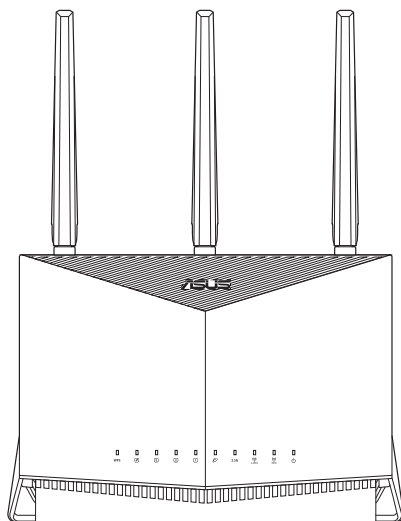


# Ghidul utilizatorului

## RT-AX86U PRO

Ruter Gigabit Wireless-AX5700 de  
bandă duală



**ASUS**  
IN SEARCH OF INCREDIBLE

RO22539

Prima ediție

Octombrie 2023

**Copyright © 2023 ASUSTeK COMPUTER INC. Toate drepturile rezervate.**

Nicio parte a acestui manual, inclusiv produsele și software-ul descris în el, poate fi reprodusă, transmisă, transcrisă, stocată într-un sistem de căutare sau tradus în altă limbă, sub orice formă sau prin orice mijloace, cu excepția documentației păstrate de cumpărător pentru backup, fără permisiunea expresă scrisă a ASUSTeK COMPUTER INC. ("ASUS").

Garanția produsului sau service-ul vor fi extinse dacă: (1) produsul este reparat, modificat sau schimbat, în așa fel încât repararea, modificarea sau schimbarea să fie autorizată de ASUS, sau (2) numărul de serie al produsului este deteriorat sau lipsește.

ASUS OFERĂ ACEST MANUAL "CA ATARE", FĂRĂ NICIO GARANȚIE, FIE EA EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, ÎNSĂ NELIMITÂNDU-SE LA GARANȚIILE IMPLICITE SAU CONDIȚIILE DE VALDABILITATE SAU POTRIVIRE ÎNTR-UN SCOP ANUME. ÎN NICIO EVENTUALITATE ASUS, DIRECTORII, FUNCȚIONARII SAU AGENȚII SĂI SUNT RĂSUNZĂTORI PENTRU ORICE PAGUBE INDIRECTE, SPECIALE, ACCIDENTALE (INCLUSIV PIERDERE PROFITURI, PIERDEREA AFACERII, PIERDEREA FOLOSINȚEI SAU A DATELOR, ÎNTRERUPEREA AFACERII ETC.), CHIAR DACĂ ASUS A FOST ÎN PREALABIL SFĂTUIT DE POSIBILITATEA UNOR ASEMENEA DAUNE PROVENITE DIN ORICE EROARE SAU DEFECT DIN ACEST MANUAL AU PRODUS.

SPECIFICAȚIILE ȘI INFORMAȚIILE PREZENTATE ÎN ACEST MANUAL SUNT FURNIZARE EXCLUSIV CU TITLU INFORMATIV, ȘI POT FI MODIFICATE ORICÂND, FĂRĂ PREAVIZ, ACEASTA NEINTRÂND ÎN OBLIGAȚIILE ASUS. ASUS NU ÎȘI ASUMĂ NICIO RESPONSABILITATE SAU OBLIGAȚIE PENTRU ORICE ERORI SAU INEXACTITĂȚI CE POT APĂREA ÎN ACEST MANUAL, INCLUSIV PRODUSELE ȘI SOFTWARE-UL DESCRISE ÎN EL.

Numele produselor și companiilor din acest manual pot sau nu pot fi mărci înregistrate sau drepturi de autor ale companiilor respective, și sunt folosite doar pentru identificare sau explicații și în beneficiul proprietarilor lor, fără intenție de a încălca legea.

# Sumar

## 1 Cum să vă cunoașteți routerul

1.1	Bine ați venit! .....	6
1.2	Conținutul pachetului .....	6
1.3	Ruter wireless .....	7
1.4	Poziționarea router-ului wireless.....	9
1.5	Cerințe pentru configurare.....	10

## 2 Inițializarea

2.1	Configurarea ruterului.....	11
	A. Conexiune cu fir.....	11
	B. Conexiune fără fir.....	12
2.2	Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată.....	14
2.3	Conectarea la rețeaua dvs. wireless.....	17

## 3 Configurarea setărilor generale și setărilor avansate

3.1	Conectarea la interfața Web GUI .....	18
	3.1.1 Configurarea setărilor de securitate pentru rețeaua wireless .....	20
	3.1.2 Administrarea clienților din rețea.....	21
	3.1.3 Monitorizarea dispozitivului USB .....	22
3.2	Adaptive QoS (QoS adaptiv).....	25
	3.2.1 Gestionarea lățimii de bandă pentru funcția QoS (Calitatea serviciului).....	25
3.3	Administration (Administrare).....	28
	3.3.1 Operation mode (Mod de funcționare) .....	28
	3.3.2 System (Sistem).....	29
	3.3.3 Actualizarea softului integrat .....	30
	3.3.4 Refacerea/Salvarea/Încărcarea setărilor.....	30
3.4	AiCloud 2.0 .....	31
	3.4.1 Cloud Disk.....	32

# Sumar

3.4.2	Smart Access.....	33
3.4.3	AiCloud Sync.....	34
3.5	<b>AiProtection .....</b>	<b>35</b>
3.5.1	Funcția Network Protection (Protecție rețea) .....	35
3.5.2	Configurarea controlului parental .....	39
3.6	<b>Paravan de protecție.....</b>	<b>42</b>
3.6.1	Aspecte generale .....	42
3.6.2	URL Filter (Filtru URL) .....	43
3.6.3	Keyword filter (Filtru cuvinte cheie) .....	44
3.6.4	Network Services Filter (Filtru servicii rețea) .....	45
3.7	<b>Game (Joc).....</b>	<b>47</b>
3.7.1	Gear Accelerator (Accelerator de viteză) .....	47
3.7.2	Mobile Game Mode (Mod jocuri pe mobil) .....	48
3.7.3	Open NAT.....	49
3.8	<b>Rețelei de vizitatori.....</b>	<b>50</b>
3.9	<b>IPv6.....</b>	<b>52</b>
3.10	<b>LAN.....</b>	<b>53</b>
3.10.1	LAN IP .....	53
3.10.2	Serverului DHCP .....	54
3.10.3	Rută.....	56
3.10.4	IPTV.....	57
3.11	<b>System Log (Jurnal de sistem).....</b>	<b>58</b>
3.12	<b>Analizor de trafic .....</b>	<b>59</b>
3.13	<b>Aplicației USB .....</b>	<b>60</b>
3.13.1	Utilizarea AiDisk.....	61
3.13.2	Utilizarea centrului de servere.....	63
3.13.3	3G/4G .....	68
3.14	<b>WAN .....</b>	<b>70</b>
3.14.1	Conexiune la Internet.....	70
3.14.2	Dual WAN (WAN dual) .....	73
3.14.3	Triggering de port.....	74



# Sumar

3.14.4	Server virtual/Redirecționare porturi .....	76
3.14.5	DMZ.....	79
3.14.6	DDNS .....	80
3.14.7	NAT Passthrough (Trecere NAT).....	81
<b>3.15</b>	<b>Wireless.....</b>	<b>82</b>
3.15.1	Aspecte generale .....	82
3.15.2	WPS .....	85
3.15.3	Modul Punte .....	87
3.15.4	Wireless MAC Filter (Filtru MAC wireless) .....	89
3.15.5	Setarea RADIUS.....	90
3.15.6	Professional (Profesional).....	91
<b>4</b>	<b>Utilitarelor</b>	
4.1	Detectarea Dispozitivului.....	94
4.2	Restaurare firmware .....	95
4.3	Configurarea serverului de tipărire.....	97
4.3.1	Partajarea imprimante EZ ASUS.....	97
4.3.2	Utilizarea protocolului LPR pentru partajarea imprimantei.....	101
4.4	Download Master (Coordonator de descărcări).....	106
4.4.1	Configurarea setărilor de descărcare pentru Bit Torrent.....	107
4.4.2	Setări NZB .....	108
<b>5</b>	<b>Remediarea defecțiunilor</b>	
5.1	Depanarea de bază.....	109
5.2	Întrebări frecvente .....	112
	<b>Anexă</b>	
	Service și Asistență .....	130

# 1 Cum să vă cunoașteți routerul

## 1.1 Bine ați venit!

Vă mulțumim pentru achiziționarea unui ruter wireless ASUS, model RT-AX86U PRO!

Șasiul negru cu design superb, cu accente roșii inspirate de jocuri, acest ruter RT-AX86U PRO dispune de: o bandă duală de 2.4GHz și 5GHz pentru redarea în flux HD, server SMB, server UPnP AV și server FTP pentru partajare de fișiere 24 de ore/7 zile; capacitate de administrare a până la 300 000 de sesiuni; tehnologie de rețea Green de la ASUS, care asigură până la 70% dintre soluțiile de economisire a energiei.

## 1.2 Conținutul pachetului

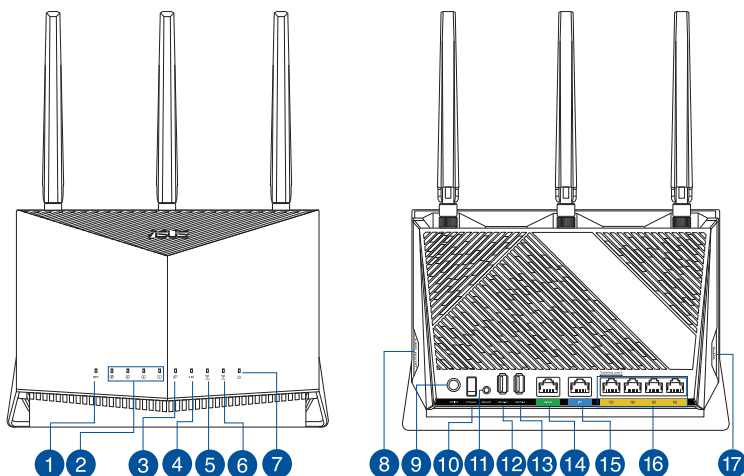
- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Router fără cablu RT-AX86U PRO | <input checked="" type="checkbox"/> Cablu RJ45            |
| <input checked="" type="checkbox"/> Adaptor de alimentare          | <input checked="" type="checkbox"/> Ghid rapid de pornire |
| <input checked="" type="checkbox"/> Card De Garanție               |   |

---

### NOTE:

- Dacă oricare dintre articole este deteriorat sau lipsește, contactați ASUS pentru informații și asistență tehnică. Consultați lista de linii telefonice de asistență ASUS de pe partea din spate a acestui manual de utilizare.
  - Păstrați ambalajul original în caz că veți avea nevoie de servicii ulterioare în garanție, cum ar fi reparare sau înlocuire.
-

## 1.3 Ruter wireless



- 
- 1 LED WPS**  
**Roșu:** Nu se procesează funcția WPS.  
**Aprins:** Se procesează funcția WPS.
- 
- 2 LED LAN 1~4**  
**Roșu:** Sistemul nu este alimentat sau nu există conexiune fizică.  
**Aprins:** Există conexiune fizică la o rețea locală (LAN).
- 
- 3 LED WAN (Internet)**  
**Stins:** Nicio IP sau nicio conexiune fizică.  
**Aprins:** Există conexiune fizică la o rețea de arie largă (WAN).
- 
- 4 2.5G LED**  
**Roșu:** Nu există conexiune pentru portul 2.5G.  
**Aprins:** Are conexiune fizică la portul 2.5G.
- 
- 5 2.4GHz LED**  
**Stins:** Nu există semnal de 2.4 GHz.  
**Aprins:** Sistemul fără fir este pregătit.  
**Intermitent:** Se transmit sau se primesc date printr-o conexiune fără fir.
- 
- 6 5GHz LED**  
**Stins:** Nu există semnal de 5 GHz.  
**Aprins:** Sistemul fără fir este pregătit.  
**Intermitent:** Se transmit sau se primesc date printr-o conexiune fără fir.
-

- 
- 7 LED alimentare**  
**Stins:** Fără alimentare.  
**Aprins:** Dispozitivul este pregătit.  
**Intermitent lent:** Mod de salvare.
- 
- 8 Buton LED activat/dezactivat**  
 Acest buton pornește/oprește indicatorii LED.
- 
- 9 Port alimentare (intrare c.c.)**  
 Inserați adaptorul de c.a. în acest port și conectați ruterul la o sursă de alimentare.
- 
- 10 Comutator de pornire**  
 Apăsați pe acest buton pentru a porni/a opri sistemul.
- 
- 11 Buton Reset (Reinițializare)**  
 Acest buton reinițializează sau restabilește sistemul la setările implicite din fabrică.
- 
- 12 Port USB 3.2 Gen 1**  
 Inserați dispozitive USB 3.2 Gen 1 cum ar fi hard diskuri USB sau unități flash USB în aceste porturi.  
 Inserați cablul USB al dispozitivului iPad în unul din aceste porturi pentru a vă încărca dispozitivul iPad.
- 
- 13 Port USB 2.0**  
 Inserați dispozitive USB 2.0 cum ar fi hard diskuri USB sau unități flash USB în aceste porturi.
- 
- 14 Port 2.5G**  
 Conectați un cablu de rețea la acest port pentru a obține viteze de 2 Gbps.
- 
- 15 Port WAN (Internet)**  
 Conectați un cablu de rețea la acest port pentru a stabili o conexiune WAN.
- 
- 16 Porturi LAN 1 ~ 4**  
 Conectați cabluri de rețea la aceste porturi pentru a stabili o conexiune LAN.
- 
- 17 Buton WPS**  
 Acest buton lansează Expertul WPS.
- 

## NOTE:

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

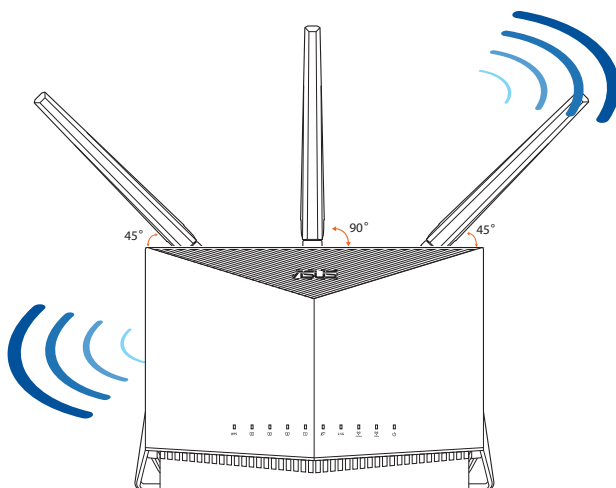
<b>Adaptor de alimentare c.c.</b>	leșire c.c.: +12 V cu curent max. de 3 A +19.5 V cu curent max. de 2.31 A		
<b>Temperatură în stare de funcționare</b>	0~40°C	Stocare	0~70°C
<b>Umiditate în stare de funcționare</b>	50~90%	Stocare	20~90%

---

## 1.4 Poziționarea router-ului wireless

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

- Așezați ruterul fără fir într-o zonă centrală pentru o acoperire fără fir maximă pentru dispozitivele de rețea.
- Feriți dispozitivul de obstacole de metal și 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, frigider și 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.
- Orientați cele 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/1000Base-TX)
- 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 duală, routerul dvs. wireless acceptă simultan semnale de rețea wireless 2,4 GHz și 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 același timp puteți reda în flux fișiere 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 depășească 100 de metri.

---

### IMPORTANT!

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

## 2 Inițializarea

### 2.1 Configurarea ruterului

#### IMPORTANT!

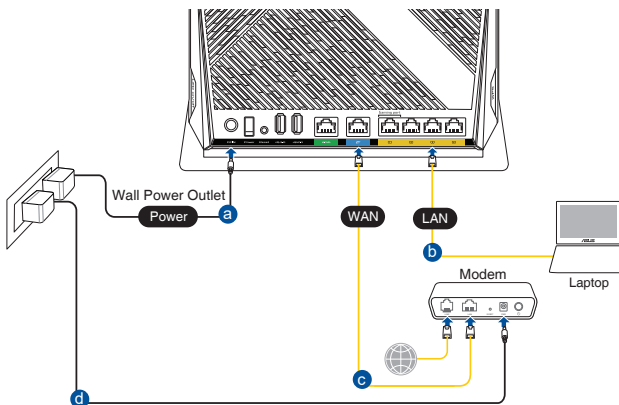
- Utilizați o conexiune cu fir pentru setarea ruterului wireless pentru a evita eventualele probleme de configurare.
- Înainte de a configura ruterul fără fir ASUS, efectuați următoarele acțiuni:
  - Dacă înlocuiți un ruter existent, deconectați-l de la rețea.
  - Deconectați cablurile/firele de la instalația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

#### A. Conexiune cu fir

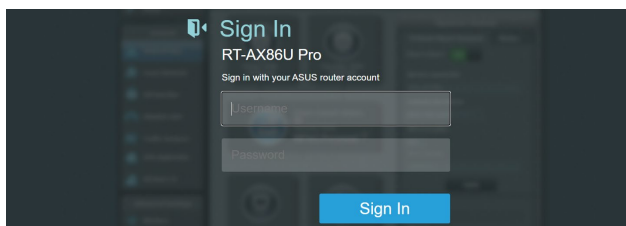
**NOTĂ:** Puteți folosi un cablu de conexiune directă sau un cablu crossover (inversor) pentru conexiunea cu fir.

#### Puteți configura ruterul prin conexiune cu fir sau wireless.

1. Conectați ruterul la o priză de curent și porniți-l. Conectați cablul de rețea de la computer la un port LAN de pe ruter.



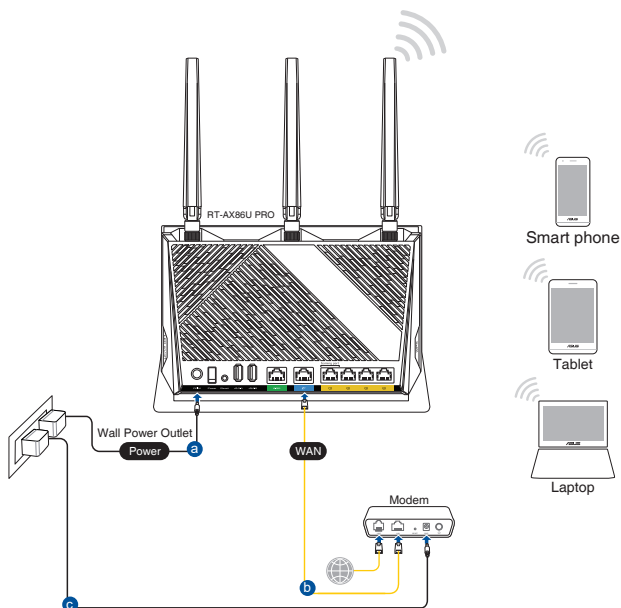
2. Interfața GUI web se lansează automat atunci când deschideți un browser web. Dacă nu se lansează automat, introduceți <http://www.asusrouter.com>.
3. Configurați o parolă pentru ruter în vederea prevenirii accesului neautorizat.



## B. Conexiune fără fir

**Puteți configura ruterul prin conexiune cu fir sau wireless.**

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





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

Nume rețea Wi-Fi (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 ruterul.
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 **3.1.1 Configurarea setărilor de securitate pentru rețea** din capitolul al treilea al acestui manual de utilizare.

**Login Information Setup**

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name	<input type="text" value="admin"/>
New Password	<input type="password"/>
Retype Password	<input type="password"/> <input type="checkbox"/> Show password

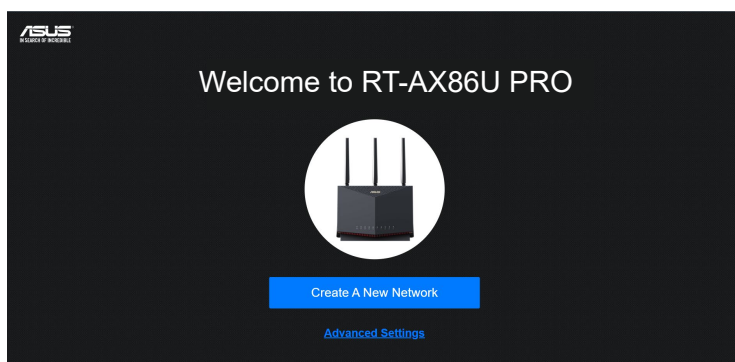
## 2.2 Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată

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 Reset (Reinițializare) 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.

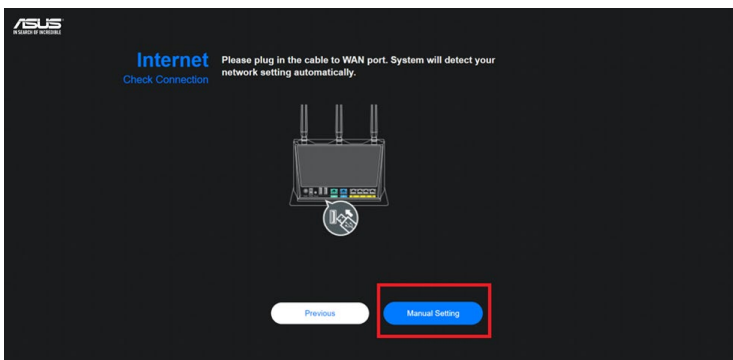


2. Ruterul wireless detectează automat dacă tipul conexiunii de la ISP este **Dynamic IP (IP dinamic)**, **PPPoE**, **PPTP**, și **L2TP**. Tastați informațiile utile pentru tipul de conexiune furnizat de ISP.

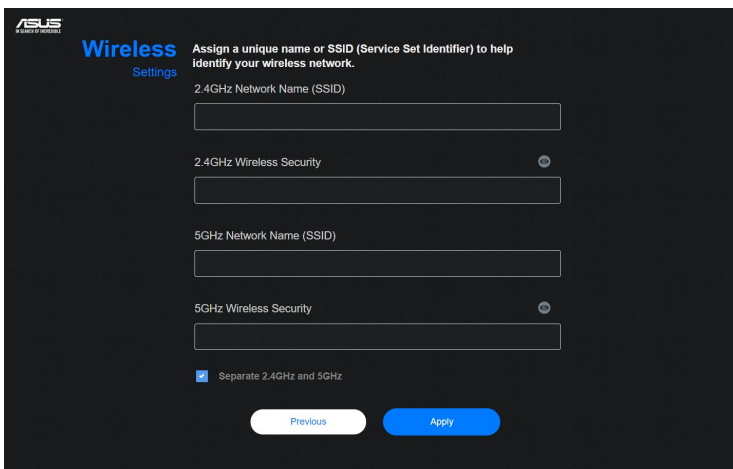
**IMPORTANT!** Obțineți informațiile necesare referitoare la tipul de conexiune la Internet de la ISP-ul dvs.

## 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 reușit să detecteze tipul de conexiune la Internet, faceți clic pe **Skip to manual setting (Salt la setare manuală)** (consultați captura de ecran de la pasul 1) și configurați manual setările de conexiune.



3. Atribuiți numele de rețea (SSID) și cheia de securitate pentru conexiunea fără fir de 2,4 GHz și 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.

ASUS  
WIRELESS

**Login**  
Username / Password  
Settings

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New password 🔒

Retype Password

Previous Next

**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. Așteptați până când computerul dvs. stabilește cu succes conexiunea la rețeaua wireless. Starea conexiunii este afișată și pictograma de rețea afișează 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 și setărilor avansate

### 3.1 Conectarea la interfața Web GUI

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

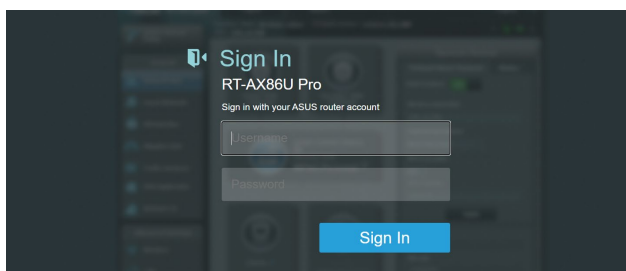
---

**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**) și 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.

## Butoane de comandă din partea superioară

The screenshot displays the ASUS RT-AX82U web interface. At the top, there are buttons for 'Logout' and 'Reboot'. Below these, the 'Operation Mode' is set to 'Wireless router', and the 'Firmware version' is '3.0.0.4.384.017'. The 'SSID' is 'RT-AX82U'. A 'Banner cu informații' (Information banner) is visible at the top right. The main content area is divided into several sections: 'Internet status' (Connected), 'Security level' (WPA2-Personal), 'System Status' (2.4GHz and 5GHz), 'Clients' (1), and 'USB 3.0' (No Device). A 'Panou de navigare' (Navigation panel) is located on the left side, containing various settings categories like 'Quick Internet Setup', 'General', 'Network Map', 'Guest Network', 'Adaptive QoS', 'Traffic Analyzer', 'Game', 'Open NAT', 'USB Application', 'AirCloud 2.0', 'Advanced Settings', 'Wireless', 'LAN', 'WAN', 'AirPlay & BT LE', 'IPv6', 'VPN', 'Firewall', 'Administration', 'System Log', and 'Network Tools'. The 'QIS' (Quick Internet Setup) button is highlighted in the top left corner.

\* Imaginea este doar pentru referință.

**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).

### 3.1.1 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:

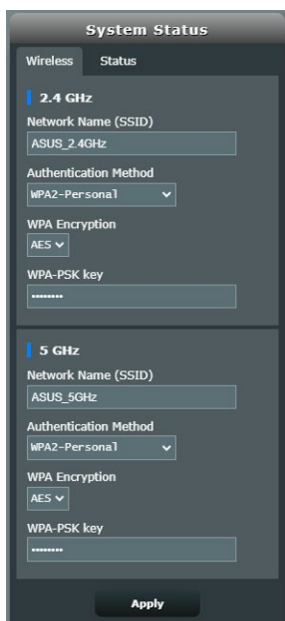
1. Din panoul de navigare, mergeți la **General > Network Map (Hartă rețea)**.
2. Din ecranul Network Map (Hartă rețea) selectați pictograma **System Status (Stare Sistem)** pentru afișarea setărilor de securitate wireless, cum sunt de exemplu SSID, nivel de securitate și setările de criptare.

---

**NOTĂ:** Puteți configura setări diferite de securitate wireless pentru benzile 2.4 GHz și 5 GHz.

---

#### Setări de securitate pentru banda 2.4 GHz / 5 GHz



3. În câmpul **Network Name (SSID) (Nume rețea (SSID))** tastați un nume unic pentru rețeaua dvs. wireless.



- Din lista verticală **WEP Encryption (Criptare WEP)** selectați metoda de criptare pentru rețeaua dvs. wireless.

**IMPORTANT!** Standardul IEEE 802.11n/ac/ax interzice utilizarea unei rate mari de transfer cu WEP sau WPA-TKP ca și 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.

- Tastați cheia de acces de securitate.
- Faceți clic pe **Apply (Aplicare)** după ce ați terminat.

### 3.1.2 Administrarea clienților din rețea



**Pentru a administra clienții din rețea:**

- Din panoul de navigare, mergeți la **General > Network Map (Hartă rețea)**.
- Din ecranul Network Map (Hartă rețea), selectați pictograma **Client status (Stare client)** pentru afișarea informațiilor referitoare la clienții de rețea.
- Pentru a bloca accesul unui client la rețea, selectați clientul și apoi faceți clic pe **block (blocare)**.

### 3.1.3 Monitorizarea dispozitivului USB

Router-ul wireless ASUS oferă două porturi USB pentru conectarea dispozitivelor USB sau a imprimantelor USB, pentru a vă permite să partajați fișiere și imprimante cu clienții din rețeaua dvs.



\* Imaginea este doar pentru referință.

**NOTĂ:** 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 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>

---

**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 2.0. Pentru mai multe detalii, consultați secțiunile **3.13 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 > 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:**

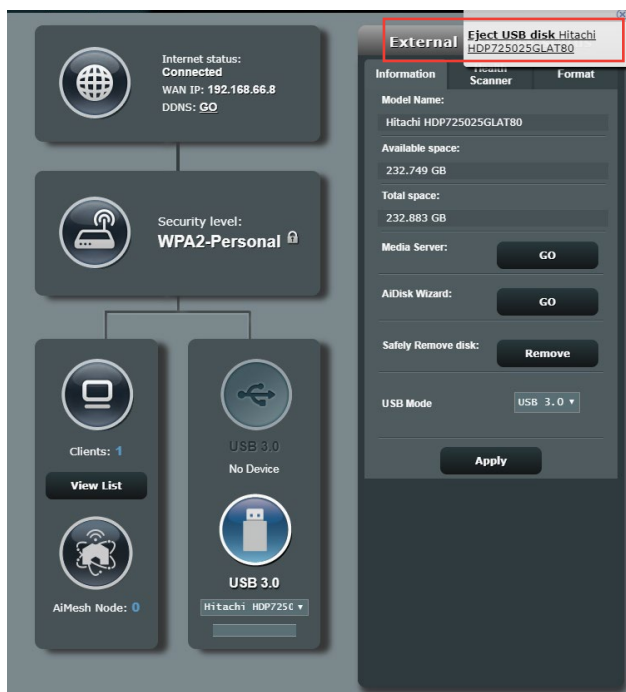
- Pentru mai multe detalii, consultați secțiunea **3.13.2 Using Servers Center (Utilizarea centrului de servere)** din acest manual de utilizare.
  - Ruterul fără fir funcționează cu majoritatea unităților de hard disk/discurilor flash USB (dimensiune de până la 2 TO) și acceptă acces de citire-scriere pentru FAT16, FAT32, EXT2, EXT3 și NTFS.
-

## 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 > 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)**.

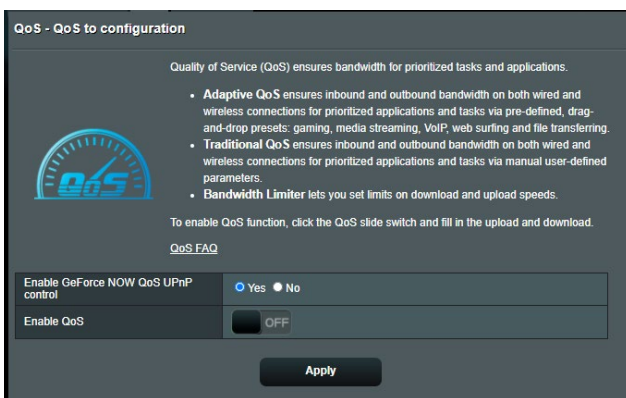


\* Imaginea este doar pentru referință.

## 3.2 Adaptive QoS (QoS adaptiv)

### 3.2.1 Gestionarea lățimii de bandă pentru funcția QoS (Calitatea serviciului)

Funcția QoS (Quality of Service – Calitatea serviciului) vă permite să setați prioritatea de lățime de bandă și să gestionați traficul în rețea.



**Pentru a seta prioritatea lățimii de bandă:**

1. Din panoul de navigare, mergeți la **General > Adaptive QoS (QoS adaptiv) > QoS**.
2. Faceți clic pe **ON (ACTIVARE)** pentru a activa regula implicită și completați câmpurile pentru lățimea de bandă de descărcare și încărcare.

---

**NOTĂ:** Obțineți informațiile pentru lățimea de bandă de la furnizorul de servicii Internet.

---

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

---

**NOTĂ:** Lista cu reguli specificate de utilizatori face parte din setările avansate. Dacă doriți să prioritizați anumite aplicații și servicii de rețea, selectați **User-defined QoS rules (Reguli QoS definite de utilizator)** sau **User-defined Priority (Prioritate definită de utilizator)** din lista verticală aflată în colțul din dreapta sus.

---

4. În pagina **user-defined QoS rules (Reguli QoS definite de utilizator)** există patru tipuri implicite de servicii online – navigare web, HTTPS și transferuri de fișiere. Selectați serviciul preferat, completați cu valori parametrul **Source IP or MAC (IP sau MAC sursă)**, **Destination Port (Port destinație)**, **Protocol, Transferred (Transferat)** și **Priority (Prioritate)**, apoi faceți clic pe **Apply (Aplicare)**. Informațiile vor fi configurate în ecranul cu reguli QoS.
- 

**NOTE:**

- Pentru a completa cu valori adresa IP sau MAC sursă, puteți:
    - a) Să introduceți o adresă IP specifică, precum „192.168.122.1”.
    - b) Să introduceți adrese IP din cadrul aceleiași sub-rețele sau din cadrul aceleiași sector IP, precum „192.168.123.\*” sau „192.168.\*”.
    - c) Să introduceți toate adresele IP ca „\*.\*.\*” sau să lăsați câmpul necompletat.
    - d) Formatul adreselor MAC este reprezentat de șase grupuri de câte două caractere hexazecimale, separate prin două puncte (:), în ordinea transmiterii (de exemplu, 12:34:56:aa:bc:ef)
  - Pentru intervalul de porturi sursă sau destinație, puteți:
    - a) Să introduceți un port specific, precum „95”.
    - b) Să introduceți porturi din cadrul unui interval, precum „103:315” sau „>100” sau „<65535”.
  - Coloana **Transferred (Transferat)** conține informații despre traficul de încărcare și descărcare (traficul de rețea de intrare și de ieșire) pentru o secțiune. În această coloană puteți seta limita pentru traficul de rețea (în KB) pentru un anumit serviciu, pentru a genera proprietăți specifice pentru serviciul atribuit unui anumit port. De exemplu, dacă doi clienți de rețea, PC 1 și PC 2, accesează concomitent Internetul (setat la portul 80), dar PC 1 depășește limita pentru traficul de rețea ca urmare a unor sarcini de descărcare, PC 1 va avea o prioritate mai redusă. Dacă nu doriți să introduceți limita pentru traficul de rețea, nu completați câmpul.
-

5. În pagina **User-defined Priority (Prioritate definită de utilizator)**, puteți prioritiza pe cinci niveluri aplicațiile de rețea sau dispozitivele din rețea, din lista verticală **user-defined QoS rules (Reguli QoS definite de utilizator)**. În funcție de nivelul priorității, puteți utiliza următoarele metode pentru a trimite pachete de date.
- Modificați ordinea pachetelor de rețea care sunt trimise către Internet.
  - Sub tabelul **Upload Bandwidth (Lățime de bandă pentru încărcare)**, setați **Minimum Reserved Bandwidth (Lățime de bandă minim rezervată)** și **Maximum Bandwidth Limit (Lățime de bandă maxim rezervată)** în cazul în care aveți mai multe aplicații de rețea cu diferite niveluri de prioritate. Procentajele indică ratele de încărcare disponibile pentru aplicațiile de rețea specificate.

---

**NOTE:**

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

- 
6. Setați pachetul cu cea mai mare prioritate. Pentru a asigura o experiență optimă a jocurilor online, puteți seta cea mai mare prioritate pentru pachetul ACK, SYN sau ICMP.

---

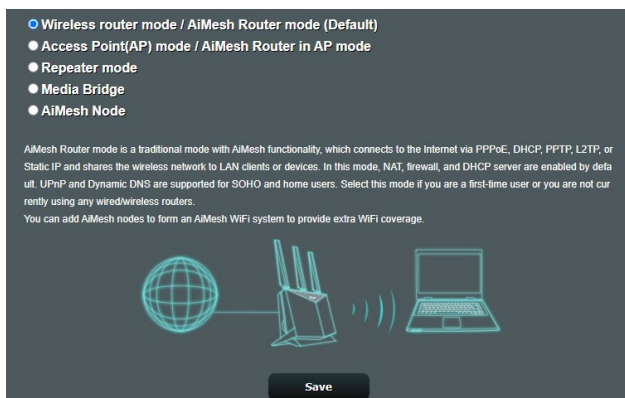
**NOTĂ:** Asigurați-vă că ați activat anterior opțiunea QoS și că ați configurat limite pentru ratele de încărcare și descărcare.

---

## 3.3 Administration (Administrazione)

### 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 (Administrazione) > Operation Mode (Mod de funcționare)**.
2. Selectați oricare dintre aceste moduri de funcționare:
  - **Mod ruter wireless (implicit):** În modul ruter wireless, ruterul wireless se conectează la Internet și furnizează acces la Internet dispozitivelor disponibile din propria rețea locală.
  - **Mod punct de acces:** În acest mod, ruterul creează o rețea wireless nouă pe baza unei rețele existente.
  - **Mod repeter:** Acest mod transformă routerul într-un repeter fără fir pentru a extinde intervalul semnalului.
  - **Media Bridge (Punte media):** Modul Media Bridge (Punte media) asigură cea mai rapidă conexiune Wi-Fi pentru conectarea simultană a mai multor dispozitive media. Pentru a configura modul Media Bridge (Punte media), aveți nevoie de două RT-AX86U PRO: unul configurat ca stație media și celălalt ca router.
  - **Nod AiMesh:** Puteți seta RT-AX86U PRO ca nod AiMesh pentru a extinde o acoperire WiFi a routerelor AiMesh existente.



3. Faceți clic pe **Save (Salvare)**.

---

**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 și numele de conectare pentru ruterul wireless introducând un nume nou și o parolă nouă.
  - **Comportament buton WPS:** Butonul fizic WPS de pe routerul wireless poate fi utilizat pentru activarea funcției WPS.
  - **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.
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 **Firmware Version (Versiune firmware)**, faceți clic pe **Check (Verificare)** pentru a localiza fișierul descărcat.
3. Faceți click pe **Upload (Încărcare)**.

---

#### NOTE:

- Când procesul de actualizare este finalizat, așteptați un timp pentru ca sistemul să repornească.
- Dacă procesul de actualizare eșuează, routerul va intra automat în modul de urgență sau de defecțiune și 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 **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 setting (Salvați setarea)**, navigați la folderul în care intenționați să salvați fișierul și faceți clic pe **Save (Salvare)**.
  - Pentru a reface setarea sistemului anterior, click **Upload (Încărcare)** pentru a localiza fișierul sistemului pe care doriți să-l refaceți apoi faceți click pe **Deschidere**.

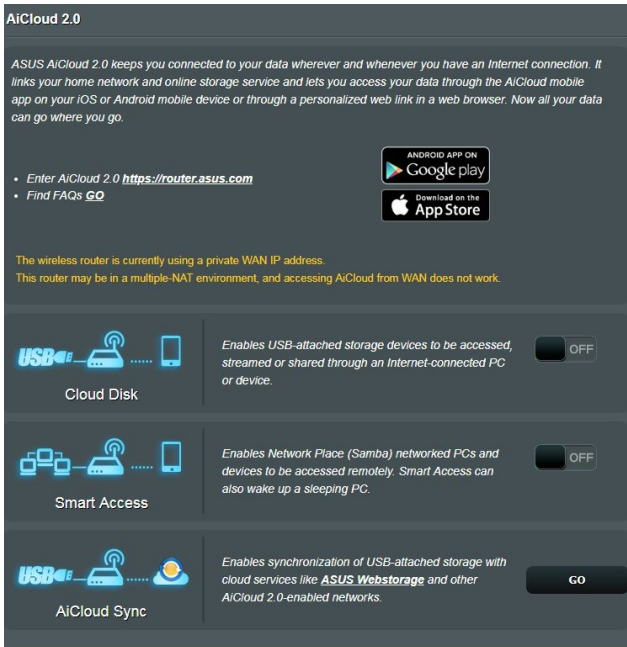
---

**IMPORTANT!** Dacă apar probleme, încărcați cea mai recentă versiune de firmware și 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.



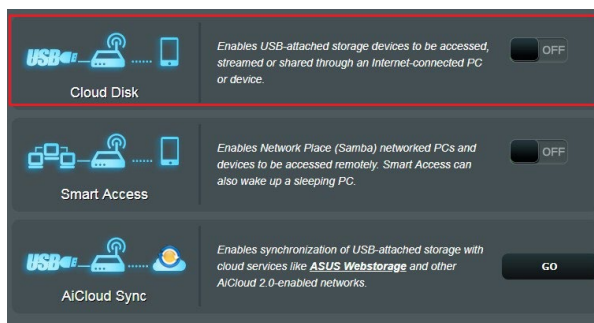
### Pentru a utiliza AiCloud 2.0:

1. Din Google Play Store sau Apple Store, descărcați și instalați aplicația ASUS AiCloud 2.0 pe dispozitivul dvs. inteligent.
2. Conectați dispozitivul inteligent la rețeaua dvs. Urmați instrucțiunile pentru finalizarea procesului de configurare AiCloud 2.0.

## 3.4.1 Cloud Disk

### Pentru a crea un disc cloud:

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



3. Mergeți la <http://www.asusrouter.com> și introduceți numele de cont și 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.

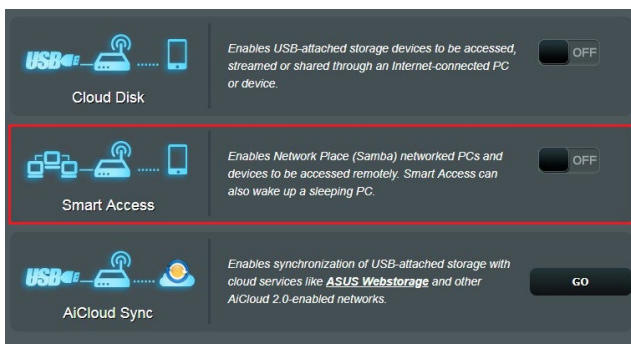
---

**NOTĂ:** Când accesați dispozitivele care sunt conectate la rețea, trebuie să introduceți manual numele de utilizator și parola dispozitivului, deoarece acestea nu sunt salvate de către AiCloud 2.0, din motive de securitate.

---

## 3.4.2 Smart Access

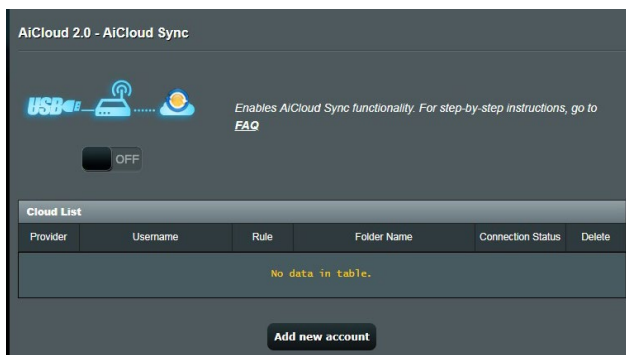
Funcția Smart Access vă permite să accesați cu ușurință rețeaua de acasă, prin intermediul numelui de domeniu al ruterului dvs.



### NOTE:

- Puteți crea un nume de domeniu pentru ruterul dvs. cu ajutorul ASUS DDNS. Pentru mai multe detalii, consultați secțiunea **3.14.6 DDNS**.
- În mod implicit, AiCloud oferă o conexiune HTTPS securizată. Introduceți adresa [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) pentru a utiliza aplicațiile Cloud Disk și Smart Access în cele mai sigure condiții.

### 3.4.3 AiCloud Sync



#### Pentru utilizarea caracteristicii AiCloud Sync:

1. Lansați AiCloud 2.0, faceți clic pe **AiCloud Sync**.
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 AiProtection

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

### 3.5.1 Funcția Network Protection (Protecție rețea)

Funcția Network Protection (Protecție rețea) previne abuzarea rețelei și securizează rețeaua împotriva accesului nedorit.

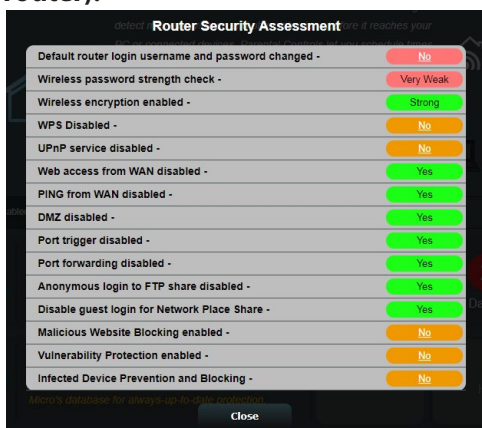


## Configurarea funcției Network Protection (Protecție rețea)

### Pentru a configura funcția Network Protection (Protecție rețea):

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

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



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

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

- a. Faceți clic pe un element.

**NOTĂ:** Atunci când faceți clic pe un element, utilitarul vă va redirecționa către pagina de configurare a elementului respectiv.

- b. Din pagina cu setări de securitate a elementului respectiv, configurați și efectuați modificările necesare și faceți clic pe **Apply (Se aplică)** când terminați;



- c. Reveniți la pagina **Router Security Assessment (Evaluare securitate router)** și faceți clic pe **Close (Închidere)** pentru a ieși din pagină;
5. Pentru a configura în mod automat setările de securitate, faceți clic pe **Secure Your Router (Securizați-vă routerul)**;
6. Când apare un mesaj, faceți clic pe **OK**.

### **Malicious Sites Blocking (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 > AiProtection**.
2. Din pagina principală **AiProtection**, faceți clic pe **Network Protection (Protecție rețea)**.
3. Din panoul **Malicious Sites Blocking (Blocare site-uri rău intenționate)**, faceți clic pe **ON (Activat)**.

### **Sistem de prevenire a intruziunii bilateral**

SPI (Sistem de prevenire a intruziunii) bilateral vă protejează routerul împotriva atacurilor din rețea blocând pachetele de date primite rău intenționate și detectând pachetele de date de ieșire suspecte.

---

**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 > AiProtection**.
2. Din pagina principală **AiProtection**, faceți clic pe **Network Protection (Protecție rețea)**.
3. Din panoul **Sistem de prevenire a intruziunii**, faceți clic pe **ON (Activat)**.

## **Infected Device Prevention and Blocking (Prevenire și 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 > AiProtection**.
2. Din pagina principală **AiProtection**, faceți clic pe **Network Protection (Protecție rețea)**.
3. Din panoul **Infected Device Prevention and Blocking (Prevenire și blocare dispozitiv infectat)**, faceți clic pe **ON (Activat)**.

### **Pentru a configura funcția Alert Preference (Preferință alerte):**

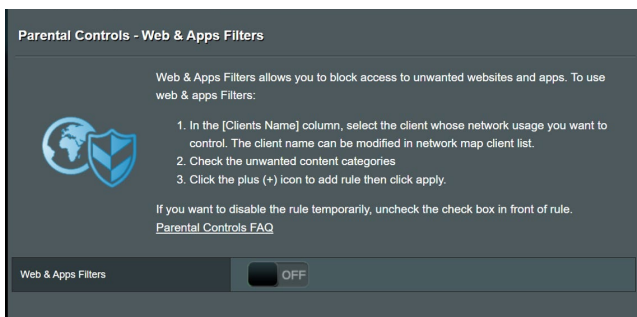
1. Din panoul **Infected Device Prevention and Blocking (Prevenire și blocare dispozitiv infectat)**, faceți clic pe **Alert Preference (Preferință alerte)**.
2. Selectați sau introduceți manual furnizorul de servicii e-mail, contul de e-mail și parola și apoi faceți clic pe **Apply (Se aplică)**.

## 3.5.2 Configurarea controlului parental

Opțiunea de control parental 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 accesa pagina principală Parental Controls (Controale parentale):

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




### Web & Apps Filters (Filtre aplicații și Web)

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


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

1. Din panoul de navigare, mergeți la **General > Parental Controls (Controale parentale)**.
2. Din panoul **Web & Apps Filters (Filtre aplicații și 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 și comunicare), P2P and File Transfer (P2P și transfer de fișiere) și Streaming and Entertainment (Redare în flux și divertisment)**
6. Faceți clic pe  pentru a adăuga profilul clientului;
7. Faceți clic pe **Apply (Se aplică)** pentru a salva setările.

Parental Controls - Web & Apps Filters

Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:




1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.  
[Parental Controls FAQ](#)

Web & Apps Filters  ON

Client List (Max Limit : 64)

<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	192.168.1.100	<input type="checkbox"/> <b>Adult</b> Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.	
		<input type="checkbox"/> <b>Instant Message and Communication</b> Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.	
		<input type="checkbox"/> <b>P2P and File Transfer</b> By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.	
		<input type="checkbox"/> <b>Streaming and Entertainment</b> By blocking streaming and entertainment services you can limit the time your children spend online.	
No data in table.			

**Apply**

## 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.

Parental Controls - Time Scheduling

By enabling Block All Devices, all of the connected devices will be blocked from Internet access.

Enable block all devices  OFF

This feature allows you to set up a scheduled time for specific devices' Internet access.

1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling  ON

System Time Thu, Sep 21 12:34:41 2023

Client List (Max Limit : 64)

Select	Client Name (MAC Address)	Time Management	Add / Delete
Time		-	+

No data in table.

Apply

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

1. Din panoul de navigare, mergeți la **General > 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 **Clients Name (Nume clienți)**, 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.

## 3.6 Paravan de protecție

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

---

**NOTĂ:** Caracteristică de firewall este activată implicit.

---

### 3.6.1 Aspecte generale

Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.  
[DoS Protection FAQ](#)

Enable Firewall  Yes  No

Enable DoS protection  Yes  No

Logged packets type

Respond ICMP Echo (ping) Request from WAN  Yes  No

Basic Config

Enable IPv4 inbound firewall rules  Yes  No

Inbound Firewall Rules (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>
No data in table.			

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified.  
(2001::1111:2222:3333:64 for example)

Basic Config

Enable IPv6 Firewall  Yes  No

Famous Server List

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>
No data in table.					

**Pentru a configura setările de bază pentru firewall:**

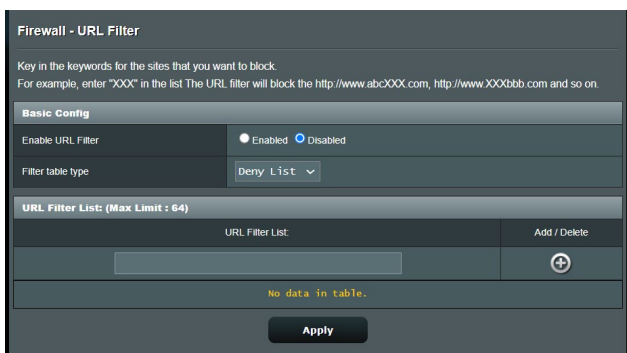
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Firewall > General**.
2. În câmpul **Enable Firewall (Activare firewall)**, selectați **Yes (Da)**.

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 și conexiunea WAN. Pentru parametrul Logged packets type (Tip pachete înregistrate), selectați **Dropped (Refuzate)**, **Accepted (Acceptate)** sau **Both (Ambele)**.
5. Faceți clic pe **Apply (Aplicare)**.

### 3.6.2 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, ștergeți memoria cache a serverului DNS înainte de a configura filtrul URL.

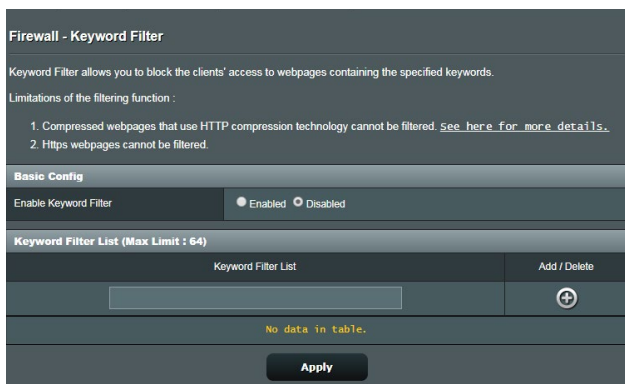


**Pentru configurarea unui filtru URL:**

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 și apoi faceți clic pe butonul .
4. Faceți clic pe **Apply (Aplicare)**.

### 3.6.3 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 și apoi faceți clic pe butonul **Add (Adăugare)**.
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, ștergeți 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.
-



### 3.6.4 Network Services Filter (Filtru serviciii rețea)

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

Firewall - Network Services Filter

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked). Leave the source IP field blank to apply this rule to all LAN devices.

**Deny List Duration :** During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

**Allow List Duration :** During the scheduled duration, clients in the Allow List can ONLY use the specified network

**NOTE :** If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

**Network Services Filter**

Enable Network Services Filter  Yes  No

Filter table type

Well-Known Applications

Date to Enable LAN to WAN Filter  Mon  Tue  Wed  Thu  Fri

Time of Day to Enable LAN to WAN Filter  :  -  :

Date to Enable LAN to WAN Filter  Sat  Sun

Time of Day to Enable LAN to WAN Filter  :  -  :


Filtered ICMP packet types

**Network Services Filter Table (Max Limit : 32)**

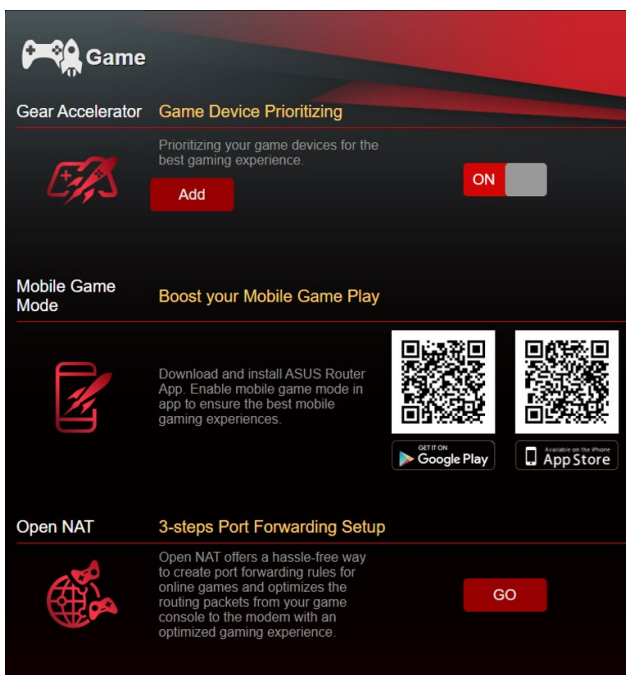
Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>

No data in table.

## 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 și 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 și protocolul. Faceți clic pe butonul .
6. Faceți clic pe **Apply (Aplicare)**.


## 3.7 Game (Joc)



### 3.7.1 Gear Accelerator (Accelerator de viteză)

Gear Accelerator (Accelerator de viteză) vă permite să acordați prioritate dispozitivelor de joc fără fir prin intermediul panoului de control online, pentru cea mai bună experiență de joc.

#### Pentru a configura Gear Accelerator (Accelerator de viteză)

1. Din panoul de navigare, mergeți la **General > Game (Joc)**.
2. Din **Gear Accelerator (Accelerator de viteză)**, faceți clic pe **ON (Activat)**.
3. După aplicarea setării, faceți clic pe **Add (Adăugare)** pentru a alege numele clientului.
4. Faceți clic pe  pentru a adăuga profilul clientului.
5. Faceți clic pe **Apply (Aplicare)** pentru a salva setările.

---


**NOTĂ:** Dacă doriți să ștergeți profilul clientului, faceți clic pe  .

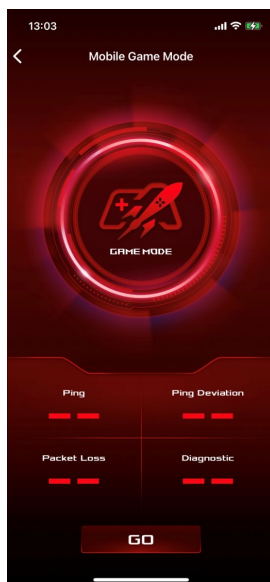
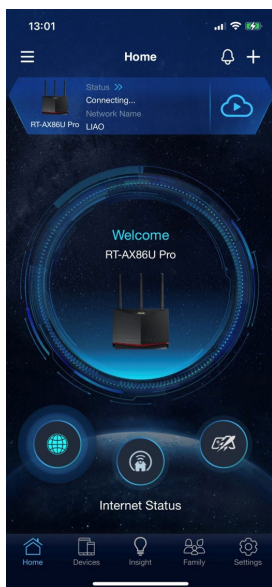
---

### 3.7.2 Mobile Game Mode (Mod jocuri pe mobil)

Descărcăți aplicația ASUS router pe telefonul dvs. mobil, activați modul de joc mobil cu un singur clic pentru a acorda prioritate telefonului mobil pentru o experiență de joc online mai bună.

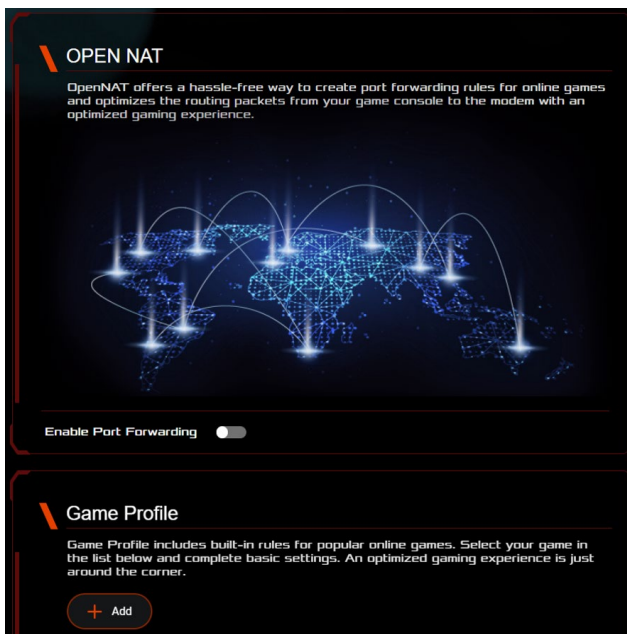
#### Pentru a configura modul de jocuri pe mobil

1. Descărcăți aplicația ASUS router, urmați pașii pentru a finaliza setările de rețea.
2. Din pagina principală, faceți clic pe .
3. Faceți clic pe **GO (Start)** pentru a configura modul de joc mobil pe telefonul dvs. mobil..



### 3.7.3 Open NAT

Open NAT oferă o modalitate fără probleme de a crea reguli de redirectionare a porturilor pentru jocurile online și optimizează pachetele de rutare de la consola de jocuri la modem, cu o experiență de joc optimizată.



#### Pentru a configura Open NAT

1. Din panoul de navigare, mergeți la **General > Game (Joc)**.
2. Din fila **Open NAT**, faceți clic pe **GO (Start)**.
3. Activare redirectionare porturi.
4. Din câmpul **Game Profile (Profil joc)**, faceți clic pe **Add (Adăugare)**.
5. Selectați jocul și completați setările de bază.
6. Faceți clic pe **OK**.

## 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.

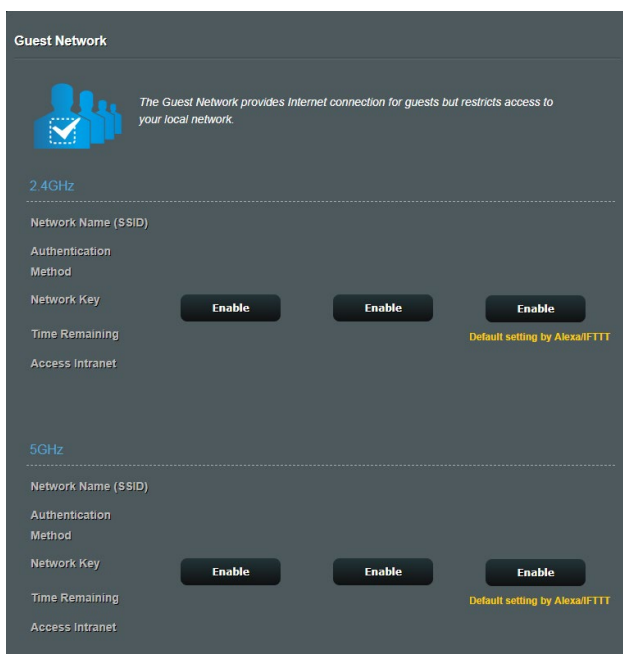
---

**NOTĂ:** Routerul RT-AX86U PRO acceptă până la șase identificatoare SSID (trei la 2,4 GHz și 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 configura opțiuni suplimentare, faceți clic pe **Modify (Modificare)**.

The screenshot displays the 'Guest Network' configuration page. At the top, there is a header 'Guest Network' and a descriptive text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' Below this, there are two sections for configuring networks: '2.4GHz' and '5GHz'. Each section contains a table of settings and two 'Enable' buttons. The 2.4GHz section has a 'Remove' button below the table. The 5GHz section also has a 'Remove' button below its table. The 'Enable' buttons are highlighted in yellow in the original image.

2.4GHz	
Network Name (SSID)	ASUS_2G_Guest
Authentication Method	Open System
Network Key	None
Time Remaining	Unlimited access
Access Intranet	off
<b>Enable</b> <b>Enable</b>	
<b>Remove</b>	

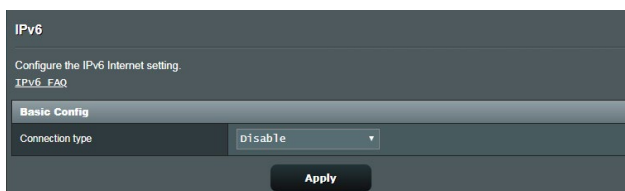
  

5GHz	
Network Name (SSID)	ASUS_5G_Guest
Authentication Method	Open System
Network Key	None
Time Remaining	Unlimited access
Access Intranet	off
<b>Enable</b> <b>Enable</b>	
<b>Remove</b>	

5. Faceți clic pe **Yes (Da)** în ecranul **Enable Guest Network (Activare rețea vizitatori)**.
6. Atribuiți un nume pentru rețeaua temporară în câmpul **Network Name (SSID) (Nume rețea (SSID))**.
7. Selectați o opțiune **Authentication Method (Metodă de autentificare)**.
8. Selectați o metodă pentru **Encryption (Criptare)**.
9. Specificați o valoare pentru **Access time (Timp de acces)** sau faceți clic pe **Limitless (Nelimitat)**.
10. Selectați **Disable (Dezactivare)** sau **Enable (Activare)** pe elementul **Access Intranet (Acces la Intranet)**.
11. 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 și 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

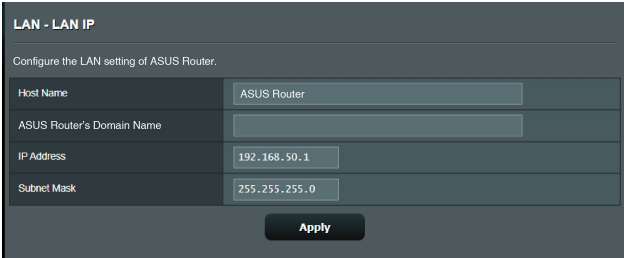
### 3.10.1 LAN IP

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.

---



LAN - LAN IP	
Configure the LAN setting of ASUS Router.	
Host Name	ASUS Router
ASUS Router's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0
<b>Apply</b>	

#### **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)** și **Subnet mask (Mască subrețea)**.
3. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

## 3.10.2 Serverului DHCP

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

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. RT-AX88U Pro supports up to 253 IP addresses for your local network.

[Manually Assigned IP around the DHCP list FAQ](#)

**Basic Config**

Enable the DHCP Server  Yes  No

RT-AX88U Pro's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

**DNS and WINS Server Setting**

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS  Yes  No

WINS Server

**Manual Assignment**

Enable Manual Assignment  Yes  No

**Manually Assigned IP around the DHCP list (Max Limit : 64)**

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>
No data in table.				

**Pentru configurarea serverului DHCP:**

1. Din panoul de navigare, bifați **Advanced Settings > LAN > DHCP Server**.
2. În câmpul **Enable the DHCP Server (Activați serverul DHCP)** bifați **Yes (Da)**.
3. În caseta **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 sfârșit)**, tastați adresa IP de sfârșit.
6. În câmpul **Lease Time (Perioadă de închiriere)** tastați data la care expiră adresele IP și ruterul wireless va aloca automat adrese IP noi pentru clienții rețelei.

---

**NOTE:**

- Vă recomandăm să utilizați un format de adresă IP de tip 192.168.50.xxx (unde xxx poate fi orice număr între 2 și 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 sfârșit pentru plaja respectivă.
- 
7. În secțiunea **DNS and Server Settings (Setări DNS și server)**, introduceți adresa IP pentru serverul DNS și 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.

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

**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 (Ștergere)**  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. Fila IPTV oferă setările necesare pentru configurarea serviciilor IPTV, VoIP, de distribuire multiplă și UDP. Contactați furnizorul de servicii Internet pentru a obține informații specifice cu privire la serviciile disponibile.

**LAN - IPTV**

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾

Special Applications	
Use DHCP routes	Microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
UDP Proxy (Udpxy)	0

**Apply**

## 3.11 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.

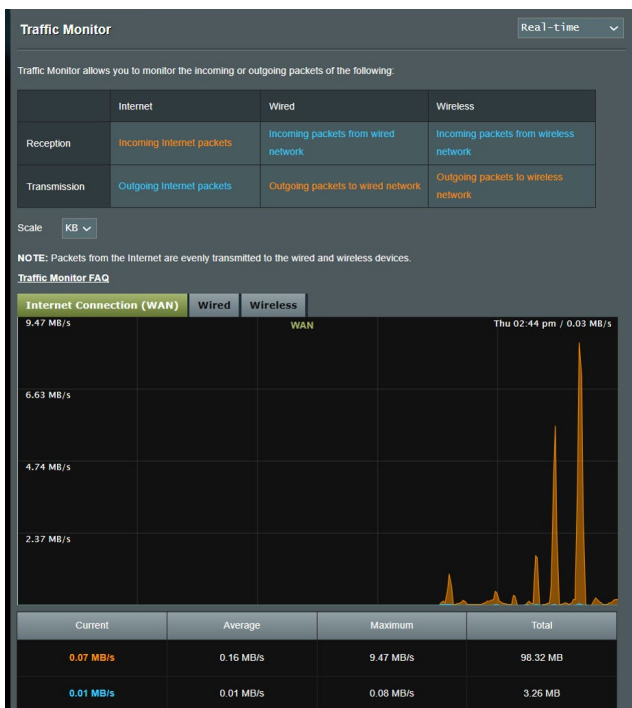
### Pentru vizualizarea jurnalului de sistem:

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 fișe:
  - Jurnal General (Generalități)
  - Jurnal wireless
  - Atribuirii DHCP
  - IPv6
  - Tabel direcționare
  - Redirecționare porturi
  - Conexiune

```
System Log - General Log
This page shows the detailed system's activities.
System Time Thu, Aug 23 07:15:34 2018
Uptime 0 days 1 hours 10 minute(s) 11 seconds
Remote Log Server [ ] Apply
Aug 23 06:51:04 miniupnpd[7139]: version 1.9 started
Aug 23 06:51:04 miniupnpd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 miniupnpd[7139]: Listening for NAT-FMP/PCP traffic on port 5351
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_patchkey != PATH_EX_INVAL
Aug 23 07:07:14 rc_service: httpd 1079:notify_rc start_multipath
Aug 23 07:07:14 miniupnpd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 nat: apply nat rules (/tmp/nat_rules.eth0.eth0)
Aug 23 07:07:14 miniupnpd[7688]: version 1.9 started
Aug 23 07:07:14 miniupnpd[7688]: HTTP listening on port 60855
Aug 23 07:07:14 miniupnpd[7688]: Listening for NAT-FMP/PCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 ntp: start NTP update
Aug 23 07:07:15 miniupnpd[7688]: shutting down MiniUPnPd
Aug 23 07:07:15 miniupnpd[7729]: version 1.9 started
Aug 23 07:07:15 miniupnpd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 miniupnpd[7729]: Listening for NAT-FMP/PCP traffic on port 5351
Clear Save
```

## 3.12 Analizor de trafic

Funcția de monitorizare a traficului vă permite să evaluați utilizarea lățimii de bandă și viteza conexiunilor la Internet sau a rețelelor cu fir sau wireless. Această funcție vă permite să monitorizați traficul din rețea în timp real sau zilnic. De asemenea, aveți posibilitatea de a afișa traficul de rețea din ultimele 24 de ore.

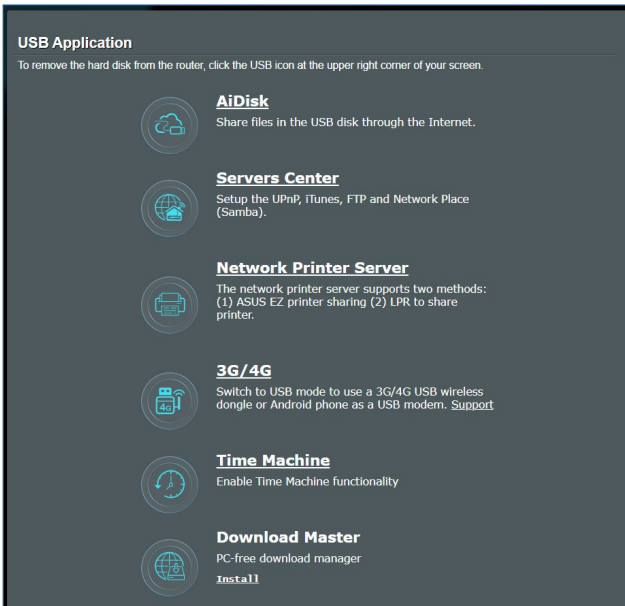


**NOTĂ:** Pachetele primite de la Internet sunt transmise în mod uniform către dispozitivele cu fir și wireless.

## 3.13 Aplicației USB

Funcția USB Extension (Extensie USB) oferă submeniurile AiDisk, Servers Center (Centru servere), Network Printer Server (Server de imprimantă în rețea) și 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 și 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 fișiere.



**USB Application**

To remove the hard disk from the router, click the USB icon at the upper right corner of your screen.

- AiDisk**  
Share files in the USB disk through the Internet.
- Servers Center**  
Setup the UPnP, iTunes, FTP and Network Place (Samba).
- Network Printer Server**  
The network printer server supports two methods:  
(1) ASUS EZ printer sharing (2) LPR to share printer.
- 3G/4G**  
Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem. [Support](#)
- Time Machine**  
Enable Time Machine functionality
- Download Master**  
PC-free download manager  
[Install](#)

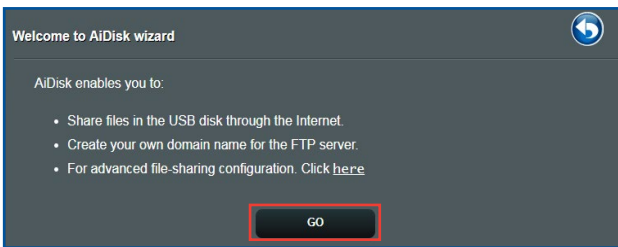


### 3.13.1 Utilizarea AiDisk

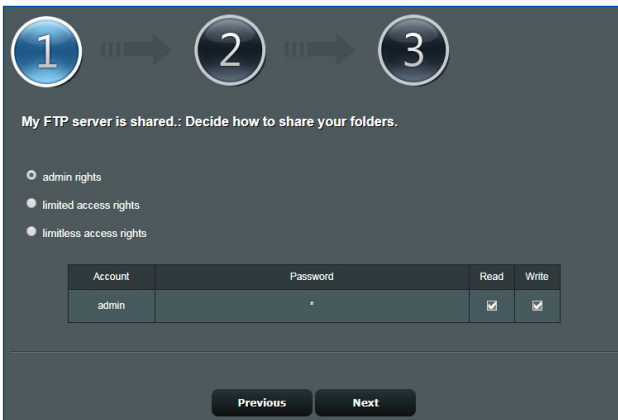
Funcția AiDisk vă permite să partajați fișiere de pe discul USB prin Internet. AiDisk vă va oferi asistență pentru configurarea parametrilor DDNS ASUS DDNS și ai serverului FTP.

#### Pentru a utiliza AiDisk:

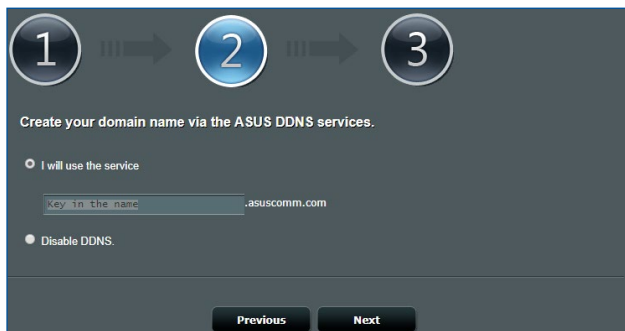
1. Din panoul de navigare, mergeți la **General (Generalități)** > **USB Application (Aplicație USB)**, apoi faceți clic pe pictograma **AiDisk**.
2. Din ecranul Welcome to AiDisk wizard (Bun venit la asistentul AiDisk), faceți clic pe **Go (Salt)**.



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.

### 3.13.2 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.

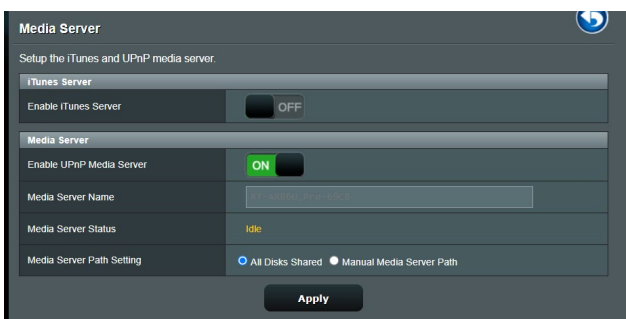
#### Utilizarea serverului media

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

---

**NOTĂ:** Înainte de a utiliza funcția de server media DLNA, conectați RT-AX86U PRO la rețeaua router.

---

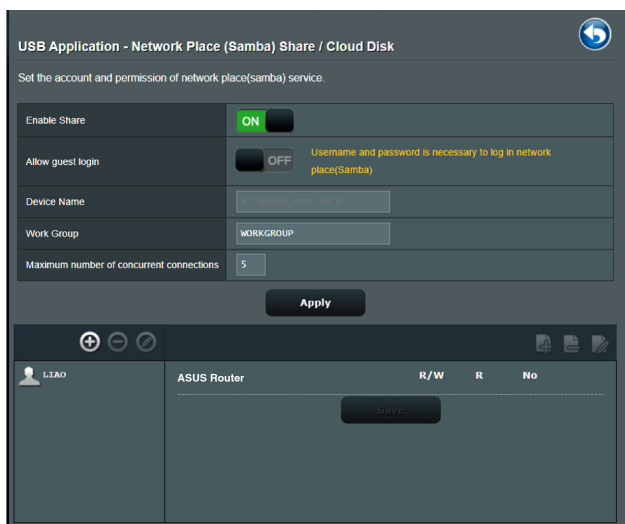


Pentru a lansa pagina de configurare a serverului media, mergeți la **General (Generalități) > USB Application > Servers Center (Centru servere) > Media Server (Server media)**. Consultați informațiile de mai jos pentru a obține descrieri ale câmpurilor:

- **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 și permisiunea pentru serviciul Samba.



### Pentru a utiliza partajarea Samba:

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

---

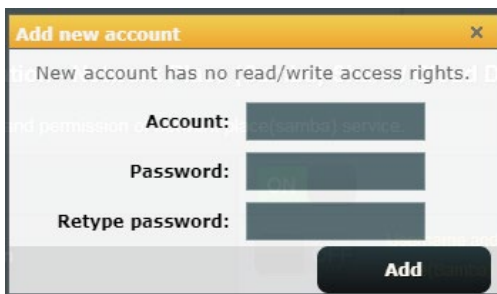
**NOTĂ:** Locația de rețea (Samba) Share (Partajare (Samba)) este activată în mod implicit.

---


2. Urmați pașii de mai jos pentru a adăuga, șterge 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)** și **Password (Parolă)**, introduceți numele și parola pentru clientul de rețea. Reintroduceți parola pentru confirmare. Faceți clic pe **Add (Adăugare)** pentru adăugarea contului în listă.

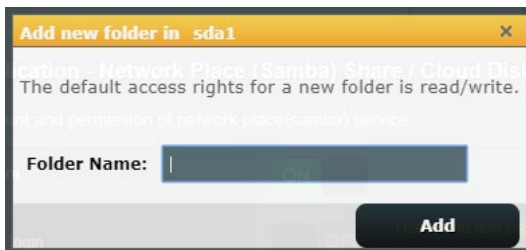


### Pentru a șterge un cont existent:

- Selecțați contul pe care doriți să-l ștergeți.
- Faceți clic pe .
- Când vi se solicită, faceți clic pe **Delete (Ștergere)** pentru a confirma ștergerea contului.

### Pentru a adăuga un folder:

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



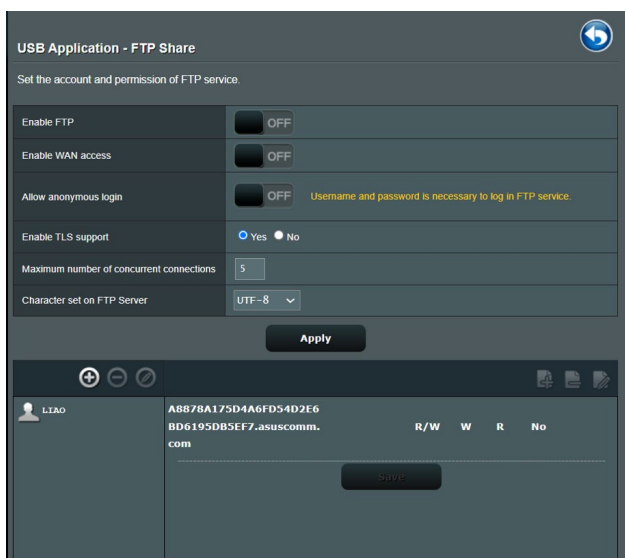
3. Selecțați drepturile de acces pe care doriți să le atribuiți pentru fiecare director în parte, astfel:
  - **R/W (C/S)**: Selecțați această opțiune pentru a atribui accesul de citire/scriere.
  - **R**: Selecțați această opțiune pentru a atribui acces numai pentru citire.
  - **No (Nu)**: Selecțați această opțiune dacă nu doriți să partajați un anumit folder de fișiere
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 fișiere de pe un disc USB cu alte dispozitive, prin intermediul rețelei locale sau al Internetului.

### IMPORTANT!

- Asigurați-vă că eliminați în siguranță discul USB. Eliminarea incorectă a discului USB poate să cauzeze coruperea datelor.
- Pentru a scoate în siguranță discul USB, consultați secțiunea **Safely removing the USB disk (Eliminarea în siguranță a discului USB)** sub **3.1.3 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 **3.13.1 Using AiDisk (Utilizarea AiDisk)**.

---

1. Din panoul de navigare, faceți clic pe **General > USB application (Aplicație USB) > Servers Center (Centru Servere) > 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. Faceți clic pe **Apply (Aplicare)** pentru a aplica modificările.
4. Pentru a accesa serverul FTP, tastați linkul ftp **ftp://<numegazdă>.asuscomm.com** și numele de utilizator și parola într-un browser de Web sau într-un utilitar terț FTP.

### 3.13.3 3G/4G

Modemurile 3G/4G prin USB pot fi conectate la dispozitivul RT-AX86U PRO pentru a permite accesul la Internet.

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

USB Modem / USB Tethering

Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem.

**Basic Config**

Enable USB Mode	<input checked="" type="checkbox"/> ON
Select USB Device	Auto
APN Configuration	Auto
Telecommunications Standards	WCDMA (UMTS) / LTE
APN Service(optional)	internet
Dial Number	*99#
Username	
Password	
Authentication	None
PIN code	
USB Adaptor	Auto
USB MTU	0

**Special Requirement from ISP**

Extend the TTL value	<input checked="" type="radio"/> Yes <input type="radio"/> No
Spoof LAN TTL value	<input checked="" type="radio"/> Yes <input type="radio"/> No



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

1. Din panoul de navigare, faceți clic pe **General > 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 și cod PIN:** Numărul de acces și 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 și 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.

---

## 3.14 WAN

### 3.14.1 Conexiune la Internet

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

#### WAN - Internet Connection

RT-AX86U Pro supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of RT-AX86U Pro.

Basic Config	
WAN Connection Type	Automatic IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP <small>UPnP_EAG</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). <a href="#">WAN Aggregation FAQ</a></small>

WAN DNS Setting	
DNS Server	Default status: Get the DNS IP from your ISP automatically. <small>Assign a DNS service to improve security, block advertisement and gain faster performance.</small> <span>Assign</span>
Forward local domain queries to upstream DNS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNS Rebind protection	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNSSEC support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

DHCP Option	
Class Identifier (Option 60)	
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID
Class Identifier (Option 60)	
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID

Account Settings	
Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

Special Requirement from ISP	
Host Name	
MAC Address	<span>MAC Clone</span>
DHCP query frequency	Aggressive Mode
Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

## 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 **fixed IP (IP fix)**. 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 - traducere 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 și 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 și 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 și transfer de fișiere 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 și servere web sau proxy. Spre deosebire de protocolul de direcționare a porturilor, care implică o configurare manuală a setărilor pentru porturi, UPnP configurează în mod automat ruterul să accepte conexiunile primite și să direcționeze solicitările către un anumit PC din rețeaua locală.

- **Enable WAN Aggregation (Activare agregare WAN):** Agregarea WAN combină două conexiuni de rețea pentru a crește viteza WAN până la 2 Gbps. Conectați router-ul.
- **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 și 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, 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 aceștia și 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 și 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.

### 3.14.2 Dual WAN (WAN dual)

WAN dual vă permite să selectați două conexiuni ISP la router, una WAN primară și una WAN secundară.

#### Pentru a configura WAN dual:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > WAN**.
2. Mergeți la câmpul **WAN**, selectați **ON (Activat)**.
3. Alegeți **WAN-ul principal** și **WAN-ul secundar**. Există opțiuni WAN, USB, Ethernet LAN și 2.5G WAN.
4. Alegeți **Fail Over** sau **Load Balance**.
5. Faceți clic pe **Apply (Aplicare)**.

**NOTE:** Explicații detaliate sunt disponibile pe site-ul de asistență pentru întrebări frecvente **ASUS** <https://www.asus.com/support/FAQ/1011719>

The screenshot shows the 'WAN - Dual WAN' configuration page. At the top, there is a title 'WAN - Dual WAN' and a paragraph of introductory text: 'RT-AX86U Pro provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)'. Below this is a link: 'To enable WAN Aggregation go to the [WAN-Internet Connection](#) page.'

The configuration is divided into two sections:

- Basic Config:**
  - 'Enable Dual WAN' is a toggle switch currently set to 'OFF'.
  - 'Primary WAN' is a dropdown menu currently set to '1G WAN'.
  - 'Auto USB Backup WAN' has radio buttons for 'Yes' (selected) and 'No'.
- Auto Network Detection:**
  - A note: 'Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.'
  - 'Detect Interval' is set to 'Every 3 seconds'.
  - 'Internet Connection Diagnosis' is set to 'When the current WAN fails 2 continuous times, it is deemed a disconnection.'
  - 'Network Monitoring' has checkboxes for 'DNS Query' and 'Ping', both of which are currently unchecked.

At the bottom of the form is an 'Apply' button.

### 3.14.3 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 ieșire pe un port specificat. Triggeringul de port este utilizat în următoarele situații:

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

WAN - Port Trigger

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.  
[Port\\_Trigger\\_FAQ](#)

**Basic Config**

Enable Port Trigger  Yes  No

Well-Known Applications

Trigger Port List ( Max Limit : 32 )

Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
No data in table					

#### Pentru a configura triggeringul de port:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > WAN > Port Trigger (Triggering de port)**.
2. Configurați următoarele setări: Când ați terminat, faceți clic pe **Apply (Aplicare)**.
  - **Activare triggering de port:** Selectați **Yes (Da)** pentru a activa triggeringul de port.
  - **Aplicații cunoscute:** Selectați jocurile și serviciile web populare pe care doriți să le adăugați în lista de triggering de port.
  - **Descriere:** Introduceți o scurtă denumire sau o descriere pentru serviciu.

- **Port declanșator:** Specificați un port care să declanșeze deschiderea portului de intrare.
- **Protocol:** Selectați protocolul, TCP sau UDP.
- **Port de intrare:** Specificați un port de intrare pentru a primi date transmise dinspre Internet.

---

**NOTE:**

- Când vă conectați la un server IRC, un PC client realizează o conexiune de ieșire folosind intervalul de porturi declanșatoare cuprins între 66660 și 70000. Serverul IRC răspunde prin verificarea numelui de utilizator și crearea unei noi conexiuni la PC-ul client, utilizând un port de intrare.
- Dacă opțiunea de triggering de port este dezactivată, ruterul anulează conexiunea deoarece nu poate stabili care PC solicită accesul la serverul IRC. Când opțiunea 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 cu siguranță momentul închiderii aplicației.
- Opțiunea de triggering de port permite unui singur client din rețea să utilizeze concomitent un anumit serviciu și un anumit port de intrare.
- Nu puteți utiliza aceeași aplicație pentru a declanșa un port pentru mai multe PC-uri în același timp. Ruterul va direcționa portul numai către ultimul computer, în vederea trimiterii de către acesta a unei solicitări/unui semnal de declanșare către ruter.

### 3.14.4 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.

**NOTĂ:** Când opțiunea de redirecționare a porturilor este activată, ruterul ASUS blochează traficul de intrare nesolicitat dinspre Internet și permite răspunsuri numai din partea solicitărilor de ieșire ale rețelei LAN. Clientul de rețea nu are acces direct la Internet, și vice versa.

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network. If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200-10300), the LAN IP address, and leave the Local Port blank.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with ASUS Server's web user interface.
- When you set 20.21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with ASUS Server's native FTP server.

Virtual\_Server / Port\_Forwarding\_Edit

**Basic Config**

Enable Port Forwarding  OFF

**Port Forwarding List (Max Limit : 64)**

Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
No data in table.							

[Add profile](#)

**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. Configurați următoarele setări: Când ați terminat, faceți clic pe **ON**.

- **Activare redirecționare porturi:** Porniți **ON** pentru a activa redirecționarea portului.
- **Listă servere cunoscute:** Stabiliți tipul de serviciu pe care doriți să îl accesați.
- **Listă jocuri cunoscute:** Element listează porturile necesare pentru ca jocurile online cunoscute să funcționeze corect.
- **Port server FTP:** Evitați atribuirea intervalului de porturi 20:21 pentru serverul FTP, deoarece acest lucru va duce la intrarea în conflict cu atribuirea nativă a ruterului în ceea ce privește serverul FTP.
- **Nume serviciu:** Introduceți numele serviciului.
- **Interval porturi:** Dacă doriți să specificați un interval de porturi pentru clienții din aceeași rețea, introduceți numele serviciului, intervalul de porturi (de exemplu, 10200:10300), adresa IP din LAN și lăsați necompletat parametrul Local Port (Port local). Parametrul Port Range (Interval porturi) acceptă diverse formate, precum interval de porturi (300:350), porturi individuale (566,789) sau modul Mix (Mixt) (1015:1024,3021).

---

**NOTE:**

- Când firewall-ul rețelei dvs. este dezactivat și dvs. setați valoarea 80 ca interval de porturi pentru serverul HTTP în configurația WAN, serverul HTTP/web va intra în conflict cu interfața de utilizare web a ruterului.
- O rețea folosește porturi pentru a realiza schimbul de date, fiecărui port fiindu-i atribuit un număr și o anumită sarcină. De exemplu, portul 80 este utilizat pentru HTTP. Un anumit port poate fi utilizat de către o singură aplicație sau de către un singur serviciu la un moment dat. Prin urmare, nu este posibil ca două PC-uri să acceseze date prin același port și în același timp. De exemplu, nu veți putea configura opțiunea Port Forwarding (Redirecționare porturi) pe portul 100 pentru două PC-uri în același timp.

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

---

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

---

- **Port local:** Introduceți un port specific pentru a primi pachetele redirectionate. Lăsați acest câmp necompletat dacă doriți ca pachetele primite să fie redirectionate către intervalul de porturi specificat.
- **Protocol:** Selectați protocolul. În cazul în care aveți dubii, selectați opțiunea **BOTH (Ambele)**.

### **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 redirectionarea porturilor este configurată cu succes, ar trebui să puteți accesa fișierele sau aplicațiile.

### **Diferențe între triggeringul de port și redirectionarea porturilor:**

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

### 3.14.5 DMZ

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

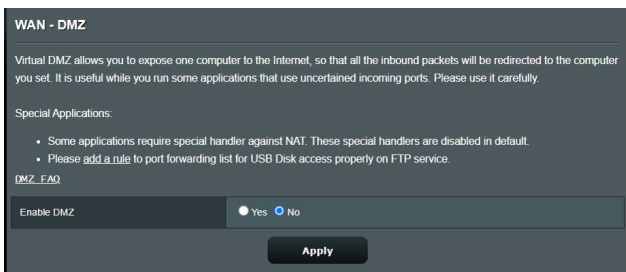
Traficul primit de pe Internet este de obicei direcționat către un anumit client numai dacă pentru rețeaua respectivă s-a configurat redirecționarea porturilor sau un declanșator de porturi. Într-o configurație de tip DMZ, un client din rețea primește toate pachetele de intrare.

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:** Deschiderea tuturor porturilor unui client face ca rețeaua să fie vulnerabilă la atacurile din exterior. Trebuie să fiți conștient 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 și care va fi expus pe Internet. Asigurați-vă că clientul de server are o adresă IP statică.

## Pentru eliminarea DMZ:

1. Ștergeți 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)**.

### 3.14.6 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.

**WAN - DDNS**

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.  
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.  
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.  
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.asus.com <input type="button" value="Deregister"/>
Host Name	A8878A175D4A6FD54D2E6BD6195D85EF7.asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input checked="" type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input type="radio"/> None

## 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 și nu prin intermediul adresei IP WAN.
  - **Nume server și 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) și înregistrați-vă online mai întâi. Completați numele de utilizator sau adresa de mail și 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.
- 

### 3.14.7 NAT Passthrough (Trecere NAT)

Parametrul NAT Passthrough (Trecere NAT) permite unei conexiuni aparținând unei rețele private virtuale să treacă prin ruter și să fie direcționată către clienții din rețea. Opțiunile PPTP Passthrough (Trecere PPTP), L2TP Passthrough (Trecere L2TP), IPsec Passthrough (Trecere IPsec) și 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)**.

WAN - NAT Passthrough	
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.	
PPTP Passthrough	Enable ▾
L2TP Passthrough	Enable ▾
IPSec Passthrough	Enable ▾
RTSP Passthrough	Enable ▾
H.323 Passthrough	Enable ▾
SIP Passthrough	Enable ▾
PPPoE Relay	Disable ▾
FTP ALG port	2021

Apply

## 3.15 Wireless

### 3.15.1 Aspecte generale

Fila General vă permite să configurați setările de bază pentru rețeaua wireless.

Wireless - General	
Set up the wireless related information below	
Enable Smart Connect	OFF
Band	2.4 GHz
Network Name (SSID)	LIAO
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> big Protection <input type="checkbox"/> Disable 11b
802.11ax / WIFI 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WIFI 6 mode, please check: FAQ</small>
WIFI Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto <small>Current Control Channel: 6</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** <span>Weak</span>
Group Key Rotation Interval	3600
<span>Apply</span>	

### Pentru configurarea setărilor de bază pentru rețeaua wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Wireless > General**.
2. Selectați banda de frecvență de 2.4 GHz sau de 5 GHz pentru rețeaua dvs. wireless.
3. 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 și 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 și de 5 GHz.

---

4. 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.
5. 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 și 802.11b să se conecteze la ruterul wireless.
  - **Moștenit:** Selectați **Legacy (Moștenit)** pentru a permite dispozitivelor 802.11b/g/n să se conecteze la ruterul wireless. Cu toate acestea, dispozitivele care acceptă în mod nativ standardul 802.11n vor beneficia de o viteză maximă de 54 Mbps.
  - **Doar N:** Selectați **N only (Doar N)** pentru a maximiza performanțele standardului wireless N. Această setare previne conectarea la ruterul wireless a dispozitivelor 802.11g și 802.11b.
6. Selectați oricare din aceste lățimi de bandă pentru a obține viteze de transmitere mai mari:
  - 40 MHz:** Selectați această lățime de bandă pentru a maximiza randamentul rețelei wireless.
  - 20 MHz (implicit):** Selectați această lățime de bandă dacă întâmpinați probleme cu conexiunea wireless.
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 oricare dintre aceste metode de autentificare:
  - **Sistem deschis:** Această opțiune nu oferă niciun tip de securitate.

- **Shared Key (Cheie partajată):** Trebuie să utilizați criptarea WEP și să introduceți cel puțin o cheie partajată.
- **WPA/WPA2 Personal/WPA Auto-Personal:** Această opțiune oferă o securitate puternică. Puteți utiliza WPA (cu TKIP), sau WPA2 (cu AES). Dacă selectați această opțiune, trebuie să utilizați criptarea TKIP + AES și să introduceți expresia de acces WPA (cheia de rețea).
- **WPA/WPA2 Enterprise/WPA Auto-Enterprise:** Această opțiune oferă o securitate foarte puternică. Opțiunea are integrat serverul EAP sau un server RADIUS extern, cu autentificare de fundal.

---

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

---

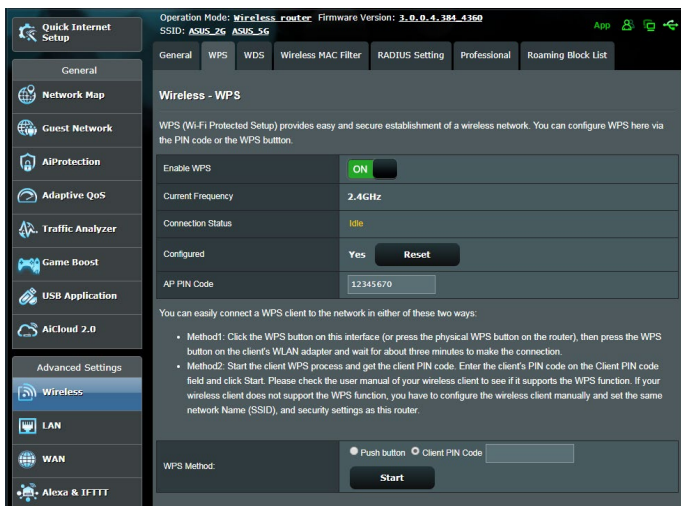
9. Selectați oricare din aceste opțiuni de criptare WEP (Wired Equivalent Privacy - confidențialitate echivalentă cu cea a rețelelor cu fir) pentru datele transmise prin rețeaua dvs. wireless:
  - **Off (Dezactivat):** Dezactivează criptarea WEP
  - **64-bit (64 de biți):** Activează o criptare WEP slabă
  - **128-bit (128 de biți):** Activează o criptare WEP îmbunătățită
10. Când ați terminat, faceți clic pe **Apply (Aplicare)**.



## 3.15.2 WPS

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

**NOTĂ:** Verificați dacă dispozitivele acceptă WPS.



### Pentru a activa WPS în rețeaua dvs. wireless:

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

---

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

---

4. În câmpul WPS Method (Metodă WPS), selectați **Push Button (Buton de comandă)** sau Cod **Client PIN (PIN client)**. Dacă selectați opțiunea **Push Button (Buton de comandă)**, mergeți la pasul 5. Dacă selectați opțiunea Cod **Client PIN (PIN client)**, mergeți la pasul 6.
5. Pentru a configura WPS folosind butonul WPS al ruterului, urmați pașii de mai jos:
  - a. Faceți clic pe **Start** sau apăsați butonul WPS care poate fi găsit în partea din spate 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 găsește niciun dispozitiv WPS, acesta va fi comutat în modul de așteptare.
6. Pentru a configura WPS folosind codul PIN al clientului, urmați pașii de mai jos:
  - a. Localizați codul PIN WPS în manualul de utilizare al dispozitivului dvs. wireless sau de pe dispozitivul însuși.
  - b. Introduceți codul PIN al clientului în caseta de text.
  - c. Faceți clic pe **Start** pentru a comuta ruterul wireless în modul de cercetare WPS. Indicatorii cu LED ai ruterului vor clipi rapid de trei ori până când configurarea WPS este finalizată.

### 3.15.3 Modul 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 și ca un repetator wireless, unde ruterul dvs. wireless ASUS comunică cu un alt punct de acces și cu alte dispozitive wireless.

**Wireless - Bridge**

Bridge (or named WDS - Wireless Distribution System) function allows your RT-AX88U Pro to connect to an access point wirelessly. WDS may also be considered a repeater mode.

**Note:**

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first. [Click Here](#) to modify. Please refer to this [FAQ](#) for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. [Click Here](#) to modify.

You are currently using the Auto channel. [Click Here](#) to modify.

**Basic Config**

2.4 GHz MAC	<input type="text" value="C8:7F:54:12:69:C8"/>
5 GHz MAC	<input type="text" value="C8:7F:54:12:69:CC"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

**Remote AP List (Max Limit : 4)**

Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="⊕"/>
No data in table.	

Pentru a configura puntea wireless:

1. Din panoul de navigare, mergeți la **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) și 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 câmpul **Control Channel (Canal control)**, selectați canalul operațional pentru puntea wireless. Selectați **Auto (Automat)** pentru a permite ruterului să selecteze automat canalul care are cele mai puține interferențe.

---

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

---

6. În lista cu puncte de acces la distanță, introduceți o adresă MAC și 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 același canal de control ca și ruterul wireless ASUS.

---

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

### 3.15.4 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.

Wireless - Wireless MAC Filter	
Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.	
<b>Basic Config</b>	
Band	2.4GHz
Enable MAC Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No
MAC Filter Mode	Accept
<b>MAC filter list (Max Limit : 64)</b>	
Client Name (MAC Address)	Add / Delete
<input type="text"/>	
No data in table.	
<b>Apply</b>	

**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. Bifați **Yes (Da)** în câmpul **Enable Mac Filter (Activare filtru Mac)**.
3. 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.
4. În lista de filtrare MAC, faceți clic pe butonul **Add (Adăugare)** și introduceți adresa MAC a dispozitivului wireless.
5. Faceți clic pe **Apply (Aplicare)**.

### 3.15.5 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.

Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	2.4GHz ▾
Server IP Address	<input type="text"/>
Server Port	1812
Connection Secret	<input type="text"/>

Apply

#### Pentru a configura setările wireless RADIUS:

1. Asigurați-vă că modul de autentificare al ruterului wireless este setat la WPA-Enterprise, WPA2-Enterprise sau Radius cu 802.1x.

---

**NOTĂ:** Consultați secțiunea **3.15.1 Aspecte generale** 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 **Connection Secret (Secret conexiune)**, atribuiți parola pentru accesarea serverului RADIUS.
6. Faceți clic pe **Apply (Aplicare)**.

### 3.15.6 Professional (Profesional)

Ecranul Professional (Profesional) oferă opțiuni avansate de configurare.

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

Wireless - Professional	
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.	
Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
Set AP Isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No
Roaming assistant	Enable <input type="checkbox"/> Disconnect clients with RSSI lower than: -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="range"/> Performance
<b>Apply</b>	

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

- **Band (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):** Puteți alege formatul pentru afișarea ceasului, cu 24 de ore sau cu 12 ore. Culoarea din tabel indică Allow (Se permite) sau Deny (Se respinge). Faceți clic pe fiecare cadru pentru a schimba setările pentru ora din zilele săptămânii și faceți clic pe **OK** când terminați.

Wireless - Professional

\* Reminder: The System time zone is different from your locale setting.

Clock Format: 24-hour  Allow  Deny

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **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.
- **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) definește 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.
- **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 și 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) reprezintă intervalul de timp înainte ca un semnal să fie trimis către un dispozitiv wireless în modul de inactivitate, indicând faptul că se așteaptă 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 și 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.
- **Reglare putere TX:** Acest parametru se referă la cantitatea de miliWatti (mW) necesară pentru a alimenta semnalul radiu al ruterului wireless. Introduceți o valoare cuprinsă între 0 și 100.
- **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.

## 4 Utilitățile

---

### NOTE:

- Descărcați și instalați utilitățile routerului wireless de pe site-ul web ASUS:
    - Utilitarul Device Discovery, versiunea 1.4.7.1, poate fi descărcat de la adresa <https://www.asus.com/Networking/RT-AX86U PRO/HelpDesk Download/>
    - Utilitarul Firmware Restoration, versiunea 1.9.0.4, poate fi descărcat de la adresa <https://www.asus.com/Networking/RT-AX86U PRO/HelpDesk Download/>
    - 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>
  - Utilitățile 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 utilitarul Detectează Dispozitivul:**

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

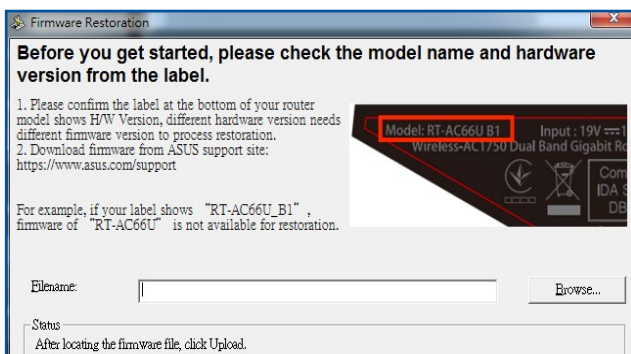
---

**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 reușit 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 și 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 și 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. și 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 (Utilitară ASUS) > Wireless Router (Ruter fără fir) > Firmware Restoration (Restaurare firmware)**.
5. Specificați un fișier de firmware, apoi faceți clic pe **Upload (Încărcare)**.

---

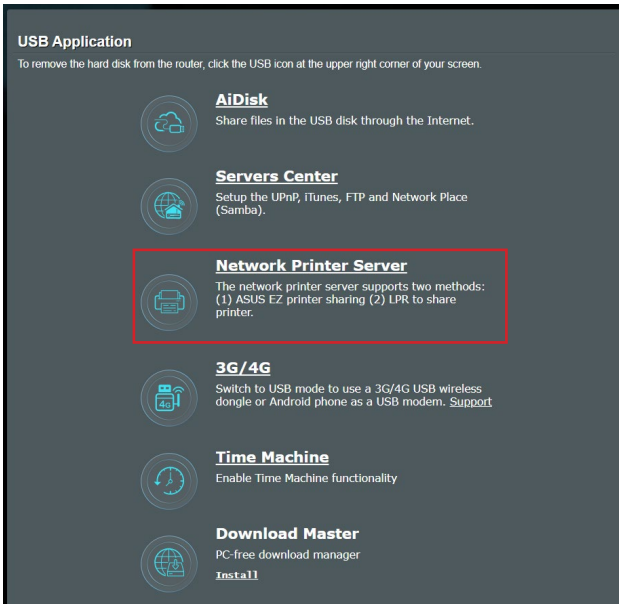
**NOTĂ:** Acesta nu este un utilitar de upgrade de firmware și nu poate fi utilizat pe un ruter fără fir ASUS în funcțiune. Upgrade-urile normale de firmware trebuie efectuate prin intermediul interfeței Web. Consultați **Capitolul 3: Configurarea setărilor generale și setărilor avansate** pentru mai 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 și să configurați un server de tipărire. Acest lucru permite clienților din rețeaua dvs. să tipărească și să scaneze fișiere în modul wireless.



---

**NOTĂ:** Funcția server de tipărire este acceptată în sistemele de operare Windows® 10 și Windows® 11.

---

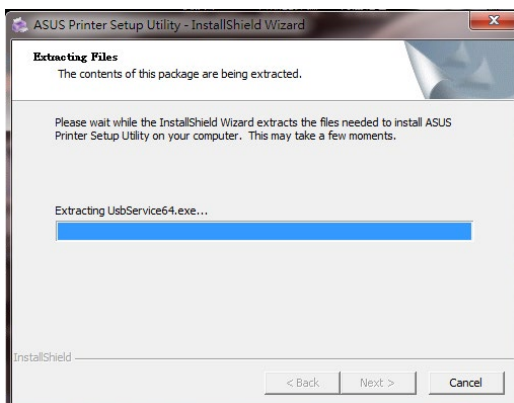
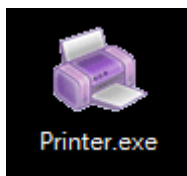
## Pentru a configura modul de partajare a imprimantei EZ:

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.

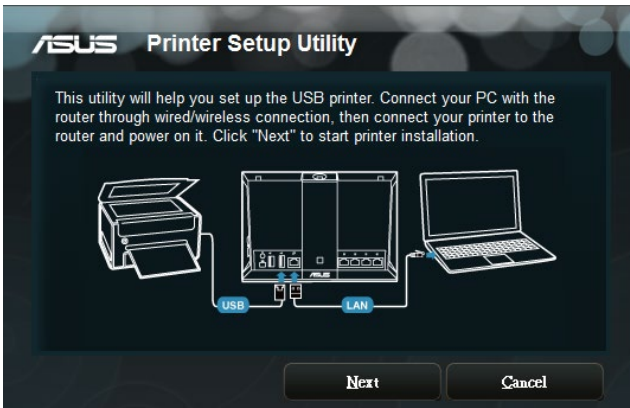


**NOTĂ:** Utilitarul de tipărire în rețea este acceptat numai în sistemele de operare Windows® 10 și Windows® 11. Pentru a instala utilitarul pe un sistem de operare Mac, selectați opțiunea **Use LPR protocol for sharing printer (Utilizare protocol LPR pentru partajarea imprimantei)**.

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



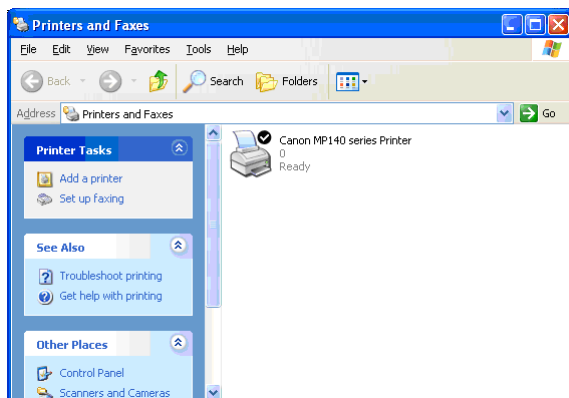
4. Urmăți instrucțiunile de pe ecran pentru a configura componentele hardware, apoi faceți clic pe **Next (Următorul)**.



5. Așteptați câteva minute pentru finalizarea instalării inițiale. Faceți clic pe **Next (Următorul)**.
6. Faceți clic pe **Finish (Finalizare)** pentru a încheia instalarea.
7. Urmăți instrucțiunile Windows® OS pentru a instala driverul de imprimantă.



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





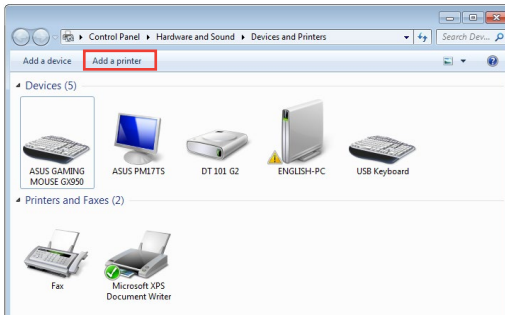
### 4.3.2 Utilizarea protocolului LPR pentru partajarea imprimantei

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

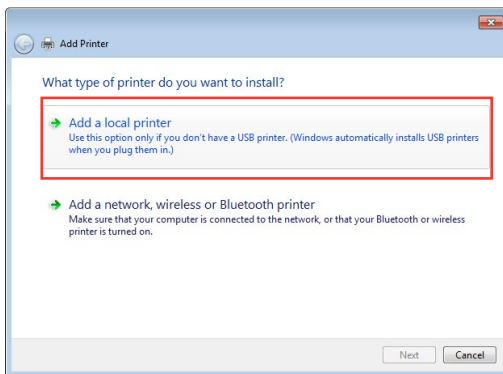
#### Partajarea imprimantei compatibile LPR

**Pentru partajarea imprimantei compatibile LPR:**

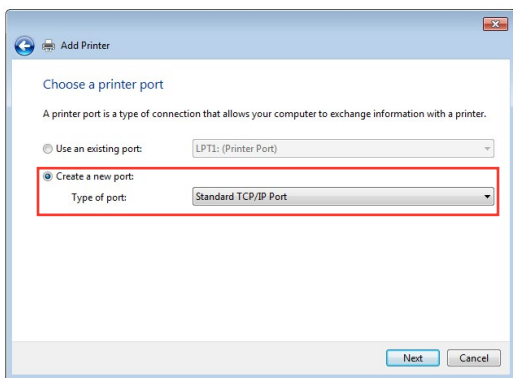
1. Din desktopul Windows®, faceți clic pe **Start (Pornire) > Devices and Printers (Dispozitive și imprimante) > Add a printer (Adăugare imprimantă)** pentru a executa **Add Printer Wizard (Expert adăugare imprimantă)**.



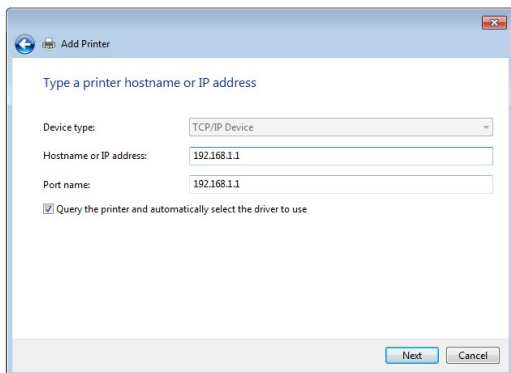
2. Selectați **Add a local printer (Adăugare imprimantă locală)** și apoi faceți clic pe **Next (Următorul)**.



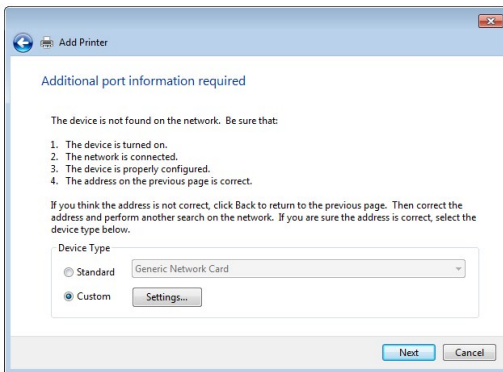
3. Selectați **Create a new port (Se creează un port nou)** apoi setați **Type of Port (Tip port)** la **Standard TCP/IP Port (Port TCP/IP standard)**. Faceți clic pe **Next (Următorul)**.



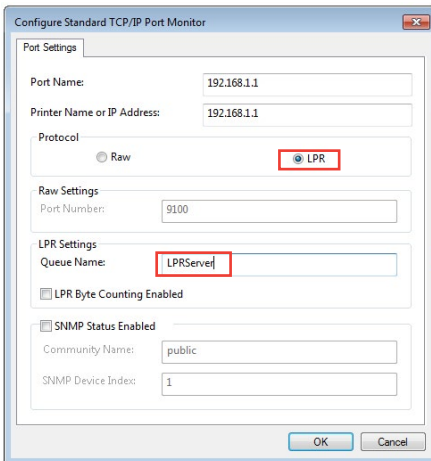
4. În câmpul **Hostname or IP address (Nume de gazdă sau adresă IP)**, introduceți adresa IP a ruterului wireless și apoi faceți clic pe **Next (Următorul)**.



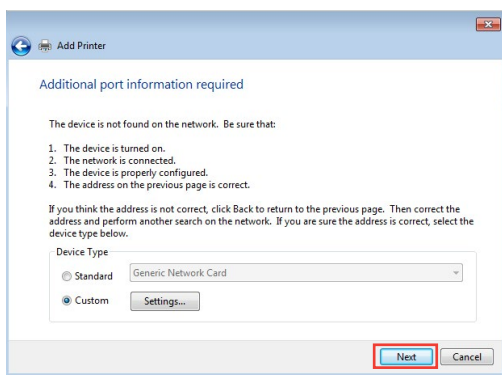
5. Selectați **Custom (Particularizat)** și apoi faceți clic pe **Settings (Setări)**.



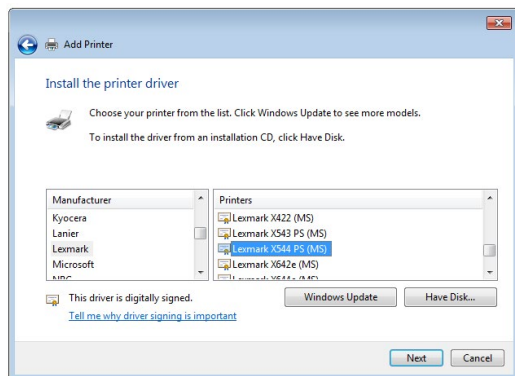
6. Setăți **Protocol** la **LPR**. În câmpul **Queue Name (Nume coadă)**, introduceți o valoare pentru **LPR Server (Server LPR)** și apoi faceți clic pe **OK** pentru a continua.



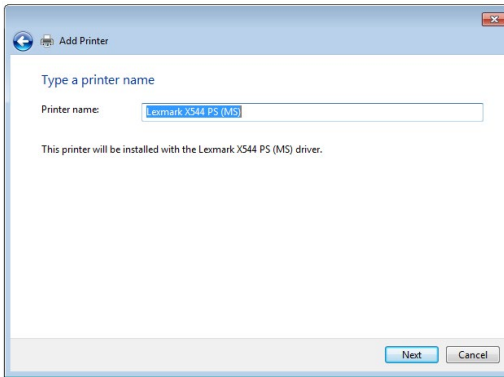
7. Faceți clic pe pe **Next (Următorul)** pentru a finaliza configurarea portului standard TCP/IP.



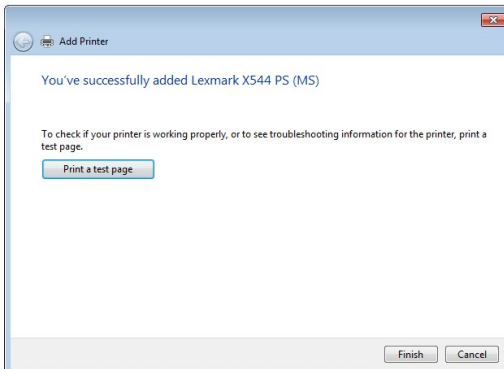
8. Instalați driverul de imprimantă din lista cu modelele distribuitorului. Dacă imprimanta dvs. nu figurează în listă, faceți clic pe **Have Disk (Obținere disc)** pentru a instala manual driverele imprimantei de pe un CD-ROM sau dintr-un fișier.



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



10. Faceți 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):

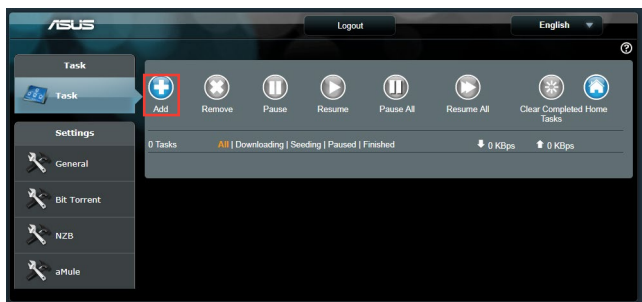
1. Faceți clic pe **General (Generalități) > USB Application (Aplicație USB) > Download Master (Coordonator de descărcări)** pentru a descărca și instala automat acest utilitar.

---

**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.



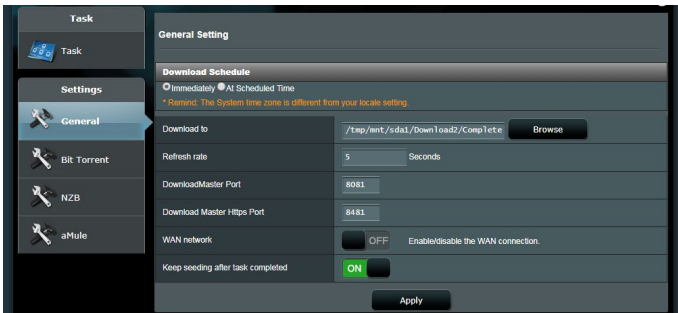
4. Selectați un tip de descărcare, precum BitTorrent, HTTP sau FTP. Furnizați un fișier de tip torrent sau o locație URL pentru a începe descărcarea.

---

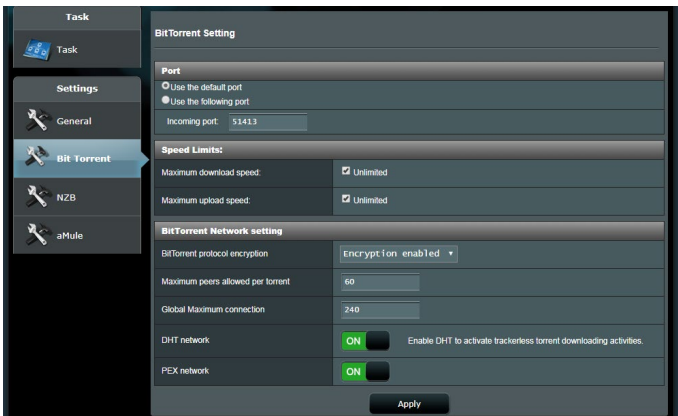
**NOTĂ:** Pentru detalii referitoare la Bit Torrent, consultați secțiunea **4.4.1 Configuring Bit Torrent download settings (Configurarea setărilor de descărcare Bit Torrent)**.

---

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



#### 4.4.1 Configurarea setărilor de descărcare pentru Bit Torrent

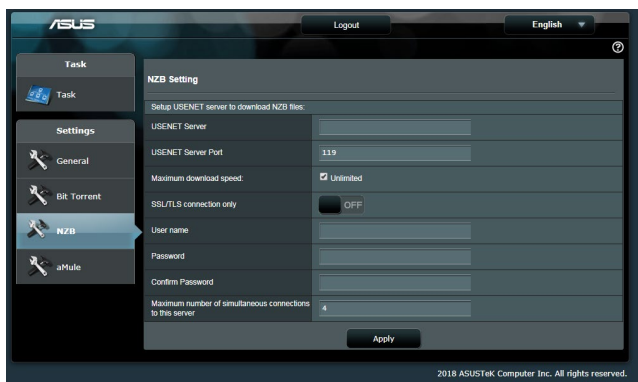


#### Pentru a configura setările de descărcare pentru Bit Torrent:

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 și descărcare sub **Speed Limits (Limite viteză)**.
4. Puteți limita numărul maxim de perechi și puteți activa sau dezactiva criptarea fișierelor 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

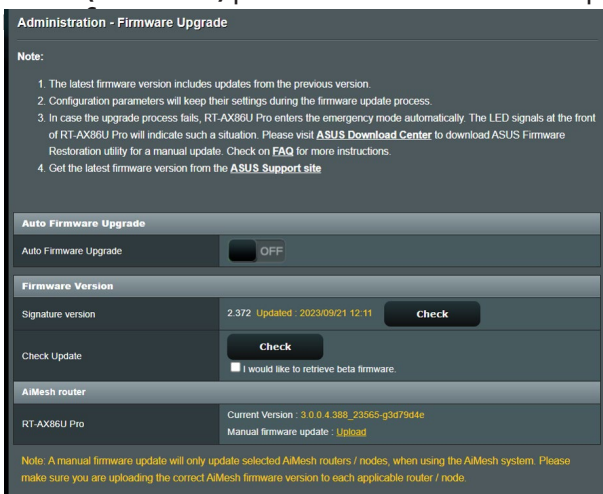
Acest capitol oferă soluții pentru problemele pe care le puteți întâmpina la folosirea ruterului. În cazul în care întâmpinați probleme care nu sunt menționate în acest capitol, accesați siteul de asistență ASUS, la adresa: <http://support.asus.com/>. Aici puteți găsi mai multe informații despre produs,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

### 5.1 Depanarea de bază

Dacă întâmpinați probleme la folosirea ruterului, parcurgeți pașii 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



2. Dacă cel mai recent firmware este disponibil, accesați site-ul global ASUS, la adresa <https://www.asus.com/Networking/RT-AX86U-PRO/HelpDesk/>, pentru a descărca cel mai recent firmware.
3. Din pagina **Firmware Version (Versiune firmware)**, faceți clic pe **Check (Verificare)** pentru a localiza fișierul firmware.
4. Faceți clic pe **Upload (Încărcare)** pentru upgradarea firmware-ului.

### **Reporniți rețeaua în următoarea secvență:**

1. Opriți funcționarea modemului.
2. Deconectați modemul.
3. Opriți funcționarea ruterului și computerelor.
4. Conectați modemul.
5. Porniți funcționarea modemului și apoi așteptați 2 minute.
6. Porniți funcționarea ruterului și apoi așteptați 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 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 și 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. afișat în **Client Status (Stare client)**.



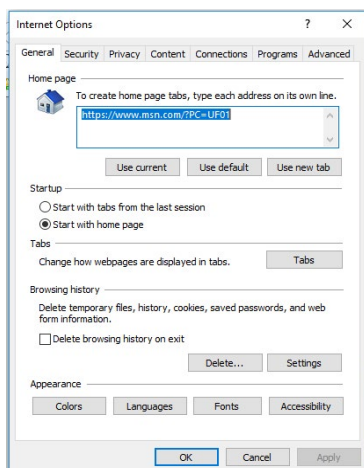
## 5.2 Întrebări frecvente

### Nu pot accesa interfața de utilizare a ruterului folosind un browser web.

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

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... (Ștergere...)**, selectați **Temporary Internet Files and website files (Fișiere Internet temporare și fișiere site web)** și **Cookies and website data (Module cookie și date privind site-ul web)**, iar apoi faceți clic pe **Delete (Ștergere)**.



#### NOTE:

- Comenzile pentru ștergerea modulelor cookie și a fișierelor diferă în funcție de browserul Web.
- Dezactivați setările de server proxy, revocați conexiunea pe linie comutată și 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 routerului 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 router.
  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)**.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. RT-AX86U Pro supports up to 253 IP addresses for your local network.  
Manually Assigned IP around the DHCP list FAQ

**Basic Config**

Enable the DHCP Server  Yes  No

RT-AX86U Pro's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

**DNS and WINS Server Setting**

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS  Yes  No

WINS Server

**Manual Assignment**

Enable Manual Assignment  Yes  No

**Manually Assigned IP around the DHCP list (Max Limit : 64)**

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

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

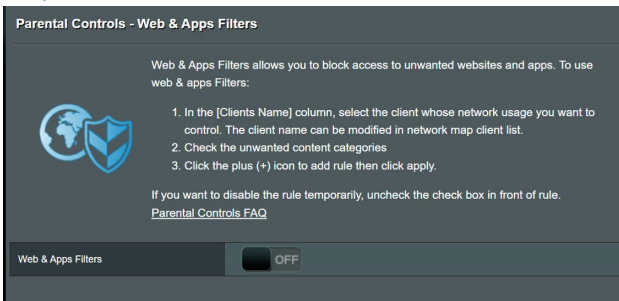
- Dacă utilizați un adaptor LAN wireless, verificați conformitatea canalului wireless în uz cu canalele disponibile în regiunea/țara dvs. Dacă nu există conformitate, ajustați canalul, lățimea de bandă a canalului și modul wireless.
- Dacă în continuare nu vă puteți conecta wireless la ruter, puteți 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)** și 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 și mergeți la **General (Generalități)** > **Network Map (Hartă rețea)** și 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 așa 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)** și vedeți dacă dispozitivul se află în listă. Dacă dispozitivul apare sub **Client Name (Nume client)**, eliminați dispozitivul folosind butonul **Delete (Ștergere)** sau ajustați setările privind gestionarea timpului.



- Dacă în continuare nu puteți accesa Internetul, încercați să reporniți computerul și să verificați adresa IP a rețelei și adresa gateway-ului.
- Verificați indicatorii de stare de pe modemul ADSL și 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 și 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 și o nouă cheie de criptare și 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)** și faceți clic pe **Restore (Restaurare)**. Contul și 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)** și faceți clic pe **Restore (Restaurare)**.

### Upgradeul de firmware a eșuat.

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).



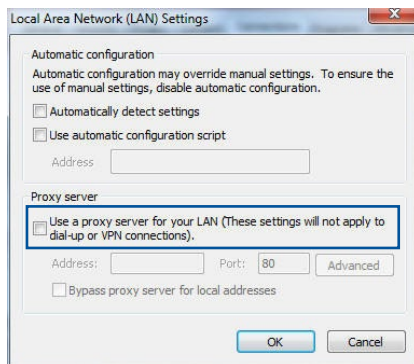
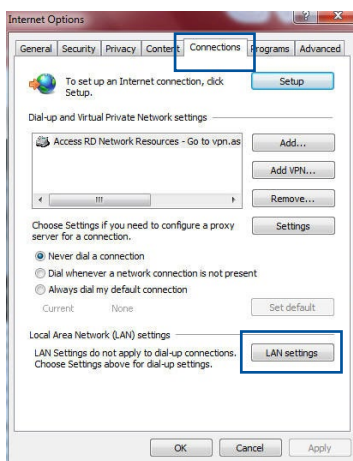
## Nu se poate accesa interfața de utilizare web

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

### A. Dezactivați serverul proxy, dacă este activat.

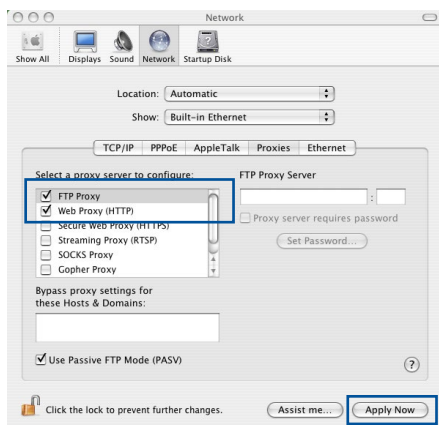
#### Windows®

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))**.



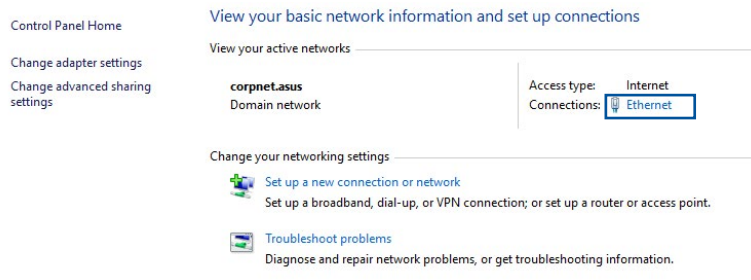
3. Faceți clic pe **Apply Now (Se aplică acum)** când ați terminat.

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

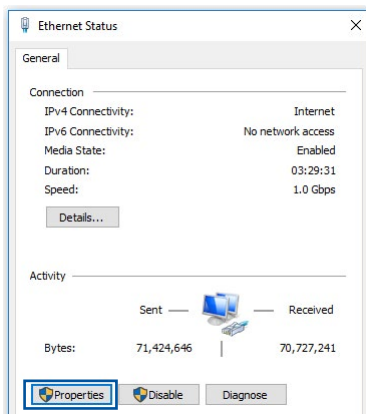
## B. Configurați setările TCP/IP pentru obținerea automată a unei adrese IP.

### Windows®

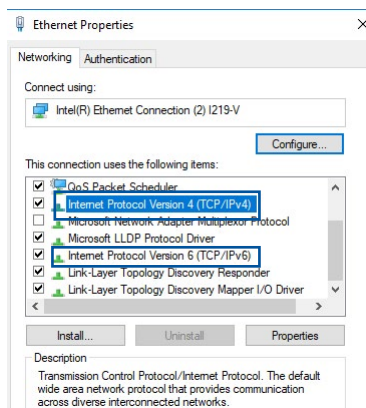
1. Faceți clic pe **Start (Pornire)** > **Control Panel (Panou de control)** > **Network and Internet (Rețea și Internet)** > **Network and Sharing Center (Centru de rețea și partajare)**, apoi faceți clic pe conexiunea de rețea pentru a afișa fereastra de stare.



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



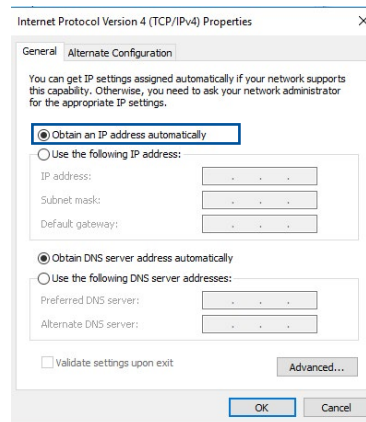
3. Selectați **Internet Protocol Version 4 (TCP/IPv4) (Protocol Internet versiunea 4 (TCP/IPv4))** sau **Internet Protocol Version 6 (TCP/IPv6) (Protocol Internet versiunea 6 (TCP/IPv6))**, apoi faceți clic pe **Properties (Proprietăți)**.




4. Pentru a obține automat setările IP IPv4, bifați **Obtain an IP address automatically (Se obține automat o adresă IP)**.

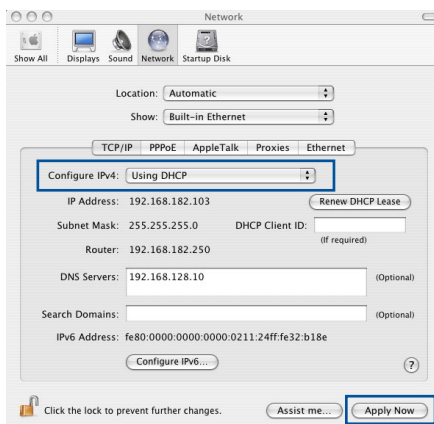
Pentru a obține automat setările IP IPv6, bifați **Obtain an IPv6 address automatically (Se obține automat o adresă IPv6)**.

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.

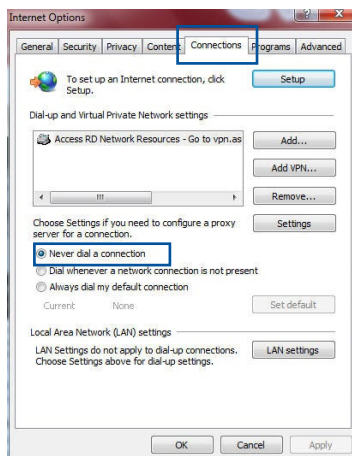


**NOTĂ:** Consultați caracteristica de ajutor și asistență a sistemului de operare pentru detalii despre configurarea setărilor TCP/IP ale computerului.

## 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/>.

