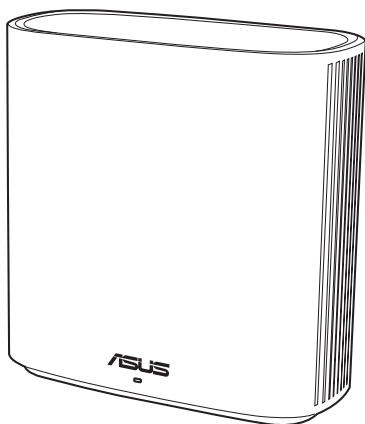


Ghidul utilizatorului

ASUS ZenWiFi XD6

**AX5400 Router Wi-Fi cu două benzi de
frecvență**

Model: XD6



ASUS
IN SEARCH OF INCREDIBLE

RO19060
Prima ediție
Octombrie 2021

Copyright © 2021 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	8
1.5	Cerințe pentru configurare	9
1.6	Configurarea ruterului	10
1.6.1	Conexiune cu fir	11
1.6.2	Conexiune wireless	12

2 Inițializarea

2.1	Conectarea la interfața Web GUI	13
2.2	Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată	14
2.3	Conectarea la rețeaua dvs. wireless	18

3 Configurarea setărilor generale

3.1	Utilizarea hărții rețelei	19
3.1.1	Configurarea setărilor de securitate pentru rețeaua wireless	20
3.1.2	Administrarea clienților din rețea	21
3.2	Crearea rețelei de vizitatori	22
3.3	AiProtection	24
3.3.1	Funcția Network Protection (Protecție rețea)	25
3.3.2	Configurarea controlului parental	28
3.4	Utilizarea funcției Traffic Manager (Manager trafic)	30
3.4.1	Gestionarea lățimii de bandă pentru funcția QoS (Calitatea serviciului)	30

Sumar

4 Configurarea setărilor Complexe

4.1	Wireless.....	33
4.1.1	Aspecte generale	33
4.1.2	WPS	36
4.1.3	Punte.....	38
4.1.4	Wireless MAC Filter (Filtru MAC wireless)	40
4.1.5	Setarea RADIUS.....	41
4.1.6	Professional (Profesional)	42
4.2	LAN.....	45
4.2.1	LAN IP	45
4.2.2	Serverului DHCP	46
4.2.3	Rută.....	48
4.2.4	IPTV	49
4.3	WAN	50
4.3.1	Conexiune la Internet.....	50
4.3.2	Triggering de port.....	53
4.3.3	Server virtual/Redirecționare porturi	55
4.3.4	DMZ.....	58
4.3.5	DDNS	59
4.3.6	NAT Passthrough (Trecere NAT).....	60
4.4	IPv6.....	61
4.5	Paravan de protecție.....	62
4.5.1	Aspecte generale	62
4.5.2	URL Filter (Filtru URL)	62
4.5.3	Keyword filter (Filtru cuvinte cheie)	63
4.5.4	Network Services Filter (Filtru servicii rețea)	64
4.6	Administration (Administrare).....	66
4.6.1	Operation mode (Mod de funcționare)	66
4.6.2	System (Sistem).....	67
4.6.3	Actualizarea softului integrat	69

Sumar

4.6.4	Refacerea/Salvarea/Încărcarea setărilor.....	69
4.7	System Log (Jurnal de sistem)	70

5 Utilităților

5.1	Detectarea Dispozitivului.....	71
5.2	Refacerea softului integrat.....	72

6 Remedierea defecțiunilor

6.1	Depanarea de bază.....	74
6.2	Întrebări frecvente	77

Anexă

Notices	86
Service și Asistență	123

1 Cum să vă cunoașteți routerul

1.1 Bine ați venit!

Vă mulțumim pentru achiziționarea unui ruter wireless ASUS, model ZenWiFi XD6!

Acest ruter ZenWiFi XD6 ultrasubțire și plin de stil dispune de: o bandă duală de 2,4 GHz și 5 GHz pentru redarea în flux HD, server SMB, server UPnP AV și server FTP pentru partajare de fișiere 24 de ore/7 zile; capacitate de administrare a până la 300 000 de sesiuni; tehnologie de rețea Green de la ASUS, care asigură până la 70% dintre soluțiile de economisire a energiei.

1.2 Conținutul pachetului

- | | |
|---|---|
| <input checked="" type="checkbox"/> Router fără cablu ZenWiFi XD6 | <input checked="" type="checkbox"/> Cablu RJ45 |
| <input checked="" type="checkbox"/> Adaptor de alimentare | <input checked="" type="checkbox"/> Ghid rapid de pornire |

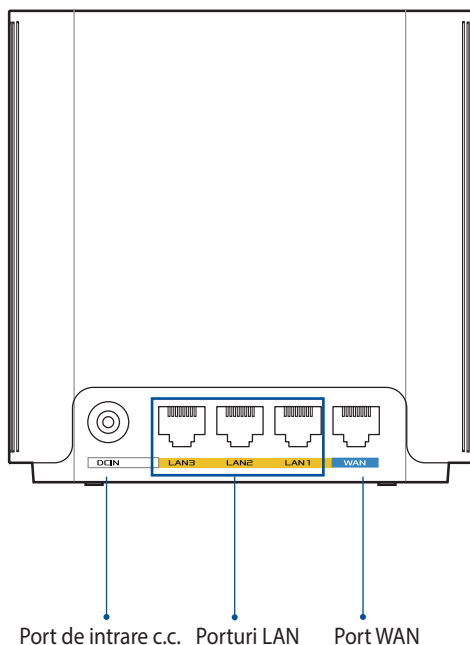
NOTE:

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

1.3 Ruter wireless

- 1 Conectați adaptorul la portul de intrare c.c.
- 2 LED-ul de alimentare luminează atunci când hardware-ul este pregătit.

Explicații pentru butoane și porturi



Port WAN

Conectați modemul optic la acest port cu un cablu de rețea.

Porturi LAN

Conectați PC-ul la unul dintre aceste porturi LAN cu un cablu de rețea.

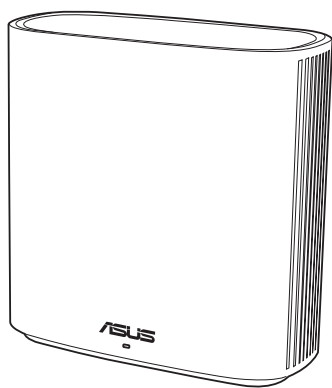
Specificații

Adaptor de alimentare c.c.	Ieșire c.c.: +12 V cu curent max. de 2A		
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.



1.5 Cerințe pentru configurare

Pentru a vă configura rețeaua, aveți nevoie de unul sau de două computere care să întrunească următoarele cerințe de sistem:

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

NOTĂ:

- 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.
-

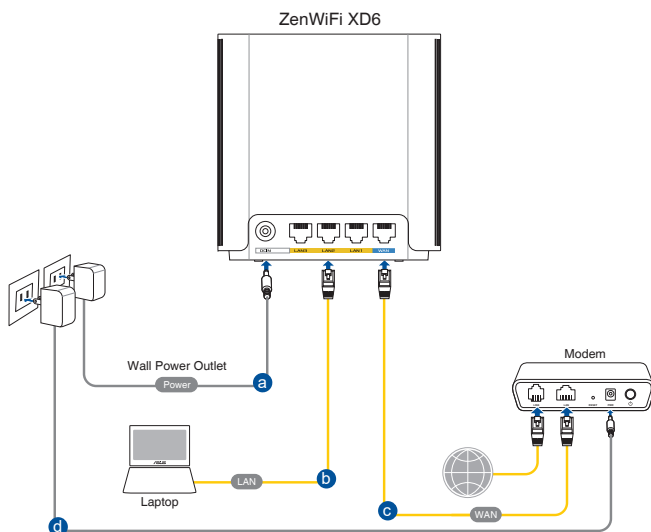
1.6 Configurarea ruterului

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

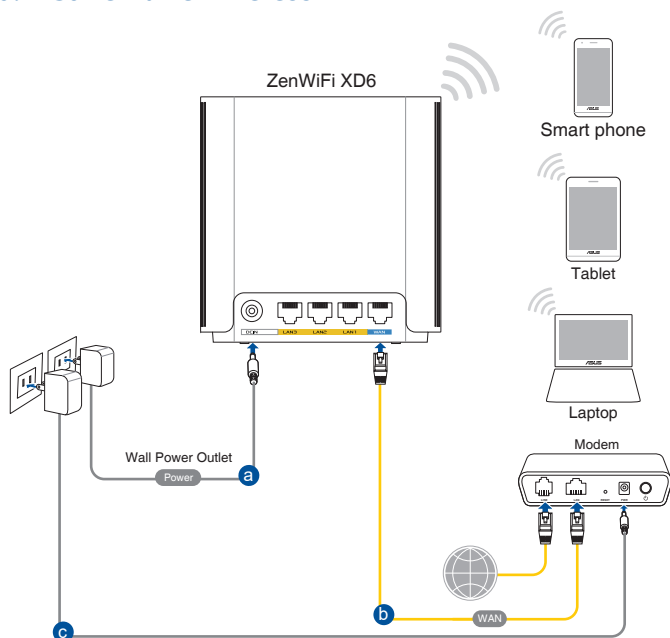
NOTĂ: Puteți folosi un cablu de conexiune directă sau un cablu crossover (inversor) pentru conexiunea cu fir.



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..
2. Utilizând cablul de rețea inclus, conectați computerul la portul LAN al ruterului fără fir.
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..

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..
2. Utilizând cablul de rețea inclus, conectați modemul la portul WAN al ruterului fără fir.
3. Introduceți adaptorul de c.a. al modemului în portul de intrare c.c..
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 Inițierea

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 accesați <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).

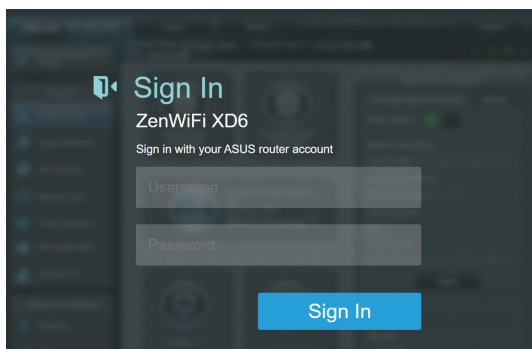
2.2 Configurarea rapidă a conexiunii la Internet (QIS) cu detectare automată

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.



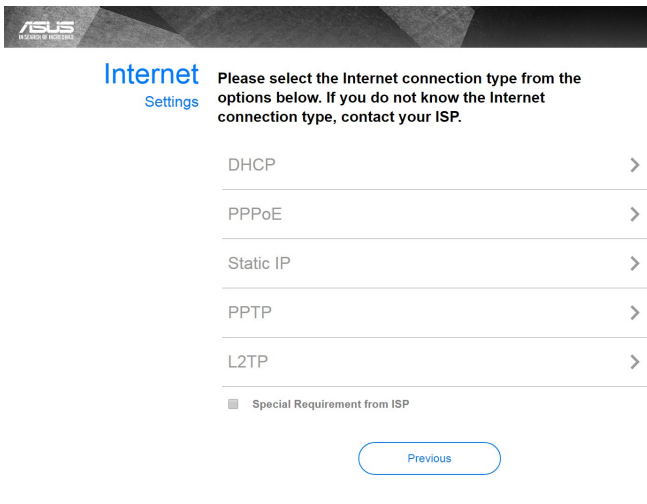
NOTE:

- Pentru detalii legate de schimbarea numelui de utilizator și parolei ruterului dvs. wireless, consultați secțiunea **4.6.2 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.

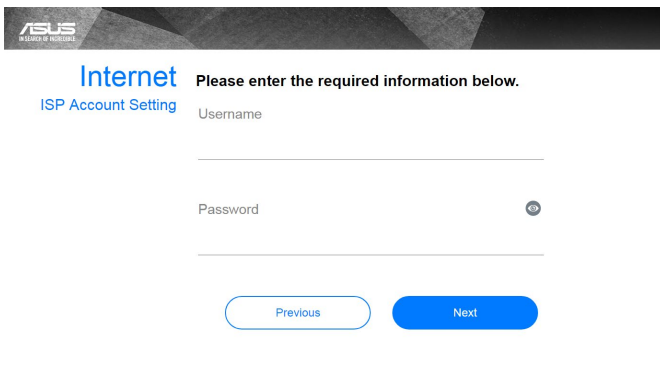
IMPORTANT! Obțineți informațiile necesare referitoare la tipul de conexiune la Internet de la ISP-ul dvs.

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



The screenshot shows the 'Internet Settings' page in the ASUS router interface. The title is 'Internet Settings'. Below the title, there is a message: 'Please select the Internet connection type from the options below. If you do not know the Internet connection type, contact your ISP.' There are five radio button options: 'DHCP', 'PPPoE', 'Static IP', 'PPTP', and 'L2TP'. Each option has a right-pointing arrow. Below these options is a checkbox labeled 'Special Requirement from ISP'. At the bottom of the page is a 'Previous' button.

pentru modurile de conectare PPPoE, PPTP și L2TP



The screenshot shows the 'Internet Account Setting' page in the ASUS router interface. The title is 'Internet Account Setting'. Below the title, there is a message: 'Please enter the required information below.' There are two input fields: 'Username' and 'Password'. The 'Password' field has a toggle icon to its right. At the bottom of the page are two buttons: 'Previous' and 'Next'.

pentru IP static

ASUS
IN SEARCH OF INCREDIBLE

Internet

Static IP

Static IP allows your PC to use a fixed IP address provided by your ISP.

IP Address
192.168.1.215

Subnet Mask
255.255.255.0

Default Gateway
192.168.1.1

DNS Server1
192.168.1.1

DNS Server2

Previous Next

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.

Wireless
Settings

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

Network Name (SSID)

Wireless Security ⓘ

Separate 2.4GHz and 5GHz

NOTĂ: Dacă doriți să atribuiți SSID-uri diferite pentru conexiunile wireless de 2,4 GHz și 5 GHz, bifați **Separate 2,4GHz and 5 GHz (2,4 GHz și 5 GHz separate)**.

Wireless
Settings

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

2.4GHz Network Name (SSID)

2.4GHz Wireless Security ⓘ

5GHz-1 Network Name (SSID)

5GHz-1 Wireless Security ⓘ

Separate 2.4GHz and 5GHz

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 și să monitorizați dispozitivul USB.

The screenshot displays the ASUS router's web management interface. The top navigation bar includes 'Quick Internet Setup', 'Operation Mode: **wireless_router**', 'Firmware Version: **3.0.0.4_385_43373**', and 'SSID: **980030**'. The left sidebar contains menu items for 'General' (Network Map, AiMesh, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer) and 'Advanced Settings' (Wireless, LAN, WAN, Amazon Alexa, IPv6, VPN, Firewall, Administration, System Log, Network Tools). The main content area is divided into three sections: 'Internet status' (Connected, WAN IP: 192.168.123.23, DNS: 8.8.8), 'Security level: WPA2-Personal' (with a lock icon), and 'Clients: 2' (with a 'View List' button) and 'AiMesh Nodes: 1'. On the right, the 'System Status' panel shows 'Wireless Status' with 'Smart Connect' set to 'Dual-Band Smart Connect' and 'Dual-Band Smart Connect' settings including 'Network Name (SSID): 000030', 'Authentication Method: WPA2-Personal', 'WPA Encryption: AES', and 'WPA-PSK key: 88880000'. An 'Apply' button is located below these settings. The footer contains links for 'Help & Support', 'Manual', 'Product Registration', 'Feedback', and 'FAQ', along with the copyright notice '© 2020 ASUS/ASUS Computer Inc. All rights reserved.'

3.1.1 Configurarea setărilor de securitate pentru rețeaua wireless

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

Pentru a configura setările de securitate pentru rețeaua wireless:

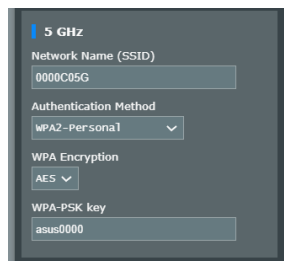
1. Din panoul de navigare, mergeți la **General > Network Map (Hartă rețea)**.
2. Din ecranul Network Map (Hartă rețea) selectați pictograma **System status (Stare sistem)** pentru afișarea setărilor de securitate wireless, cum sunt de exemplu SSID, nivel de securitate și setările de criptare.

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

Setări de securitate pentru banda 2,4 GHz



Setări de securitate pentru banda 5 GHz

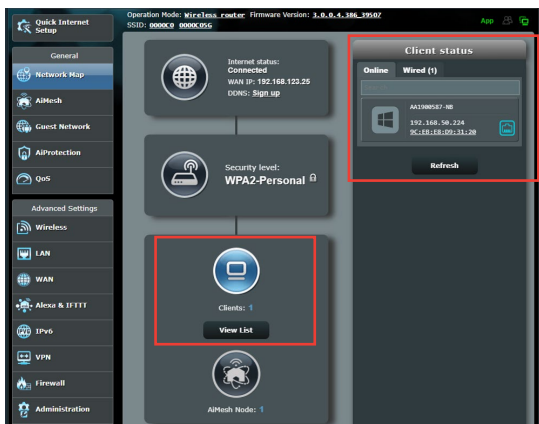


3. În câmpul **Wireless name (SSID) (Nume rețea wireless (SSID))** tastați un nume unic pentru rețeaua dvs. wireless.
4. Din lista verticală **WEP Encryption (Criptare WEP)** selectați metoda de criptare pentru rețeaua dvs. wireless.

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. Tastați cheia de acces de securitate.
6. 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 (Blocare)**.

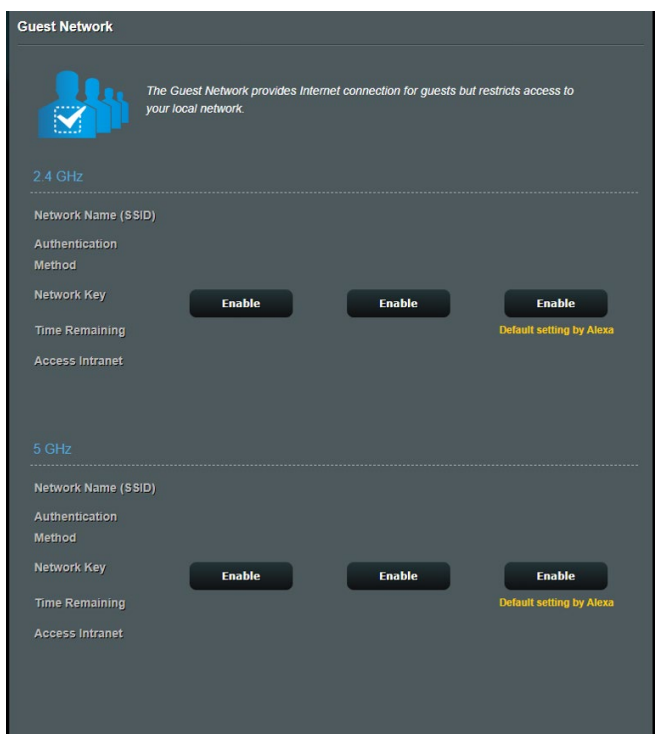
3.2 Crearea rețelei de vizitatori

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.

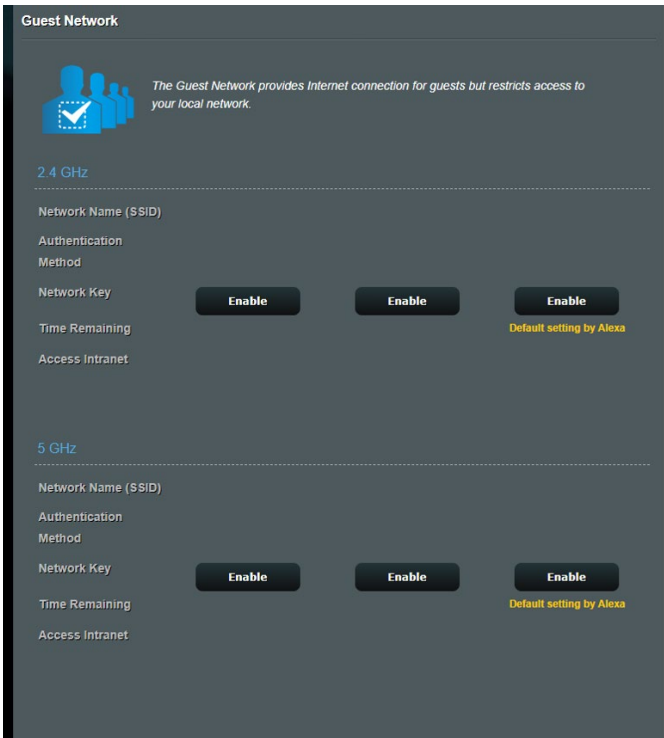
NOTĂ: ZenWiFi XD6 acceptă până la nouă SSID-uri.

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 sau de 5GHz pentru rețeaua de vizitatori pe care doriți să o creați.
3. Faceți clic pe **Enable (Activare)**.



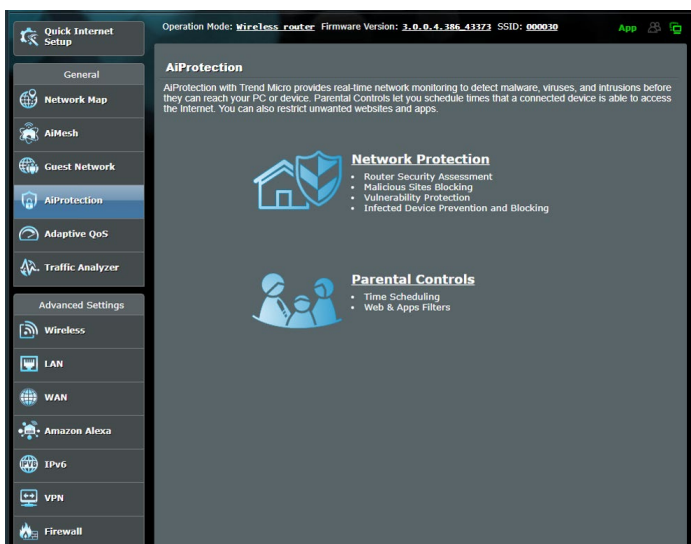
4. Pentru a modifica setările unui invitat, faceți clic pe setările invitatului pe care doriți să le modificați. Faceți clic pe **Remove (Eliminare)** pentru a șterge setările invitatului.
5. Atribuiți un nume pentru rețeaua temporară în câmpul Network Name (SSID) (Nume rețea (SSID)).



6. Selectați o opțiune Authentication Method (Metodă de autentificare).
7. Dacă selectați o metodă de autentificare de tip WPA, selectați o opțiune WPAEncryption.
8. Specificați o valoare pentru Access time (Timp de acces) sau faceți clic pe **Limitless (Nelimitat)**.
9. Selectați **Disable (Dezactivare)** sau **Enable (Activare)** pe elementul **Access Intranet (Acces la Intranet)**.
10. Când ați terminat, faceți clic pe **Apply (Aplicare)**.

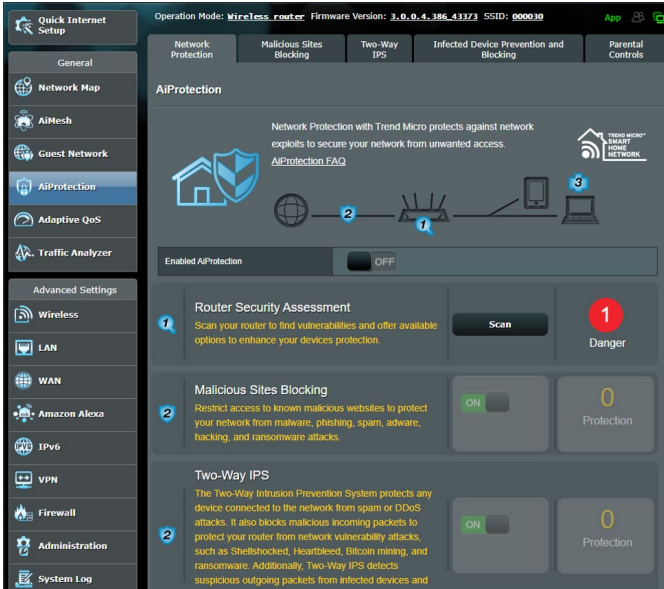
3.3 AiProtection

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



3.3.1 Funcția Network Protection (Protecție rețea)

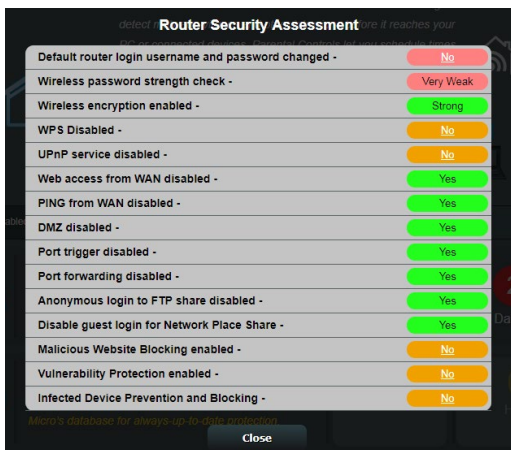
Funcția Network Protection (Protecție rețea) previne abuzarea rețelei și securizează rețeaua împotriva accesului nedorit.



Configurarea funcției Network Protection (Protecție rețea) Pentru a configura funcția Network Protection (Protecție rețea):

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

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



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

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

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

- b. Din pagina cu setări de securitate a elementului respectiv, configurați și efectuați modificările necesare și faceți clic pe **Apply (Se aplică)** când terminați.
 - c. Reveniți la pagina **Router Security Assessment (Evaluare securitate router)** și faceți clic pe **Close (Închidere)** pentru a ieși din pagină.
5. Pentru a configura în mod automat setările de securitate, faceți clic pe **Secure Your Router (Securizați-vă routerul)**;
6. Când apare un mesaj, faceți clic pe **OK**.
-

Malicious Sites Blocking (Blocare site-uri rău intenționate)

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

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

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

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

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

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

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

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

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

Pentru a configura funcția Alert Preference (Preferință alerte):

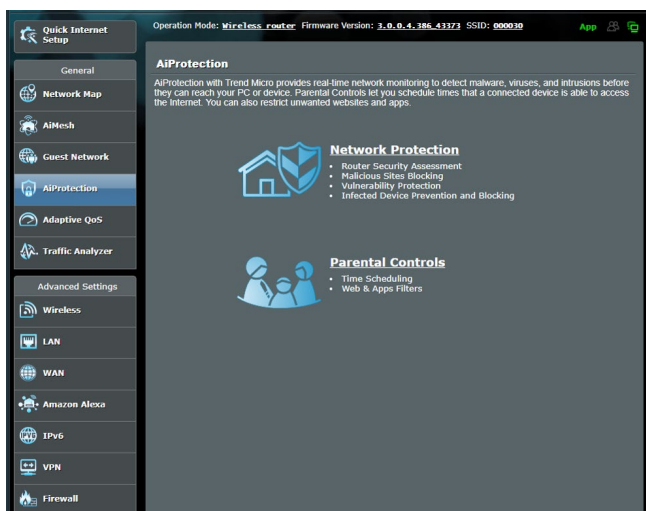
1. Din panoul **Infected Device Prevention and Blocking (Prevenire și blocare dispozitiv infectat)**, faceți clic pe **Alert Preference (Preferință alerte)**.
2. Selectați sau introduceți manual furnizorul de servicii e-mail, contul de e-mail și parola și apoi faceți clic pe **Apply (Se aplică)**.

3.3.2 Configurarea controlului parental

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

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

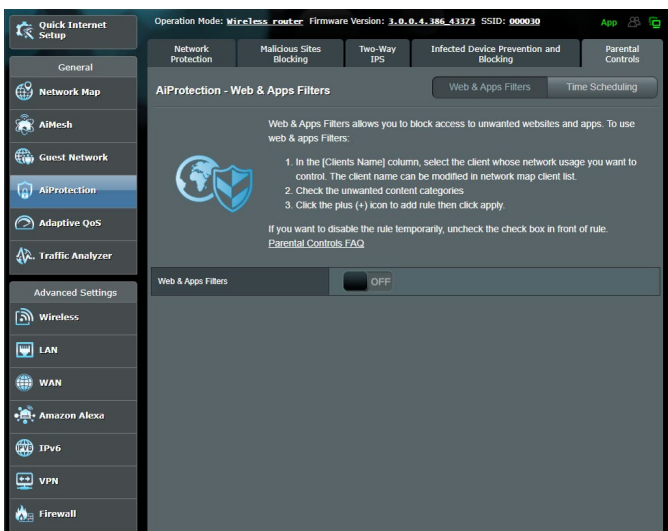
1. Din panoul de navigare, mergeți la **General > AiProtection**.
2. Din pagina principală **AiProtection**, faceți clic pe fila **Parental Controls (Controale parentale)**.



Time Scheduling (Programare în timp)

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

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



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

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

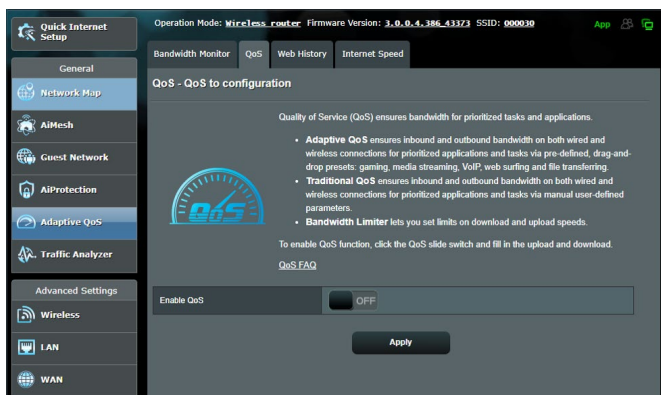
NOTĂ: De asemenea, puteți să introduceți adresa MAC a clientului în coloana **Client MAC Address (Adresă MAC client)**. Asigurați-vă că numele clientului nu conține caractere speciale sau spații, deoarece acest lucru poate face ca ruterul să funcționeze anormal.

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

3.4 Utilizarea funcției Traffic Manager (Manager trafic)

3.4.1 Gestionarea lățimii de bandă pentru funcția QoS (Calitatea serviciului)

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



Pentru a seta prioritatea lățimii de bandă:

1. Din panoul de navigare, mergeți la **General > Adaptive QoS (QoS adaptiv) > 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 parametrii **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 aceluiși 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”, „>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.

4 Configurarea setărilor Complexe

4.1 Wireless

4.1.1 Aspecte generale

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

The screenshot shows the 'Wireless - General' configuration page in a router's web interface. The interface is dark-themed with a sidebar on the left containing navigation options like 'Quick Internet Setup', 'General', 'Network Map', 'AiMesh', 'Guest Network', 'AiProtection', 'Adaptive QoS', 'Traffic Analyzer', 'Advanced Settings', 'Wireless', 'LAN', 'WAN', 'Amazon Alexa', 'IPv6', 'VPN', 'Firewall', 'Administration', 'System Log', and 'Network Tools'. The 'Wireless' option is selected and highlighted in blue. The main content area is titled 'Wireless - General' and contains the following settings:

- Operation Mode: **Wireless router** | Firmware Version: **3.0.0.4_386_43373** | SSID: **000030**
- General | WPS | WDS | Wireless MAC Filter | RADIUS Setting | Professional | Roaming Block List
- Set up the wireless related information below.
- Enable Smart Connect: **ON** | [Smart Connect Rule](#)
- Smart Connect: **Dual-Band Smart Connect (2.4 GHz and 5 GHz)**
- Network Name (SSID): **000030**
- Hide SSID: **Yes** (selected) | No
- Wireless Mode: **Auto**
- 802.11ax / WiFi 6 mode: **Enable** | If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check [FAQ](#)
- WiFi Agile Multiband: **Disable**
- Target Wake Time: **Disable**
- Authentication Method: **WPA2-Personal**
- WPA Encryption: **AES**
- WPA Pre-Shared Key: **axus0000** | **Weak**
- Protected Management Frames: **Disable**
- Group Key Rotation Interval: **3600**
- 2.4 GHz**
 - Channel bandwidth: **20/40 MHz**
 - Control Channel: **Auto** | Current Control Channel: **8**
 - Auto select channel including channel 12, 13
 - Extension Channel: **Auto**
- 5 GHz**
 - Channel bandwidth: **20/40/80 MHz** | Enable 160 MHz
 - Control Channel: **Auto** | Current Control Channel: **116**
 - Auto select channel including DFS channels
 - Extension Channel: **Auto**

At the bottom of the configuration area is an **Apply** button. At the very bottom of the page, there are links for [Help & Support](#), [Manual](#), [Product Registration](#), [Feedback](#), and an **FAQ** search box.

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 oricare din aceste lățimi de bandă pentru a obține viteze de transmitere mai mari:
 - 40 MHz:** Selectați această lățime de bandă pentru a maximiza randamentul rețelei wireless.
 - 20 MHz (implicit):** Selectați această lățime de bandă dacă întâmpinați probleme cu conexiunea wireless.
7. Selectați canalul de funcționare pentru ruterul dvs. wireless. Selectați **Auto (Automat)** pentru a permite ruterului wireless să selecteze automat canalul care are cele mai puține interferențe.
8. Selectați oricare dintre aceste metode de autentificare:
 - **Sistem deschis:** Această opțiune nu oferă niciun tip de securitate.
 - **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.
 - **Radius cu 802.1x**

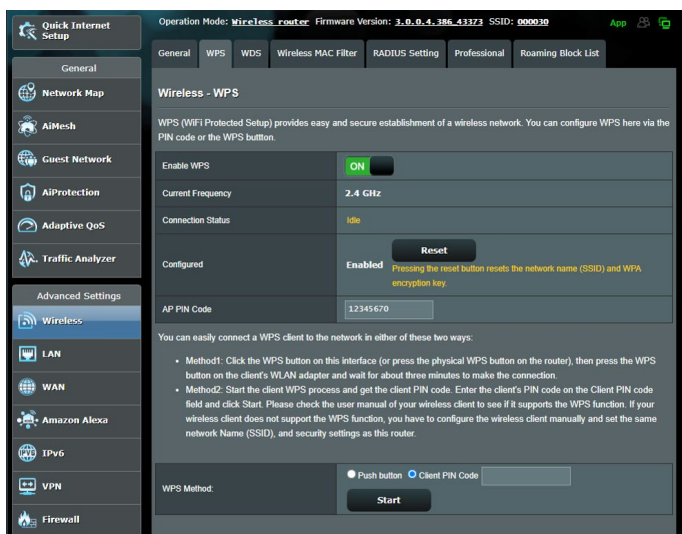
NOTĂ: Ruterul dvs. wireless acceptă o rată de transmitere maximă de 54 Mbps când **Wireless Mode (Mod wireless)** este setat la **Auto (Automat)** și **metoda de criptare** este **WEP** sau **TKIP**.

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

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)**.

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

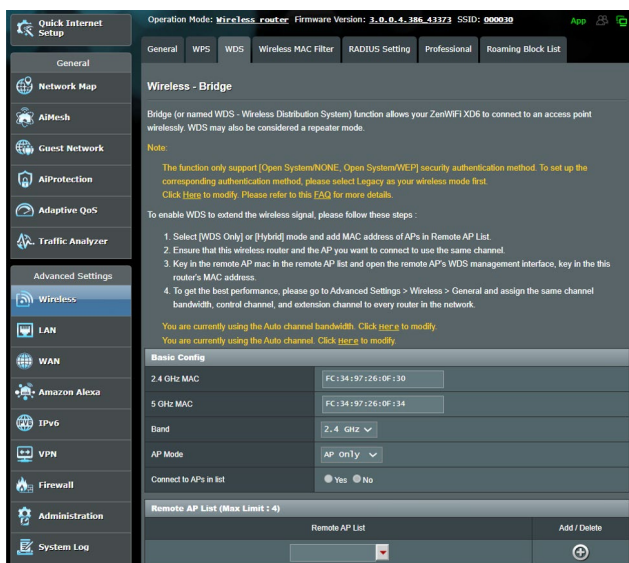
4. În câmpul WPS Method (Metodă WPS), selectați **Push button (Buton de comandă)** sau **Client PIN Code (Cod PIN client)**. Dacă selectați opțiunea **Push Button (Buton de comandă)**, mergeți la pasul 5. Dacă selectați opțiunea **Client PIN code (Cod PIN client)**, mergeți la pasul 6.
5. Pentru a configura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

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

- c. Ruterul wireless va efectua scanarea pentru a detecta toate dispozitivele WPS disponibile. Dacă ruterul wireless nu găsește niciun dispozitiv WPS, acesta va fi comutat în modul de așteptare.
6. Pentru a configura WPS folosind codul PIN al clientului, urmați pașii de mai jos:
 - a. Localizați codul PIN WPS în manualul de utilizare al dispozitivului dvs. wireless sau de pe dispozitivul însuși.
 - b. Introduceți codul PIN al clientului în caseta de text.
 - c. Faceți clic pe **Start** pentru a comuta ruterul wireless în modul de cercetare WPS. Indicatorii cu LED ai ruterului vor clipi rapid de trei ori până când configurarea WPS este finalizată.

4.1.3 Punte

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



Pentru a configura puntea wireless:


1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate) > Wireless > fila WDS**.
2. Selectați banda de frecvență pentru puntea wireless.
3. În câmpul **AP Mode (Mod AP)**, selectați una din aceste opțiuni:
 - **Numai AP:** Dezactivează funcția Wireless Bridge (Punte wireless).

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

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

4. În câmpul **Connect to APs in list (Conectare la AP-uri din listă)**, faceți clic pe **Yes (Da)** dacă doriți să vă conectați la un punct de acces din lista cu puncte de acces la distanță.
5. În câmpul **Control Channel (Canal control)**, selectați canalul operațional pentru puntea wireless. Selectați **Auto (Automat)** pentru a permite ruterului să selecteze automat canalul care are cele mai puține interferențe.

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

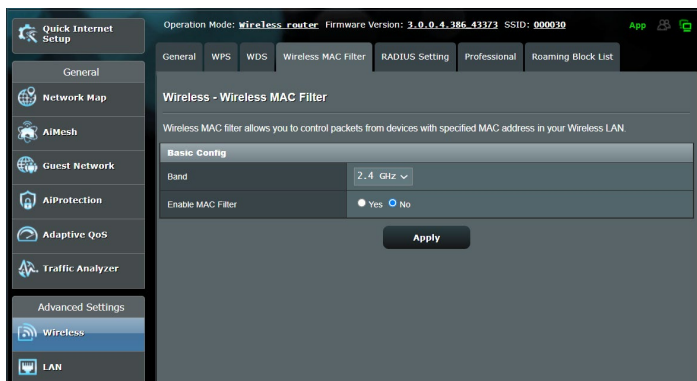
6. În lista cu puncte de acces la distanță, introduceți o adresă MAC și faceți clic pe butonul **Add (Adăugare)**  pentru a introduce adresa MAC a altor puncte de acces disponibile.

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


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

4.1.4 Wireless MAC Filter (Filtru MAC wireless)

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

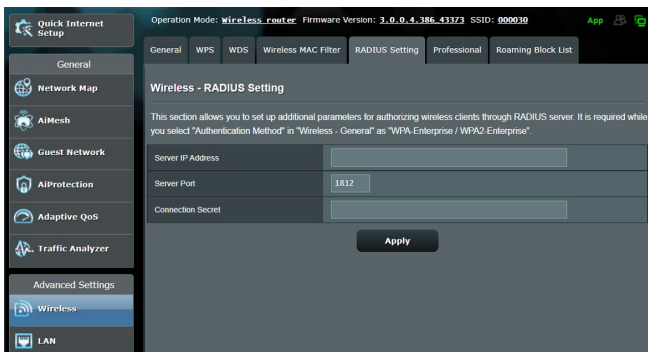


Pentru a configura filtrul MAC wireless:

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

4.1.5 Setarea RADIUS

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



Pentru a configura setările wireless RADIUS:

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

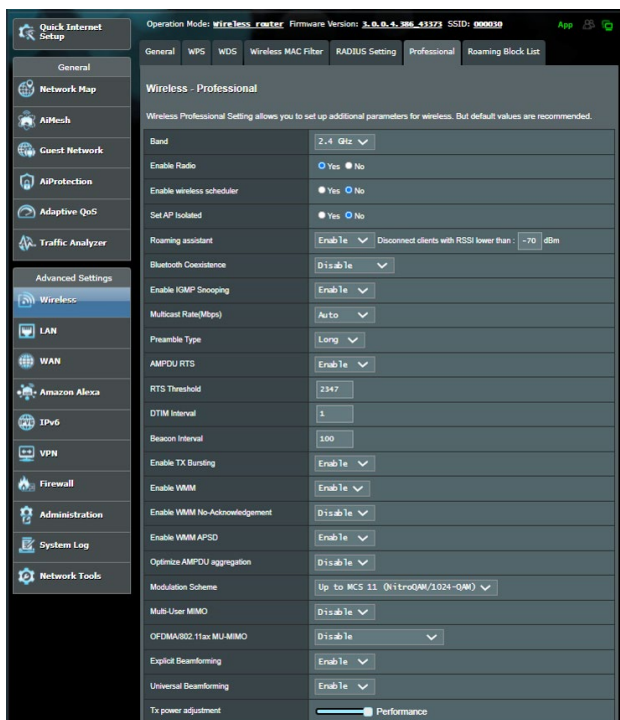
NOTĂ: Consultați secțiunea **4.1.1 Aspecte generale** pentru detalii privind configurarea modului de autentificare al ruterului wireless.

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)**.

4.1.6 Professional (Professional)

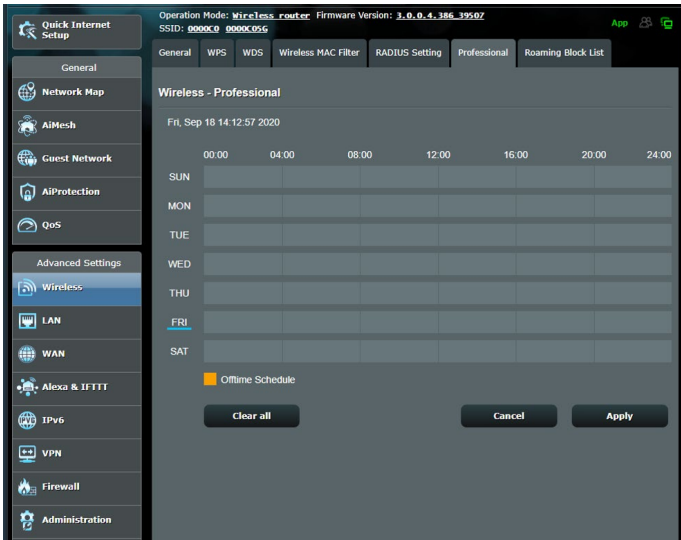
Ecranul Professional (Professional) oferă opțiuni avansate de configurare.

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



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

- **Band (Bandă):** Selectați banda de frecvență pentru care se vor aplica setările profesionale.
- **Activare radio:** Selectați **Yes (Da)** pentru a activa caracteristica wireless a rețelei. Selectați **No (Nu)** pentru a dezactiva caracteristica wireless a rețelei.
- **Enable wireless scheduler (Activare planificator fără fir):** Puteți alege formatul pentru afișarea ceasului, cu 24 de ore sau cu 12 ore. Culoarea din tabel indică Allow (Se permite) sau Deny (Se respinge). Faceți clic pe fiecare cadru pentru a schimba setările pentru ora din zilele săptămânii și faceți clic pe **OK** când terminați.



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

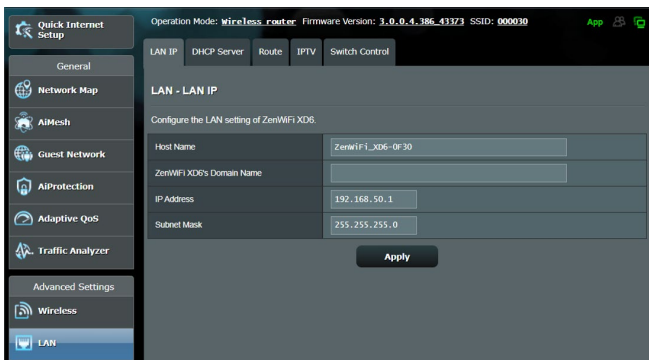
- **Prag RTS:** Selectați o valoare mai mică pentru RTS (Request to Send - solicitare de trimitere) pentru a îmbunătăți comunicarea wireless într-o rețea wireless ocupată sau cu multe interferențe, cu trafic intens și numeroase dispozitive wireless.
- **Interval DTIM:** Parametrul DTIM (Delivery Traffic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

4.2 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.

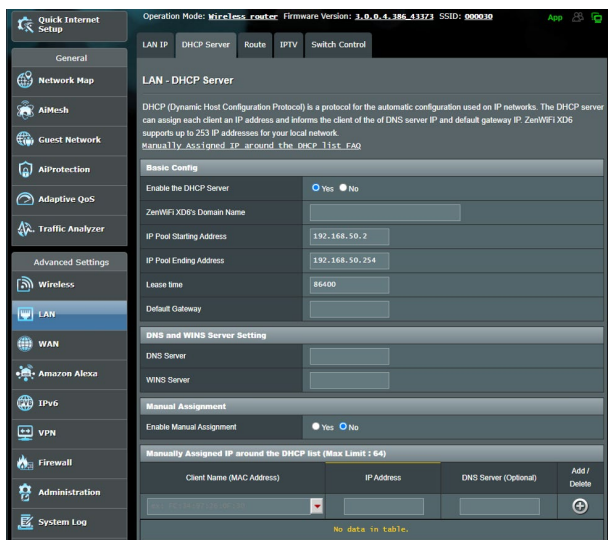


Pentru a modifica setările IP ale rețelei LAN:

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.



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 **ZenWiFi XD6's Domain Name (Numele de domeniu ZenWiFi XD6)**, introduceți un nume de domeniu pentru ruterul wireless.
4. În câmpul **IP Pool Starting Address (Plajă adresă IP de pornire)**, tastați adresa IP de pornire.
5. În câmpul **IP Pool Ending Address (Plajă adresă IP de sfârșit)**, tastați adresa IP de sfârșit.
6. În câmpul **Lease time (Perioadă de închiriere)** tastați data la care expiră adresele IP și ruterul wireless va aloca automat adrese IP noi pentru clienții rețelei.

NOTE:

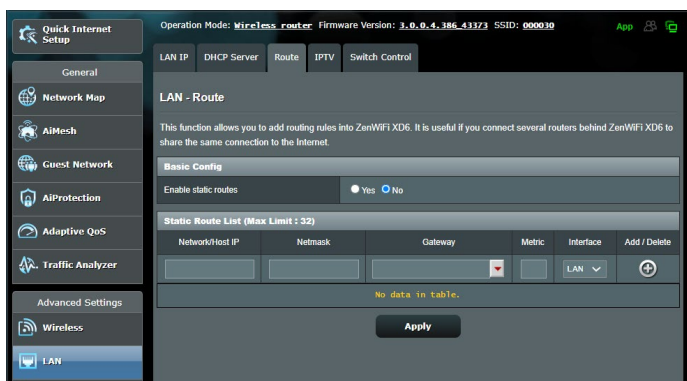
- Vă recomandăm să utilizați un format de adresă IP de tip 192.168.1.xxx (unde xxx poate fi orice număr între 2 și 254) când specificați un interval de adrese IP.
 - Adresa de pornire pentru plaja de adrese IP nu trebuie să fie mai mare decât adresa de sfârșit pentru plaja respectivă.
-

7. În secțiunea **DNS Server (Server DNS)** și **WINS Server (Server WINS)**, 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.

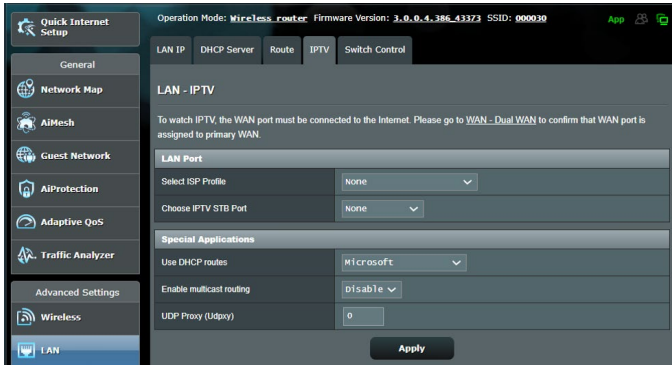


Pentru a configura tabelul de direcționare în rețeaua LAN:

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

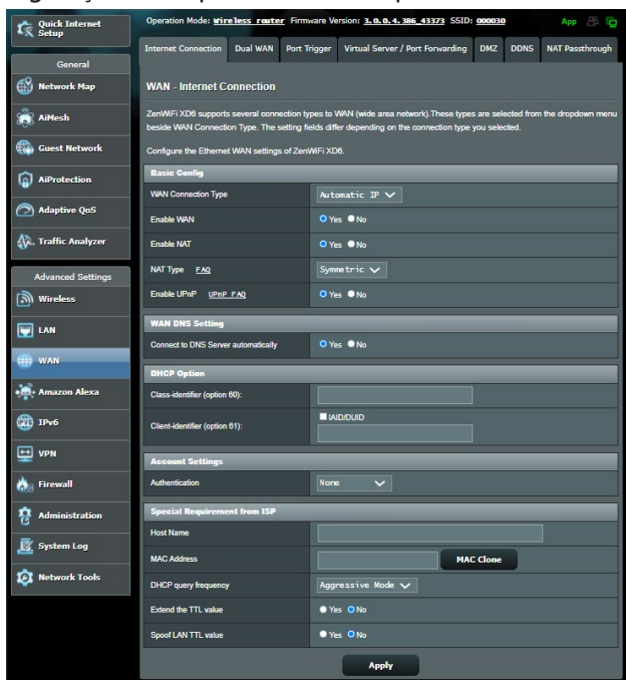
Ruterul wireless acceptă conectarea la servicii IPTV prin intermediul unui ISP sau al unei rețele LAN. Fila IPTV oferă setările necesare pentru configurarea serviciilor IPTV, VoIP, de distribuire multiplă și UDP. Contactați furnizorul de servicii Internet pentru a obține informații specifice cu privire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

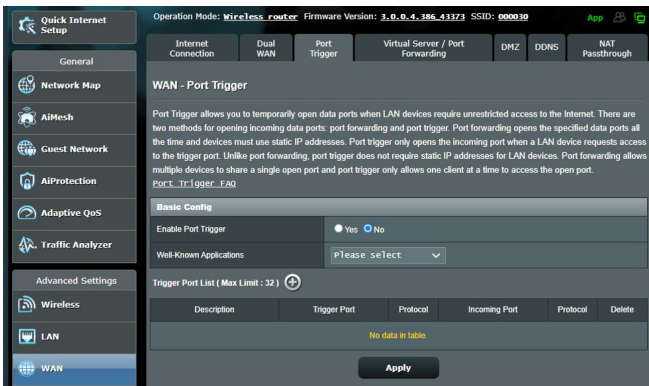
- **Activare NAT:** NAT (Network Address Translation - traducere adresă de rețea) este un sistem unde un IP public (IP de WAN) este utilizat pentru a furniza acces la Internet clienților de rețea care au o adresă IP privată într-un mediu LAN. Adresa IP privată a fiecărui client din rețea este salvată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

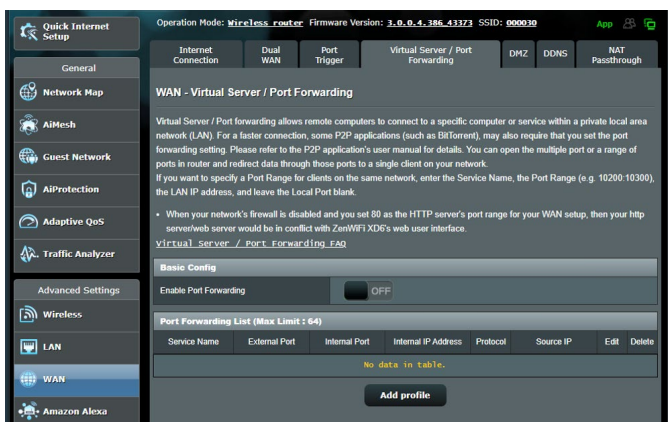
NOTE:

- 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 trimerii de către acesta a unei solicitări/unui semnal de declanșare către ruter.
-

4.3.3 Server virtual/Redirecționare porturi

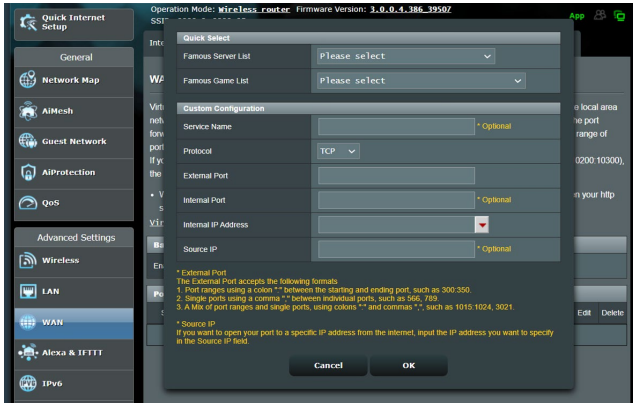
Redirecționarea porturilor este o metodă de direcționare a traficului de rețea dinspre Internet, printr-un anumit port sau printr-un anumit interval de porturi, către un dispozitiv sau mai multe dispozitive din rețeaua dvs. locală. Configurarea redirecționării porturilor pe ruterul dvs. permite PC-urilor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

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



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. Glisați bara la **ON (PORNIT)** pentru a activa Port Forwarding (Redirecționare porturi), apoi bifați **Add Profile (Adăugare profil)**. După configurarea următoarelor setări, faceți clic pe **OK**.



- **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.
- **Service Name:** Enter a service name.
- **Protocol:** Selectați protocolul. În cazul în care aveți dubii, selectați opțiunea **BOTH (Ambele)**.
- **External Port (Port extern):** Acceptă următoarele formate:
 - 1) Un interval de porturi folosind două puncte „:” în mijloc pentru a specifica limitele superioare și inferioare ale intervalului, cum ar fi 300:350;
 - 2) Numerele porturilor individuale folosind o virgulă „,” pentru a le separa, cum ar fi 566, 789;
 - 3) Un amestec de intervale de porturi și porturi individuale, folosind două puncte „:” și virgule „,” cum ar fi 1015:1024, 3021.
- **Port intern:** Introduceți un port specific pentru a primi pachetele redirecționate. Lăsați acest câmp necompletat dacă doriți ca pachetele primite să fie redirecționate către intervalul de porturi specificat.

- **Adresă IP internă:** Introduceți adresa IP a clientului din rețeaua LAN.
- **IP sursă:** Dacă doriți să deschideți portul la o anumită adresă IP de pe internet, introduceți adresa IP la care doriți să oferiți acces în acest câmp.

NOTĂ: Folosiți o adresă IP statică pentru clientul local, pentru ca operația de redirecționare a porturilor să se deruleze corect. Consultați secțiunea **4.2 LAN** pentru mai multe informații.

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

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

Diferențe între triggeringul de port și redirecționarea porturilor:

- Triggeringul de port va funcționa chiar dacă nu se configurează o adresă IP specifică în rețeaua LAN. Spre deosebire de redirecționarea porturilor, care necesită o adresă IP statică în rețeaua LAN, triggeringul de port permite redirecționarea dinamică a porturilor prin intermediul ruterului. Intervale predeterminate de porturi sunt configurate să accepte pentru o anumită perioadă de timp conexiunile primite. Triggeringul de port permite mai multor computere să execute aplicații care în mod normal ar necesita redirecționarea manuală a acelorași porturi către fiecare PC din rețea.
- Triggeringul de port oferă o mai mare securitate decât redirecționarea porturilor, deoarece porturile de intrare nu sunt deschise în permanență. Acestea se deschid numai când o aplicația realizează o conexiune de 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 redirectionarea 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:

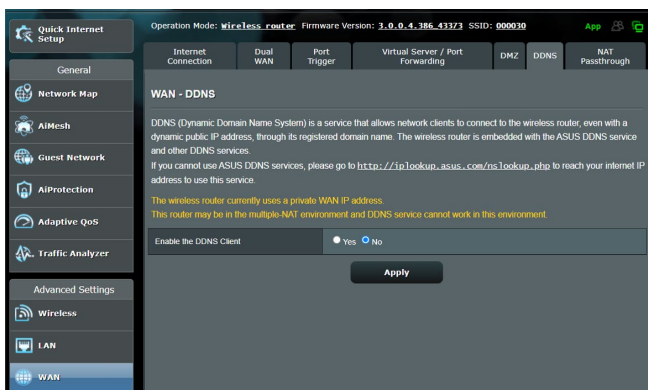
1. Din panoul de navigare, mergeți la **Advanced Settings (Setări avansate)** > **WAN** > fila **DMZ**.
2. Configurați următoarele setări. Când ați terminat, faceți clic pe **Apply (Aplicare)**.
 - **Adresa IP a stației expuse:** Introduceți adresa IP pentru clientul din rețeaua LAN, client care va furniza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

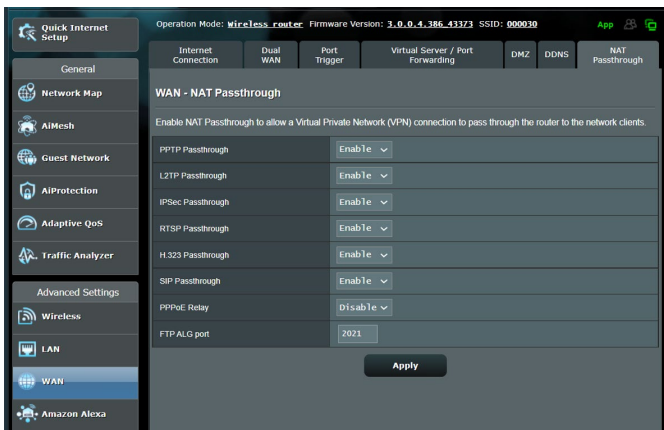
Serviciul DDNS nu va funcționa în următoarele condiții:

- 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)

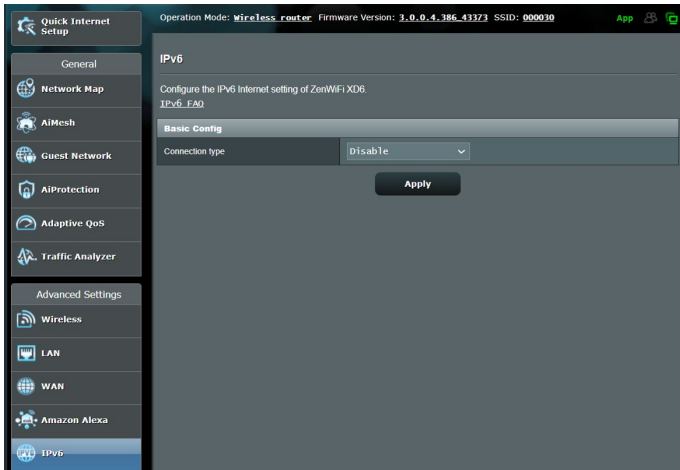
Parametrul NAT Passthrough (Trecere NAT) permite unei conexiuni aparținând unei rețele private virtuale să treacă prin ruter și să fie direcționată către clienții din rețea. Opțiunile PPTP Passthrough (Trecere PPTP), L2TP Passthrough (Trecere L2TP), IPsec Passthrough (Trecere IPsec) și RTSP Passthrough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

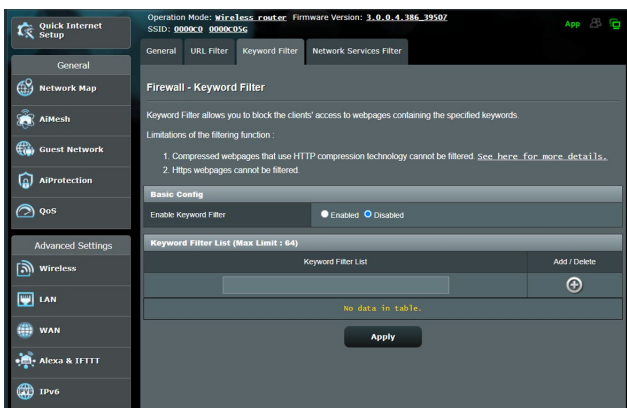
NOTĂ: Filtrul URL se bazează pe o interogare a serverului DNS. Dacă un client din rețea a accesat deja un site web precum <http://www.abcxxx.com>, atunci siteul web nu va fi blocat (siteurile web accesate în trecut sunt stocate într-o memorie cache a serverului DNS). Pentru a rezolva această problemă,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

- Introduceți un cuvânt sau o expresie și apoi faceți clic pe butonul **Add (Adăugare)**.
- 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 WinBox interface for configuring the Firewall Network Services Filter. The left sidebar contains navigation options like Quick Internet Setup, General, Network Map, AiMesh, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, Advanced Settings, Wireless, LAN, WAN, Amazon Alexa, IPv6, VPN, Firewall, Administration, and System Log. The main panel is titled 'Firewall - Network Services Filter' and includes the following configuration options:

- Enable Network Services Filter: Yes No
- Filter table type: Deny 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 field)

Below the configuration options 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 table is currently empty, with a message 'No data in table.' at the bottom.

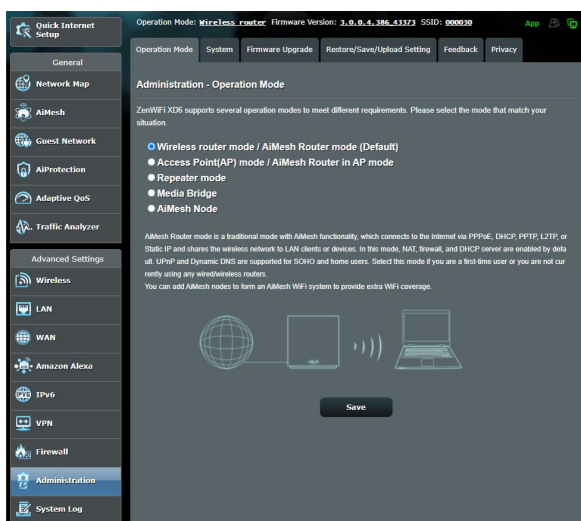
Pentru configurarea unui filtru de servicii de rețea:

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 / Mod ruter AiMesh (implicit):** În modul ruter wireless, ruterul wireless se conectează la Internet și furnizează acces la Internet dispozitivelor disponibile din propria rețea locală.
 - **Punct de acces (AP)/ruter AiMesh în modul AP:** În acest mod, ruterul creează o rețea wireless nouă pe baza unei rețele existente.
 - **Mod repeto:** Acest mod transformă routerul într-un repeto fără fir pentru a extinde intervalul semnalului.
3. Faceți clic pe **Save (Salvare)**.

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.
 - **USB setting (Setare USB):** Puteți activa Hibernarea HDD și schimba modul USB.
 - **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.
 - **Network Monitoring (Monitorizare rețea):** Puteți activa DNS Query (Interogare DNS) pentru a bifa Resolve Hostname (Rezolvare nume gazdă) și Resolved IP Addresses (Adrese IP rezolvate) sau puteți activa Ping, apoi puteți verifica Ping Target (Țintă ping).
 - **Auto Logout (Deconectare automată):** Puteți seta ora deconectării automate.
 - **Activați notificarea de redirecționare a browserului WAN deconectat:** Această caracteristică permite browserului să afișeze o pagină de avertizare atunci când routerul este deconectat de la internet. Când este dezactivată, pagina de avertizare nu va apărea.
 - **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 planificator repornire:** Când este activată, puteți seta Date to Reboot (Data de repornire) și Time od Day to Reboot (Ora de repornire).
 - **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.
 - **Activare serviciu restricții:** 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/LAN.
 - **De acces:** Această caracteristică vă permite să configurați Enable Telnet (Activare Telnet)/Enable SSH (Activare SSH)/SSH Port (Port SSH)/Allow Password Login (Permitere conectare cu parolă)/Authorized Keys (Chei autorizate)/Idle Timeout (Expirare inactivitate).
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)**.
-

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

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
 - Jurnal wireless
 - Atribuirii DHCP
 - IPv6
 - Tabel direcționare
 - Redirecționare porturi
 - Conexiuni

Operation Mode: **Wireless router** Firmware Version: **3.0.0.4.386.43373** SSID: **900030**

General Log Wireless Log DHCP leases IPv6 Routing Table Port Forwarding Connections

System Log - General Log

This page shows the detailed system's activities.

System Time **Wed, Aug 04 16:44:33 2021**

Uptime **0 days 6 hour(s) 47 minute(s) 31 seconds**

Remote Log Server

Remote Log Server Port **514**
The default port is 514. If you reconfigure the port number, please make sure that the remote log server or IoT device's settings match your current configuration.

Apply

Aug 4 08:16:15	wificlientd: wificlientd_proc_event(527): eth6: Auth 26:93:62:64:2D:84, status: Success
Aug 4 08:16:15	wificlientd: wificlientd_proc_event(558): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:16:30	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:16:30	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:17:08	wificlientd: wificlientd_proc_event(537): eth6: Auth 26:93:62:64:2D:84, status: Success
Aug 4 08:17:08	wificlientd: wificlientd_proc_event(555): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:17:22	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:17:22	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:17:24	wificlientd: wificlientd_proc_event(527): eth6: Auth 26:93:62:64:2D:84, status: Success
Aug 4 08:17:24	wificlientd: wificlientd_proc_event(558): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:17:40	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:17:40	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:18:01	wificlientd: wificlientd_proc_event(527): eth6: Auth 26:93:62:64:2D:84, status: Success
Aug 4 08:18:01	wificlientd: wificlientd_proc_event(558): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:18:14	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:18:14	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:20:23	wificlientd: wificlientd_proc_event(527): eth6: Auth 26:93:62:64:2D:84, status: Success
Aug 4 08:20:23	wificlientd: wificlientd_proc_event(558): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:20:29	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:20:29	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:34:27	wificlientd: wificlientd_proc_event(556): eth6: Assoc 26:93:62:64:2D:84, status: Success
Aug 4 08:34:33	wificlientd: wificlientd_proc_event(508): eth6: Disassoc 26:93:62:64:2D:84, status: 0
Aug 4 08:34:33	wificlientd: wificlientd_proc_event(509): eth6: Disassoc 26:93:62:64:2D:84, status: 0

5 Utilitățile

NOTE:

- Descărcați și instalați utilitățile routerului wireless de pe site-ul web ASUS:
 - Utilitarul Device Discovery, versiunea 1.4.7.1, poate fi descărcat de la adresa <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.

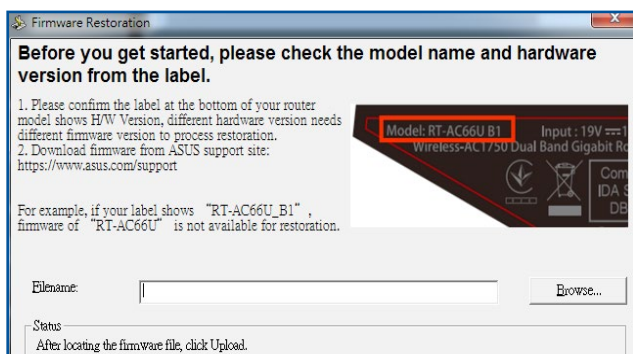
Pentru a lansa utilitarul Detectează Dispozitivul

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

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

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.

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

1. Deconectați ruterul fără fir de la sursa de alimentare.
2. Țineți apăsat butonul Reset (Reinițializare) de pe panoul din spate și simultan conectați din nou ruterul fără fir la sursa de alimentare. Eliberați butonul Reset (Reinițializare) atunci când LED-ul de alimentare de pe panoul frontal luminează intermitent lent, ceea ce indică faptul că ruterul fără fir este în modul de salvare.

3. Setați un IP static pentru computerul dvs. și utilizați următoarele instrumente pentru a configura setările TCP/IP.

Adresă IP: 192.168.1.x

Mască subrețea: 255.255.255.0

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

NOTĂ: Acesta nu este un utilitar de upgrade de firmware și nu poate fi utilizat pe un ruter fără fir ASUS în funcțiune. Upgrade-urile normale de firmware trebuie efectuate prin intermediul interfeței Web. Consultați **Capitolul 4: Configurarea setărilor Complexe** pentru mai multe detalii.

6 Remedierea defecțiunilor

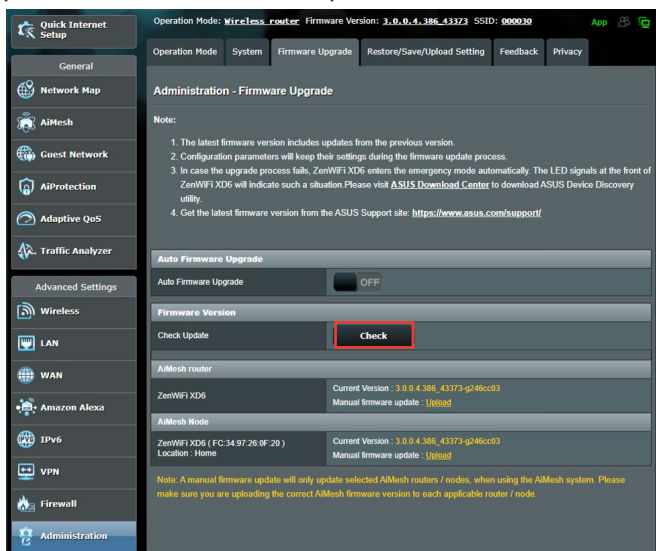
Acest capitol oferă soluții pentru problemele pe care le puteți întâmpina la folosirea ruterului. În cazul în care întâmpinați probleme care nu sunt menționate în acest capitol, accesați siteul de asistență ASUS, la adresa: <https://www.asus.com/support/>. Aici puteți găsi mai multe informații despre 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 <https://www.asus.com/Mesh-WiFi-System/ZenWiFi-XD6/HelpDesk/>, 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 cu ruterul este conectat corect, LEDul pentru conexiunea LAN corespunzătoare va fi aprins.

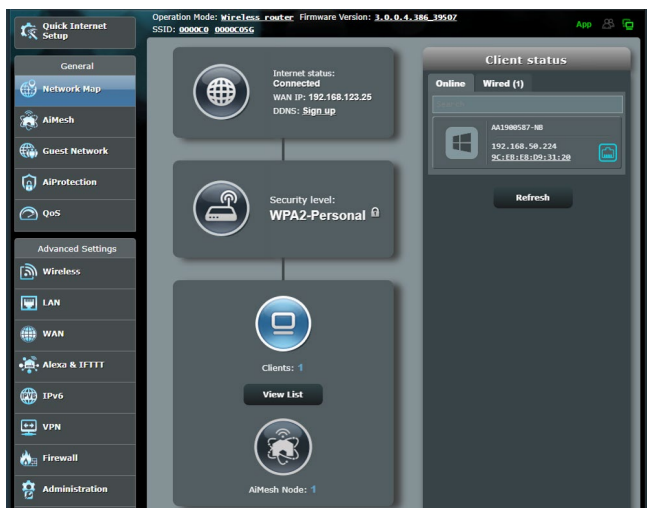
Verificați dacă setarea wireless de pe computerul dvs. corespunde cu cea a ruterului.

- 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)**.



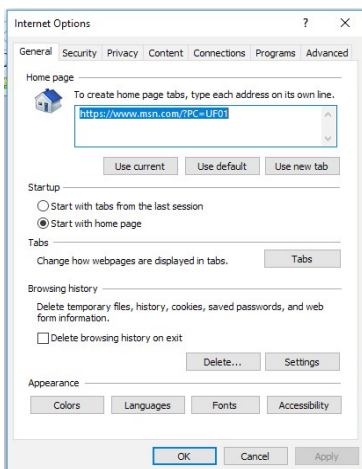
6.2 Întrebări frecvente

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, urmați acești pași:

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



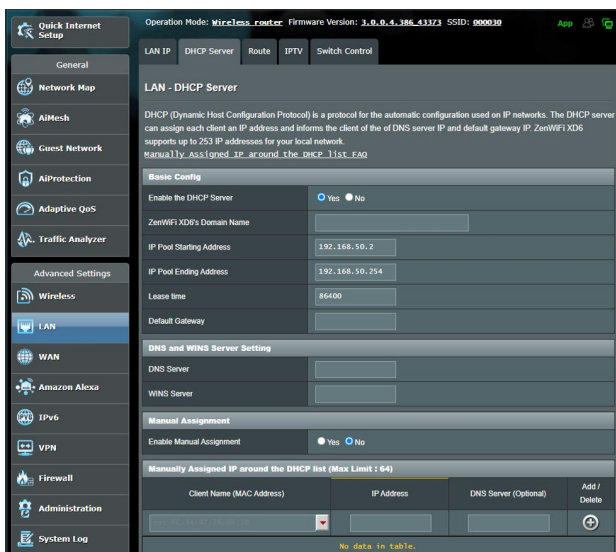
NOTE:

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

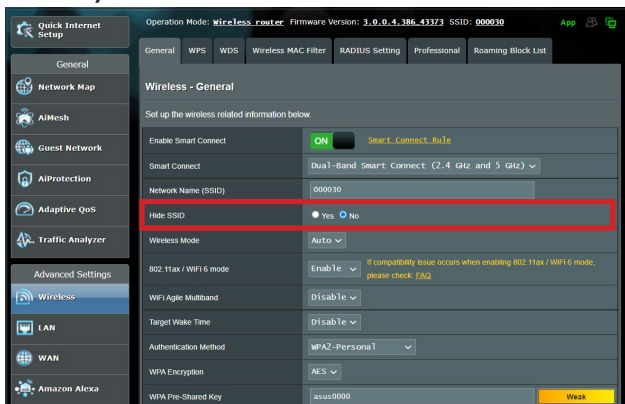
Clientul nu poate stabili o legătura wireless cu routerul.

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

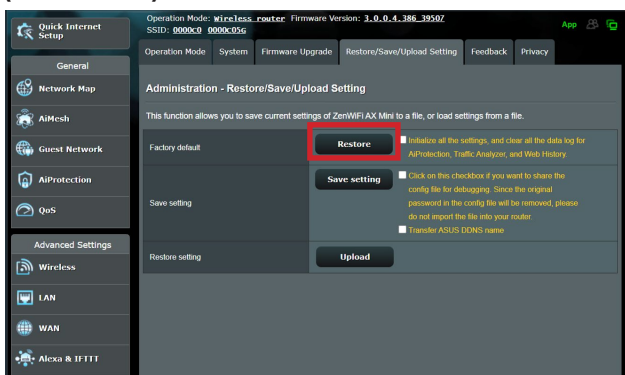
- **În afara razei:**
 - Puneți routerul mai aproape de clientul wireless.
 - Încercați să reglați antenele routerului pentru a obține direcția de propagare optimă, după cum se descrie în secțiunea **1.4 Positioning your router (Poziționarea routerului)**.
- **Serverul DHCP a fost dezactivat:**
 1. Lansați 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)**.

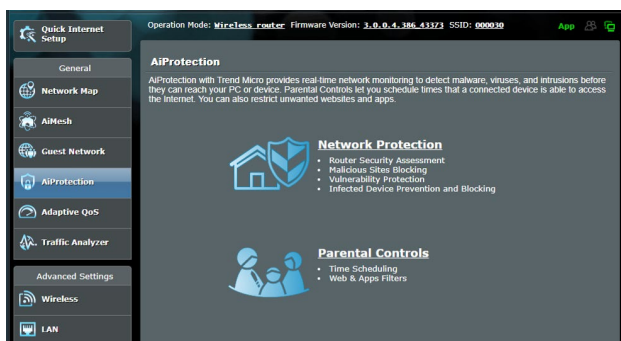


Internetul nu este accesibil.

- 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 > AiProtection > 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:

Validează DHCP: Da (când cablul WAN este conectat)

Adresă IP: 192.168.50.1

Nume domeniu: (Gol)

Subnet Mask: 255. 255. 255.0

DNS Server 1: router.asus.com

DNS Server 2: (Gol)

SSID: ASUS_XX

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).

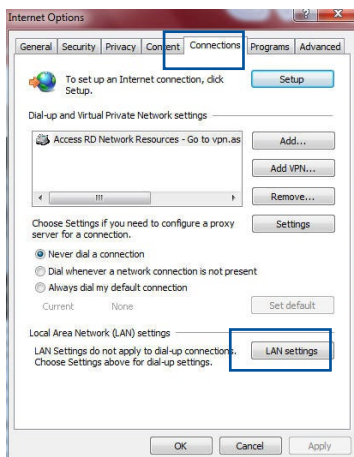
Nu se poate accesa interfața de utilizare web

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

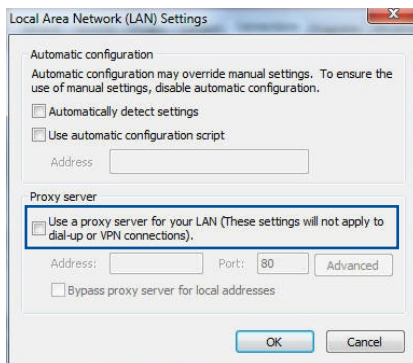
A. Dezactivați serverul proxy, dacă este activat.

Windows®

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)**.

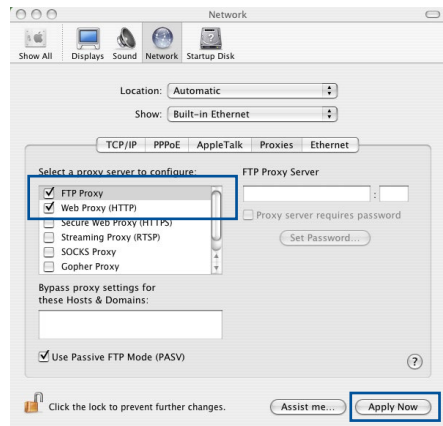


3. Din ecranul Local Area Network (LAN) Settings (Setări pentru rețeaua locală (LAN)), debifați opțiunea **Use a proxy server for your LAN (Utilizare server proxy pentru rețeaua locală)**.
4. Faceți clic pe **OK** când ați terminat.



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))**.



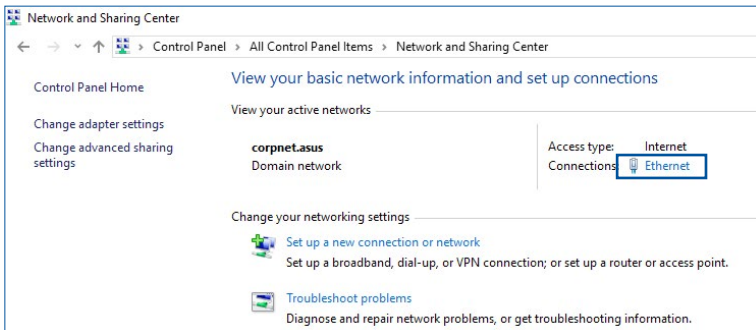
3. Faceți clic pe **Apply Now (Se aplică acum)** când ați terminat.

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

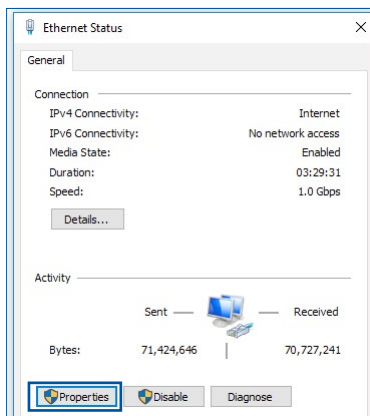
B. Configurați setările TCP/IP pentru obținerea automată a unei adrese IP.

Windows®

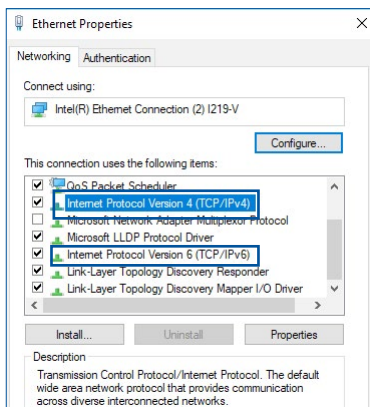
1. Faceți clic pe **Start > Control Panel (Panou de control) > Network and Internet (Rețea și Internet) > Network and Sharing Center (Centru de rețea și partajare)**, apoi faceți clic pe conexiunea de rețea pentru a afișa fereastra de stare.



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



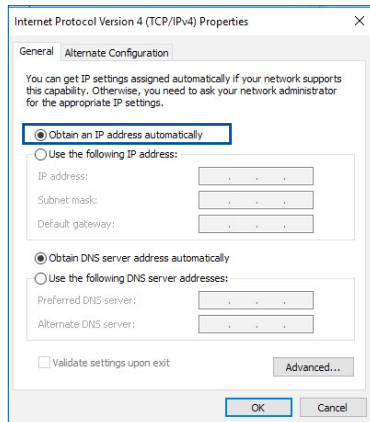
3. Selectați **Internet Protocol Version 4 (TCP/IPv4) (Protocol Internet versiunea 4 (TCP/IPv4))** sau **Internet Protocol Version 6 (TCP/IPv6) (Protocol Internet versiunea 6 (TCP/IPv6))**, apoi faceți clic pe **Properties (Proprietăți)**.




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

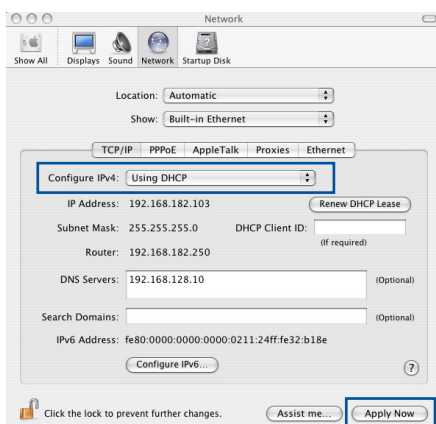
Pentru a obține automat setările IP IPv6, bifați **Obtain an IPv6 address automatically (Se obține automat o adresă IPv6)**.

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



MAC OS

1. Faceți clic pe pictograma Apple  localizată în partea stângă sus a ecranului.
2. Faceți clic pe **System Preferences (Preferințe sistem) > Network (Rețea) > Configure... (Configurare...)**
3. În 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.

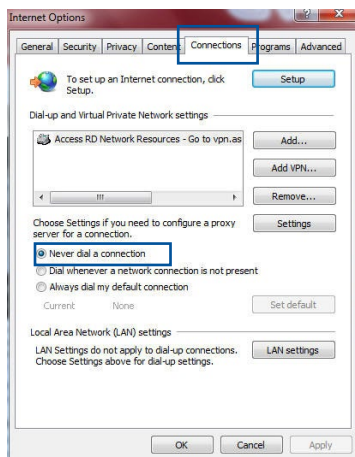


NOTA: Consultați caracteristica de ajutor și asistență a sistemului de operare pentru detalii despre configurarea setărilor TCP/IP ale computerului.

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

Windows®

1. Faceți clic pe **Start > 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.



NOTA: Consultați caracteristica de ajutor a browserului pentru detalii despre dezactivarea conexiunii pe linie comutată.

Anexă

Notices

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), the power consumption will be less than 12 watts when the system is in network standby mode (idle mode).

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.

IMPORTANT NOTE:

Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating

instructions for satisfying RF exposure compliance. To maintain compliance with FCC exposure compliance requirement, please follow operation instruction as documented in this manual. This equipment should be installed and operated with a minimum distance of 15 cm between the radiator and any part of your body.

NCC 警語

取得審驗證明之低功率射頻器材，非經核准，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。低功率射頻器材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。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材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。

「產品之限用物質含有情況」之相關資訊，請參考下表：

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr ⁺⁶)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
印刷電路板及電子組件	-	○	○	○	○	○
結構組件（金屬 / 塑膠）	○	○	○	○	○	○
其他組件（如天線/ 指示燈/連接線）	○	○	○	○	○	○
其他及其配件（如電源供應器）	-	○	○	○	○	○
備考1. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。 備考2. “-” 係指該項限用物質為排除項目。						

安全說明：

- 請在溫度為 0° C (32° F) 至 40° C (104° F) 之間的環境中使用本產品。
- 請依照產品上的電源功率貼紙說明使用正確的電源適配器，如果使用錯誤規格的電源適配器可能會造成內部零件的損壞。
- 請勿將產品放置於不平坦或不穩定的表面，若產品的外殼損壞，請聯繫維修服務人員。
- 請勿在產品上放置其他物品，請勿將任何物品塞入產品內，以避免引起組件短路或電路損壞。

- 請保持机器在干燥的环境下使用，雨水、濕氣、液体等含有礦物質會腐蝕電子線路，請勿在雷電天气下使用調製解調器。
- 請勿堵塞產品的通風孔，以避免因散熱不良而導致系統過熱。
- 請勿使用破損的電源線、附件或其他周邊產品。
- 如果電源已損壞，請不要嘗試自行修復，請將其交給專業技術服務人員或經銷商來處理。
- 為了防止電擊風險，在搬動主機前，請先將電源線插頭暫時從電源插座上拔除。

使用警語：

- 推薦您在環境溫度為 0° C (32° F) ~ 40° C (104° F) 的情況下使用本產品。
- 請依照產品底部的電源功率貼紙說明使用符合此功率的電源變壓器。
- 請勿將產品放置在不平坦或不穩定的物體表面。若產品外殼有所損毀，請將產品送修。
- 請勿將任何物體放置在產品上方，並不要將任何外物插入產品。
- 請勿將產品置於或在液體、雨天或潮濕的環境中使用。雷暴天氣請不要使用數據機。
- 請勿擋住產品的散熱孔，以防止系統過熱。
- 請勿使用損毀的電源線、配件或其他周邊裝置。
- 若電源變壓器已損毀，請不要嘗試自行修復，請聯絡專業的服務技術人員或您的零售商。
- 為防止觸電，在重新放置產品前，請從電源插座上拔下電源線。
- 無線資訊傳輸設備避免影響附近雷達系統之操作。

華碩聯絡資訊

華碩電腦公司 ASUSTeK COMPUTER INC. (台灣)

市場訊息

地址：台灣臺北市北投區立德路 15 號 1 樓

電話：+886-2-2894-3447

傳真：+886-2-2890-7698

電子郵件：info@asus.com.tw

全球資訊網：<https://www.asus.com/tw>

技術支援

電話：+886-2-2894-3447 (0800-093-456)

線上支援：<https://www.asus.com/tw/support/>

Precautions for the use of the device

- a. Pay particular attention to the personal safety when use this device in airports, hospitals, gas stations and professional garages.
- b. Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products in order to reduce the risk of interference.
- c. Kindly use ASUS products in good reception conditions in order to minimize the radiation's level.
- d. Keep the device away from pregnant women and the lower abdomen of the teenager.

Précautions d'emploi de l'appareil

- a. Soyez particulièrement vigilant quant à votre sécurité lors de l'utilisation de cet appareil dans certains lieux (les avions, les aéroports, les hôpitaux, les stations-service et les garages professionnels).
- b. Évitez d'utiliser cet appareil à proximité de dispositifs médicaux implantés. Si vous portez un implant électronique (stimulateurs cardiaques, pompes à insuline, neurostimulateurs...), veuillez impérativement respecter une distance minimale de 15 centimètres entre cet appareil et votre corps pour réduire les risques d'interférence.
- c. Utilisez cet appareil dans de bonnes conditions de réception pour minimiser le niveau de rayonnement. Ce n'est pas toujours le cas dans certaines zones ou situations, notamment dans les parkings souterrains, dans les ascenseurs, en train ou en voiture ou tout simplement dans un secteur mal couvert par le réseau.
- d. Tenez cet appareil à distance des femmes enceintes et du bas-ventre des adolescents.

Условия эксплуатации:

- Температура эксплуатации устройства: 0-40 °С. Не используйте устройство в условиях экстремально высоких или низких температур.
- Не размещайте устройство вблизи источников тепла, например, рядом с микроволновой печью, духовым шкафом или радиатором.
- Использование несовместимого или несертифицированного адаптера питания может привести к возгоранию, взрыву и прочим опасным последствиям.
- При подключении к сети электропитания устройство следует располагать близко к розетке, к ней должен осуществляться беспрепятственный доступ.
- Утилизация устройства осуществляется в соответствии с местными законами и положениями. Устройство по окончании срока службы должны быть переданы в сертифицированный пункт сбора для вторичной переработки или правильной утилизации.
- Данное устройство не предназначено для детей. Дети могут пользоваться устройством только в присутствии взрослых.
- Не выбрасывайте устройство и его комплектующие вместе с обычными бытовыми отходами.



AEEE Yönetmeliğine Uygundur. IEEE Yönetmeliğine Uygundur.

- Bu Cihaz Türkiye analog şebekelerde çalışabilecek şekilde tasarlanmıştır.
- Cihazın ayrıntılı kurulum rehberi kutu içeriğinden çıkan CD içerisinde. Cihazın kullanıcı arayüzü Türkçe'dir.
- Cihazın kullanılması planlanan ülkelerde herhangi bir kısıtlaması yoktur. Ülkeler simgeler halinde kutu üzerinde belirtilmiştir.

Manufacturer	ASUSTeK Computer Inc. Tel: +886-2-2894-3447 Address: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Authorised representative in Europe	ASUS Computer GmbH Address: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY
Authorised distributors in Turkey	BOGAZICI BILGISAYAR TICARET VE SANAYI A.S. Tel./FAX No.: +90 212 331 10 00 / +90 212 332 28 90 Address: ESENTEPE MAH. BUYUKDERE CAD. ERCAN HAN B BLOK NO.121 SISLI, ISTANBUL 34394
	CIZGI Elektronik San. Tic. Ltd. Sti. Tel./FAX No.: +90 212 356 70 70 / +90 212 356 70 69 Address: GURSEL MAH. AKMAN SK.47B 1 KAGITHANE/ ISTANBUL
	KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİŞ TIC. A.S. Tel. No.: +90 216 5288888 Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZI, SANCAKTEPE ISTANBUL
	ENDEKS BİLİŞİM SAN VE DİŞ TİC LTD ŞTİ Tel./FAX No.: +90 216 523 35 70 / +90 216 523 35 71 Address: NECİP FAZİL BULVARI, KEYAP CARSI SITESİ, G1 BLOK, NO:115 Y.DUDULLU, UMRANIYE, ISTANBUL
	PENTA TEKNOLOJİ URUNLERİ DAGITIM TICARET A.S Tel./FAX No.: +90 216 528 0000 Address: ORGANİZE SANAYİ BOLGESİ NATO YOLU 4.CADDE NO:1 UMRANIYE, ISTANBUL 34775

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

[English] CE statement

EU Declaration of Conformity



We, the undersigned,

Manufacturer: ASUSTeK COMPUTER INC.
Address: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Authorized representative in Europe: ASUS COMPUTER GmbH
Address, City: HARKORT STR. 21-23, 40880 RATINGEN
Country: GERMANY

declare the following apparatus:

Product name: AX5400 Dual Band WiFi Router
Model name: XD6

Additional information: ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

Radio Equipment Directive – 2014/53/EU

Article 3.1(a)
EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)
Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2
EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class
Class 2

Ecodesign Directive – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Directive – 2011/65/EU

2015/863/EU, EN 50581:2012

Signature:

S.y. Shian, CEO

Place of issue:

Taipei, Taiwan

Date of issue:

12/04/2021

EU Overensstemmelseserklæring



Vi, undertegnede,

Fabrikant: ASUSTeK COMPUTER INC.
Adresse: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Autoriseret repræsentant i Europa: ASUS COMPUTER GmbH
Adresse, By: HARKORT STR. 21-23, 40880 RATINGEN
Land: GERMANY

erklærer, at følgende apparat:

Produktnavn: AX5400 Dual Band WiFi Router
Modelnavn: XD6

Supplerende oplysninger: ANNEX 1

Ovenstående produkt er i overensstemmelse med den relevante harmoniseringslovgivning for EU:

Radioudstyr Direktiv – 2014/53/EU

Artikel 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artikel 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artikel 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radioudstyr Klasse

Klasse 2

Miljøvenligt design Direktiv – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktiv – 2011/65/EU

2015/863/EU, EN 50581:2012

Underskrift:

S.y. Shian, Administrerende direktør/CEO

Udstedelsessted:

Taipei, Taiwan

Udstedelsesdato:

12/04/2021

1 of 2

[Dutch] CE statement

EU-conformiteitsverklaring



Wij, de ondergetekenden,

Fabrikant: ASUSTeK COMPUTER INC.
Adres: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Geautoriseerde vertegenwoordiger in Europa: ASUS COMPUTER GmbH
Adres, plaats: HARKORT STR. 21-23, 40880 RATINGEN
Land: GERMANY

Verklaren dat het volgende apparaat:

Productnaam: AX5400 Dual Band WiFi Router
Modelnaam: XD6

Aanvullende informatie: ANNEX I

Het onderwerp van de bovenstaande verklaring is in overeenstemming met de desbetreffende harmoniseringswetgeving van de Europese Unie:

Radioapparatuur Richtlijn – 2014/53/EU

Artikel 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artikel 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artikel 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio apparaatuur Klasse
Klasse 2

Ecologisch ontwerp Richtlijn – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Richtlijn – 2011/65/EU

2015/863/EU, EN 50581:2012

Handtekening:

S.y. Shian, Directeur/CEO

Plaats van afgifte:

Taipei, Taiwan

Datum van afgifte:

12/04/2021

Déclaration UE de Conformité



Nous, soussignés,

Fabricant: ASUSTeK COMPUTER INC.
Address: 1F, No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Représentant autorisé en Europe: ASUS COMPUTER GmbH
Adresse, ville: HARKORT STR. 21-23, 40880 RATINGEN
Pays: GERMANY

Déclarons l'appareil suivant:

Nom du produit: AX5400 Dual Band WiFi Router
Nom du modèle: XD6

Informations complémentaires: ANNEX I

L'objet de la déclaration décrit ci-dessus est conforme avec la législation d'harmonisation de l'Union applicable:

Directive Équipement Radioélectrique – 2014/53/EU

Article 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Classe d'équipement Radio

Classe 2

Directive écoconception – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

Directive RoHS – 2011/65/EU

2015/863/EU, EN 50581:2012

Signature:

S.y. Shian, Directeur Général/CEO

Lieu de délivrance:

Taipei, Taiwan

Date d'émission:

12/04/2021

EU-vaatimustenmukaisuusvakuutus



Me, allekirjoittaneet,

Valmistaja:	ASUSTeK COMPUTER INC.
Osoite:	1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Valtuutettu edustaja Euroopassa:	ASUS COMPUTER GmbH
Osoite, kaupunki:	HARKORT STR. 21-23, 40880 RATINGEN
Maa:	GERMANY

ilmoitamme seuraavan laitteen:

Tuotenimi:	AX5400 Dual Band WiFi Router
Mallinimi:	XD6

Lisätietoja: ANNEX I

Yllä olevan ilmoituksen kohde on asiaa koskevan unionin yhdenmukaistamislainsäädännön mukainen:

Radiolaitteet Direktiiv - 2014/53/EU

3.1a artikla

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

3.1b artikla

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

3.2 artikla

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio-laitteiden luokka
luokka 2

Ekologisella suunnittelulla Direktiivi - 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktiivi - 2011/65/EU

2015/863/EU, EN 50581:2012

Allekirjoitus:

S.y. Shian, Toimitusjohtaja/CEO

Myöntämispaikka:

Taipei, Taiwan

Myöntämispäivä:

12/04/2021

EU Konformitätserklärung



Hiermit erklären wir,

Hersteller: ASUSTeK COMPUTER INC.
Anschrift: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Bevollmächtigter: ASUS COMPUTER GmbH
Anschrift des Bevollmächtigten: HARKORT STR. 21-23, 40880 RATINGEN
Land: GERMANY

dass nachstehend bezeichnete Produkte:

Produktbezeichnung: AX5400 Dual Band WiFi Router
Modellbezeichnung: XD6

Zusatzangaben: ANNEX I

mit den nachstehend angegebenen, für das Produkt geltenden Richtlinien/Bestimmungen übereinstimmen:

Funkanlagen Richtlinie – 2014/53/EU

Artikel 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artikel 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artikel 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Funkanlagen Klasse

Klasse 2

Ökodesign Richtlinie – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Richtlinie – 2011/65/EU

2015/863/EU, EN 50581:2012

Unterschrift:

S.y. Shian, Geschäftsführer/CEO

Ort:

Taipei, Taiwan

Datum:

12/04/2021

1 of 2

Δήλωση Συμμόρφωσης ΕΕ



Εμείς, τα υπογράφοντα μέλη,

Κατασκευαστής:

ASUSTeK COMPUTER INC.

Διεύθυνση:

1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan

Εξουσιοδοτημένος αντιπρόσωπος στην Ευρώπη:

ASUS COMPUTER GmbH

Διεύθυνση, Πόλη:

HARKORT STR. 21-23, 40880 RATINGEN

Χώρα:

GERMANY

δηλώνουμε την εξής συσκευή:

Όνομα προϊόντος:

AX5400 Dual Band WiFi Router

Όνομα μοντέλου:

XD6

Συμπληρωματικές πληροφορίες: ANNEX I

Το αντικείμενο της δήλωσης που περιγράφεται παραπάνω είναι σύμφωνο προς την σχετική ενωσιακή νομοθεσία εναρμόνισης:

Ραδιοεξοπλισμό Οδηγία - 2014/53/EU

Άρθρο 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Άρθρο 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Άρθρο 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Κατηγορία Ραδιοεξοπλισμού

Τάξη 2

Οικολογικός σχεδιασμός Οδηγία - 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Οδηγία- 2011/65/EU

2015/863/EU, EN 50581:2012

Υπογραφή:

S.y. Shian, Διευθύνων Σύμβουλος/CEO

Τόπος έκδοσης:

Taipei, Taiwan

Ημερομηνία έκδοσης:

12/04/2021

Dichiarazione di conformità UE



I sottoscritti,

Produttore: ASUSTeK COMPUTER INC.
Indirizzo: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Rappresentante autorizzato per l'Europa: ASUS COMPUTER GmbH
Indirizzo, Città: HARKORT STR. 21-23, 40880 RATINGEN
paese: GERMANY

dichiarano che il seguente apparecchio:

Nome prodotto: AX5400 Dual Band WiFi Router
Nome modello: XD6

Informazioni supplementari: ANNEX I

L'oggetto della dichiarazione di cui sopra è conforme alla pertinente normativa di armonizzazione dell'Unione Europea

Apparecchi radio Directive – 2014/53/EU

Articolo 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Articolo 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Articolo 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Classe di apparecchiature radio

Classe 2

Progettazione ecocompatibile Direttiva – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direttiva – 2011/65/EU

2015/863/EU, EN 50581:2012

Firma:

S.y. Shian, Amministratore delegato/CEO

Luogo:

Taipei, Taiwan

Data del rilascio:

12/04/2021

[Portuguese] CE statement

Declaração UE de Conformidade



Nós, os abaixo-assinados,

Fabricante: ASUSTeK COMPUTER INC.
Endereço: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Representante autorizado na Europa: ASUS COMPUTER GmbH
Endereço, cidade: HARKORT STR. 21-23, 40880 RATINGEN
País: GERMANY

declaramos o seguinte aparelho:

Nome do produto: AX5400 Dual Band WiFi Router
Nome do modelo: XD6

Informações adicionais: ANNEX I

O objeto da declaração acima descrito está em conformidade com a legislação de harmonização da União aplicável:

Equipamento de rádio Diretiva - 2014/53/EU

Artigo 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artigo 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artigo 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Classe de equipamento de Rádio

Classe 2

Concepção Ecológica Diretiva - 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Diretiva - 2011/65/EU

2015/863/EU, EN 50581:2012

Assinatura:

S.y. Shian, Diretor Executivo/CEO

Local de emissão:

Taipei, Taiwan

Data de emissão:

12/04/2021

1 of 2

[Spanish] CE statement

UE Declaración de Conformidad



Nosotros, los abajo firmantes,

Fabricante: ASUSTeK COMPUTER INC.
Dirección: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Representante autorizado en Europa: ASUS COMPUTER GmbH
Dirección, Ciudad: HARKORT STR. 21-23, 40880 RATINGEN
País: GERMANY

Declaramos el siguiente producto:

Nombre del aparato: AX5400 Dual Band WiFi Router
Nombre del modelo: XD6

Información adicional: ANNEX I

El objeto de la declaración descrita anteriormente es conforme con la legislación de armonización pertinente de la Unión:

Equipos Radioeléctricos Directiva – 2014/53/EU

Artículo 3.1a
EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artículo 3.1b
Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artículo 3.2
EN 300 328 V2.2.2, EN 301 893 V2.1.1

Clase de Equipos de Radio
Clase 2

Directiva Diseño Ecológico – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

Directiva RoHS – 2011/65/EU

2015/863/EU, EN 50581:2012

Firma:

S.y. Shian, Director Ejecutivo/CEO

Lugar de emisión:

Taipei, Taiwan

Fecha de emisión:

12/04/2021

[Swedish] CE statement

Försäkran om överensstämmelse



Undertecknande,

Tillverkare:	ASUSTeK COMPUTER INC.
Adress:	1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Auktoriserad representant i Europa:	ASUS COMPUTER GmbH
Adress, Ort:	HARKORT STR. 21-23, 40880 RATINGEN
Land:	GERMANY

förklarar att följande apparat:

Produktnamn:	AX5400 Dual Band WiFi Router
Modellnamn:	XD6

Ytterligare information: ANNEX I

Syftet med deklARATIONEN som beskrivs ovan är i enlighet med relevant harmonisering av EU-lagstiftningen:

Radioutrustning Direktiv – 2014/53/EU

Artikel 3.1a
EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artikel 3.1b
Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artikel 3.2
EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radioutrustningsklass
Klass 2

Ekodesign Direktiv – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktiv – 2011/65/EU

2015/863/EU, EN 50581:2012

Namnsteckning:

S.y. Shian, Verkställande director/CEO

Plats för utfärdande:

Taipei, Taiwan

Dag för utfärdande:

12/04/2021

[Bulgarian] CE statement



ЕС декларация за съответствие

Ние, долуподписаните,

Производител: ASUSTEK COMPUTER INC.
Адрес: 1F, No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Упълномощен представител в Европа: ASUS COMPUTER GmbH

Адрес, град: HARKORT STR. 21-23, 40880 RATINGEN
Държава: GERMANY

декларираме, че следният апарат:

Име на продукта: AX5400 Dual Band WiFi Router
Име на модела: XD6

Допълнителна информация: ANNEX I

Предметът на декларацията, описан по-горе, съответства на съответното законодателство на Съюза за хармонизация:

Директива за радионавигационно оборудване – 2014/53/EC

Article 3.1(a)

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class
Class 2

Директива за екологично проектиране – 2009/125/EU

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

електрическото и електронното оборудване – 2011/65/EU

2015/863/EU, EN 50581:2012

Подпис:

S.y. Shian, Главен изпълнителен директор/CEO

Място на издаване:

Taipei, Taiwan

Дата на издаване:

12/04/2021

1 of 2

EU izjava o sukladnosti



Mi, dolje potpisani,

Proizvođač: ASUSTek COMPUTER INC.
Adresa: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Ovlašteni predstavnik u Europi: ASUS COMPUTER GmbH
Adresa, grad: HARKORT STR. 21-23, 40880 RATINGEN
Zemlja: GERMANY

izjavljujemo da sljedeći uređaj:

Naziv proizvoda: AX5400 Dual Band WiFi Router
Naziv modela: XD6

Dodatni podaci: ANNEX I

Predmet gore opisane izjave u sukladnosti je s relevantnim usklađenim zakonima Unije:

Direktiva o radijskoj opremi - 2014/53/EU

Article 3.1(a)
EN 50385:2017 , EN 50665:2017 , EN 62311:2008 , EN 62368-1:2014/A11:2017
Article 3.1(b)
Draft EN 301 489-1 V2.2.0 , Draft EN 301 489-17 V3.2.0 , EN 55024:2010/A1:2015 , EN 55032:2015/AC:2016 ,
EN 55035:2017 , EN 61000-3-2:2014 , EN 61000-3-3:2013
Article 3.2
EN 300 328 V2.2.2 , EN 301 893 V2.1.1

Radio Equipment Class
Class 2

Direktiva o ekodizajnu - 2009/125/EZ

(EU) 2019/1782 , 1275/2008/EC , EU 801/2013

RoHS Direktiva - 2011/65/EU

2015/863/EU , EN 50581:2012

Potpis:

S.y. Shian, Glavni izvršni direktor/CEO

Mjesto potpisa: Taipei, Taiwan
Datum izdavanja: 12/04/2021

EU Prohlášení o shodě



Níže podepsaný,

Výrobce: ASUSTeK COMPUTER INC.
Adresa: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Autorizovaný zástupce v Evropě: ASUS COMPUTER GmbH
Adresa, město: HARKORT STR. 21-23, 40880 RATINGEN
Země: GERMANY
prohlašuje, že následující přístroj:
Název produktu: AX5400 Dual Band WiFi Router
Název modelu: XD6

Další informace: ANNEX I

Výše uvedený předmět tohoto prohlášení vyhovuje příslušné unijní harmonizační legislativě:

Rádiová Zařízení Směrnice - 2014/53/EU

Článek 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Článek 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Článek 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Třída rádiových zařízení

Třída 2

Ekodesignu Směrnice - 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Směrnice - 2011/65/EU

2015/863/EU, EN 50581:2012

Podpis:

S.y. Shian, Výkonný ředitel/CEO

Místo vydání:

Taipei, Taiwan

Datum vydání:

12/04/2021

1 of 2

[Hungarian] CE statement

EU-megfelelőségi nyilatkozat



Mi, alulírottak

Gyártó: ASUSTek COMPUTER INC.
Cím: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Hivatalos képviselő Európában: ASUS COMPUTER GmbH
Cím (város): HARKORT STR. 21-23, 40880 RATINGEN
Ország: GERMANY

kijelentjük, hogy az alábbi berendezés:

Terméknév: AX5400 Dual Band WiFi Router
Típusnév: XD6

További információk: ANNEX I

A fent ismertetett nyilatkozat tárgya megfelel az Unió ide vonatkozó összehangolt jogszabályainak:
Rádióberendezésekre vonatkozó irányelv - 2014/53/EU

Article 3.1(a)
EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)
Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2
EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class
Class 2

Környezetbarát tervezésre vonatkozó irányelv - 2009/125/EK
(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS irányelv - 2011/65/EU
2015/863/EU, EN 50581:2012

Alíráás:

S.y. Shian, Vezérigazgató/CEO

Kiadás helye:
Kiadás dátuma:

Taipei, Taiwan
12/04/2021

1 OF 2

ES Atbilstības deklarācija



Mēs, zemāk parakstījušies,

Ražotājs:

ASUSTeK COMPUTER INC.

Adrese:

1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan

Pilnvarotais pārstāvis Eiropā:

ASUS COMPUTER GmbH

Adrese, pilsēta:

HARKORT STR. 21-23, 40880 RATINGEN

Valsts:

GERMANY

paziņojam, ka šāda ierīce:

Izstrādājuma nosaukums:

AX5400 Dual Band WiFi Router

Modeļa nosaukums:

XD6

Additional information: ANNEX I

Iepriekš minētais deklarācijas priekšmets atbilst attiecīgajiem ES saskaņošanas tiesību aktiem:

Radioaprikojuma direktīva – 2014/53/ES

Article 3.1(a)

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class

Class 2

Ekodizaina direktīva – 2009/125/EK

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktīva – 2011/65/ES

2015/863/EU, EN 50581:2012

Paraksts:

S.y. Shian, Izpilddirektors/CEO

Izdošanas vieta:

Taipei, Taiwan

Izdošanas datums:

12/04/2021

1 of 2

[Lithuanian] CE statement

ES atitikties deklaracija



Mes, toliau pasirašiusieji:

Gamintojas:	ASUSTeK COMPUTER INC.
Adresas:	1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Igaliotasis atstovas Europoje:	ASUS COMPUTER GmbH
Adresas, miestas:	HARKORT STR. 21-23, 40880 RATINGEN
Šalis:	GERMANY

atsakingai pareiškiamo, kad šis prietaisas:

Gaminio pavadinimas:	AX5400 Dual Band WiFi Router
Modelio pavadinimas:	XD6

Papildoma informacija: ANNEX I

Pirmiau nurodytas deklaracijos objektas atitinka taikytinus suderintus Sąjungos teisės aktus:

Radio ryšio įrenginių direktyva – 2014/53/ES

Article 3.1(a)
EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)
Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2
EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class
Class 2

Ekodizaino direktyva – 2009/125/EB

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS direktyva – 2011/65/ES

2015/863/EU, EN 50581:2012

Parašas:

S.y. Shian, Vyriausiasis pareigūnas/CEO

Leidimo vieta:

Taipei, Taiwan

Leidimo data:

12/04/2021

1 of 2

Deklaracja zgodności UE



My, niżej podpisani,

Producent: ASUSTeK COMPUTER INC.
Adres: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Autoryzowany przedstawiciel w Europie: ASUS COMPUTER GmbH
Adres, miasto: HARKORT STR. 21-23, 40880 RATINGEN
Kraj: GERMANY

oświadczamy, że niniejsze urządzenie:

Nazwa produktu: AX5400 Dual Band WiFi Router
Nazwa modelu: XD6

Informacje dodatkowe: ANNEX I

będące przedmiotem opisanej powyżej deklaracji spełnia wymogi właściwych przepisów unijnego prawodawstwa harmonizacyjnego:

Urządzenia radiowe Dyrektywa – 2014/53/EU

Artykuł 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Artykuł 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Artykuł 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Klasa urządzeń Radiowych

Klasa 2

Ekoprojekt Dyrektywa – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Dyrektywa – 2011/65/EU

2015/863/EU, EN 50581:2012

Podpis:

S.y. Shian, Dyrektor naczelny/CEO

Miejsce wystawienia:

Taipei, Taiwan

Data wystawienia:

12/04/2021

[Romanian] CE statement

Declarația UE de Conformitate



Subsemnatul,

Subsemnatul: ASUSTeK COMPUTER INC.
Adresă: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Reprezentant autorizat în Europa: ASUS COMPUTER GmbH
Adresă, Oraș: HARKORT STR. 21-23, 40880 RATINGEN
Țară: GERMANY

declară următorul aparat:

Nume Produs: AX5400 Dual Band WiFi Router
Nume Model: XD6

Informații suplimentare: ANNEX I

Obiectul declarației descris mai sus este în conformitate cu legislația relevantă de armonizare a Uniunii:

Echipamentele radio Directiva – 2014/53/EU

Articolul 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Articolul 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Articolul 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Clasa echipamentului Radio

Clas 2

Ecologică Directiva – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Directiva – 2011/65/EU

2015/863/EU, EN 50581:2012

Semnătură:

S.y. Shian, Director executive/CEO

Locul emiterii:

Taipei, Taiwan

Data emiterii:

12/04/2021

Izjava EU o skladnosti



Spodaj podpisani

Proizvajalec: ASUSTeK COMPUTER INC.
Naslov: 1F, No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Pooblaščen zastopnik v Evropi: ASUS COMPUTER GmbH
Naslov, mesto: HARKORT STR. 21-23, 40880 RATINGEN
Država: GERMANY
izjavljamo, da je ta naprava:
Ime izdelka: AX5400 Dual Band WiFi Router
Ime modela: XD6

Dodatne informacije: ANNEX I

Predmet zgoraj navedene izjave je v skladu z ustrežno harmonizacijsko zakonodajo Unije:

Direktiva o radijski opremi - 2014/53/EU

Article 3.1 (a)

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1 (b)

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class

Class 2

Direktiva o okoljsko primernih zasnovi - 2009/125/ES

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktiva - 2011/65/EU

2015/863/EU, EN 50581:2012

Podpis:

S.y. Shian, Izvršni direktor/CEO

Kraj izdaje:

Taipei, Taiwan

Datum izdaje:

12/04/2021

Vyhlasenie o zhode EÚ



My, dolu podpísaní,

Výrobca: ASUSTeK COMPUTER INC.
Adresa: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Oprávnený zástupca v Európe: ASUS COMPUTER GmbH
Adresa, mesto: HARKORT STR. 21-23, 40880 RATINGEN
Krajina: GERMANY

týmto vyhlasujeme, že nasledovné zariadenie:

Názov výrobku: AX5400 Dual Band WiFi Router
Názov modelu: XD6

Doplnujúce informácie: ANNEX I

Predmet vyhlásenia, ktorý je vyššie opísaný, je v súlade s príslušnou harmonizáciou právnych predpisov v EÚ:

Smernica o rádiových zariadeniach č. 2014/53/EÚ

Article 3.1(a)

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class

Class 2

Smernica o ekodizajne č. 2009/125/ES

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

Smernica RoHS č. 2011/65/EÚ

2015/863/EU, EN 50581:2012

Podpis:

Sy. Shian, Výkonný riaditeľ/CEO

Miesto vydania:

Taipei, Taiwan

Dátum vydania:

12/04/2021

1 of 2

[Turkish] CE statement

EU Uygunluk Beyanı



Biz, bu imza altındakiler

Üretici: ASUSTeK COMPUTER INC.
Adres: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
Avrupa'daki Yetkili: ASUS COMPUTER GmbH
Adres, Şehir: HARKORT STR. 21-23, 40880 RATINGEN
Ülke: GERMANY

Aşağıdaki ürünleri beyan ediyoruz:

Ürün adı: AX5400 Dual Band WiFi Router
Model adı: XD6

Ek bilgi: ANNEX I

Yukarıda belirtilen beyanın konusu birlik yasalarına göre uygundur:

Telsiz Donanım Direktifi - 2014/53/EU

Madde 3.1a

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Madde 3.1b

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016,
EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Madde 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radyo Ekipman snf

Classe 2

Ekotasarım Direktif - 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Direktif - 2011/65/EU

2015/863/EU, EN 50581:2012

İmza:

S.y. Shian, Baş yönetici/CEO

Sürüm yeri:

Taipei, Taiwan

Sürüm tarihi:

12/04/2021

1 of 2

Service și Asistență

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

