

Ghidul utilizatorului

RT-AC53

Ruter Gigabit Wireless-AC750 de bandă duală



ASUS[®]
IN SEARCH OF INCREDIBLE

RO11412
Prima ediție
Mai 2016

Copyright © 2016 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 ruterului	9
1.5	Cerințe pentru configurare	10
1.6	Configurarea ruterului.....	11
	1.6.1 Conexiune cu fir.....	11
	1.6.2 Conexiune wireless.....	12

2 Inițializarea

2.1	Conectarea la interfața Web GUI	14
2.2	Configurarea rapidă a conexiunii la.....	15
	Internet (QIS) cu detectare automată	15
2.3	Conectarea la rețeaua dvs. wireless.....	19

3 Configurarea setărilor generale

3.1	Utilizarea hărții rețelei	20
	3.1.1 Configurarea setărilor de securitate pentru rețeaua wireless	21
	3.1.2 Administrarea clienților din rețea.....	22
3.2	Crearea rețelei de vizitatori.....	23
3.3	Utilizarea funcției Traffic Manager	25
	(Manager trafic)	25
	3.3.1 Gestionarea lățimii de bandă pentru funcția QoS (Calitatea serviciului).....	25
	3.3.2 Monitorizarea traficului	28
3.4	Configurarea controlului parental	29

Sumar

4 Configurarea setărilor Complexe

4.1	Wireless.....	31
4.1.1	Aspecte generale	31
4.1.2	WPS	34
4.1.3	Wireless MAC Filter (Filtru MAC wireless)	36
4.1.4	Setarea RADIUS.....	37
4.1.5	Professional (Profesional).....	38
4.2	LAN.....	40
4.2.1	LAN IP	40
4.2.2	serverului DHCP.....	41
4.2.3	Rută.....	43
4.2.4	IPTV	44
4.3	WAN	45
4.3.1	Conexiune la Internet	45
4.3.2	Triggering de port.....	48
4.3.3	Server virtual/Redirecționare porturi	49
4.3.4	DMZ.....	53
4.3.5	DDNS	54
4.3.6	NAT Passthrough (Trecere NAT).....	55
4.4	IPv6.....	56
4.5	Paravan de protecție.....	57
4.5.1	Aspecte generale	57
4.5.2	URL Filter (Filtru URL)	57
4.5.3	Keyword filter (Filtru cuvinte cheie)	58
4.5.4	Network Services Filter (Filtru servicii rețea)	59
4.6	Administration (Administrare).....	61
4.6.1	Operation mode (Mod de funcționare)	61
4.6.2	System (Sistem).....	62
4.6.3	Actualizarea softului integrat	63
4.6.4	Refacerea/Salvarea/Încărcarea setărilor.....	63
4.7	System Log (Jurnal de sistem).....	64

Sumar

5 utilităților

5.1	Detectarea Dispozitivului.....	65
5.2	Refacerea softului integrat.....	66

6 Remedierea defecțiunilor 67

6.1	Depanarea de bază.....	67
6.2	Întrebări frecvente	70

Anexă

Anunțuri.....	79
Informații de contact despre producător	93
Informații privind liniile telefonice de asistență globale.....	94

1 Cum să vă cunoașteți routerul

1.1 Bine ați venit!

Vă mulțumim pentru cumpărarea unui router fără fir ASUS RT-AC53!

Routerul RT-AC53 ultrasubțire și elegant dispune de benzi duble de 2,4 GHz și 5 GHz, care furnizează viteze wireless AC gigabit foarte rapide de până la 867 Mbps în banda de 5 GHz și de 300 Mbps în banda de 2,5 GHz simultan.

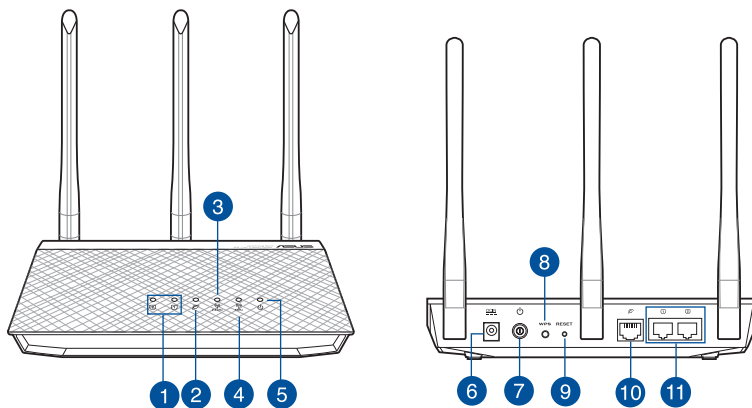
1.2 Conținutul pachetului

- | | |
|---|---|
| <input checked="" type="checkbox"/> Router fără cablu RT-AC53 | <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



2 LED LAN 1~2

Stins: Sistemul nu este alimentat sau nu există conexiune fizică.

Aprins: Există conexiune fizică la o rețea locală (LAN).

3 LED WAN (Internet)

Stins: Sistemul nu este alimentat sau nu există conexiune fizică.

Aprins: Există conexiune fizică la o rețea de arie largă (WAN).

4 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.

4 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.

1 LED alimentare

Stins: Fără alimentare.

Aprins: Dispozitivul este pregătit.

Intermitent lent: Mod de salvare

Intermitent rapid: Se procesează funcția WPS.

6 Port alimentare (intrare c.c.)

Inserați adaptorul de c.a. în acest port și conectați ruterul la o sursă de alimentare.

7 Buton de alimentare

Apăsăți pe acest buton pentru a porni/a opri sistemul.

-
- 12 Buton WPS**
Acest buton lansează Expertul WPS.
-
- 9 Buton Reset (Reinițializare)**
Acest buton reinițializează sau restabilește sistemul la setările implicite din fabrică.
-
- 10 Port WAN (Internet)**
Conectați un cablu de rețea la acest port pentru a stabili o conexiune WAN.
-
- 11 Porturi LAN 1 ~ 2**
Conectați cabluri de rețea la aceste porturi pentru a stabili o conexiune LAN.
-

NOTE:

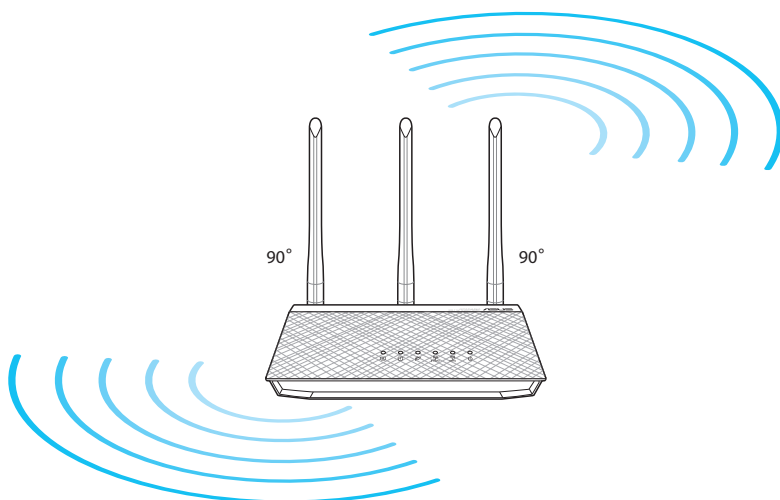
- Utilizați numai adaptorul livrat în pachet. Utilizarea altor adaptoare poate deteriora dispozitivul.
- **Specificații:**

Adaptor de alimentare c.c.	leșire c.c.: +19 V cu curent max. de 21A;		
Temperatură în stare de funcționare	0~40°C	Stocare	0~70°C
Umiditate în stare de funcționare	50~90%	Stocare	20~90%

1.4 Poziționarea ruterului

Pentru transmisia optimă a semnalului fără fir între ruterul fără fir 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.
- Pentru a beneficia de un semnal wireless optim, orientați cele 3 antene detașabile 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
- 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 în computerul dvs. pentru a vă conecta la rețea.
 - Dispunând de tehnologia de bandă duală, ruterul dvs. wireless acceptă simultan semnale wireless de 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.
-

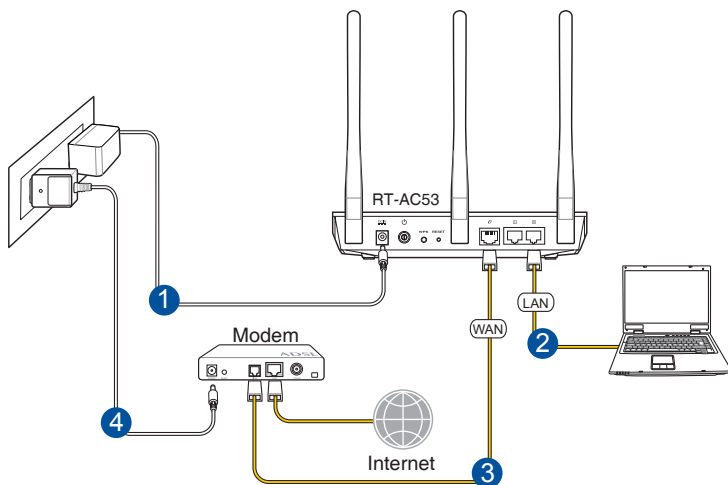
1.6 Configurarea ruterului

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).

1.6.1 Conexiune cu fir

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



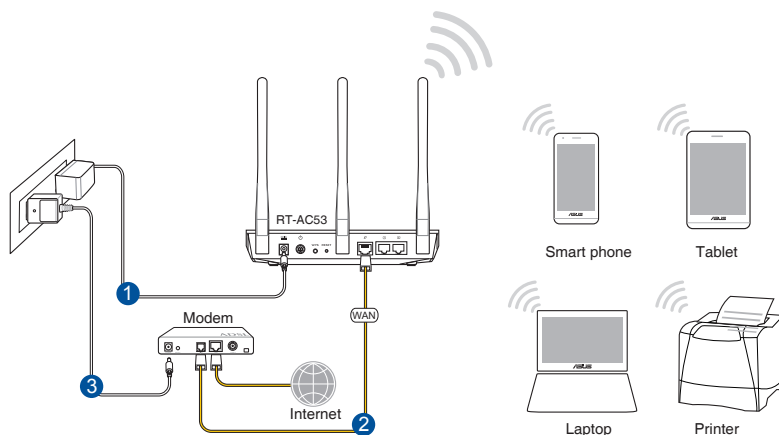
Pentru a configura ruterul fără fir printr-o conexiune prin cablu:

1. Inserați adaptorul de c.a. al ruterului fără fir în portul de intrare c.c. și conectați-l la o priză.
2. Utilizând cablul de rețea inclus, conectați computerul la portul LAN al ruterului fără fir.

IMPORTANT! Asigurați-vă că LED-ul LAN luminează intermitent.

- 3 Utilizând un alt cablu de rețea, conectați modemul la portul WAN al ruterului fără fir.
4. Inserați adaptorul de c.a. al modemului în portul de intrare c.c. și conectați-l la o priză.

1.6.2 Conexiune wireless



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

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

Note:

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

2 Inițilizarea

2.1 Conectarea la interfața Web GUI

Ruterul dvs. wireless de la ASUS se furnizează împreună 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://router.asus.com>**.
2. Pe pagina de acces, tastați numele inițial al utilizatorului (**admin**) și parola (**admin**).
3. Puteți utiliza interfața de utilizare web pentru a configura diverse setări pentru ruterul dvs. wireless ASUS.



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

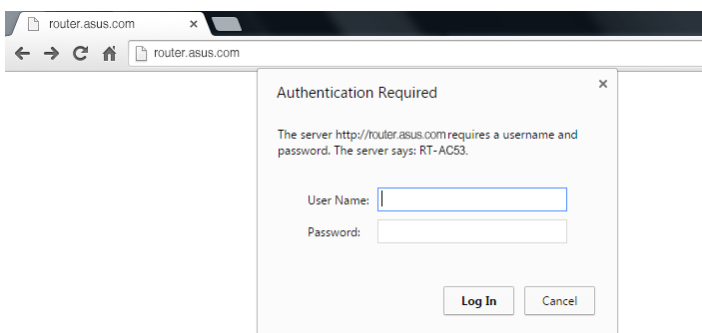
2.2 Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată

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. Conectați-vă la interfața de utilizare Pagina QIS va fi lansată în mod automat.



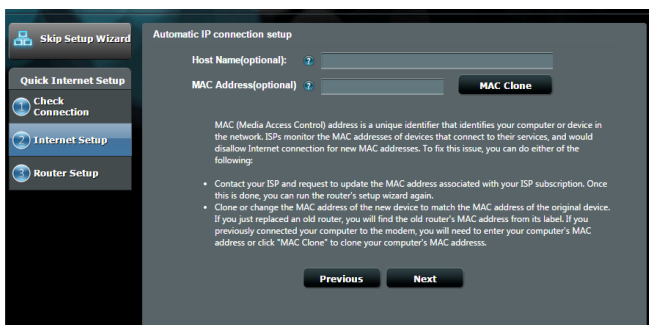
NOTE:

- În mod implicit, numele de utilizare și parola de conectare pentru interfața de utilizare web a ruterului dvs. wireless sunt ambele **admin**. Pentru detalii legate de schimbarea numelui de utilizator și parolei ruterului dvs. wireless, consultați secțiunea **4.7.2 System (Sistem)**.
- 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.

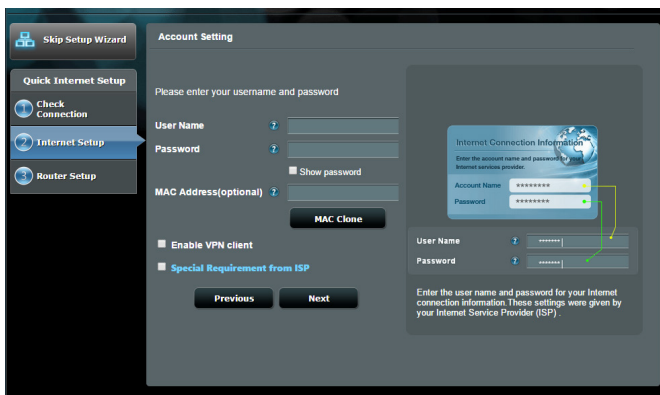
2. Ruterul wireless detectează automat dacă tipul conexiunii de la ISP este **Dynamic IP (IP dinamic), PPPoE, PPTP, L2TP și Static IP (IP static)**. Tastați informațiile utile pentru tipul de conexiune furnizat de ISP.

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

pentru modul de obținere automat a adresei IP (prin DHCP)



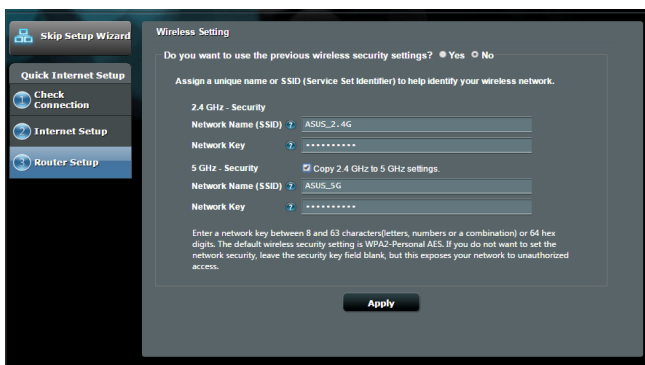
pentru modulele de conectare PPPoE, PPTP și L2TP



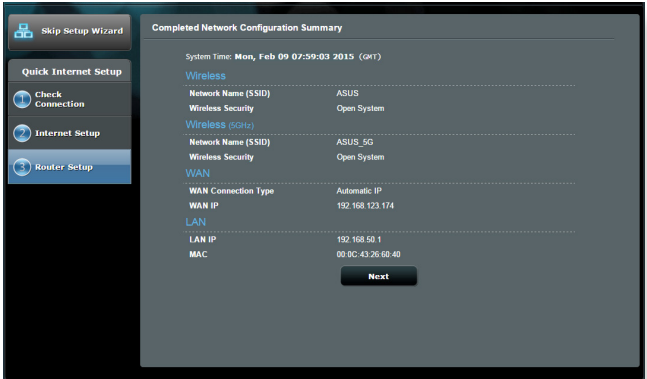
Note:

- **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. Your Internet and wireless settings are displayed. Click **Next** to continue.
5. Read the wireless network connection tutorial. When done, click **Finish**.



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

3.1 Utilizarea hărții rețelei

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



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 , 5 GHz-1 și 5 GHz-2.

Setări de securitate pentru banda 2,4 GHz

The screenshot shows the 'System Status' configuration screen for the 2.4GHz band. It features three tabs: '2.4GHz', '5GHz', and 'Status', with '2.4GHz' selected. The 'Wireless name(SSID)' field contains 'ASUS'. The 'Authentication Method' dropdown is set to 'Open System'. An 'Apply' button is visible. Below this, the LAN IP is '192.168. 1 .1', PIN code is '12345670', LAN MAC address is '00:0C:43:26:60:40', and Wireless 2.4GHz MAC address is '00:0C:43:76:20:58'.

Setări de securitate pentru banda 5 GHz

The screenshot shows the 'System Status' configuration screen for the 5GHz band. It features three tabs: '2.4GHz', '5GHz', and 'Status', with '5GHz' selected. The 'Wireless name(SSID)' field contains 'ASUS_5G'. The 'Authentication Method' dropdown is set to 'Open System'. The 'AiRadar' toggle switch is turned 'ON'. An 'Apply' button is visible. Below this, the LAN IP is '192.168. 1 .1', PIN code is '12345670', LAN MAC address is '00:0C:43:26:60:40', and Wireless 2.4GHz MAC address is '00:0C:43:76:20:58'.

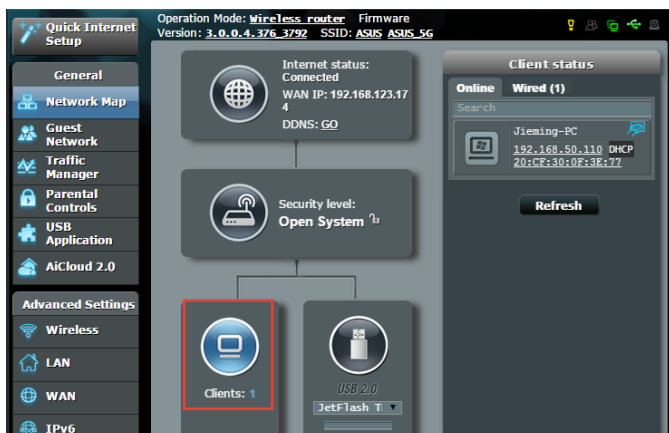
3. În câmpul **Wireless name (SSID) (Nume rețea wireless (SSID))** tastați un nume unic pentru rețeaua dvs. wireless.
4. Din lista verticală **Nivel securitate**, selectați metoda de autentificare pentru rețeaua dvs. wireless.

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

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

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

3.1.2 Administrarea clienților din rețea



Pentru a administra clienții din rețea:

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

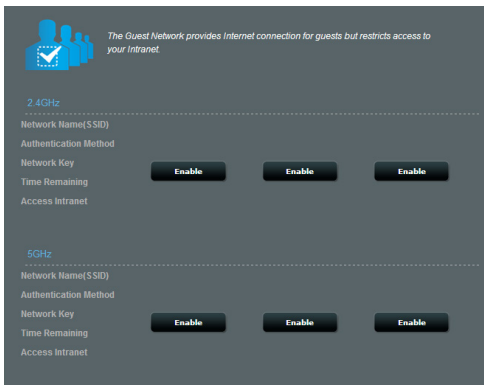
3.2 Crearea rețelei de vizitatori

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: RT-AC53 acceptă până la SSID-uri (trei în banda de frecvență de 2,4 GHz și trei în banda de frecvență de 5 GHz).

Pentru a vă crea o rețea de vizitatori:

1. Din panoul de navigare, mergeți la **General > Guest Network (Rețea vizitatori)**.
2. În ecranul Guest Network (Rețea vizitatori), selectați banda de frecvență de 2,4 Ghz, 5 Ghz-1 5 Ghz-2 sau de 5Ghz 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)**

Guest Network

The guest network can provide internet connectivity for temporary visitors without accessing your private network.

2.4GHz

Network name: ASUS_Guest1
Wireless Security: Open System
Security key: None
Access Time: Limitless
Access Intranet: off

5GHz

Network name: ASUS_5G_Guest1
Wireless Security: Open System
Security key: None
Access Time: Limitless
Access Intranet: off

5. Faceți clic pe **Yes (Da)** în ecranul **Enable Guest Network (Activare rețea vizitatori)**.
6. Atribuiți un nume pentru rețeaua wireless temporară în câmpul **Network Name (SSID) (Nume rețea (SSID))**.
7. Selectați o opțiune pentru **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)**.

3.3 Utilizarea funcției Traffic Manager (Manager trafic)

3.3.1 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 > Traffic Manager (Manager trafic) > fila 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 **Save (Salvare)**.

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.

3.3.2 Monitorizarea traficului

Funcția de monitorizare a traficului vă permite să evaluați utilizarea lățimii de bandă și viteza conexiunilor la Internet și a rețelelor cu fir sau wireless. Această funcție vă permite să monitorizați traficul din rețea chiar zilnic.



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

3.4 Configurarea controlului parental

Funcția de control parental vă permite să controlați intervalele orare pentru accesul la Internet. Utilizatorii pot seta limita de timp pentru utilizarea rețelei de către un client.

Operation Mode: **Wireless router** Firmware Version: **3.0.0.4.376_3792** SSID: **ASUS_5G**

Parental Controls

Parental Controls allow you to set the time limit for a client's network usage. To use Parental Controls:

1. In the [Clients Name] column, select the client whose network usage you want to control. You may also key in the clients MAC address in the [Clients MAC Address] column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In the [Time Management] column, click the edit icon to edit the Active Schedule.
4. Select the desired time slots for allowed access times. Drag and hold to create longer time slots.
5. Click [OK] to save the settings made.

• [Click to open the tutorial video.](#)

Note: Clients that are added to Parental Controls will have their internet access restricted by default.

Enable Parental Controls **ON**

System Time **Mon, Feb 09 07:58:11**
**Remind: The System time zone is different from your locale setting.*



Client List (Max Limit : 16)				
	Client's Name	Client's MAC Address	Time Management	Add / Delete
<input checked="" type="checkbox"/>			-	
<input checked="" type="checkbox"/>	Jieming-PC	20:CF:30:0F:3E:70		

Apply

Pentru a utiliza funcția de control parental:

1. Din panoul de navigare, mergeți la **General > Parental control (Control parental)**.
2. Faceți clic pe **ON (Activat)** pentru a activa funcția de control parental.
3. Selectați clientul pentru care doriți să controlați utilizarea rețelei. Puteți să introduceți adresa MAC a clientului în coloana **Client MAC Address (Adresă MAC client)**.

NOTĂ: Asigurați-vă că numele clientului nu conține caractere speciale sau spații, deoarece acest lucru poate face ca ruterul să funcționeze anormal.

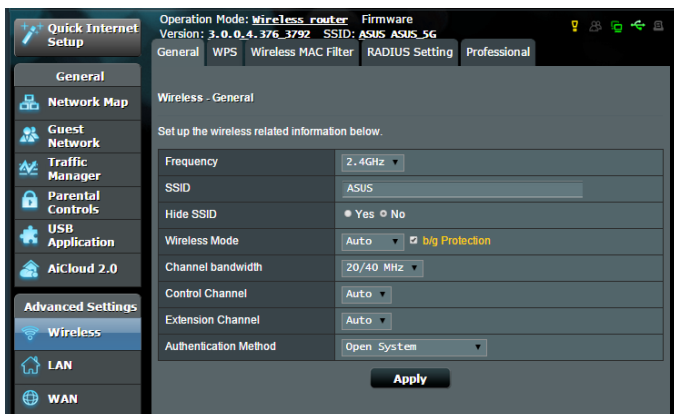
4. Faceți clic pe  sau pe  pentru a adăuga sau șterge profilul clientului.
5. Configurați limita de timp permisă în harta **Time Management (Gestionare timp)**. Glisați și fixați zona de timp dorită pentru a permite clientului să utilizeze rețeaua.
6. Faceți clic pe **OK**.
7. Faceți clic pe **Apply (Aplicare)** pentru a salva setările.

4 Configurarea setărilor Complexe

4.1 Wireless

4.1.1 Aspecte generale

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



Pentru configurarea setărilor de bază pentru rețeaua wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Wireless > fila 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 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.
7. 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 (default) (20 MHz (implicit)):** Selectați această lățime de bandă dacă întâmpinați probleme cu conexiunea fără fir.
8. Selectați oricare dintre aceste metode de autentificare:
 - **Open System (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.
- **Rază cu 802.1x**

NOTĂ: Routerul 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 (Oprit):** Dezactivează criptarea WEP
- **64-bit (64 de biți):** Activează o criptare WEP slabă
- **28-bit (64 de biți):** Activează o criptare WEP

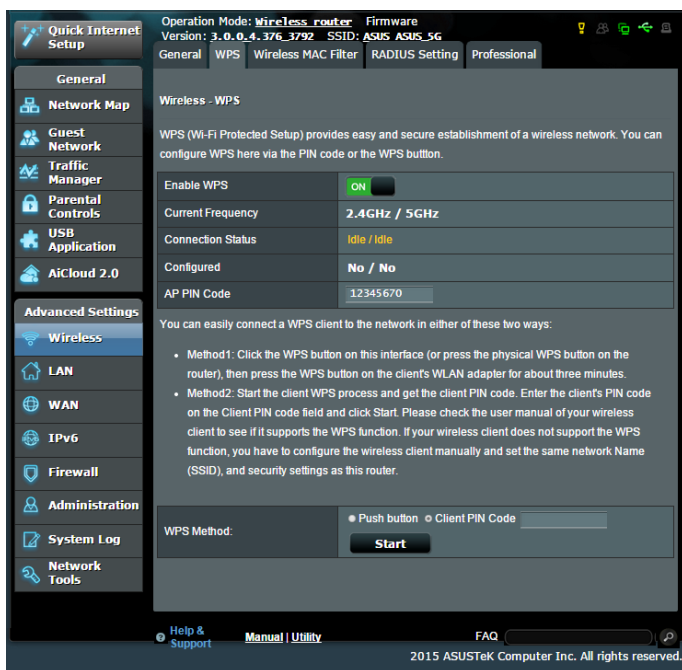
îmbunătățită.

10. După ce terminați, faceți clic pe **Apply (Se aplică)**.

4.1.2 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 > fila 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)**.

NOTE: WPS supports authentication using Open System, WPA-Personal, and WPA2-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.

4. In the WPS Method field, select **Push Button** or **Client PIN** code. If you select **Push Button**, go to step 4. If you select **Client PIN** code, go to step 5.
5. To set up WPS using the router's WPS button, follow these steps:
 - a. Click **Start** or press the WPS button found at the rear of the wireless router.
 - b. Press the WPS button on your wireless device. This is normally identified by the WPS logo.

NOTE: Check your wireless device or its user manual for the location of the WPS button.

- c. The wireless router will scan for any available WPS devices. If the wireless router does not find any WPS devices, it will switch to standby mode.
6. To set up WPS using the Client's PIN code, follow these steps:
 - a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.
 - b. Key in the Client PIN code on the text box.
 - c. Click **Start** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

4.1.3 Wireless MAC Filter (Filtru MAC wireless)

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

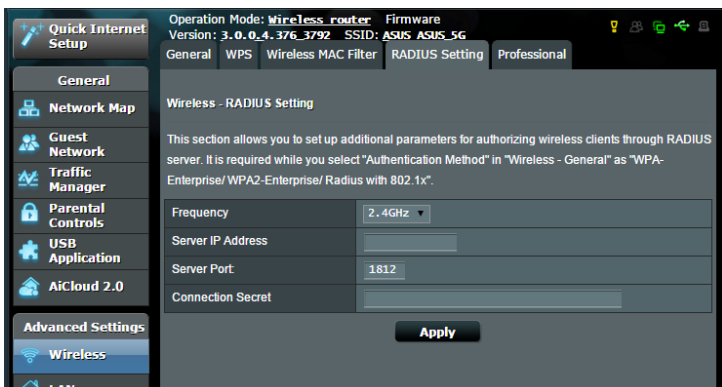


Pentru a configura filtrul MAC wireless:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Wireless > fila Wireless MAC Filter (Filtru MAC wireless)**.
2. În câmpul **Frequency (Frecvență)**, selectați banda de frecvență pe care doriți să o utilizați pentru filtrul MAC wireless.
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)**.

4.1.4 Setarea RADIUS

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



Pentru a configura setările wireless RADIUS:

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

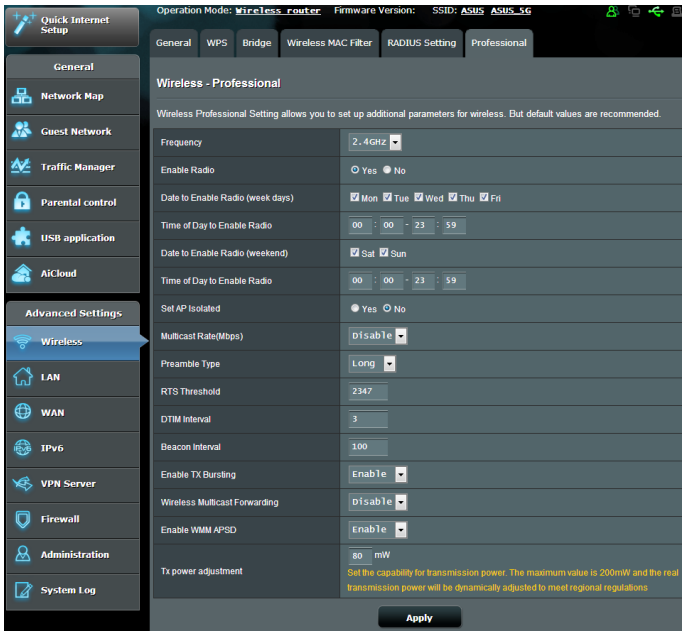
NOTĂ: Consultați secțiunea **4.1.1 Aspecte generale** pentru detalii privind configurarea modului de autentificare al ruterului wireless.

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)**.

4.1.5 Professional (Profesional)

Ecranul Professional (Profesional) oferă opțiuni avansate de configurare.

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



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

- **Frecvență:** 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.
- **Data de activare radio (zile ale săptămânii):** Puteți specifica zilele săptămânii în care caracteristica wireless a rețelei să fie activată.
- **Perioadă din zi pentru activarea radio:** Puteți specifica un interval de timp în care caracteristica wireless a rețelei să fie activată în timpul săptămânii.

- **Data de activare radio (weekend):** Puteți specifica zilele de weekend în care caracteristica wireless a rețelei să fie activată.
- **Perioadă din zi pentru activarea radio:** Puteți specifica un interval de timp în care caracteristica wireless a rețelei să fie activată în timpul weekendului.
- **Setare AP izolat:** Elementul Set AP isolated (Setare AP izolat) împiedică dispozitivele wireless din rețeaua dvs. să comunice între ele. Această caracteristică este utilă dacă se întâmplă adesea ca mulți vizitatori să se conecteze sau să se deconecteze de la rețeaua dvs. Selectați **Yes (Da)** pentru a activa această caracteristică sau **No (Nu)** pentru a o dezactiva.
- **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.
- **Activare rafală TX:** Acest parametru îmbunătățește viteza de transmitere între ruterul wireless și dispozitivele 802.11g.

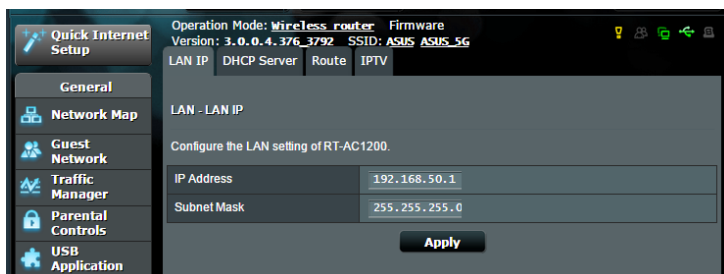
- **Redirecționare distribuire multiplă wireless:** Selectați **Enable (Activare)** pentru a permite ruterului wireless să redirecționeze traficul de distribuire multiplă către alte dispozitive wireless care acceptă acest tip de distribuire. Selectați **Disable (Dezactivare)** pentru a împiedica ruterul să redirecționeze transmișori de tip distribuire multiplă.
- **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.
- **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.

4.2 LAN

4.2.1 LAN IP

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

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



Pentru a modifica setările IP ale rețelei LAN:

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

4.2.2 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.

The screenshot shows the 'LAN - DHCP Server' configuration page in the ASUS router's web interface. The top status bar indicates 'Operation Mode: wireless_router' and 'Firmware Version: 3.0.0.4.376_3792'. The left sidebar has 'LAN' selected under 'Advanced Settings'. The main content area is titled 'LAN - DHCP Server' and includes a descriptive paragraph about DHCP. Below this are several configuration sections: 'Basic Config' with fields for 'Enable the DHCP Server' (radio buttons for Yes/No), 'RT-AC1200's Domain Name', 'IP Pool Starting Address' (192.168.50.2), 'IP Pool Ending Address' (192.168.50.25), 'Lease time' (86400), and 'Default Gateway'; 'DNS and WINS Server Setting' with fields for 'DNS Server' and 'WINS Server'; 'Enable Manual Assignment' with radio buttons for Yes/No; and a table for 'Manually Assigned IP around the DHCP list (Max Limit : 64)'. The table has columns for 'MAC address', 'IP Address', and 'Add / Delete', and currently contains no data. An 'Apply' button is at the bottom.

Pentru configurarea serverului DHCP:

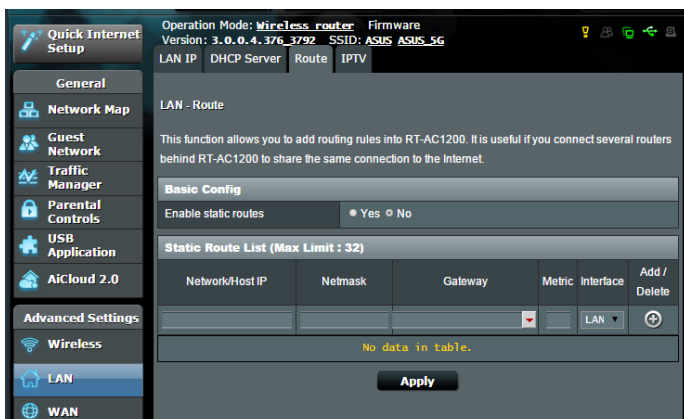
1. Din panoul de navigare, bifați **Advanced Settings > LAN > DHCP Server**.
2. În câmpul **Enable the DHCP Server? (Activați serverul DHCP?)** bifați **Yes (Da)**.

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.
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.

4.2.3 Rută

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

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

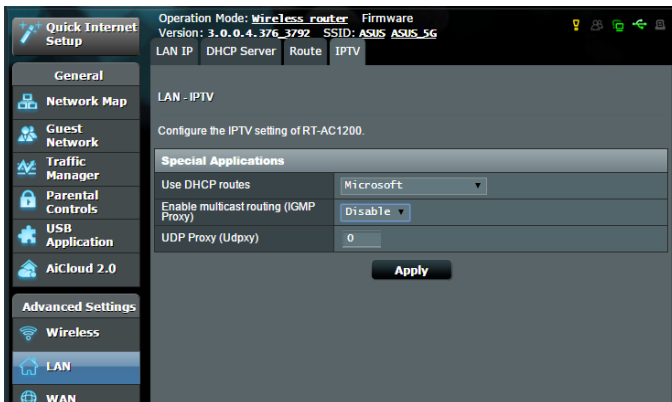


Pentru a configura tabelul de direcționare în rețeaua LAN:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > LAN > fila 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)**.

4.2.4 IPTV

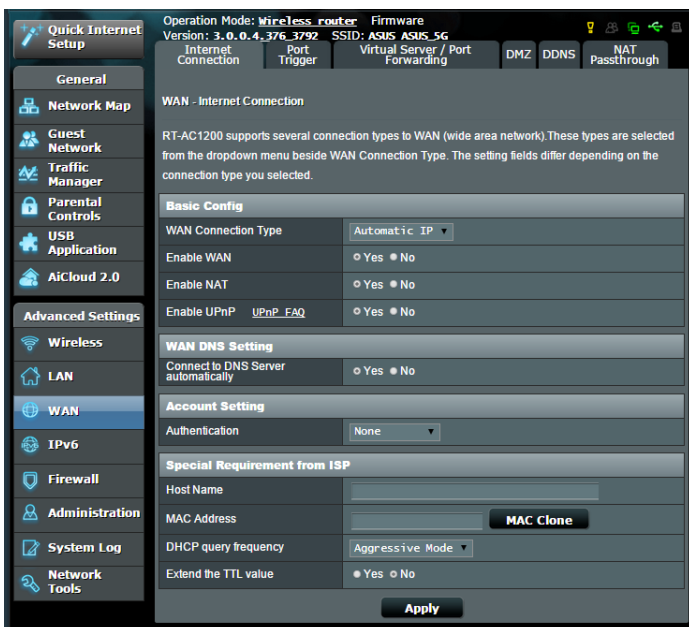
Ruterul wireless acceptă conectarea la servicii IPTV prin intermediul unui ISP sau al unei rețele LAN. Fila IPTV oferă setările necesare pentru configurarea serviciilor IPTV, VoIP, de distribuire multiplă și UDP. Contactați furnizorul de servicii Internet pentru a obține informații specifice cu privire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



4.3 WAN

4.3.1 Conexiune la Internet

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



Pentru configurarea setărilor conexiunii WAN:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > WAN > fila 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.

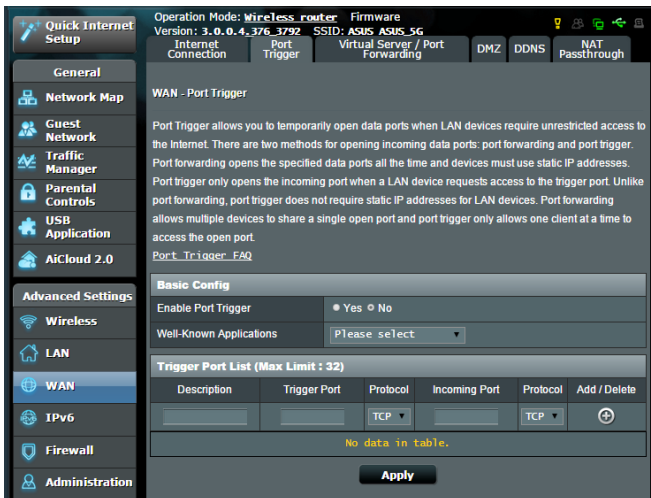
- **Activare NAT:** NAT (Network Address Translation - traducere adresă de rețea) este un sistem unde un IP public (IP de WAN) este utilizat pentru a furniza acces la Internet clienților de rețea care au o adresă IP privată într-un mediu LAN. Adresa IP privată a fiecărui client din rețea este salvată 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.
- **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.

4.3.2 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.



Pentru a configura triggeringul de port:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > WAN > fila 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.
- **Protocol:** Selectați protocolul, TCP sau UDP.

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.

4.3.3 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, routerul 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.

Operation Mode: **Wireless router** Firmware Version: 3.0.0.4.376.3792 SSID: ASUS ASUS 5G

Internet Connection Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

WAN - Virtual Server / Port Forwarding

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 empty.

- 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 RT-AC1200'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 RT-AC1200's native FTP server.

Virtual Server / Port Forwarding FAQ

Basic Config

Enable Port Forwarding Yes No

Famous Server List

Famous Game List

FTP Server Port

Port Forwarding List (Max Limit : 32)

Service Name	Port Range	Local IP	Local Port	Protocol	Add / Delete
				TCP	+

No data in table.

Apply

Pentru a configura redirecționarea porturilor:

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

2. Configurați următoarele setări: Când ați terminat, faceți clic pe **Apply (Aplicare)**.

- **Activare redirecționare porturi:** Selectați **Yes (Da)** pentru a activa redirecționarea porturilor.
- **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 **4.2 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 aplicație realizează o conexiune de ieșire prin intermediul portului de declanșare.

4.3.4 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:

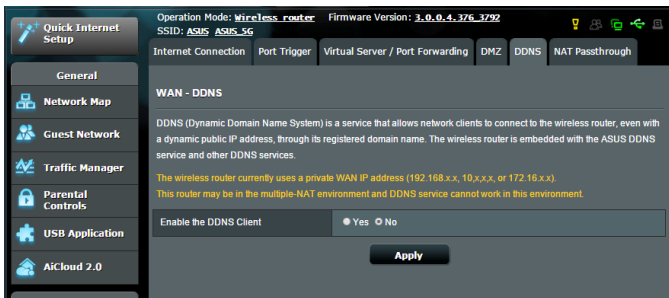
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > fila **DMZ**.
2. Configurați următoarele setări. Când ați terminat, faceți clic pe **Apply (Aplicare)**.
 - **Adresa IP a stației expuse:** Introduceți adresa IP pentru clientul din rețeaua LAN, client care va furniza 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)**.

4.3.5 DDNS

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



Pentru a configura DDNS:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > WAN > fila 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:

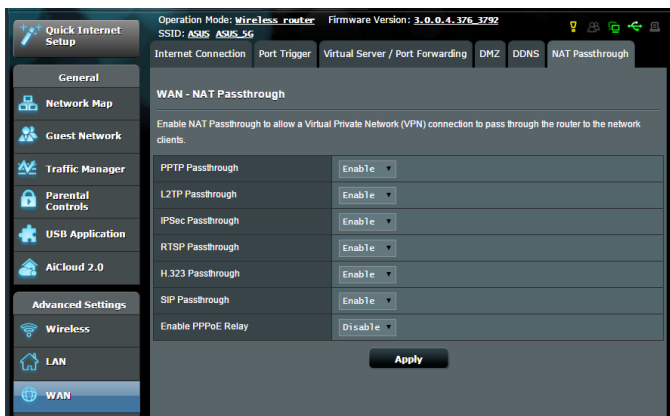
Serviciul DDNS nu va funcționa în următoarele condiții:

- 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.

4.3.6 NAT Passthrough (Trecere NAT)

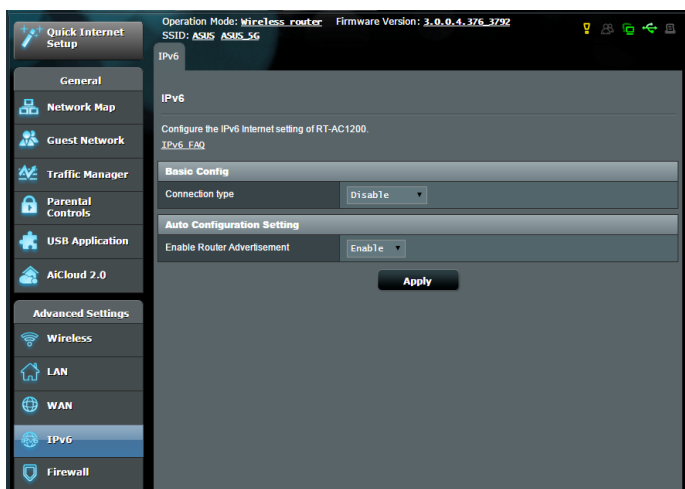
Parametrul NAT Passthrough (Trecere NAT) permite unei conexiuni aparținând unei rețele private virtuale să treacă prin ruter și să fie direcționată către clienții din rețea. Opțiunile PPTP Passthrough (Trecere PPTP), L2TP Passthrough (Trecere L2TP), IPsec Passthrough (Trecere IPsec) și RTSP Passthrough (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 > fila NAT Passthrough (Trecere NAT)**. Când ați terminat, faceți clic pe **Apply (Aplicare)**.



4.4 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.

4.5 Paravan de protecție

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

NOTĂ: Caracteristică de firewall este activată implicit.

4.5.1 Aspecte generale

Pentru a configura setările de bază pentru firewall:


1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Firewall > fila 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)**.

4.5.2 URL Filter (Filtru URL)

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

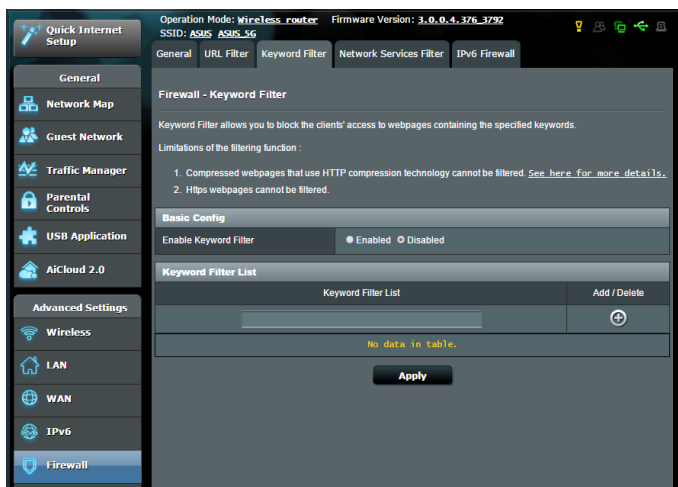
NOTĂ: Filtrul URL se bazează pe o interogare a serverului DNS. Dacă un client din rețea a accesat deja un site web precum <http://www.abcxxx.com>, atunci siteul web nu va fi blocat (siteurile web accesate în trecut sunt stocate într-o memorie cache a serverului DNS). Pentru a rezolva această problemă,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

4.5.3 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** > fila **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.

4.5.4 Network Services Filter (Filtru servicii 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.


The screenshot shows the Mikrotik WinBox interface for configuring the Network Services Filter. The left sidebar contains navigation options like General, Network Map, Guest Network, Traffic Manager, Parental Controls, USB Application, AiCloud 2.0, Advanced Settings, Wireless, LAN, WAN, IPv6, Firewall (selected), Administration, System Log, and Network Tools. The main content area is titled 'Firewall - Network Services Filter' and contains the following configuration details:

- Enable Network Services Filter:** Yes No
- Filter table type:** Black List
- Well-Known Applications:** User Defined
- Date to Enable LAN to WAN Filter:** Mon Tue Wed Thu Fri
- Time of Day to Enable LAN to WAN Filter:** 00 : 00 - 23 : 59
- Date to Enable LAN to WAN Filter:** Sat Sun
- Time of Day to Enable LAN to WAN Filter:** 00 : 00 - 23 : 59
- Filtered ICMP packet types:** (empty)

Below the configuration fields is a table titled 'Network Services Filter Table (Max Limit : 32)'. The table has columns for Source IP, Port Range, Destination IP, Port Range, Protocol, and Add / Delete. The current table is empty, showing 'No data in table.' at the bottom.

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	+

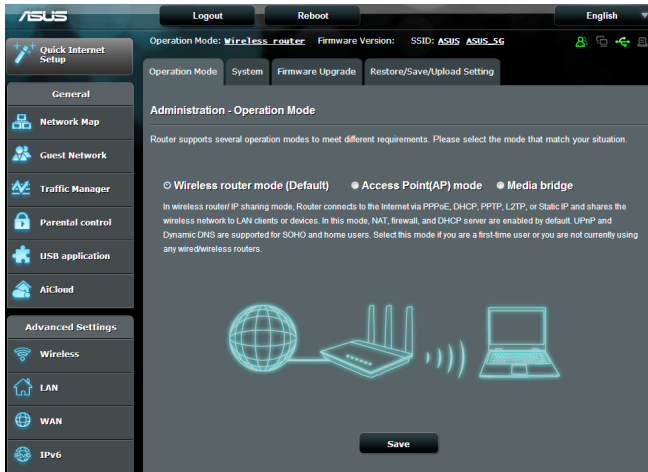
Pentru configurarea unui filtru de servicii de rețea:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **Firewall** > fila **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)**.

4.6 Administration (Administare)

4.6.1 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 (Administare) > fila 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.
3. Faceți clic pe **Apply (Aplicare)**.

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

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

4.6.3 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) >** fila **Firmware Upgrade (Upgrade firmware)**.
2. În câmpul **New Firmware File (Fișier firmware nou)**, faceți clic pe **Browse (Navigare)** 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 **5.2 Firmware Restoration (Restaurare firmware)**.

4.6.4 Refacerea/Salvarea/Încărcarea setărilor

Pentru a reface/salva/încărca setările:

1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Administration (Administrare) >** fila **Restore/Save/Upload Setting (Setări restaurare/salvare/încărcare)**.
2. Selectați sarcina pe care doriți s-o îndepliniți:
 - Pentru a reface setările inițiale din fabrică, faceți click pe **Restore (Refacere)** apoi click **OK** în mesajul de confirmare.
 - Pentru a salva setările curente de sistem, faceți clic pe **Save (Salvare)**, navigați la folderul în care intenționați să salvați fișierul și faceți clic pe **Save (Salvare)**.
 - Pentru a reface setarea sistemului anterior, click **Browse (Răsfoiește)** pentru a localiza fișierul sistemului pe care doriți să-l refaceți apoi faceți click pe **Upload (Încărcare)**.

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

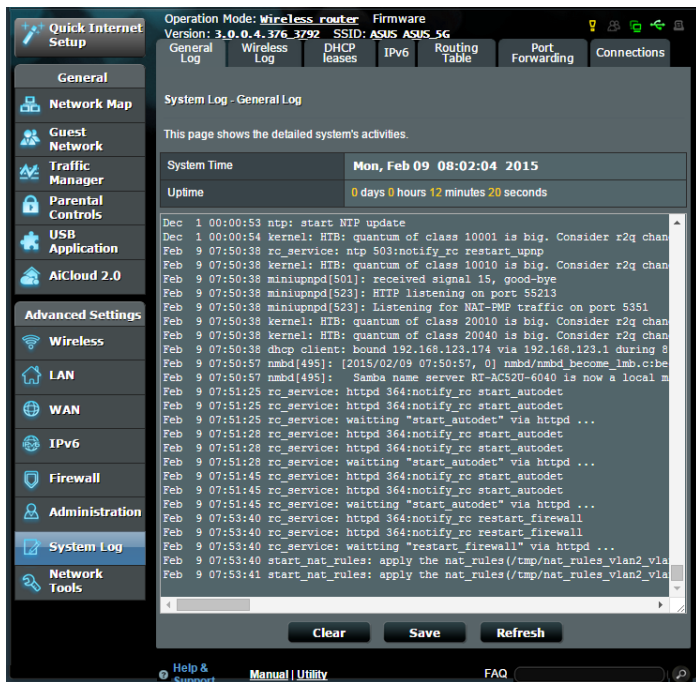
4.7 System Log (Jurnal de sistem)

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
 - Atribuirei DHCP
 - Jurnal wireless
 - Redirecționare porturi
 - Tabel direcționare



5 utilitățile

NOTE:

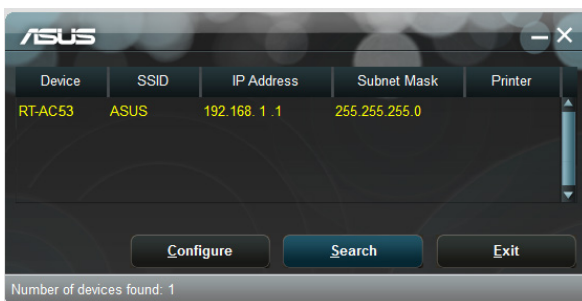
- Descărcați și instalați utilitățile routerului wireless de pe site-ul web ASUS:
 - Utilitarul Device Discovery, versiunea 2.0.0.0, poate fi descărcat de la adresa <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
 - Utilitarul Firmware Restoration, versiunea 1.9.0.4, poate fi descărcat de la adresa <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Utilitarul Windows Printer Utility, versiunea 1.0.5.5, poate fi descărcat de la adresa <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
- Utilitățile nu sunt acceptate în sistemul de operare MAC.

5.1 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

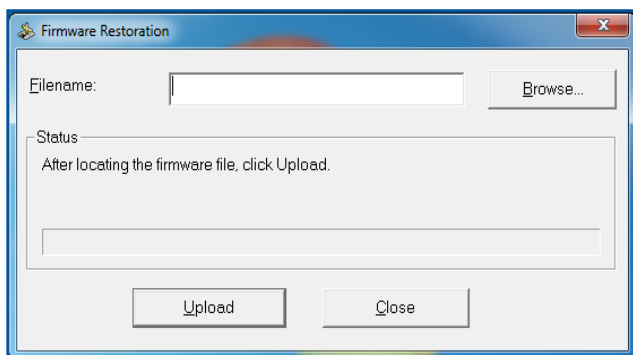
- De pe desktopul computerului dvs click **Start > All programs (Toate Programele) > ASUS Utility (Utilitară ASUS) > RT-AC53 Wireless Router (Router fără cablu RT-AC53) > Device Discovery (Detectare Dispozitiv)**.



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.

5.2 Refacerea softului integrat

Utilitarul Firmware Restoration (Restabilire 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 (Restabilire firmware).

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

6 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:

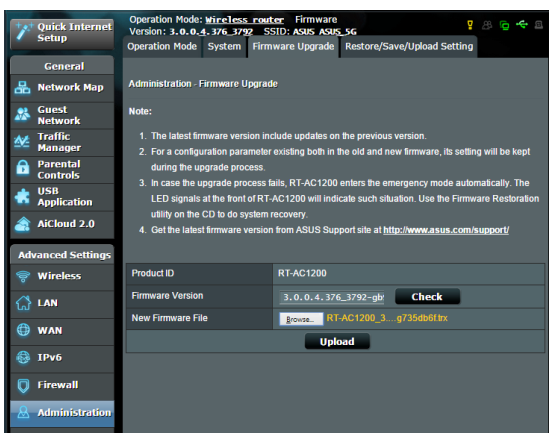
<http://support.asus.com/>. Aici puteți găsi mai multe informații despre produs, dar și detalii de contact pentru departamentul de asistență tehnică ASUS.

6.1 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) > fila Firmware Upgrade (Upgrade firmware)**. Faceți clic pe **Check (Verificare)** pentru a verifica dacă este disponibil cel mai recent firmware.



2. Dacă cel mai recent firmware este disponibil, accesați site-ul global ASUS, la adresa [http://www.asus.com/Networks/Wireless Routers/RTAC53/#download](http://www.asus.com/Networks/Wireless_Routers/RTAC53/#download), pentru a descărca cel mai recent firmware.
3. Din pagina **Firmware Upgrade (Upgrade firmware)**, faceți clic pe **Browse (Navigare)** 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.

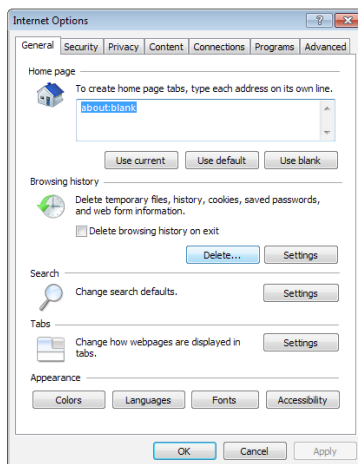
- Unii furnizori de servicii prin cablu necesită să utilizați adresa MAC a computerului care a fost înregistrat inițial în cont. Puteți vizualiza adresa MAC în interfața de utilizare web, pagina **Network Map (Hartă rețea) > Clients (Clienți)**, după care poziționați cursorul mouseului deasupra dispozitivului dvs. afișat în **Client Status (Stare client)**.



6.2 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 8, urmați acești pași:
 1. Lansați Internet Explorer 8, apoi faceți clic pe **Tools (Instrumente) > Internet Options (Opțiuni Internet)**.
 2. În fila **General**, sub **Browsing history (Istoric navigare)**, faceți clic pe **Delete... (Ștergere...)**, selectați **Temporary Internet Files (Fișiere Internet temporare)** și **Cookies (Module cookie)**, iar apoi faceți clic pe **Delete (Ștergere)**.



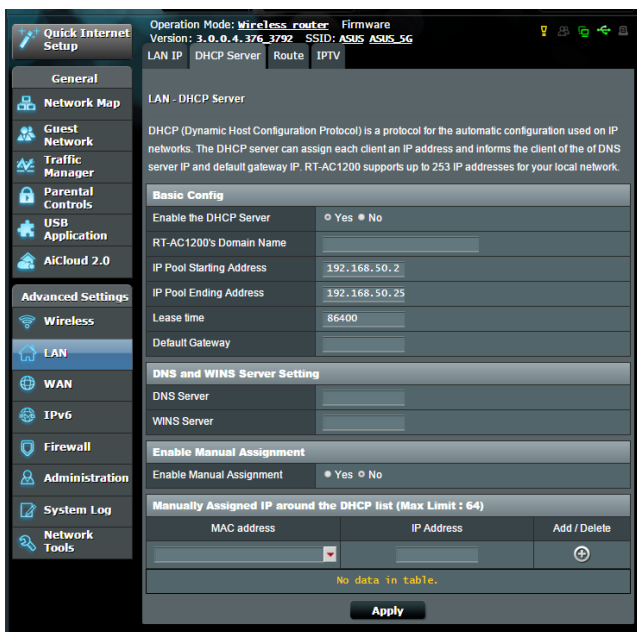
NOTE:

- 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.

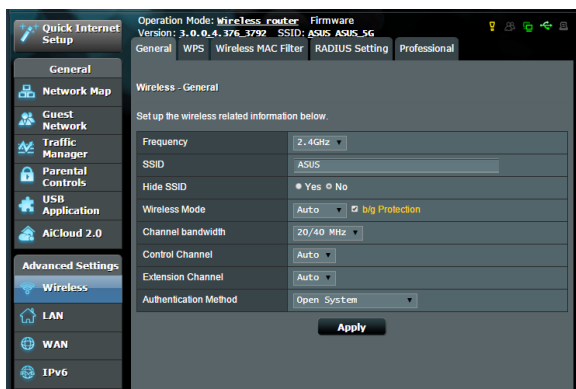
Clientul nu poate stabili o legătura wireless cu routerul.

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.

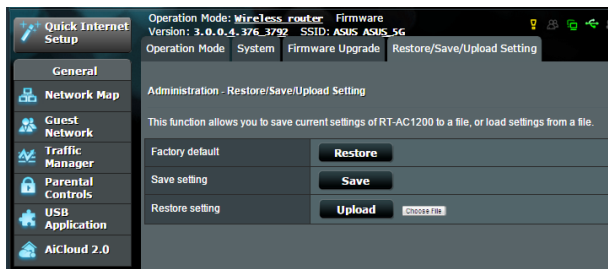
- **În afara razei:**
 - Puneți routerul mai aproape de clientul wireless.
 - Încercați să reglați antenele routerului pentru a obține direcția de propagare optimă, după cum se descrie în secțiunea **1.4 Positioning your router (Poziționarea routerului)**.
- **Serverul DHCP a fost dezactivat:**
 1. Lansați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



- Numele rețelei (SSID) este ascuns. Dacă dispozitivul dvs. poate găsi nume de rețea (SSID) ale altor rutere, dar nu și numele de rețea al ruterului dvs., mergeți la **Advanced Settings (Setări avansate) > Wireless > General**, 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)**.

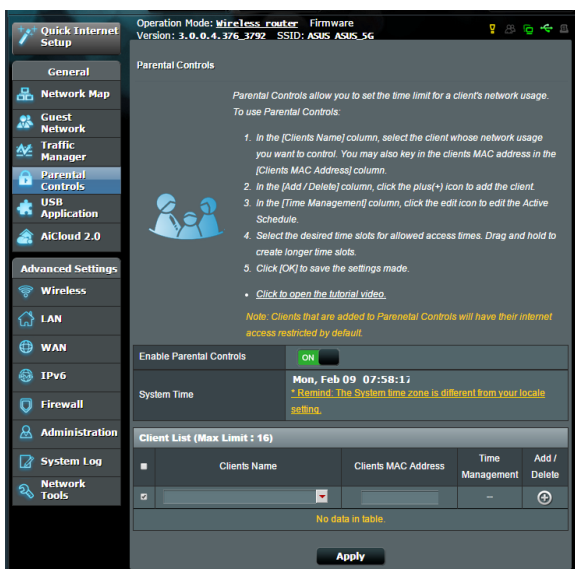


Internetul nu este accesibil

- 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 > 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 > Parental Control (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)**.

Următoarele sunt setări inițiale de fabrică:

Nume utilizator:	admin
Parolă:	admin
Adresă IP:	http://router.asus.com
SSID (2.4GHz):	Consultați eticheta din partea de jos a routerului
SSID (5GHz):	Consultați eticheta din partea de jos a routerului

Upgradeul de firmware a eșuat.

Lansați modul de recuperare înainte de a utiliza utilitarul Firmware Restoration (Restaurare firmware). Consultați secțiunea **5.2**

Firmware Restoration (Restaurare firmware) pentru a afla cum să utilizați utilitarul Firmware Restoration (Restaurare firmware).

Nu se poate accesa interfața de utilizare web

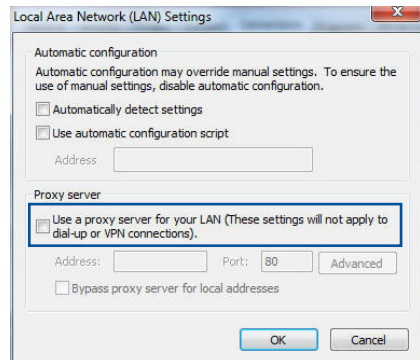
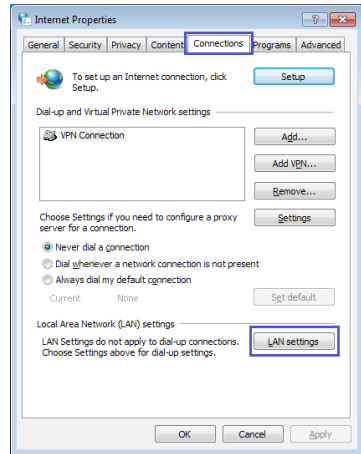
Înainte de a configura ruterul fără fir, efectuați pașii descriși în această secțiune pentru computerul gazdă și clienții de rețea.

A. Dezactivați serverul proxy, dacă este activat.

Notă: Capturile de ecran afișate au fost realizate pe sistemul de operare Windows® 7. Este posibil ca pașii și opțiunile să difere pentru sistemele de operare Windows® 8 și Windows® 8.1.

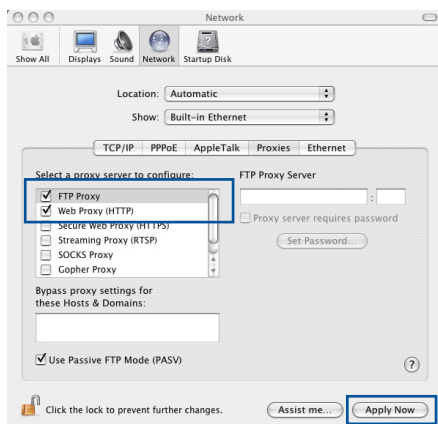
Windows® 7/8

1. Faceți clic pe **Start > Internet Explorer** pentru a lansa browserul web.
2. Faceți clic pe **Tools (Instrumente) > Internet options (Opțiuni Internet) > fila 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))**.



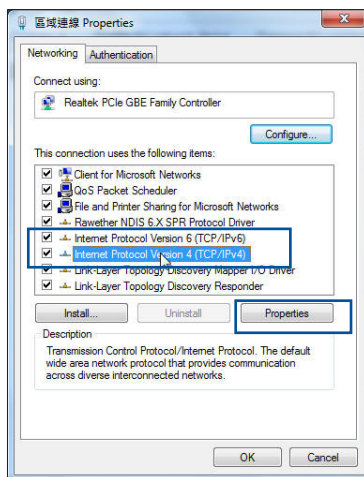
3. Faceți clic pe **Apply Now (Se aplică acum)** când ați terminat.

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®7/8

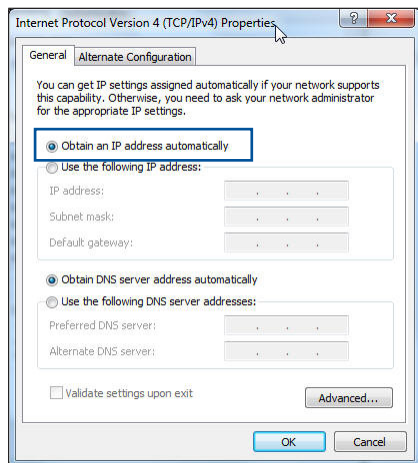
1. Faceți clic pe **Start > Control Panel (Panou de control) > Network and Internet (Rețea și Internet) > Network and Sharing Center (Centru de rețea și partajare) > Manage network connections (Gestionare conexiuni rețea)**.
2. Selectați **Internet Protocol Version 4 (TCP/IPv4) (Protocol Internet versiunea 4 (TCP/IPv4))** sau **Internet Protocol Version 6 (TCP/IPv6) (Protocol Internet versiunea 6 (TCP/IPv6))**, apoi faceți clic pe **Properties (Proprietăți)**.



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

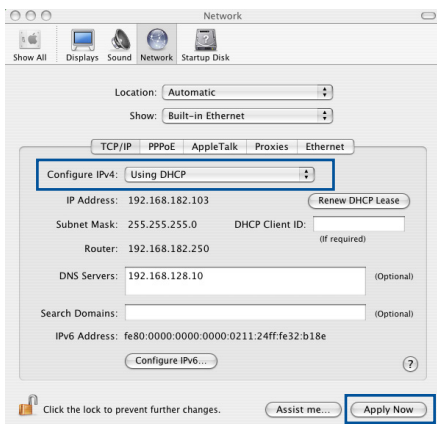
Pentru a obține automat setările IP IPv6, bifați **Obtain an IPv6 address automatically (Se obține automat o adresă IPv6).**

4. 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 fila **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.

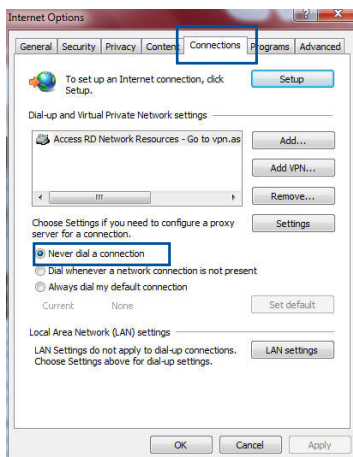


Notă: Consultați caracteristica de ajutor și asistență a sistemului de operare pentru detalii despre configurarea setărilor TCP/IP ale computerului.

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

Windows® 7/8

1. Faceți clic pe **Start > Internet Explorer** pentru a lansa browserul web.
2. Faceți clic pe **Tools (Instrumente) > Internet options (Opțiuni Internet) > fila 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

Anunțuri

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <http://csr.asus.com/english/Takeback.htm> for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

<http://csr.asus.com/english/index.aspx>

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection

against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT! This device within the 5.15 ~ 5.25 GHz is restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

CAUTION: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: <http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng>

Additional Canadian information on RF exposure also can be found at the following web: <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html>

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes:

(1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

電磁波曝露量 MPE 標準值 1mWcm^2 ，送測產品實測值為：。

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

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BİL GİSAYAR SAN. VE TİC. A.S.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/İSTANBUL

CİZGİ Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

Address: CEMAL SURURI CD. HALİM MERİC İS MERKEZİ
No: 15/C D:5-6 34394 MECİDİYEKOY/
İSTANBUL

KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİŞ TİC. A.S.

Tel. No.: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARİGAZİ,
SANCAKTEPE İSTANBUL

AEEE Yönetmeliğine Uygundur.

Informații de contact despre producător

ASUSTeK COMPUTER INC.

Adresa companiei 4F, No. 150, Li-Te Road, Peitou, Taipei 112, Taiwan
Telefon +886-2-2894-3447
Fax +886-2-2890-7798
Site web www.asus.com/

Asistență tehnică

Telefon +86-21-38429911
Fax +86-21-5866-8722, ext. 9101#
Asistență online <http://qr.asus.com/techserv>

ASUS COMPUTER INTERNATIONAL (America)

Adresa companiei 800 Corporate Way, Fremont, CA 94539, USA
Telefon +1-510-739-3777
Fax +1-510-608-4555
Site web <http://www.asus.com/us/>

Asistență tehnică

Asistență fax +1-812-284-0883
Telefon +1-812-282-2787
Asistență online <http://qr.asus.com/techserv>

ASUS COMPUTER GmbH (Germany și Austria)

Adresa companiei Harkort Str. 21-23, D40880 Ratingen, Germany
Fax +49-2102-959931
Site web <http://www.asus.com/de>
Contact online <http://eu-rma.asus.com/sales>

Asistență tehnică

Telefon +49-2102-5789555
Asistență fax +49-2102-959911
Asistență online <http://qr.asus.com/techserv>

Informații privind liniile telefonice de asistență globale

Region	Country	Hotline Number	Service Hours	
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	France	0033-170949400	09:00-18:00 Mon-Fri	
	Germany	0049-1805010920		
		0049-1805010923 (component support)		09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
		0049-2102959911 (Fax)		
	Hungary	0036-15054561	09:00-17:30 Mon-Fri	
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Austria	0043-820240513	09:00-18:00 Mon-Fri	
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri	
	Belgium	0032-78150231	09:00-17:00 Mon-Fri	
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri	
	Sweden	+46-858769407	09:00-18:00 Mon-Fri	
	Finland	00358-969379690	10:00-19:00 Mon-Fri	
	Denmark	0045-38322943	09:00-18:00 Mon-Fri	
	Poland	0048-225718040	08:30-17:30 Mon-Fri	
	Spain	0034-902889688	09:00-18:00 Mon-Fri	
	Portugal	00351-707500310	09:00-18:00 Mon-Fri	
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri	
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri	
Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri		
Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri		
Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri		
United Kingdom	+44-1442265548	09:00-17:00 Mon-Fri		
Ireland	0035-31890719918	09:00-17:00 Mon-Fri		
Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri		
Ukraine	0038-0445457727	09:00-18:00 Mon-Fri		

Informații privind liniile telefonice de asistență globale

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
	Korea	0081-570783886 (Non-Toll Free)	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917 0065-67203835 (Repair Status Only)	11:00-19:00 Mon-Fri
			11:00-19:00 Mon-Fri
			11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
09:00-21:00 Mon-Sun			
Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri	
		9:30 – 12:00 Sat	
Vietnam	1900-555581	08:00-12:00	
		13:30-17:30 Mon-Sat	
Hong Kong	00852-35824770	10:00-19:00 Mon-Sat	
Americas	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
	Canada		9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri
08:00-15:00 CST Sat			

Informații privind liniile telefonice de asistență globale

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800 *9770/00972-35598555	08:00-17:00 Sun-Thu 08:30-17:30 Sun-Thu
Balkan Countries	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
Slovenia	00368-59045400 00368-59045401	08:00-16:00 Mon-Fri	
Baltic Countries	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTE: For more information, visit the ASUS support site at:
<http://support.asus.com>

SUPPORT HOTLINE

USA/ CANADA

Hotline Number: 1-812-282-2787

Language: English

Availability: **Mon. to Fri.**
8:30-12:00am EST
(5:30am-9:00pm PST)

Sat. to Sun.
9:00am-6:00pm EST
(6:00am-3:00pm PST)

BRAZIL

Hotline Number: 4003 0988
(Capital) / 0800 880 0988 (demais localidades)

Language: Portuguese

Availability: **Mon. to Fri.**
9:00am-18:00

Manufacturer

ASUSTeK Computer Inc.

Tel: +886-2-2894-3447

Address: No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN

Authorised representative in Europe

ASUS Computer GmbH

Address: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

Authorised distributors in Turkey

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel: +90 212 3567070 Address: CEMAL SURURI CD. HALIM MERIC IS MERKEZI

No: 15/C D:5-6 34394 MECIDIYEKOY/ ISTANBUL

KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİS TIC. A.S.

Tel: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZI, SANCAKTEPE ISTANBUL