]* nelze měnit. Další informace najdete na https://www.asus.com/support/FAQ/114892/.

3.16.2 OpenVPN

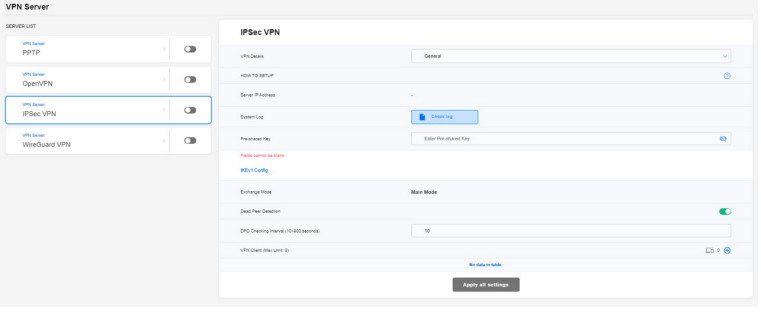
1. Z navigačního panelu přejděte na **VPN Server (Server VPN)** > **OpenVPN** a posuňte posuvník doprava (ve výchozím nastavení je na levé straně vypnutý).
2. Nakonfigurujte obecná nastavení v poli **VPN Details (Podrobnosti VPN)**.
3. Do prázdného sloupce zadejte vaše uživatelské jméno a heslo.
4. V poli **VPN Client (Max Limit: 16)** (**Klient VPN (max. limit: 16))** klikněte na ⊕ a přidejte účet.
5. Heslo je automaticky skryto. Klikněte na **Apply all settings (Použít všechna nastavení)**.



POZNÁMKA: Další informace najdete na https://www.asus.com/support/FAQ/1008713/.

3.16.3 IPSec VPN

1. Z navigačního panelu přejděte na **VPN Server (Server VPN)** > **IPSec VPN** a posuňte posuvník doprava (ve výchozím nastavení je na levé straně vypnutý).
2. Zadejte klíč do pole **Předsdílený klíč**.
3. V poli **VPN Client (Max Limit: 8)** (**Klient VPN (max. limit: 8)**) klikněte na ⊕ a přidejte účet.
4. Zadejte vlastní [Uživatelské jméno] a [Heslo] a klikněte na **Apply all settings (Použít všechna nastavení)**.

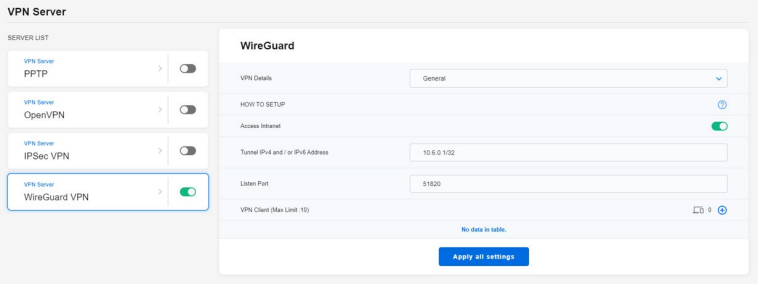


POZNÁMKA: Nastavené *[Uživatelské jméno]* a *[Heslo]* nelze měnit. Další informace najdete na https://www.asus.com/support/FAQ/1044190/.

3.16.4 WireGuard® VPN

1. Z navigačního panelu přejděte na **VPN Server (Server VPN)** > **WireGuard VPN**.
2. V poli **VPN Client (Max Limit: 10)** (**Klient VPN (max. limit: 10))** klikněte na ⊕ a přidejte účet. U běžných zařízení, jako jsou notebooky nebo chytré telefony, klikněte na **Apply (Použít)**.
3. Kliknutím na **Apply all settings (Použít všechna nastavení)** aktivujte WireGuard® VPN.
4. Kliknutím na " ••• " zobrazíte další podrobnosti.

POZNÁMKA: Pokud používáte k připojení k síti WireGuard® VPN chytrý telefon, stáhněte si aplikaci WireGuard® z portálu Google Play nebo App Store a naskenujte kód v aplikaci pro stažení konfiguračního souboru.

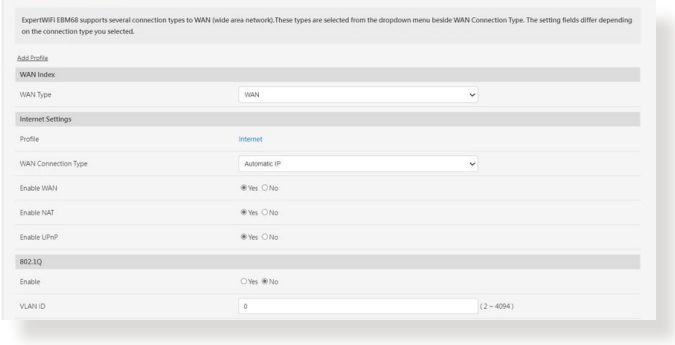


POZNÁMKA: Další informace najdete na https://www.asus.com/support/FAQ/1048280/.

3.17 WAN

3.17.1 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 **Settings (Nastavení)** > **WAN** > **Internet Connection (Internetové připojení)**.
2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **Typ připojení WAN:** Vyberte typ poskytovatele internetových služeb. K dispozici jsou možnosti **Automatic IP (Automatická adresa IP)**, **PPPoE**, **PPTP**, **L2TP** nebo **Static IP (Statická IP)**. Pokud směrovač nemůže získat platnou adresu IP nebo pokud neznáte typ připojení WAN, požádejte o pomoc vašeho ISP.
   - **Povolit WAN**: Výběrem možnosti **Yes (Ano)** aktivujte přístup směrovače k Internetu. Výběrem možnosti **No (Ne)** zakážete přístup k Internetu.
   - **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.

- **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.
- **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.
- **Ověřování**: Někteří ISP mohou tuto položku specifikovat. Informujte se u vašeho ISP a případně zadejte.
- **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.
- **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 drátový router ASUS tak, aby se shodovala s adresou MAC předchozího síťového zařízení, která byla poskytovatelem ISP registrována.

3.17.2 Multi-WAN

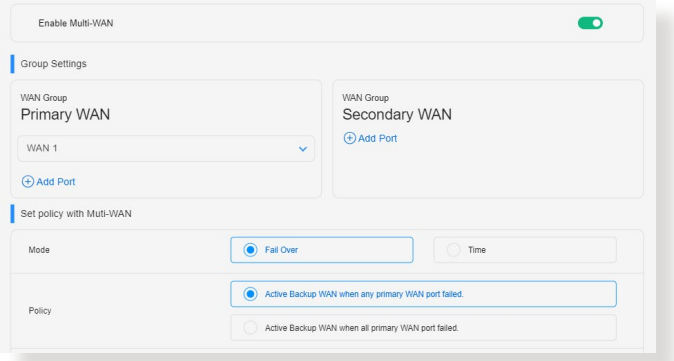
Multi-WAN vám umožňuje vybrat připojení více poskytovatelů internetu k vašemu routeru a skupiny WAN pro primární i sekundární WAN.

Konfigurace Multi-WAN:

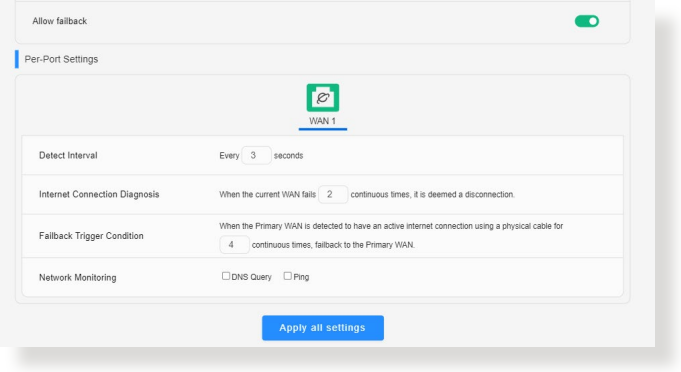
1. Na navigačním panelu přejděte na **Settings (Nastavení) > WAN > Multi-WAN**.
2. Zapněte možnost **Enable Multi-WAN (Povolit multi-WAN)**.
3. Vyberte **Primary WAN (Primární WAN)** a **Secondary WAN (Sekundární WAN)**. Je možné vybrat z možností WAN, USB a Ethernet LAN.
4. Vyberte možnost **Fail Over (Záložní)** nebo **Time (Čas)**.

   Fail Over (Záložní): Použijte sekundární WAN pro záložní přístup k síti.

   Time (Čas): Nastavte čas naplánování zásad pro multi-WAN.
5. Zvolte **Active Backup WAN when any primary WAN port failed (Aktivní zálohování WAN, když některý primární port WAN selhal)**, nebo **Active Backup WAN when all primary WAN port failed (Aktivní zálohování WAN, když selhaly všechny primární porty WAN)**.



6. Zapněte nebo vypněte možnost **Allow failback (Povolit obnovení)** služeb při selhání.
7. Zadejte interval detekce.
8. Zadejte počet nepřetržitých selhání, než bude aktuální WAN považována za odpojenou.
9. Zadejte počet nepřetržitých případů, kdy je primární síť WAN detekována jako aktivní připojení k internetu prostřednictvím fyzického kabelu, které spustí návrat k primární síti WAN.
10. Vyberte **DNS Query** nebo **Ping**.
11. Klikněte na **Apply all settings (Použít všechna nastavení)**.



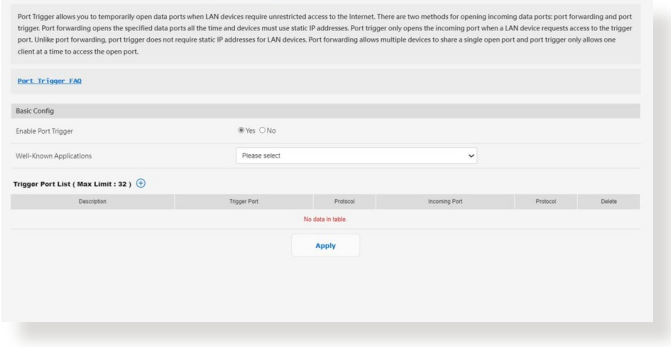
POZNÁMKA: Podrobná vysvětlení jsou k dispozici v odpovědích na časté dotazy na webu podpory ASUS **https://www.asus.com/support/FAQ/1011719**.

3.17.3 Aktivace portů

Port Aktivace vám umožňuje dočasně povolit datové porty, když zařízení LAN vyžadují neomezený přístup k internetu. Existují dva způsoby otevírání příchozích datových portů: přesměrování portu a aktivace portu.

- Přesměrování portů umožňuje zadané datové porty po celou dobu a zařízení musí používat statické adresy IP.
- Port Aktivace povolí příchozí port pouze tehdy, když zařízení LAN požaduje přístup k portu aktivace.

Na rozdíl od předávání portů nevyžaduje aktivace portů pro zařízení LAN statické adresy IP. Přesměrování portů umožňuje více zařízením sdílet jeden otevřený port a portu aktivace umožňuje přístup k otevřenému portu vždy pouze jednomu klientovi.



Pokyny pro nastavení aktivace portů:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **WAN** > **Port Trigger (Aktivace portů)**.
2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **Povolit aktivaci portů**: Výběrem možnosti **Yes (Ano)** povolíte aktivaci portů.
   - **Známé aplikace**: Vyberte oblíbené hry a webové služby, které chcete přidat do seznamu aktivace portů.

- **Popis**: Zadejte krátký název nebo popis služby.
- **Aktivační port**: Určete aktivační port pro otevření příchozího portu.
- **Protokol**: Vyberte protokol TCP nebo UDP.
- **Příchozí port**: Určete příchozí port pro příjem příchozích dat z Internetu.

POZNÁMKY:

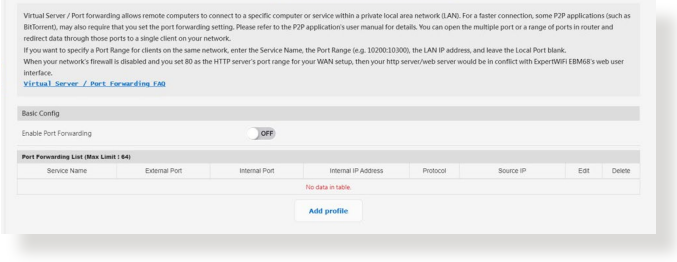
- Při připojování k serveru IRC provede klientský počítač odchozí připojení pomocí rozsahu aktivačních portů 66660 - 7000. Server IRC server odpoví ověřením uživatelského jména a vytvořením nového připojení ke klientskému počítači pomocí příchozího portu.
- Pokud je aktivace portů deaktivována, směrovač 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.
- Další informace najdete na https://www.asus.com/support/FAQ/114110.

3.17.4 Virtuální server/předávání portů

Virtuální server/přesměrování portů umožňuje vzdáleným počítačům připojení ke konkrétnímu počítači nebo službě v privátní místní síti (LAN). Pro rychlejší připojení mohou některé aplikace P2P (jako je BitTorrent) vyžadovat, abyste zadali nastavení přesměrování portů. Podrobnosti najdete v uživatelské příručce aplikace P2P. Můžete povolit více portů nebo rozsah portů ve routeru a přesměrovat data prostřednictvím těchto portů jednomu klientu v síti.

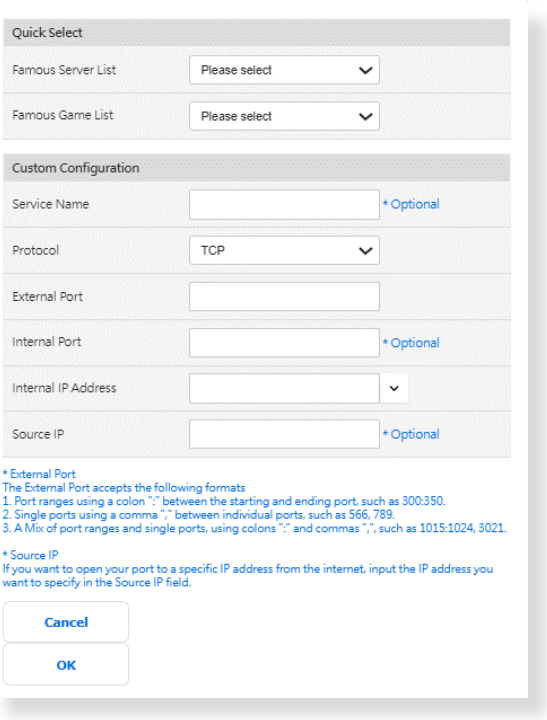
Chcete-li stanovit rozsah portů pro klienty ve stejné síti, zadejte údaje Service Name (Název služby), Port Range (Rozsah portů) (například 10200:10300), LAN IP address (Adresa IP místní sítě LAN) a položku Local Port (Místní port) ponechte prázdnou.

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 **Settings (Nastavení)** > **WAN** > **Virtual Server / Port Forwarding (Virtuální server / předávání portů)**.
2. Přesunutím přepínače do polohy **ON (ZAPNUTO)** povolte předávání portů a potom klikněte na možnost **Add Profile (Přidat profil)**. Po nakonfigurování následujících nastavení klikněte na tlačítko **OK**.



- **Seznam slavných serverů**: Určete typ služby, ke které chcete přistupovat.
- **Seznam slavných her**: Zobrazí porty vyžadované pro správné fungování oblíbených online her.
- **Název služby**: Zadejte název služby.
- **Protokol**: Vyberte protokol. Pokud si nejste jisti, vyberte možnost **BOTH (OBOJE)**.
- **External Port (Externí port):** Podporuje následující formáty:
  1) Rozsah portů s dvojtečkou se stanovením dolní a horní meze rozsahu, například 300:350;
  2) Čísla jednotlivých portů oddělená čárkou, například 566, 789;
  3) Směs rozsahů portů a jednotlivých portů, například 1015:1024, 3021.

- **Interní port**: Zadejte konkrétní port pro příjem předávaných paketů. Toto pole ponechte prázdné, pokud chcete, aby byly příchozí pakety přesměrovávány na určený rozsah portů.
- **Interní IP adresa**: Zadejte síťovou adresu IP klienta.
- **Zdrojová IP adresa**: Pokud chcete otevřít port pro konkrétní IP adresu z internetu, zadejte do tohoto políčka IP adresu, které chcete poskytnout přístup.

POZNÁMKA: Aby předávání portů fungovalo správně, použijte pro místního klienta statickou adresu IP. Další informace viz část **3.9 LAN**.

Pokyny pro kontrolu úspěšné konfigurace předávání portů:

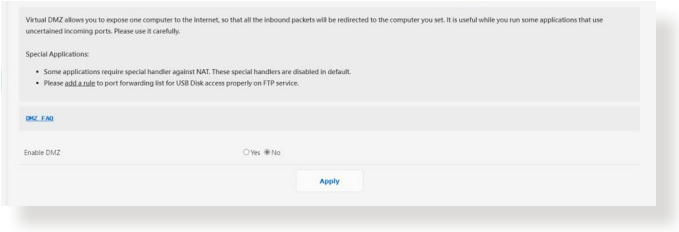
- Zkontrolujte, zda je nakonfigurován a spuštěn váš server nebo aplikace.
- Budete potřebovat klienta mimo vaši místní síť LAN, který má ovšem přístup k Internetu (též„internetový klient"). Tento klient nesmí být připojen ke směrovači ASUS.
- V internetovém klientovi zadejte adresu IP sítě WAN směrovače 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.

3.17.5 DMZ

Virtuální DMZ umožňuje vystavit jeden počítač internetu, takže všechny příchozí pakety budou přesměrovány do počítače, který nastavíte. Je to užitečné, když spouštíte některé aplikace, které používají nejisté příchozí porty. Používejte obezřetně.



Pokyny pro nastavení DMZ:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **WAN** > **DMZ**.
2. Nakonfigurujte následující nastavení. Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **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.

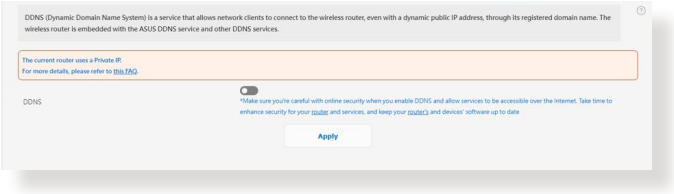
Pokyny pro odebrání DMZ:

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)**.

POZNÁMKA: Další informace najdete na https://www.asus.com/support/FAQ/1011723.

3.17.6 DDNS

Služba DDNS (Dynamic Domain Name System) umožňuje síťovým klientům připojit se k drátový routeru (i s dynamickou veřejnou IP adresou) prostřednictvím jeho registrovaného názvu domény. Drátový router je vybaven službou ASUS DDNS a dalšími službami DDNS.



Pokyny pro nastavení DDNS:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **WAN** > **DDNS**.
2. Nakonfigurujte níže uvedená nastavení: Po dokončení klepněte na tlačítko **Apply (Použít)**.
   - **Povolit klienta DDNS**: Povolte, aby mohl server DDNS přistupovat ke směrovači ASUS prostřednictvím názvu DNS, nikoli adresy IP sítě WAN.
   - **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).
   - **Povolit zástupný znak**: Povolte zástupný znak, pokud jej služba DDNS vyžaduje.

POZNÁMKY:

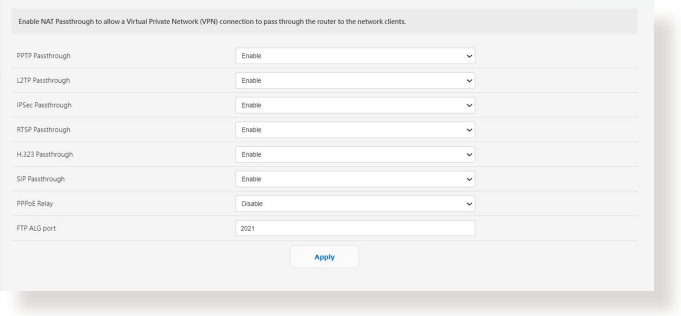
Za následujících podmínek služba DDNS nefunguje:

- Když drátový router 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.

3.17.7 Průchod NAT

Povolte funkci Průchod NAT, aby mohlo připojení VPN (Virtual Private Network) procházet routerem k síťovým klientům.

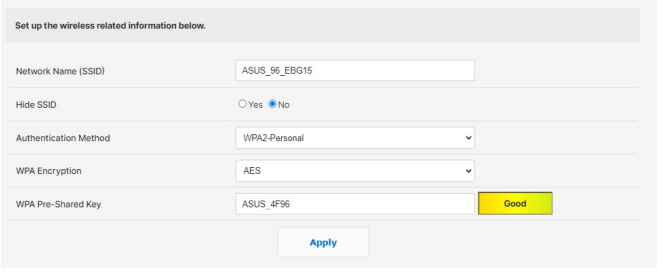
Chcete-li nastavit Průchod NAT, přejděte na **Settings (Nastavení)** > **WAN** > **NAT Passthrough (Průchod NAT)**. Po dokončení klepněte na tlačítko **Apply (Použít)**.



3.18 Bezdrátové připojení

3.18.1 Obecné

Na kartě **General (Obecné)** lze konfigurovat základní nastavení bezdrátového připojení.



Pokyny pro konfigurování základních nastavení bezdrátového připojení:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Wireless (Bezdrátové připojení)** > **General (Obecné)**.
2. Přiřaďte jedinečný název jako SSID (Service Set Identifier) nebo název sítě pro identifikaci vaší bezdrátové sítě. Prostřednictvím přiřazeného SSID mohou zařízení Wi-Fi identifikovat bezdrátovou síť a připojit se. Při uložení nových SSID do nastavení jsou zaktualizovány SSID na informačním panelu.

DŮLEŽITÉ! Chcete-li zpřístupnit funkci Wi-Fi, zajistěte integraci bezdrátového přístupového bodu (AP), jako je ExpertWiFi EBA63 nebo router, jako je ExpertWiFi EBR63 nebo ExpertWiFi EBM68, do sítě AiMesh EBG15.

---

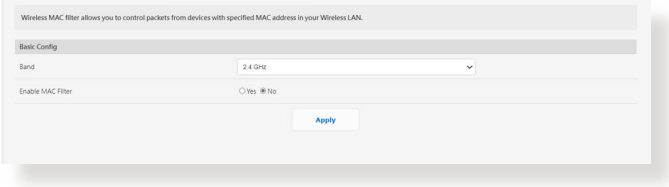
3. Výběrem **Yes (Ano)** v poli **Hide SSID (Skrýt SSID)** zabráníte bezdrátovým zařízením v rozpoznání vašeho SSID. Když je tato funkce aktivována, bude třeba při přístup k bezdrátové síti ručně zadat SSID v bezdrátovém zařízení.
4. Vyberte některý z následujících způsobů ověřování:
   - **Otevřený systém**: Tato volba neposkytuje žádné zabezpečení.

- **WPA/WPA2/WPA3-osobní**: Tato volba poskytuje silné zabezpečení. Můžete použít ověřování WPA (s TKIP) nebo WPA2 (s AES). V případě výběru této volby musíte použít šifrování TKIP + AES a zadat přístupové heslo WPA (síťový klíč).
- **WPA/WPA2/WPA3-podnikový**: Tato volba poskytuje velmi silné zabezpečení. Je k dispozici s integrovaným serverem EAP nebo externím ověřovacím serverem RADIUS.

5. Přidělte jedinečné heslo předsdílenému klíči WPA.

3.18.2 Bezdrátový filtr MAC

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

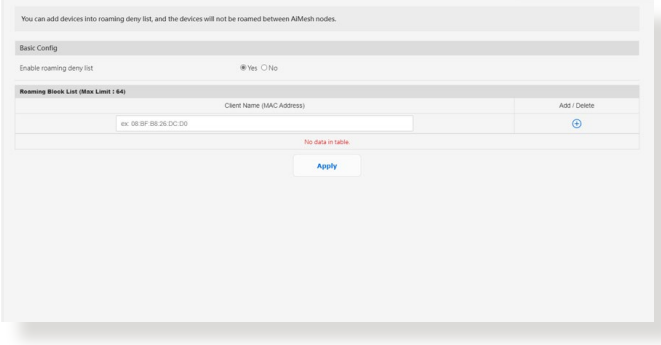


Pokyny pro konfigurování bezdrátového filtru MAC:

1. Na navigačním panelu přejděte na **Settings (Nastavení)** > **Wireless (Bezdrátové připojení)** > **Wireless MAC Filter (Bezdrátový filtr MAC)**.
2. Zatrhněte **Yes (Ano)** v poli **Enable Mac Filter (Povolit filtr Mac)**.
3. V rozevíracím seznamu **MAC Filter Mode (Režim filtru 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.
4. V seznamu filtru MAC klepněte na tlačítko ⊕ a zadejte adresu MAC bezdrátového zařízení.
5. Klepněte na **Apply (Použít)**.

3.18.3 Seznam blokování roamingu

Tato funkce umožňuje přidat zařízení do seznamu blokovaných roamingu a zabránit jim v roamingu mezi uzly AiMesh.



4 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.

4.1 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 **Settings (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 a stáhněte nejaktuálnější firmware.
3. Na stránce **Firmware Upgrade (Upgrade firmwaru)** klepněte na tlačítko **Browse (Procházet)** 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 jsou ethernetové kabely řádně připojeny.

- Když je ethernetový kabel, který spojuje směrovač s modemem, řádně připojen, svítí indikátor LED sítě WAN.
- Když je ethernetový kabel, který spojuje spuštěný počítač se směrovačem, řádně připojen, svítí příslušný indikátor LED místní sítě LAN.

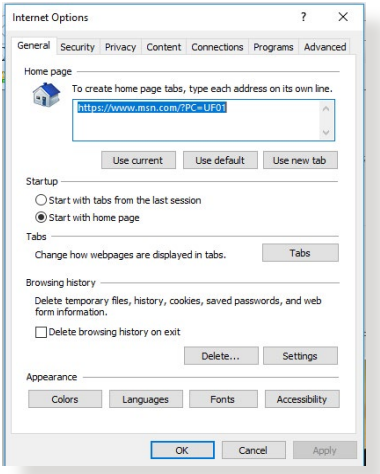
Zkontrolujte správnost síťových nastavení.

- Každý klient v síti musí mít platnou adresu IP. Společnost ASUS doporučuje používat server DHCP drátový router 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), **Dashboard (Ovládací panel)** > **Clients (Klienti)**.

4.2 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)**.

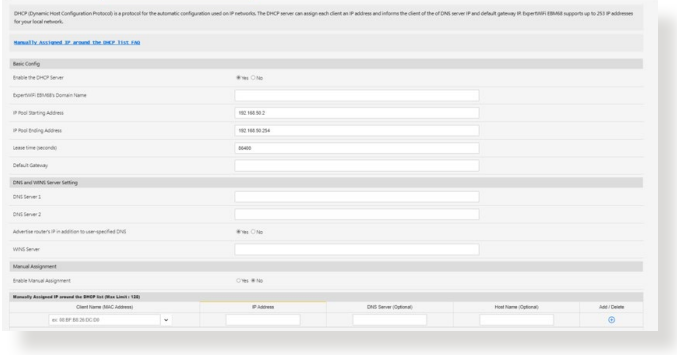
POZNÁMKY:

- 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.

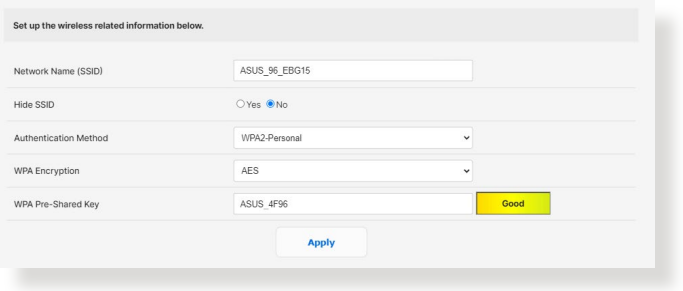
Klient nemůže navázat bezdrátové připojení ke směrovači.

DŮLEŽITÉ! Chcete-li zpřístupnit funkci Wi-Fi, zajistěte integraci bezdrátového přístupového bodu (AP), jako je ExpertWiFi EBA63 nebo router, jako je ExpertWiFi EBR63 nebo ExpertWiFi EBM68, do sítě AiMesh EBG15.

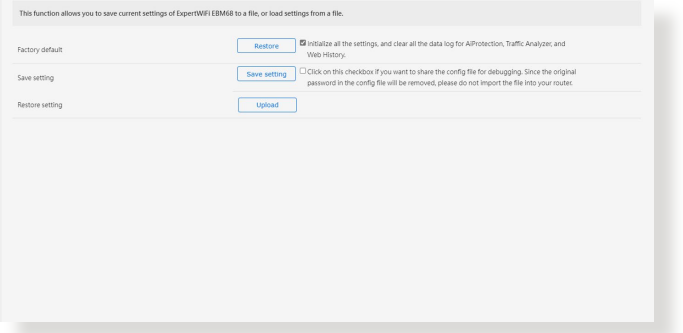
- **Server DHCP je deaktivován:**
  1. Spusťte webové grafické uživatelské rozhraní GUI. Přejděte na **Dashboard (Ovládací panel)** > **Clients (Klienti)** a vyhledejte zařízení, které chcete připojit ke směrovači.
  2. Pokud zařízení nelze najít v části **Dashboard (Ovládací panel)**, přejděte na **Settings (Nastavení)** > **LAN** > **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 **Settings (Nastavení)** > **Wireless (Bezdrát)** > **General (Obecné)**, vyberte **No (Ne)** v části **Hide SSID (Skrýt SSID)**.



- 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 připojit k routeru drátově, můžete obnovit výchozí tovární nastavení směrovače. V grafickém uživatelském rozhraní (GUI) klepněte na **Settings (Nastavení)** > **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 **Dashboard (Ovládací panel)**, 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 **Restartujte síť v následujícím pořadí** v kapitole **Odstraňování nejčastějších problémů**.
- Pokud stále nelze přistupovat k Internetu, zkuste restartovat počítač a ověřte adresu IP a adresu brány sítě.
- Zkontrolujte stavové indikátory na modemu ADSL a na drátový router. Pokud indikátor LED sítě WAN na drátový router NESVÍTÍ, zkontrolujte, zda jsou všechny kabely řádně připojeny.

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 **Dashboard (Ovládací panel)**, 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 **Settings (Nastavení)** > **Administration (Správa)** > **Restore/Save/Upload Setting (Obnovit/uložit/načíst nastavení)** a klepněte na **Restore (Obnovit)**.

Pokyny pro obnovení výchozích nastavení systému

- Přejděte na **Settings (Nastavení)** > **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).

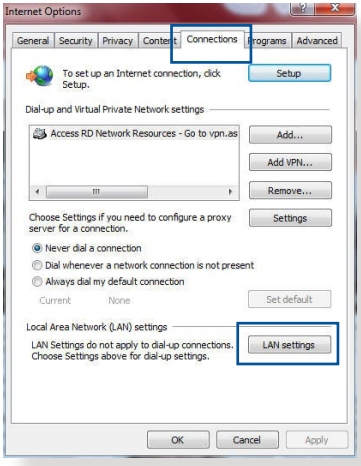
Nelze přistupovat k webovému grafickému uživatelskému rozhraní (GUI)

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

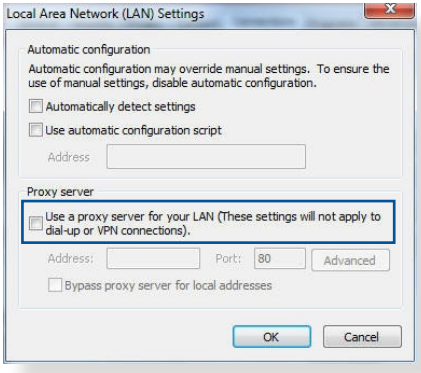
A. Deaktivujte server proxy, je-li aktivován.

Windows®

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

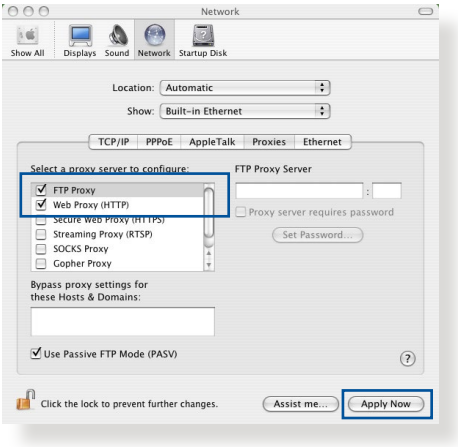


3. Na obrazovce Nastavení místní sítě (LAN) zrušte zaškrtnutí políčka **Use a proxy server for your LAN (Použít pro síť LAN server proxy)**.
4. Po dokončení klepněte na **OK**.



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))**.



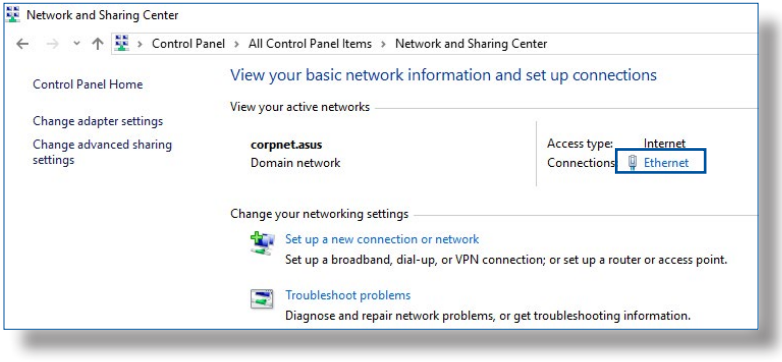
3. Po dokončení klepněte na **Apply Now (Použít)**.

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

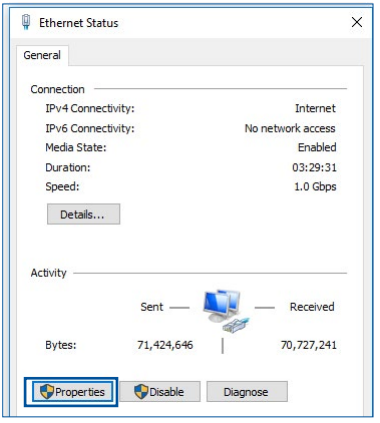
B. Proveďte nastavení TCP/IP pro automatické získání adresy IP.

Windows®

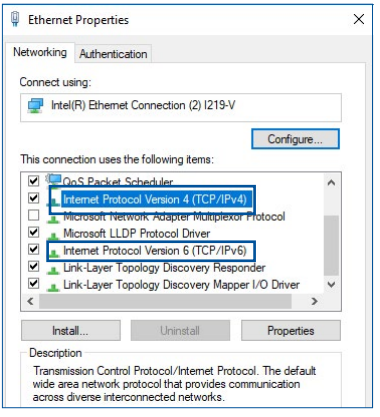
1. Klepněte na **Start** > **Control Panel (Ovládací panely)** > **Network and Sharing Center (Centrum sítí a sdílení),** potom kliknutím na síťové připojení zobrazíte jeho stavové okno.



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



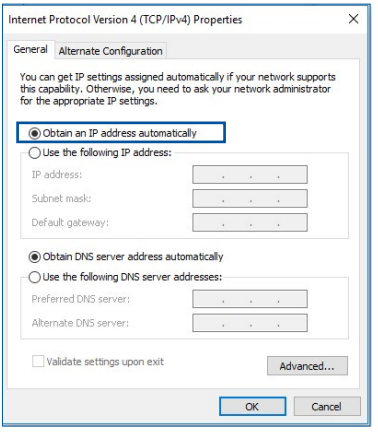
3. Vyberte **Internet Protocol Version 4 (TCP/IPv4) (Protokol Internet verze 4 (TCP/IPv4))** nebo **Internet Protocol Version 6 (TCP/IPv6) (Protokol Internet verze 6 (TCP/IPv6)** a potom klepněte na **Properties (Vlastnosti)**.



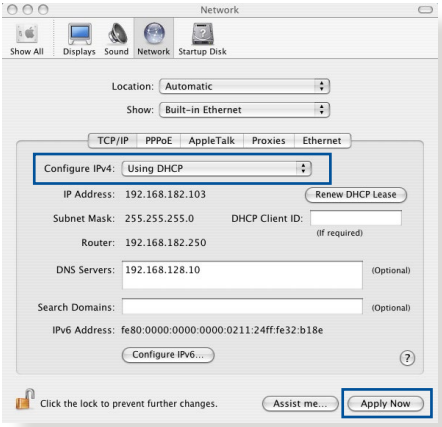
4. Zaškrtnutím položky **Obtain an IP address automatically (Získat adresu IP automaticky)** budou nastavení iPv4 IP získána automaticky.

   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

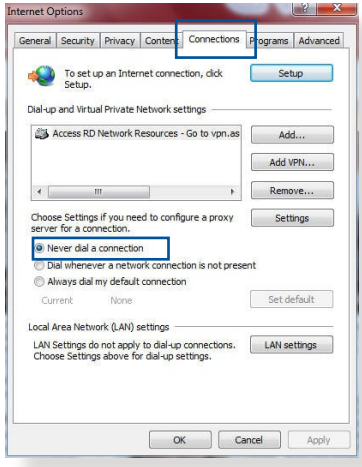


1. Klepněte na ikonu Apple v levé horní části obrazovky.
2. Klepněte na **System Preferences (Systémové preference)** > **Network (Síť)** > **Configure... (Konfigurovat...)**.
3. Na kartě **TCP/IP** vyberte **Using DHCP (Použití protokolu DHCP)** v rozevíracím seznamu **Configure IPv4 (Konfigurovat IPv4)**.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