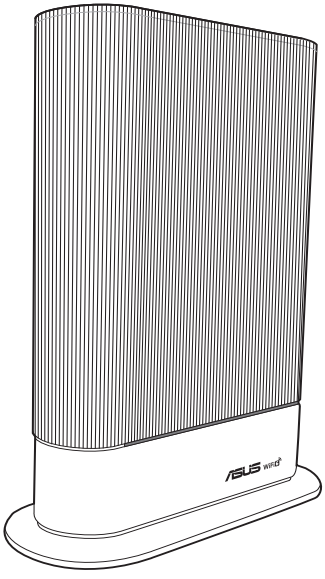
Ghidul utilizatorului

RT-AX59U

Router Wi-Fi cu două benzi



IN SEARCH OF INCREDIBLE

RO22545
Prima ediție
Octombrie 2023

Sumar

Sumar

Sumar

1 Cum să vă cunoaşteţi routerul

1.1 Bine aţi venit!

Vă mulţumim pentru achiziţionarea unui ruter wireless ASUS, model RT-AX59U!

Routerul elegant dispune de benzi dual la 2,4 GHz şi 5 GHz pentru redare concomitentă în flux HD wireless de neegalat; server SMB, server UPnP AV şi server FTP pentru partajare de fişiere 24 de ore/7 zile; capacitate de administrare a până la 300 000 de sesiuni; tehnologie de reţea Green de la ASUS, care asigură până la 70% dintre soluţiile de economisire a energiei.

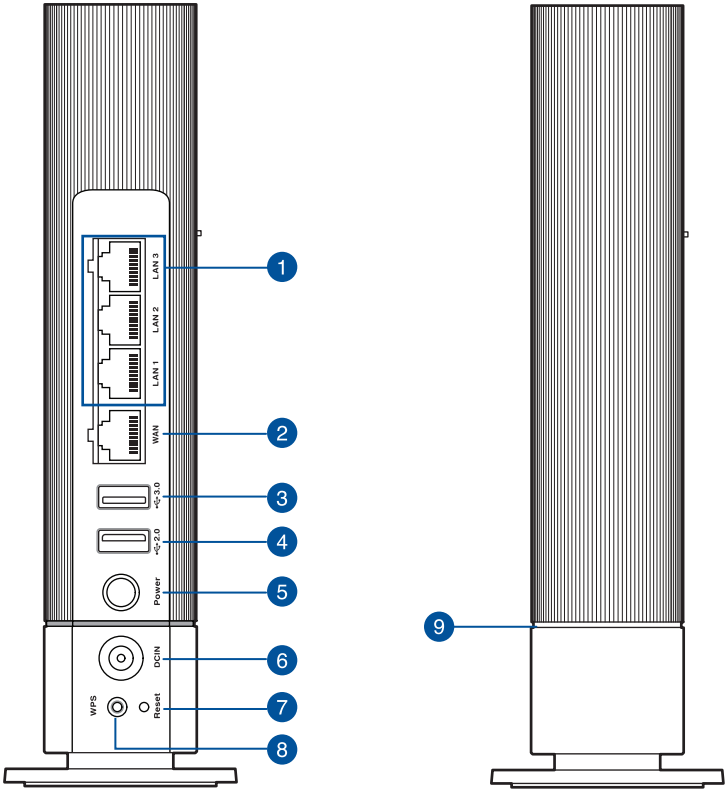
1.2 Conţinutul pachetului

☑ Router RT-AX59U TUF fără fir
☑ Adaptor de alimentare
☑ Cablu RJ45
☑ Ghid rapid de pornire

NOTE:

- Dacă oricare dintre articole este deteriorat sau lipseşte, contactaţi ASUS pentru informaţii şi asistenţă tehnică. Consultaţi lista de linii telefonice de asistenţă ASUS 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	**Porturi LAN 1 ~ 3** Conectați cabluri de rețea la aceste porturi pentru a stabili o conexiune LAN.
2	**Port WAN (Internet)** Conectați un cablu de rețea la acest port pentru a stabili o conexiune WAN.
3	**Port USB 3.2 Gen 1** Introduceți un dispozitiv compatibil cu USB 3.2 Gen 1 din prima generație, cum ar fi un hard disk USB, o unitate flash pentru USB, un smartphone sau o imprimantă, în acest port.
4	**Port USB 2.0** Introduceți un dispozitiv compatibil cu USB 2.0, cum ar fi un hard disk USB, o unitate flash pentru USB, un smartphone sau o imprimantă, în acest port.

5	**Buton de alimentare** Apăsați acest buton pentru a porni sau opri sistemul.
6	**Port alimentare (Intrare c.c.)** Inserați adaptorul de c.a. în acest port și conectați ruterul la o sursă de alimentare.
7	**Buton resetare** Acest buton reinițializează sau restabilește sistemul la setările implicite din fabrică.
8	**Buton WPS** Apăsați lung butonul pentru a lansa Expertul WPS.
9	**Indicator LED** Albastru constant: RT-AX59U este pregătit pentru configurare Alb constant: RT-AX59U este online și funcționează bine Roșu constant: Router-ul dvs. RT-AX59U nu are conexiune la Internet Nodul dvs. este deconectat de la router Galben constant: Semnalul dintre router-ul dvs. RT-AX59U și nod este slab

NOTE:

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

Adaptor de alimentare c.c.	Ieşire c.c.: +12 V cu curent max. de 2.5 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 Poziționarea ruterului

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

- Aşezați ruterul fără fir într-o zonă centrală pentru o acoperire fără fir maximă pentru dispozitivele de rețea.
- Feriți dispozitivul de obstacole de metal şi de lumina directă a soarelui.
- Feriți 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 interferențele sau pierderea semnalului.
- Actualizați întotdeauna la cel mai recent firmware. Vizitați site-ul Web ASUS la adresa **http://www.asus.com** pentru a obține cele mai recente actualizări de firmware.
- Pentru a asigura un semnal optim de rețea fără fir, orientați cele patru antene detaşabile conform ilustrației de mai jos.

1.5 Cerințe pentru configurare

Pentru a vă configura rețeaua, aveți nevoie de unul sau de două computere care să întrunească următoarele cerințe 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 capabilități încorporate de wireless, puteți instala un adaptor WLAN IEEE 802.11a/b/g/n/ac/ax în computerul dvs. pentru a vă conecta la rețea.
- Dispunând de tehnologia de bandă dual, routerul dvs. wireless acceptă simultan semnale de rețea wireless 2,4 GHz şi 5 GHz. Acest lucru vă permite să efectuați activități legate de Internet, de exemplu puteți naviga pe Internet sau puteți citi/scrie mesaje de mail utilizând banda de 2,4 GHz, iar în acelaşi timp puteți reda în flux fişiere de definiție ridicată audio/video, ca de exemplu muzică sau filme, pe banda de 5 GHz.
- Unele dispozitive compatibile cu standardul IEEE 802.11n pe care doriți să le conectați la rețeaua dvs. este posibil să accepte sau nu banda de frecvență de 5 GHz. Citiți manualul dispozitivului pentru specificații.
- Cablurile Ethernet RJ-45 care vor fi utilizate pentru conectarea dispozitivelor de rețea 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 şi 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!

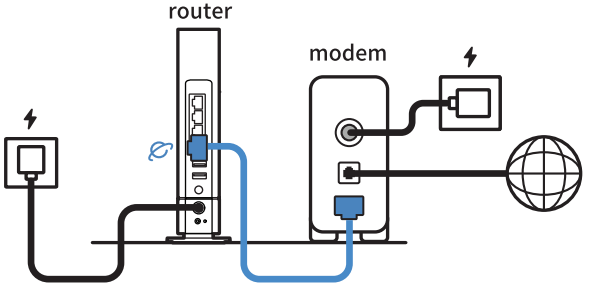
- Utilizați o conexiune cu fir pentru setarea ruterului wireless pentru a evita eventualele probleme de configurare.
- Înainte de a configura ruterul fără fir ASUS, efectuați următoarele acțiuni:
- Dacă înlocuiți un ruter existent, deconectați-l de la rețea.
- Deconectați cablurile/firele de la instalația de modem existentă. Dacă modemul dispune de o baterie de rezervă, scoateți-o şi pe aceasta.
- Reporniți computerul (recomandat).

A. Conexiune cu fir

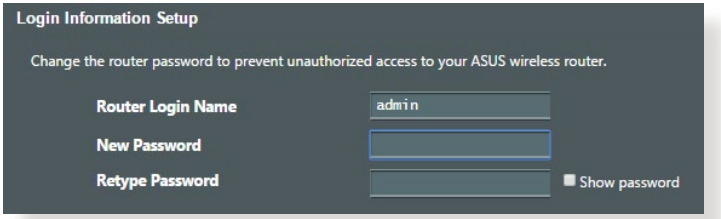
NOTĂ: Puteți folosi un cablu de conexiune directă sau un cablu crossover (inversor) pentru conexiunea cu fir.

Puteți configura ruterul prin conexiune cu fir sau wireless:

1. După ce lumina de stare se aprinde albastru solid, este gata de configurare.



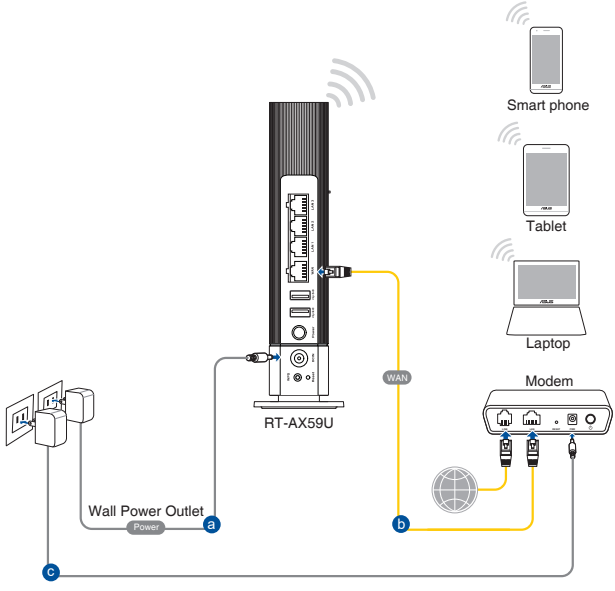
2. Interfața GUI web se lansează automat atunci când deschideți un browser web. Dacă nu se lansează automat, introduceți http://www.asusrouter.com.
3. Configurați o parolă pentru ruter în vederea prevenirii accesului neautorizat.



B. Conexiune fără fir

Puteți configura ruterul prin conexiune cu fir sau wireless:

1. Conectați ruterul la o priză de curent şi porniți-l.



2. Conectați-vă la numele de rețea (SSID) afişat pe eticheta de produs de pe partea din spate a ruterului. Pentru o securitate de rețea mai bună, modificați la un SSID unic şi atribuiți o parolă.

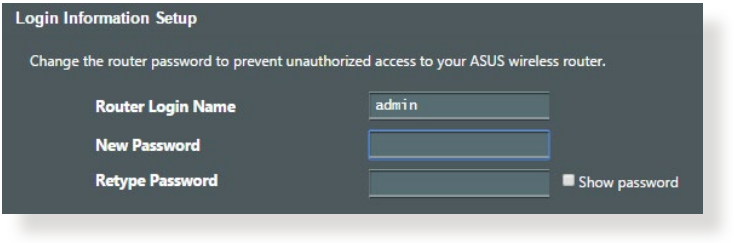
Wi-Fi Name (SSID):	ASUS_XX

* **XX** se referă la ultimele două cifre ale adresei MAC 2,4 GHz. O puteți găsi pe eticheta de pe spatele dispozitivului router ASUS.

3. Odată ce sunteți conectat, interfața GUI web se lansează automat atunci când deschideți un browser web. Dacă nu se lansează automat, introduceți http://www.asusrouter.com.
4. Configurați o parolă pentru ruter în vederea prevenirii accesului neautorizat.

NOTE:

- Pentru detalii referitoare la o rețea wireless, consultați manualul de utilizare al adaptorului WLAN.
- Pentru a configura setările de securitate pentru rețeaua dvs., consultați secțiunea **Configurarea setărilor de securitate pentru rețea** din Capitolul 3 al acestui manual de utilizare.



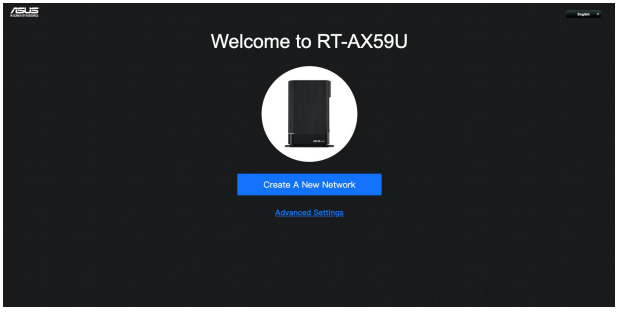
2.2 Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată

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

NOTĂ: Când setați conexiunea la Internet pentru prima dată, apăsați pe butonul de resetare de pe ruterul fără fir pentru a-l reinițializa la setările implicite din fabrică.

Pentru a utiliza QIS cu detectare automată:

1. Lansați un browser web. Veți fi redirecționat către expertul de configurare ASUS (configurare rapidă internet). Dacă nu sunteți redirecționat, introduceți adresa http://www.asusrouter.com manual.

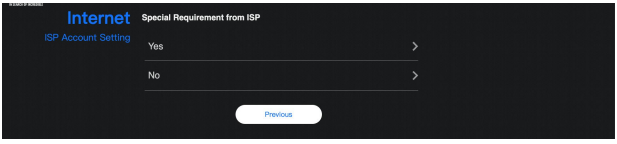


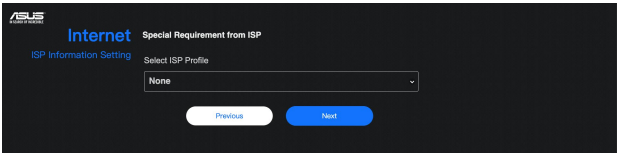
2. Ruterul wireless detectează automat dacă tipul conexiunii de la ISP este **Dynamic IP (IP dinamic)**, **PPPoE**, **PPTP**, şi **L2TP**. Tastați informațiile utile pentru tipul de conexiune furnizat de ISP.

IMPORTANT! Obțineți informațiile necesare referitoare la tipul de conexiune la Internet de la ISP-ul dvs.

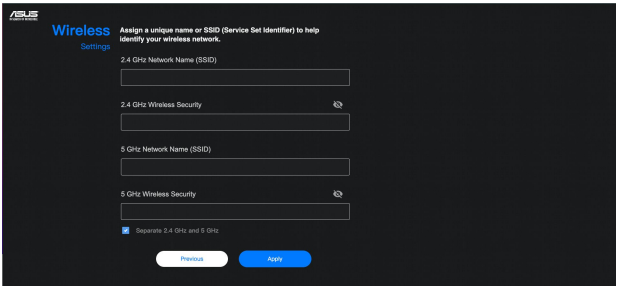
NOTE:

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

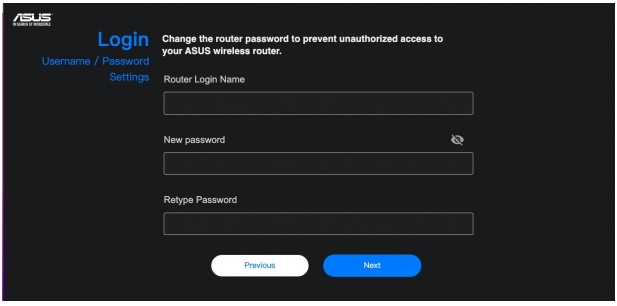




3. Atribuiți numele de rețea (SSID) şi cheia de securitate pentru conexiunea fără fir de 2,4 GHz şi 5 GHz. Faceți clic pe **Apply (Se aplică)** când ați terminat.



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



NOTĂ: Numele de utilizator și parola ruterului dvs. wireless sunt diferite față de numele rețelei (SSID) în banda de frecvență de 2,4 GHz/5 GHz și față de cheia de securitate a acesteia. Numele de utilizator și parola ruterului dvs. wireless vă permit să vă conectați la interfața de utilizare web a ruterului dvs. wireless, cu scopul de a configura setările ruterului dvs. wireless. Numele de rețea (SSID) în banda de frecvență de 2,4 GHz/5 GHz și cheia de securitate a acesteia permit dispozitivelor Wi-Fi să se autentifice și să se conecteze la rețeaua dvs. în banda de frecvență de 2,4 GHz/5 GHz.

2.3 Conectarea la rețeaua dvs. wireless

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

Pentru a vă conecta la rețea:

1. Pe computer, faceți clic pe pictograma de rețea  din zona de notificări pentru a afișa rețelele wireless disponibile.
2. Selectați rețeaua wireless la care doriți să vă conectați, apoi faceți clic pe **Connect (Conectare)**.
3. Pentru o rețea wireless securizată este posibil să fie necesară introducerea cheii de securitate, după care faceți clic pe **OK**.
4. Aşteptați până când computerul dvs. stabileşte cu succes conexiunea la rețeaua wireless. Starea conexiunii este afişată şi pictograma de rețea afişează starea de conectare  .

NOTE:

- Consultați capitolele următoare pentru mai multe detalii cu privire la configurarea setărilor rețelei dvs. wireless.
- Consultați manualul de utilizare al dispozitivului dvs. pentru mai multe detalii privind conectarea la o rețea wireless.

3 Configurarea setărilor generale şi setărilor avansate

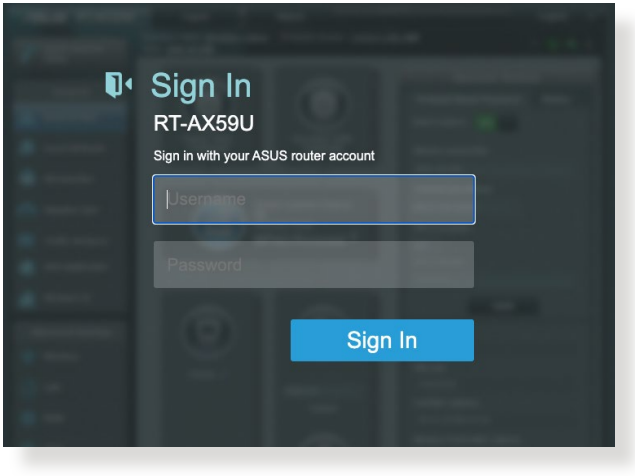
3.1 Conectarea la interfața Web GUI

Routerul wireless ASUS are o interfață grafică web intuitivă, care vă permite să configurați cu ușurință diversele sale funcții printr-un browser web, cum ar fi Internet Explorer, Firefox, Safari sau Google Chrome.

NOTĂ: Caracteristicile pot diferi în funcție de versiunea firmware.

Pentru a vă conecta la interfața Web GUI:

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



3. Puteți utiliza interfața de utilizare web pentru a configura diverse setări pentru ruterul dvs. wireless ASUS.

NOTĂ: Dacă vă conectați la interfața de utilizare web pentru prima dată, veți fi direcționat automat către pagina Quick Internet Setup (QIS – Configurare rapidă Internet).

3.2 Adaptive QoS (QoS adaptiv)

Această caracteristică asigură lățimea de bandă necesară pentru activitățile şi aplicațiile prioritizate.

Pentru a configura QoS adaptiv:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Adaptive QoS (QoS adaptiv)** > **QoS**.
2. Din panoul **Enable QoS (Activare QoS)**, faceți clic pe **ON (ACTIVAT)**.
3. Selectați QoS Type (Tip QoS) (Adaptive (Adaptiv) QoS, Traditional (Tradițional) QoS sau Badwidth limiter (Limitator lățime de bandă)) pentru configurația dvs.

   NOTĂ: Consultați informațiile dinQoS pentru a afla definiția tipului de QoS.

4. Faceți clic pe **Automatic Setting (Setare automată)** pentru lățimea de bandă optimă în mod automat sau pe **Manual Setting (Setare manuală)** pentru a seta manual lățimea de bandă de încărcare și descărcare.

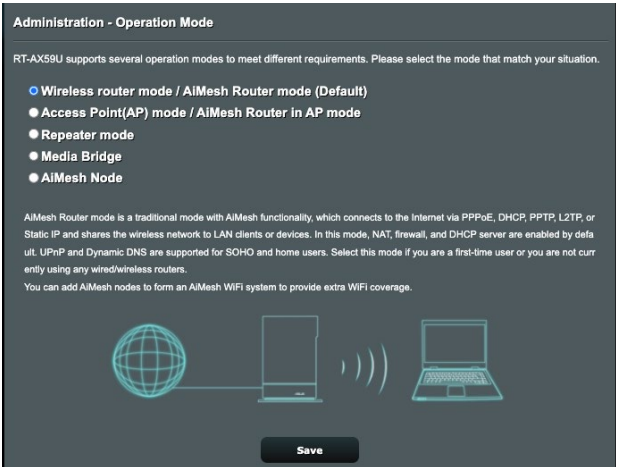
   NOTĂ: Obțineți informațiile pentru lățimea de bandă de la furnizorul de servicii Internet. De asemenea, puteți accesa http://speedtest.net pentru a verifica și obține informații cu privire la lățimea de bandă.

5. Faceți clic pe **Apply (Aplicare)**.

3.3 Administration (Administrare)

3.3.1 Operation mode (Mod de funcționare)

Pagina Operation Mode (Mod funcționare) vă permite să selectați un mod de funcționare corespunzător pentru rețeaua dvs.



Pentru a configura modul de funcționare:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > **Operation Mode (Mod de funcționare)**.
2. Selectați oricare dintre aceste moduri de funcționare:
   - **Mod ruter wireless / Mod ruter AiMesh (implicit)**: În modul ruter wireless, ruterul wireless se conectează la Internet şi furnizează acces la Internet dispozitivelor disponibile din propria rețea locală.
   - **Mod punct de acces (AP) / Router AiMesh în modul AP**: În acest mod, ruterul creează o rețea wireless nouă pe baza unei rețele existente.
   - **Mod Repetator:** În modul Repetator, dispozitivul RT-AX59U se conectează wireless la o rețea wireless existentă, cu scopul de a extinde aria de acoperire. În acest mod, funcțiile paravanului de protecție, de partajare IP şi NAT sunt dezactivate.

- **Punte media:** Această configurație necesită două rutere wireless. Cel de-al doilea ruter joacă rolul de punte media, iar în această situație mai multe dispozitive, precum televizoare inteligente şi console de jocuri, pot fi conectate prin Ethernet.
- **Nod AiMesh**: Această configurare necesită cel puțin două rutere ASUS care acceptă AiMesh. Activați nodul AiMesh și conectați-vă la interfața web a ruterului AiMesh pentru a căuta nodurile AiMesh disponibile din apropiere pentru a vă alătura sistemului AiMesh. Sistemul AiMesh oferă o acoperire în toată casa și o gestionare centralizată.

3. Faceți clic pe **Apply (Aplicare)**.

NOTĂ: Ruterul va reporni după ce schimbați modul de funcționare.

3.3.2 System (Sistem)

Pagina **System (Sistem)** vă permite să configurați setările ruterului wireless.

Pentru configurarea setărilor sistemului:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > **System (Sistem)**.
2. Puteți configura următoarele setări:
   - **Schimbare parolă de conectare ruter**: Puteți schimba parola şi numele de conectare pentru ruterul wireless introducând un nume nou şi o parolă nouă.
   - **Fus orar**: Selectați fusul orar pentru rețeaua dvs.
   - **Server NTP**: Ruterul wireless poate accesa un server NTP (Network time Protocol - Protocol oră rețea) pentru a sincroniza ora.
   - **Activare Telnet**: Faceți clic pe **Yes (Da)** pentru a activa serviciile Telnet pentru rețea. Faceți clic pe **No (Nu)** pentru a dezactiva serviciile Telnet.
   - **Metodă autentificare**: Puteți selecta HTTP, HTTPS sau ambele protocoale pentru a securiza accesul la ruter.
   - **Activare acces web prin WAN**: Selectați **Yes (Da)** pentru a permite dispozitivelor din afara rețelei să acceseze setările interfeței de utilizare a ruterului wireless. Selectați **No (Nu)** pentru a interzice accesul.

- **Se permit doar anumite IP-uri**: Faceți clic pe **Yes (Da)** dacă doriți să specificați adresele IP ale dispozitivelor care au permisiunea de a accesa setările interfeței de utilizare a ruterului wireless din WAN.
- **Listă clienți**: Introduceți adresele IP WAN ale dispozitivelor din rețea care au permisiunea de a accesa setările ruterului wireless. Lista va fi utilizată dacă ați făcut clic pe **Yes (Da)** în elementul **Only allow specific IP (Se permit doar anumite IP-uri)**.

3. Faceți clic pe **Apply (Aplicare)**.

3.3.3 Actualizarea softului integrat

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

Pentru actualizarea softului integrat:

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

NOTE:

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

3.3.4 Refacerea/Salvarea/Încărcarea setărilor

Pentru a reface/salva/încărca setările:

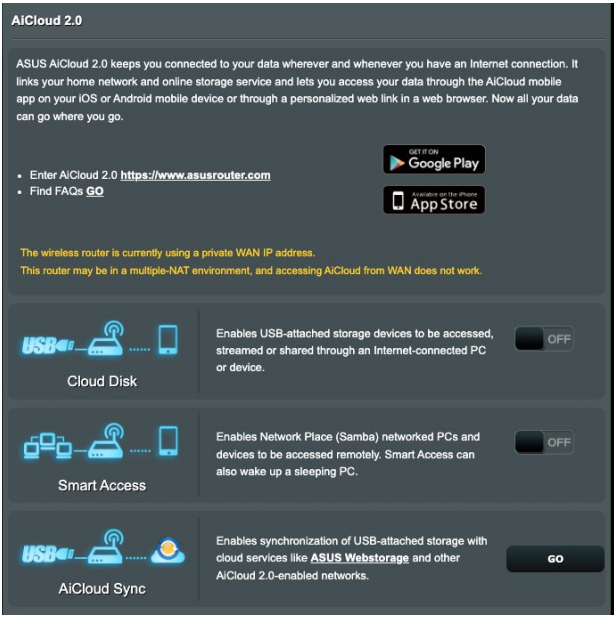
1. Din panoul de navigare, mergeți la fila **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)**.
2. Selectați sarcina pe care doriți s-o îndepliniți:

- Pentru a reface setările inițiale din fabrică, faceți click pe **Restore (Refacere)** apoi click **OK** în mesajul de confirmare.
- Pentru a salva setările curente de sistem, faceți clic pe **Save (Salvare)**, navigați la folderul în care intenționați să salvați fișierul şi faceți clic pe **Save (Salvare)**.
- Pentru a reface setarea sistemului anterior, click **Browse (Răsfoiește)** pentru a localiza fișierul sistemului pe care doriți să.l refaceți apoi faceți click pe **Upload (Încărcare)**.

IMPORTANT! Dacă apar probleme, încărcați cea mai recentă versiune de firmware şi configurați noile setări. Nu restaurați setările implicite ale ruterului.

3.4 AiCloud 2.0

AiCloud 2.0 este o aplicație de servicii cloud care vă permite să salvați, sincronizați, partajați și accesați fișierele dvs.



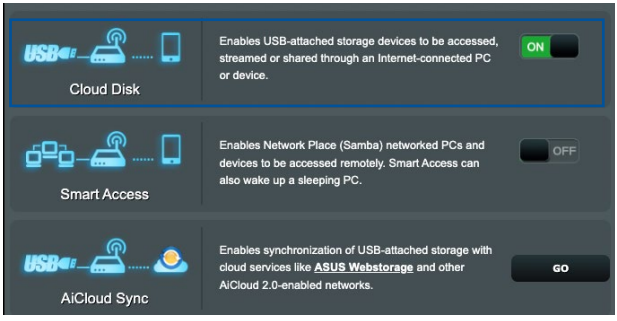
Pentru a utiliza AiCloud:

1. Din Google Play Store sau Apple Store, descărcați și instalați aplicația ASUS AiCloud pe dispozitivul dvs. inteligent.
2. Conectați dispozitivul inteligent la rețeaua dvs. Urmați instrucțiunile pentru finalizarea procesului de configurare AiCloud.

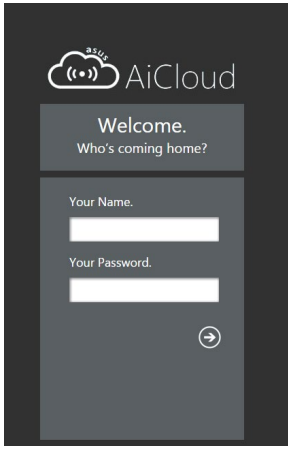
3.4.1 Cloud Disk

Pentru a crea un disc cloud:

1. Inserați un dispozitiv de stocate USB în ruterul wireless.
2. Porniți aplicația **Cloud Disk**.

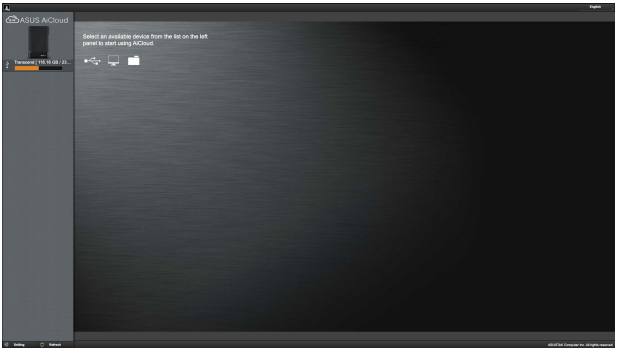


3. Mergeți la **http://www.asusrouter.com** şi introduceți numele de cont şi parola pentru ruterul dvs. Pentru o experiență optimă, vă recomandăm să utilizați **Google Chrome** sau **Firefox**.



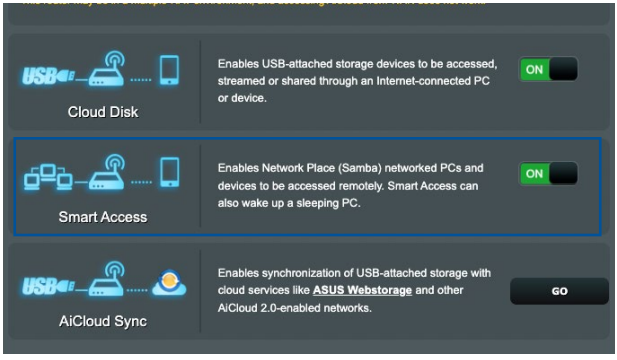
4. Acum veți putea începe să accesați fișierele aflate pe dispozitivele conectate în rețea, prin intermediul Cloud Disk.

NOTĂ: Când accesați dispozitivele care sunt conectate la rețea, trebuie să introduceți manual numele de utilizator şi parola dispozitivului, deoarece acestea nu sunt salvate de către AiCloud, din motive de securitate.



3.4.2 Smart Access

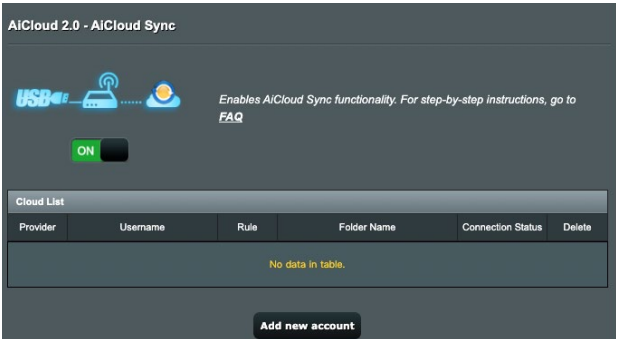
Funcția Smart Access vă permite să accesați cu ușurință rețeaua de acasă, prin intermediul numelui de domeniu al ruterului dvs.



NOTE:

- Puteți crea un nume de domeniu pentru ruterul dvs. cu ajutorul ASUS DDNS. Pentru mai multe detalii, consultați secțiunea **3.18.6 DDNS**.
- În mod implicit, AiCloud oferă o conexiune HTTPS securizată. Introduceți adresa https://[yourASUSDDNSname].asuscomm.com pentru a utiliza aplicațiile Cloud Disk şi Smart Access în cele mai sigure condiții.

3.4.3 AiCloud Sync



Pentru utilizarea caracteristicii AiCloud Sync:

1. Lansați AiCloud, faceți clic pe **AiCloud Sync** > **GO (SALT)**.
2. Selectați **ON (ACTIVAT)** pentru a activa caracteristica AiCloud Sync.
3. Faceți clic pe **Add new account (Adăugare cont nou)**.
4. Introduceți parola contului ASUS WebStorage și selectați directorul pe care doriți să îl sincronizați cu WebStorage.
5. Faceți clic pe **Apply (Aplicare)**.

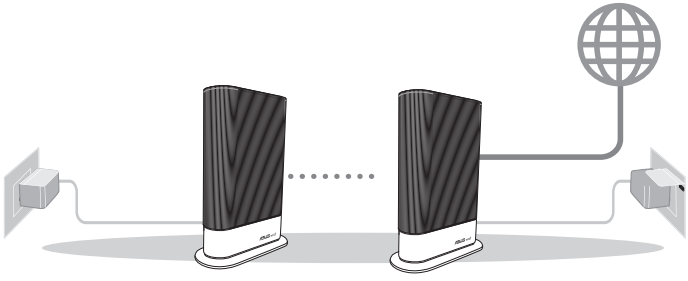
3.5 AiMesh

3.5.1 Înainte de setare

Pregătirea configurării sistemului WiFi AiMesh

1. Două (2) rutere ASUS (care acceptă AiMesh: https://www.asus.com/AiMesh/).
2. Atribuiți unul ca router AiMesh și altul ca nod AiMesh.

NOTĂ: Dacă aveți mai multe rutere AiMesh, vă recomandăm să îl utilizați pe cel cu cele mai bune specificații AiMesh și pe celelalte ca noduri AiMesh.



Nod AiMesh Router AiMesh

3.5.2 Pași de configurare AiMesh

Pregătirea

Amplasai AiMesh router-ul și nodul la 1-3 metri între ele în timpul procesului de configurare.

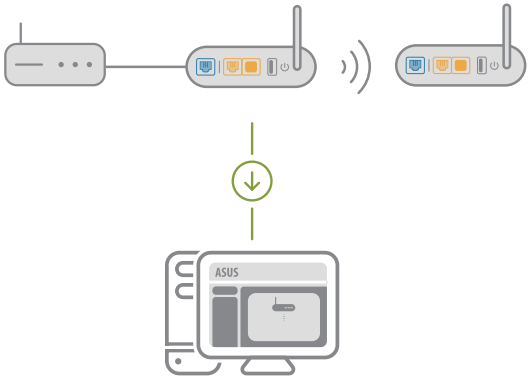
Nod AiMesh

Starea implicită din fabrică. Mențineți alimentarea pornită și în așteptare pentru setările sistemului AiMesh.

Nod AiMesh Router AiMesh

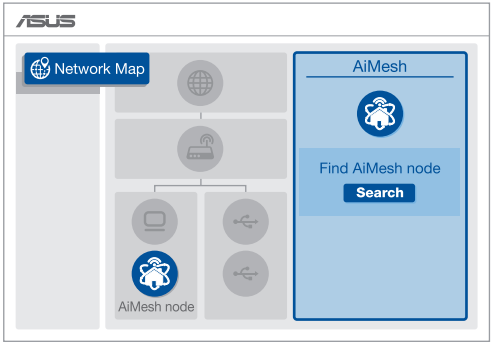
AiMesh router

1) Consultați **Quick Start Guide (Ghid de pornire rapidă)** al celuilalt ruter pentru a conecta ruterul AiMesh la PC și modem și apoi autentificați-vă în GUI web.



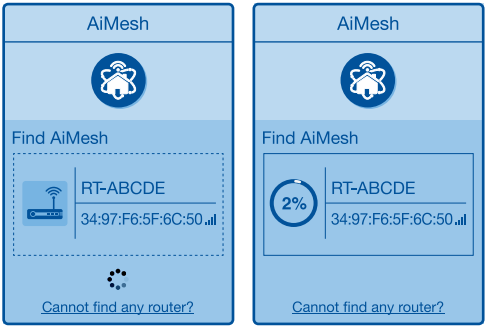
2) Accesați pagina Network Map (Hartă rețea), faceți clic pe pictograma AiMesh și apoi Search (Căutare) pentru nodul AiMesh folosit pentru extindere.

NOTĂ: Dacă nu găsiți pictograma AiMesh aici, faceți clic pe versiunea firmware și actualizați firmware-ul.

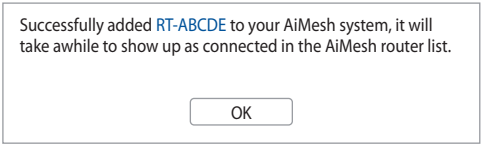


3) Faceți clic pe **Search (Căutare)**, va căuta automat nodul AiMesh în apropiere. Când nodul AiMesh este afișat pe această pagină, faceți clic pe acesta pentru a-l adăuga în sistemul AiMesh.

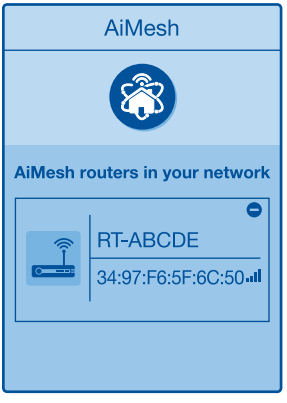
NOTE: Dacă nu puteși găsi niciun nod AiMesh, accesați **DEPANAREA**.



4) După finalizarea sincronizării este afișat un mesaj.



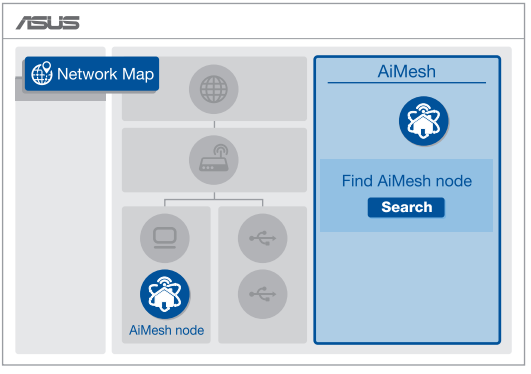
5) Felicitări! Veți descoperi că paginile de mai jos apar când un nod AiMesh a fost adăugat cu succes la rețeaua AiMesh.



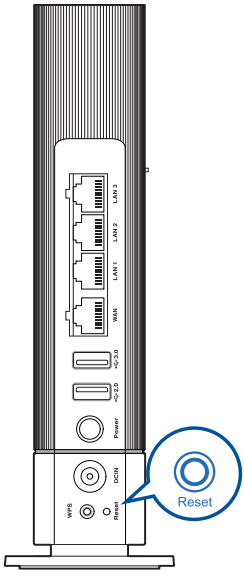
3.5.3 Depanarea

Dacă routerul AiMesh nu poate găsi niciun nod AiMesh în apropiere sau dacă sincronizarea nu reușește, verificați următoarele și încercați din nou.

1) În mod ideal, mutați nodul AiMesh mai aproape de routerul AiMesh. Asigurați-vă că distanța dintre dispozitive este de 1-3 metri.
2) Nodul AiMesh este pornit.
3) Router AiMesh folosește un firmware care include tehnologia AiMesh.
   i. Descărcați un firmware care include tehnologia AiMesh de la: https://www.asus.com/AiMesh/
   ii. Porniți nodul AiMesh și conectați-l la PC printr-un cablu de rețea.
   iii. Accesați interfața grafică web. Veți fi redirecționat către ASUS Setup Wizard (Expertul de configurare ASUS). Dacă acest lucru nu se întâmplă, navigați la adresa http://www.asusrouter.com
   iv. Accesați **Administration (Administrare)** > **Firmware Upgrade (Actualizare firmware)**. Faceți clic pe **Choose File (Selectare fișier)** și încărcați firmware-ul care include tehnologia AiMesh.
   v. După ce firmware-ul este încărcat, accesați pagina Network Map (Hartă rețea) pentru a verifica dacă pictograma Aimesh este afișată.



   vi. Apăsați pe butonul de resetare de pe nodul AiMesh timp de cel puțin 5 secunde. Eliberați butonul de resetare atunci când LED-ul de alimentare clipește lent.



3.5.4 Relocare

Performante optime:

Amplasați nodul și routerul AiMesh în cel mai bun loc posibil.

NOTE:

- Pentru a reduce la minimum interferențele, mențineți routerele la distanță față de dispozitive precum telefoane fără fir, dispozitive Bluetooth și cuptoare cu microunde.
- Vă recomandăm să amplasați routerele într-un spațiu deschis sau larg.

3.5.5 FAQs (Întrebări frecvente)

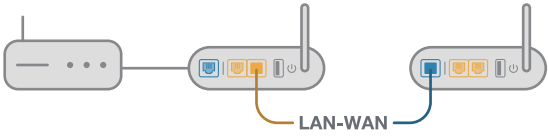
Q1: Acceptă routerul AiMesh modul Access Point (Punct de acces)?

A: Da. Puteți alege să setați routerul AiMesh fie în modul de router, fie în modul de punct de acces. Accesați interfața grafică web (http://www.asusrouter.com), și mergeți la pagina **Administration (Administrare)** > **Operation Mode (Mod funcționare)**.

Q2: Pot configura o conexiune cu fir între router-ele AiMesh (backhaul Ethernet)?

A: Da. Sistemul AiMesh acceptă conexiunea wireless și prin fir dintre router-ul AiMesh și nod pentru a maximiza rata de transfer stabilitatea. AiMesh analizează puterea semnalului wireless pentru fiecare bandă de frecvență disponibilă, apoi determină automat dacă o conexiune wireless sau prin fir este mai potrivită pentru a servi pe post de conexiune între routere.

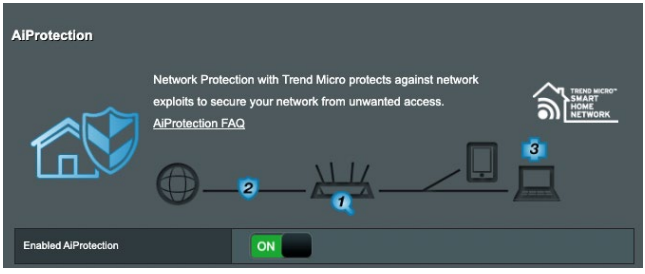
1) Urmați pașii de configurare pentru a stabili o conexiune între nodul și router-ul AiMesh prin Wi-Fi mai întâi.
2) Așezați nodul în locațiile ideale pentru cea mai bună acoperire. Conectați un cablu Ethernet la portul LAN al router-ului AiMesh și la portul LAN al nodului AiMesh.



3) Sistemul AiMesh va selecta automat cea mai bună cale pentru transmisia datelor, fie prin fir, fie wireless.

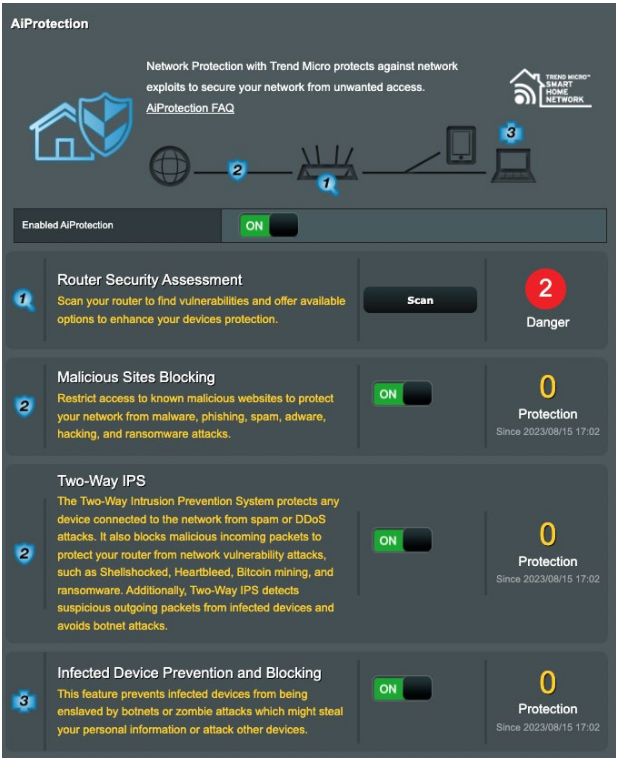
3.6 AiProtection

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



3.6.1 Configurarea AiProtection

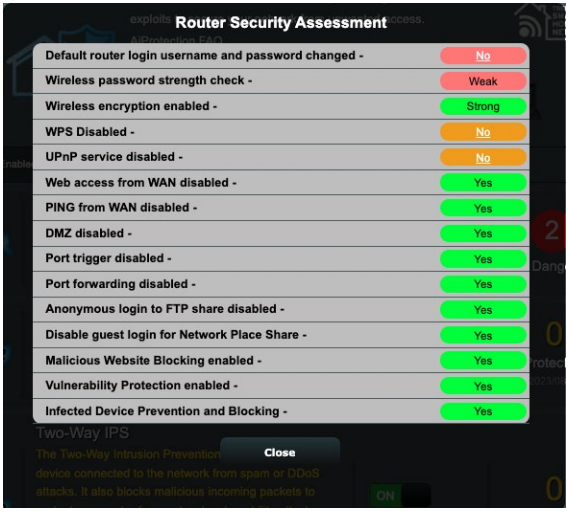
Funcția AiProtection previne abuzarea rețelei şi securizează rețeaua împotriva accesului nedorit.



Pentru a configura funcția AiProtection:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **AiProtection**.
2. Din pagina principală a funcției AiProtection, faceți clic pe **Network Protection (Protecție rețea)**.
3. Din Network Protection (Protecție rețea), faceți clic pe **Scan (Scanare)**.

Rezultatele căutării sunt afişate pe pagina **Router Security Assessment (Evaluare securitate router)**.



IMPORTANT! Elementele marcate cu **Yes (Da)** pe pagina **Router Security Assessment (Evaluare securitate router)** sunt considerate sigure.

4. (Opțional) De pe pagina **Router Security Assessment (Evaluare securitate router)**, configurați manual articolele marcate cu **No (Nu)**, **Weak (Slab)** sau **Very Weak (Foarte slab)**. Pentru aceasta:
   a. Faceți clic pe un articol pentru a accesa pagina de configurare a articolului respectiv.
   b. Din pagina cu setări de securitate a elementului respectiv, configurați şi efectuați modificările necesare şi faceți clic pe **Apply (Aplicare)**.
   c. Reveniți la pagina **Router Security Assessment (Evaluare securitate router)** şi faceți clic pe **Close (Închidere)** pentru a ieşi din pagină.
5. Faceți clic pe **OK** în mesajul de confirmare.

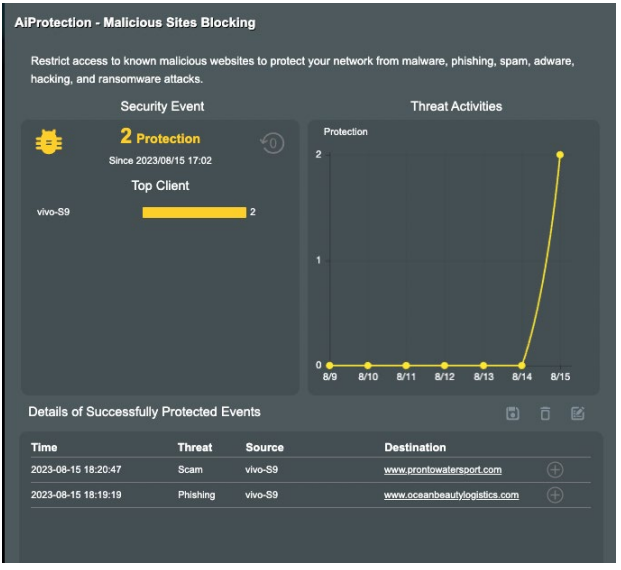
3.6.2 Blocare site-uri rău intenționate

Această caracteristică restricționează accesul la site-uri Web rău intenționate cunoscute în baza de date cloud, pentru o protecție actualizată în permanență.

NOTĂ: Această funcție este activată în mod automat dacă executați funcția Router Weakness Scan (Scanare vulnerabilități router).

Pentru a activa funcția Malicious Sites Blocking (Blocare site-uri rău intenționate):

1. Din panoul de navigare, mergeți la **General (Generalități)** > **AiProtection**.
2. Din pagina principală a AiProtection, faceți clic pe **Malicious Sites Blocking (Blocare Site-uri Rău Intenționate)**.



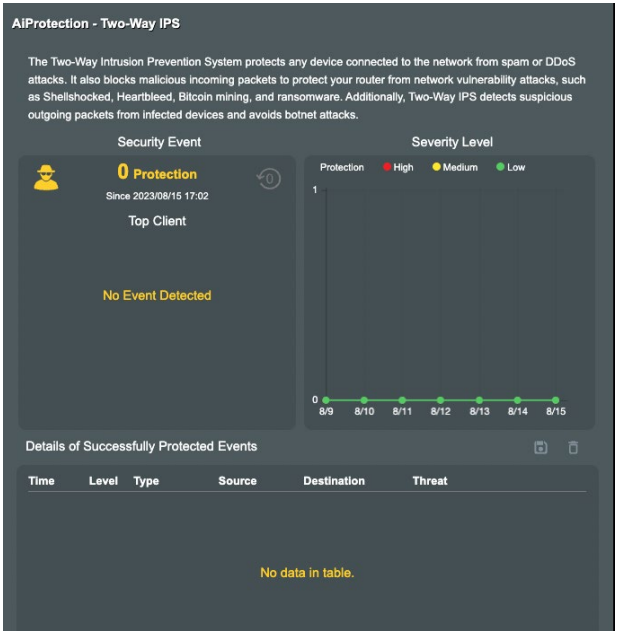
3.6.3 IPS bidirecțional

Această caracteristică rezolvă abuzuri comune în cadrul configurației ruterului.

> **NOTĂ:** Această funcție este activată în mod automat dacă executați funcția Router Weakness Scan (Scanare vulnerabilități router).

Pentru a activa funcția Two-Way IPS (IPS bidirecțional):

1. Din panoul de navigare, mergeți la **General (Generalități)** > **AiProtection**.
2. Din pagina principală a AiProtection, faceți clic pe **Two-Way IPS (IPS bidirecțional)**.



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

Această caracteristică împiedică dispozitivele infectate să comunice informații personale sau starea de infectare către părți externe.

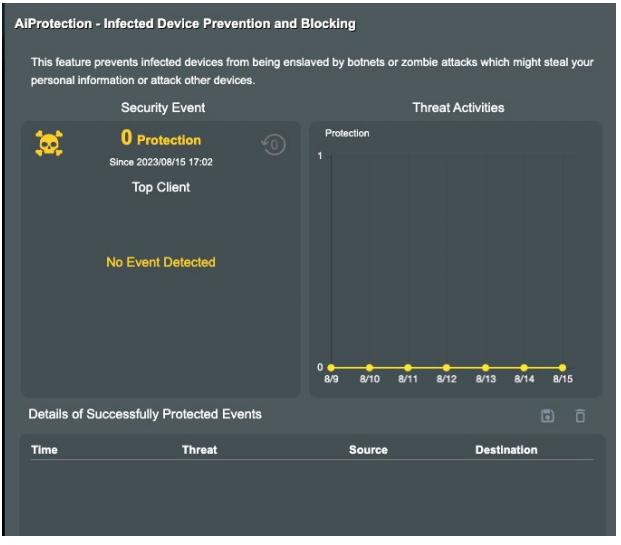
NOTĂ: Această funcție este activată în mod automat dacă executați funcția Router Weakness Scan (Scanare vulnerabilități router).

Pentru a activa funcția Vulnerability protection (Protecție împotriva vulnerabilităților):

1. Din panoul de navigare, mergeți la **General (Generalități)** > **AiProtection**.
2. Din pagina principală a AiProtection, faceți clic pe **Infected Device Prevention and Blocking (Prevenire şi blocare dispozitiv infectat)**.

Pentru a configura funcția Alert Preference (Preferință alerte):

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



3.7 Paravan de protecție

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

NOTĂ: Caracteristică de firewall este activată implicit.

3.7.1 General (Generalități)

Pentru a configura setările de bază pentru firewall:

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

3.7.2 URL Filter (Filtru URL)

Puteți să specificați cuvinte cheie sau adrese web pentru a preveni accesul la anumite locații URL.

NOTĂ: Filtrul URL se bazează pe o interogare a serverului DNS. Dacă un client din rețea 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, ştergeți memoria cache a serverului DNS înainte de a configura filtrul URL.

Pentru configurarea unui filtru URL:

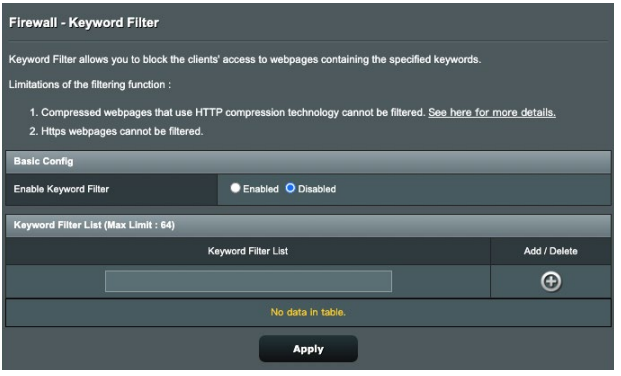
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Firewall** > **URL Filter (Filtru URL)**.
2. În câmpul **Enable URL Filter (Activare filtru URL)**, selectați

Enabled (Activat).

3. Introduceți o locație URL şi apoi faceți clic pe butonul ⊕.
4. Faceți clic pe **Apply (Aplicare)**.

3.7.3 Keyword filter (Filtru cuvinte cheie)

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



Pentru configurarea unui filtru de cuvinte cheie:

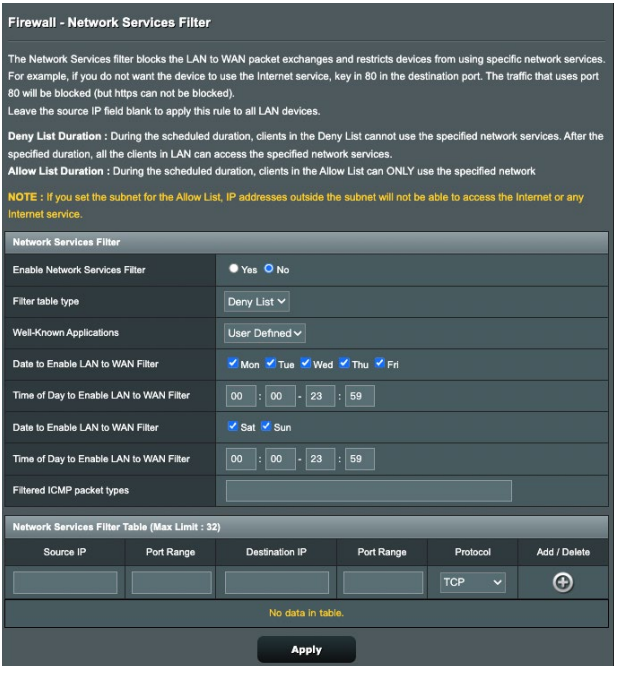
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Firewall** > **Keyword filter (Filtru cuvinte cheie)**.
2. În câmpul **Enable Keyword Filter (Activare filtru cuvinte cheie)**, selectați **Enabled (Activat)**.
3. Introduceți un cuvânt sau o expresie şi apoi faceți clic pe butonul ⊕.
4. Faceți clic pe **Apply (Aplicare)**.

NOTE:

- Filtrul de cuvinte cheie se bazează pe o interogare a serverului DNS. Dacă un client din rețea 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, ştergeți 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.

3.7.4 Network Services Filter (Filtru servicii rețea)

Filtrul pentru serviciile din rețea blochează pachetele schimbate între rețeaua LAN şi conexiunea WAN şi restricționează clienții din rețea să acceseze anumite servicii web, cum ar fi Telnet sau FTP.



Pentru configurarea unui filtru de servicii de rețea:

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

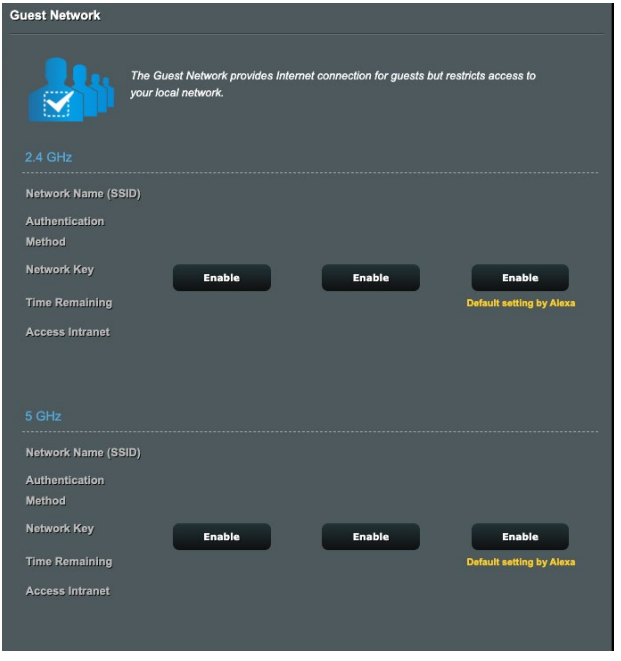
3.8 Rețelei de vizitatori

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

NOTĂ: Routerul RT-AX59U acceptă până la sase identificatoare SSID (trei la 2,4 GHz şi trei la 5 GHz).

Pentru a vă crea o rețea de vizitatori:

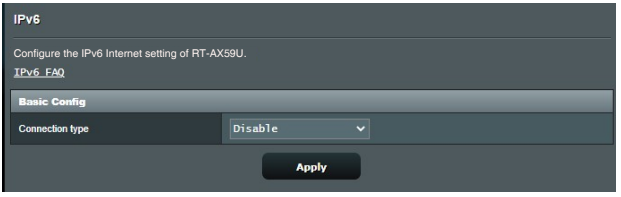
1. Din panoul de navigare, mergeți la **General (Generalități)** > **Guest Network (Rețea vizitatori)**.
2. În ecranul Guest Network (Rețea vizitatori), selectați banda de frecvență de 2,4 GHz sau de 5 GHz pentru rețeaua de vizitatori pe care doriți să o creați.
3. Faceți clic pe **Enable (Activare)**.



4. Pentru a modifica setările pentru un oaspete, faceți clic pe setările pe care doriți să le modificați. Faceți clic pe **Remove (Eliminare)** pentru a şterge setările pentru oaspete.
5. Atribuiţi un nume pentru rețeaua wireless temporară în câmpul Network Name (SSID) (Nume rețea (SSID)).
6. Selectați o opțiune pentru Authentication Method (Metodă de autentificare)
7. Dacă selectați o metodă de autentificare WPA, selectați o opțiune pentru WPA Encryption (Criptare WPA).
8. Specificați o valoare pentru Access time (Timp de acces) sau faceți clic pe **Limitless (Nelimitat)**.
9. Selectați **Disable (Dezactivare)** sau **Enable (Activare)** pe elementul Access Intranet (Acces la Intranet).
10. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

3.9 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. Contactați furnizorul de servicii internet dacă abonamentul dvs. include standardul IPv6.



Pentru a configura IPv6:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **IPv6**.
2. Selectați o opțiune pentru **Connection type (Tip conexiune)**. Opțiunile de configurare variază în funcție de tipul de conexiune selectat.
3. Introduceți setările pentru IPv6 şi DNS.
4. Faceți clic pe **Apply (Aplicare)**.

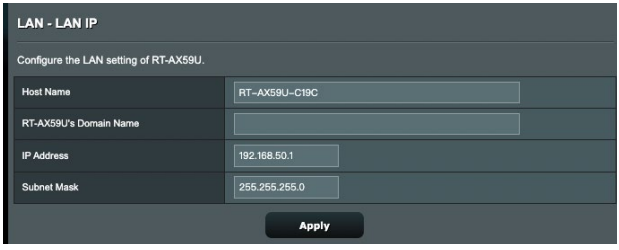
NOTĂ: Consultați furnizorul de servicii Internet cu pentru a primi informații specifice despre standardul IPv6 inclus în abonamentul dvs.

3.10 LAN

3.10.1 LAN IP

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

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

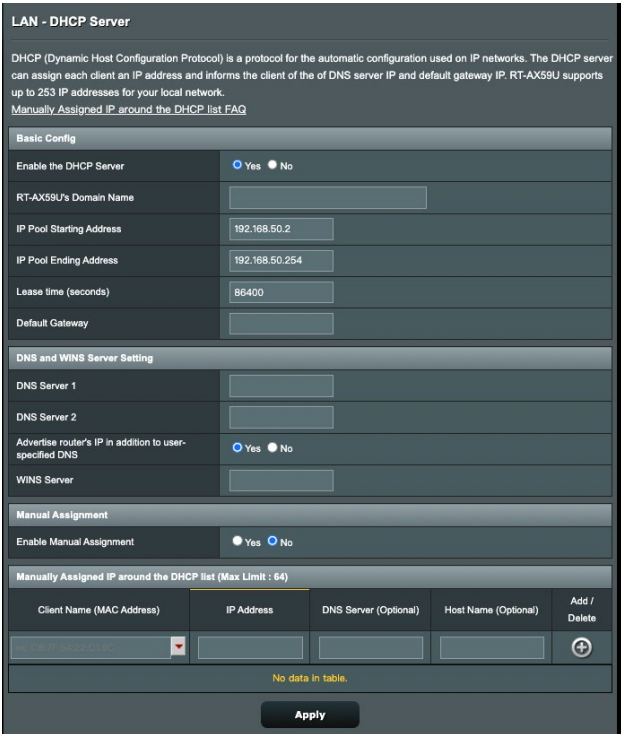


Pentru a modifica setările IP ale rețelei LAN:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **LAN** > **LAN IP**.
2. Modificați valorile pentru **IP address (Adresă IP)** şi **Subnet mask (Mască subrețea)**.
3. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

3.10.2 Serverului DHCP

Ruterul dvs. wireless foloseşte protocolul DHCP pentru a atribui automat adresele IP în rețeaua dvs. Puteți specifica intervalul de adrese IP şi durata de atribuire pentru clienții din rețeaua dvs.



Pentru configurarea serverului DHCP:

1. Din panoul de navigare, bifați **Advanced Settings (Setări avansate)** > **LAN** > **DHCP Server**.
2. În câmpul **Enable the DHCP Server (Activați serverul DHCP)** bifați **Yes (Da)**.
3. În caseta **RT-AX59U Domain Name (Nume domeniu)**, introduceți un nume de domeniu pentru ruterul wireless.
4. În câmpul **IP Pool Starting Address (Plajă adresă IP de pornire)**, tastați adresa IP de pornire.
5. În câmpul **IP Pool Ending Address (Plajă adresă IP de sfârşit)**, tastați adresa IP de sfârşit.

6. În câmpul **Lease Time (Perioadă de închiriere) (secunde)** tastați data la care expiră adresele IP şi ruterul wireless va aloca automat adrese IP noi pentru clienții rețelei.

NOTE:

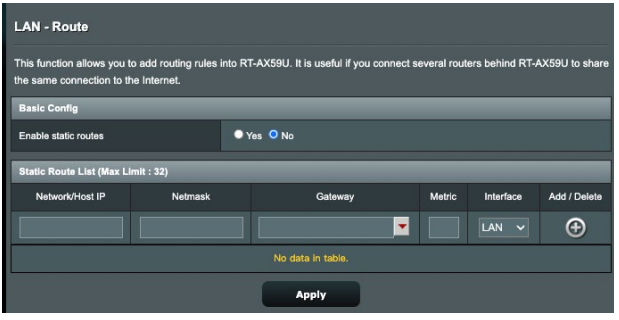
- Vă recomandăm să utilizați un format de adresă IP de tip 192.168.1.xxx (unde xxx poate fi orice număr între 2 şi 254) când specificați un interval de adrese IP.
- Adresa de pornire pentru plaja de adrese IP nu trebuie să fie mai mare decât adresa de sfârşit pentru plaja respectivă.

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

3.10.3 Rută

Dacă rețeaua dvs. utilizează mai multe rutere wireless, puteți configura un tabel de direcționare pentru a beneficia de același serviciu de Internet.

NOTĂ: Vă recomandăm să nu modificați setările implicite ale rutei, decât dacă aveți cunoștințe legate de tabelele de direcționare.

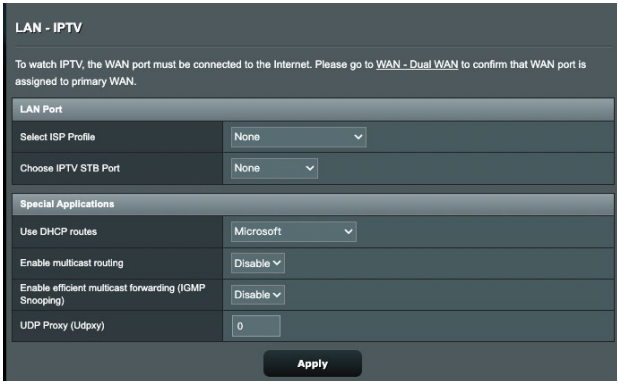


Pentru a configura tabelul de direcționare în rețeaua LAN:

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

3.10.4 IPTV

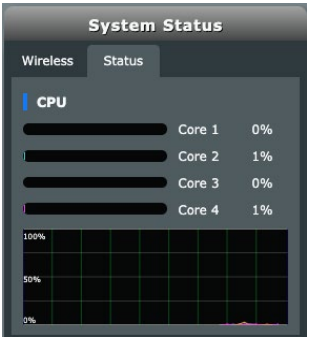
Ruterul wireless acceptă conectarea la servicii IPTV prin intermediul unui ISP sau al unei rețele LAN. IPTV oferă setările necesare pentru configurarea serviciilor IPTV, VoIP, de distribuire multiplă şi UDP. Contactați furnizorul de servicii Internet pentru a obține informații specifice cu privire la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

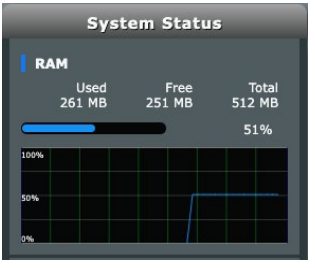


3.11 Hărții rețelei

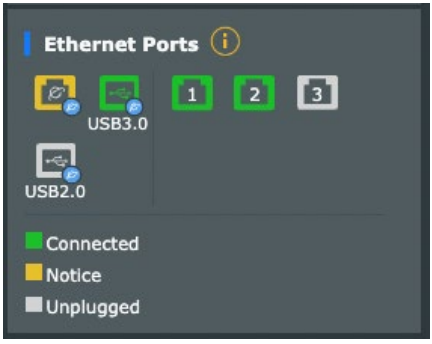
Harta rețelei vă permite să configurați setările de securitate ale rețelei dvs., să gestionați clienții din rețea și să monitorizați dispozitivul USB.

Puteți monitoriza starea CPU a fiecărui nucleu, starea de utilizare a memoriei RAM și starea porturilor Ethernet. Următorul este un exemplu de stare de utilizare a CPU, RAM și a porturilor Ethernet.





Stare port: Vă permite să verificați porturile Ethernet și porturile USB.



3.11.1 Configurarea setărilor de securitate pentru rețeaua wireless

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

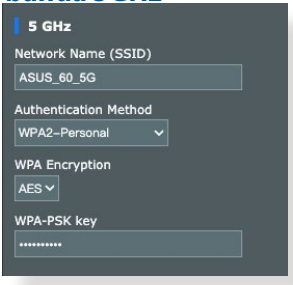
Pentru a configura setările de securitate pentru rețeaua wireless:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Network Map (Hartă rețea)**.
2. Din ecranul Network Map (Hartă rețea) selectați pictograma **System Status (Stare Sistem)** pentru afișarea setărilor de securitate wireless, cum sunt de exemplu SSID, nivel de securitate şi setările de criptare.

NOTĂ: Puteți configura setări diferite de securitate wireless pentru benzile 2,4 GHz şi 5 GHz.

Setări de securitate pentru banda 2,4GHz

Setări de securitate pentru banda 5GHz



3. În câmpul **Network Name (SSID) (Nume rețea (SSID))** tastați un nume unic pentru rețeaua dvs. wireless.
4. Din lista verticală **Authentication Method (Metodă de autentificare)**, selectați metoda de autentificare pentru rețeaua dvs. wireless.

   Dacă selectați opțiunea WPA-Personal sau WPA-2 Personal drept metodă de autentificare, introduceți cheia WPA-PSK sau cheia de securitate.

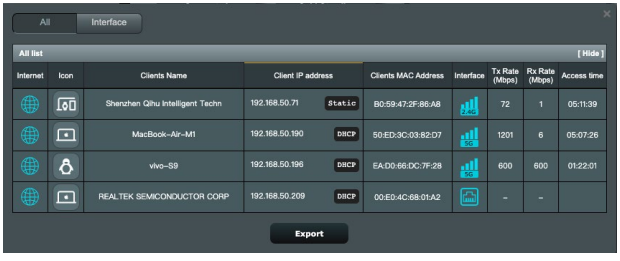
IMPORTANT! Standardul IEEE 802.11n/ac interzice utilizarea unei rate mari de transfer cu WEP sau WPA-TKP ca şi cifru unicast. În cazul în care utilizați aceste metode de criptare, rata de date va scădea la o conexiune IEEE 802.11g de 54 Mbps.

5. Faceți clic pe **Apply (Aplicare)** după ce ați terminat.

3.11.2 Administrarea clienților din rețea

Pentru a administra clienții din rețea:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Network Map (Hartă rețea)**.
2. Din ecranul **Network Map (Hartă rețea)**, selectați pictograma **Clients (Clienți)** pentru afișarea informațiilor referitoare la clienții de rețea.
3. Faceți clic pe **View List (Vizualizare listă)** de sub pictograma **Clients (Clienți)** pentru a afișa toți clienții.
4. Pentru a bloca accesul unui client la rețea, selectați clientul și faceți clic pe pictograma cu lacătul deschis.



3.11.3 Monitorizarea dispozitivului USB

Ruterul wireless ASUS este prevăzut cu două porturi USB pentru conectarea dispozitivelor USB sau a unei imprimante USB, pentru a vă permite să partajați fișiere și imprimante cu clienții din rețea.

NOTE:

- Pentru a utiliza această caracteristică, este necesar să conectați un dispozitiv de stocare USB, cum ar fi un hard disk USB sau o unitate flash USB, la portul USB3.0/2.0 de pe panoul din spate al router-ului fără fir. Asigurați-vă că dispozitivul de stocare USB este formatat și partiționat corespunzător. Consultați Lista de compatibilitate a discurilor Plug-n-Share la adresa **http://event.asus.com/networks/disksupport**
- Porturile USB acceptă conectarea simultană a două unități USB sau a unei imprimante și unei unități USB.

IMPORTANT! Mai întâi trebuie să creați un cont de partajare și să-i configurați permisiunile/drepturile de acces în vederea permiterii altor clienți din rețea să acceseze dispozitivul USB prin intermediul unui site FTP/unui utilitar client FTP terț, prin intermediul caracteristicii Servers Center (Centru servicii) sau prin intermediul serviciului Samba sau AiCloud. Pentru mai multe detalii, consultați secțiunile **3.16 USB Application (Aplicației USB)** și **3.4 AiCloud 2.0** din acest manual de utilizare.

Pentru a monitoriza dispozitivul USB:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Network Map (Hartă rețea)**.
2. Din ecranul Network Map (Hartă rețea), selectați pictograma **USB Disk Status (Stare disc USB)** pentru afișarea informațiilor referitoare la dispozitivul USB.
3. Din câmpul AiDisk Wizard (Expert AiDisk), faceți clic pe **GO (SALT)** pentru a configura un server FTP pentru partajarea fișierelor de pe Internet.

NOTE:

- Pentru mai multe detalii, consultați secțiunea **3.16.2 Using Servers Center (Utilizarea centrului de servere)** din acest manual de utilizare.
- Ruterul fără fir funcționează cu majoritatea unităților de hard disk/discurilor flash USB (dimensiune de până la 2 TO) și acceptă acces de citire-scriere pentru FAT16, FAT32, NTFS și HFS+.

Eliminarea în siguranță a discului USB

IMPORTANT! Eliminarea incorectă a unității USB poate să cauzeze coruperea datelor.

Pentru a elimina în siguranță discul USB:

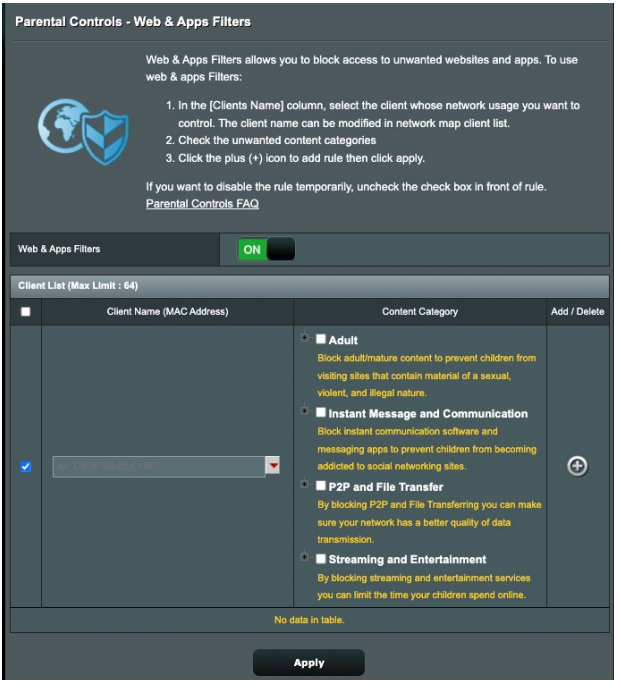
1. Din panoul de navigare, mergeți la **General (Generalități)** > **Network Map (Hartă rețea)**.
2. În colțul din dreapta sus, faceți clic pe > **Eject USB disk (Scoatere disc USB)**. Când discul USB este scos cu succes, starea pentru USB indică **Unmounted (Demontat)**.

3.12 Controale parentale

Opțiunea de Controale parentale vă permite să controlați intervalul orar de acces la internet sau să setați limita de timp pentru utilizarea rețelei de către un client.

Pentru a activa funcția Parental Controls (Controale parentale):

Din panoul de navigare, mergeți la **General (Generalități)** > **Parental Controls (Controale parentale)**.



Web & Apps Filters (Filtre aplicații şi Web)

Web & Apps Filters (Filtre aplicații şi Web) este o caracteristică a funcției Parental Controls (Controale parentale) care vă permite să blocați accesul la site-uri web şi aplicații nedorite.

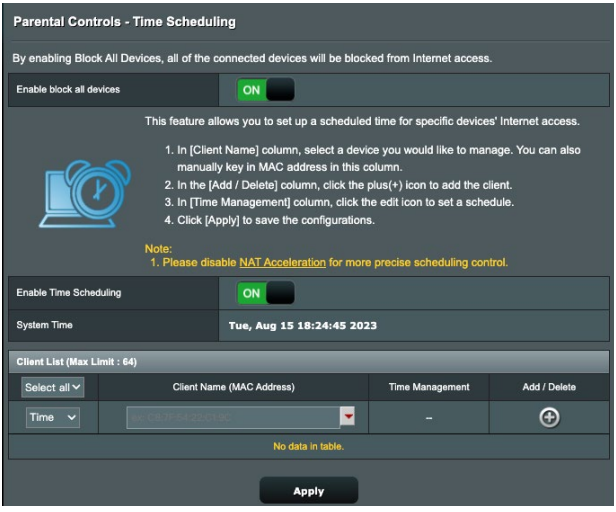
Pentru a configura caracteristica Web & Apps Filters (Filtre aplicații şi Web):

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Parental Controls (Controale parentale)** > **Web & Apps Filters (Filtre aplicații şi Web)**.
2. Din panoul **Web & Apps Filters (Filtre aplicații şi web)**, faceți clic pe **ON (ACTIVAT)**.
3. Atunci când apare mesajul cu acordul de licențiere a utilizatorilor finali, faceți clic pe **I agree (Sunt de acord)** pentru a continua.
4. Din coloana **Client List (Listă clienți)**, selectați sau introduceți manual numele clientului din lista verticală.
5. Din coloana **Content Category (Categorie conținut)**, selectați filtrele din cele patru categorii principale: **Adult, Instant Message and Communication (Mesagerie instantanee şi comunicare)**, **P2P and File Transfer (P2P şi transfer de fişiere)** şi **Streaming and Entertainment (Redare în flux şi divertisment)**.
6. Faceți clic pe ⊕ pentru a adăuga profilul clientului.
7. Faceți clic pe **Apply (Se aplică)** pentru a salva setările.

Time Scheduling (Programare în timp)

Opțiunea Time Scheduling (Programare în timp) vă permite să setați limita de timp pentru utilizarea rețelei de către clienți.

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



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

1. Din panoul de navigare, mergeți la **General (Generalități)** > **Parental Controls (Controale parentale)** > **Time Scheduling (Programare în timp)**.
2. Din panoul **Enable Time Scheduling (Activare programare în timp)**, faceți clic pe **ON (ACTIVAT)**.
3. Din coloana **Client Name (Nume client)**, selectați sau introduceți manual numele clientului din lista verticală.

NOTĂ: De asemenea, puteți să introduceți adresa MAC a clientului în coloana Client MAC Address (Adresă MAC client). Asigurați-vă că numele clientului nu conține caractere speciale sau spații, deoarece acest lucru poate face ca ruterul să funcționeze anormal.

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

3.13 Smart Connect (Conectare inteligentă)

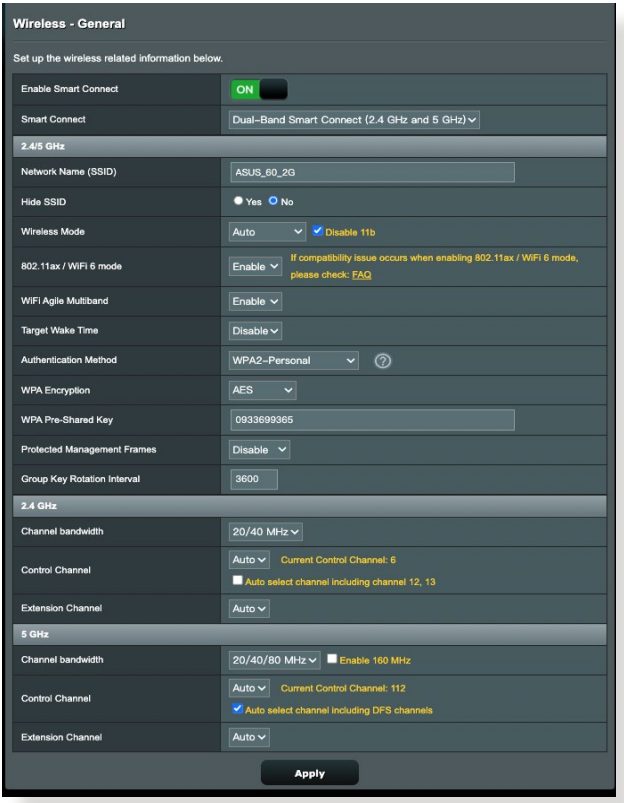
Funcția Smart Connect (Conectare inteligentă) este concepută să ghideze în mod automat clienții către una dintre cele trei frecvențe radio (una de 2,4 GHz şi una în bandă înaltă de 5 GHz) pentru a maximiza utilizarea totală a randamentului rețelei wireless.

3.13.1 Configurarea funcției Smart Connect (Conectare inteligentă)

Puteți activa funcția Smart Connect (Conectare inteligentă) din interfața grafică web în următoarele două moduri:

- ***prin afişajul wireless***

1. În browserul web, tastați manual adresa IP implicită a routerului wireless: http://www.asusrouter.com.
2. Pe pagina de conectare, tastați numele de utilizator (**admin**) şi parola (**admin**) implicite, apoi faceți clic pe **OK**. Pagina QIS se lansează automat.
3. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Wireless** > **General (Generalități)**.
4. Deplasați glisorul la **ON (ACTIVAT)** în câmpul **Enable Smart Connect (Activare conectare inteligentă)**. Această funcție va conecta în mod automat clienții din rețeaua dvs. la banda corespunzătoare pentru ca aceştia să beneficieze de cea mai bună viteză.


Wireless - General
Set up the wireless related information below.
Enable Smart Connect
ON
Smart Connect
Dual-Band Smart Connect (2.4 GHz and 5 GHz)
2.4/5 GHz
Network Name (SSID)
ASUS_60_2G
Hide SSID
Yes
No
Wireless Mode
Auto
Disable 11b
802.11ax / WiFi 6 mode
Enable
If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ
WiFi Agile Multiband
Enable
Target Wake Time
Disable
Authentication Method
WPA2-Personal
WPA Encryption
AES
WPA Pre-Shared Key
0933699365
Protected Management Frames
Disable
Group Key Rotation Interval
3600
2.4 GHz
Channel bandwidth
20/40 MHz
Control Channel
Auto
Current Control Channel: 6
Auto select channel including channel 12, 13
Extension Channel
Auto
5 GHz
Channel bandwidth
20/40/80 MHz
Enable 160 MHz
Control Channel
Auto
Current Control Channel: 112
Auto select channel including DFS channels
Extension Channel
Auto
Apply

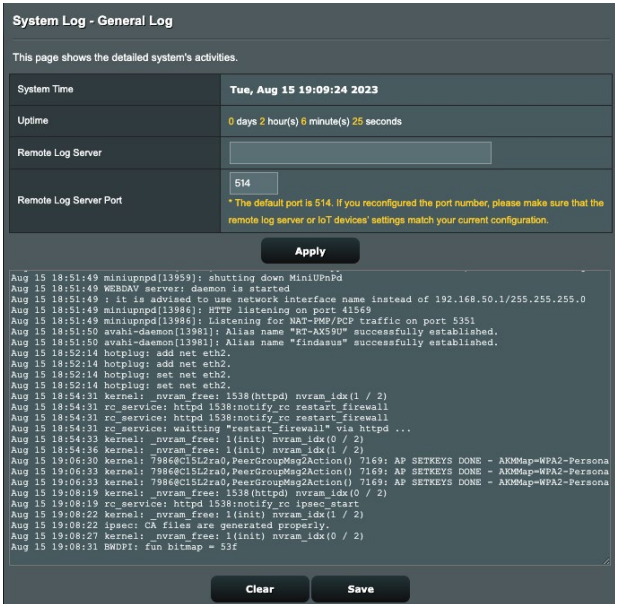
3.14 System Log (Jurnal de sistem)

Jurnalul de sistem conține activitățile de rețea care au fost înregistrate.

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

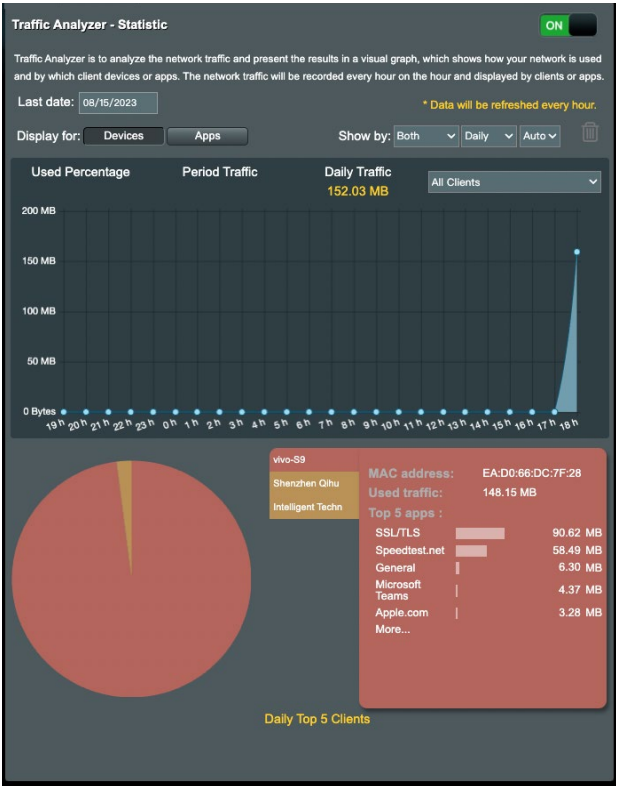
Pentru vizualizarea jurnalului de sistem:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **System Log (Jurnal de sistem)**.
2. Puteți vizualiza activitățile din rețea în oricare din aceste file:
   - Jurnal General (Generalități)
   - Jurnal wireless
   - Atribuiri DHCP
   - IPv6
   - Tabel direcționare
   - Redirecționare porturi
   - Conexiune



3.15 Analizor de trafic

Funcția Traffic Analyzer (Analizor de trafic) vă oferă informații succinte cu privire la evenimentele din rețeaua dvs., zilnic, săptămânal sau lunar. Acest instrument vă permite să vedeți imediat utilizarea lățimii de bandă de către fiecare utilizator, precum și dispozitivele sau aplicațiile utilizate. Astfel, puteți să reduceți punctele critice de supra-utilizare a conexiunii la internet. Este, de asemenea, o modalitate excelentă de a monitoriza modul de utilizare a internetului sau activitățile utilizatorilor.



Pentru a configura analizorul de trafic:

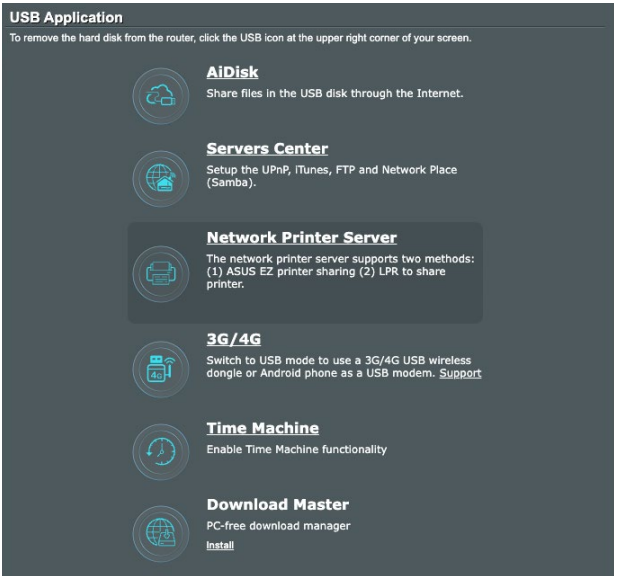
1. Din panoul de navigare, Accesați **General (Generalități)** > **Traffic Analyzer (Analizor de trafic)**.
2. De pe pagina principală **Traffic Analyzer (Analizor de trafic)**, activați statisticile analizorului de trafic.

3. Selectați data pentru care doriți să afișați graficul.
4. În câmpul **Display for (Afişare pentru)**, selectați Router sau Apps (Aplicații) pentru a afișa informațiile despre trafic.
5. În câmpul Show by (Afişare după), selectați modul în care doriți să afișați informațiile despre trafic.

3.16 Aplicației USB

Funcția USB Extension (Extensie USB) oferă submeniurile AiDisk, Servers Center (Centru servere), Network Printer Server (Server de imprimantă în rețea) şi Download Master (Coordonator de descărcări).

IMPORTANT! Pentru a utiliza funcțiile serverului, este necesar să introduceți un dispozitiv de stocare USB, cum ar fi un hard disk USB sau o unitate flash USB, în portul USB 3.0 de pe panoul din spate al ruterului wireless. Asigurați-vă că dispozitivul de stocare USB este formatat şi partiționat corespunzător. Consultați site-ul web ASUS la adresa http://event.asus.com/2009/networks/disksupport/, pentru a vedea tabelul de asistență cu privire la sistemul de fişiere.



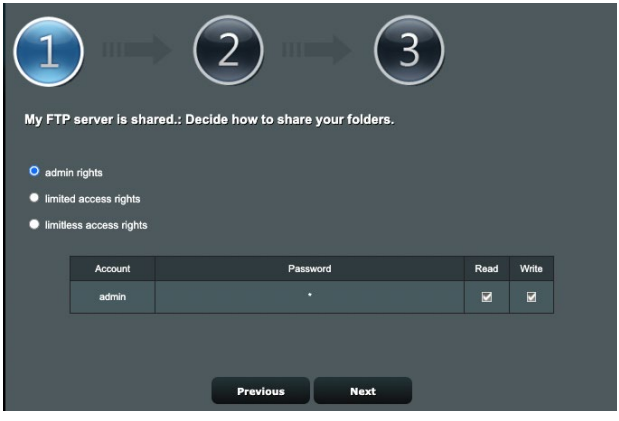
3.16.1 Utilizarea AiDisk

Funcția AiDisk vă permite să partajați fișiere de pe discul USB prin Internet. AiDisk vă va oferi asistență pentru configurarea parametrilor DDNS ASUS DDNS şi ai serverului FTP.

Pentru a utiliza AiDisk:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **USB Application (Aplicație USB)**, apoi faceți clic pe pictograma **AiDisk**.
2. Din ecranul Welcome to AiDisk wizard (Bun venit la asistentul AiDisk), faceți clic pe **Go (Salt)**.

3. Selectați drepturile de acces pe care doriți să le atribuiți clienților care accesează datele partajate.



4. Creați numele de domeniu prin serviciile DDNS ASUS, selectați **I will use the service and accept the Terms of service (Voi utiliza acest serviciu și sunt de acord cu condițiile serviciului)** și tastați numele domeniului. Când ați terminat, faceți clic pe **Next (Următorul)**.

   Puteți selecta **Skip ASUS DDNS settings (Omitere setări DDNS ASUS)** și apoi face clic pe **Next (Următorul)** pentru a omite realizarea setărilor DDNS.

5. Faceți clic pe **Finish (Terminare)** pentru a încheia configurarea.
6. Pentru a accesa site-ul FTP pe care l-ați creat, lansați un browser de Web sau un utilitar terț de client FTP și tastați linkul ftp (**ftp://<domain name>.asuscomm.com**) pe care l-ați creat.

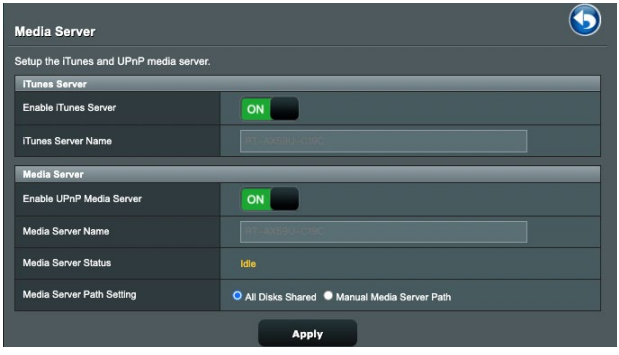
3.16.2 Utilizarea centrului de servere

Centrul de servere vă permite să partajați fișierele media de pe discul USB prin intermediul unui director de server media, prin intermediul serviciului de partajare Samba sau prin intermediul unui serviciu de partajare prin FTP. De asemenea, în centrul de servere puteți configura și alte setări pentru discul USB.

Utilizarea serverului media

Ruterul dvs. wireless permite dispozitivelor compatibile UPnP să acceseze fișierele multimedia aflate pe un disc USB conectat a ruterul wireless.

NOTĂ: Înainte de a utiliza funcția de server media UPnP, conectați dispozitivul la rețeaua router.

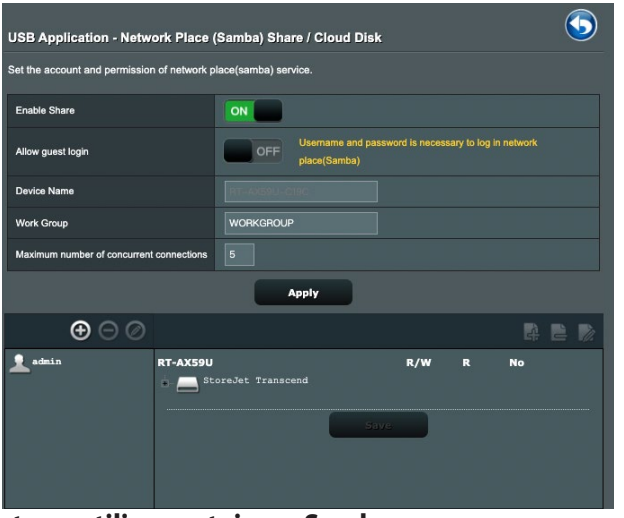


Pentru a lansa pagina de configurare a serverului media, mergeți la **General (Generalități)** > **USB Application** > **Media Server (Server media)**. Consultați informațiile de mai jos pentru a obține descrieri ale câmpurilor:

- **Activați serverul iTunes**: Selectați ON/OFF (ACTIVAT/DEZACTIVAT) pentru a activa sau dezactiva serverul iTunes.
- **Activare server media UPnP**: Selectați ON/OFF (ACTIVAT/DEZACTIVAT) pentru a activa sau dezactiva serverul media UPnP.
- **Stare server media**: Afișează starea serverului media.
- **Configurarea căii pentru serverul media:** Select **All Disks Shared (Toate discurile partajate)** sau **Manual Media Server Path (Cale manuală server media)**.

Utilizarea serviciului Network Place (Samba) Share (Partajare locație rețea (Samba))

Serviciul Network Place (Samba) Share (Partajare locație rețea (Samba)) vă permite să setați contul şi permisiunea pentru serviciul Samba.



Pentru a utiliza partajarea Samba:

1. Din panoul de navigare, mergeți la **General (Generalități)** > **USB application** > **Network Place (Samba) Share/Cloud Disk (Partajare locație rețea (Samba)/Disc cloud)**.

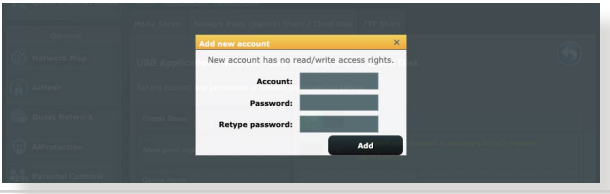
   NOTĂ: Locația de rețea (Samba) Share (Partajare (Samba)) este activată în mod implicit.

2. Urmați paşii de mai jos pentru a adăuga, şterge sau modifica un cont.

Pentru a crea un nou cont:

a) Faceți clic pe ⊕ pentru a adăuga un cont nou.

b) În câmpurile **Account (Cont)** şi **Password (Parolă)**, introduceți numele şi parola pentru clientul de rețea. Reintroduceți parola pentru confirmare. Faceți clic pe **Add (Adăugare)** pentru adăugarea contului în listă.



Pentru a şterge un cont existent:

a) Selectați contul pe care doriți să-l ştergeți.

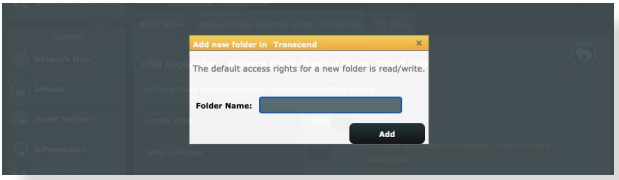
b) Faceți clic pe .

c) Când vi se solicită, faceți clic pe **Delete (Ştergere)** pentru a confirma ştergerea contului.

Pentru a adăuga un folder:

a) Faceți clic pe .

b) Introduceți numele folderului şi faceți clic pe **Add (Adăugare)**. Folderul pe care l-ați creat va fi adăugat în lista de foldere.



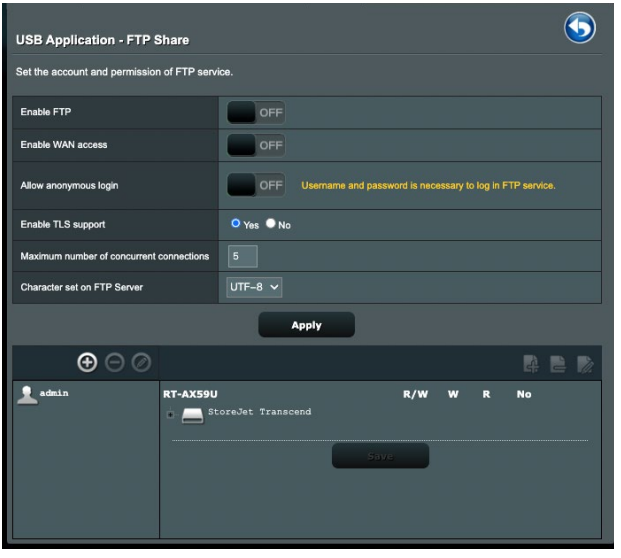
3. Selectați drepturile de acces pe care doriți să le atribuiți pentru fiecare director în parte, astfel:
   - **R/W (C/S):** Selectați această opțiune pentru a atribui accesul de citire/scriere.
   - **R:** Selectați această opțiune pentru a atribui acces numai pentru citire.
   - **No (Nu):** Selectați această opțiune dacă nu doriți să partajați un anumit folder de fişiere.
4. Faceți clic pe **Apply (Aplicare)** pentru a aplica modificările.

Utilizarea serviciului FTP Share (Partajare FTP)

Caracteristica de partajare prin FTP permite unui server FTP să partajeze fişiere de pe un disc USB cu alte dispozitive, prin intermediul reţelei locale sau al Internetului.

IMPORTANT!

- Asiguraţi-vă că eliminaţi în siguranţă discul USB. Eliminarea incorectă a discului USB poate să cauzeze coruperea datelor.
- Pentru a scoate în siguranţă discul USB, consultaţi secţiunea **Safely removing the USB disk (Eliminarea în siguranţă a discului USB)** sub **3.11.3 Monitoring your USB device (Monitorizarea dispozitivului USB)**.



Pentru a utiliza serviciul de partajare prin FTP:

NOTĂ: Verificați dacă ați configurat serverul FTP prin AiDisk. Pentru mai multe detalii, consultați secțiunea **3.16.1 Using AiDisk (Utilizarea AiDisk)**.

1. Din panoul de navigare, faceți clic pe **General (Generalități)** > **USB Application (Aplicație USB)** > **FTP Share (Partajare FTP)**.
2. Selectați drepturile de acces pe care doriți să le atribuiți pentru fiecare director în parte, astfel:
   - **R/W:** Selectați această opțiune pentru a atribui drepturi de citire/scriere pentru un anumit director.
   - **W:** Selectați această opțiune pentru a atribui drepturi de scriere pentru un anumit director**.**
   - **R:** Selectați această opțiune pentru a atribui doar drepturi de citire pentru directorul specificat.
   - **Niciun drept de acces:** Selectați această opțiune dacă nu doriți să partajați un anumit director.
3. Dacă preferați, puteți seta câmpul **Allow anonymous login (Permitere conectare anonimă)** la **ON (ACTIVAT)**.
4. În câmpul **Maximum number of concurrent connections (Număr maxim de conexiuni concomitente)**, introduceți manual numărul de dispozitive care pot fi conectate simultan la serverul de partajare FTP.
5. Faceți clic pe **Apply (Aplicare)** pentru a aplica modificările.
6. Pentru a accesa serverul FTP, tastați linkul ftp **ftp://<numegazdă>.asuscomm.com** şi numele de utilizator şi parola într-un browser de Web sau într-un utilitar terț FTP.

3.16.3 3G/4G

Modemurile 3G/4G prin USB pot fi conectate la router pentru a permite accesul la Internet.

NOTĂ: Pentru a vedea o listă cu modemuri USB verificate, accesați: http://event.asus.com/2009/networks/3gsupport/

Pentru a configura accesul la Internet prin 3G/4G:

1. Din panoul de navigare, faceți clic pe **General (Generalități)** > **USB application (Aplicație USB)** > **3G/4G**.
2. În câmpul **Enable USB Modem (Activare modem USB)**, selectați **Yes (Da)**.
3. Configurați următoarele:
   - **Locație:** Selectați locația furnizorului de servicii 3G/4G din lista verticală.
   - **ISP**: Selectați furnizorul de servicii Internet (ISP) din lista verticală.
   - **Serviciu APN (opțional)**: Pentru detalii, contactați furnizorul de servicii 3G/4G.
   - **Număr apelare şi cod PIN**: Numărul de acces şi codul PIN pentru conectare la furnizorul de servicii 3G/4G

   NOTĂ: Este posibil ca pentru diferiți furnizori codul PIN să difere.

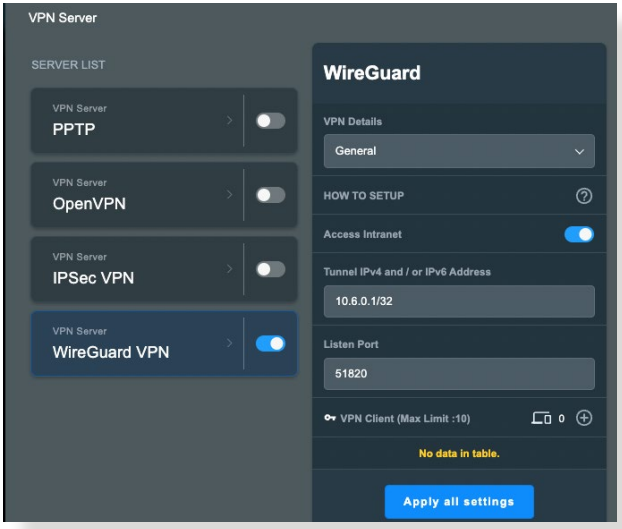
   - **Nume utilizator/Parolă:** Numele de utilizator şi parola vor fi furnizate de către operatorul rețelei 3G/4G.
   - **Adaptor USB**: Alegeți adaptorul USB pentru rețeaua 3G/4G din lista verticală. Dacă nu sunteți sigur cu privire la modelul adaptorului USB sau dacă modelul acestuia nu este listat printre opțiuni, selectați **Auto (Automat)**.
4. Faceți clic pe **Apply (Aplicare)**.

NOTĂ: Ruterul va reporni pentru ca setările să fie aplicate.

3.17 VPN

VPN (Virtual Private Network - rețea privată virtuală) oferă o comunicație securizată cu un computer sau cu o rețea aflată la distanță, prin intermediul unei rețele publice, cum este Internetul.

NOTĂ: Înainte de a configura o conexiune VPN, veți avea nevoie de adresa IP sau de numele de domeniu al serverului VPN pe care încercați să îl accesați.



3.17.1 Server VPN

Pentru configurarea accesului la un server VPN:

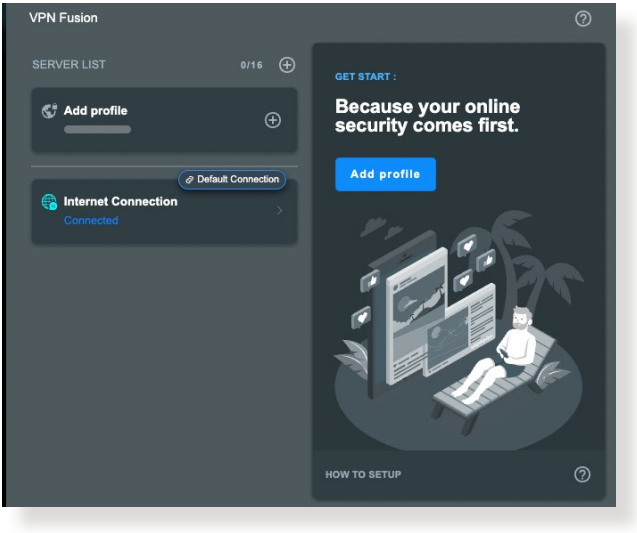
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **VPN**.
2. În câmpul **PPTP**, faceți clic pe **ON (ACTIVAT)**.
3. în lista verticală **VPN Details (Detalii VPN)**, selectați **Advanced Settings (Setări avansate)** dacă doriți să configurați setări avansate pentru VPN, precum suportul pentru transmisiune, setările de autentificare, setările de criptare MPPE şi intervalul de adrese pentru clienții IP.
4. în câmpul **Network Place (Samba) Support (Suport locație rețea (Samba))**, selectați **ON (ACTIVAT)**.
5. Introduceți numele de utilizator şi parola pentru accesarea serverului VPN. Faceți clic pe butonul ⊕.
6. Faceți clic pe **Apply all settings (Aplicare toate setările)**.

3.17.2 VPN Fusion (Fuziune VPN-uri)

VPN Fusion (Fuziune VPN-uri vă permite să vă conectați simultan la servere VPN multiple și să vă conectați dispozitivele client la tuneluri VPN diferite. Unele dispozitive, cum ar fi set-top boxuri, televizoare inteligente și playere Blu-ray, nu acceptă software-urile VPN. Această funcție asigură acces prin VPN pentru aceste dispozitive într-o rețea de domiciliu, fără a trebui să instalați software VPN, în timp ce smartphone-ul dvs. rămâne conectat la internet, nu la VPN. În modul Gamer (Jocuri), conexiunea VPN combate atacurile de tip DDoS, astfel încât PC-ul sau fluxul dvs. să nu se deconecteze de la serverele jocului. Realizarea unei conexiuni VPN vă poate ajuta și să vă schimbați cu ușurință adresa IP la regiunea în care sunt amplasate serverele jocului care vă interesează, îmbunătățind durata de ping către serverele de joc.

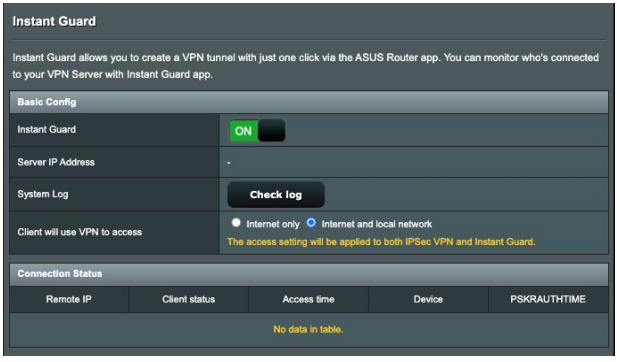
Pentru a începe, urmați pașii de mai jos:

1. Faceți clic pe ⊕ de sub **SERVER LIST (LISTĂ DE SERVERE)** sau **Add profile (Adăugare profil)** pentru a adăuga un tunel VPN nou.
2. Activați conexiunea VPN pe care ați creat-o în Server List (Listă de servere).



3.17.3 Instant Guard

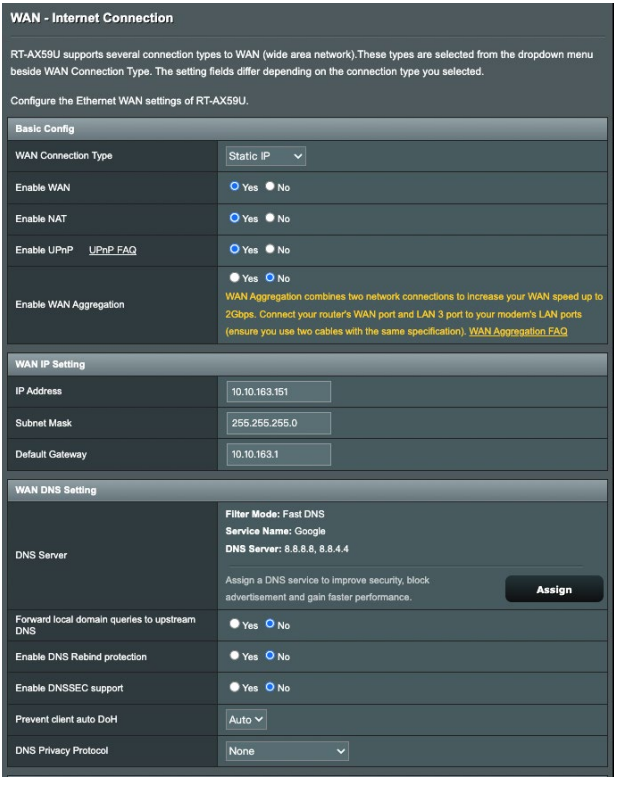
Instant Guard rulează propriul dvs. server VPN privat, pe propriul dvs. ruter. Când utilizați un tunel VPN, toate datele dvs. trec prin server. Cu Instant Guard, dețineți controlul total asupra propriului server, făcându-l cea mai sigură soluție posibilă.



3.18 WAN

3.18.1 Conexiune la Internet

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



Pentru configurarea setărilor conexiunii WAN:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **Internet Connection (Conexiune Internet)**.
2. Configurați următoarele setări: Când ați terminat, faceți clic pe **Apply (Aplicare)**.

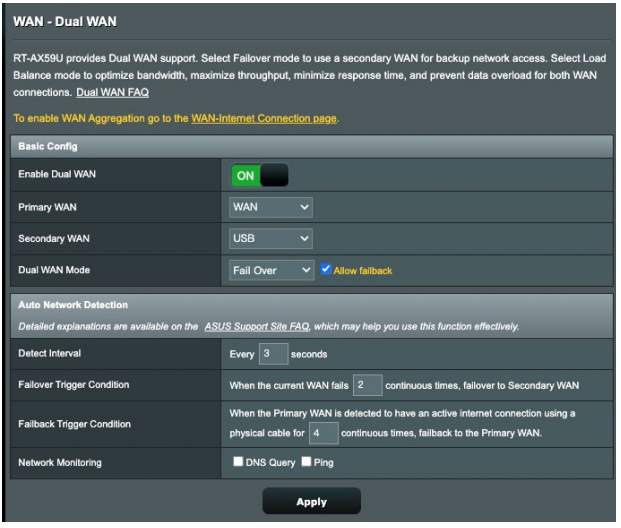
- **Tip conexiune WAN**: Alegeți tipul furnizorului de servicii Internet. Puteți alege între **Automatic IP (IP automat)**, **PPPoE**, **PPTP**, **L2TP** sau **static IP (IP static)**. Consultați-vă furnizorul de servicii Internet dacă ruterul dvs. nu poate obține o adresă IP validă sau dacă aveți dubii cu privire la tipul conexiunii WAN.
- **Activare WAN**: Selectați **Yes (Da)** pentru a permite ruterului să acceseze Internetul. Selectați **No (Nu)** pentru a dezactiva accesul la Internet.
- **Activare NAT**: NAT (Network Address Translation - translatare adresă de rețea) este un sistem unde un IP public (IP de WAN) este utilizat pentru a furniza acces la Internet clienților de rețea care au o adresă IP privată într-un mediu LAN. Adresa IP privată a fiecărui client din rețea este salvată într-un tabel NAT şi este utilizată pentru a direcționa 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 rețea 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 rețea simplificată pentru cu capacitatea de configurare şi transfer de fişiere la distanță. Folosind UPnP, noile dispozitive din rețea sunt descoperite în mod automat. După ce sunt conectate la rețea, dispozitivele pot fi configurate la distanță pentru a accepta aplicații P2P, jocuri interactive, conferințe video şi servere web sau proxy. Spre deosebire de protocolul de direcționare a porturilor, care implică o configurare manuală a setărilor pentru porturi, UPnP configură în mod automat ruterul să accepte conexiunile primite şi să direcționeze solicitările către un anumit PC din rețeaua locală.
- **Conectare la serverul DNS**: Permite acestui ruter să obțină 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. Consultați-vă furnizorul de servicii Internet şi completați câmpurile de autentificare, dacă este necesar.
- **Nume gazdă**: Acest câmp vă permite să introduceți un nume de gazdă pentru ruterul dvs. Aceasta este, în General (Generalități), o cerință specială din partea furnizorului de servicii Internet. Dacă furnizorul dvs. de servicii Internet a atribuit un nume de gazdă computerului dvs., introduceți aici numele respectiv.

- **Adresă MAC**: Adresa MAC este un identificator unic pentru dispozitivul dvs. conectat în rețea. Unii furnizori de servicii Internet monitorizează adresa MAC a dispozitivelor din rețea 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, puteți:
  - să contactați ISP-ul şi să îi solicitați să vă actualizeze adresa MAC asociată abonamentului.
  - să clonați sau să modificați adresa MAC a ruterului wireless ASUS pentru a corespunde adresei MAC a dispozitivului care era anterior recunoscut în rețea de către ISP.
- **DHCP query frequency (Frecvență interogare DHCP):** schimbă setările pentru intervalul de descoperire DHCP, cu scopul de a evita supraîncărcarea serverului DHCP.

3.18.2 WAN dual

Routerul dvs. wireless ASUS oferă suport dual WAN. Puteți seta caracteristica dual WAN la oricare dintre următoarele două moduri:

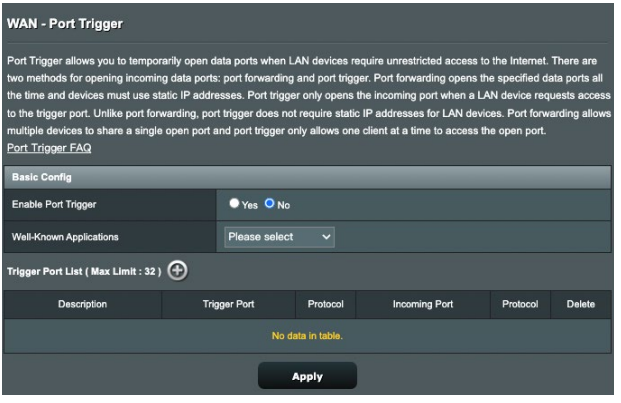
- **Failover Mode (Mod failover):** Selectați acest mod pentru a utiliza rețeaua WAN secundară drept rețea de acces de rezervă.
- **Load Balance Mode (Mod echilibrare sarcină):** Selectați acest mod pentru a optimiza lățimea de bandă, minimiza timpul de răspuns şi preveni suprasolicitarea cu date pentru conexiunile WAN principală şi secundară.



3.18.3 Triggering de port

Operația 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 rețeaua locală realizează o conexiune de ieşire pe un port specificat. Triggeringul de port este utilizat în următoarele situații:

- Mai mulți clienți locali necesită redirecționarea prin porturi pentru aceeaşi aplicație, în momente diferite.
- O aplicație necesită anumite porturi de intrare, care diferă de porturile de ieşire.



Pentru a configura triggeringul de port:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **Port Trigger (Triggering de port)**.
2. În câmpul **Enable Port Trigger (Activare declanşare port)**, bifați opțiunea **Yes (Da)**.
3. În câmpul **Well-Known Applications (Aplicații cunoscute)**, selectați jocurile şi serviciile web populare pe care doriți să le adăugați în Port Trigger List (Listă declanşare porturi).
4. În tabelul **Trigger Port List (Listă porturi declanşare)**, introduceți manual următoarele informații:
   - **Descriere**: Introduceți 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.

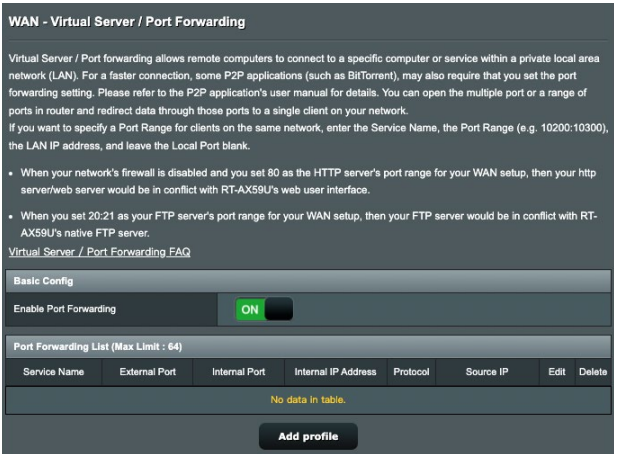
5. Faceţi clic pe **Add (Adăugare)** pentru a introduce în listă informaţiile referitoare la declanşarea porturilor. Faceţi clic pe butonul **Delete (Ştergere)** pentru a elimina o intrare de declanşare a porturilor din listă.
6. Când aţi terminat, faceţi clic pe **Apply (Se aplică)**.

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.

3.18.4 Server virtual/Redirecționare porturi

Redirecționarea porturilor este o metodă de direcționare a traficului de rețea dinspre Internet, printr-un anumit port sau printr-un anumit interval de porturi, către un dispozitiv sau mai multe dispozitive din rețeaua dvs. locală. Configurarea redirecționării porturilor pe ruterul dvs. permite PC-urilor din afara rețelei să acceseze anumite servicii furnizate de un PC din rețeaua dvs.



Pentru a configura redirecționarea porturilor:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **Virtual Server/Port Forwarding (Server virtual/Redirecționare porturi)**.
2. În câmpul **Enable Port Forwarding (Activare redirecționare porturi)**, bifați **Yes (Da).**
3. Faceți clic pe **Adăugare profil** și introduceți următoarele informații în tabelul **Listă redirecționare porturi**:
   - **Nume serviciu**: Introduceți numele serviciului.
   - **Protocol**: Selectați protocolul. În cazul în care aveți dubii, selectați opțiunea **BOTH (Ambele)**.
   - **Port extern:** Portul extern acceptă următoarele formate:
     1) Intervalele de porturi cu separație prin două puncte „:" între portul de început și cel de sfârșit, de exemplu, 300:350.

2) Porturi individuale separate prin virgulă „,", de exemplu, 566, 789.

3) O combinație de intervale de porturi și porturi individuale, separate prin două puncte „:" și virgule „,", de exemplu, 1015:1024, 3021.

- **Adresă IP internet:** Introduceți adresa IP a clientului din rețeaua LAN.

NOTĂ: Folosiți o adresă IP statică pentru clientul local, pentru ca operația de redirecționare a porturilor să se deruleze corect. Consultați secțiunea **3.10 LAN** pentru mai multe informații.

- **Port internet:** Introduceți un port specific pentru a primi pachetele redirecționate. Lăsați acest câmp necompletat dacă doriți ca pachetele primite să fie redirecționate către intervalul de porturi specificat.
- **IP sursă:** Dacă doriți să deschideți portul pentru o anumită adresă IP de internet, introduceți adresa IP pe care doriți să o specificați în câmpul IP sursă.

4. Faceți clic pe **Add (Adăugare)** pentru a introduce în listă informațiile referitoare la declanșarea porturilor. Faceți clic pe butonul **Delete (Ştergere)** pentru a elimina o intrare de declanșare a porturilor din listă.
5. Când ați terminat, faceți clic pe **Apply (Se aplică).**

Pentru a verifica dacă opțiunea Port Forwarding (Redirecționare porturi) a fost configurată cu succes:

- Verificați dacă serverul sau aplicația este configurată și funcționează.
- Veți avea nevoie de un client din afara rețelei LAN, dar care să aibă acces la Internet (denumit „client Internet"). Acest client nu trebuie să fie conectat la ruterul ASUS.
- Pe clientul Internet, folosiți IP-ul WAN al ruterului pentru a accesa serverul. Dacă redirecționarea porturilor este configurată cu succes, ar trebui să puteți accesa fişierele sau aplicațiile.

Diferențe între triggeringul de port şi redirecționarea porturilor:

- Triggeringul de port va funcționa chiar dacă nu se configurează o adresă IP specifică în rețeaua LAN. Spre deosebire de redirecționarea porturilor, care necesită o adresă IP statică în rețeaua LAN, triggeringul de port permite redirecționarea 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 aplicații care în mod normal ar necesita redirecționarea manuală a aceloraşi porturi către fiecare PC din rețea.
- Triggeringul de port oferă o mai mare securitate decât redirecționarea porturilor, deoarece porturile de intrare nu sunt deschise în permanență. Acestea se deschid numai când o aplicația realizează o conexiune de ieşire prin intermediul portului de declanşare.

3.18.5 DMZ

Un DMZ virtual expune un client la rețeaua Internet, permițând acestui client să primească toate pachetele direcționate către rețeaua dvs. LAN.

Traficul primit de pe Internet este de obicei direcționat către un anumit client numai dacă pentru rețeaua respectivă s-a configurat redirecționarea porturilor sau un declanşator de porturi. Într-o configurație de tip DMZ, un client din rețea primeşte toate pachetele de intrare.

Configurarea DMZ pentru o rețea este utilă când aveți nevoie ca porturile de intrare să fie deschise sau când doriți să găzduiți un server de domenii, un server web sau un server e-mail.

ATENȚIE: Deschierea tuturor porturilor unui client face ca rețeaua să fie vulnerabilă la atacurile din exterior. Trebuie să fiți conştient de riscurile de securitate pe care le implică o configurație DMZ.

Pentru a configura DMZ:

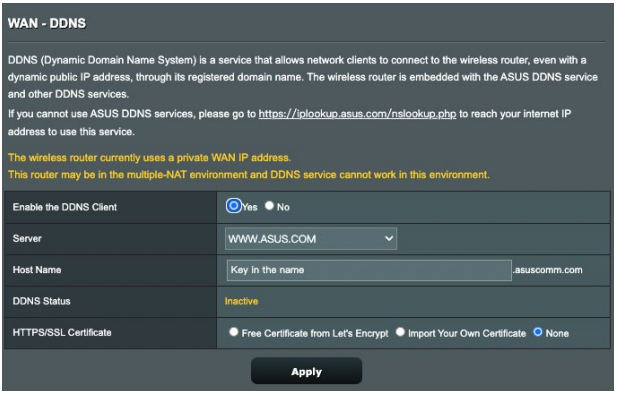
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **DMZ**.
2. Configurați următoarele setări. Când ați terminat, faceți clic pe **Apply (Aplicare)**.
   - **Adresa IP a stației expuse:** Introduceți adresa IP pentru clientul din rețeaua LAN, client care va furniza serviciul DMZ şi care va fi expus pe Internet. Asigurați-vă că clientul de server are o adresă IP statică.

Pentru eliminarea DMZ:

1. Ştergeți adresa IP a clientului din rețea LAN din caseta de text **IP Address of Exposed Station (Adresa IP a stației expuse)**.
2. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

3.18.6 DDNS

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



Pentru a configura DDNS:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **DDNS**.
2. Configurați următoarele setări: Când ați terminat, faceți clic pe **Apply (Aplicare)**.
   - **Activare client DDNS**: Activați DDNS pentru a accesa ruterul ASUS prin intermediul numelui DNS şi nu prin intermediul adresei IP WAN.
   - **Nume server şi gazdă**: Alegeți ASUS DDNS sau un alt serviciu DDNS. Dacă doriți să utilizați ASUS DDNS, completați numele gazdei în formatul xxx.asuscomm.com (xxx este numele gazdei).
   - Dacă doriți să utilizați un alt serviciu DDNS, faceți clic pe FREE TRIAL (Perioadă de încercare gratuită) şi înregistrați-vă online mai întâi. Completați numele de utilizator sau adresa de mail şi parola sau cheia DDNS.
   - **Activare caracter wildcard**: Activați caracterul wildcard, dacă serviciul DDNS necesită acest lucru.

NOTE:

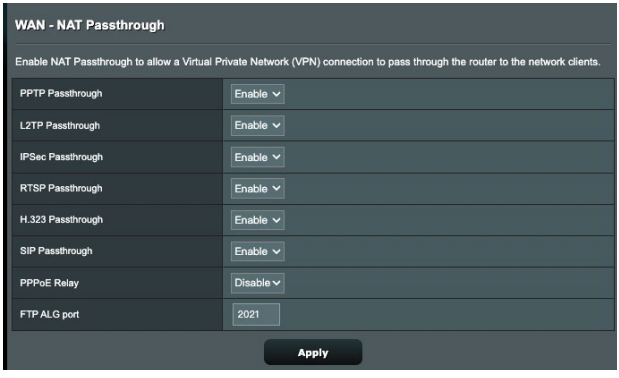
Serviciul DDNS nu va funcționa în următoarele condiții:

- 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 rețea care utilizează mai multe tabele NAT.

3.18.7 NAT Passthrough (Trecere NAT)

Parametrul NAT Passthrough (Trecere NAT) permite unei conexiuni aparținând unei rețele private virtuale să treacă prin ruter şi să fie direcționară către clienții din rețea. Opțiunile PPTP Passthrough (Trecere PPTP), L2TP Passthrough (Trecere L2TP), IPsec Passthrough (Trecere IPsec) şi RTSP Passthrough (Trecere RTSP) sunt activate în mod implicit.

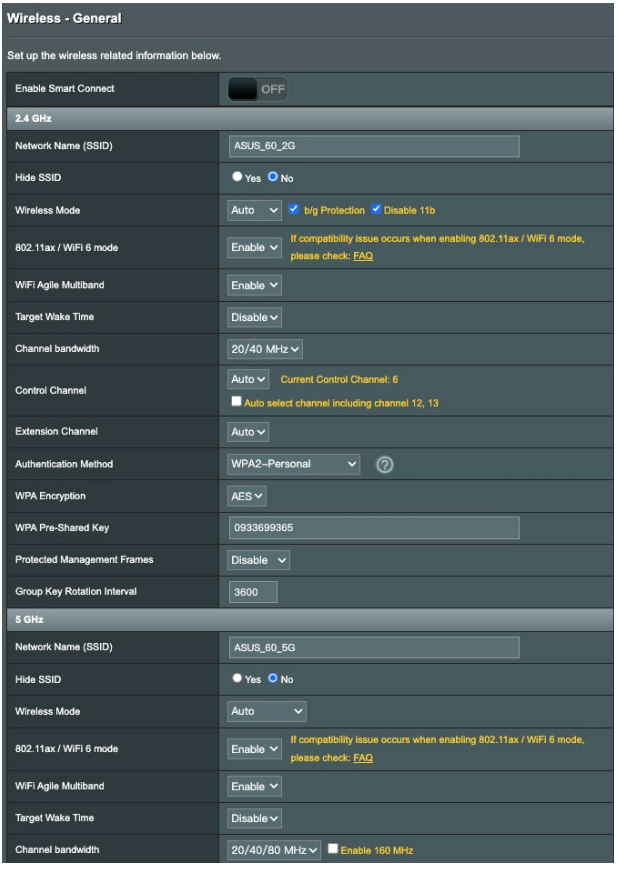
Pentru a activa/dezactiva setările pentru parametrul NAT Passthrough (Trecere NAT), mergeți la **Advanced Settings (Setări avansate)** > **WAN** > **NAT Passthrough (Trecere NAT)**. Când ați terminat, faceți clic pe **Apply (Aplicare)**.



3.19 Wireless

3.19.1 General (Generalități)

General (Generalități) vă permite să configurați setările de bază pentru rețeaua wireless.



Pentru configurarea setărilor de bază pentru rețeaua wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Wireless** > **General (Generalități)**.
2. Selectați banda de frecvență de 2,4 GHz sau de 5 GHz pentru rețeaua dvs. wireless.
3. Dacă doriți să utilizați funcția Smart Connect (Conectare inteligentă), deplasați glisorul la **ON (ACTIVAT)** în câmpul **Enable Smart Connect (Activare conectare inteligentă).**

Această funcție va conecta în mod automat clienții din rețeaua dvs. la banda corespunzătoare (2,4 GHz sau 5 GHz) pentru ca aceştia să beneficieze de cea mai bună viteză.

4. Atribuiți un nume unic, care să conțină maximum 32 de caractere, pentru SSID (Service Set Identifier - identificator set servicii) sau pentru numele rețelei, cu scopul de a identifica rețeaua wireless. Dispozitivele Wi-Fi pot identifica rețeaua wireless şi se pot conecta la aceasta prin intermediul SSID-ului atribuit. SSID-urile de pe bannerul cu informații sunt actualizate după ce în setări sunt salvate noi SSID-uri.

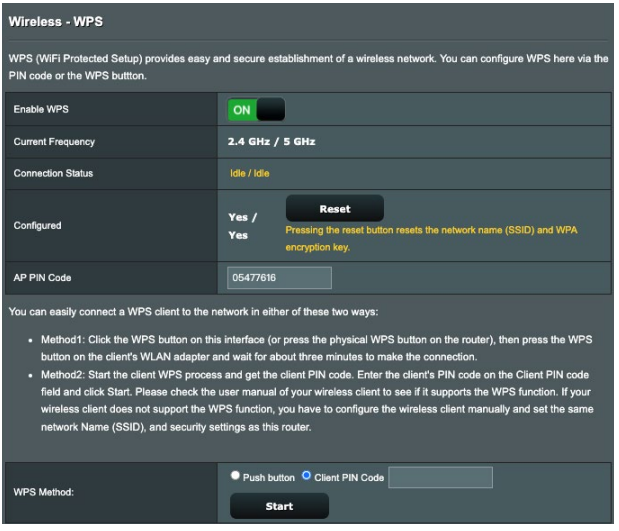
NOTĂ: Puteți atribui SSID-uri unice pentru benzile de frecvență de 2,4 GHz şi de 5 GHz.

5. În câmpul **Hide SSID (Ascundere SSID)**, selectați **Yes (Da)** pentru a împiedica dispozitivele wireless să detecteze SSID-ul dvs. Când este activată această funcție, va trebui să introduceți manual SSID-ul pe dispozitivul wireless pentru a accesa rețeaua wireless.
6. Selectați oricare din aceste opțiuni privind modul wireless pentru a stabili tipurile de dispozitive wireless care se pot conecta la ruterul wireless:
   - **Automat**: Selectați **Auto (Automat)** pentru a permite dispozitivelor 802.11ac, 802.11n, 802.11g şi 802.11b să se conecteze la ruterul wireless.
   - **Doar N**: Selectați **N only (Doar N)** pentru a maximiza performanțele standardului wireless N. Această setare previne conectarea la ruterul wireless a dispozitivelor 802.11g şi 802.11b.
   - **Moştenit**: Selectați **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.
7. Selectați canalul de funcționare pentru ruterul dvs. wireless. Selectați **Auto (Automat)** pentru a permite ruterului wireless să selecteze automat canalul care are cele mai puține interferențe.
8. Selectați lățimea de bandă a canalului pentru a obține viteze de transmitere mai mari.
9. Selectați metoda de autentificare.
10. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

3.19.2 WPS

WPS (WiFi Protected Setup - configurare WiFi 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 sau 6 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/WPA2/WPA3-Personal. WPS nu acceptă rețelele wireless care utilizează metodele de criptare Shared Key (Cheie partajată), WPA-Enterprise, WPA2-Enterprise şi RADIUS.

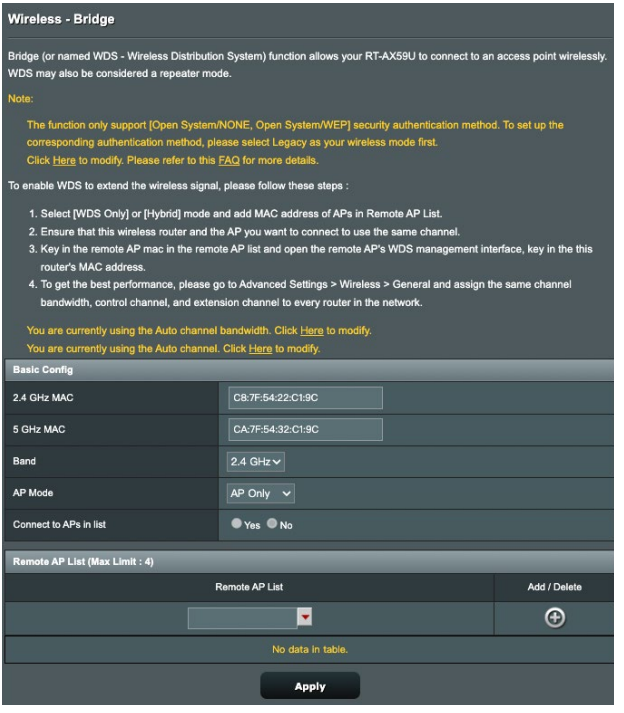
4. În câmpul WPS Method (Metodă WPS), selectați **Push button (Buton de comandă)** sau **Client PIN Code (Cod PIN client)**. Dacă selectați opțiunea **Push button (Buton de comandă)**, mergeți la pasul 5. Dacă selectați opțiunea **Client PIN Code (Cod PIN client)**, mergeți la pasul 6.
5. Pentru a configura WPS folosind butonul WPS al ruterului, urmați paşii de mai jos:
   a. Faceți clic pe **Start (Pornire)** sau apăsați butonul WPS care poate fi găsit în partea din spat a ruterului wireless.
   b. Apăsați pe butonul WPS de pe dispozitivului wireless. Acesta poate fi identificat cu ajutorul siglei WPS.

   NOTĂ: Verificați dispozitivul wireless sau consultați 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, urmați paşii de mai jos:
   a Localizați codul PIN WPS în manualul de utilizare al dispozitivului dvs. wireless sau de pe dispozitivul însuşi.
   b. Introduceți codul PIN al clientului în caseta de text.
   c. Faceți clic pe **Start (Pornire)** 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.

3.19.3 Punte

Modul Punte sau WDS (Wireless Distribution System - sistem de distribuție wireless) permite ruterului dvs. wireless ASUS să se conecteze la un alt punct de acces wireless, în mod exclusiv, împiedicând alte dispozitive sau stații 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, mergeți **Advanced Settings (Setări avansate)** > **Wireless** > **WDS**.
2. Selectați banda de frecvență pentru puntea wireless.

3. În câmpul **AP Mode (Mod AP)**, selectați una din aceste opțiuni:
   - **Numai AP**: Dezactivează funcția Wireless Bridge (Punte wireless).
   - **Numai WDS**: Activează funcția Wireless Bridge (Punte wireless), dar împiedică alte dispozitive/stații de lucru wireless să se conecteze la ruter.
   - **HIBRID**: Activează funcția Wireless Bridge (Punte wireless) şi permite altor dispozitive/stații 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)** , faceți clic pe **Yes (Da)** dacă doriți să vă conectați la un punct de acces din lista cu puncte de acces la distanță.
5. În mod implicit, canalul funcțional/de control pentru puntea wireless este setat la **Auto (Automat)** pentru a permite routerului să selecteze în mod automat canalul cu cea mai mică interferență.

   Puteți modifica opțiunea **Control Channel (Canal de control)** din **Advanced Settings (Setări avansate)** > **Wireless** > **General (Generalități)**.

   NOTĂ: Disponibilitatea canalelor diferă în funcție de țară sau regiune.

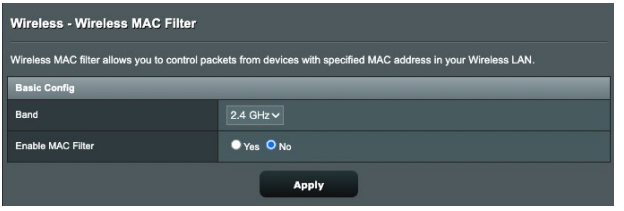
6. În lista cu puncte de acces la distanță, introduceți o adresă MAC şi faceți clic pe butonul **Add (Adăugare)** ⊕ pentru a introduce adresa MAC a altor puncte de acces disponibile.

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

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

3.19.4 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 rețeaua dvs. wireless.

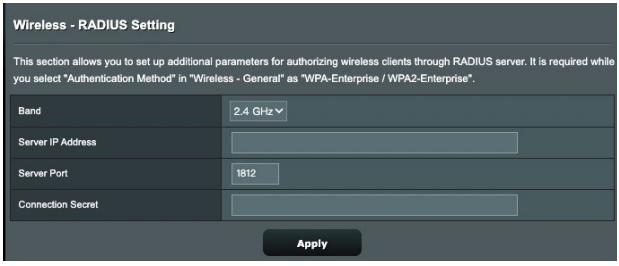


Pentru a configura filtrul MAC wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Wireless** > **Wireless MAC Filter (Filtru MAC wireless)**.
2. Selectați banda de frecvență.
3. Bifați **Yes (Da)** în câmpul **Enable Mac Filter (Activare filtru Mac)**.
4. În lista verticală **MAC Filter Mode (Mod filtru MAC)**, selectați **Accept (Acceptare)** sau **Reject (Respingere)**.
   - Selectați **Accept (Acceptare)** pentru a permite dispozitivelor din lista de filtrare MAC să acceseze rețeaua wireless.
   - Selectați **Reject (Respingere)** pentru a împiedica dispozitivele din lista de filtrare MAC să acceseze rețeaua wireless.
5. În lista de filtrare MAC, faceți clic pe butonul **Add (Adăugare)** ⊕ și introduceți adresa MAC a dispozitivului wireless.
6. Faceți clic pe **Apply (Aplicare)**.

3.19.5 Setarea RADIUS

Setarea RADIUS (Remote Authentication Dial In User Service - serviciu de autentificare la distanță a utilizatorilor, prin apelare) oferă un strat suplimentar de siguranță atunci când alegeți opțiunea WPA-Enterprise, WPA2-Enterprise sau Radius cu 802.1x ca și mod de autentificare.



Pentru a configura setările wireless RADIUS:

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

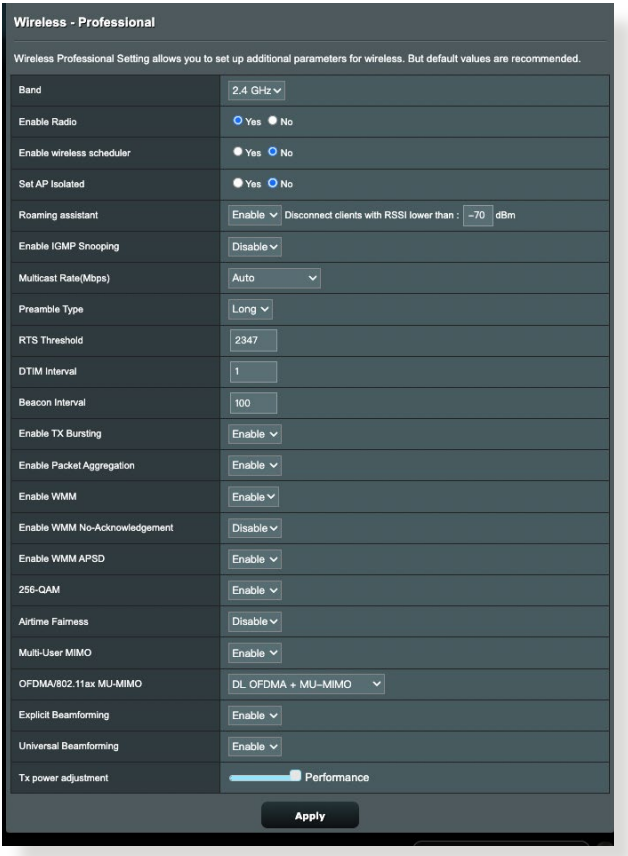
   NOTĂ: Consultați secțiunea **3.19.1 General (Generalități)e** pentru detalii privind configurarea modului de autentificare al ruterului wireless.

2. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Wireless** > **RADIUS Setting (Setare RADIUS)**.
3. Selectați banda de frecvență.
4. În câmpul **Server IP Address (Adresă IP server)**, introduceți adresa IP a serverului RADIUS.
5. În câmpul **Server Port (Port server)**, introduceți portul pentru server.
6. În câmpul **Connection Secret (Secret conexiune)**, atribuiți parola pentru accesarea serverului RADIUS.
7. Faceți clic pe **Apply (Aplicare)**.

3.19.6 Professional (Profesional)

Ecranul Professional (Profesional) oferă opțiuni avansate de configurare.

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



În ecranul setări **Professional (Profesionale)** , puteți configura următoarele:

- **Bandă**: Selectați banda de frecvență pentru care se vor aplica setările profesionale.
- **Activare radio**: Selectați **Yes (Da)** pentru a activa caracteristica wireless a rețelei. Selectați **No (Nu)** pentru a dezactiva caracteristica wireless a rețelei.

- **Enable wireless scheduler (Activare planificator fără fir)**: Selectați **Yes (Da)** pentru a activa și configura planificatorul wireless. Selectați **No (Nu)** pentru a dezactiva caracteristica wireless a rețelei.
  - **Dată de activare radio (zile ale săptămânii)**: Puteți specifica zilele săptămânii în care caracteristica wireless a rețelei să fie activată.
  - **Perioadă din zi pentru activarea radio**: Puteți specifica un interval de timp în care caracteristica wireless a rețelei să fie activată în timpul săptămânii.
  - **Dată de activare radio (weekend)**: Puteți specifica zilele de weekend în care caracteristica wireless a rețelei să fie activată.
  - **Perioadă din zi pentru activarea radio**: Puteți specifica un interval de timp în care caracteristica wireless a rețelei să fie activată în timpul weekendului.
- **Setare AP izolat**: Elementul Set AP isolated (Setare AP izolat) împiedică dispozitivele wireless din rețeaua dvs. să comunice între ele. Această caracteristică este utilă dacă se întâmplă adesea ca mulți vizitatori să se conecteze sau să se deconecteze de la rețeaua dvs. Selectați **Yes (Da)** pentru a activa această caracteristică sau **No (Nu)** pentru a o dezactiva.
- **Roaming Assistant (Asistent roaming):** În configurațiile de rețea care implică mai multe puncte de acces sau repetitoare wireless, clienții wireless nu se pot conecta uneori automat la cel mai bun PA disponibil deoarece sunt conectați în continuare la routerul wireless principal. Activați această setare astfel încât clientul se va deconecta de la routerul wireless principal dacă puterea semnalului este sub un prag specific şi se va conecta la un semnal mai puternic.
- **Enable IGMP Snooping (Activare snooping IGMP):** Activarea acestei funcții permite monitorizarea IGMP (Internet Group Management Protocol) între dispozitive şi optimizează traficul cu distribuire multiplă în rețeaua wireless.
- **Rată distribuire multiplă (Mbps)**: Selectați rata de transmisie pentru distribuirea multiplă sau faceți 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 redundanță ciclică). CRC este o metodă de detectare a erorilor care au loc în timpul transmiterii datelor. Selectați **Short (Scurt)** în cazul unei rețele wireless ocupate, cu trafic intens. Selectați **Long (Lung)** dacă rețeaua dvs. wireless are în componență dispozitive wireless mai vechi.

- **AMPDU RTS:** Activarea acestei funcții permite crearea unui grup de cadre înainte de transmiterea acestora şi utilizarea funcției RTS pentru fiecare cadru AMPDU pentru comunicarea între dispozitivele cu standard wireless 802.11g şi 802.11b.
- **RTS Threshold (Prag RTS):** Selectați o valoare mai mică pentru RTS (Request to Send - solicitare de trimitere) pentru a îmbunătăți comunicarea wireless într-o rețea wireless ocupată sau cu multe interferențe, 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. Reduceți valoarea pentru Beacon Interval (Interval semnalizator) în cazul unei conexiuni wireless instabile sau pentru dispozitive aflate în roaming.
- **Activare rafală TX**: Acest parametru îmbunătățeşte viteza de transmitere între ruterul wireless şi dispozitivele 802.11g.
- **Activare WMM APSD**: Activați 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. Selectați **Disable (Dezactivare)** pentru a dezactiva caracteristica WMM APSD.
- **Optimize AMPDU aggregation (Optimizare agregare AMPDU):** Optimizați numărul maxim de unități MPDU dintr-un cadru AMPDU şi evitați pierderea sau deteriorarea

pachetelor în timpul transmisiei în canalele wireless predispuse la erori.

- **Turbo QAM:** Activarea acestei funcţii permite compatibilitatea 256-QAM (MCS 8/9) pentru banda de 2,4 GHz pentru a obține o acoperire mai bună pe frecvența respectivă.
- **Airtime Fairness (Repartizare echitabilă a spectrului radio):** Grație funcției Airtime Fairness (Repartizare echitabilă a spectrului radio), viteza de rețea nu este determinată de cel mai lent trafic. Alocând durate de timp egale fiecărui client, funcția Airtime Fairness (Repartizare echitabilă a spectrului radio) permite fiecărei transmisii să se desfăşoare la viteza cu potențialul cel mai ridicat.
- **Explicit Beamforming (Formare undă clară):** Atât adaptorul, cât şi routerul WLAN al clientului acceptă tehnologia de formare a undei. Această tehnologie permite acestor dispozitive să îşi comunice reciproc estimarea privind canalul şi direcția de ghidare pentru a îmbunătăți viteza de descărcare şi de încărcare.
- **Universal Beamforming (Formare undă universală):** Pentru adaptoarele de rețea wireless de generație veche care nu acceptă formarea undei, routerul estimează canalul şi stabileşte direcția de ghidare în vederea îmbunătățirii vitezei de descărcare.

4 Utilitarelor

NOTE:

- Descărcați și instalați 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/Rescue.zip
- Utilitarul Windows Printer Utility, versiunea 1.0.5.5, poate fi descărcat de la adresa http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.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 și vă permite să configurați setările de conectare în rețeaua wireless.

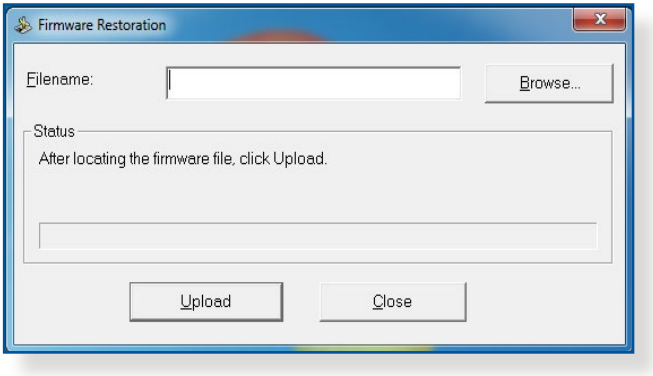
Pentru a lansa utilitara Detectează Dispozitivul:

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

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

4.2 Restaurare firmware

Utilitarul Firmware Restoration (Restaurare 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! Lansați modul de salvare înainte de a utiliza utilitarul Firmware Restoration (Restaurare firmware).

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

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

1. Deconectați ruterul fără fir de la sursa de alimentare.
2. Țineți apăsat butonul Reset (Reinițializare) de pe panoul din spate şi simultan conectați din nou ruterul fără fir la sursa de alimentare. Eliberați butonul Reset (Reinițializare) 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. Setați un IP static pentru computerul dvs. şi utilizați următoarele instrumente pentru a configura setările TCP/IP.

   Adresă IP: 192.168.1.x

   Mască subrețea: 254.254.255.0

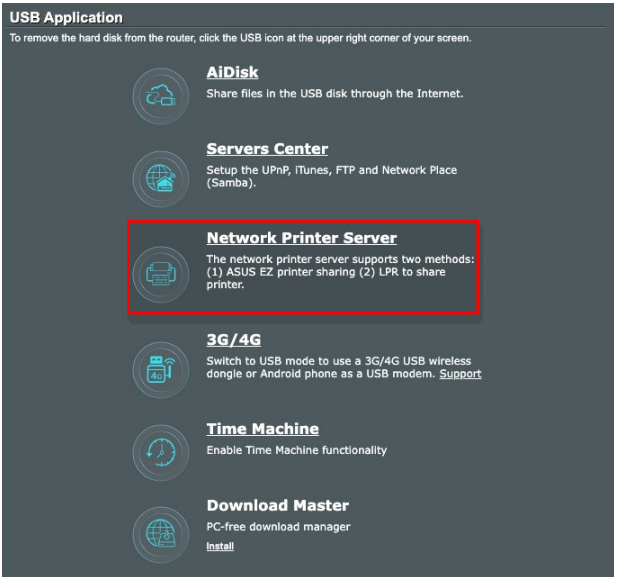
4. De pe desktopul computerului, faceți clic pe **Start (Pornire)** > **All Programs (Toate programele)** > **ASUS Utility RT-AX59U Wireless Router (Ruter fără fir RT-AX59U utilitar ASUS)** > **Firmware Restoration (Restaurare firmware)**.
5. Specificați un fișier de firmware, apoi faceți clic pe **Upload (Încărcare)**.

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

4.3 Configurarea serverului de tipărire

4.3.1 Partajarea imprimante EZ ASUS

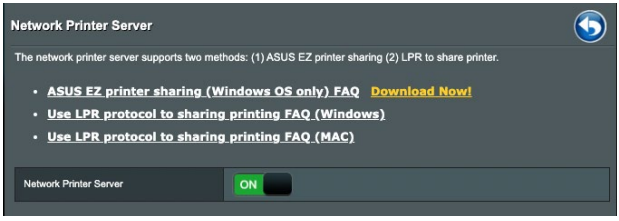
Utilitarul de partajare a imprimantei EZ ASUS vă permite să conectați o imprimantă USB la ruterul USB al ruterului wireless şi să configurați un server de tipărire. Acest lucru permite clienților din rețeaua dvs. să tipărească şi să scaneze fişiere în modul wireless.



NOTĂ: Funcția server de tipărire este acceptată în sistemele de operare Windows® 7/8/8.1/10/11.

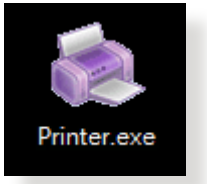
Pentru a configura modul de partajare a imprimantei EZ:

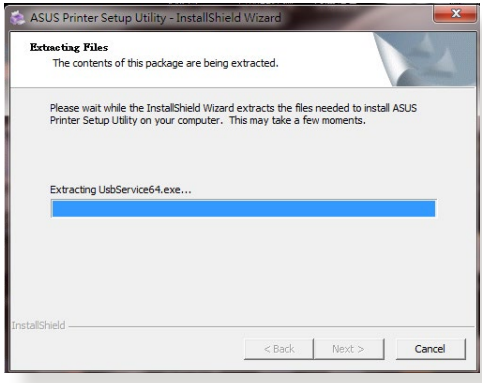
1. Din panoul de navigare, mergeți la **General (Generalități)** > **USB Application (Aplicație USB)** > **Network Printer Server (Server imprimantă rețea)**.
2. Faceți clic pe **Download Now! (Descărcare acum!)** pentru a descărca utilitarul de tipărire în rețea.



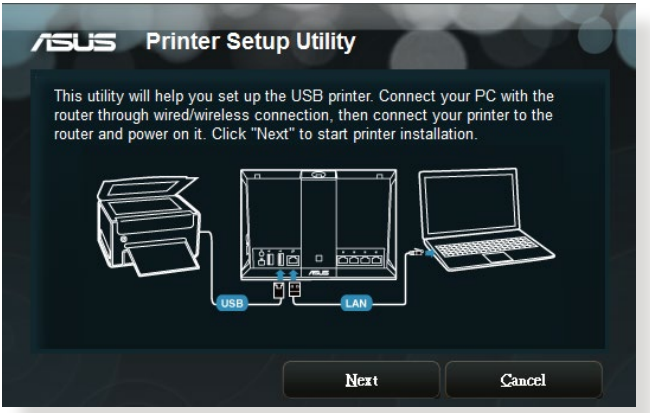
NOTĂ: Utilitarul de tipărire în rețea este acceptat numai în sistemele de operare Windows® 7/8/8.1/10/11. Pentru a instala utilitarul pe un sistem de operare Mac, selectați opțiunea **Use LPR protocol for sharing printer (Utilizare protocol LPR pentru partajarea imprimantei)**.

3. Dezarhivați fișierul descărcat şi faceți clic pe pictograma Printer (Imprimantă) pentru a executa programul de configurare a imprimantei în rețeas.





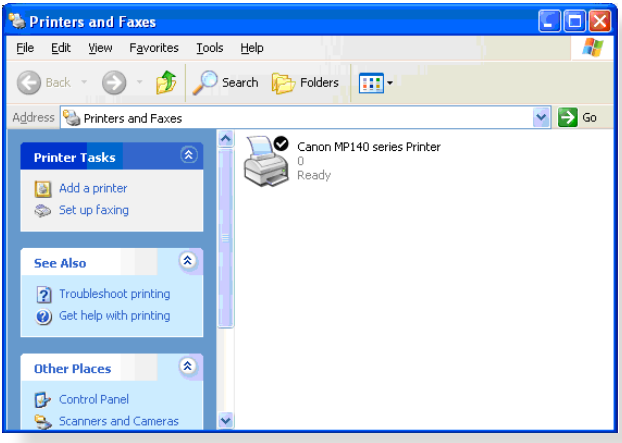
4. Urmați instrucțiunile de pe ecran pentru a configura componentele hardware, apoi faceți clic pe **Next (Următorul)**.



5. Aşteptați câteva minute pentru finalizarea instalării inițiale. Faceți clic pe **Next (Următorul)**.
6. Faceți clic pe **Finish (Finalizare)** pentru a încheia instalarea.

7. Urmați instrucțiunile Windows® OS pentru a instala driverul de imprimantă.

8. După ce instalarea driverului imprimantei este completă, clienții de rețea vor putea utiliza imprimanta.



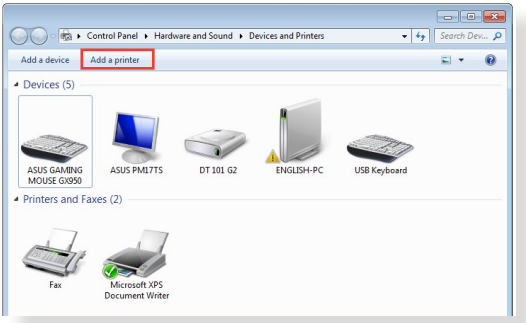
4.3.2 Utilizarea protocolului LPR pentru partajarea imprimantei

Puteți partaja imprimanta cu computere care funcționează cu sistemele de operare Windows® şi MAC prin utilizarea protocolului LPR/LPD (Line Printer Remote/Line Printer Daemon - Control la distanță imprimantă de linie/Daemon imprimantă de linie).

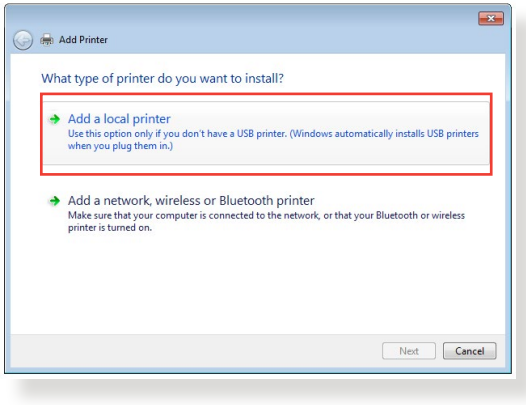
Partajarea imprimantei compatibile LPR

Pentru partajarea imprimantei compatibile LPR:

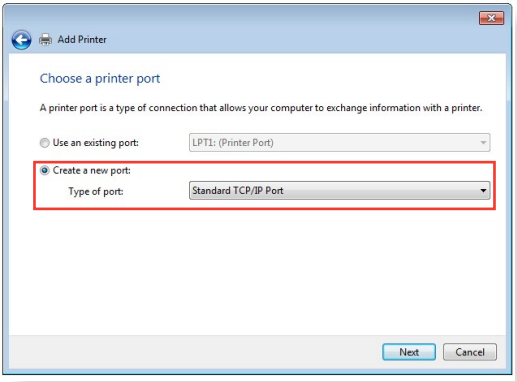
1. Din desktopul Windows®, faceți clic pe **Start (Pornire)** > **Devices and Printers (Dispozitive şi imprimante)** > **Add a printer (Adăugare imprimantă)** pentru a executa **Add Printer Wizard (Expert adăugare imprimantă)**.



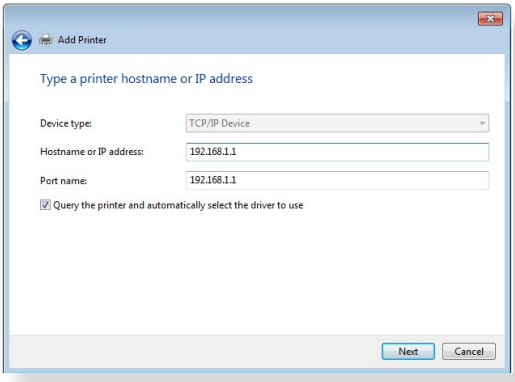
2. Selectați **Add a local printer (Adăugare imprimantă locală)** şi apoi faceți clic pe **Next (Următorul)**.



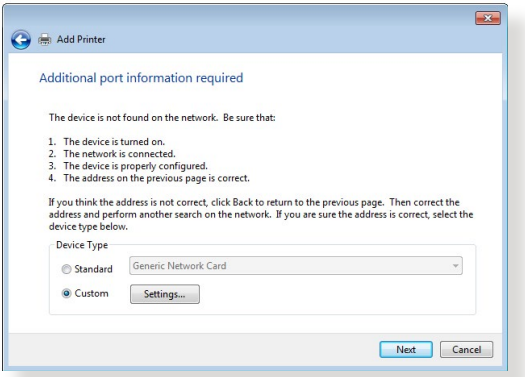
3. Selectați **Create a new port (Se creează un port nou)** apoi setați **Type of Port (Tip port)** la **Standard TCP/IP Port (Port TCP/IP standard)**. Faceți clic pe **Next (Următorul)**.



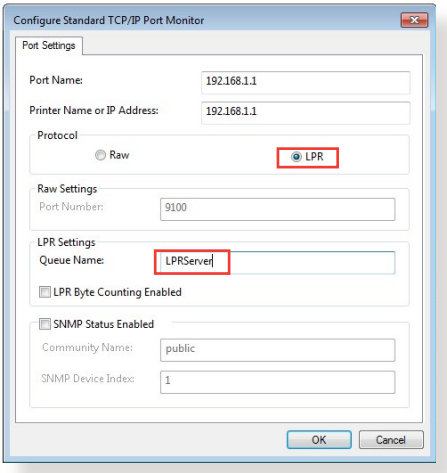
4. În câmpul **Hostname or IP address (Nume de gazdă sau adresă IP)**, introduceți adresa IP a ruterului wireless şi apoi faceți clic pe **Next (Următorul)**.



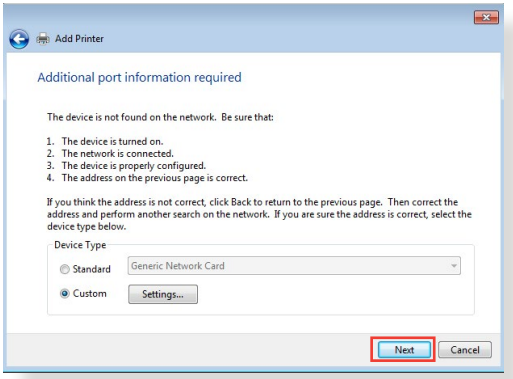
5. Selectați **Custom (Particularizat)** şi apoi faceți clic pe **Settings (Setări)**.



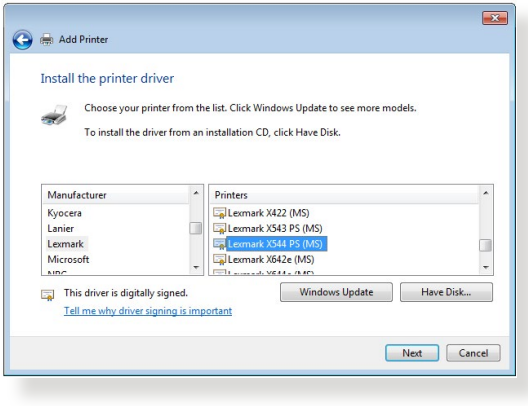
6. Setați **Protocol** la **LPR**. În câmpul **Queue Name (Nume coadă)**, introduceți o valoare pentru **LPR Server (Server LPR)** şi apoi faceți clic pe **OK** pentru a continua.



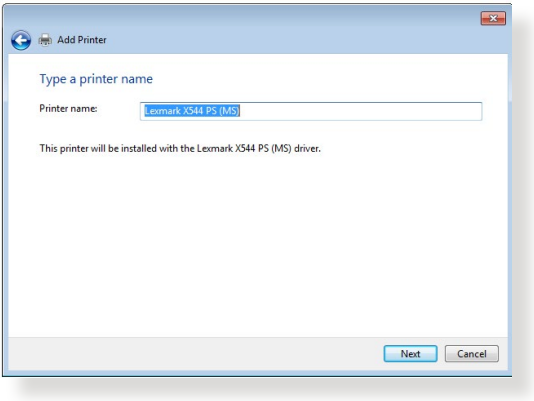
7. Faceți clic pe pe **Next (Următorul)** pentru a finaliza configurarea portului standard TCP/IP.



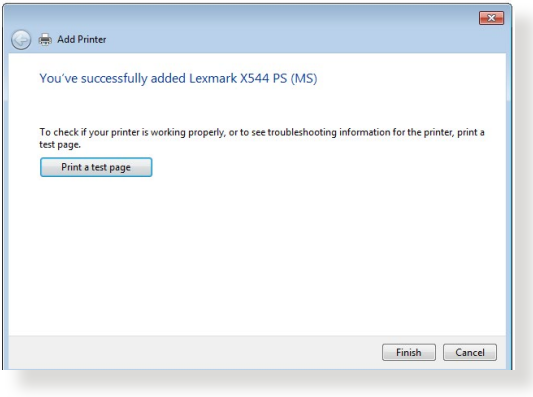
8. Instalați driverul de imprimantă din lista cu modelele distribuitorului. Dacă imprimanta dvs. nu figurează în listă, faceți clic pe **Have Disk (Obținere disc)** pentru instala manual driverele imprimantei de pe un CD-ROM sau dintr-un fișier.



9. Faceţi clic pe **Next (Următorul)** pentru a accepta numele implicit pentru imprimantă.



10. Faceţi clic pe **Finish (Terminare)** pentru a finaliza instalarea.



4.4 Download Master (Coordonator de descărcări)

Download Master (Coordonator de descărcări) este un utilitar care vă ajută să descărcați fișiere chiar și în timp ce laptopurile dvs. sau alte dispozitive sunt oprite.

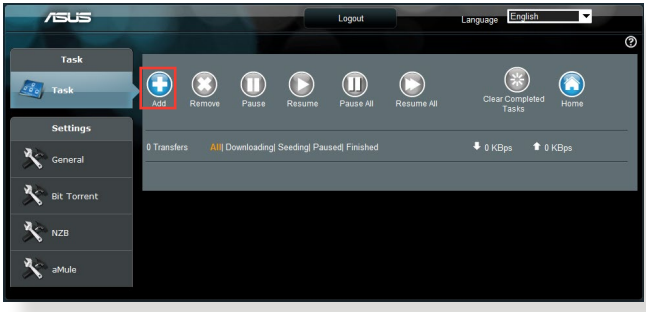
NOTĂ: Aveți nevoie de un dispozitiv USB conectat la ruterul wireless pentru a utiliza utilitarul Coordonator de descărcări.

Pentru a utiliza Download Master (Coordonator de descărcări):

1. Faceți clic pe **General (Generalități)** > **USB Application (Aplicație USB)** > **Download Master (Coordonator de descărcări)** pentru a descărca și instala automat acest utilitar.

   NOTĂ: Dacă aveți mai multe unități USB, selectați dispozitivul USB pe care doriți să fie descărcate fișierele.

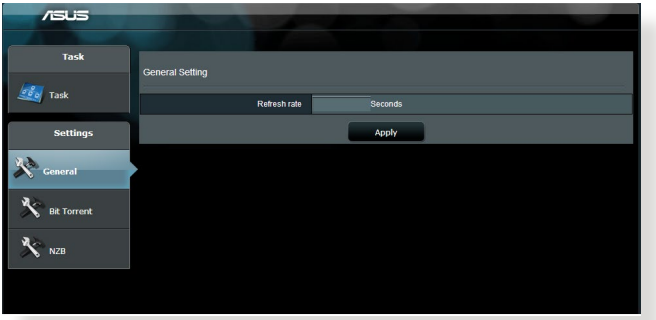
2. După finalizarea procesului de descărcare, faceți clic pe pictograma Coordonator de descărcări pentru a porni utilitarul.
3. Faceți clic pe **Add (Adăugare)** pentru a adăuga o sarcină de descărcare.



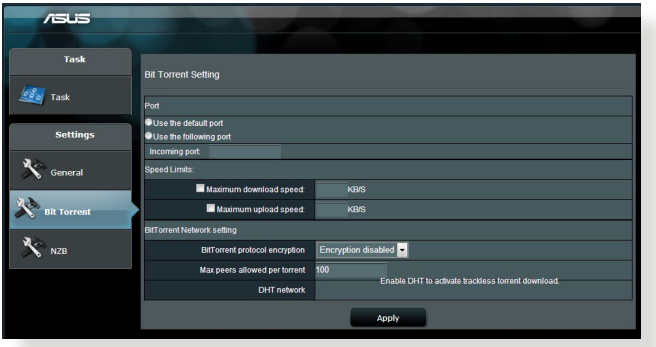
4. Selectați un tip de descărcare, precum BitTorrent, HTTP sau FTP. Furnizați un fișier de tip torrent sau o locație URL pentru a începe descărcarea.

   NOTĂ: Pentru detalii referitoare la Bit Torrent, consultați secțiunea **4.4.1 Configuring Bit Torrent download settings (Configurarea setărilor de descărcare Bit Torrent)**.

5. Utilizați panoul de navigare pentru a configura setările avansate.



4.4.1 Configurarea setărilor de descărcare pentru Bit Torrent

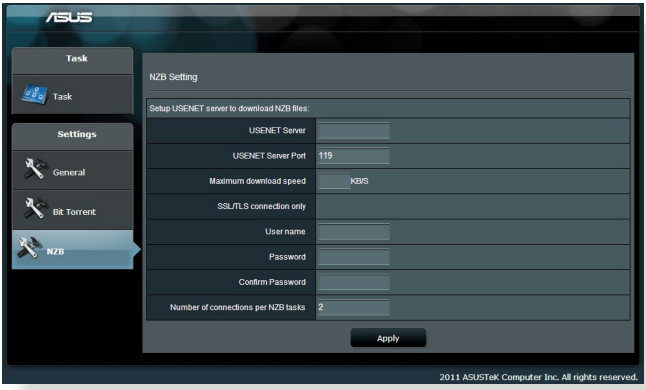


Pentru a configura setările de descărcare pentru Bit Torrent:

1. Din panoul de navigare al Download Master (Coordonator de descărcări), faceți clic pe **Bit Torrent** pentru a lansa pagina **Bit Torrent Setting (Setări Bit Torrent)**.
2. Selectați un anumit port pentru sarcina dvs. de descărcare.
3. Pentru a preveni congestionarea rețelei, puteți limita vitezele maxime pentru încărcare şi descărcare sub **Speed Limits (Limite viteză)**.
4. Puteți limita numărul maxim de perechi şi puteți activa sau dezactiva criptarea fişierelor în timpul descărcărilor.

4.4.2 Setări NZB

Puteți configura un server USENET pentru descărcarea fișierelor NZB. După introducerea setărilor USENET, selectați **Apply (Aplicare)**.



5 Remedierea defecțiunilor

Acest capitol oferă soluții pentru problemele pe care le puteți întâmpina la folosirea ruterului. În cazul în care întâmpinați probleme care nu sunt menționate în acest capitol, accesați siteul de asistență ASUS, la adresa: http://support.asus.com/. Aici puteți găsi mai multe informații despre produs, dar şi detalii de contact pentru departamentul de asistență tehnică ASUS.

5.1 Depanarea de bază

Dacă întâmpinați probleme la folosirea ruterului, parcurgeți paşii din această secțiune înainte de a căuta alte soluții.

Upgradați firmware-ul la cea mai recentă versiune.

1. Lansați interfața de utilizare web. Mergeți la **Advanced Settings (Setări avansate)** > **Administration (Administrare)** > **Firmware Upgrade (Upgrade firmware)**. Faceți clic pe **Check (Verificare)** pentru a verifica dacă este disponibil cel mai recent firmware.
2. Dacă cel mai recent firmware este disponibil, accesați siteul global ASUS, la adresa https://rog.asus.com/networking/rog-rapture-RT-AX59U-model/helpdesk_download, pentru a descărca cel mai recent firmware.
3. Din pagina **Firmware Upgrade (Upgrade firmware)**, faceți clic pe **Browse (Navigare)** pentru a localiza fişierul firmware.
4. Faceți clic pe **Upload (Încărcare)** pentru upgradarea firmwareului.

Reporniți rețeaua în următoarea secvență:

1. Opriți funcționarea modemului.
2. Deconectați modemul.
3. Opriți funcționarea ruterului şi computerelor.
4. Conectați modemul.
5. Porniți funcționarea modemului şi apoi aşteptați 2 minute.
6. Porniți funcționarea ruterului şi apoi aşteptați 2 minute.
7. Porniți funcționarea computerelor.

Verificați dacă ați 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.

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

- Când conectați computerul la ruter în modul wireless, asigurați-vă că numele rețelei wireless (SSID), metoda de criptare şi parola sunt corecte.

Verificați dacă setările rețelei sunt corecte.

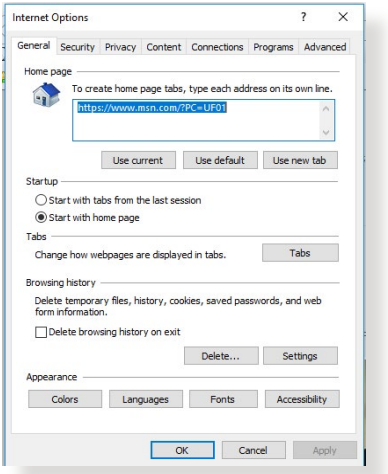
- Fiecare client din rețea trebuie să aibă o adresă IP validă. ASUS recomandă utilizarea serverului DHCP al ruterului wireless pentru alocarea automată a adreselor IP pentru computerele din rețea.
- Unii furnizori de servicii prin cablu necesită să utilizați adresa MAC a computerului care a fost înregistrat inițial în cont. Puteți vizualiza adresa MAC în interfața de utilizare web, pagina **Network Map (Hartă rețea)** > **Clients (Clienți)**, după care poziționați cursorul mouseului deasupra dispozitivului dvs. afişat în **Client status (Stare client)**.

5.2 Întrebări frecvente (FAQs)

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

- În cazul în care computerul dvs. este conectat prin cablu, verificați conectarea cablului Ethernet şi starea LEDului, după cum s-a descris în secțiunea precedentă.
- Asigurați-vă că utilizați informații de conectare corecte. Numele şi parola de conectare implicite sunt ambele „admin”. Asigurați-vă că tasta Caps Lock este dezactivată când introduceți informațiile de conectare.
- Ştergeți modulele cookie şi fişierele din browserul Web. Pentru Internet Explorer, urmați aceşti paşi:

  1. Lansați Internet Explorer, apoi faceți clic pe **Tools (Instrumente)** > **Internet Options (Opțiuni Internet)**.
  2. În**General (Generalități)**, sub **Browsing history (Istoric navigare)**, faceți clic pe **Delete... (Ştergere...)**, selectați **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 faceți clic pe **Delete (Ştergere)**.



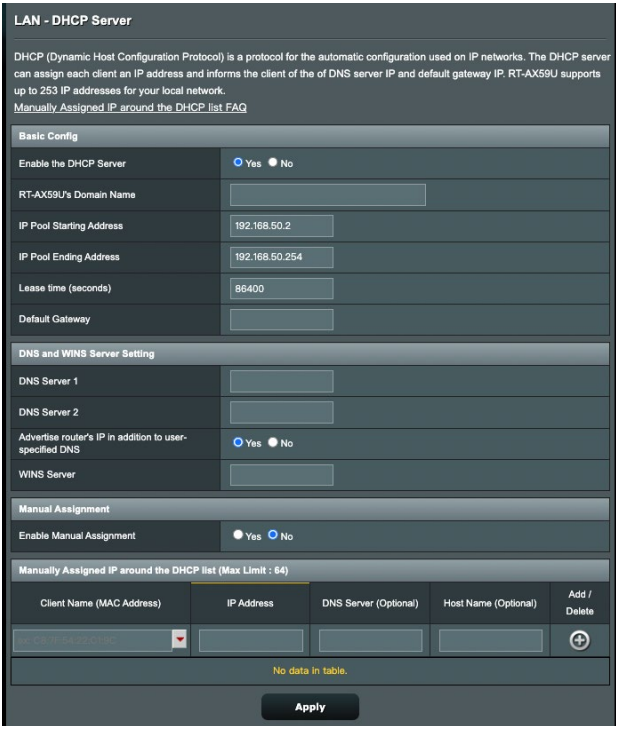
NOTE:

- Comenzile pentru ştergerea modulelor cookie şi a fişierelor diferă în funcție de browserul Web.
- Dezactivați setările de server proxy, revocați conexiunea pe linie comutată şi configurați setările TCP/IP pentru a obține automat adrese IP. Pentru mai multe detalii, consultați capitolul 1 din manualul utilizatorului.
- Asigurați-vă că utilizați cabluri Ethernet de tip CAT5e sau CAT6.

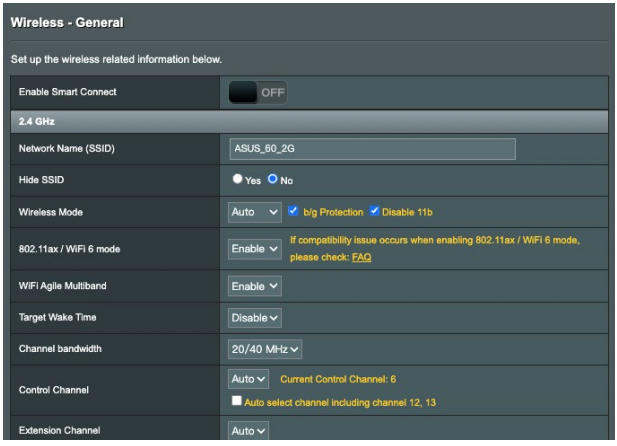
Clientul nu poate stabili o legătura wireless cu routerul.

NOTĂ: Dacă aveți probleme la conectarea la rețeaua în banda de frecvență de 5 GHz, asigurați-vă că dispozitivul wireless acceptă această bandă sau dispune de caracteristici de conectare în bandă dublă.

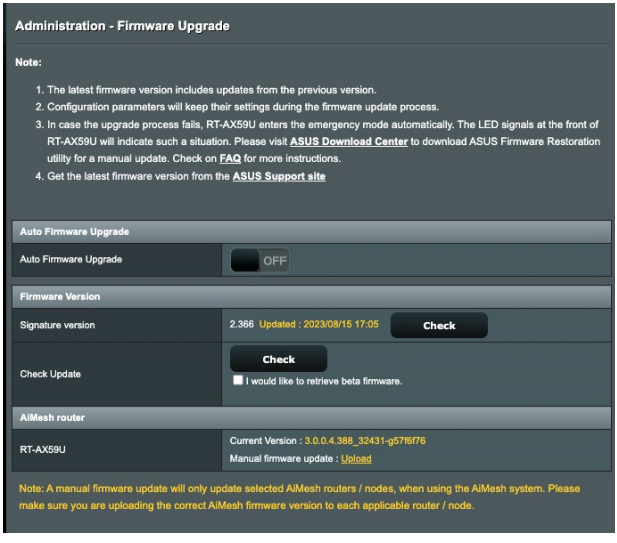
- **În afara razei:**
  - Puneți routerul mai aproape de clientul wireless.
  - Încercați să reglați antenele ruterului pentru a obține direcția de propagare optimă, după cum se descrie în secțiunea **1.4 Positioning your wireless router (Poziționarea router-ului wireless)**.
- **Serverul DHCP a fost dezactivat:**
  1. Lansați interfața de utilizare web. Mergeți la **General (Generalități)** > **Network Map (Hartă rețea)**> **Clients (Clienți)** și apoi căutați dispozitivul pe care doriți să îl conectați la ruter.
  2. Dacă nu puteți găsi dispozitivul în **Network Map (Hartă rețea)**, mergeți la **Advanced Settings (Setări avansate)** > **LAN** > **DHCP Server (Server DHCP)**, lista **Basic Config (Configurație de bază)**, selectați **Yes (Da)** pentru parametrul **Enable the DHCP Server (Activare server DHCP)**.



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



- Dacă utilizați un adaptor LAN wireless, verificați conformitatea canalului wireless în uz cu canalele disponibile în regiunea/țara dvs. Dacă nu există conformitate, ajustați canalul, lățimea de bandă a canalului şi modul wireless.
- Dacă în continuare nu vă puteți conecta wireless la ruter, puteți reseta ruterul la setările implicite din fabrică. În interfața de utilizare a ruterului, faceți clic pe **Administration (Administrare)** > **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)** şi faceți clic pe **Restore (Restaurare)**.



Internetul nu este accesibil.

- Verificați dacă ruterul dvs. se poate conecta la adresa IP WAN a furnizorului dvs. de servicii Internet. Pentru aceasta, lansați interfața de utilizare web şi mergeți la **General (Generalități)** > **Network Map (Hartă rețea)** şi verificați parametrul **Internet Status (Stare rețea)**.
- Dacă ruterul dvs. nu se poate conecta la adresa IP WAN a furnizorului dvs. de servicii Internet, încercați să reporniți rețeaua aşa cum se descrie în secțiunea **Restart your network in following sequence (Reporniți rețeaua în următoarea secvență)** sub **Basic Troubleshooting (Depanare de bază)**.

- Dispozitivul a fost blocat prin intermediul funcției Parental Control (Control parental). Mergeți la **General (Generalități)** > **Parental Controls (Control parental)** şi vedeți dacă dispozitivul se află în listă. Dacă dispozitivul apare sub **Client Name (Nume client)**, eliminați dispozitivul folosind butonul **Delete (Ştergere)** sau ajustați setările privind gestionarea timpului.
- Dacă în continuare nu puteți accesa Internetul, încercați să reporniți computerul şi să verificați adresa IP a rețelei şi adresa gateway-ului.
- Verificați indicatorii de stare de pe modemul ADSL şi ruterul wireless. Dacă LEDul WAN de pe ruterul wireless nu este aprins, verificați dacă ați conectat corect cablurile.

Ați uitat numele rețelei (SSID) sau parola rețelei.

- Configurați un nou SSID şi o nouă cheie de criptare prin intermediul unei rețele prin cablu (cablu Ethernet. Lansați interfața de utilizare web, mergeți la **Network Map (Hartă rețea)**, faceți clic pe pictograma ruterului, introduceți un nou SSID şi o nouă cheie de criptare şi apoi faceți clic pe **Apply (Aplicare)**.
- Resetați ruterul la setările implicite. Lansați interfața de utilizare web, mergeți la **Administration (Administrare)** > **Restore/ Save/Upload Setting (Setări restaurare/salvare/încărcare)** şi faceți clic pe **Restore (Restaurare)**. Contul şi parola de conectare implicite sunt ambele „admin”.

Cum să readuc sistemul la setările sale inițiale?

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

  Următoarele sunt setări inițiale de fabrică:

Nume utilizator:	admin
Parolă:	admin
Validează DHCP:	Da (când cablul WAN este conectat)
Adresă IP:	http://www.asusrouter.com (sau 192.168.50.1)
Nume domeniu:	(Gol)
Subnet Mask:	254.254.255.0
DNS Server 1:	192.168.50.1
DNS Server 2:	(Gol)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz):	ASUS_XX_5G

Upgradeul de firmware a eşuat.

Lansați modul de recuperare înainte de a utiliza utilitarul Firmware Restoration (Restaurare firmware). Consultați secțiunea **4.2 Firmware Restoration (Restaurare firmware)** pentru a afla cum să utilizați utilitarul Firmware Restoration (Restaurare firmware).

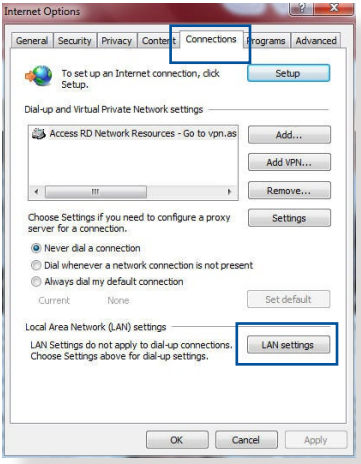
Nu se poate accesa interfața de utilizare web

Înainte de a configura ruterul fără fir, efectuați pașii descrişi în această secțiune pentru computerul gazdă şi clienții de rețea.

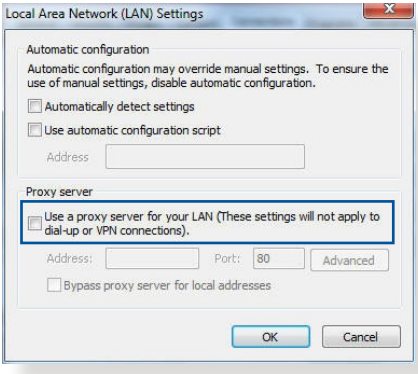
A. Dezactivați serverul proxy, dacă este activat.

Windows®

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

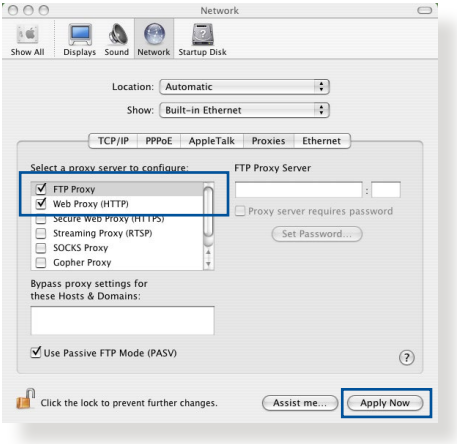


3. Din ecranul Local Area Network (LAN) Settings (Setări pentru rețeaua locală (LAN)), debifați opțiunea **Use a proxy server for your LAN (Utilizare server proxy pentru rețeaua locală)**.
4. Faceți clic pe **OK** când ați terminat.



MAC OS

1. În browserul Safari, faceți clic pe **Safari** > **Preferences (Preferințe)** > **Advanced (Complex)** > **Change Settings... (Modificare setări…).**
2. În ecranul Network (Rețea), deselectați **FTP Proxy (Server proxy FTP)** și **Web Proxy (HTTP) (Server proxy Web (HTTP))**.



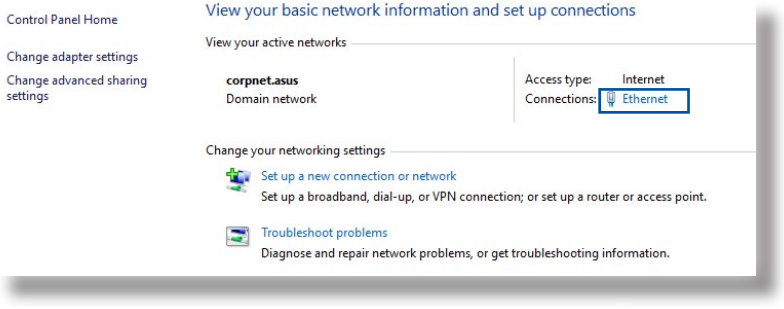
3. Faceți clic pe **Apply Now (Se aplică acum)** când ați terminat.

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

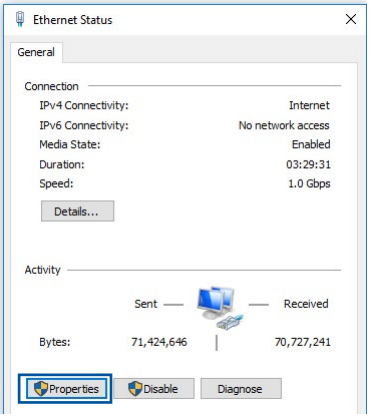
B. Configurați setările TCP/IP pentru obținerea automată a unei adrese IP.

Windows®

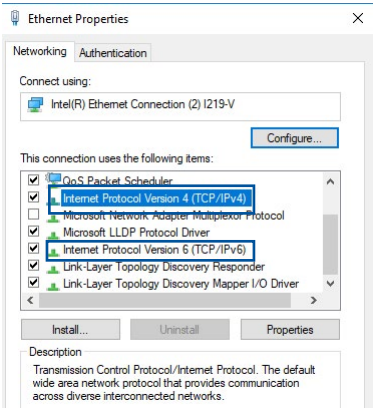
1. Faceți clic pe **Start (Pornire)** > **Control Panel (Panou de control)** > **Network and Internet (Rețea şi Internet)** > **Network and Sharing Center (Centru de rețea şi partajare)**, apoi faceți clic pe conexiunea de rețea pentru a afișa fereastra de stare.



2. Faceți clic pe **Properties (Proprietăți)** pentru a afișa fereastra Ethernet Properties (Proprietăți Ethernet).



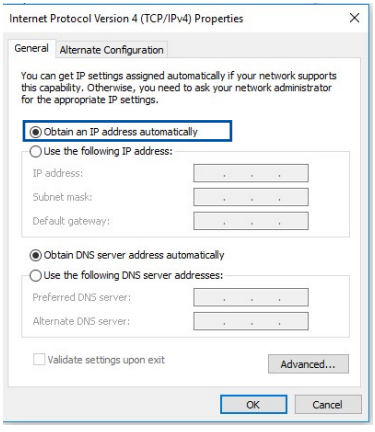
3. Selectați **Internet Protocol Version 4 (TCP/IPv4) (Protocol Internet versiunea 4 (TCP/IPv4))** sau **Internet Protocol Version 6 (TCP/IPv6) (Protocol Internet versiunea 6 (TCP/IPv6))**, apoi faceți clic pe **Properties (Proprietăți)**.



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

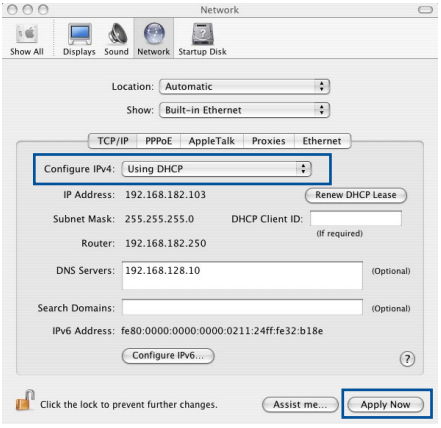
   Pentru a obține automat setările IP iPv6, bifați **Obtain an IPv6 address automatically (Se obține automat o adresă IPv6)**.

5. Faceți clic pe **OK** când ați terminat



MAC OS

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

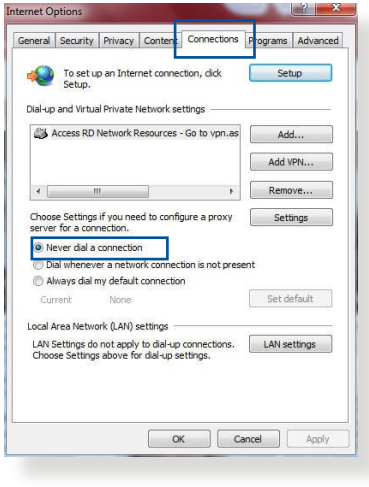


NOTĂ: Consultați caracteristica de ajutor şi asistență a sistemului de operare pentru detalii despre configurarea setărilor TCP/IP ale computerului.

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

Windows®

1. Faceți clic pe **Start (Pornire)** > **Internet Explorer** pentru a lansa browserul web.
2. Faceți clic pe **Tools (Instrumente)** > **Internet options (Opțiuni Internet)** > **Connections (Conexiuni)**.
3. Bifați **Never dial a connection (Nu se apelează niciodată o conexiune)**.
4. Faceți clic pe **OK** când ați terminat.



NOTĂ: Consultați 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

Service și Asistență

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