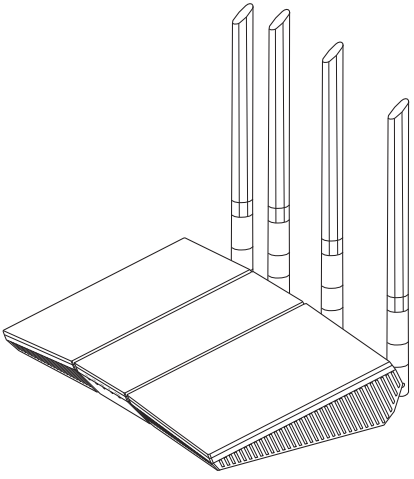
Ghidul utilizatorului

RT-AX57

Router Wi-Fi cu două benzi de frecvență



IN SEARCH OF INCREDIBLE

RO25463
Ediţie Revizuită V3
Noiembrie 2024

Sumar

Sumar

Sumar

1 Cum să vă cunoaşteţi routerul

1.1 Bine aţi venit!

Vă mulţumim pentru achiziţionarea unui ruter wireless ASUS, model RT-AX57!

Acest ruter RT-AX57 ultrasubţire şi plin de stil dispune de: o bandă dual de 2.4GHz şi 5GHz pentru redarea în flux HD, tehnologie de reţea Green de la ASUS, care asigură până la 70% dintre soluţiile de economisire a energiei.

1.2 Conţinutul pachetului

☑ Router fără cablu RT-AX57

☑ Cablu RJ45

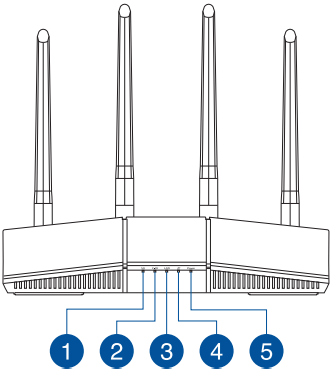
☑ Adaptor de alimentare

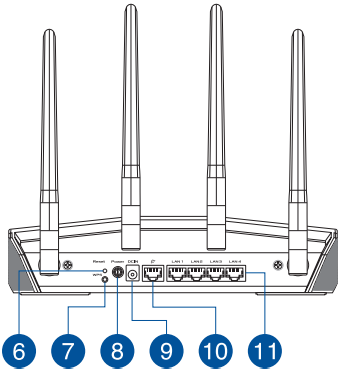
☑ Ghid rapid de pornire

NOTE:

- Dacă oricare dintre articole este deteriorat sau lipseşte, contactaţi ASUS pentru informaţii şi asistenţă tehnică. Consultaţi **Service and Support (Service și Asistență)** de pe partea din spate a acestui manual de utilizare.
- Păstraţi ambalajul original în caz că veţi avea nevoie de servicii ulterioare în garanţie, cum ar fi reparare sau înlocuire.

1.3 Ruter wireless





1 **5GHz LED**
Stins: Nu există semnal de 5 GHz.
Aprins: Sistemul fără fir este pregătit.
Intermitent: Se transmit sau se primesc date printr-o conexiune fără fir.

2 **2.4GHz LED**
Stins: Nu există semnal de 2.4 GHz.
Aprins: Sistemul fără fir este pregătit.
Intermitent: Se transmit sau se primesc date printr-o conexiune fără fir.

3 **LED LAN**
Stins: Sistemul nu este alimentat sau nu există conexiune fizică.
Aprins: Există conexiune fizică la o rețea locală (LAN).

4 **LED WAN (Internet)**
Roșu: Nicio IP sau nicio conexiune fizică.
Aprins: Există conexiune fizică la o rețea de arie largă (WAN).

5 **LED alimentare**
Stins: Fără alimentare.
Aprins: Dispozitivul este pregătit.
Intermitent lent: Mod de salvare.

6 **Buton Reset (Reinițializare)**
Acest buton reinițializează sau restabilește sistemul la setările implicite din fabrică.

7 **Buton WPS**
Acest buton lansează Expertul WPS.

8 **Comutator de pornire/oprire**
Apăsați pe acest buton pentru a porni/a opri sistemul.

9	**Port alimentare (intrare c.c.)** Inserați adaptorul de c.a. în acest port și conectați ruterul la o sursă de alimentare.
10	**Port WAN (Internet)** Conectați un cablu de rețea la acest port pentru a stabili o conexiune WAN.
11	**Porturi LAN 1 ~ 4** Conectați cabluri de rețea la aceste porturi pentru a stabili o conexiune LAN.

NOTE:

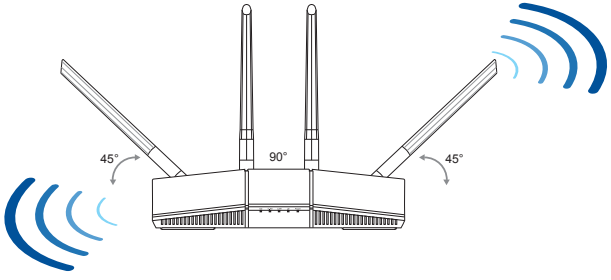
- Utilizați numai adaptorul livrat în pachet. Utilizarea altor adaptoare poate deteriora dispozitivul.
- **Specificații:**

Adaptor de alimentare c.c.	Ieșire c.c.: +12 V cu curent max. de 1 A/1.5 A		
Temperatură în stare de funcționare	0~40°C	Stocare	0~70°C
Umiditate în stare de funcționare	50~90%	Stocare	20~90%

1.4 Poziţionarea ruterului

Pentru transmisia optimă a semnalului fără fir între ruterul fără fir şi dispozitivele de reţea conectate la acesta, asiguraţi-vă că:

- Aşezaţi ruterul fără fir într-o zonă centrală pentru o acoperire fără fir maximă pentru dispozitivele de reţea.
- Feriţi dispozitivul de obstacole de metal şi de lumina directă a soarelui.
- Feriţi dispozitivul de dispozitive Wi-Fi numai de 802.11g sau 20 MHz, echipamente periferice de 2.4 GHz, dispozitive Bluetooth, telefoane fără fir, transformatoare, motoare de mare putere, lumini fluorescente, cuptoare cu microunde, frigidere şi alte echipamente industriale pentru a preveni interferenţele sau pierderea semnalului.
- Actualizaţi întotdeauna la cel mai recent firmware. Vizitaţi site-ul Web ASUS la adresa **http://www.asus.com** pentru a obţine cele mai recente actualizări de firmware.



1.5 Cerinţe pentru configurare

Pentru a vă configura reţeaua, aveţi nevoie de unul sau de două computere care să întrunească următoarele cerinţe de sistem:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Capabilitate wireless IEEE 802.11a/b/g/n/ac/ax
- Un serviciu TCP/IP instalat
- Browser de Web, ca de exemplu Internet Explorer, Firefox, Safari sau Google Chrome

NOTE:

- În cazul în care computerul dvs. nu dispune de capabilităţi încorporate de wireless, puteţi instala un adaptor WLAN IEEE 802.11a/b/g/n/ac/ax în computerul dvs. pentru a vă conecta la reţea.
- Dispunând de tehnologia de bandă dual, routerul dvs. wireless acceptă simultan semnale de reţea wireless 2,4 GHz şi 5 GHz. Acest lucru vă permite să efectuaţi activităţi legate de Internet, de exemplu puteţi naviga pe Internet sau puteţi citi/scrie mesaje de mail utilizând banda de 2,4 GHz, iar în acelaşi timp puteţi reda în flux fişiere de definiţie ridicată audio/video, ca de exemplu muzică sau filme, pe banda de 5 GHz.
- Unele dispozitive compatibile cu standardul IEEE 802.11n pe care doriţi să le conectaţi la reţeaua dvs. este posibil să accepte sau nu banda de frecvenţă de 5 GHz. Citiţi manualul dispozitivului pentru specificaţii.
- Cablurile Ethernet RJ-45 care vor fi utilizate pentru conectarea dispozitivelor de reţea nu trebuie să depăşească 100 de metri.

IMPORTANT!

- Unele adaptoare wireless pot avea probleme de conectivitate la AP-urile WiFi 802.11ax.
- Dacă întâmpinați o astfel de problemă, asigurați-vă că actualizați driverul la cea mai recentă versiune. Verificați site-ul oficial de asistență al producătorului pentru a obține drivere de software, actualizări și alte informații conexe.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

2 Inițilizarea

2.1 Configurarea ruterului

IMPORTANT!

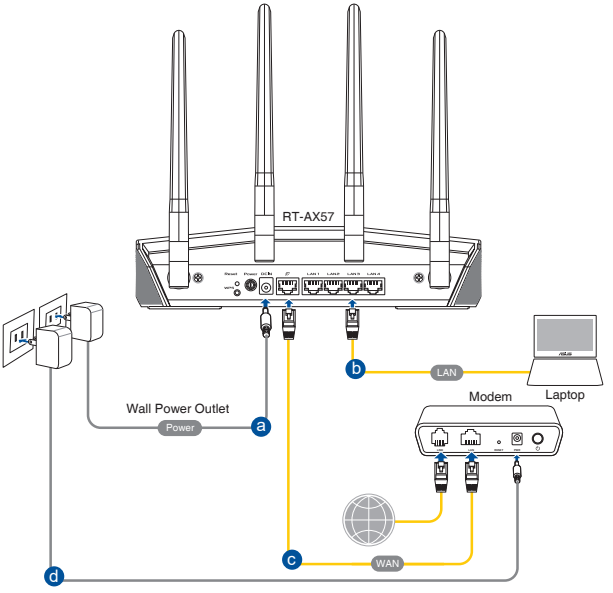
- Utilizaţi o conexiune cu fir pentru setarea ruterului wireless pentru a evita eventualele probleme de configurare.
- Înainte de a configura ruterul fără fir ASUS, efectuaţi următoarele acţiuni:
  - Dacă înlocuiţi un ruter existent, deconectaţi-l de la reţea.
  - Deconectaţi cablurile/firele de la instalaţia de modem existentă. Dacă modemul dispune de o baterie de rezervă, scoateţi-o şi pe aceasta.
  - Reporniţi computerul (recomandat).

AVERTISMENT!

- Cablurile de alimentare trebuie să fie conectate la prize prevăzute cu o împământare adecvată. Conectați echipamentul numai la o priză din apropiere, ușor accesibilă.
- Dacă sursa de alimentare se defectează, nu încercaţi să o reparaţi singur. Contactaţi un tehnician de service calificat sau distribuitorul local.
- NU utilizaţi cabluri de alimentare, accesorii sau echipamente periferice deteriorate.
- NU montați acest echipament la o înălțime mai mare de 2 m.
- Utilizaţi PC-ul desktop în medii cu temperatura ambiantă cuprinsă între 0 ˚C (32 ˚F) şi 40 ˚C (104 ˚F).

A. Conexiune cu fir

NOTĂ: Puteţi folosi un cablu de conexiune directă sau un cablu crossover (inversor) pentru conexiunea cu fir.



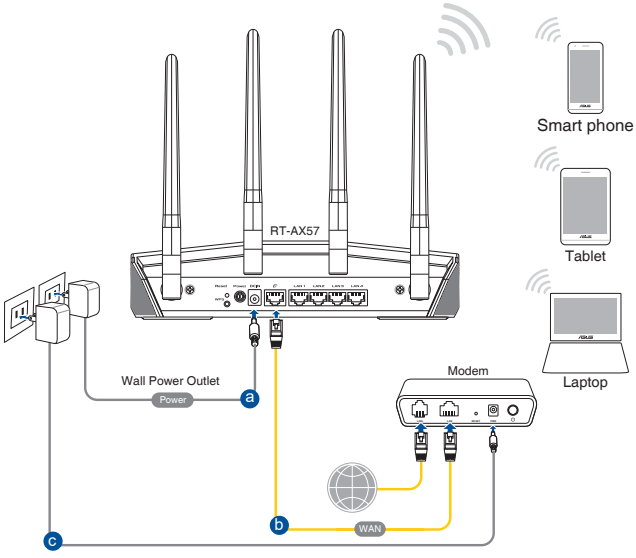
Pentru a configura ruterul fără fir printr-o conexiune prin cablu:

1. Inseraţi adaptorul de c.a. al ruterului fără fir în portul de intrare c.c. şi conectaţi-l la o priză.
2. Utilizând cablul de reţea inclus, conectaţi computerul la portul LAN al ruterului fără fir.

IMPORTANT! Asiguraţi-vă că LED-ul LAN iluminează intermitent.

3. Utilizând un alt cablu de reţea, conectaţi modemul la portul WAN al ruterului fără fir.
4. Inseraţi adaptorul de c.a. al modemului în portul de intrare c.c. şi conectaţi-l la o priză.

B. Conexiune wireless



Pentru a configura ruterul fără fir printr-o conexiune prin cablu:

1. Inseraţi adaptorul de c.a. al ruterului fără fir în portul de intrare c.c. şi conectaţi-l la o priză.
2. Utilizând cablul de reţea inclus, conectaţi modemul la portul WAN al ruterului fără fir.
3. Insert your modem's AC adapter to the DC-In port and plug it to a power outlet.
4. Instalaţi un adaptor WLAN IEEE 802.11a/b/g/n/ac/ax pe computer.

NOTE:

- Pentru detalii referitoare la o reţea wireless, consultaţi manualul de utilizare al adaptorului WLAN.
- Pentru a configura setările de securitate pentru reţeaua dvs., consultaţi secţiunea **3.2.1 Configurarea setărilor de securitate pentru reţea** din capitolul al treilea al acestui manual de utilizare.

2.2 Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată

Funcţia Quick Internet Setup (QIS – Configurare rapidă Internet) vă ghidează pentru setarea rapidă a conexiunii la Internet.

NOTĂ: Când setaţi conexiunea la Internet pentru prima dată, apăsaţi pe butonul Reset (Reiniţializare) de pe ruterul fără fir pentru a-l reiniţializa la setările implicite din fabrică.

Pentru a utiliza QIS cu detectare automată:

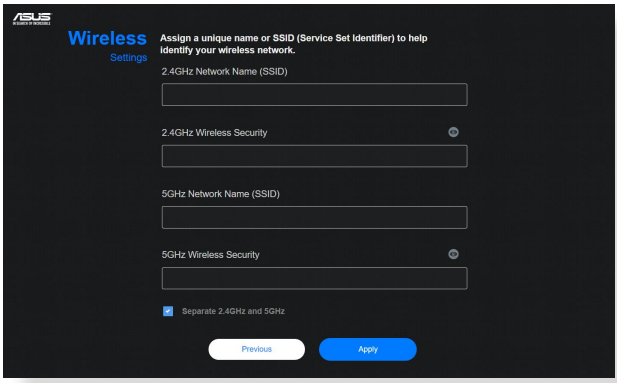
1. Lansaţi un browser web. Veţi fi redirecţionat către expertul de configurare ASUS (configurare rapidă internet). Dacă nu sunteţi redirecţionat, introduceţi adresa http://www.asusrouter.com manual.
2. Ruterul wireless detectează automat dacă tipul conexiunii de la ISP este **Dynamic IP (IP dinamic)**, **PPPoE**, **PPTP**, şi **L2TP**. Tastaţi informaţiile utile pentru tipul de conexiune furnizat de ISP.

IMPORTANT! Obţineţi informaţiile necesare referitoare la tipul de conexiune la Internet de la ISP-ul dvs.

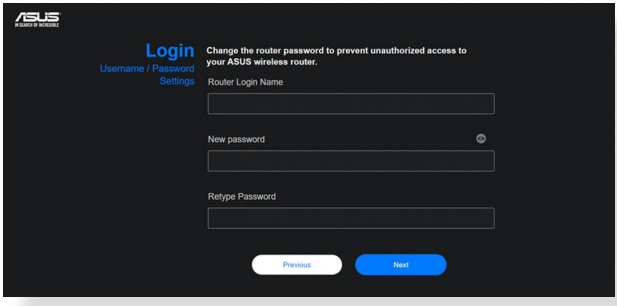
NOTE:

- Detectarea automată a tipului de conexiune furnizat de ISP are loc atunci când configuraţi prima dată ruterul wireless sau atunci când ruterul wireless este resetat la valorile implicite.
- Dacă funcţia QIS nu a reuşit să detecteze tipul de conexiune la Internet, faceţi clic pe **Skip to manual setting (Salt la setare manuală)** (consultaţi captura de ecran de la pasul 1) şi configuraţi manual setările de conexiune.

3. Atribuiţi numele de reţea (SSID) şi cheia de securitate pentru conexiunea fără fir de 2,4 GHz şi 5 GHz. Faceţi clic pe **Apply (Se aplică)** când aţi terminat.



4. Pe pagina **Login Information Setup (Configurare informaţii de conectare)**, schimbaţi parola de conectare a routerului pentru a preveni accesul neautorizat la routerul dvs. wireless.



NOTĂ: Numele de utilizator şi parola ruterului dvs. wireless sunt diferite faţă de numele reţelei (SSID) în banda de frecvenţă de 2,4 GHz/5 GHz şi faţă de cheia de securitate a acesteia. Numele de utilizator şi parola ruterului dvs. wireless vă permit să vă conectaţi la interfaţa de utilizare web a ruterului dvs. wireless, cu scopul de a configura setările ruterului dvs. wireless. Numele de reţea (SSID) în banda de frecvenţă de 2,4 GHz/5 GHz şi cheia de securitate a acesteia permit dispozitivelor Wi-Fi să se autentifice şi să se conecteze la reţeaua dvs. în banda de frecvenţă de 2,4 GHz/5 GHz.

2.3 Conectarea la reţeaua dvs. wireless

După configurarea ruterului dvs. wireless prin QIS, veţi putea conecta computerul sau alte dispozitive inteligente la reţeaua wireless.

Pentru a vă conecta la reţea:

1. Pe computer, faceţi clic pe pictograma de reţea din zona de notificări pentru a afişa reţelele wireless disponibile.
2. Selectaţi reţeaua wireless la care doriţi să vă conectaţi, apoi faceţi clic pe **Connect (Conectare)**.
3. Pentru o reţea wireless securizată este posibil să fie necesară introducerea cheii de securitate, după care faceţi clic pe **OK**.
4. Aşteptaţi până când computerul dvs. stabileşte cu succes conexiunea la reţeaua wireless. Starea conexiunii este afişată şi pictograma de reţea afişează starea de conectare .

NOTE:

- Consultaţi capitolele următoare pentru mai multe detalii cu privire la configurarea setărilor reţelei dvs. wireless.
- Consultaţi manualul de utilizare al dispozitivului dvs. pentru mai multe detalii privind conectarea la o reţea wireless.

3 Configurarea setărilor generale şi setărilor avansate

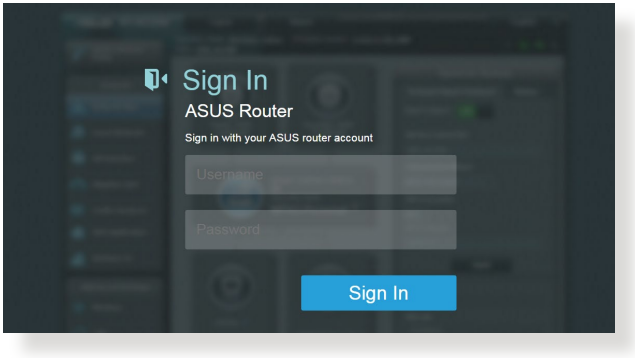
3.1 Conectarea la interfaţa Web GUI

Ruterul dvs. wireless de la ASUS se furnizează cu o interfaţă grafică Web intuitivă cu utilizatorul (GUI) care vă permite să-i configuraţi cu uşurinţă numeroasele funcţii printr-un browser de Web, ca de exemplu prin Internet Explorer, Firefox, Safari sau Google Chrome.

NOTĂ: Caracteristicile pot diferi în funcţie de versiunea firmware.

Pentru a vă conecta la interfaţa Web GUI:

1. În browserul de Web (Internet Explorer, Firefox, Safari sau Google Chrome) tastaţi manual adresa IP implicită a ruterului wireless: http://www.asusrouter.com**.**
2. Pe pagina de acces, tastaţi numele de utilizator şi parola pe care aţi configurat-o la **2.2 Configurare rapidă internet cu detectare automată**.

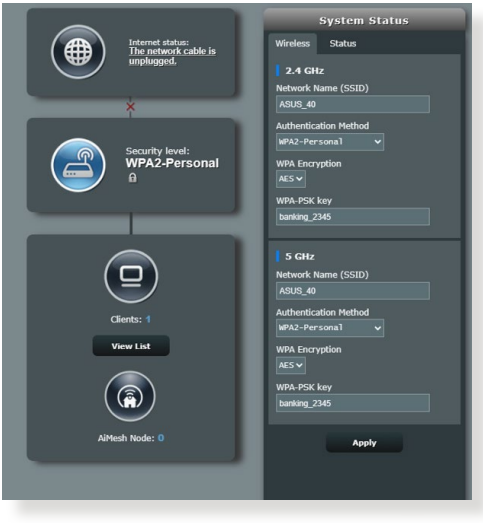


3. Puteţi utiliza interfaţa de utilizare web pentru a configura diverse setări pentru ruterul dvs. wireless ASUS.

NOTĂ: Dacă vă conectaţi la interfaţa de utilizare web pentru prima dată, veţi fi direcţionat automat către pagina Quick Internet Setup (QIS – Configurare rapidă Internet).

3.2 Utilizarea hărţii reţelei

Harta reţelei vă permite să configuraţi setările de securitate ale reţelei dvs., să gestionaţi clienţii din reţea şi să monitorizaţi dispozitivul USB.



3.2.1 Configurarea setărilor de securitate pentru reţeaua wireless

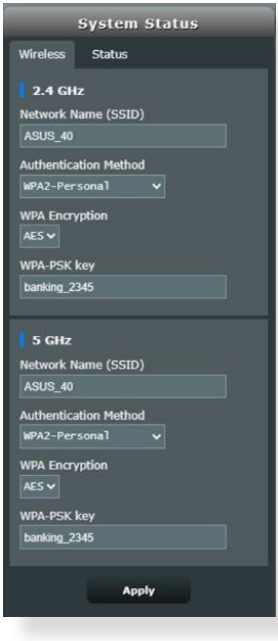
Pentru a vă proteja reţeaua wireless împotriva accesului neautorizat, este necesar să configuraţi setările de securitate.

Pentru a configura setările de securitate pentru reţeaua wireless:

1. Din panoul de navigare, mergeţi la **General > Network Map (Hartă reţea)**.
2. Din ecranul Network Map (Hartă reţea) selectaţi pictograma **System Status (Stare Sistem)** pentru afişarea setărilor de securitate wireless, cum sunt de exemplu SSID, nivel de securitate şi setările de criptare.

NOTĂ: Puteţi configura setări diferite de securitate wireless pentru benzile 2.4 GHz şi 5 GHz.

Setări de securitate pentru banda 2.4 GHz / 5 GHz



3. În câmpul **Network Name (SSID) (Nume reţea (SSID))** tastaţi un nume unic pentru reţeaua dvs. wireless.

4. Din lista verticală **WEP Encryption (Criptare WEP)** selectaţi metoda de criptare pentru reţeaua dvs. wireless.

IMPORTANT! Standardul IEEE 802.11n/ac/ax interzice utilizarea unei rate mari de transfer cu WEP sau WPA-TKP ca şi cifru unicast. În cazul în care utilizaţi aceste metode de criptare, rata de date va scădea la o conexiune IEEE 802.11g de 54 Mbps.

5. Tastaţi cheia de acces de securitate.
6. Faceţi clic pe **Apply (Aplicare)** după ce aţi terminat.

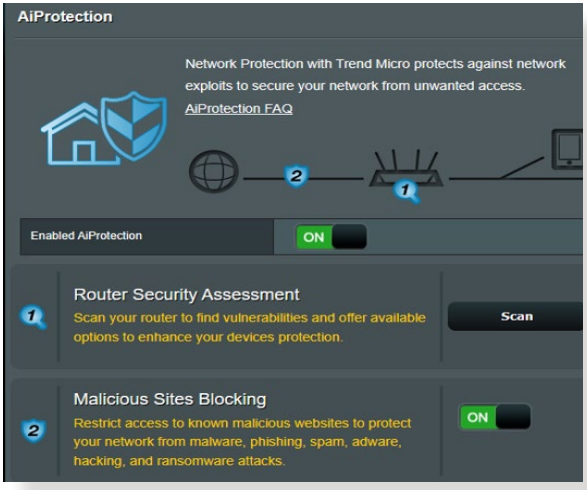
3.2.2 Administrarea clienţilor din reţea

Pentru a administra clienţii din reţea:

1. Din panoul de navigare, mergeţi la **General** > **Network Map (Hartă reţea)**.
2. Din ecranul Network Map (Hartă reţea), selectaţi pictograma **Client Status (Stare client)** pentru afişarea informaţiilor referitoare la clienţii de reţea.
3. Pentru a bloca accesul unui client la reţea, selectaţi clientul şi apoi faceţi clic pe **Block (Blocare)**.

3.3 AiProtection

Funcţia AiProtection asigură monitorizare în timp real pentru a detecta software-ul rău intenţionat, software-ul de spionare şi cazurile de acces nedorit. De asemenea, funcţia filtrează site-urile web şi aplicaţiile nedorite şi vă permite să programaţi un interval orar în care un dispozitiv conectat poate accesa internetul.



3.3.1 Funcţia Network Protection (Protecţie reţea)

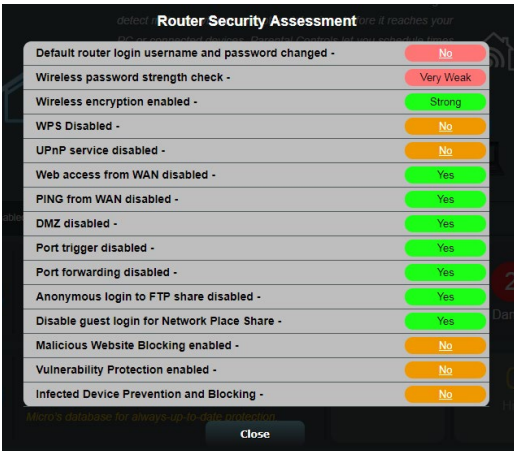
Funcţia Network Protection (Protecţie reţea) previne abuzarea reţelei şi securizează reţeaua împotriva accesului nedorit.

Configurarea funcţiei Network Protection (Protecţie reţea)

Pentru a configura funcţia Network Protection (Protecţie reţea):

1. Din panoul de navigare, mergeţi la **General > AiProtection.**
2. Din pagina principală **AiProtection** , faceţi clic pe **Network Protection (Protecţie reţea)**.
3. Din fila **Network Protection (Protecţie reţea)**, faceţi clic pe **Scan (Scanare)**.

   După terminarea scanării, utilitarul afişează rezultatele în pagina **Router Security Assessment (Evaluare securitate router).**



IMPORTANT! Elementele marcate cu **Yes (Da)** în pagina **Router Security Assessment (Evaluare securitate router)** sunt considerate a avea o stare **sigură**. Pentru elementele marcate cu **No (Nu)**, **Weak (Slab)** sau **Very Weak (Foarte slab)** se recomandă efectuarea unei configurări corespunzătoare.

4. (Opţional) din pagina **Router Security Assessment (Evaluare securitate router),** configuraţi manual elementele marcate cu **No (Nu), Weak (Slab)** sau **Very Weak (Foarte slab)**. Pentru aceasta:

   a. Faceţi clic pe un element.

NOTĂ: atunci când faceţi clic pe un element, utilitarul vă va redirecţiona către pagina de configurare a elementului respectiv.

   b. Din pagina cu setări de securitate a elementului respectiv, configuraţi şi efectuaţi modificările necesare şi faceţi clic pe **Apply (Se aplică)** când terminaţi;

   c. Reveniţi la pagina **Router Security Assessment (Evaluare securitate router)**şi faceţi clic pe **Close (Închidere)** pentru a ieşi din pagină;

5. Pentru a configura în mod automat setările de securitate, faceţi clic pe **Secure Your Router (Securizaţi-vă routerul)**;

6. Când apare un mesaj, faceţi clic pe **OK.**

Malicious Sites Blocking (Blocare site-uri rău intenţionate)

Această caracteristică restricţionează accesul la site-uri Web rău intenţionate cunoscute în baza de date cloud, pentru o protecţie actualizată în permanenţă.

NOTĂ: Această funcţie este activată în mod automat dacă executaţi funcţia **Router Weakness Scan (Scanare vulnerabilităţi router).**

Pentru a activa funcţia Malicious Sites Blocking (Blocare site-uri rău intenţionate):

1. Din panoul de navigare, mergeţi la **General > AiProtection**.
2. Din pagina principală **AiProtection**, faceţi clic pe **Network Protection (Protecţie reţea)**.
3. Din panoul **Malicious Sites Blocking (Blocare site-uri rău intenţionate)**, faceţi clic pe **ON (Activat).**

Infected Device Prevention and Blocking (Prevenire şi blocare dispozitiv infectat)

Această caracteristică împiedică dispozitivele infectate să comunice informaţii personale sau starea de infectare către părţi externe.

NOTĂ: Această funcţie este activată în mod automat dacă executaţi funcţia **Router Weakness Scan (Scanare vulnerabilităţi router).**

Pentru a activa funcţia Vulnerability protection (Protecţie împotriva vulnerabilităţilor):

1. Din panoul de navigare, mergeţi la **General > AiProtection**.
2. Din pagina principală **AiProtection**, faceţi clic pe **Network Protection (Protecţie reţea)**.
3. Din panoul **Infected Device Prevention and Blocking (Prevenire şi blocare dispozitiv infectat)**, faceţi clic pe **ON (Activat)**.

Pentru a configura funcţia Alert Preference (Preferinţă alerte):

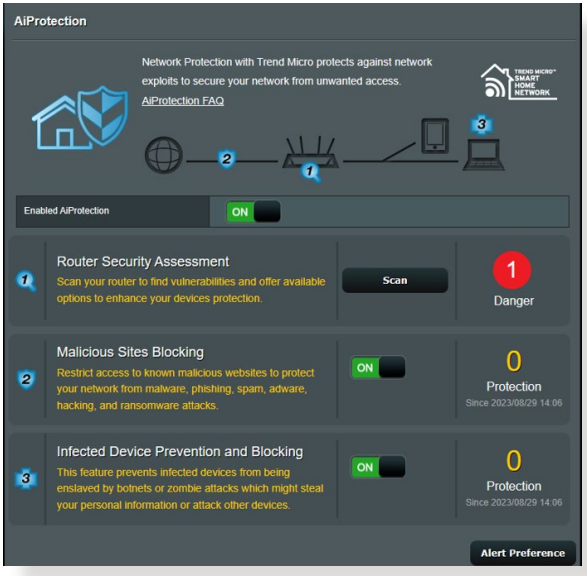
1. Din panoul **Infected Device Prevention and Blocking (Prevenire şi blocare dispozitiv infectat)**, faceţi clic pe **Alert Preference (Preferinţă alerte).**
2. Selectaţi sau introduceţi manual furnizorul de servicii e-mail, contul de e-mail şi parola şi apoi faceţi clic pe **Apply (Se aplică).**

3.3.2 Configurarea controlului parental

Opţiunea de control parental vă permite să controlaţi intervalul orar de acces la internet sau să setaţi limita de timp pentru utilizarea reţelei de către un client.

Pentru a accesa pagina principală Parental Controls (Controale parentale):

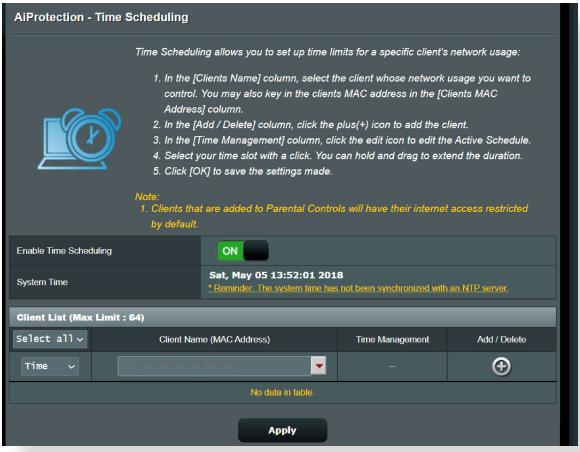
1. Din panoul de navigare, mergeţi la **General > AiProtection**.
2. Din pagina principală **AiProtection**, faceţi clic pe **Parental Controls (Controale parentale).**



Time Scheduling (Programare în timp)

Opţiunea Time Scheduling (Programare în timp) vă permite să setaţi limita de timp pentru utilizarea reţelei de către clienţi.

NOTĂ: Asiguraţi-vă că ora sistemului dvs. este sincronizată cu cea a serverului NTP.



Pentru a configura funcţia Time Scheduling (Programare în timp):

1. Din panoul de navigare, mergeţi la **General** > **AiProtection** > **Parental Controls (Controale parentale)** > **Time Scheduling (Programare în timp)**.
2. Din panoul **Enable Time Scheduling (Activare programare în timp)**, faceţi clic pe **ON (Activat).**
3. Din coloana **Clients Name (Nume clienţi)**, selectaţi sau introduceţi manual numele clientului din lista verticală.

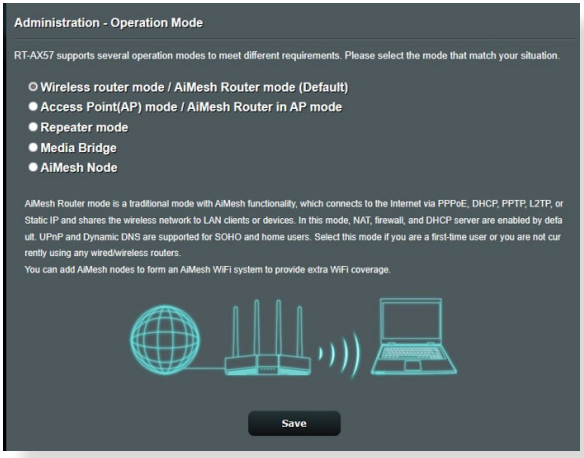
NOTĂ: De asemenea, puteţi să introduceţi adresa MAC a clientului în coloana **Client MAC Address (Adresă MAC client).** Asiguraţi-vă că numele clientului nu conţine caractere speciale sau spaţii, deoarece acest lucru poate face ca ruterul să funcţioneze anormal.

4. Faceţi clic pe ⊕ pentru a adăuga profilul clientului;
5. Faceţi clic pe **Apply (Se aplică)** pentru a salva setările.

3.4 Administration (Administrare)

3.4.1 Operation mode (Mod de funcţionare)

Pagina Operation Mode (Mod funcţionare) vă permite să selectaţi un mod de funcţionare corespunzător pentru reţeaua dvs.



Pentru a configura modul de funcţionare:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > **Operation Mode (Mod de funcţionare)**.
2. Selectaţi oricare dintre aceste moduri de funcţionare:
   - **Mod ruter wireless (implicit)**: În modul ruter wireless, ruterul wireless se conectează la Internet şi furnizează acces la Internet dispozitivelor disponibile din propria reţea locală.
   - **Punte media**: Această configuraţie necesită două rutere wireless. Cel de-al doilea ruter joacă rolul de punte media, iar în această situaţie mai multe dispozitive, precum televizoare inteligente şi console de jocuri, pot fi conectate prin Ethernet.
   - **Mod punct de acces**: În acest mod, ruterul creează o reţea wireless nouă pe baza unei reţele existente.
3. Faceţi clic pe **Save (Salvare)**.

NOTĂ: Ruterul va reporni după ce schimbaţi modul de funcţionare.

3.4.2 Actualizarea softului integrat

NOTĂ: Descărcaţi ultimul soft integrat de pe pagina web a ASUS la: **http://www.asus.com.**

Pentru actualizarea softului integrat:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Administration (Administrare)**> **Firmware Upgrade (Upgrade firmware)**.
2. În câmpul **New Firmware File (Fişier firmware nou)**, faceţi clic pe **Browse (Navigare)** pentru a localiza fişierul descărcat.
3. Faceţi click pe **Upload (Încărcare**).

NOTE:

- Când procesul de actualizare este finalizat, aşteptaţi un timp pentru ca sistemul să repornească.
- Dacă procesul de actualizare eşuează, routerul va intra automat în modul de urgenţă sau de defecţiune şi indicatorul LED de curent de pe partea frontală pâlpâie lent. Pentru a reface sistemul, consultaţi secţiunea **4.2 Firmware Restoration (Restaurare firmware)**.

3.4.3 Refacerea/Salvarea/Încărcarea setărilor

Pentru a reface/salva/încărca setările:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Administration (Administrare)**> **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)**.
2. Selectaţi sarcina pe care doriţi s-o îndepliniţi:
   - Pentru a reface setările iniţiale din fabrică, faceţi click pe **Restore (Refacere)** apoi click **OK** în mesajul de confirmare.
   - Pentru a salva setările curente de sistem, faceţi clic pe **Save (Salvare)**, navigaţi la folderul în care intenţionaţi să salvaţi fişierul şi faceţi clic pe **Save (Salvare)**.
   - Pentru a reface setarea sistemului anterior, click **Browse (Răsfoieşte)** pentru a localiza fişierul sistemului pe care doriţi să.l refaceţi apoi faceţi click pe **Upload (Încărcare)**.

IMPORTANT! Dacă apar probleme, încărcaţi cea mai recentă versiune de firmware şi configuraţi noile setări. Nu restauraţi setările implicite ale ruterului.

3.5 Paravan de protecţie

Ruterul wireless poate juca rolul de firewall hardware pentru reţeaua dvs.

NOTĂ: Caracteristică de firewall este activată implicit.

3.5.1 Aspecte generale

Pentru a configura setările de bază pentru firewall:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Firewall** > **General**.
2. În câmpul **Enable Firewall (Activare firewall)**, selectaţi **Yes (Da)**.
3. Pentru parametrul **Enable DoS protection (Activare protecţie DoS)**, selectaţi **Yes (Da)** pentru a proteja reţeaua împotriva atacurilor DoS (Denial of Service - respingerea serviciilor), cu toate că este posibil ca performanţele ruterului să fie afectate de această setare.
4. De asemenea, puteţi monitoriza pachetele schimbate între reţeaua LAN şi conexiunea WAN. Pentru parametrul Logged packets type (Tip pachete înregistrate), selectaţi **Dropped (Refuzate)**, **Accepted (Acceptate)** sau **Both (Ambele)**.
5. Faceţi clic pe **Apply (Aplicare)**.

3.5.2 URL Filter (Filtru URL)

Puteţi să specificaţi cuvinte cheie sau adrese web pentru a preveni accesul la anumite locaţii URL.

NOTĂ: Filtrul URL se bazează pe o interogare a serverului DNS. Dacă un client din reţea a accesat deja un site web precum http://www.abcxxx.com, atunci siteul web nu va fi blocat (siteurile web accesate în trecut sunt stocate într-o memorie cache a serverului DNS). Pentru a rezolva această problemă, ştergeţi memoria cache a serverului DNS înainte de a configura filtrul URL.

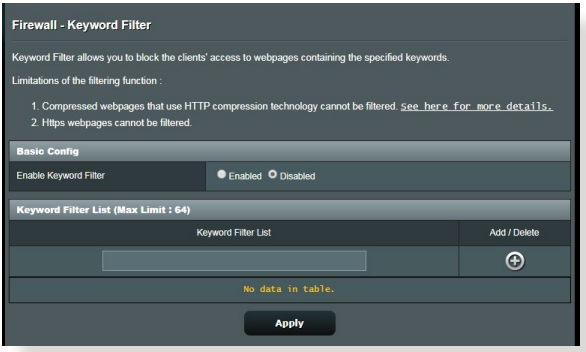
Pentru configurarea unui filtru URL:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Firewall** > **URL Filter (Filtru URL)**.

2. În câmpul Enable URL Filter (Activare filtru URL), selectaţi **Enabled (Activat)**.
3. Introduceţi o locaţie URL şi apoi faceţi clic pe butonul .
4. Faceţi clic pe **Apply (Aplicare)**.

3.5.3 Keyword filter (Filtru cuvinte cheie)

Filtrul de cuvinte cheie blochează accesul la paginile web care conţin anumite cuvinte cheie.



Pentru configurarea unui filtru de cuvinte cheie:

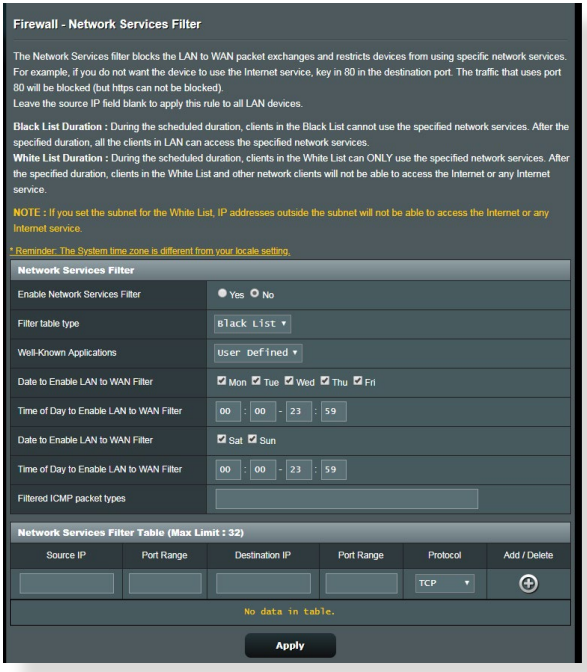
1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Firewall** > **Keyword filter (Filtru cuvinte cheie)**.
2. În câmpul Enable Keyword Filter (Activare filtru cuvinte cheie), selectaţi **Enabled (Activat)**.
3. Introduceţi un cuvânt sau o expresie şi apoi faceţi clic pe butonul **Add (Adăugare)**.
4. Faceţi clic pe **Apply (Aplicare)**.

NOTE:

- Filtrul de cuvinte cheie se bazează pe o interogare a serverului DNS. Dacă un client din reţea a accesat deja un site web precum http://www.abcxxx.com, atunci siteul web nu va fi blocat (siteurile web accesate în trecut sunt stocate într-o memorie cache a serverului DNS). Pentru a rezolva această problemă, ştergeţi memoria cache a serverului DNS înainte de a configura filtrul de cuvinte cheie.
- Paginile web comprimate prin utilizarea mecanismului de compresie HTTP nu pot fi supuse filtrării. Paginile HTTPS nu pot fi blocate prin utilizarea unui filtru de cuvinte cheie.

3.5.4 Network Services Filter (Filtru servicii reţea)

Filtrul pentru serviciile din reţea blochează pachetele schimbate între reţeaua LAN şi conexiunea WAN şi restricţionează clienţii din reţea să acceseze anumite servicii web, cum ar fi Telnet sau FTP.



Pentru configurarea unui filtru de servicii de reţea:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Firewall** > **Network Services Filter (Filtru servicii reţea)**.
2. În câmpul Enable Network Services Filter (Activare filtru servicii reţea), selectaţi **Yes (Da)**.
3. Selectaţi tipul de tabel de filtrare. **Black List (Listă neagră)** blochează serviciile de reţea specificate. **White List (Listă albă)** limitează accesul numai la serviciile de reţea specificate.
4. Specificaţi ziua şi intervalul orar în care filtrele vor fi active.
5. Pentru a specifica un serviciu de reţea ce urmează să fie filtrat, introduceţi IP-ul sursă, IP-ul destinaţie, intervalul de porturi şi protocolul. Faceţi clic pe butonul  .
6. Faceţi clic pe **Apply (Aplicare)**.

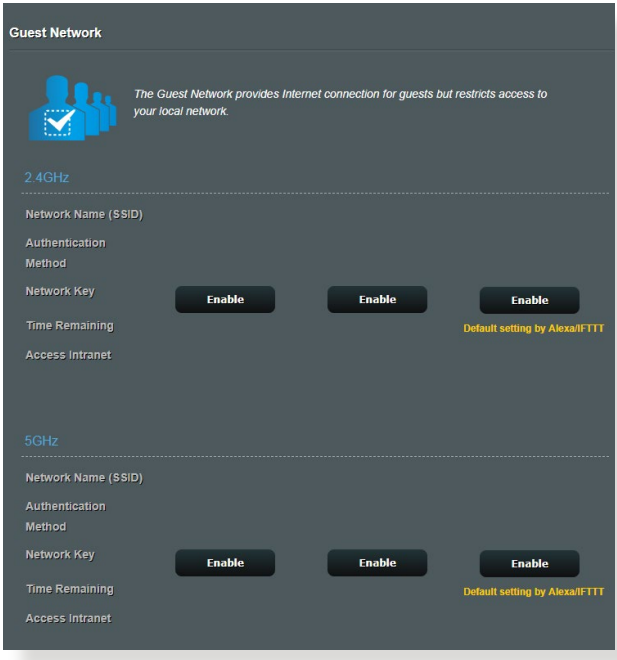
3.6 Reţelei de vizitatori

Reţeaua de vizitatori oferă vizitatorilor temporari conectivitate la Internet prin intermediul accesului la SSID-uri sau reţele separate, fără a le oferi acces acestora la reţeaua dvs. privată.

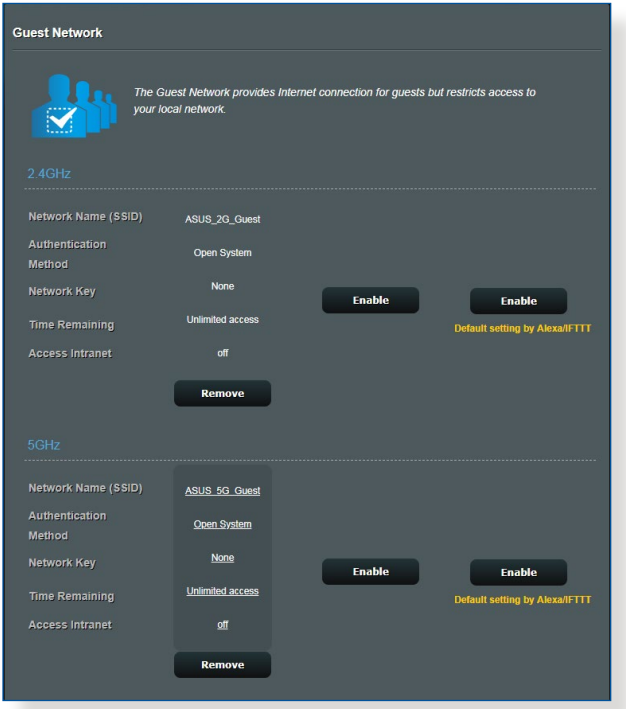
NOTĂ: RT-AX57 acceptă până la SSID-uri (trei în banda de frecvenţă de 2.4 GHz şi trei în banda de frecvenţă de 5 GHz).

Pentru a vă crea o reţea de vizitatori:

1. Din panoul de navigare, mergeţi la **General** > **Guest Network (Reţea vizitatori)**.
2. În ecranul Guest Network (Reţea vizitatori), selectaţi banda de frecvenţă de 2.4GHz sau de 5GHz pentru reţeaua de vizitatori pe care doriţi să o creaţi.
3. Faceţi clic pe **Enable (Activare)**.



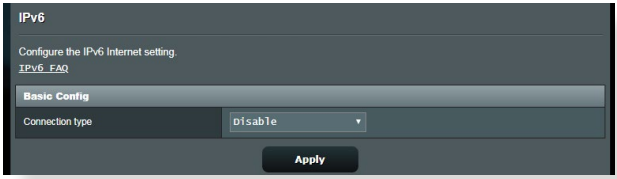
4. Pentru a configura opţiuni suplimentare, faceţi clic pe **Modify (Modificare)**.



5. Faceţi clic pe **Yes (Da)** în ecranul **Enable Guest Network (Activare reţea vizitatori)**.
6. Atribuiţi un nume pentru reţeaua temporară în câmpul **Network Name (SSID) (Nume reţea (SSID))**.
7. Selectaţi o opţiune **Authentication Method (Metodă de autentificare)**.
8. Selectaţi o metodă pentru **Encryption (Criptare)**.
9. Specificaţi o valoare pentru **Access time (Timp de acces)** sau faceţi clic pe **Limitless (Nelimitat)**.
10. Selectaţi **Disable (Dezactivare)** sau **Enable (Activare)** pe elementul **Access Intranet (Acces la Intranet)**.
11. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.

3.7 IPv6

Acest ruter wireless acceptă adresele de tip IPv6, un sistem care oferă suport pentru mai multe adrese IP. Acest standard nu este încă disponibil pe scară largă. Contactaţi furnizorul de servicii internet dacă abonamentul dvs. include standardul IPv6.



Pentru a configura IPv6:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **IPv6**.
2. Selectaţi o opţiune pentru **Connection type (Tip conexiune)**. Opţiunile de configurare variază în funcţie de tipul de conexiune selectat.
3. Introduceţi setările pentru IPv6 şi DNS.
4. Faceţi clic pe **Apply (Aplicare)**.

NOTĂ: Consultaţi furnizorul de servicii Internet cu pentru a primi informaţii specifice despre standardul IPv6 inclus în abonamentul dvs.

3.8 LAN

3.8.1 LAN IP

Ecranul LAN IP vă permite să modificaţi setările de IP pentru LAN ale ruterului dvs. wireless.

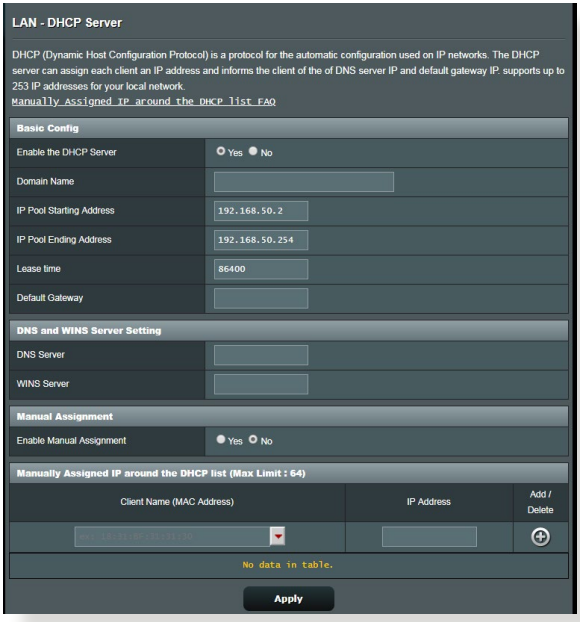
NOTĂ: Toate modificările aduse adresei IP a reţelei LAN vor fi reflectate în setările DHCP.

Pentru a modifica setările IP ale reţelei LAN:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **LAN** > **LAN IP**.
2. Modificaţi valorile pentru **IP address (Adresă IP)** şi **Subnet mask (Mască subreţea)**.
3. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.

3.8.2 Serverului DHCP

Ruterul dvs. wireless foloseşte protocolul DHCP pentru a atribui automat adresele IP în reţeaua dvs. Puteţi specifica intervalul de adrese IP şi durata de atribuire pentru clienţii din reţeaua dvs.



Pentru configurarea serverului DHCP:

1. Din panoul de navigare, bifaţi **Advanced Settings** > **LAN** > **DHCP Server**.
2. În câmpul **Enable the DHCP Server (Activaţi serverul DHCP)** bifaţi **Yes (Da)**.
3. În caseta **Domain Name (Nume domeniu)**, introduceţi un nume de domeniu pentru ruterul wireless.
4. În câmpul **IP Pool Starting Address (Plajă adresă IP de pornire)**, tastaţi adresa IP de pornire.
5. În câmpul **IP Pool Ending Address (Plajă adresă IP de sfârşit)**, tastaţi adresa IP de sfârşit.
6. În câmpul **Lease Time (Perioadă de închiriere)** tastaţi data la care expiră adresele IP şi ruterul wireless va aloca automat adrese IP noi pentru clienţii reţelei.

NOTE:

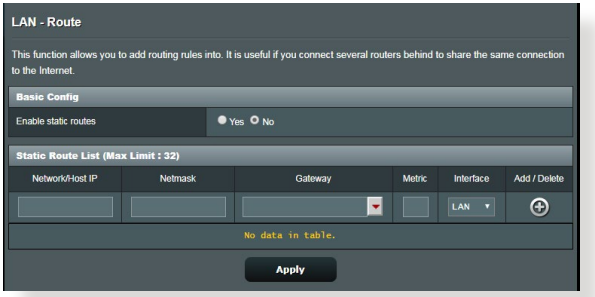
- Vă recomandăm să utilizaţi un format de adresă IP de tip 192.168.50.xxx (unde xxx poate fi orice număr între 2 şi 254) când specificaţi un interval de adrese IP.
- Adresa de pornire pentru plaja de adrese IP nu trebuie să fie mai mare decât adresa de sfârşit pentru plaja respectivă.

7. În secţiunea **DNS and Server Settings (Setări DNS şi server)**, introduceţi adresa IP pentru serverul DNS şi pentru serverul WINS, dacă este necesar.
8. Ruterul dvs. wireless poate atribui manual adrese IP pentru dispozitivele din reţea. În câmpul **Enable Manual Assignment (Activare atribuire manuală)**, alegeţi **Yes (Da)** pentru a atribui o adresă IP pentru anumite adrese MAC din reţea. În lista DHCP pot fi adăugate până la 32 de adrese MAC pentru atribuirea automată a adreselor IP.

3.8.3 Rută

Dacă reţeaua dvs. utilizează mai multe rutere wireless, puteţi configura un tabel de direcţionare pentru a beneficia de acelaşi serviciu de Internet.

NOTĂ: Vă recomandăm să nu modificaţi setările implicite ale rutei, decât dacă aveţi cunoştinţe legate de tabelele de direcţionare.

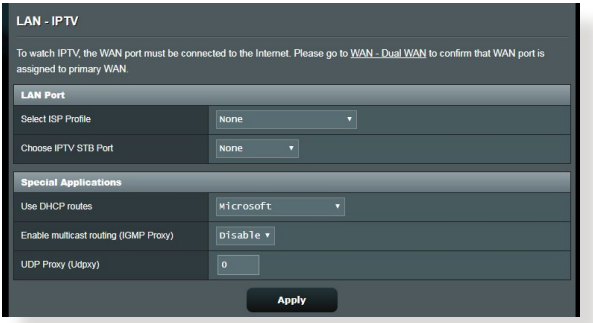


Pentru a configura tabelul de direcţionare în reţeaua LAN:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **LAN** > **Route (Rută)**.
2. În câmpul **Enable static routes (Activare rute statice)**, selectaţi **Yes (Da)**.
3. În **Static Route List (Listă rute statice)**, introduceţi informaţiile de reţea a altor puncte sau noduri de acces. Faceţi clic pe butonul **Add (Adăugare)** sau **Delete (Ştergere)** pentru a adăuga un dispozitiv în listă sau pentru a elimina un dispozitiv din listă.
4. Faceţi clic pe **Apply (Aplicare)**.

3.8.4 IPTV

Ruterul wireless acceptă conectarea la servicii IPTV prin intermediul unui ISP sau al unei reţele LAN. Fila IPTV oferă setările necesare pentru configurarea serviciilor IPTV, VoIP, de distribuire multiplă şi UDP. Contactaţi furnizorul de servicii Internet pentru a obţine informaţii specifice cu privire la serviciile disponibile.



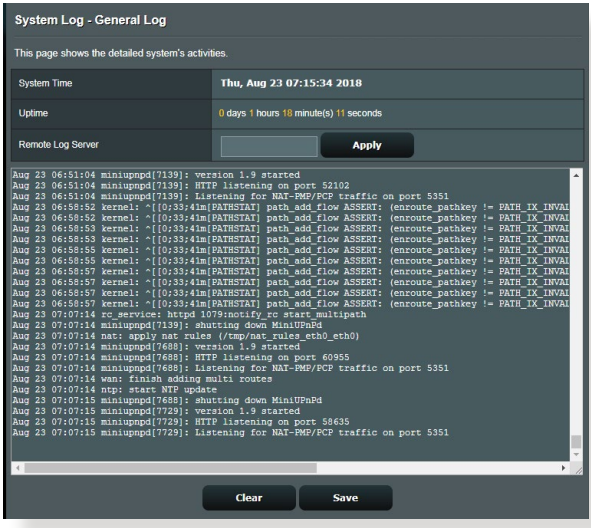
3.9 System Log (Jurnal de sistem)

Jurnalul de sistem conţine activităţile de reţea care au fost înregistrate.

NOTĂ: Jurnalul de sistem se resetează când ruterul este repornit sau oprit din funcţionare.

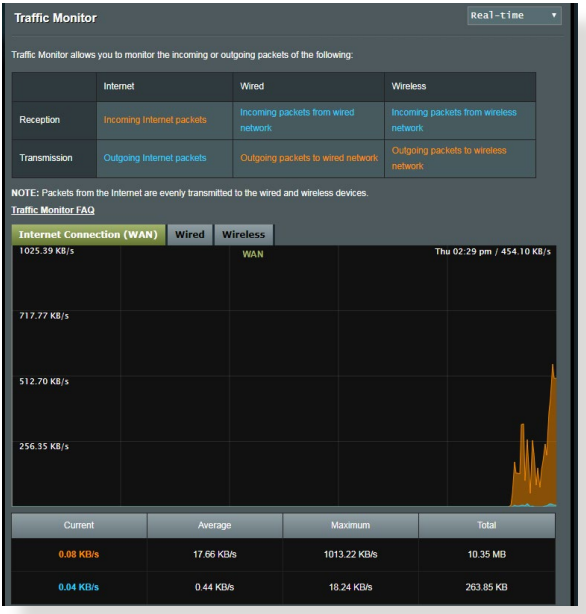
Pentru vizualizarea jurnalului de sistem:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **System Log (Jurnal de sistem)**.
2. Puteţi vizualiza activităţile din reţea în oricare din aceste file:
   - Jurnal general
   - Atribuiri DHCP
   - Jurnal wireless
   - Redirecţionare porturi
   - Tabel direcţionare



3.10 Analizor de trafic

Funcţia de monitorizare a traficului vă permite să evaluaţi utilizarea lăţimii de bandă şi viteza conexiunilor la Internet sau a reţelelor cu fir sau wireless. Această funcţie vă permite să monitorizaţi traficul din reţea în timp real sau zilnic. De asemenea, aveţi posibilitatea de a afişa traficul de reţea din ultimele 24 de ore.

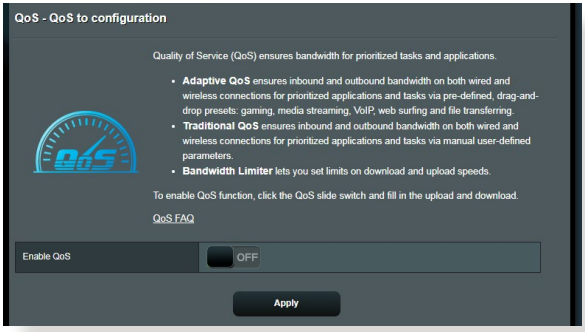


NOTĂ: Pachetele primite de la Internet sunt transmise în mod uniform către dispozitivele cu fir şi wireless.

3.11 Traffic Manager (Manager trafic)

3.11.1 Gestionarea lăţimii de bandă pentru funcţia QoS (Calitatea serviciului)

Funcţia QoS (Quality of Service – Calitatea serviciului) vă permite să setaţi prioritatea de lăţime de bandă şi să gestionaţi traficul în reţea.



Pentru a seta prioritatea lăţimii de bandă:

1. Din panoul de navigare, mergeţi la **General** > **Traffic Manager (Manager trafic)** > **QoS**.
2. Faceţi clic pe **ON (ACTIVARE)** pentru a activa regula implicită şi completaţi câmpurile pentru lăţimea de bandă de descărcare şi încărcare.

NOTĂ: Obţineţi informaţiile pentru lăţimea de bandă de la furnizorul de servicii Internet.

3. Faceţi clic pe **Save (Salvare)**.

NOTĂ: Lista cu reguli specificate de utilizatori face parte din setările avansate. Dacă doriţi să prioritizaţi anumite aplicaţii şi servicii de reţea, selectaţi **User-defined QoS rules (Reguli QoS definite de utilizator)** sau **User-defined Priority (Prioritate definită de utilizator)** din lista verticală aflată în colţul din dreapta sus.

4. În pagina **user-defined QoS rules (Reguli QoS definite de utilizator)** există patru tipuri implicite de servicii online – navigare web, HTTPS şi transferuri de fişiere. Selectaţi serviciul preferat, completaţi cu valori parametrii **Source IP or MAC (IP sau MAC sursă)**, **Destination Port (Port destinaţie)**, **Protocol**, **Transferred (Transferat)** şi **Priority (Prioritate)**, apoi faceţi clic pe **Apply (Aplicare)**. Informaţiile vor fi configurate în ecranul cu reguli QoS.

NOTE:

- Pentru a completa cu valori adresa IP sau MAC sursă, puteţi:

  a) Să introduceţi o adresă IP specifică, precum „192.168.122.1".

  b) Să introduceţi adrese IP din cadrul aceleiaşi sub-reţele sau din cadrul aceluiaşi sector IP, precum „192.168.123.*", sau „192.168.*.*"

  c) Să introduceţi toate adresele IP ca „*.*.*.*" sau să lăsaţi câmpul necompletat.

  d) Formatul adreselor MAC este reprezentat de şase grupuri de câte două caractere hexazecimale, separate prin două puncte (:), în ordinea transmiterii (de exemplu, 12:34:56:aa:bc:ef)

- Pentru intervalul de porturi sursă sau destinaţie, puteţi:

  a) Să introduceţi un port specific, precum „95".

  b) Să introduceţi porturi din cadrul unui interval, precum „103:315", „>100" sau „<65535".

- Coloana **Transferred (Transferat)** conţine informaţii despre traficul de încărcare şi descărcare (traficul de reţea de intrare şi de ieşire) pentru o secţiune. În această coloană puteţi seta limita pentru traficul de reţea (în KB) pentru un anumit serviciu, pentru a genera proprietăţi specifice pentru serviciul atribuit unui anumit port. De exemplu, dacă doi clienţi de reţea, PC 1 şi PC 2, accesează concomitent Internetul (setat la portul 80), dar PC 1 depăşeşte limita pentru traficul de reţea ca urmare a unor sarcini de descărcare, PC 1 va avea o prioritate mai redusă. Dacă nu doriţi să introduceţi limita pentru traficul de reţea, nu completaţi câmpul.

5. În pagina **User-defined Priority (Prioritate definită de utilizator)**, puteţi prioritiza pe cinci niveluri aplicaţiile de reţea sau dispozitivele din reţea, din lista verticală **user-defined QoS rules (Reguli QoS definite de utilizator)**. În funcţie de nivelul priorităţii, puteţi utiliza următoarele metode pentru a trimite pachete de date.
   - Modificaţi ordinea pachetelor de reţea care sunt trimise către Internet.
   - Sub tabelul **Upload Bandwidth (Lăţime de bandă pentru încărcare)**, setaţi **Minimum Reserved Bandwidth (Lăţime de bandă minim rezervată)** şi **Maximum Bandwidth Limit (Lăţime de bandă maxim rezervată)** în cazul în care aveţi mai multe aplicaţii de reţea cu diferite niveluri de prioritate. Procentajele indică ratele de încărcare disponibile pentru aplicaţiile de reţea specificate.

NOTE:

- Pachetele cu prioritate redusă sunt omise pentru a se asigura transmiterea pachetelor cu prioritate ridicată .
- Sub tabelul **Download Bandwidth (Lăţime de bandă pentru descărcare)**, setaţi **Maximum Bandwidth Limit (Limită maximă lăţime de bandă)** pentru a aranja într-o ordine corespunzătoare diferitele aplicaţii de reţea. Pachetele care au prioritatea mai mare la încărcare vor avea prioritate mai mare şi la descărcare.
- Dacă nu există pachete trimise de la aplicaţiile cu prioritate ridicată, întreaga rată de transmitere a conexiunii la Internet va fi disponibilă pentru pachetele cu prioritate redusă.

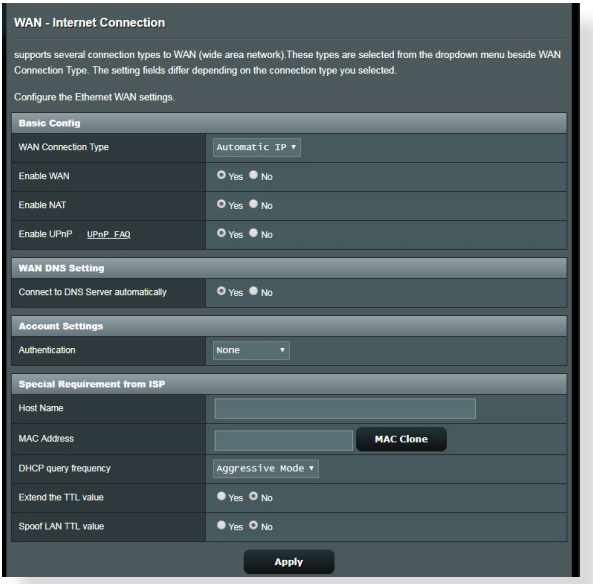
6. Setaţi pachetul cu cea mai mare prioritate. Pentru a asigura o experienţă optimă a jocurilor online, puteţi seta cea mai mare prioritate pentru pachetul ACK, SYN sau ICMP.

NOTĂ: Asiguraţi-vă că aţi activat anterior opţiunea QoS şi că aţi configurat limite pentru ratele de încărcare şi descărcare.

3.12 WAN

3.12.1 Conexiune la Internet

Ecranul Internet Connection (Conexiune Internet) vă permite să configuraţi setările pentru diverse tipuri de conexiuni WAN.



Pentru configurarea setărilor conexiunii WAN:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > **Internet Connection (Conexiune Internet)**.
2. Configuraţi următoarele setări: Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.
   - **Tip conexiune WAN**: Alegeţi tipul furnizorului de servicii Internet. Puteţi alege între Automatic IP (IP automat), PPPoE, PPTP, L2TP sau fixed IP (IP fix). Consultaţi-vă furnizorul de servicii Internet dacă ruterul dvs. nu poate obţine o adresă IP validă sau dacă aveţi dubii cu privire la tipul conexiunii WAN.
   - **Activare WAN**: Selectaţi **Yes (Da)** pentru a permite ruterului să acceseze Internetul. Selectaţi **No (Nu)** pentru a dezactiva accesul la Internet.

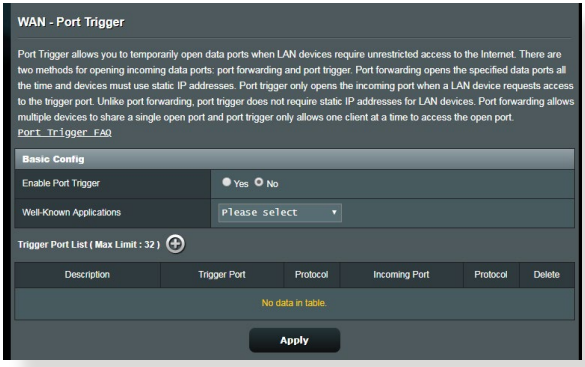
- **Activare NAT**: NAT (Network Address Translation - translatare adresă de reţea) este un sistem unde un IP public (IP de WAN) este utilizat pentru a furniza acces la Internet clienţilor de reţea care au o adresă IP privată într-un mediu LAN. Adresa IP privată a fiecărui client din reţea este salvată într-un tabel NAT şi este utilizată pentru a direcţiona pachetele de date primite.
- **Activare UPnP**: UPnP (Universal Plug and Play - plug and play universal) permite mai multor dispozitive (cum ar fi rutere, televizoare, sisteme stereo, console de jocuri şi telefoane celulare) să fie controlate printr-o reţea bazată pe IP-uri, cu sau fără un centru de comandă, prin intermediul unui gateway. UPnP conectează PC-uri indiferent de dimensiunea acestora, asigurând o reţea simplificată pentru cu capacitatea de configurare şi transfer de fişiere la distanţă. Folosind UPnP, noile dispozitive din reţea sunt descoperite în mod automat. După ce sunt conectate la reţea, dispozitivele pot fi configurate la distanţă pentru a accepta aplicaţii P2P, jocuri interactive, conferinţe video şi servere web sau proxy. Spre deosebire de protocolul de direcţionare a porturilor, care implică o configurare manuală a setărilor pentru porturi, UPnP configură în mod automat ruterul să accepte conexiunile primite şi să direcţioneze solicitările către un anumit PC din reţeaua locală.
- **Conectare la serverul DNS**: Permite acestui ruter să obţină adresa IP DNS în mod automat de la furnizorul de servicii Internet. Un server DNS este o gazdă pe Internet care translatează numele de Internet în adrese IP numerice.
- **Autentificare**: Acest element poate fi specificat de unii furnizori de servicii Internet. Consultaţi-vă furnizorul de servicii Internet şi completaţi câmpurile de autentificare, dacă este necesar.
- **Nume gazdă**: Acest câmp vă permite să introduceţi un nume de gazdă pentru ruterul dvs. Aceasta este, în general, o cerinţă specială din partea furnizorului de servicii Internet. Dacă furnizorul dvs. de servicii Internet a atribuit un nume de gazdă computerului dvs., introduceţi aici numele respectiv.

- **Adresă MAC**: Adresa MAC este un identificator unic pentru dispozitivul dvs. conectat în reţea. Unii furnizori de servicii Internet monitorizează adresa MAC a dispozitivelor din reţea care se conectează la serviciile furnizate de aceştia şi resping orice dispozitiv nerecunoscut care încearcă să se conecteze. Pentru a evita problemele de conectare cauzate de o adresă MAC neînregistrată, puteţi:
  - Să contactaţi ISP-ul şi să îi solicitaţi să vă actualizeze adresa MAC asociată abonamentului.
  - Să clonaţi sau să modificaţi adresa MAC a ruterului wireless ASUS pentru a corespunde adresei MAC a dispozitivului care era anterior recunoscut în reţea de către ISP.

3.12.2 Triggering de port

Operaţia de triggering pentru intervalul de porturi deschide un port de intrare predeterminat pentru o perioadă limitată de timp, ori de câte ori un client din reţeaua locală realizează o conexiune de ieşire pe un port specificat. Triggeringul de port este utilizat în următoarele situaţii:

- Mai mulţi clienţi locali necesită redirecţionarea prin porturi pentru aceeaşi aplicaţie, în momente diferite.
- O aplicaţie necesită anumite porturi de intrare, care diferă de porturile de ieşire.



Pentru a configura triggeringul de port:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > **Port Trigger (Triggering de port)**.
2. Configuraţi următoarele setări: Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.
   - **Activare triggering de port**: Selectaţi **Yes (Da)** pentru a activa triggeringul de port.
   - **Aplicaţii cunoscute**: Selectaţi jocurile şi serviciile web populare pe care doriţi să le adăugaţi în lista de triggering de port.
   - **Descriere**: Introduceţi o scurtă denumire sau o descriere pentru serviciu.

- **Port declanşator**: Specificaţi un port care să declanşeze deschiderea portului de intrare.
- **Protocol**: Selectaţi protocolul, TCP sau UDP.
- **Port de intrare**: Specificaţi un port de intrare pentru a primi date transmise dinspre Internet.

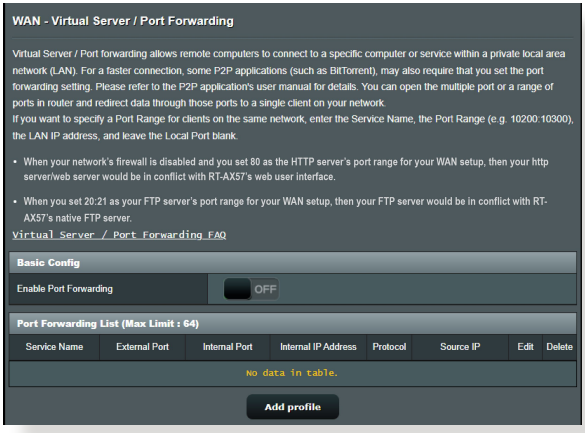
NOTE:

- Când vă conectaţi la un server IRC, un PC client realizează o conexiune de ieşire folosind intervalul de porturi declanşatoare cuprins între 66660 şi 70000. Serverul IRC răspunde prin verificarea numelui de utilizator şi crearea unei noi conexiuni la PC-ul client, utilizând un port de intrare.
- Dacă opţiunea de triggering de port este dezactivată, ruterul anulează conexiunea deoarece nu poate stabili care PC solicită accesul la serverul IRC. Când opţiunea de triggering de port este activată, ruterul atribuie un port de intrare pentru a se putea primi datele. Acest port de intrare se închide după trecerea unei anumite perioade de timp, deoarece ruterul nu poate stabili c u siguranţă momentul închiderii aplicaţiei.
- Opţiunea de triggering de port permite unui singur client din reţea să utilizeze concomitent un anumit serviciu şi un anumit port de intrare.
- Nu puteţi utiliza aceeaşi aplicaţie pentru a declanşa un port pentru mai multe PC-uri în acelaşi timp. Ruterul va direcţiona portul numai către ultimul computer, în vederea trimiterii de către acesta a unei solicitări/unui semnal de declanşare către ruter.

3.12.3 Server virtual/Redirecţionare porturi

Redirecţionarea porturilor este o metodă de direcţionare a traficului de reţea dinspre Internet, printr-un anumit port sau printr-un anumit interval de porturi, către un dispozitiv sau mai multe dispozitive din reţeaua dvs. locală. Configurarea redirecţionării porturilor pe ruterul dvs. permite PC-urilor din afara reţelei să acceseze anumite servicii furnizate de un PC din reţeaua dvs.

NOTĂ: Când opţiunea de redirecţionare a porturilor este activată, ruterul ASUS blochează traficul de intrare nesolicitat dinspre Internet şi permite răspunsuri numai din partea solicitărilor de ieşire ale reţelei LAN. Clientul de reţea nu are acces direct la Internet, şi vice versa.



Pentru a configura redirecţionarea porturilor:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > **Virtual Server/Port Forwarding (Server virtual/Redirecţionare porturi)**.

2. Configuraţi următoarele setări: Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.
   - **Activare redirecţionare porturi**: Selectaţi **Yes (Da)** pentru a activa redirecţionarea porturilor.
   - **Listă servere cunoscute**: Stabiliţi tipul de serviciu pe care doriţi să îl accesaţi.
   - **Listă jocuri cunoscute**: Element listează porturile necesare pentru ca jocurile online cunoscute să funcţioneze corect.
   - **Port server FTP**: Evitaţi atribuirea intervalului de porturi 20:21 pentru serverul FTP, deoarece acest lucru va duce la intrarea în conflict cu atribuirea nativă a ruterului în ceea ce priveşte serverul FTP.
   - **Nume serviciu**: Introduceţi numele serviciului.
   - **Interval porturi**: Dacă doriţi să specificaţi un interval de porturi pentru clienţii din aceeaşi reţea, introduceţi numele serviciului, intervalul de porturi (de exemplu, 10200:10300), adresa IP din LAN şi lăsaţi necompletat parametrul Local Port (Port local). Parametrul Port Range (Interval porturi) acceptă diverse formate, precum interval de porturi (300:350), porturi individuale (566,789) sau modul Mix (Mixt) (1015:1024,3021).

NOTE:

- Când firewall-ul reţelei dvs. este dezactivat şi dvs. setaţi valoarea 80 ca interval de porturi pentru serverul HTTP în configuraţia WAN, serverul HTTP/web va intra în conflict cu interfaţa de utilizare web a ruterului.
- O reţea foloseşte porturi pentru a realiza schimbul de date, fiecărui port fiindu-i atribuit un număr şi o anumită sarcină. De exemplu, portul 80 este utilizat pentru HTTP. Un anumit port poate fi utilizat de către o singură aplicaţie sau de către un singur serviciu la un moment dat. Prin urmare, nu este posibil ca două PC-uri să acceseze date prin acelaşi port şi în acelaşi timp. De exemplu, nu veţi putea configura opţiunea Port Forwarding (Redirecţionare porturi) pe portul 100 pentru două PC-uri în acelaşi timp.

- **IP local**: Introduceţi adresa IP a clientului din reţeaua LAN.

NOTĂ: Folosiţi o adresă IP statică pentru clientul local, pentru ca operaţia de redirecţionare a porturilor să se deruleze corect. Consultaţi secţiunea **3.8 LAN** pentru mai multe informaţii.

- **Port local**: Introduceţi un port specific pentru a primi pachetele redirecţionate. Lăsaţi acest câmp necompletat dacă doriţi ca pachetele primite să fie redirecţionate către intervalul de porturi specificat.
- **Protocol**: Selectaţi protocolul. În cazul în care aveţi dubii, selectaţi opţiunea **BOTH (Ambele)**.

Pentru a verifica dacă opţiunea Port Forwarding (Redirecţionare porturi) a fost configurată cu succes:

- Verificaţi dacă serverul sau aplicaţia este configurată şi funcţionează.
- Veţi avea nevoie de un client din afara reţelei LAN, dar care să aibă acces la Internet (denumit „client Internet"). Acest client nu trebuie să fie conectat la ruterul ASUS.
- Pe clientul Internet, folosiţi IP-ul WAN al ruterului pentru a accesa serverul. Dacă redirecţionarea porturilor este configurată cu succes, ar trebui să puteţi accesa fişierele sau aplicaţiile.

Diferenţe între triggeringul de port şi redirecţionarea porturilor:

- Triggeringul de port va funcţiona chiar dacă nu se configurează o adresă IP specifică în reţeaua LAN. Spre deosebire de redirecţionarea porturilor, care necesită o adresă IP statică în reţeaua LAN, triggeringul de port permite redirecţionarea dinamică a porturilor prin intermediul ruterului. Intervale predeterminate de porturi sunt configurate să accepte pentru o anumită perioadă de timp conexiunile primite. Triggeringul de port permite mai multor computere să execute aplicaţii care în mod normal ar necesita redirecţionarea manuală a aceloraşi porturi către fiecare PC din reţea.
- Triggeringul de port oferă o mai mare securitate decât redirecţionarea porturilor, deoarece porturile de intrare nu sunt deschise în permanenţă. Acestea se deschid numai când o aplicaţia realizează o conexiune de ieşire prin intermediul portului de declanşare.

3.12.4 DMZ

Un DMZ virtual expune un client la reţeaua Internet, permiţând acestui client să primească toate pachetele direcţionate către reţeaua dvs. LAN.

Traficul primit de pe Internet este de obicei direcţionat către un anumit client numai dacă pentru reţeaua respectivă s-a configurat redirecţionarea porturilor sau un declanşator de porturi. Într-o configuraţie de tip DMZ, un client din reţea primeşte toate pachetele de intrare.

Configurarea DMZ pentru o reţea este utilă când aveţi nevoie ca porturile de intrare să fie deschise sau când doriţi să găzduiţi un server de domenii, un server web sau un server e-mail.

ATENŢIE: Deschierea tuturor porturilor unui client face ca reţeaua să fie vulnerabilă la atacurile din exterior. Trebuie să fiţi conştient de riscurile de securitate pe care le implică o configuraţie DMZ.

Pentru a configura DMZ:

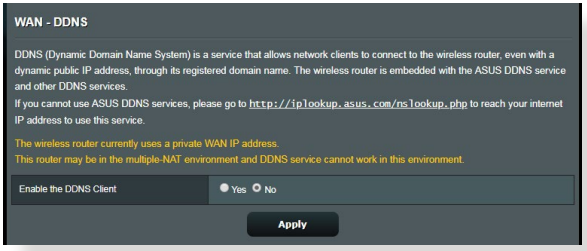
1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > **DMZ**.
2. Configuraţi următoarele setări. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.
   - **Adresa IP a staţiei expuse:** Introduceţi adresa IP pentru clientul din reţeaua LAN, client care va furniza serviciul DMZ şi care va fi expus pe Internet. Asiguraţi-vă că clientul de server are o adresă IP statică.

Pentru eliminarea DMZ:

1. Ştergeţi adresa IP a clientului din reţea LAN din caseta de text **IP address of Exposed Station (Adresa IP a staţiei expuse)**.
2. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.

3.12.5 DDNS

Configurarea DDNS (Dynamic DNS - DNS dinamic) vă permite să accesaţi ruterul din exteriorul reţelei prin intermediul serviciului ASUS DDNS sau al unui alt serviciu DDNS.



Pentru a configura DDNS:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > **DDNS**.
2. Configuraţi următoarele setări: Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.
   - **Activare client DDNS**: Activaţi DDNS pentru a accesa ruterul ASUS prin intermediul numelui DNS şi nu prin intermediul adresei IP WAN.
   - **Nume server şi gazdă**: Alegeţi ASUS DDNS sau un alt serviciu DDNS. Dacă doriţi să utilizaţi ASUS DDNS, completaţi numele gazdei în formatul xxx.asuscomm.com (xxx este numele gazdei).
   - Dacă doriţi să utilizaţi un alt serviciu DDNS, faceţi clic pe FREE TRIAL (Perioadă de încercare gratuită) şi înregistraţi-vă online mai întâi. Completaţi numele de utilizator sau adresa de mail şi parola sau cheia DDNS.
   - **Activare caracter wildcard**: Activaţi caracterul wildcard, dacă serviciul DDNS necesită acest lucru.

NOTE:

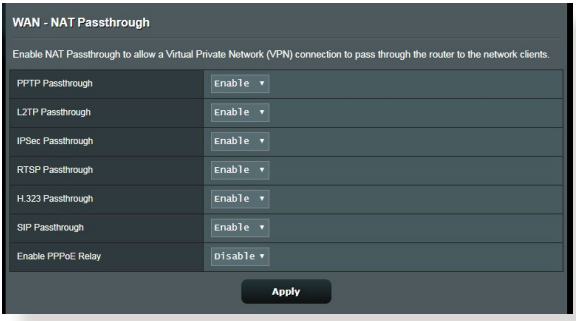
Serviciul DDNS nu va funcţiona în următoarele condiţii:

- Când ruterul wireless utilizează o adresă IP WAN privată (192.168.x.x, 10.x.x.x sau 172.16.x.x), fapt indicat printr-un text de culoare galbenă.
- Este posibil ca ruterul să se afle într-o reţea care utilizează mai multe tabele NAT.

3.12.6 NAT Passthrough (Trecere NAT)

Parametrul NAT Passthrough (Trecere NAT) permite unei conexiuni aparţinând unei reţele private virtuale să treacă prin ruter şi să fie direcţionară către clienţii din reţea. Opţiunile PPTP Passthrough (Trecere PPTP), L2TP Passthrough (Trecere L2TP), IPsec Passthrough (Trecere IPsec) şi RTSP Passthrough (Trecere RTSP) sunt activate în mod implicit.

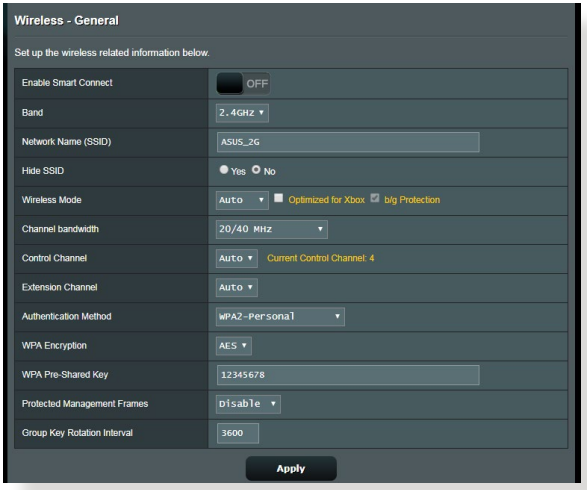
Pentru a activa/dezactiva setările pentru parametrul NAT Passthrough (Trecere NAT), mergeţi la **Advanced Settings (Setări avansate)** > **WAN** > fila **NAT Passthrough (Trecere NAT)**. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.



3.13 Wireless

3.13.1 Aspecte generale

Fila General vă permite să configuraţi setările de bază pentru reţeaua wireless.



Pentru configurarea setărilor de bază pentru reţeaua wireless:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Wireless** > **General**.
2. Selectaţi banda de frecvenţă de 2.4 GHz sau de 5 GHz pentru reţeaua dvs. wireless.
3. Atribuiţi un nume unic, care să conţină maximum 32 de caractere, pentru SSID (Service Set Identifier - identificator set servicii) sau pentru numele reţelei, cu scopul de a identifica reţeaua wireless. Dispozitivele Wi-Fi pot identifica reţeaua wireless şi se pot conecta la aceasta prin intermediul SSID-ului atribuit. SSID-urile de pe bannerul cu informaţii sunt actualizate după ce în setări sunt salvate noi SSID-uri.

NOTĂ: Puteţi atribui SSID-uri unice pentru benzile de frecvenţă de 2.4 GHz şi de 5 GHz.

4. În câmpul **Hide SSID (Ascundere SSID)**, selectaţi **Yes (Da)** pentru a împiedica dispozitivele wireless să detecteze SSID-ul dvs. Când este activată această funcţie, va trebui să introduceţi manual SSID-ul pe dispozitivul wireless pentru a accesa reţeaua wireless.
5. Selectaţi oricare din aceste opţiuni privind modul wireless pentru a stabili tipurile de dispozitive wireless care se pot conecta la ruterul wireless:
   - **Automat**: Selectaţi **Auto (Automat)** pentru a permite dispozitivelor 802.11AC, 802.11n, 802.11g şi 802.11b să se conecteze la ruterul wireless.
   - **Moştenit**: Selectaţi **Legacy (Moştenit)** pentru a permite dispozitivelor 802.11b/g/n să se conecteze la ruterul wireless. Cu toate acestea,dispozitivele care acceptă în mod nativ standardul 802.11n vor beneficia de o viteză maximă de 54 Mbps.
   - **Doar N**: Selectaţi **N only (Doar N)** pentru a maximiza performanţele standardului wireless N. Această setare previne conectarea la ruterul wireless a dispozitivelor 802.11g şi 802.11b.
6. Selectaţi oricare din aceste lăţimi de bandă pentru a obţine viteze de transmitere mai mari:

   40 MHz: Selectaţi această lăţime de bandă pentru a maximiza randamentul reţelei wireless.

   20 MHz (implicit): Selectaţi această lăţime de bandă daca întâmpinaţi probleme cu conexiunea wireless.
7. Selectaţi canalul de funcţionare pentru ruterul dvs. wireless. Selectaţi **Auto (Automat)** pentru a permite ruterului wireless să selecteze automat canalul care are cele mai puţine interferenţe.
8. Selectaţi oricare dintre aceste metode de autentificare:
   - **Sistem deschis**: Această opţiune nu oferă niciun tip de securitate.
   - **Cheie partajată**: Trebuie să utilizaţi criptarea WEP şi să introduceţi cel puţin o cheie partajată.

- **WPA/WPA2/WPA3 Personal/WPA Auto-Personal**: Această opţiune oferă o securitate puternică. Puteţi utiliza WPA (cu TKIP), WPA2 sau WPA3 (cu AES). Dacă selectaţi această opţiune, trebuie să utilizaţi criptarea TKIP + AES şi să introduceţi expresia de acces WPA (cheia de reţea).
- **WPA/WPA2/WPA3 Enterprise/WPA Auto-Enterprise**: Această opţiune oferă o securitate foarte puternică. Opţiunea are integrat serverul EAP sau un server RADIUS extern, cu autentificare de fundal.
- **Radius cu 802.1x**

NOTĂ: Ruterul dvs. wireless acceptă o rată de transmitere maximă de 54 Mbps când **Wireless Mode (Mod wireless)** este setat la **Auto (Automat)** şi **metoda de criptare** este **WEP** sau **TKIP**.

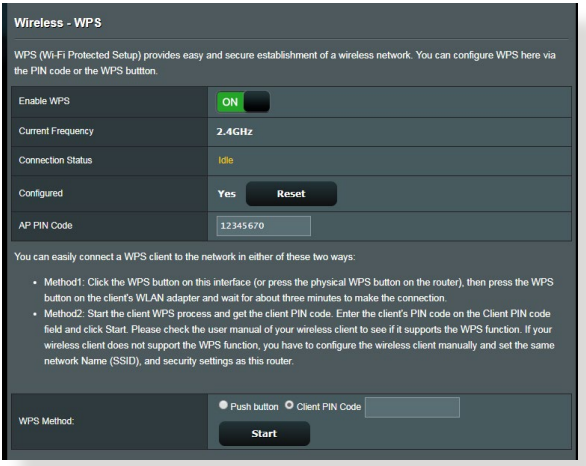
---

9. Selectaţi oricare din aceste opţiuni de criptare WEP (Wired Equivalent Privacy - confidenţialitate echivalentă cu cea a reţelelor cu fir) pentru datele transmise prin reţeaua dvs. wireless:
   - **Off (Dezactivat)**: Dezactivează criptarea WEP.
   - **64-bit (64 de biţi)**: Activează o criptare WEP slabă.
   - **128-bit (128 de biţi)**: Activează o criptare WEP îmbunătăţită.
10. Când aţi terminat, faceţi clic pe **Apply (Aplicare)**.

3.13.2 WPS

WPS (Wi-Fi Protected Setup - configurare Wi-Fi protejată) este un standard de securitate pentru rețele wireless care vă permite să conectați cu ușurință dispozitive la o rețea wireless. Puteți configura funcția WPS printr-un cod PIN sau utilizând butonul WPS.

NOTĂ: Verificați dacă dispozitivele acceptă WPS.



Pentru a activa WPS în rețeaua dvs. wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Wireless** > **WPS**.
2. În câmpul **Enable WPS (Activare WPS)**, deplasați cursorul la **ON (Activat)**.
3. În mod implicit, WPS utilizează banda de frecvență de 2.4 GHz. Dacă doriți să schimbați frecvența la 5 GHz, setați funcția WPS la **OFF (Dezactivat)**, faceți clic pe **Switch Frequency (Comutare frecvență)** din câmpul **Current Frequency (Frecvență curentă)** și apoi setați din nou funcția WPS la **ON (Activat)**.

NOTĂ: WPS acceptă autentificarea prin utilizarea standardelor Open System (Sistem deschis), WPA-Personal, WPA2-Personal şi WPA3-Personal. WPS nu acceptă reţelele wireless care utilizează metodele de criptare Shared Key (Cheie partajată), WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise şi RADIUS.

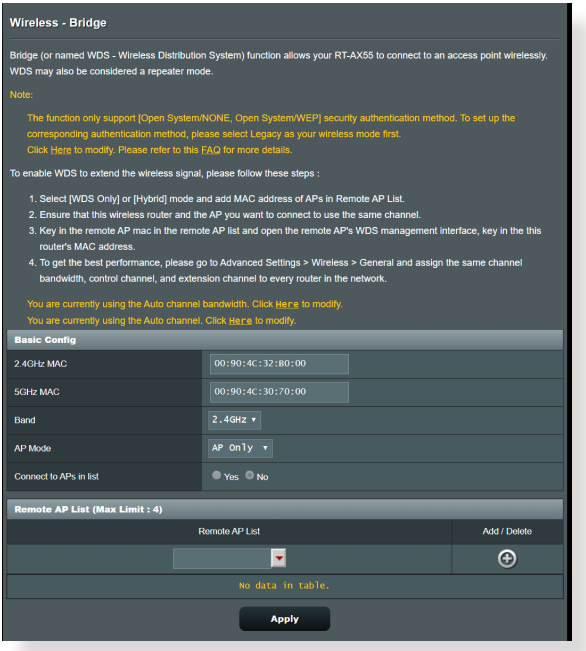
4. În câmpul WPS Method (Metodă WPS), selectaţi **Push Button (Buton de comandă)** sau **Client PIN Code (Cod PIN Client)**. Dacă selectaţi opţiunea **Push Button (Buton de comandă)**, mergeţi la pasul 5. Dacă selectaţi opţiunea **Client PIN Code (Cod PIN Client)**, mergeţi la pasul 6.
5. Pentru a configura WPS folosind butonul WPS al ruterului, urmaţi paşii de mai jos:
   a Faceţi clic pe **Start** sau apăsaţi butonul WPS care poate fi găsit în partea din spat a ruterului wireless.
   b. Apăsaţi pe butonul WPS de pe dispozitivului wireless. Acesta poate fi identificat cu ajutorul siglei WPS.

NOTĂ: Verificaţi dispozitivul wireless sau consultaţi manualul de utilizare al acestuia pentru a afla unde se află butonul WPS.

   c. Ruterul wireless va efectua scanarea pentru a detecta toate dispozitivele WPS disponibile. Dacă ruterul wireless nu găseşte niciun dispozitiv WPS, acesta va fi comutat în modul de aşteptare.
6. Pentru a configura WPS folosind codul PIN al clientului, urmaţi paşii de mai jos:
   a Localizaţi codul PIN WPS în manualul de utilizare al dispozitivului dvs. wireless sau de pe dispozitivul însuşi.
   b. Introduceţi codul PIN al clientului în caseta de text.
   c. Faceţi clic pe **Start** pentru a comuta ruterul wireless în modul de cercetare WPS. Indicatorii cu LED ai ruterului vor clipi rapid de trei ori până când configurarea WPS este finalizată.

3.13.3 WDS

Modul Punte sau WDS (Wireless Distribution System - sistem de distribuţie wireless) permite ruterului dvs. wireless ASUS să se conecteze la un alt punct de acces wireless, în mod exclusiv, împiedicând alte dispozitive sau staţii de lucru wireless să acceseze ruterul wireless ASUS. Acest mod poate fi considerat şi ca un repetator wireless, unde ruterul dvs. wireless ASUS comunică cu un alt punct de acces şi cu alte dispozitive wireless.



Pentru a configura puntea wireless:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Wireless** > **WDS.**
2. Selectaţi banda de frecvenţă pentru puntea wireless.
3. În câmpul **AP Mode (Mod AP)**, selectaţi una din aceste opţiuni:
   - **Numai AP**: Dezactivează funcţia Wireless Bridge (Punte wireless).

- **Numai WDS**: Activează funcţia Wireless Bridge (Punte wireless), dar împiedică alte dispozitive/staţii de lucru wireless să se conecteze la ruter.
- **HIBRID**: Activează funcţia Wireless Bridge (Punte wireless) şi permite altor dispozitive/staţii de lucru wireless să se conecteze la ruter.

NOTĂ: În modul Hybrid (Hibrid), dispozitivele wireless conectate la ruterul wireless ASUS vor beneficia numai de jumătate din viteza conexiunii la punctul de acces.

4. În câmpul **Connect to APs in list (Conectare la AP-uri din listă)**, faceţi clic pe **Yes (Da)** dacă doriţi să vă conectaţi la un punct de acces din lista cu puncte de acces la distanţă.
5. În câmpul **Control Channel (Canal control)**, selectaţi canalul operaţional pentru puntea wireless. Selectaţi **Auto (Automat)** pentru a permite ruterului să selecteze automat canalul care are cele mai puţine interferenţe.

NOTĂ: Disponibilitatea canalelor diferă în funcţie de ţară sau regiune.

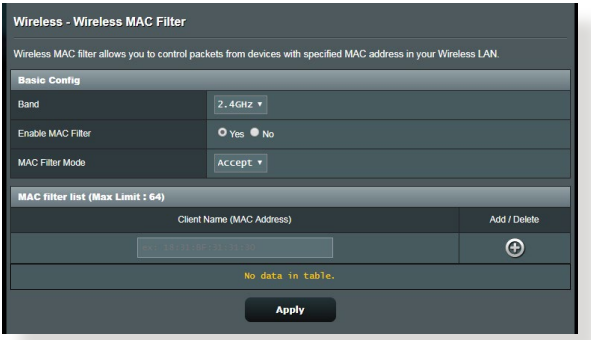
6. În lista cu puncte de acces la distanţă, introduceţi o adresă MAC şi faceţi clic pe butonul **Add (Adăugare)**  pentru a introduce adresa MAC a altor puncte de acces disponibile.

NOTĂ: Orice punct de acces adăugat la listă trebuie să se afle pe acelaşi canal de control ca şi ruterul wireless ASUS.

7. Faceţi clic pe **Apply (Aplicare)**.

3.13.4 Wireless MAC Filter (Filtru MAC wireless)

Filtrul MAC wireless asigură controlul asupra pachetelor transmise către o anumită adresă MAC (Media Access Control - control acces media) din reţeaua dvs. wireless.

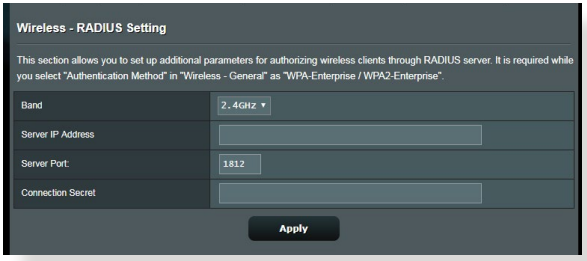


Pentru a configura filtrul MAC wireless:

1. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Wireless** > **Wireless MAC Filter (Filtru MAC wireless)**.
2. Bifaţi **Yes (Da)** în câmpul **Enable Mac Filter (Activare filtru Mac)**.
3. În lista verticală **MAC Filter Mode (Mod filtru MAC)**, selectaţi **Accept (Acceptare)** sau **Reject (Respingere)**.
   - Selectaţi **Accept (Acceptare)** pentru a permite dispozitivelor din lista de filtrare MAC să acceseze reţeaua wireless.
   - Selectaţi **Reject (Respingere)** pentru a împiedica dispozitivele din lista de filtrare MAC să acceseze reţeaua wireless.
4. În lista de filtrare MAC, faceţi clic pe butonul **Add (Adăugare)** şi introduceţi adresa MAC a dispozitivului wireless.
5. Faceţi clic pe **Apply (Aplicare)**.

3.13.5 Setarea RADIUS

Setarea RADIUS (Remote Authentication Dial In User Service - serviciu de autentificare la distanţă a utilizatorilor, prin apelare) oferă un strat suplimentar de siguranţă atunci când alegeţi opţiunea WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise sau Radius cu 802.1x ca şi mod de autentificare.



Pentru a configura setările wireless RADIUS:

1. Asiguraţi-vă că modul de autentificare al ruterului wireless este setat la WPA-Enterprise, WPA2-Enterprise sau WPA3-Enterprise.

NOTĂ: Consultaţi secţiunea **3.13.1 Aspecte generale** pentru detalii privind configurarea modului de autentificare al ruterului wireless.

2. Din panoul de navigare, mergeţi la **Advanced Settings (Setări avansate)** > **Wireless** > **RADIUS Setting (Setare RADIUS)**.
3. Selectaţi banda de frecvenţă.
4. În câmpul **Server IP Address (Adresă IP server)**, introduceţi adresa IP a serverului RADIUS.
5. În câmpul **Connection Secret (Secret conexiune)**, atribuiţi parola pentru accesarea serverului RADIUS.
6. Faceţi clic pe **Apply (Aplicare)**.

3.13.6 Professional (Profesional)

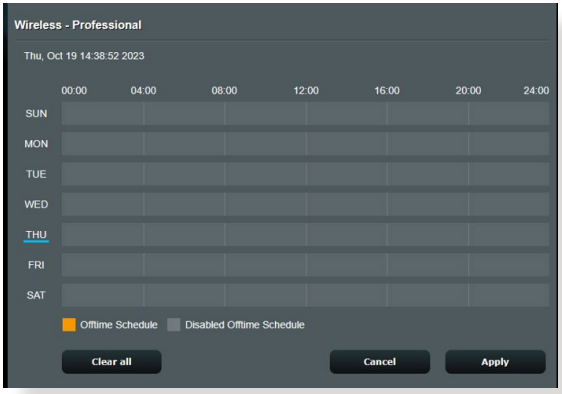
Ecranul Professional (Profesional) oferă opţiuni avansate de configurare.

NOTĂ: Vă recomandăm să folosiţi valorile implicite în această pagină.

În ecranul **Professional Settings (Setări profesionale)**, puteţi configura următoarele:

- **Frecvenţă**: Selectaţi banda de frecvenţă pentru care se vor aplica setările profesionale.
- **Activare radio**: Selectaţi **Yes (Da)** pentru a activa caracteristica wireless a reţelei. Selectaţi **No (Nu)** pentru a dezactiva caracteristica wireless a reţelei.

- **Enable wireless scheduler (Activare planificator fără fir)**: Puteţi alege formatul pentru afişarea ceasului, cu 24 de ore sau cu 12 ore. Culoarea din tabel indică Allow (Se permite) sau Deny (Se respinge). Faceţi clic pe fiecare cadru pentru a schimba setările pentru ora din zilele săptămânii şi faceţi clic pe **OK** când terminaţi.



- **Setare AP izolat**: Elementul Set AP isolated (Setare AP izolat) împiedică dispozitivele wireless din reţeaua dvs. să comunice între ele. Această caracteristică este utilă dacă se întâmplă adesea ca mulţi vizitatori să se conecteze sau să se deconecteze de la reţeaua dvs. Selectaţi **Yes (Da)** pentru a activa această caracteristică sau **No (Nu)** pentru a o dezactiva.
- **Rată distribuire multiplă (Mbps)**: Selectaţi rata de transmisie pentru distribuirea multiplă sau faceţi clic pe **Disable (Dezactivare)** pentru a dezactiva transmiterea singulară simultană.
- **Tip preambul**: Parametrul Preamble Type (Tip preambul) defineşte durata de timp pe care ruterul o alocă procesului CRC (Cyclic Redundancy Check - verificare redundanţă ciclică). CRC este o metodă de detectare a erorilor care au loc în timpul transmiterii datelor. Selectaţi **Short (Scurt)** în cazul unei reţele wireless ocupate, cu trafic intens. Selectaţi **Long (Lung)** dacă reţeaua dvs. wireless are în componenţă dispozitive wireless mai vechi.

- **Prag RTS**: Selectaţi o valoare mai mică pentru RTS (Request to Send - solicitare de trimitere) pentru a îmbunătăţi comunicarea wireless într-o reţea wireless ocupată sau cu multe interferenţe, cu trafic intens şi numeroase dispozitive wireless.
- **Interval DTIM**: Parametrul DTIM (Delivery Traffic Indication Message - mesaj de indicare a traficului de livrare) Interval (Interval DTIM) sau Data Beacon Rate (Rată semnalizator date) reprezint intervalul de timp înainte ca un semnal să fie trimis către un dispozitiv wireless în modul de inactivitate, indicând faptul că se aşteaptă livrarea unui pachet de date. Valoare implicită este de trei milisecunde.
- **Interval semnalizator**: Parametrul Beacon Interval (Interval semnalizator) reprezintă intervalul de timp între un mesaj DTIM şi următorul. Valoare implicită este de 100 milisecunde. Reduceţi valoarea pentru Beacon Interval (Interval semnalizator) în cazul unei conexiuni wireless instabile sau pentru dispozitive aflate în roaming.
- **Reglare putere TX**: Acest parametru se referă la cantitatea de miliWatti (mW) necesară pentru a alimenta semnalul radiu al ruterului wireless. Introduceţi o valoare cuprinsă între 0 şi 100.
- **Activare WMM APSD**: Activaţi parametrul WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery - livrare multimedia prin Wi-Fi cu economisire automată a energiei) pentru a optimiza modul de gestionare a energiei la transferurile între dispozitivele wireless. Selectaţi **Disable (Dezactivare)** pentru a dezactiva caracteristica WMM APSD.

4 Utilitarelor

NOTE:

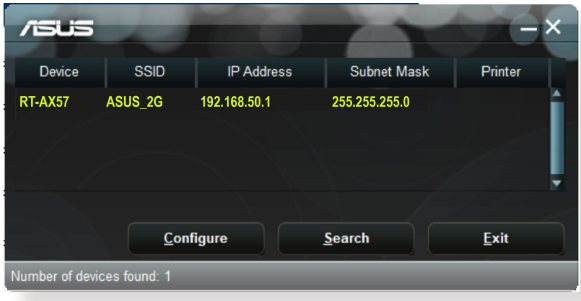
- Descărcaţi şi instalaţi utilitarele routerului wireless de pe site-ul web ASUS:
  - Utilitarul Device Discovery, versiunea 1.4.7.1, poate fi descărcat de la adresa http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
  - Utilitarul Firmware Restoration, versiunea 1.9.0.4, poate fi descărcat de la adresa http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
- Utilitarele nu sunt acceptate în sistemul de operare MAC.

4.1 Detectarea Dispozitivului

Detectarea Dispozitivului este o utilitară ASUS WLAN ce detectează dispozitivul Router ASUS şi vă permite să configuraţi setările de conectare în reţeaua wireless.

Pentru a lansa utilitara Detectează Dispozitivul

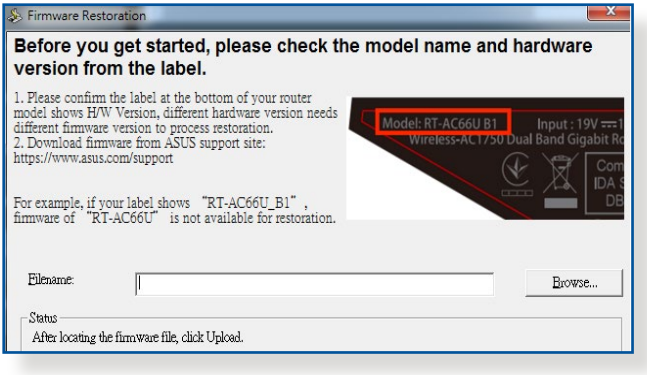
- De pe desktopul computerului dvs click **Start > All programs (Toate Programele) > ASUS Utility (Utilitară ASUS)** > **Wireless Router (Router fără cablu) > Device Discovery (Detectare Dispozitiv)**.



NOTĂ: Atunci când setaţi ruterul la modul Access Point (Punct de acces), trebuie să utilizaţi utilitarul Device Discovery (Descoperire dispozitiv) pentru a obţine adresa IP a ruterului.

4.2 Refacerea softului integrat

Utilitarul Firmware Restoration (Restabilire firmware) se utilizează pe un ruter fără fir ASUS care nu a reuşit în timpul procesului de upgrade de firmware. Acesta încarcă firmware-ul specificat. Procesul durează aproximativ trei până la patru minute.



IMPORTANT! Lansaţi modul de salvare înainte de a utiliza utilitarul Firmware Restoration (Restabilire firmware).

NOTĂ: Această caracteristică nu este acceptată în sistemul de operare MAC.

Pentru a lansa modul de salvare şi a utiliza utilitarul Firmware Restoration (Restabilire firmware):

1. Deconectaţi ruterul fără fir de la sursa de alimentare.
2. Ţineţi apăsat butonul Reset (Reiniţializare) de pe panoul din spate şi simultan conectaţi din nou ruterul fără fir la sursa de alimentare. Eliberaţi butonul Reset (Reiniţializare) atunci când LED-ul de alimentare de pe panoul frontal iluminează intermitent lent, ceea ce indică faptul că ruterul fără fir este în modul de salvare.
3. Setaţi un IP static pentru computerul dvs. şi utilizaţi următoarele instrumente pentru a configura setările TCP/IP.

   Adresă IP: 192.168.1.x

   Mască subreţea: 255.255.255.0

4. De pe desktopul computerului, faceţi clic pe **Start > All Programs (Toate programele) > ASUS Utility (Utilitară ASUS)** > **Wireless Router (Router fără cablu) > Firmware Restoration (Restabilire firmware)**.
5. Specificaţi un fişier de firmware, apoi faceţi clic pe **Upload (Încărcare)**.

NOTĂ: Acesta nu este un utilitar de upgrade de firmware şi nu poate fi utilizat pe un ruter fără fir ASUS în funcţiune. Upgrade-urile normale de firmware trebuie efectuate prin intermediul interfeţei Web. Consultaţi **Capitolul 3: Configurarea setărilor generale şi setărilor avansate** pentru mai multe detalii.

5 Remedierea defecţiunilor

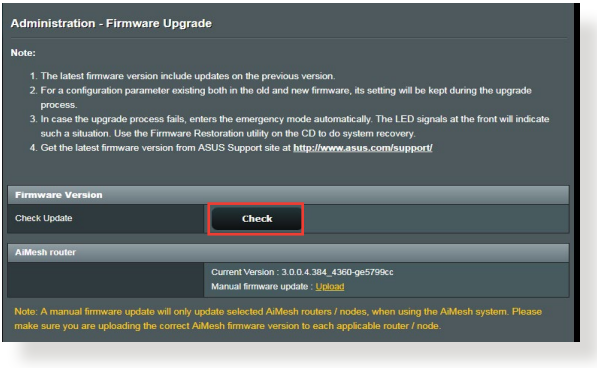
Acest capitol oferă soluţii pentru problemele pe care le puteţi întâmpina la folosirea ruterului. În cazul în care întâmpinaţi probleme care nu sunt menţionate în acest capitol, accesaţi siteul de asistenţă ASUS, la adresa: https://www.asus.com/support/. Aici puteţi găsi mai multe informaţii despre produs, dar şi detalii de contact pentru departamentul de asistenţă tehnică ASUS.

5.1 Depanarea de bază

Dacă întâmpinaţi probleme la folosirea ruterului, parcurgeţi paşii din această secţiune înainte de a căuta alte soluţii.

Upgradaţi firmware-ul la cea mai recentă versiune.

1. Lansaţi interfaţa de utilizare web. Mergeţi la **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > fila **Firmware Upgrade (Upgrade firmware)**. Faceţi clic pe **Check (Verificare)** pentru a verifica dacă este disponibil cel mai recent firmware.



2. Dacă cel mai recent firmware este disponibil, accesaţi site-ul global ASUS, la adresa https://www.asus.com/Networking/RT-AX57/HelpDesk/, pentru a descărca cel mai recent firmware.
3. Din pagina **Firmware Upgrade (Upgrade firmware)**, faceţi clic pe **Browse (Navigare)** pentru a localiza fişierul firmware.
4. Faceţi clic pe **Upload (Încărcare)** pentru upgradarea firmware-ului.

Reporniţi reţeaua în următoarea secvenţă:

1. Opriţi funcţionarea modemului.
2. Deconectaţi modemul.
3. Opriţi funcţionarea ruterului şi computerelor.
4. Conectaţi modemul.
5. Porniţi funcţionarea modemului şi apoi aşteptaţi 2 minute.
6. Porniţi funcţionarea ruterului şi apoi aşteptaţi 2 minute.
7. Porniţi funcţionarea computerelor.

Verificaţi dacă aţi conectat corect cablurile Ethernet.

- Când cablul Ethernet care conectează ruterul cu modemul este conectat corect, LEDul pentru WAN va fi aprins.
- Când cablul Ethernet care conectează computerul pornit cu ruterul cu ruterul este conectat corect, LEDul pentru conexiunea LAN corespunzătoare va fi aprins.

Verificaţi dacă setarea wireless de pe computerul dvs. corespunde cu cea a ruterului.

- Când conectaţi computerul la ruter în modul wireless, asiguraţi-vă că numele reţelei wireless (SSID), metoda de criptare şi parola sunt corecte.

Verificaţi dacă setările reţelei sunt corecte.

- Fiecare client din reţea trebuie să aibă o adresă IP validă. ASUS recomandă utilizarea serverului DHCP al ruterului wireless pentru alocarea automată a adreselor IP pentru computerele din reţea.

- Unii furnizori de servicii prin cablu necesită să utilizaţi adresa MAC a computerului care a fost înregistrat iniţial în cont. Puteţi vizualiza adresa MAC în interfaţa de utilizare web, pagina **Network Map (Hartă reţea)** > **Clients (Clienţi)**, după care poziţionaţi cursorul mouseului deasupra dispozitivului dvs. afişat în **Client status (Stare client)**.

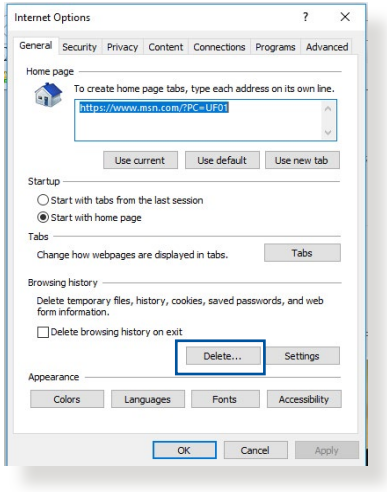
5.2 Întrebări frecvente

Nu pot accesa interfaţa de utilizare a ruterului folosindun browser web.

- În cazul în care computerul dvs. este conectat prin cablu, verificaţi conectarea cablului Ethernet şi starea LEDului, după cum s-a descris în secţiunea precedentă.
- Asiguraţi-vă că utilizaţi informaţii de conectare corecte. Asiguraţi-vă că tasta Caps Lock este dezactivată când introduceţi informaţiile de conectare.
- Ştergeţi modulele cookie şi fişierele din browserul Web. Pentru Internet Explorer, urmaţi aceşti paşi:

  1. Lansaţi Internet Explorer, apoi faceţi clic pe **Tools (Instrumente)** > **Internet Options (Opţiuni Internet)**.

  2. În**General (Generalităţi)**, sub **Browsing history (Istoric navigare)**, faceţi clic pe **Delete... (Ştergere...)**, selectaţi **Temporary Internet Files and website files (Fişiere Internet temporare şi fişiere site web)** şi **Cookies and website data (Module cookie şi date privind site-ul web)**, iar apoi faceţi clic pe **Delete (Ştergere)**.



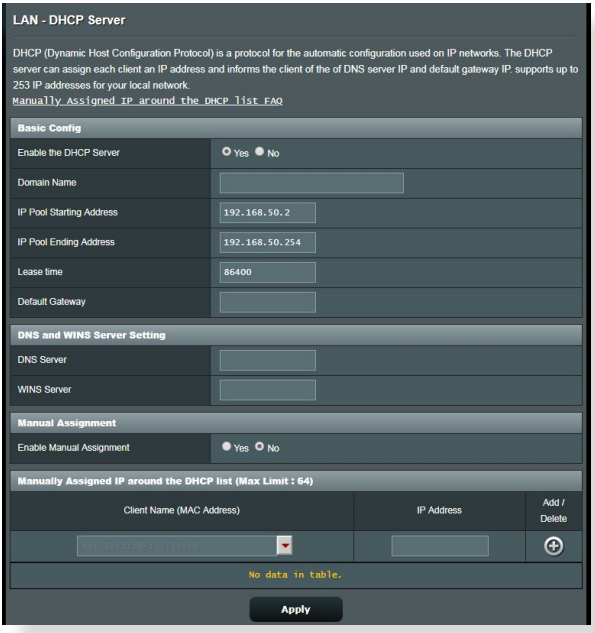
NOTE:

- Comenzile pentru ştergerea modulelor cookie şi a fişierelor diferă în funcţie de browserul Web.
- Dezactivaţi setările de server proxy, revocaţi conexiunea pe linie comutată şi configuraţi setările TCP/IP pentru a obţine automat adrese IP. Pentru mai multe detalii, consultaţi capitolul 1 din manualul utilizatorului.
- Asiguraţi-vă că utilizaţi cabluri Ethernet de tip CAT5e sau CAT6.

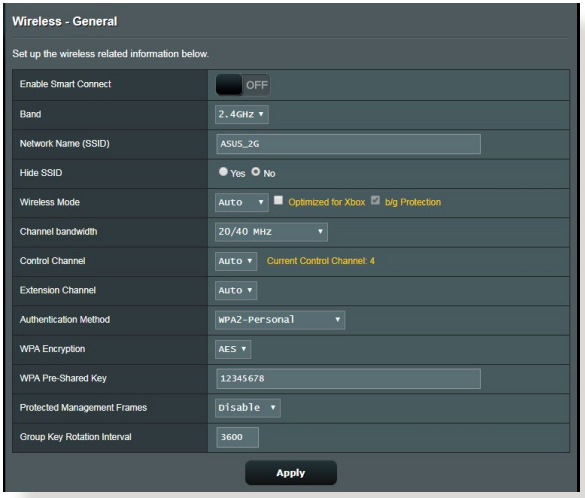
Clientul nu poate stabili o legătura wireless cu routerul.

NOTĂ: Dacă aveţi probleme la conectarea la reţeaua în banda de frecvenţă de 5 GHz, asiguraţi-vă că dispozitivul wireless acceptă această bandă sau dispune de caracteristici de conectare în bandă dublă.

- **În afara razei:**
  - Puneţi routerul mai aproape de clientul wireless.
  - Încercaţi să reglaţi antenele ruterului pentru a obţine direcţia de propagare optimă, după cum se descrie în secţiunea **1.4 Positioning your router (Poziţionarea ruterului)**.
- **Serverul DHCP a fost dezactivat:**
  1. Lansaţi interfaţa de utilizare web. Mergeţi la **General** > **Network Map (Hartă reţea)** > **Clients (Clienţi)** şi apoi căutaţi dispozitivul pe care doriţi să îl conectaţi la ruter.
  2. Dacă nu puteţi găsi dispozitivul în **Network Map (Hartă reţea)**, mergeţi la **Advanced Settings (Setări avansate)** > **LAN** > **DHCP Server (Server DHCP)**, lista **Basic Config (Configuraţie de bază)**, selectaţi **Yes (Da)** pentru parametrul **Enable the DHCP Server (Activare server DHCP)**.



- Numele reţelei (SSID) este ascuns. Dacă dispozitivul dvs. poate găsi nume de reţea (SSID) ale altor rutere, dar nu şi numele de reţea al ruterului dvs., mergeţi la **Advanced Settings (Setări avansate)** > **Wireless** > **General**, selectaţi **No (Nu)** pentru parametrul **Hide SSID (Ascundere SSID)** şi selectaţi **Auto (Automat)** pentru parametrul **Control Channel (Canal control)**.

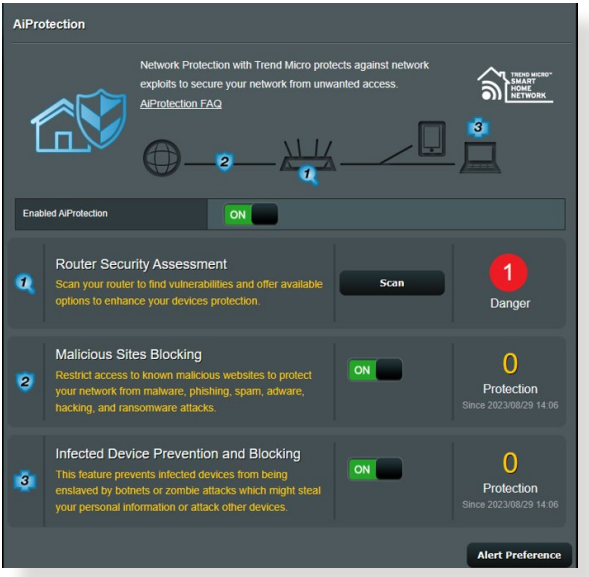


- Dacă utilizaţi un adaptor LAN wireless, verificaţi conformitatea canalului wireless în uz cu canalele disponibile în regiunea/ţara dvs. Dacă nu există conformitate, ajustaţi canalul, lăţimea de bandă a canalului şi modul wireless.
- Dacă în continuare nu vă puteţi conecta wireless la ruter, puteţi reseta ruterul la setările implicite din fabrică. În interfaţa de utilizare a ruterului, faceţi clic pe **Administration (Administrare)** > **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)** şi faceţi clic pe**Restore (Restaurare)**.

Internetul nu este accesibil.

- Verificaţi dacă ruterul dvs. se poate conecta la adresa IP WAN a furnizorului dvs. de servicii Internet. Pentru aceasta, lansaţi interfaţa de utilizare web şi mergeţi la **General**> **Network Map (Hartă reţea)** şi verificaţi parametrul **Internet status (Stare reţea)**.
- Dacă ruterul dvs. nu se poate conecta la adresa IP WAN a furnizorului dvs. de servicii Internet, încercaţi să reporniţi reţeaua aşa cum se descrie în secţiunea **Restart your network in following sequence (Reporniţi reţeaua în următoarea secvenţă)** sub **Basic Troubleshooting (Depanare de bază)**.

- Dispozitivul a fost blocat prin intermediul funcţiei Parental Control (Control parental). Mergeţi la **General** > **AiProtection** > **Parental Control (Control parental)** şi vedeţi dacă dispozitivul se află în listă. Dacă dispozitivul apare sub **Client Name (Nume client)**, eliminaţi dispozitivul folosind butonul **Delete (Ştergere)** sau ajustaţi setările privind gestionarea timpului.



- Dacă în continuare nu puteţi accesa Internetul, încercaţi să reporniţi computerul şi să verificaţi adresa IP a reţelei şi adresa gateway-ului.
- Verificaţi indicatorii de stare de pe modemul ADSL şi ruterul wireless. Dacă LEDul WAN de pe ruterul wireless nu este aprins, verificaţi dacă aţi conectat corect cablurile.

Aţi uitat numele reţelei (SSID) sau parola reţelei

- Configuraţi un nou SSID şi o nouă cheie de criptare prin intermediul unei reţele prin cablu (cablu Ethernet. Lansaţi interfaţa de utilizare web, mergeţi la **Network Map (Hartă reţea)**, faceţi clic pe pictograma ruterului, introduceţi un nou SSID şi o nouă cheie de criptare şi apoi faceţi clic pe **Apply (Aplicare)**.
- Resetaţi ruterul la setările implicite. Lansaţi interfaţa de utilizare web, mergeţi la **Administration (Administrare)** > **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)** şi faceţi clic pe**Restore (Restaurare)**.

Cum să readuc sistemul la setările sale iniţiale?

- Mergeţi la **Administration (Administrare)** > **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)** şi faceţi clic pe**Restore (Restaurare)**.

  Următoarele sunt setări iniţiale de fabrică:

  Validează DHCP: Da (când cablul WAN este conectat)

  Adresă IP: http://www.asusrouter.com (sau 192.168.50.1)

  Nume domeniu: (Gol)

  Subnet Mask: 255. 255. 255.0

  DNS Server 1: router.asus.com

  DNS Server 2: (Gol)

  SSID (2.4GHz): ASUS

  SSID (5GHz): ASUS_5G

Upgradeul de firmware a eşuat.

Lansaţi modul de recuperare înainte de a utiliza utilitarul Firmware Restoration (Restaurare firmware). Consultaţi secţiunea **4.2 Firmware Restoration (Restaurare firmware)** pentru a afla cum să utilizaţi utilitarul Firmware Restoration (Restaurare firmware).

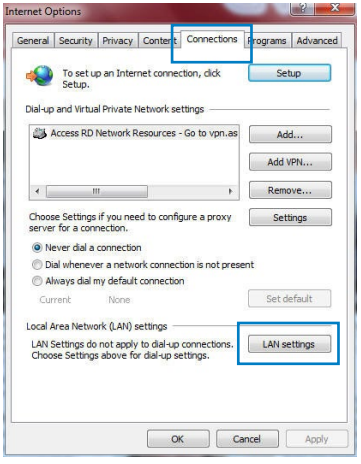
Nu se poate accesa interfaţa de utilizare web

Înainte de a configura ruterul fără fir, efectuaţi paşii descrişi în această secţiune pentru computerul gazdă şi clienţii de reţea.

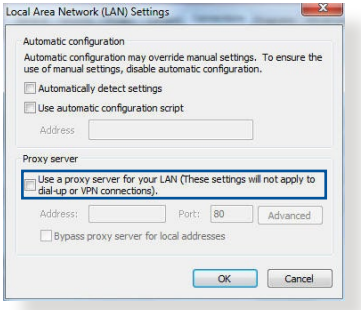
A. Dezactivaţi serverul proxy, dacă este activat.

Windows®

1. Faceţi clic pe **Start > Internet Explorer** pentru a lansa browserul web**.**
2. Faceţi clic pe **Tools (Instrumente) > Internet options (Opţiuni Internet) > fila Connections (Conexiuni) > LAN settings (Setări LAN).**

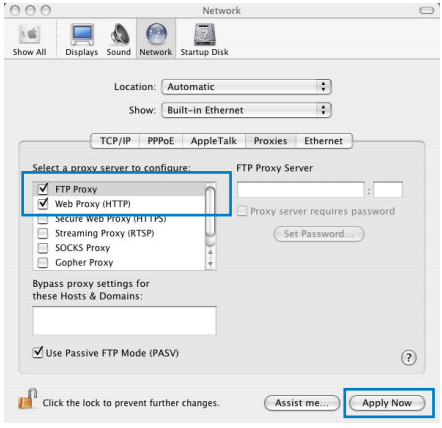


3. Din ecranul Local Area Network (LAN) Settings (Setări pentru reţeaua locală (LAN)), debifaţi opţiunea **Use a proxy server for your LAN (Utilizare server proxy pentru reţeaua locală)**.
4. Faceţi clic pe **OK** când aţi terminat.



MAC OS

1. În browserul Safari, faceţi clic pe **Safari > Preferences (Preferinţe) > Advanced (Complex) > Change Settings... (Modificare setări…)**
2. În ecranul Network (Reţea), deselectaţi **FTP Proxy (Server proxy FTP)** şi **Web Proxy (HTTP) (Server proxy Web (HTTP))**.



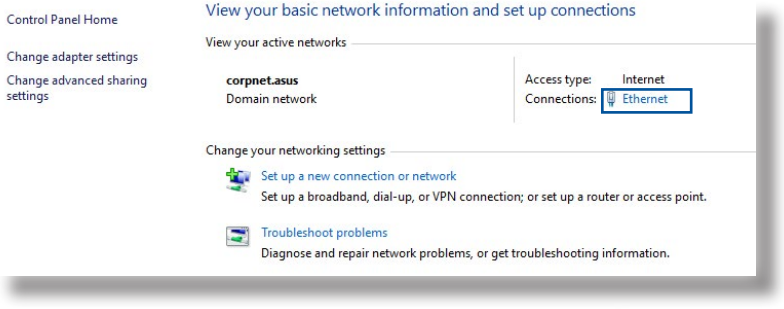
3. Faceţi clic pe **Apply Now (Se aplică acum)** când aţi terminat.

NOTĂ: Consultaţi caracteristica de ajutor a browserului pentru detalii despre dezactivarea serverului proxy.

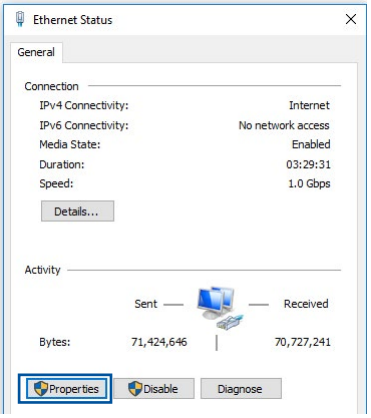
B. Configuraţi setările TCP/IP pentru obţinerea automată a unei adrese IP.

Windows®

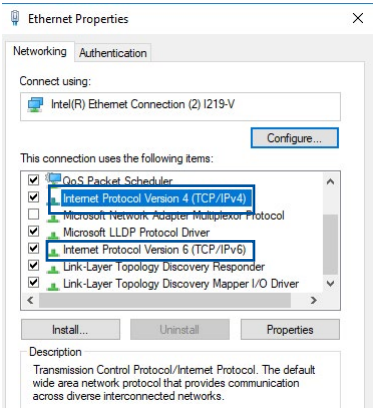
1. Faceţi clic pe **Start > Control Panel (Panou de control) > Network and Sharing Center (Centru de reţea şi partajare),** apoi faceți clic pe conexiunea de rețea pentru a afișa fereastra de stare.



2. Faceţi clic pe **Properties (Proprietăţi)** pentru a afişa fereastra Ethernet Properties (Proprietăţi Ethernet).



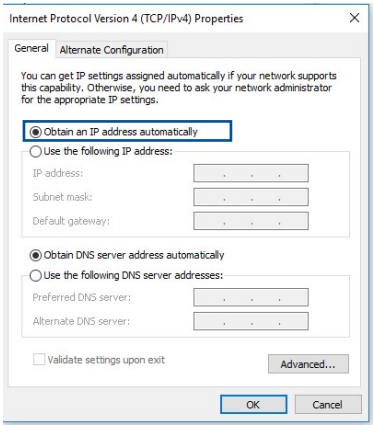
3. Selectaţi **Internet Protocol Version 4 (TCP/IPv4) (Protocol Internet versiunea 4 (TCP/IPv4)) sau Internet Protocol Version 6 (TCP/IPv6) (Protocol Internet versiunea 6 (TCP/IPv6))**, apoi faceţi clic pe **Properties (Proprietăţi)**.



4. Pentru a obţine automat setările IP iPv4, bifaţi **Obtain an IP address automatically (Se obţine automat o adresă IP)**.

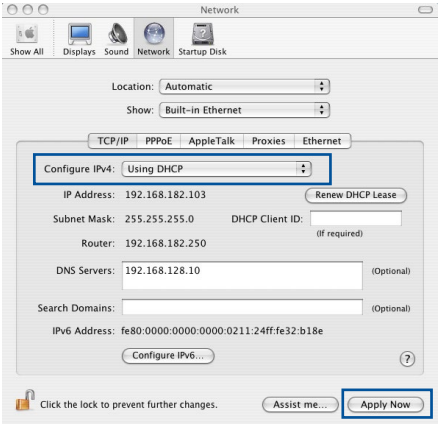
   Pentru a obţine automat setările IP iPv6, bifaţi **Obtain an IPv6 address automatically (Se obţine automat o adresă IPv6).**

5. Faceţi clic pe **OK** când aţi terminat



MAC OS

1. Faceţi clic pe pictograma Apple localizată în partea stângă sus a ecranului.
2. Faceţi clic pe **System Preferences (Preferinţe sistem) > Network (Reţea) > Configure... (Configurare...)**
3. În fila **TCP/IP**, selectaţi **Using DHCP (Se utilizează DHCP)** din lista verticală **Configure IPv4 (Configurare IPv4)**.
4. Faceţi clic pe **Apply Now (Se aplică acum)** când aţi terminat.

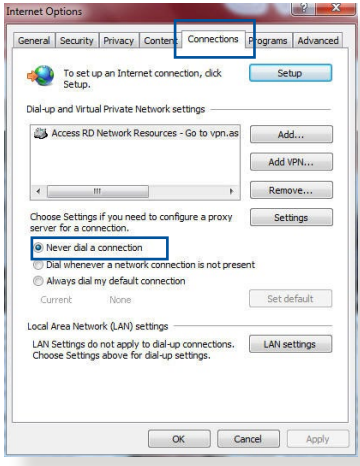


NOTĂ: Consultaţi caracteristica de ajutor şi asistenţă a sistemului de operare pentru detalii despre configurarea setărilor TCP/IP ale computerului.

C. Dezactivaţi conexiunea pe linie comutată, dacă este activată.

Windows®

1. Faceţi clic pe **Start > Internet Explorer** pentru a lansa browserul web.
2. Faceţi clic pe **Tools (Instrumente) > Internet options (Opţiuni Internet)** > fila **Connections (Conexiuni)**.
3. Bifaţi **Never dial a connection (Nu se apelează niciodată o conexiune)**.
4. Faceţi clic pe **OK** când aţi terminat.



NOTĂ: Consultaţi caracteristica de ajutor a browserului pentru detalii despre dezactivarea conexiunii pe linie comutată.

Anexă

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

Notificări de Siguranță

Când utilizați acest produs, urmați întotdeauna măsurile fundamentale de siguranță, inclusiv, dar fără a se limita la următoarele:

AVERTISMENT!

- Cablurile de alimentare trebuie să fie conectate la prize prevăzute cu o împământare adecvată. Conectați echipamentul numai la o priză din apropiere, ușor accesibilă.
- Dacă sursa de alimentare se defectează, nu încercați să o reparați singur. Contactați un tehnician de service calificat sau distribuitorul local.
- NU utilizați cabluri de alimentare, accesorii sau echipamente periferice deteriorate.
- NU montați acest echipament la o înălțime mai mare de 2 m.
- Utilizaţi PC-ul desktop în medii cu temperatura ambiantă cuprinsă între 0 ˚C (32 ˚F) şi 40 ˚C (104 ˚F).
- Citiți instrucțiunile de funcționare și intervalul de temperatură, înainte de a utiliza produsul.
- Acordați o atenție deosebită siguranței personale când utilizați acest dispozitiv în aeroporturi, spitale, benzinării și garaje profesionale.
- Interferențe cu dispozitive medicale: Mențineți o distanță minimă de cel puțin 15 cm (6 inci) între dispozitivele medicale implantate și produsele ASUS, pentru a reduce riscul de interferențe.
- Utilizați produsele ASUS în condiții bune de recepție, pentru a minimiza nivelul de radiații.
- Păstrați dispozitivul departe de femeile însărcinate și de abdomenul inferior al adolescenților.
- NU utilizați acest produs dacă pot fi observate defecte vizibile sau dacă a fost umezit, deteriorat sau modificat. Solicitați asistență din partea atelierelor de service.

AVERTISMENT!

- NU aşezaţi produsul pe suprafeţe de lucru neregulate sau instabile.
- NU plasați și nu scăpați obiecte peste produs. Evitați expunerea produsului la șocuri mecanice, cum ar fi zdrobirea, îndoirea, perforarea sau mărunțirea.
- NU dezasamblați, deschideți, încălziți cu microunde, vopsiți produsul și nu împingeți obiecte străine în produs.
- Consultați eticheta de pe partea de jos a produsului pentru a vă asigura că adaptorul dvs. este conform.
- Păstrați produsul departe de surse de foc și de căldură.
- NU expuneţi PC-ul desktop la lichide, la ploaie sau la umezeală. NU utilizați produsul în timpul unei furtuni cu descărcări electrice.
- Conectați circuitele de ieșire PoE ale acestui produs exclusiv la rețelele PoE, fără rutare către facilități externe.
- Pentru a preveni pericolul de electrocutare, deconectaţi cablul de alimentare de la priza electrică înainte de reamplasarea sistemului.
- Utilizați numai accesorii care au fost aprobate de producătorul dispozitivului pentru a funcționa cu acest model. Utilizarea altor tipuri de accesorii poate anula garanția sau poate încălca reglementările și legile locale și poate prezenta riscuri de siguranță. Contactați distribuitorul local pentru disponibilitatea accesoriilor autorizate.
- Utilizarea acestui produs într-un mod nerecomandat în instrucțiunile furnizate poate duce la un risc de incendiu sau vătămare corporală.

Service și Asistență

Vizitați site-ul nostru multilingv, la adresa https://www.asus.com/support/.