

Manual utilizare

4G09
4G07
4G06
4G06c
4G03



Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

Declarație privind drepturile de autor

© 2024 Shenzhen Tenda Technology Co., Ltd. Toate drepturile rezervate.

Tenda Este o marcă comercială înregistrată, deținută legal de Shenzhen Tenda Technology Co., Ltd. Alte mărci și nume de produse menționate aici sunt mărci comerciale sau mărci comerciale înregistrate ale deținătorilor respectivi. Drepturile de autor ale întregului produs, inclusiv accesoriile și software-ul acestuia, aparțin Shenzhen Tenda Technology Co., Ltd. Nicio parte a acestei publicații nu poate fi reprodusă, transmisă, transcrisă, stocată într-un sistem de recuperare sau tradusă în nicio limbă, sub nicio formă sau prin niciun mijloc, fără permisiunea prealabilă scrisă a Shenzhen Tenda Technology Co., Ltd.

Declinare a responsabilității

Imaginile și specificațiile produsului prezentate aici sunt doar pentru referință. Pentru a îmbunătăți designul intern, funcționalitatea operațională și/sau fiabilitatea, Tenda își rezervă dreptul de a modifica produsele fără a notifica în prealabil nicio persoană sau organizație cu privire la aceste revizuri sau modificări. Tenda nu își asumă nicio răspundere pentru eventualele probleme care pot apărea din utilizarea sau aplicarea produsului descris aici. S-au depus toate eforturile pentru a asigura acuratețea conținutului acestui document, dar toate declarațiile, informațiile și recomandările incluse nu constituie o garanție de niciun fel, expresă sau implicită.

Prefață

Vă mulțumim că ați ales Tenda! Acest ghid este o completare a *Ghidului de instalare rapidă*. *Ghidul de instalare rapidă* oferă instrucțiuni pentru configurarea rapidă a echipamentului și conectarea acestuia la internet, în timp ce acest ghid conține detalii despre fiecare funcție și vă explică cum să le configurați.

Acest manual vă prezintă funcțiile și caracteristicile echipamentelor **Tenda 4G09, 4G07, 4G06, 4G06c, 4G03**. Toate exemplificările și capturile de ecran din acest manual, dacă nu se specifică altfel, sunt preluate de la echipamentul **Tenda 4G09**.

Note importante

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termenii în română și engleză.

Funcționalitățile, configurările, informațiile dar și capturile de ecran din acest ghid sunt doar cu titlu de exemplu. Acestea pot fi diferite de produsele reale pe care le-ați achiziționat, dar nu afectează utilizarea normală.



Acest ghid explică în mare parte funcțiile din **pagina web de gestionare a echipamentului**, însă în unele secțiuni sunt prezentate și funcționalitățile **aplicației Tenda WiFi, de Android și iOS, pentru gestionarea echipamentului**.

Dacă funcția sau parametrul este afișat cu gri pe interfața de utilizare web a produsului, modelul produsului nu este acceptat sau nu poate fi modificat.

Elementele tipografice care pot fi găsite în acest document sunt definite după cum urmează.

Articol	Format text, alte simboluri	Exemplu
Meniuri în cascadă	>	Nnaviga la Stare > Stare dispozitiv
Parametru și valoare	Text aldin	Setați Numele utilizatorului la Tom .
Meniuri și opțiuni din interfața de gestionare	Text aldin	În pagina Politică , faceți clic pe butonul OK .
Variabilă	<i>Text cursiv</i>	Format: <i>XX:XX:XX:XX:XX:XX</i>
Mesaje și alte denumiri	„Ghilimele”	Apare mesajul „Succes”.

Simbolurile care pot fi găsite în acest document sunt definite după cum urmează.

Simbol	Sens
 NOTE	Notă: Acest format este folosit pentru a evidenția informații importante sau de interes special. Ignorarea acestui tip de notă poate duce la configurații ineficiente, pierderi de date sau deteriorarea dispozitivului.
 TIP	Sfat: Acest format este folosit pentru a evidenția o procedură care va economisi timp sau resurse.

Pentru mai multe documente

Dacă doriți să obțineți mai multe documente ale dispozitivului, accesați

<https://www.tendacn.com/ro> și căutați modelul de produs corespunzător apoi accesați secțiunile Specificații, Descărcări, Resurse și Video.

Suport tehnic

Contactați-ne dacă aveți nevoie de mai mult ajutor. Vom fi bucuroși să vă ajutăm cât mai curând posibil.

Adresă de e-mail: support.romania@tenda.cn

Site: <https://www.tendacn.com/ro>

Istoria reviziilor

Tenda caută în mod constant modalități de a-și îmbunătăți produsele și documentația. Următorul tabel indică orice modificări care ar fi putut fi făcute de la lansarea manualului.

Versiune	Data	Note
V1.0	2024.11.03	Prima publicare

Cuprins

Prezentare generală echipament	1
1.1 Indicatori LED	1
1.2 Porturi, conectori și butoane	2
1.3 Eticheta	4
Interfața web gestionare	5
2.1 Conectare la interfața web de gestionare	5
2.2 Deconectare de la interfața web de gestionare	6
2.3 Aspect pagină web de gestionare	7
Stare internet	8
3.1 Vizualizare stare conexiune la internet	8
3.2 Vizualizare informații rețele Wi-Fi	10
3.3 Vizualizare informații de sistem	11
3.4 Vizualizare informații dispozitive online	15
Setări Internet	17
4.1 Conectare la internet prin rețele mobile	17
4.2 Conectare la internet prin cablu Ethernet	22
4.3 Failover, redundanța conexiunii la internet	28
Setări Wi-Fi	31
5.1 Nume și parolă Wi-Fi	31
5.2 Programare funcționare Wi-Fi	38
5.3 Canalele și lățimea acestora	40
5.4 Reglare putere de transmisie Wi-Fi	42
5.5 WPS	43
5.6 Beamforming+	48
5.7 Anti-interferență	49
SMS	50
6.1 Gestionare mesaje SMS	50
6.2 Setarea numărului centrului de mesagerie SMS	54
6.3 Solicitare informații trimițând comenzi USSD	55
Rețea Wi-Fi invitați	56
7.1 Prezentare generală	56
7.2 Configurare Wi-Fi invitați	57
Control parental	59
8.1 Prezentare generală	59
8.2 Configurare reguli control parental	60

8.3 Exemplu de adăugare a unei reguli de control parental	61
VPN	64
9.1 Server PPTP	64
9.2 Vizualizare utilizatori PPTP conectați	71
9.3 Client PPTP/L2TP	72
9.4 IPSec	74
Setări avansate	83
10.1 PIN SIM	83
10.2 Date mobile	87
10.3 Controlul lățimii de bandă	91
10.4 Aplicația Tenda WiFi de Android și iOS	93
10.5 Modul repaus	95
10.6 Control indicatoare LED	97
10.7 Filtru adresă MAC	98
10.8 Firewall	101
10.9 Actualizare ISP	102
10.10 Rutare statică	103
10.11 DDNS	107
10.12 Redirecționare porturi TCP și UDP din meniul Server virtual	111
10.13 DMZ	117
10.14 UPnP	121
10.15 Setări antene	122
Setări de sistem	124
11.1 Setări LAN	124
11.2 Rezervare DHCP	126
11.3 Setări WAN	128
11.4 Setări de timp	132
11.5 Parola de conectare la interfața de gestionare	134
11.6 Repornire și resetare	135
11.7 Actualizare firmware	138
11.8 Backup și restaurare configurații	141
11.9 Accesare interfață web de gestionare din afara rețelei locale	144
11.10 Starea sistemului	147
11.11 Jurnal de sistem	154
11.12 Întreținere și repornire automată	155
Anexe	156
A.1 Configurarea computerului pentru a obține automat o adresă IPv4	156
A.2 Acronime și abrevieri	159




1 Prezentare generală echipament



1.1 Indicatori LED

Indicatorii LED pot varia în funcție de modelele de dispozitiv. Vă rugăm să consultați specificațiile tehnice pentru produsul pe care l-ați achiziționat.

4G09 este folosit pentru ilustrare.



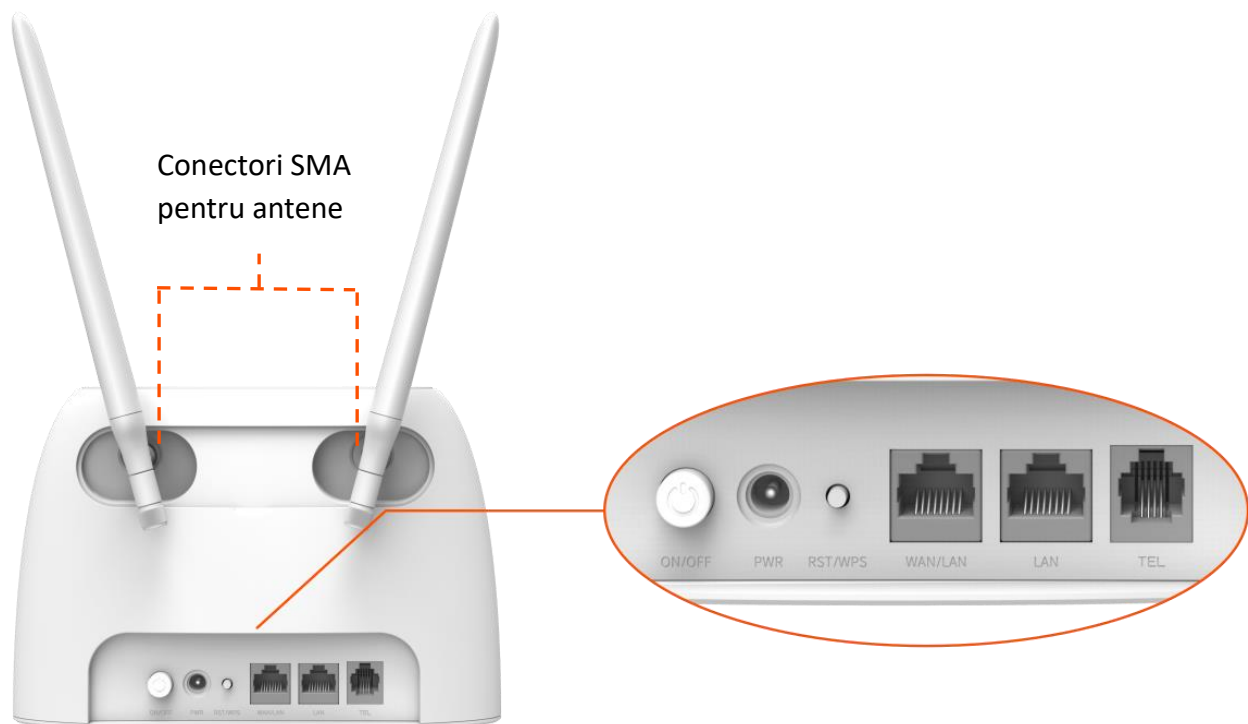
Indicator	Stare	Descriere
 Alimentare	Aprins continuu	Echipamentul este pornit.
	Oprit	Echipamentul este oprit.
 Internet	Aprins continuu	Ruterul este conectat la internet.
	Oprit	Ruterul nu reușește să se conecteze la internet.
 Wi-Fi	Aprins continuu	Rețeaua Wi-Fi a ruterului este activată.
	Clipește	Ruterul efectuează negocieri WPS.
	Oprit	Rețeaua Wi-Fi este dezactivată.

Indicator	Stare	Descriere
 Porturi RJ-45 Ethernet	Aprins continuu	Cel puțin un dispozitiv este conectat la porturile RJ-45 Ethernet de pe echipament.
	Oprit	Niciun dispozitiv conectat la porturile Ethernet.
 Nivel semnal conectare la rețelele mobile 4G/3G	3 bare	Semnal excelent.
	2 bare	Semnal bun.
	1 bară	Semnal suficient.
	Oprit	Fără semnal de la rețelele mobile.



1.2 Porturi, conectori și butoane

Porturile și butoanele pot varia în funcție de modelele de dispozitiv. Vă rugăm să consultați specificațiile tehnice pentru produsul pe care l-ați achiziționat.

4G06 este folosit pentru ilustrare aici.

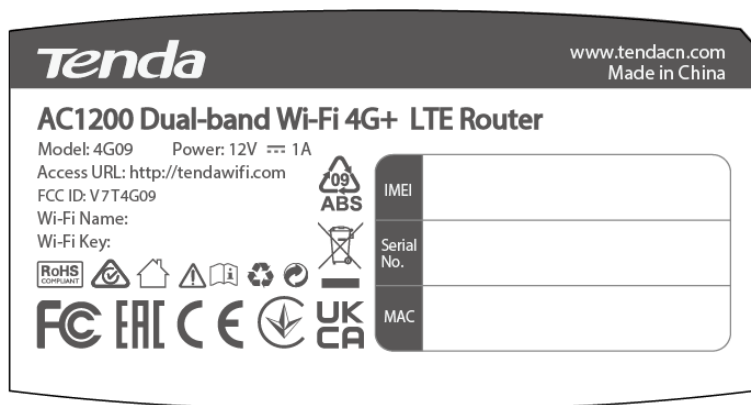


Port/Buton	Descriere
ON/OFF	Buton de pornire/oprire alimentare. Este folosit pentru a porni sau opri echipamentul Tenda.

Port/Buton	Descriere
PWR	Mufă de alimentare curent continuu. Se conectează adaptorul de curent alternativ în curent continuu inclus în pachet.
RST/WPS	Servește atât ca buton de resetare, cât și ca buton WPS. <ul style="list-style-type: none"> Resetare: Când ruterul funcționează corect, țineți apăsat butonul timp de aproximativ 8 secunde și eliberați-l când toate indicatoarele se sting și apoi se aprind. Ruterul este restaurat la setările din fabrică. WPS: Apăsați butonul și eliberați-l, indicatorul led  (Wi-Fi) va clipi. Ruterul se pregătește pentru negocierea WPS. Configurați dispozitivele wireless compatibile cu WPS în maxim 2 minute pentru a începe negocierea WPS cu ruterul.
WAN/LAN	Este un port RJ-45 Ethernet rapid, care poate servi ca port WAN sau port LAN. În mod implicit, este un port LAN.
LAN	Este un port RJ-45 LAN folosit pentru conectare dispozitive cu fir, cum ar fi un computer. Când funcția IPTV este activată, aceasta servește drept port IPTV pentru a fi conectat la set-top box.
TEL	Port RJ-11 pentru conectarea unui telefon fix. Doar pentru modelul 4G06 . Este folosit pentru conectarea la un telefon fix folosind cablul telefonic inclus pentru serviciul de voce, prin VoLTE. <p> TIP</p> <ul style="list-style-type: none"> Serviciul de voce este disponibil numai cu o cartelă SIM introdusă și serviciul VoLTE. Asigurați-vă că datele mobile sunt activate și că ruterul poate accesa internetul înainte de a utiliza serviciul de voce. Asigurați-vă că furnizorul oferă servicii de voce pentru cartela introdusă. Se pot folosi majoritatea telefoanelor fixe care permit conectarea cu un cablu cu conectori RJ-11. Telefonul trebuie introdus și puteți efectua și primi apeluri. Accesul la internet nu este disponibil atunci când efectuați apeluri telefonice prin rețeaua 3G.
Conectori SMA pentru antenele de conectare la rețelele celulare	Cele două antene detașabile se conectează la dispozitiv prin conectori SMA. Modelul 4G03 nu vine cu antene detașabile, are antene interne.
SIM	Slotul din partea inferioară a echipamentului unde se introduce cartela SIM format 2FF. În pachet sunt incluse adaptoare pentru nano-SIM și micro-SIM.

1.3 Eticheta

Eticheta de pe echipament arată modelul, puterea de alimentare, adresa URL de acces din rețeaua locală, ID-ul FCC, numele Wi-Fi implicit, cheia (parola) Wi-Fi implicită, identificatorul IMEI, numărul de serie și adresa MAC a echipamentului Tenda. Următoarea figură este doar pentru referință.



Model: specifică modelul ruterului.

Power (Puterea): specifică sursa de alimentare pentru ruter.

Access URL (URL de acces): este adresa URL utilizată pentru a vă conecta la interfața de utilizare web a ruterului.

FCC ID: specifică numărul de identificare al FCC pentru acest echipament. **FCC** (Federal Communications Commission) este agenția guvernamentală din SUA care reglementează comunicațiile prin radio, televiziune, satelit, cablu și internet, gestionând spectrul de frecvențe și promovând inovația și protecția consumatorilor.

Wi-Fi Name (Nume Wi-Fi): specifică numele Wi-Fi implicit al ruterului.

Wi-Fi Key (Cheie Wi-Fi): specifică parola Wi-Fi implicită a ruterului.

IMEI: este codul unic de identificare pentru acest dispozitiv mobil.

Serial No. (Număr de serie): este necesar dacă aveți nevoie de asistență tehnică pentru a vă repara ruterul.

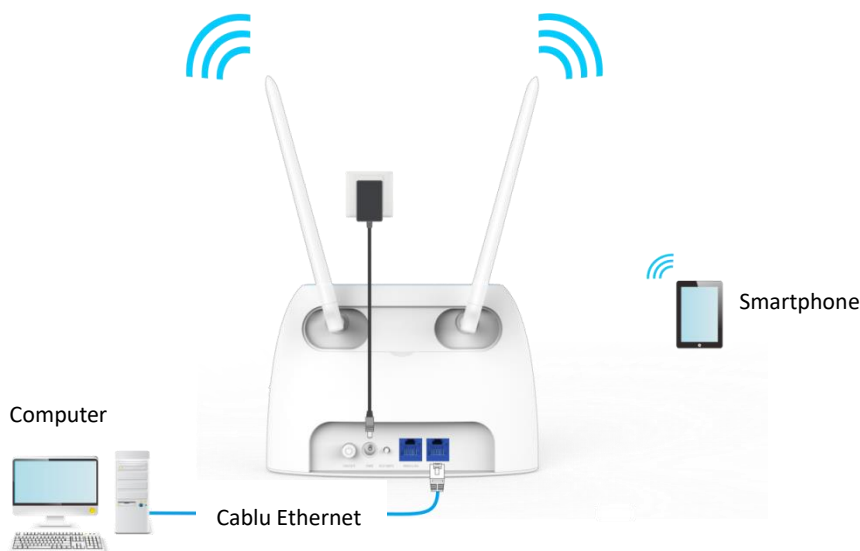
MAC: specifică adresa MAC a ruterului.

2

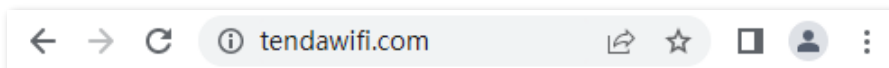
Interfața web gestionare

2.1 Conectare la interfața web de gestionare

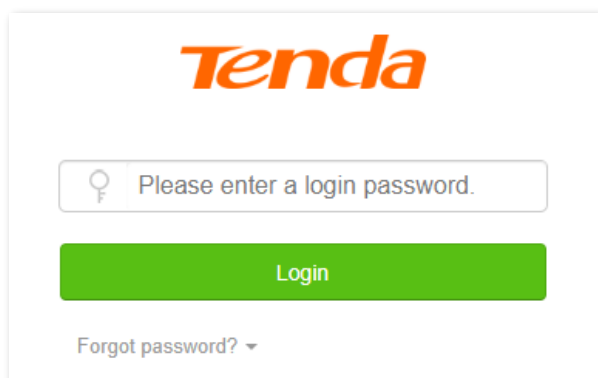
1. Conectați-vă smartphone-ul la rețeaua Wi-Fi emisă de echipament sau conectați un computer la un port LAN al ruterului. În mod implicit, porturile etichetate WAN/LAN și LAN sunt toate porturi de acces din rețeaua locală (LAN).



2. Porniți un browser web pe dispozitivul conectat la router și accesați din bara de adrese, nu câmpul Căutare, <http://tendawifi.com>.



3. Introduceți parola de conectare, dacă ați setat una, și faceți clic pe **Login (Conectare)**.



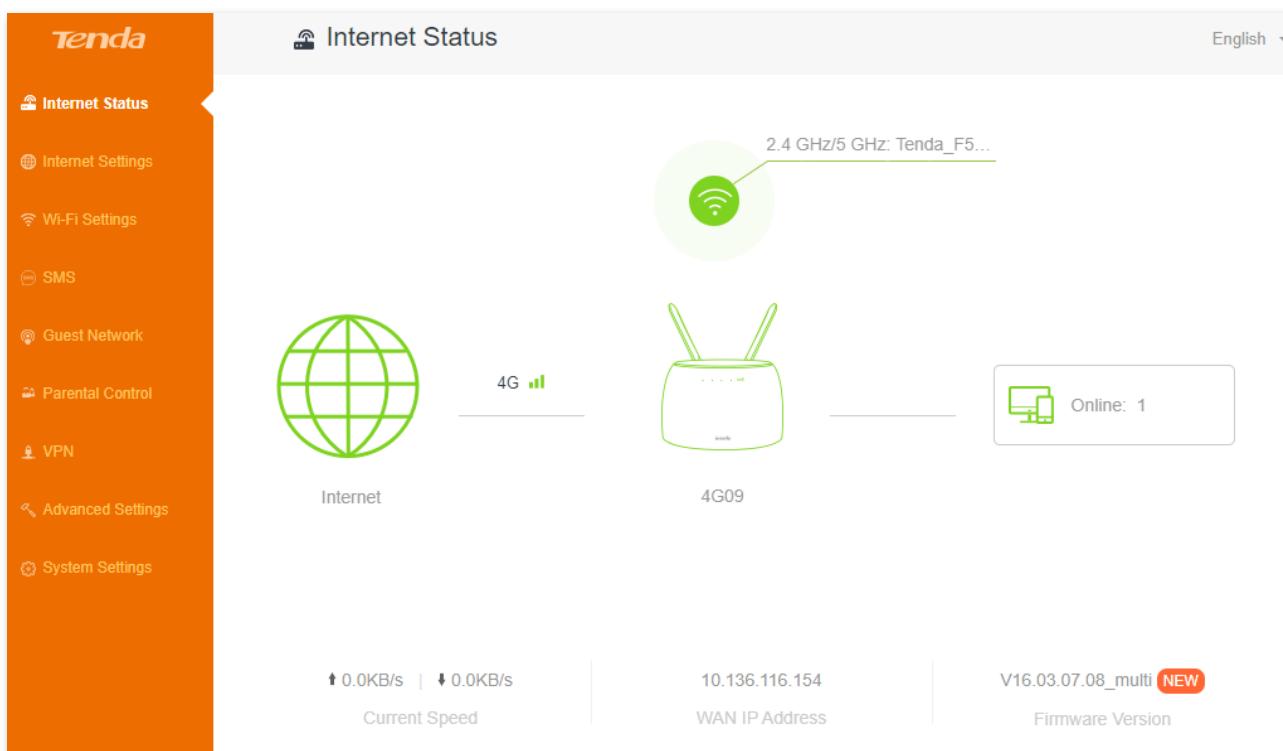
---Sfârșit



Dacă pagina de mai sus nu apare, încercați următoarele soluții:

- Asigurați-vă că ruterul este pornit.
- Asigurați-vă că computerul este conectat la un port LAN al ruterului și [configurați computerul pentru a obține automat o adresă IP](#).
- [Restabiliți ruterul la setările din fabrică](#) și încercați din nou.
- Dacă v-ați conectat inițial prin Wi-Fi, asigurați-vă că telefonul sau laptopul au rămas conectate la rețeaua Wi-Fi. În unele cazuri, sistemul de operare al dispozitivului client se deconectează de la rețeaua Wi-Fi dacă aceasta nu are încă acces la internet.

Prima pagină din interfața web de gestionare arată astfel:

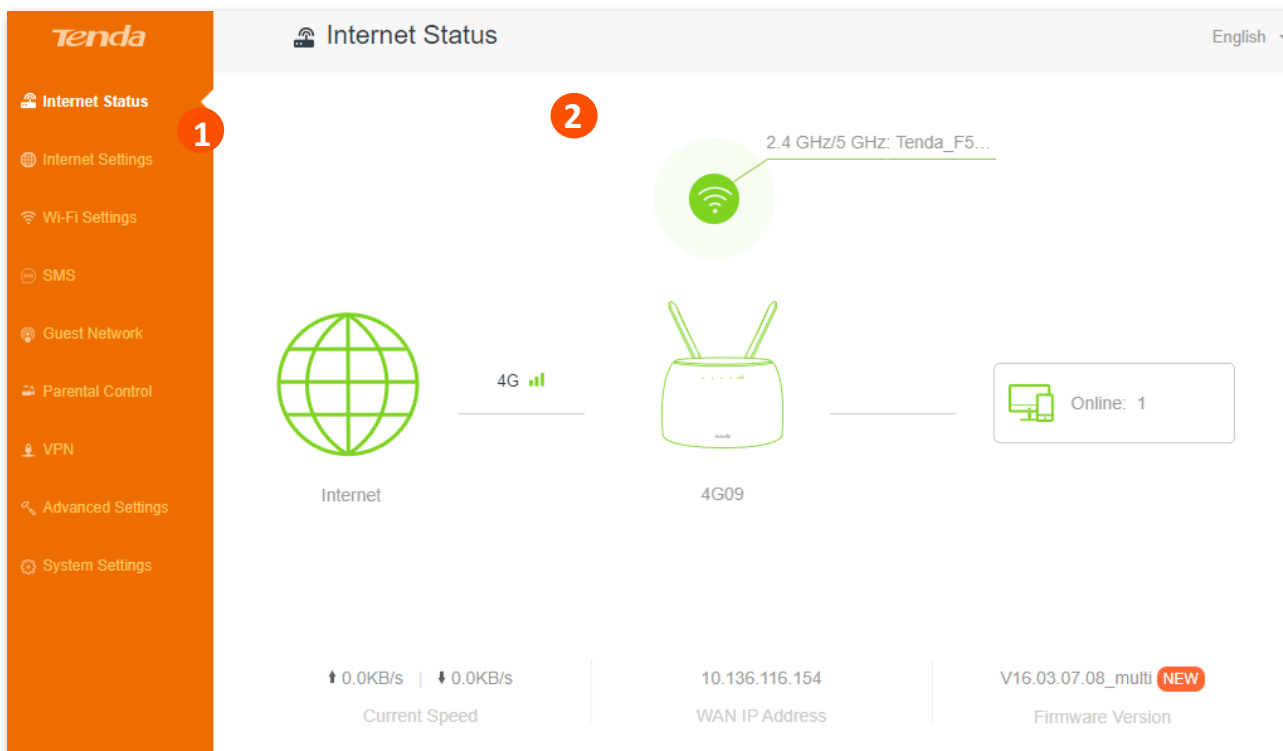


2.2 Deconectare de la interfața web de gestionare

Dacă vă conectați la interfața web de gestionare a ruterului și nu efectuați nicio operațiune în decurs de **5 minute**, ruterul vă deconectează automat. De asemenea, vă puteți deconecta făcând clic pe **Exit (Ieșire)** din colțul din dreapta sus al paginii web de gestionare.

2.3 Aspect pagină web de gestionare

Interfața web de gestionare a ruterului constă din două secțiuni, anume, bara de navigație (1) și zona de configurare (2). Următoarea figură este doar pentru referință.



SN	Nume	Descriere
1	Bara de navigare	Folosit pentru a afișa meniul de funcții de pe echipament.
2	Zona de configurare	Folosit pentru a modifica sau vizualiza configurațiile echipamentului.

3 Stare internet

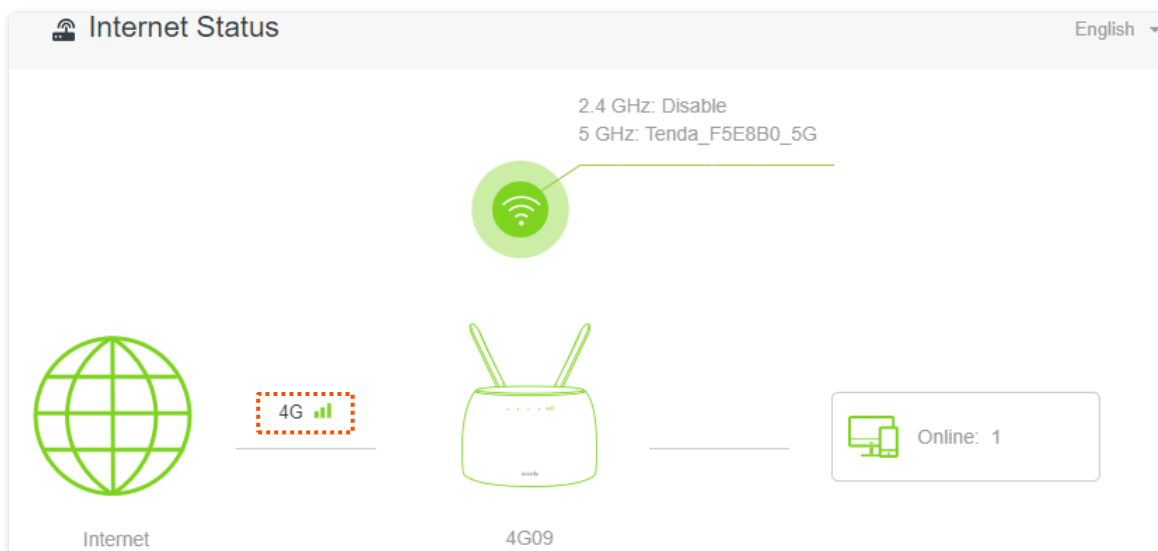
Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

3.1 Vizualizare stare conexiune la internet

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a routerului](#), și navigați la **Internet Status (Stare Internet)**.

3.1.1 Conexiune normală

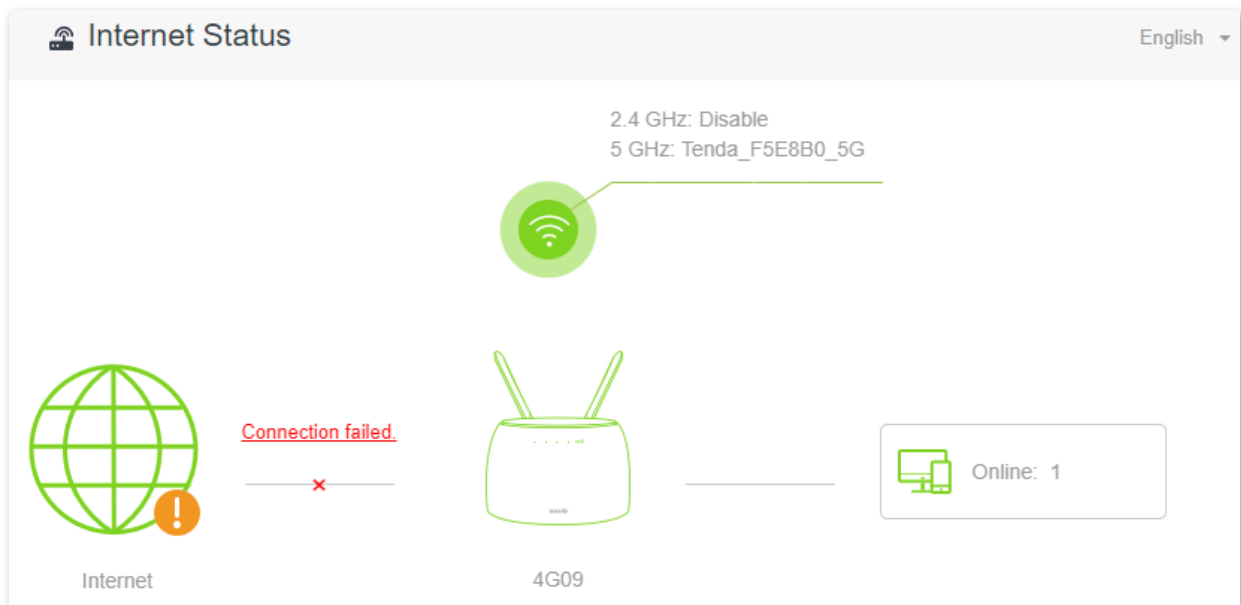
Imaginea de mai jos arată o conexiune reușită la internet prin date mobile, prin rețeaua 4G. Este afișat textul 4G cu 3 bare verzi între pictograma glob (Internet) și pictograma echipamentului Tenda.



3.1.2 Conexiune eșuată

Conexiunea a eșuat

Când mesajul "**Connection failed (Conexiunea a eșuat)**" este afișat între pictograma în formă de glob (Internet) și cea a ruterului (Model echipament), indică faptul că conexiunea la internet este anormală. Următoarea figură este doar pentru referință.



În primul rând, încercați următoarele soluții:

- Navigați la **Internet Settings (Setări Internet)** și asigurați-vă că funcțiile **Mobile Data (Date mobile)** și **Data Roaming (Roaming de date)** sunt activate, iar opțiunea de date mobile este setată la **4G Preferred (4G prioritar)**.
- Navigați la **Internet Settings (Setări Internet)** și asigurați-vă că parametrii setărilor dial-up sunt identificați automat de ruter. Dacă nu, verificați dacă cartela SIM este introdusă corect sau consultați [Crearea manuală a unui profil APN pentru a accesa internetul](#).
- Dacă cartela SIM este identificată cu succes, dar nu este disponibil acces la internet, este posibil ca cartela SIM să fi rămas fără credit. Contactați furnizorul dvs. de servicii Internet (ISP) pentru asistență.

Dacă problema persistă, încercați următoarele soluții:

- Asigurați-vă că cablul Ethernet este conectat corect.
- Asigurați-vă că alegeți tipul de conexiune potrivit. Dacă nu sunteți sigur(ă), contactați ISP-ul dvs. cu privire la tipul de conexiune.
- Contactați asistența tehnică Tenda pentru ajutor.

Cartelă SIM blocată

Dacă mesajul "**Please unlock the SIM card (Vă rugăm să deblocați cartela SIM)**" este afișat, atunci se indică faptul că cartela SIM este blocată cu un cod PIN. Consultați [Deblocarea cartelei SIM în interfața de utilizare](#) web.


Nicio cartelă SIM introdusă

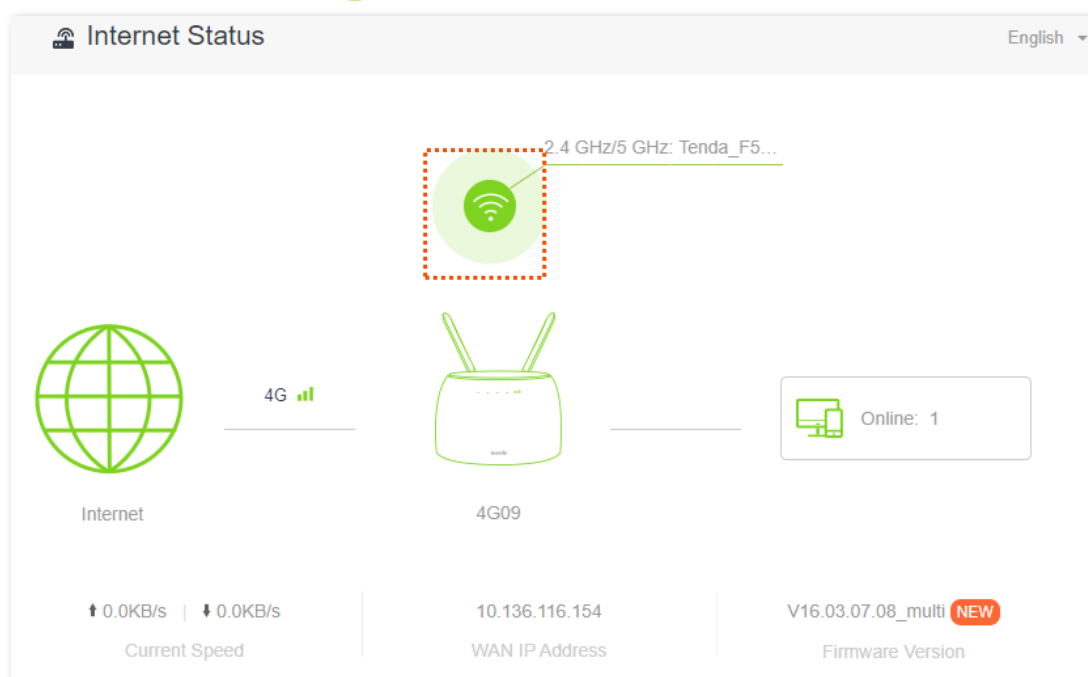
Dacă mesajul "**No SIM card inserted (Nicio cartelă SIM introdusă)**" este afișat, asigurați-vă că cartela SIM este introdusă corect.

Limita lunară de date a fost atinsă

Dacă mesajul "The monthly data limit is reached. (Limita lunară de date este atinsă.)" este afișat, atunci se indică faptul că ruterul s-a deconectat automat de la internet atunci când limita este atinsă. Consultați [Date mobile](#) pentru a modifica parametrii aferenți.

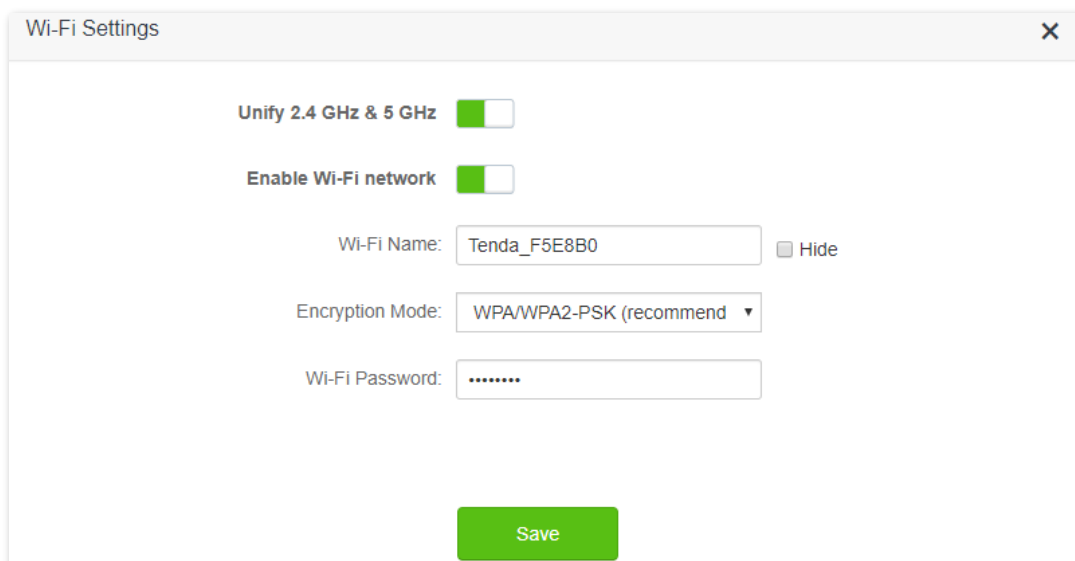
3.2 Vizualizare informații rețele Wi-Fi

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Status (Stare Internet)**.
3. Faceți clic pe pictograma .




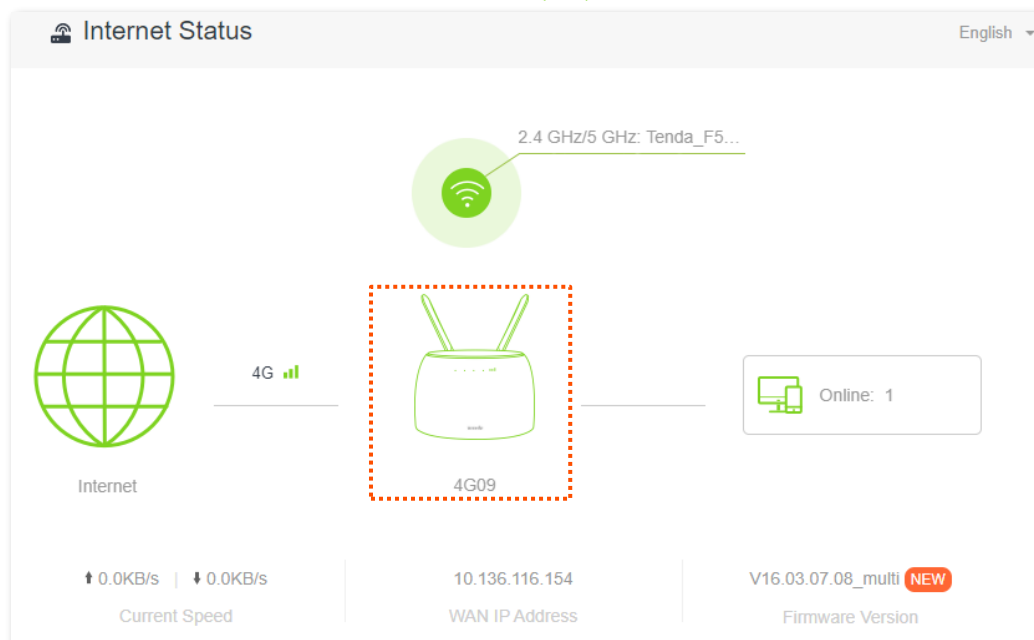
---Sfârșit

În noua pagină deschisă puteți modifica parametrii rețelelor Wi-Fi emise de echipament după cum este necesar.



3.3 Vizualizare informații de sistem

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Status (Stare Internet)**.
3. Faceți clic pe pictograma echipamentului .



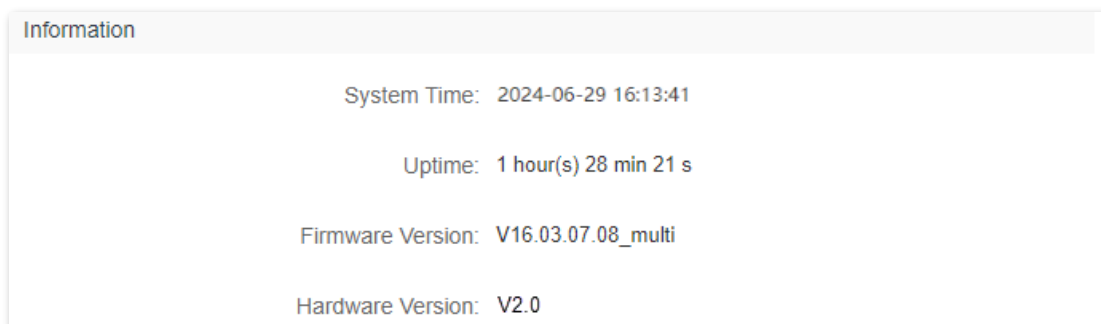
---Sfârșit



Pentru descrierea detaliată a parametrilor de pe această pagină, consultați [Starea sistemului](#).

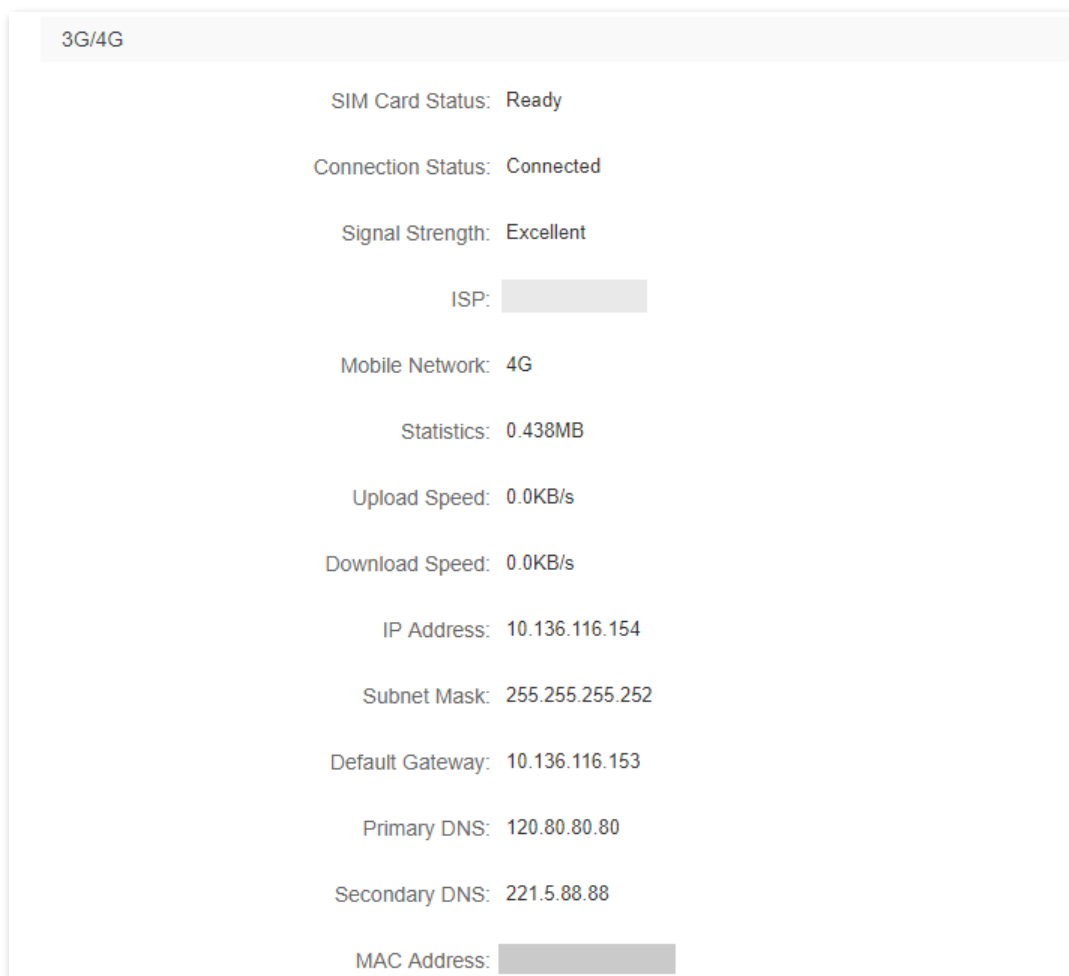
3.3.1 Informații de bază

În această secțiune, puteți vizualiza informațiile de bază ale echipamentului, cum ar fi data și ora sistemului, timpul de funcționare neîntreruptă, versiunea de firmware și versiunea hardware. Următoarea figură este doar pentru referință.



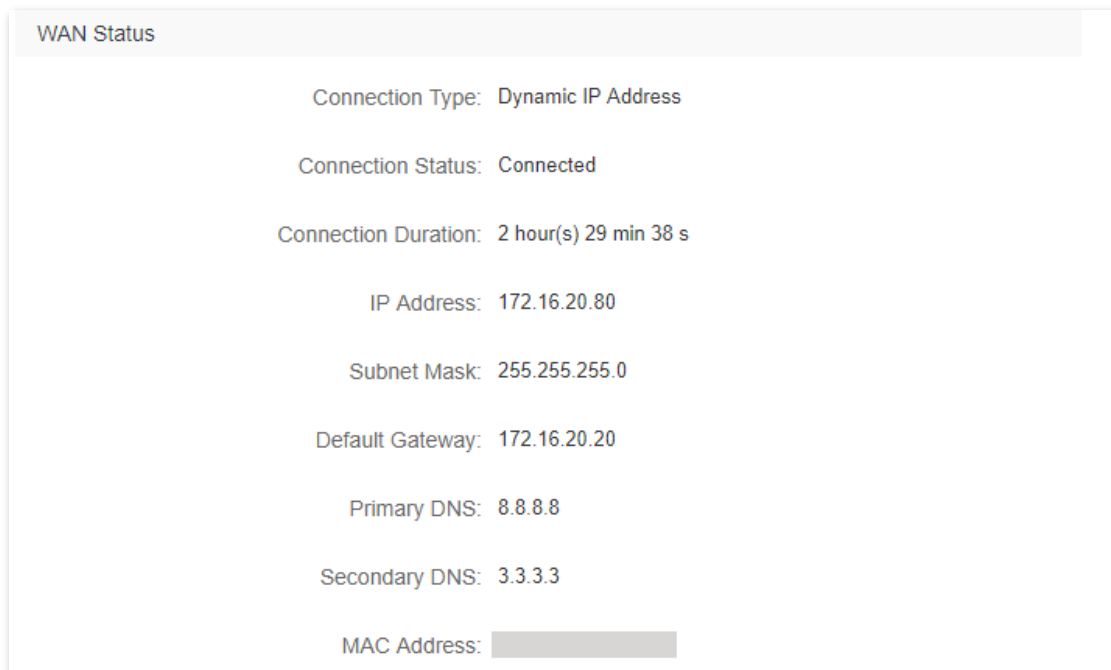
3.3.2 Stare 3G/4G

Pe această secțiune, puteți vizualiza informațiile despre cartela SIM și rețeaua 3G/4G. Următoarea figură este doar pentru referință.



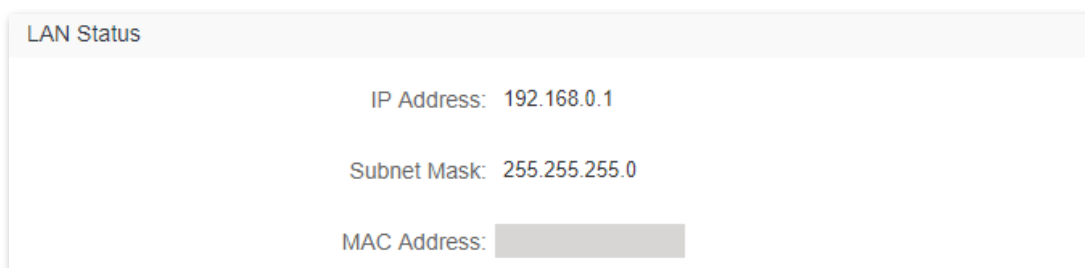
3.3.3 Stare WAN

În această secțiune, puteți vizualiza informațiile portului fizic WAN, inclusiv tipul conexiunii, starea conexiunii și durata conexiunii. Următoarea figură este doar pentru referință.



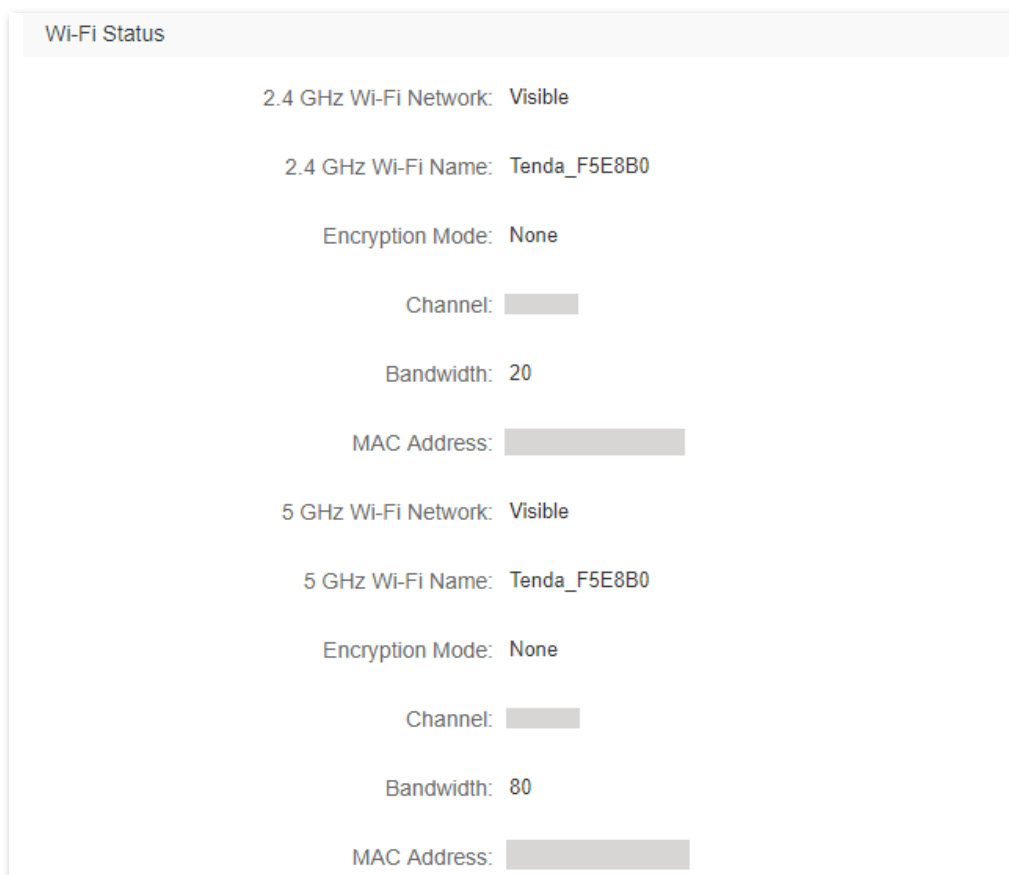
3.3.4 Stare LAN

În această secțiune, puteți vizualiza informațiile aferente echipamentului Tenda aferente rețelei interne, cum ar fi adresa IPv4 din LAN, masca de subrețea și adresa MAC. Următoarea figură este doar pentru referință.



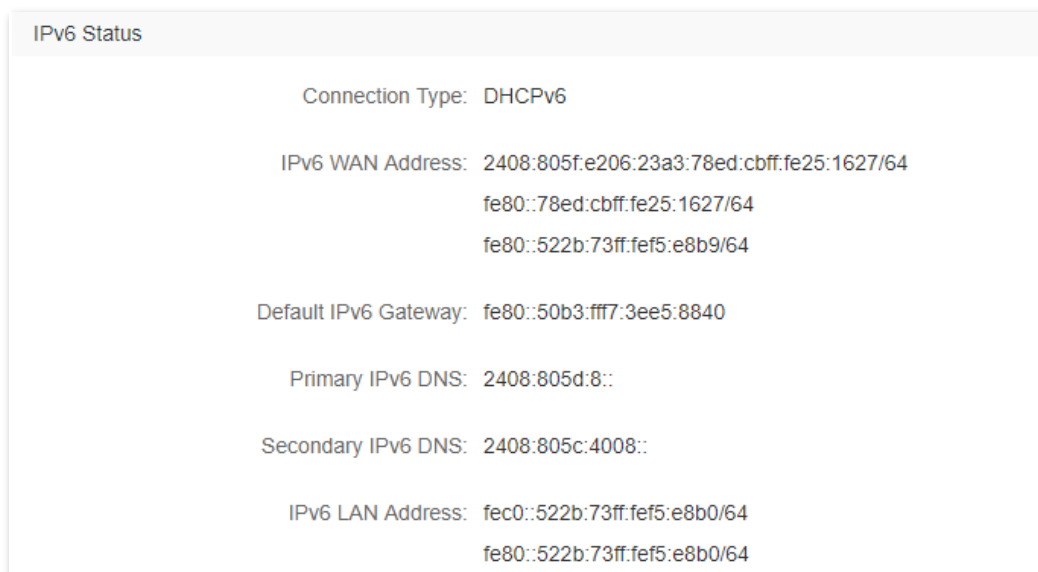
3.3.5 Stare Wi-Fi

În această secțiune, puteți vizualiza informațiile rețelelor Wi-Fi de 2,4 GHz și 5 GHz (pentru unele modele), inclusiv starea conexiunii, vizibilitatea rețelelor Wi-Fi, numele rețelelor Wi-Fi și modul de criptare, canalul și lățimea acestuia și așa mai departe. Următoarea figură este doar pentru referință.



3.3.6 Stare IPv6


În această secțiune este afișată numai când funcția IPv6 este activată. Puteți vizualiza informațiile conexiunii IPv6, inclusiv tipul de conexiune, adresele IPv6 pe WAN și din LAN. Următoarea figură este doar pentru referință.

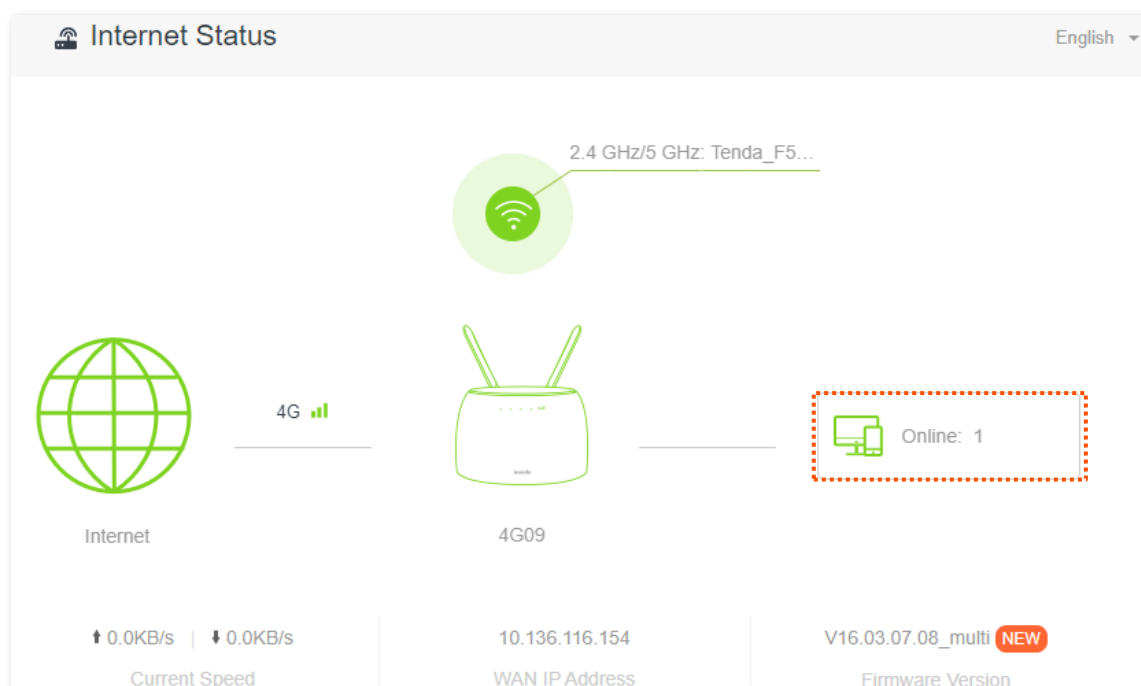


3.4 Vizualizare informații dispozitive online

Tot pe prima pagină puteți vizualiza informații despre dispozitivele conectate la router, inclusiv rata la încărcare, la descărcare și tipul de acces. De asemenea, puteți vizualiza și adăuga dispozitive la o listă de dispozitive blocate pe baza adresei MAC, anume **Blacklist**.

Pentru a vedea terminalele conectate:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Status (Stare Internet)**.
3. Faceți clic pe pictograma  Online: .






---Sfârșit

3.4.1 Blocare acces la rețea pentru dispozitivele client

Pentru a bloca accesul la rețea și, implicit, la internet al unui dispozitiv client pe baza adresei MAC (Media Access Control) a adaptorului de rețea prin care se conectează, acesta trebuie adăugat pe așa-numita **Listă neagră (Blacklist)**. Este important de reținut că un dispozitiv client poate utiliza o adresă MAC aleatorie la fiecare încercare de conectare la rețea, ceea ce înseamnă că adresele MAC ale adaptoarelor de rețea pot fi modificate.


Pentru blocare urmăm pașii:


1. Navigați la **Internet Status (Stare Internet)** > pictograma  Online: > tabul **Online Devices (Dispozitive online)** și localizați dispozitivul care urmează să fie adăugat.

Online Devices (2) Blacklist					
Device Name	Upload Speed	Download Speed	Access Type	Blacklist	
 DESKTOP-5LII2L5 192.168.0.136	0.0KB/s	0.0KB/s	Wired	Local Host	
 huazhondiyibiyi 192.168.0.174	0.0KB/s	0.0KB/s	5G	<input type="button" value="Add"/>	

2. Faceți clic pe **Add (Adăugați)**.

---Sfârșit


Pe pagina **Internet Status (Stare Internet)**, faceți clic pe  Online: , apoi pe **Blacklist (Lista neagră)**, puteți vizualiza informațiile despre dispozitivele care sunt adăugate pe această listă de dispozitive blocate pe baza adresei MAC a adaptorului de rețea.

Online Devices (1) Blacklist		
Device Name	MAC Address	Remove from Blacklist
Unknown		<input type="button" value="Remove"/>

3.4.2 Eliminați dispozitivele din lista neagră

Pentru a elimina dispozitivele din lista neagră după cum este necesar:

1. Navigați la **Blacklist (Lista neagră)** și localizați dispozitivul care urmează să fie eliminat din lista neagră.
2. Faceți clic pe **Remove (Eliminare)**.

Online Devices (1) Blacklist		
Device Name	MAC Address	Remove from Blacklist
Unknown		<input type="button" value="Remove"/>

---Sfârșit

4 Setări Internet

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

4.1 Conectare la internet prin rețele mobile

Pe această pagină, puteți modifica setările de internet atunci când accesați internetul folosind o cartelă SIM validă.


Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Internet Settings (Setări Internet)** dând clic pe meniul portocaliu din stânga. Arată astfel:


The screenshot displays the 'Internet Settings' web interface. At the top, there is a header with a home icon, the text 'Internet Settings', and a language dropdown set to 'English'. Below the header, the main content area is titled 'Internet Settings' and shows the following configuration options:

- Connection Status:** Connected
- Mobile Data:** Enable (dropdown menu)
- Data Roaming:** Disable (dropdown menu) with a note: 'Enable this function may incur roaming charges.'
- Mobile Data Options:** 4G Preferred (dropdown menu)
- Band:** Auto (dropdown menu) with a 'Search' button.
- Dial-up Settings:**
 - Profile Name:** CHN-CT (dropdown menu) with a 'Create a Profile' button.
 - PDP Type:** IPv4&IPv6 (dropdown menu)
 - APN:** ctite (text input field)
 - User Name:** (text input field)
 - Password:** (password input field with a visibility toggle)
 - Authentication Type:** NONE (dropdown menu)
 - MTU:** 1500 (text input field)
 - Compatibility Mode:** (toggle switch, currently off)
- Failover Settings:**
 - Failover:** Disable (dropdown menu)

At the bottom of the settings area, there is a green 'Disconnect' button.

Descrierea parametrilor

Parametru	Descriere
Connection Status (Starea conexiunii)	Specifică starea conexiunii la internet folosind o cartelă SIM.
Mobile Data (Date mobile)	Folosit pentru a activa sau dezactiva traficul de date mobile. Când este dezactivat, nu puteți accesa internetul prin date mobile.
Data Roaming (Roaming de date)	Folosit pentru a activa sau dezactiva roamingul de date. Data roaming (Roaming de date) reprezintă utilizarea serviciilor de date mobile atunci când se află în afara rețelei native a operatorului și se conectează la rețelele altor furnizori, de obicei într-o altă țară. Puteți dezactiva roamingul de date pentru a evita utilizarea datelor în roaming și implicit extra-taxarea.
Mobile Data Options (Opțiuni de date mobile)	Specifică tipul de rețea mobilă sau a generației de tehnologie de comunicație mobilă.
Band (Bandă)	Se referă la banda de comunicare dintre router și infrastructura ISP-ului. <ul style="list-style-type: none">- Auto: ruterul va scana automat benzile disponibile și va alege cea mai potrivită bandă de frecvență acceptată atât de router, cât și de furnizorul de servicii internet (ISP), în funcție de condițiile rețelei din zona respectivă.- Manual: puteți scana și potrivi manual banda acceptată.
Profile Name (Nume profil)	În general, toți acești parametri, cunoscuți sub denumirea generală de setări/profil APN , sunt predefiniți pentru cartela SIM, în funcție de furnizorul de servicii mobile, ISP. Ruterul va identifica acești parametri în mod automat.
PDP Type (Tip PDP)	
APN	Dacă ruterul nu reușește să identifice acești parametri aferenți cartelei SIM introduse, trebuie să îi introduceți manual făcând clic Create a Profile (Creați un profil) și introduceți manual setările pentru profilul APN aferent furnizorului de date mobile și a tipului de abonament, subscripție, cartelă preplătită etc.
User Name (Nume de utilizator)	
Password (Parolă)	 TIP Dacă ruterul nu poate identifica acești parametri, obțineți acești parametri de la
Authentication Type (Tip de autentificare)	ISP-ul dumneavoastră.
Create a Profile	Folosit pentru a crea un profil de acces APN atunci când ruterul nu reușește să identifice automat acești parametri.
MTU	Maximum Transmission Unit (MTU) este cel mai mare pachet de date transmis de un dispozitiv de rețea. Valoarea MTU implicită este 1500. Nu modificați valoarea decât dacă este necesar.

Parametru	Descriere
Compatibility Mode (Modul de compatibilitate)	<p>Puteți activa modul de compatibilitate din interfața web de gestionare pentru a modifica Time to Live (TTL) și Hop Limit (HL) valori pentru acces optim la internet. Time to Live (TTL) și Hop Limit (HL) sunt parametri utilizați în rețelele de date pentru a controla durata de viață a pachetelor de date transmise prin rețea și pentru a preveni buclele infinite în cazul rutării greșite. În rețelele mobile, TTL și Hop Limit sunt importante pentru a asigura o transmisie eficientă și controlată a pachetelor de date între dispozitivul mobil și servere sau alte destinații. Aceste setări sunt de obicei gestionate automat de operatorul de rețea mobilă, dar uneori utilizatorii pot ajusta manual valoarea TTL pentru a optimiza anumite tipuri de trafic, cum ar fi accesul la hotspot-uri mobile sau alte servicii.</p> <p> TIP</p> <p>Este aplicabil unor planuri limitate ale ISP-urilor. Valorile TTL și HL pot fi modificate și pentru analiza de captare a pachetelor în funcție de nevoile dumneavoastră.</p>

4.1.1 Schimbare tipul de rețea mobilă preferată

Când puteți accesa internetul prin date mobile, puteți modifica ordinea priorității sau selecta generația de comunicare mobilă la care să se conecteze echipamentul Tenda.

Să presupunem că utilizați ruterul în aria acoperirii ISP-ului și doriți să utilizați numai rețeaua 4G a acestuia.

Procedura de configurare:

1. [Conectați -vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Settings (Setări Internet)**.
3. Setați **Mobile Data (Date mobile)** la **Enable (Activare)**.
4. Setați **Data Roaming (Roaming de date)** la **Enable (Activare)**.
5. Setați **Mobile Data Option (Opțiunea de date mobile)** la **4G Only (Numai 4G)**.
6. Faceți clic pe **Connect (Conectare)**.

Internet Settings

English ▾

Internet Settings

Mobile Data:

Data Roaming:
Enable this function may incur roaming charges.

Mobile Data Options:

Band:

Dial-up Settings

Profile Name:

PDP Type:

APN:

User Name:

Password:

Authentication Type:

MTU:

Compatibility Mode:

Failover Settings

Failover:

---Sfârșit

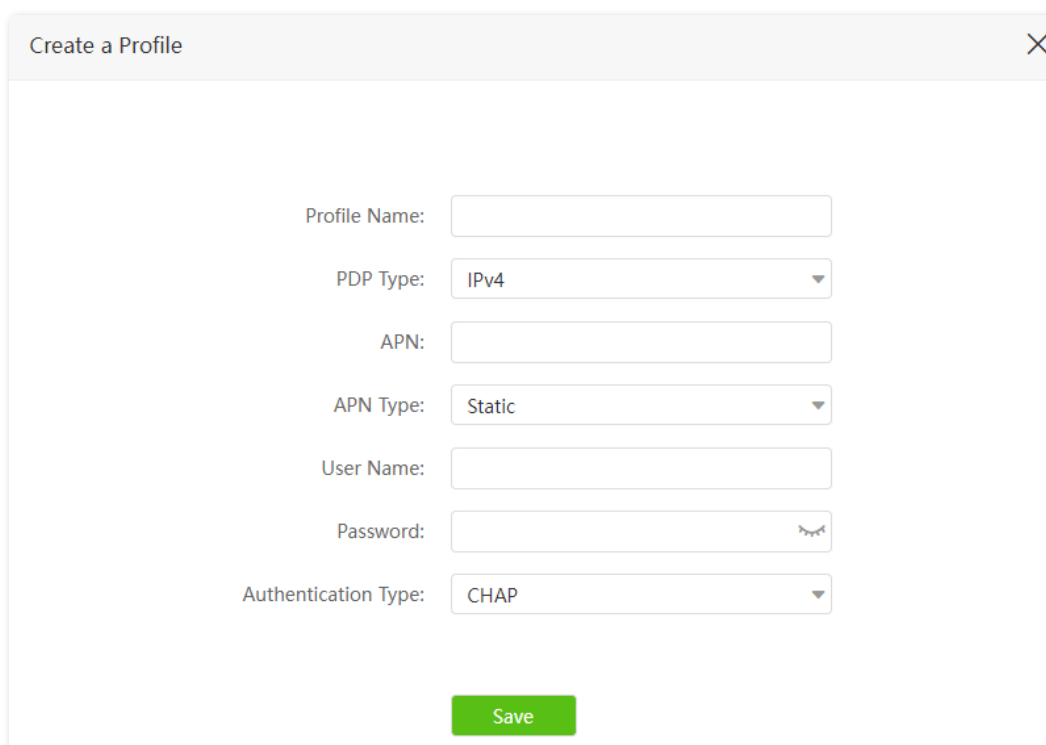
După finalizarea configurației, reîmprospătați pagina de configurare. Când se afișează **Connected (Conectat)** după **Connection Status (Starea Conexiunii)**, puteți utiliza doar rețeaua 4G pentru a accesa internetul în aria de acoperire. Așadar alte generații de comunicare, precum 3G, o să fie ignorate și nu o să se conecteze la acestea.

4.1.2 Creare manuală a unui profil APN

Dacă ruterul nu poate identifica automat parametrii APN și accesa internetul, puteți adăuga manual un nou profil APN. Obțineți acești parametri de la ISP-ul dvs. Un **profil APN** (Access Point Name) este un set de configurații de pe un dispozitiv care definește cum acesta se conectează la internet prin rețeaua operatorului mobil, permițând accesul la servicii de date mobile prin 4G, 3G etc.

Procedura de configurare:

1. [Conectati-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Settings (Setări Internet)**.
3. Faceți clic pe **Create a Profile (Creați un profil)**.
4. Introduceți parametrii necesari, aflați de la ISP.
5. Faceți clic pe **Save (Salvare)**.



The screenshot shows a 'Create a Profile' dialog box with the following fields:

- Profile Name:
- PDP Type:
- APN:
- APN Type:
- User Name:
- Password:
- Authentication Type:

A green 'Save' button is located at the bottom center of the dialog.

---Sfârșit

Așteptați un moment. Ruterul va folosi acești parametri pe care i-ați introdus pentru accesarea infrastructurii ISP-ului și în final pentru acces la internet. Când se afișează **Connected (Conectat)**, la **Connection Status (Starea conexiunii)**, puteți accesa internetul.

4.2 Conectare la internet prin cablu Ethernet

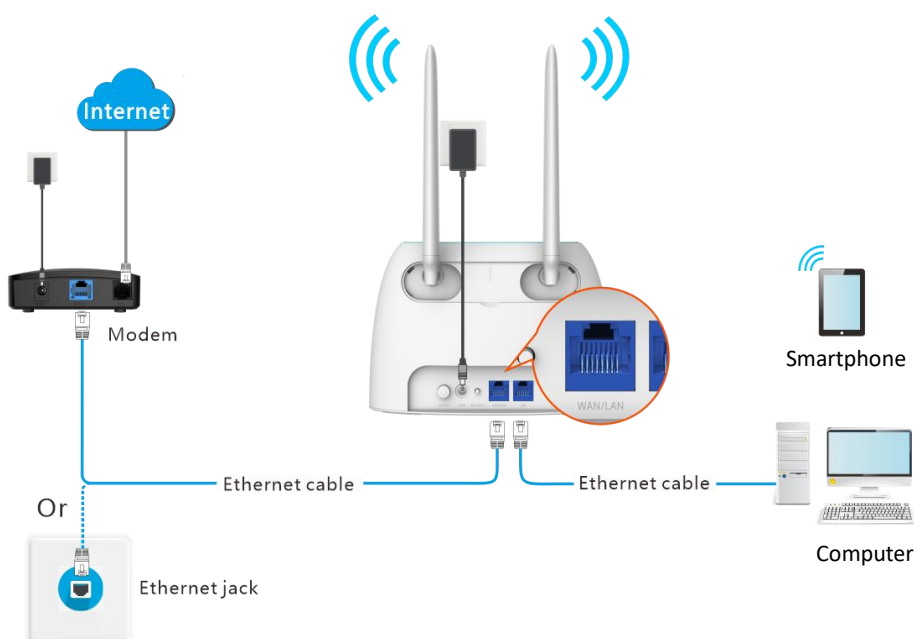
Dacă doriți să vă conectați la internet și prin servicii oferite prin cablu, atunci trebuie să activați funcția **Failover** apoi tipul de conexiune la internet. Cablul de internet ce vine de la ISP se va conecta la **portul Ethernet RJ-45**, marcat **WAN**, de pe spatele dispozitivului.



Parametrii pentru accesarea internetului sunt furnizați de ISP-ul dumneavoastră. Dacă aveți nedumeriri, contactați furnizorul de servicii de internet.

4.2.1 Accesare internet cu un cont PPPoE

Dacă ISP-ul vă oferă un nume de utilizator și o parolă PPPoE, puteți alege acest tip de conexiune pentru a accesa internetul. Credențialele PPPoE, în general, pot fi aflate direct din pagina dumneavoastră de client de pe site-ul furnizorului, fie din contractul de prestări servicii sau contactând serviciul clienți al ISP-ului, de obicei primind prin SMS aceste informații. Conectarea prin PPPoE e valabilă doar pentru conexiunea cablată, prin portul WAN.



Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare.](#)
2. Navigați la **Internet Settings (Setări Internet)**.
3. Activați funcția **Failover**. Funcția **Failover** este explicată în [subcapitolul 4.3](#).
4. Acum, setați **Connection Type (Tipul de conexiune)** la **PPPoE**.
5. Introduceți **PPPoE User Name (Nume utilizator PPPoE)** și **PPPoE Password (Parolă PPPoE)**.
6. Faceți clic pe **Connect (Conectare)**.

Failover Settings

Failover:

Connection Type:

PPPoE Username:

PPPoE Password:

DNS Settings:

---Sfârșit

După finalizarea configurației, puteți accesa internetul cu un cont PPPoE. Următoarea figură este doar pentru referință.

Internet Status

English

2.4 GHz/5 GHz: Tenda_F5...

Internet — 4G09 — Online: 1

↑ 0.0KB/s | ↓ 0.0KB/s
Current Speed

WAN IP Address

V16.03.07.08_multi **NEW**
Firmware Version

Descrierea parametrilor

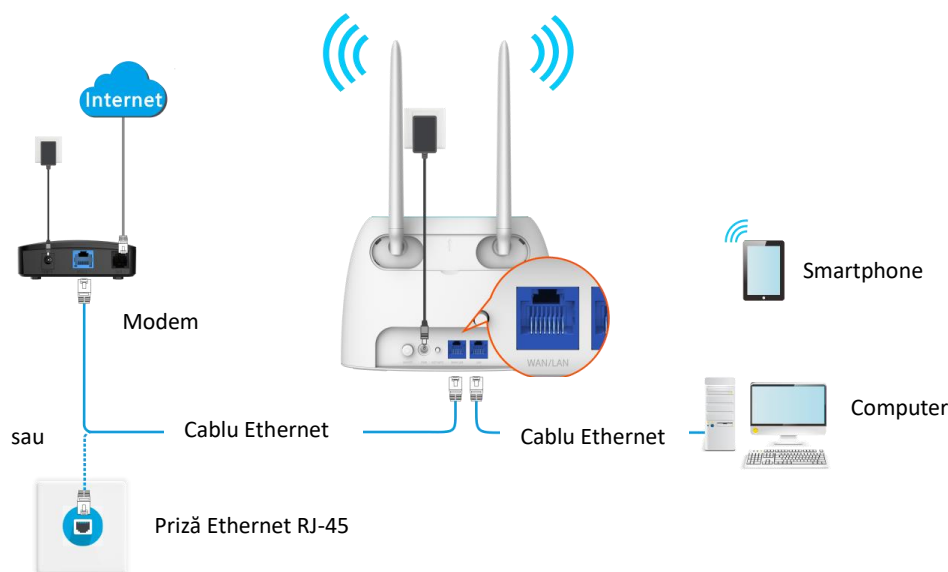
Parametru	Descriere
PPPoE Username (Nume de utilizator PPPoE)	Când PPPoE este ales ca tip de conexiune, trebuie să introduceți numele de utilizator și parola furnizate de ISP pentru a accesa internetul.
PPPoE Password (Parola PPPoE)	
DNS Settings (Setări DNS)	<p>Specifică metoda de obținere a adresei DNS pentru WAN, care este Automatic (Automată) în mod implicit. DNS (Domain Name System) este un sistem care traduce numele de domenii ușor de reținut (de exemplu, www.exemplu.com) în adrese IP numerice necesare pentru localizarea și accesarea serverelor pe internet care conțin aceste site-uri.</p> <ul style="list-style-type: none">- Automatic (Automată): Ruterul obține automat o adresă de server DNS de la serverul DHCP al ISP-ului sau de la rețeaua din amonte.- Manual: Adresa serverului DNS este configurată manual. Puteți seta DNS-uri publice oferite de Google (8.8.8.8) sau Cloudflare (1.1.1.1) sau altele.

4.2.2 Accesare internet prin adresă IP dinamică

În general, accesarea internetului prin adresa IP dinamică este aplicabilă în următoarele situații:

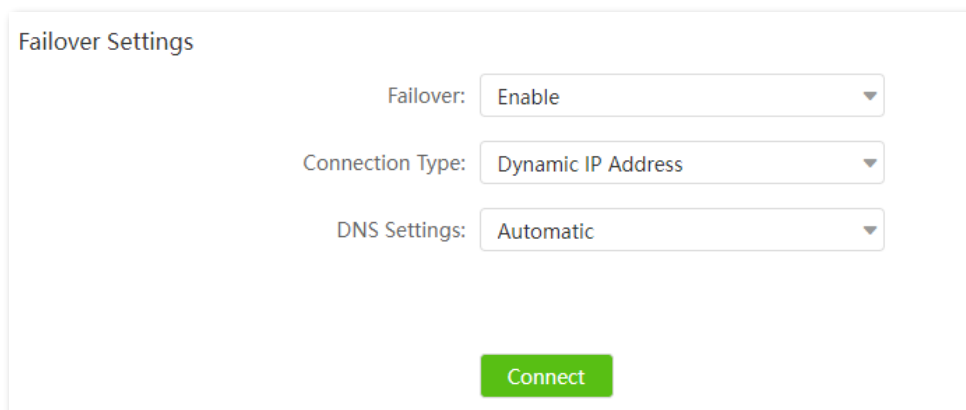
- ISP-ul dvs. nu furnizează numele de utilizator și parola PPPoE sau orice informații, inclusiv adresa IP, masca de subrețea, gateway-ul implicit și serverul DNS.
- ISP-ul oferă acces la internet prin cablu.
- Acest un ruter are acces la internet prin date mobile și doriți să conectați încă un dispozitiv de rutare, bineînțeles pe altă clasă de IP-uri.

Scenariul de aplicare este prezentat mai jos.



Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Internet Settings (Setări Internet)**.
3. Activați funcția **Failover**. Funcția **Failover** este explicată în [subcapitolul 4.3](#)
4. Setați **Connection Type (Tipul de conexiune)** pe **Dynamic IP Address (Adresă IP dinamică)**.
5. Faceți clic pe **Connect (Conectare)**.



Failover Settings

Failover: Enable

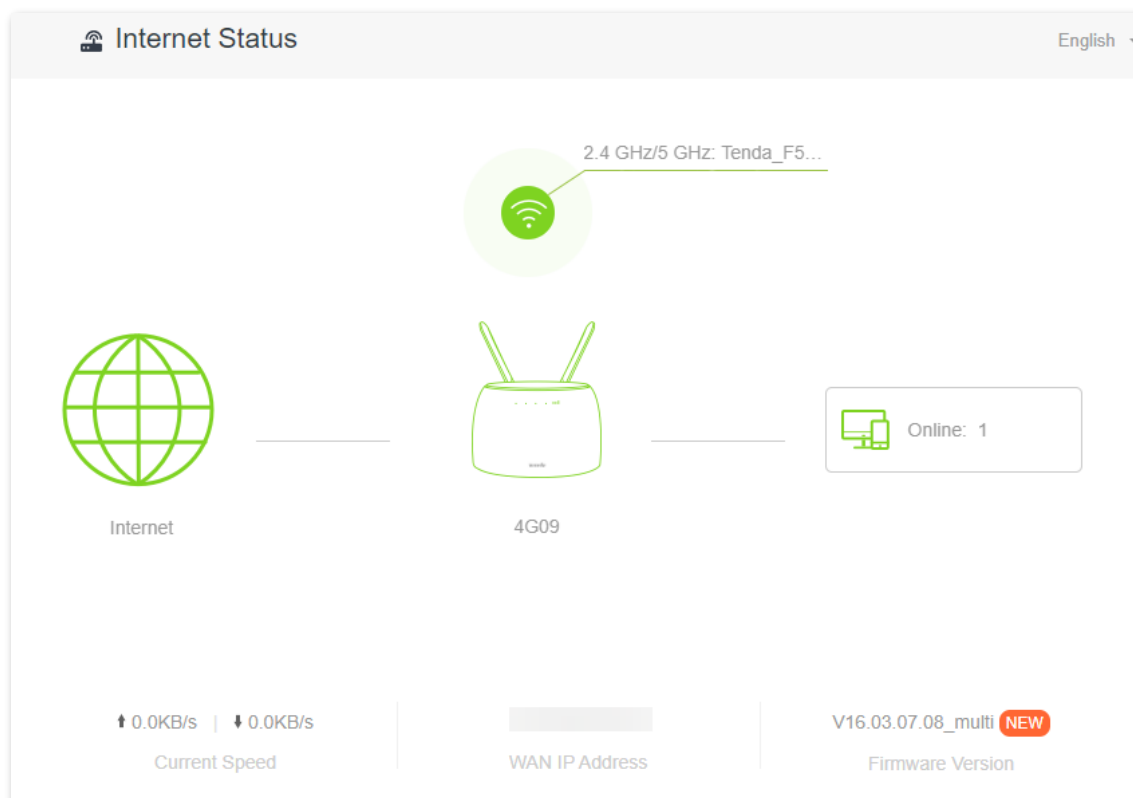
Connection Type: Dynamic IP Address

DNS Settings: Automatic

Connect

---Sfârșit

După finalizarea configurației, puteți accesa internetul prin adresă IP dinamică. Următoarea figură este doar pentru referință.



Descrierea parametrilor

Parametru	Descriere
DNS Settings (Setări DNS)	<p>Specifică metoda de obținere a adresei DNS pe WAN, care este implicit pe Automatic (Automată) în mod implicit. DNS (Domain Name System) este un sistem care traduce numele de domenii citibile (de exemplu, www.exemplu.com) în adrese IP numerice, permițând, de exemplu, browserelor să localizeze și să acceseze serverele pe internet.</p> <ul style="list-style-type: none">- Automatic (Automată): obțineți o adresă de server DNS de la serverul DHCP al ISP-ului sau al rețelei din amonte.- Manual: configurați manual adresa serverului DNS. Pentru acces la internet puteți seta o adresă DNS publică de la Google (8.8.8.8) sau Cloudflare (1.1.1.1)

4.2.3 Accesare internet prin IP static

Când ISP-ul dvs. vă oferă informații, inclusiv adresa IP, masca de subrețea, gateway-ul implicit și serverul DNS, puteți alege acest tip de conexiune pentru a accesa internetul. Iar conexiunea la internet oferită este prin cablu.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Accesați meniul **Internet Settings (Setări Internet)**.
3. Activați funcția **Failover**. Funcția **Failover** este explicată în [subcapitolul 4.3](#).
4. Setări **Connection Type (Tipul de conexiune)** pe **Static IP Address (Adresă IP statică)**.
5. Introduceți **IP Address (Adresa IP)**, **Subnet Mask (Mască de subrețea)**, **Default Gateway (Gateway implicit)** și **Primary/Secondary DNS server (Server DNS primar/secundar)**.
6. Faceți clic pe **Connect (Conectare)**.

Failover Settings

Failover:

Connection Type:

IP Address:

Subnet Mask:

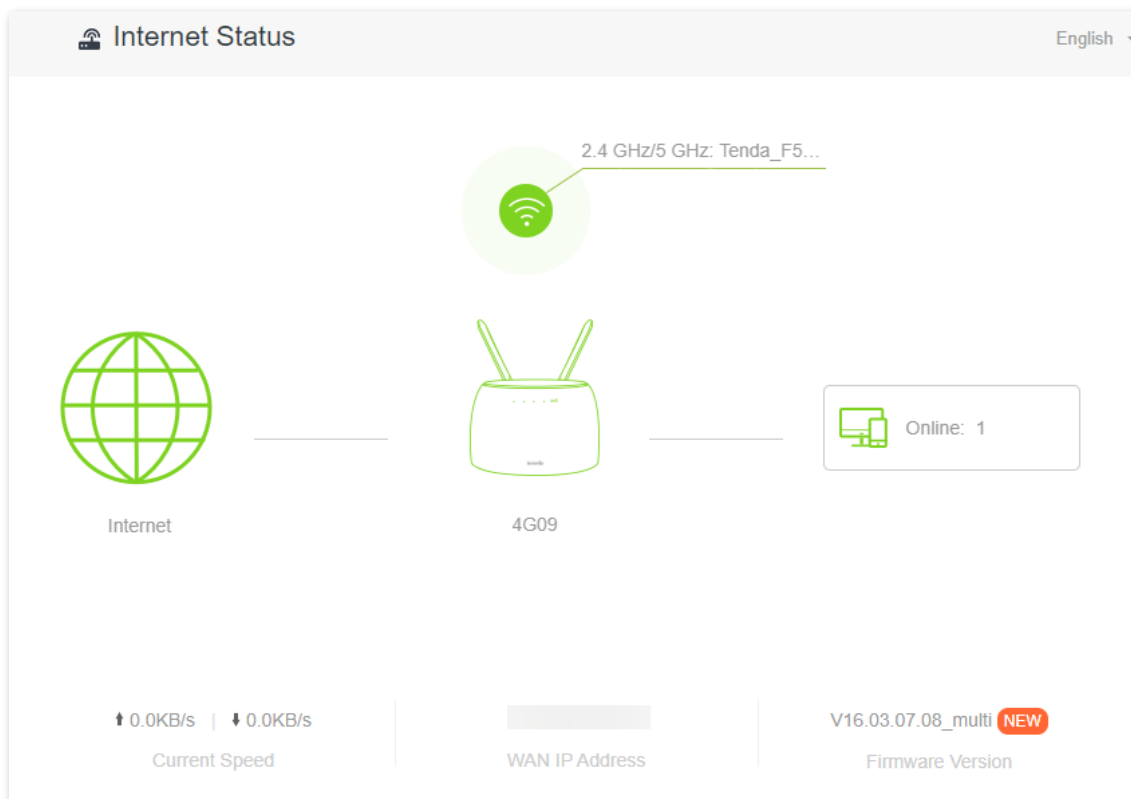
Default Gateway:

Primary DNS Server:


Secondary DNS Server:

---Sfârșit

După finalizarea configurației, puteți accesa internetul cu informații statice despre adresa IP. Următoarea figură este doar pentru referință.



Descrierea parametrilor

Parametru	Descriere
IP Address (Adresă IP)	
Subnet Mask (Mască de subrețea)	Când adresa IP statică este aleasă ca tip de conexiune, introduceți informațiile furnizate de ISP-ul dumneavoastră.
Default Gateway (Gateway implicit)	 TIP
Primary DNS Server (Server DNS primar)	Dacă ISP-ul dvs. oferă un singur server DNS, puteți lăsa necompletat serverul DNS secundar.
Secondary DNS Server (Server DNS secundar)	

4.3 Failover, redundanța conexiunii la internet

4.3.1 Prezentare generală

Failover la un router cu conexiune la internet prin date mobile și cablu asigură continuitatea conexiunii la internet prin comutarea automată de la rețeaua principală (date mobile) la rețeaua secundară (prin cablu Ethernet, prin portul WAN) în cazul în care conexiunea prin date mobile eșuează. Sau invers. Astfel, dispozitivele rămân conectate fără întreruperi semnificative. Pentru configurarea conexiunii la internet sau o rețea externă prin cablu Ethernet prin portul RJ-45 marcat WAN trebuie activată în prealabil funcția **Failover**.



Înainte de a activa funcția de failover, asigurați-vă că introduceți o cartelă SIM în router și conectați portul WAN al ruterului la internet.

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Internet Settings (Setări Internet)** și localizați secțiunea **Failover Settings (Setări Failover)**. Această funcție este dezactivată implicit.

Când funcția de failover este activată, pagina este afișată ca mai jos. Puteți configura conexiunea de failover, referindu-vă la [Acces la internet prin portul WAN](#).

Failover Settings

Failover: Enable

Connection Type: Dynamic IP Address

DNS Settings: Automatic

4.3.2 Configurarea funcției Failover

Scenariu: Aveți conexiune la internet oferită de ISP prin cablu Ethernet dar și o cartelă SIM, cu date mobile active și doriți să aveți continuitate pentru conexiunea la internet în cazul în care conexiunea prin cablu pică.



Cerințe: Setati ruterul să acceseze internetul prin cablu, prin portul WAN dar utilizați și cartela SIM oferită de un alt ISP, ca rezervă, în caz de defecțiune a conexiunii prin cablu.

Soluție: Configurați conexiunea la internet prin cablu și conexiunea la internet prin date mobile a fost deja setată.


Să presupunem că ISP-ul furnizează un nume de utilizator PPPoE și o parolă PPPoE pentru configurarea conexiunii la internet prin cablu.

Proceduri de configurare:

1. Conectați portul **WAN/LAN** al ruterului la portul LAN al gateway-ului sau media convertorului oferit de ISP, folosind un cablu Ethernet cu mufe RJ-45.
2. [Conectați-vă la interfața web de gestionare a ruterului](#) și navigați la pagina de meniu **Internet Settings (Setări Internet)**.
3. Activați funcția **Failover**, selectând **Enable (Activare)**.
4. Acum, setați **Connection Type (Tipul de conexiune)** pe **PPPoE** și apoi introduceți **PPPoE Username (Numele de utilizator PPPoE)** și **PPPoE Password (Parolă PPPoE)** furnizate de ISP-ul dumneavoastră.
5. Faceți clic pe **Connect (Conectare)**.
6. Așteptați câteva momente pentru realizarea conexiunii prin PPPoE. În funcție de ISP, conectarea poate dura și 3-4 minute.
7. Acum intrați în prima pagină de meniu **Internet Status (Stare Internet)** și o să observați o linie dublă între pictograma glob (Internet) și pictograma echipamentului Tenda. Deasupra este o linie continuă cu **4G/3G** (conexiunea primară la internet, prin date mobile) și jos o linie întreruptă notată **Eth** (conexiunea secundară la internet, prin cablu Ethernet).

Dacă dați clic pe **săgeata dublă sus-jos**  din dreapta o să comutați între cele două moduri de conectare la internet. Astfel, dând clic o dată pe  o să setați conexiunea prin cablu (Eth) ca și conexiune primară (principală) iar cea secundară o să fie pe date mobile (4G/3G). Așteptați câteva momente.

Mai jos în pagină, la câmpul **WAN IP Address (Adresă IP WAN)** o să observați schimbarea IP-ului extern.

Dacă dați clic încă o dată pe **săgeata dublă sus-jos**  din dreapta o să setați din nou conexiunea primară la internet pe date mobile (4G/3G) și cea secundară prin cablu Ethernet (Eth).

Failover Settings

Failover:

Connection Type:

PPPoE Username:

PPPoE Password:

DNS Settings:

Internet Status English ▾

2.4 GHz/5 GHz: Tenda_F5...

Internet

4G

Eth

4G09

Online: 1

↑ 0.0KB/s | ↓ 0.0KB/s
Current Speed

WAN IP Address

V16.03.07.08_multi **NEW**
Firmware Version

---Sfârșit

Când configurarea este finalizată, ruterul este conectat cu succes la internet și vă puteți bucura de acces neîntrerupt la internet garantat în bandă largă prin cablu, cât și prin date mobile.

5 Setări Wi-Fi

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

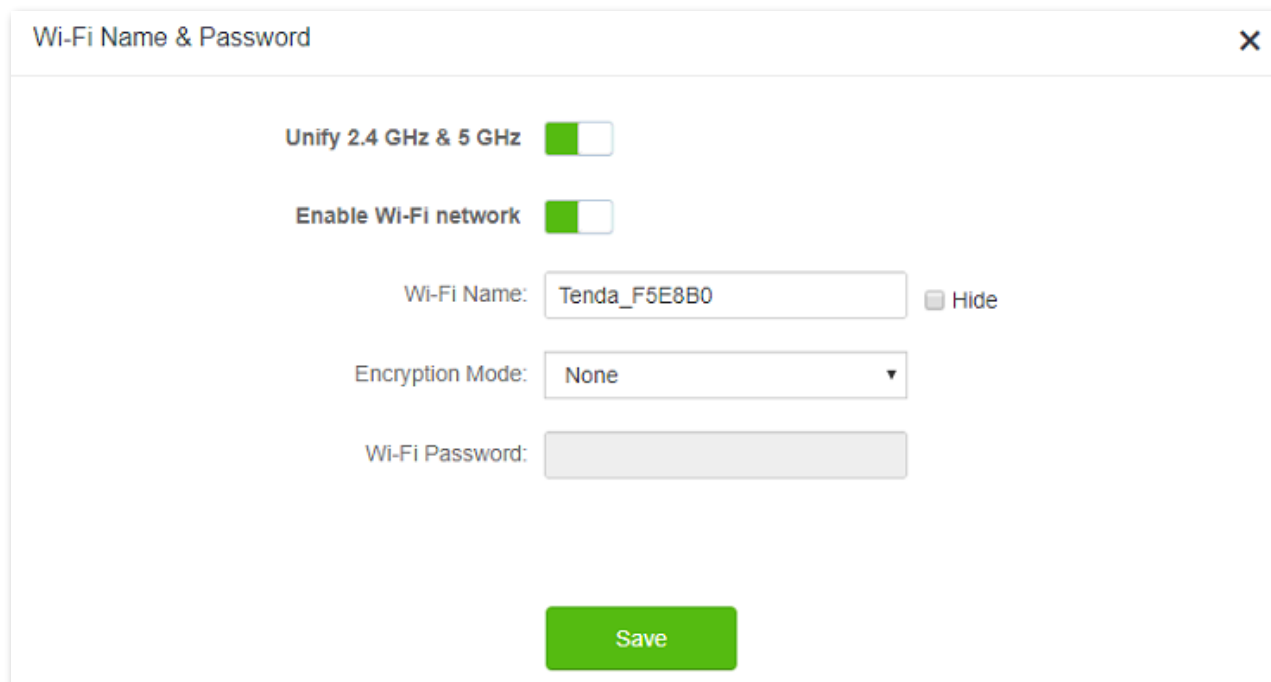
Modele **4G06**, **4G06c**, **4G03** emit doar în banda de 2,4 GHz, nu și pe 5 GHz. Așadar, anumite secțiuni din acest capitol nu se aplică. Modele care emit în ambele benzi sunt **4G07** și **4G09**.

5.1 Nume și parolă Wi-Fi

5.1.1 Prezentare generală

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Name & Password (Nume și parolă Wi-Fi)**.

Pe această pagină, puteți configura parametrii Wi-Fi de bază, cum ar fi denumirea și cheia de conectare Wi-Fi.



Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz

Enable Wi-Fi network

Wi-Fi Name: Hide


Encryption Mode:

Wi-Fi Password:

Save

Descrierea parametrilor

Parametru	Descriere
Unify 2.4 GHz & 5 GHz (Unificare 2,4 GHz și 5 GHz)	<p>Folosit pentru a activa sau dezactiva funcția de unificare a rețelelor pe 2,4 GHz și 5 GHz, care este activată implicit.</p> <p>Când această funcție este activată, rețelele Wi-Fi de 2,4 GHz și 5 GHz partajează același SSID și cheie de conectare (parolă). Dispozitivele conectate la rețeaua Wi-Fi vor folosi automat rețeaua cu o calitate mai bună a conexiunii.</p>
Enable Wi-Fi Network (Activare rețea Wi-Fi)	Folosit pentru a activa sau dezactiva rețelele Wi-Fi ale ruterului.
2.4 GHz Network (Rețea de 2,4 GHz)	<p>Puteți activa sau dezactiva separat rețeaua de 2,4 GHz și rețeaua de 5 GHz când funcția Unify 2.4 GHz & 5 GHz (Unificare 2,4 GHz și 5 GHz) este dezactivată, doar pentru modelele 4G07 și 4G09.</p> <ul style="list-style-type: none">- Dacă dispozitivele wireless, cum ar fi smartphone-urile, sunt departe de ruter, se recomandă conectarea la rețeaua care emite pe 2,4 GHz.
5 GHz Network (Rețea de 5 GHz)	<ul style="list-style-type: none">- Dacă dispozitivele wireless sunt aproape de router, se recomandă conectarea la rețeaua de 5 GHz, având o rată de comunicare mult mai mare.
Wi-Fi Name (Nume Wi-Fi)	Specifică numele rețelei Wi-Fi (SSID) pentru banda de frecvențe corespunzătoare.
Hide (Ascundere)	<p>Folosit pentru a ascunde numele Wi-Fi al rețelei Wi-Fi, pentru a îmbunătăți nivelul de securitate al rețelei Wi-Fi.</p> <p>Când această funcție este activată, rețeaua Wi-Fi este invizibilă pentru dispozitivele wireless. Trebuie să introduceți manual numele Wi-Fi al rețelei pe dispozitivele dvs. fără fir (cum ar fi un smartphone) dacă doriți să vă conectați la rețea.</p>
Encryption Mode (Mod de criptare)	<p>Specifică modurile de criptare, inclusiv:</p> <ul style="list-style-type: none">- None (Niciunul): indică faptul că rețeaua Wi-Fi nu este criptată și că orice client poate accesa rețeaua fără o parolă. Această opțiune nu este recomandată, deoarece duce la o securitate scăzută a rețelei.- WPA-PSK: rețeaua este criptată cu WPA-PSK/AES, care are o compatibilitate mai bună decât WPA2-PSK.- WPA2-PSK: rețeaua este criptată cu WPA2-PSK/AES, care are un nivel de securitate mai mare decât WPA-PSK.- WPA/WPA2-PSK (recomandat): indică faptul că WPA-PSK și WPA2-PSK sunt adoptate pentru a cripta rețeaua, oferind atât securitate, cât și compatibilitate.

Parametru	Descriere
Wi-Fi Password (Parolă Wi-Fi)	<p>Specifică parola pentru conectarea la rețeaua Wi-Fi. Vă recomandăm insistent să setați o parolă Wi-Fi pentru securitate. Puteți da clic pe câmpul de editare a parolei pentru a vedea parola în clar.</p> <p> TIP</p> <p>Este recomandat să utilizați o combinație de cifre, litere mari, litere mici și simboluri speciale în parolă pentru a spori securitatea rețelei Wi-Fi.</p>

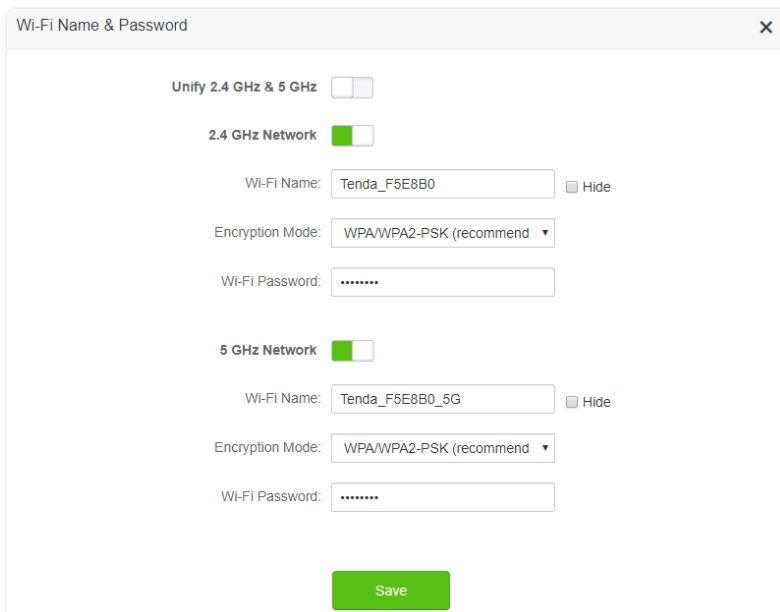
5.1.2 Unificarea și separarea rețelelor Wi-Fi

Această secțiune se aplică doar pentru modelele cu două benzi (2,4GHz și 5GHz), anume, Tenda 4G09 și Tenda 4G07.

Ambele rețele Wi-Fi de 2,4 GHz și 5 GHz sunt unificate în mod implicit și este afișată o singură denumire pentru Wi-Fi. Dacă doriți să separați rețelele utilizând două denumiri, diferite, atunci urmați procedurile de mai jos.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Name & Password (Nume și parolă Wi-Fi)**.
3. Dezactivați **Unify 2.4 GHz & 5 GHz (Unificare 2,4 GHz și 5 GHz)**.
4. Personalizați **Wi-Fi Name (Nume Wi-Fi)** și **Wi-Fi Password (Parolă Wi-Fi)** pentru fiecare bandă de frecvențe în parte.
5. Faceți clic pe **Save (Salvare)**.



---Sfârșit

Când configurarea este finalizată, vă puteți conecta la rețelele Wi-Fi ale routerului pentru a accesa internetul.

5.1.3 Schimbarea denumirii și parolei pentru Wi-Fi

Să presupunem că doriți să schimbați numele și parola Wi-Fi pentru 2,4 GHz în **John_Doe_2.4GHz** și **Tenda+Wireless24**, iar numele și parola Wi-Fi pentru 5 GHz în **John_Doe_5GHz** și **Tenda+Wireless5**. Ambele rețele adoptă **WPA/WPA2-PSK (recomandat)** ca tip de criptare.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Name & Password (Nume și parolă Wi-Fi)**.
3. Dezactivați **Unify 2.4 GHz & 5 GHz (Unificare 2,4 GHz și 5 GHz)**.
4. Modificați parametrii rețelei de 2,4 GHz.
 - 1) Schimbați **Wi-Fi Name (Numele Wi-Fi)** al rețelei de 2,4 GHz, care este **John_Doe_2,4 GHz** în acest exemplu.
 - 2) Alegeți un **Encryption Mode (Mod de criptare)**, care este **WPA/WPA2-PSK (recomandat)** în acest exemplu.
 - 3) Schimbați **Wi-Fi Password (Parola Wi-Fi)** a rețelei de 2,4 GHz, care este **Tenda +Wireless24** în acest exemplu.
5. Modificați parametrii rețelei de 5 GHz.
 - 1) Schimbați **Wi-Fi Name (Numele Wi-Fi)** al rețelei de 5 GHz, care este **John_Doe_5GHz** în acest exemplu.
 - 2) Alegeți un **Encryption Mode (Mod de criptare)**, care este **WPA/WPA2-PSK (recomandat)** în acest exemplu.
 - 3) Schimbați **Wi-Fi Password (Parola Wi-Fi)** a rețelei de 5 GHz, care este **Tenda +Wireless5** în acest exemplu.
6. Faceți clic pe **Save (Salvare)**.

Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz

2.4 GHz Network

Wi-Fi Name: John_Doe_2.4GHz Hide

Encryption Mode: WPA/WPA2-PSK (recommend ▼)

Wi-Fi Password:

5 GHz Network

Wi-Fi Name: John_Doe_5GHz Hide

Encryption Mode: WPA/WPA2-PSK (recommend ▼)

Wi-Fi Password:

Save

---Sfârșit

Când configurarea este finalizată, vă puteți conecta dispozitivele wireless la orice rețele Wi-Fi ale routerului pentru a accesa internetul.

5.1.4 Ascundere rețea Wi-Fi

Rețelele Wi-Fi **ascunse (Hide)** nu sunt vizibile în lista de rețele Wi-Fi detectate, în sistemul de operare de pe dispozitivele client. Această opțiune îmbunătățește securitatea, per ansamblu, reducând posibilitatea de accesare a rețelei prin Wi-Fi. Însă, pentru accesarea rețelei prin Wi-Fi vă puteți conecta manual, tastând denumirea rețelei Wi-Fi și apoi parola, orice sistem de operare de pe telefoane sau calculatoare permițând acest lucru.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Name & Password (Nume și parolă Wi-Fi).**
3. Bifați **Hide (Ascundeți)** pentru rețeaua în cauză.
4. Faceți clic pe **Save (Salvare).**

Wi-Fi Name & Password ✕

Unify 2.4 GHz & 5 GHz

2.4 GHz Network

Wi-Fi Name: Hide

Encryption Mode: ▾

Wi-Fi Password:

5 GHz Network

Wi-Fi Name: Hide

Encryption Mode: ▾

Wi-Fi Password:

---Sfârșit

Când configurarea este finalizată, numele rețelei Wi-Fi corespunzător este invizibil pentru dispozitivele wireless.

5.1.5 Conectarea la o rețea Wi-Fi ascunsă

Când o rețea Wi-Fi este ascunsă, trebuie să introduceți manual numele Wi-Fi și să vă conectați la ea.

Să presupunem că funcția **Unify 2,4 GHz & 5GHz (Unificare 2,4 GHz și 5 GHz)** este activată și că parametrii sunt:

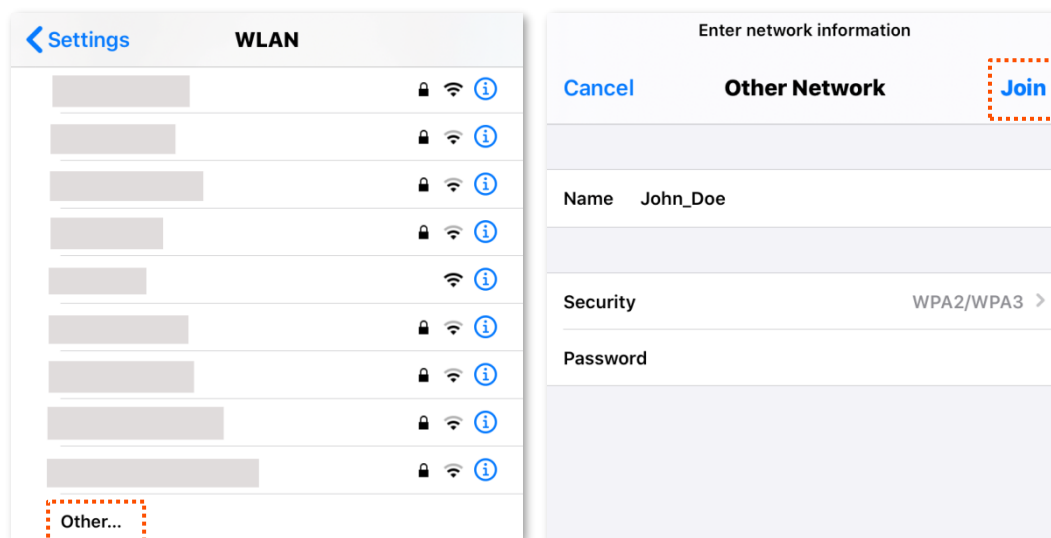
- Nume Wi-Fi: Jone_Doe
- Tip de criptare: WPA/WPA2-PSK (recomandat)
- Parola Wi-Fi: Tenda+Wireless245



Dacă nu vă amintiți parametrii wireless ai rețelei Wi-Fi, [conectați-vă la interfața web de gestionare a routerului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Name & Password (Nume și parolă Wi-Fi)** pentru a le găsi.

Proceduri pentru conectarea la rețeaua Wi-Fi ascunsă, de pe un telefon (Exemplu: iPhone):

1. Atingeți **Settings (Configurări)** pe telefon și alegeți **WLAN (Wi-Fi)**.
2. Activați **WLAN (Wi-Fi)**.
3. Derulați lista Wi-Fi până în jos și atingeți **Other...(Altele...)**.
4. Introduceți numele și parola Wi-Fi, care sunt **John_Doe** și **Tenda+Wireless245** în acest exemplu.
5. Setări securitatea la **WPA2/WPA3** (Dacă WPA2/WPA3 nu este disponibil, alegeți WPA2).
6. Atingeți **Join (Conectare)**.



--Sfârșit

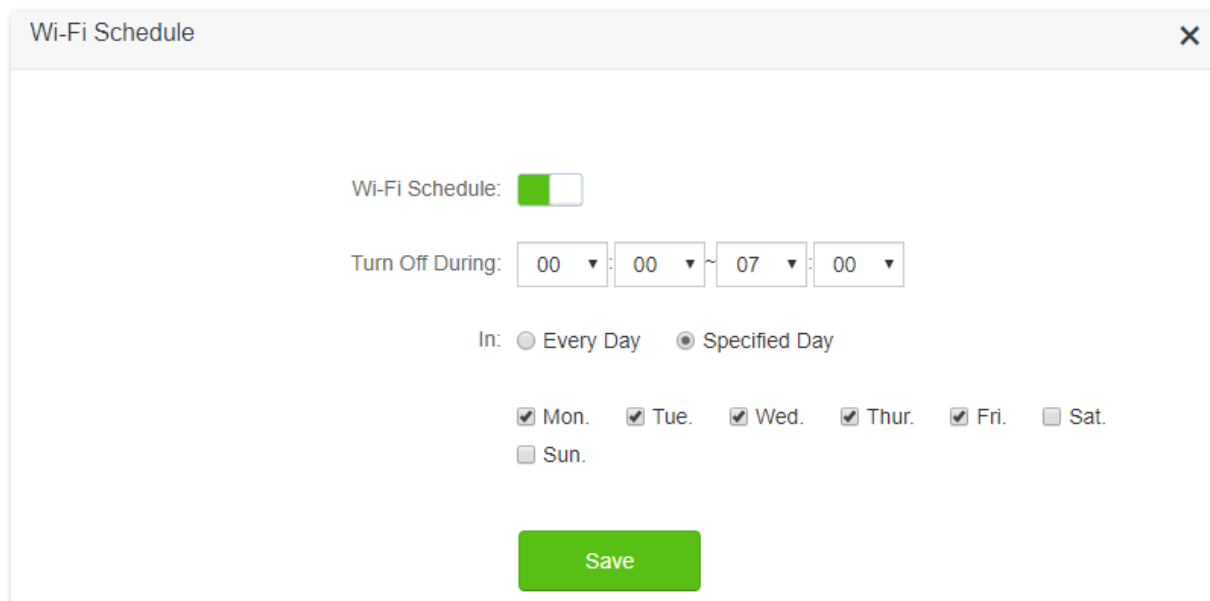
Când configurarea este finalizată, puteți accesa internetul.

5.2 Programare funcționare Wi-Fi

5.2.1 Prezentare generală

Funcția de funcționare a rețelelor Wi-Fi pe baza unui orar vă permite să dezactivați rețelele Wi-Fi a ruterului pentru o perioadă specificată. În mod implicit, funcția sa este dezactivată.

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Schedule (Programare Wi-Fi)**.



Pentru ca această opțiune să funcționeze corect, vă rugăm să vă asigurați că ora sistemului este sincronizată corect. Consultați secțiunea din manual [Sincronizarea orei sistemului cu cea a internetului](#) pentru configurare.

Descrierea parametrilor

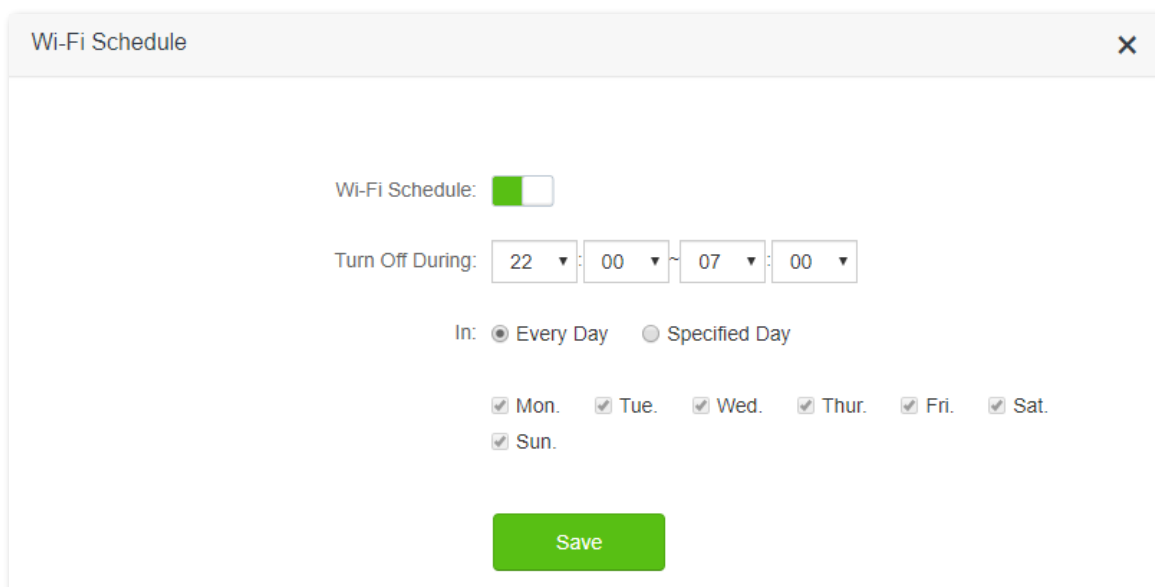
Parametru	Descriere
Wi-Fi Schedule (Programare Wi-Fi)	Folosit pentru a activa sau dezactiva rețeaua Wi-Fi pe baza unui orar.
Turn Off During (Opriiți în timpul)	Specifică ora și minutul de început și de sfârșit în care rețelele Wi-Fi sunt dezactivate.
In (în)	Se specifică dacă programul de oprire se aplică zilnic (Every Day) sau în zilele specificate din săptămână (Specified Day) .

5.2.2 Exemplu de configurare a programului Wi-Fi

Presupunem că doriți să dezactivați rețeaua Wi-Fi de la 22:00 la 07:00 în fiecare zi.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > Wi-Fi Schedule (Programare Wi-Fi)**.
3. Activați **Wi-Fi Schedule (Programare Wi-Fi)**.
4. Setați o perioadă pentru dezactivarea rețelelor Wi-Fi, care este **22:00-07:00**, în acest exemplu.
5. Setați zilele în care funcționează funcția, care este **Every Day (Zilnic)** în acest exemplu.
6. Faceți clic pe **Save (Salvare)**.



The screenshot shows a web interface titled "Wi-Fi Schedule" with a close button (X) in the top right corner. The interface contains the following elements:

- A toggle switch labeled "Wi-Fi Schedule:" which is currently turned on (green).
- A "Turn Off During:" section with four dropdown menus showing the time range "22 : 00 ~ 07 : 00".
- An "In:" section with two radio buttons: "Every Day" (selected) and "Specified Day".
- Below the radio buttons, there are seven checkboxes for the days of the week: Mon., Tue., Wed., Thur., Fri., Sat., and Sun., all of which are checked.
- A green "Save" button at the bottom center.

---Sfârșit

Când configurarea este finalizată, rețelele Wi-Fi vor fi dezactivate de la ora 22:00, seara, până la ora 7:00, dimineața, în fiecare zi. În afara perioadei rețelele o să fie funcționale.

5.3 Canalele și lățimea acestora

În această secțiune, puteți schimba standardul Wi-Fi (modul de rețea), canalul folosit din banda de frecvență și lățimea utilizată a unui canal, pentru fiecare bandă în parte.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Channel & Bandwidth (Canal și lățime canal)**.



Pentru a asigura performanța wireless, se recomandă menținerea setărilor implicite.

Channel & Bandwidth

2.4 GHz Network

Network Mode: 11b/g/n mixed ▼

Channel: Auto ▼

Bandwidth: 20/40 ▼

5 GHz Network

Network Mode: 11a/n/ac mixed ▼

Channel: Auto ▼

Bandwidth: 20/40/80 ▼

Save

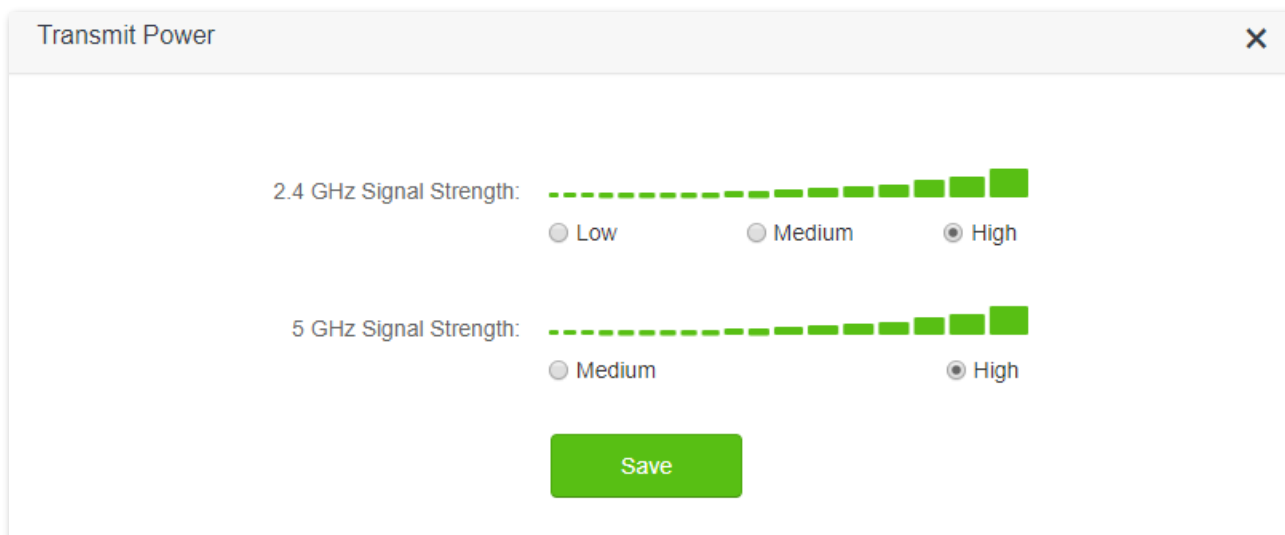
Descrierea parametrilor

Parametru	Descriere
Network Mode (Modul de rețea)	<p>Specifică diferite protocoale adoptate pentru comunicarea prin Wi-Fi.</p> <p>Rețeaua Wi-Fi de 2,4 GHz include moduri mixte 802.11n, 802.11b/g și 802.11b/g/n.</p> <ul style="list-style-type: none">- 11n: indică faptul că dispozitivele compatibile cu protocolul IEEE 802.11n se pot conecta la rețeaua Wi-Fi de 2,4 GHz a ruterului.- 11b/g mixed (11b/g mixt): indică faptul că dispozitivele compatibile cu protocolul IEEE 802.11b sau IEEE 802.11g se pot conecta la rețeaua Wi-Fi de 2,4 GHz a ruterului.- 11b/g/n mixed (11b/g/n mixt): indică faptul că toate dispozitivele se pot conecta la router dacă sunt conforme cu IEEE 802.11b sau Protocolul IEEE 802.11g sau lucrează la 2,4 GHz cu protocolul IEEE 802.11n. <p>Rețeaua Wi-Fi de 5 GHz include moduri mixte 802.11ac și 802.11a/n/ac.</p> <ul style="list-style-type: none">- 11ac: indică faptul că dispozitivele care fac reclamație cu protocolul IEEE 802.11ac se pot conecta la ruter.- 11a/n/ac mixed (11a/n/ac mixt): indică faptul că toate dispozitivele care sunt compatibile cu protocolul IEEE 802.11a sau IEEE 802.11ac sau care funcționează la 5 GHz cu protocolul IEEE 802.11n se pot conecta la ruter.
Channel (Canal)	<p>Specifică canalul utilizat din banda de frecvențe.</p> <p>În mod implicit, canalul este setat pe Auto, ceea ce înseamnă că ruterul selectează automat un canal pentru transmisie. Vi se recomandă să alegeți un canal cu mai puține interferențe pentru a îmbunătăți eficiența transmisiei wireless. Puteți utiliza un instrument terț pentru a analiza mediul înconjurător și pentru a identifica semnalele Wi-Fi existente, ceea ce vă va ajuta să înțelegeți utilizarea canalelor adiacente.</p>
Bandwidth (Lățime canal)	<p>Specifică lățimea canalului dintr-o bandă de frecvențe. Vă rugăm să modificați setările implicite numai atunci când este necesar.</p> <ul style="list-style-type: none">- 20: Indică faptul că lățimea canalului utilizat de router din banda selectată este lat de 20 MHz.- 40: Indică faptul că lățimea canalului utilizat de router din banda selectată este lat de 40 MHz.- 20/40: Acesta specifică faptul că un router își poate comuta lățimea canalului între 20 MHz și 40 MHz, în funcție de mediul ambiant. Această opțiune este disponibilă numai pentru banda de 2,4 GHz.- 80: Indică faptul că lățimea canalului utilizat de router din banda selectată este lat de 80 MHz. Această opțiune este disponibilă numai pentru banda de 5 GHz.- 20/40/80: Specifică faptul că un router poate schimba lățimea canalului între 20 MHz, 40 MHz sau 80 MHz, în funcție de mediul ambiant. Această opțiune este disponibilă numai pentru banda de 5 GHz.

5.4 Reglare putere de transmisie Wi-Fi

În această secțiune de meniu, puteți regla capacitatea de penetrare și acoperirea wireless a ruterului prin setarea puterii de transmisie Wi-Fi.

Pentru a accesa pagina, [conectați-vă la interfața de utilizare web a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Transmit Power (Putere transmisie)**.




Transmit Power

2.4 GHz Signal Strength: Low Medium High

5 GHz Signal Strength: Medium High

Save

Parametru	Descriere
Signal Strength (Puterea semnalului)	<p>Specifică modul de putere a semnalului. Modul implicit este High (Ridicat).</p> <ul style="list-style-type: none">- High (Ridicat): este utilizat de obicei pentru a îndeplini cerințele de acoperire wireless în spații mari sau cu obstacole multiple.- Medium (Medie): este de obicei utilizat pentru a îndeplini cerințele de acoperire wireless în medii cu suprafețe medii sau cu mai puține obstacole.- Low (Scăzut): este de obicei folosit pentru a îndeplini cerințele de acoperire wireless în zone mici sau medii fără obstacole.
	<p> TIP</p> <p>Recomandat să alegeți modul Low (Scăzut) dacă experiența de rețea este suficient de satisfăcătoare în acest mod.</p>

5.5 WPS

5.5.1 Prezentare generală

Funcția WPS permite dispozitivelor fără fir, cum ar fi smartphone-urile, să se conecteze rapid și ușor la rețelele Wi-Fi ale ruterului.

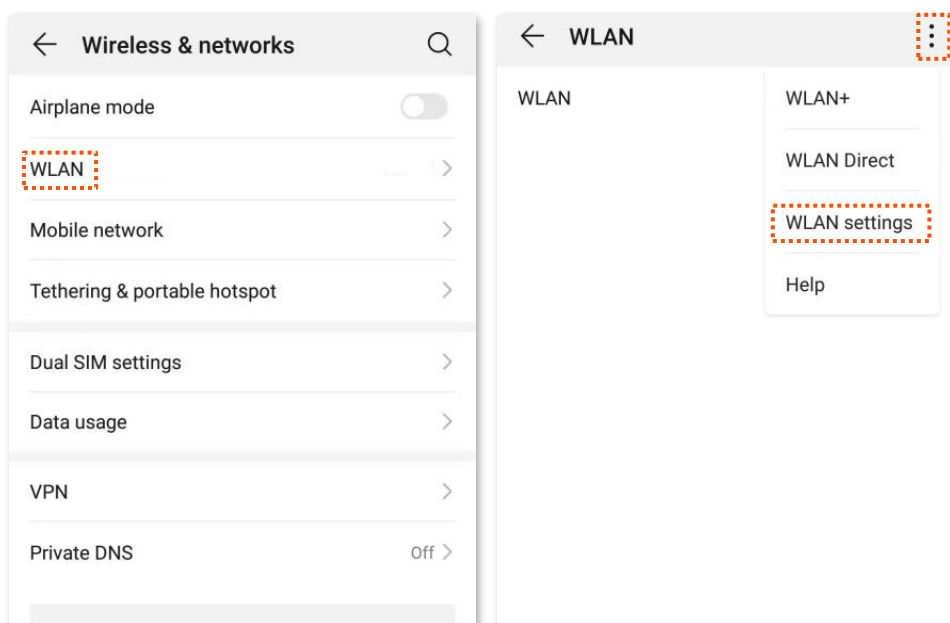
Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > WPS**.



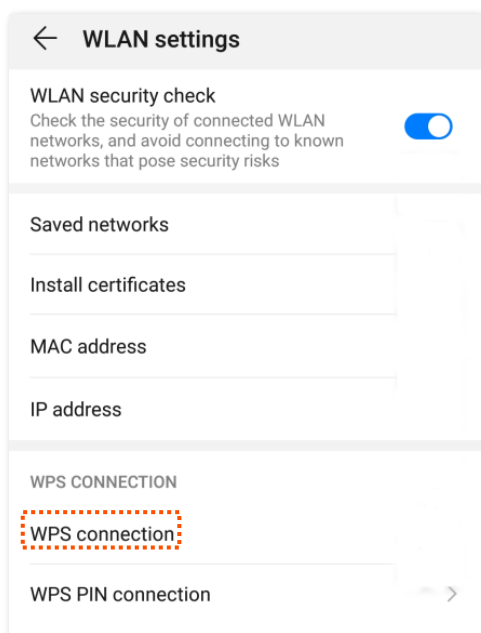
Această funcție este aplicabilă numai dispozitivelor wireless compatibile cu WPS.

5.5.2 Conectați dispozitivele la rețeaua Wi-Fi folosind butonul WPS

1. Găsiți butonul **RST/WPS** de pe spatele ruterului și țineți-l apăsat timp de 1 până la 3 secunde. Indicatorul LED Wi-Fi clipește încet.
2. Configurați funcția WPS pe dispozitivele dvs. fără fir **în decurs de maxim 2 minute**. Configurațiile pe diferite dispozitive pot diferi. Exemplificarea de mai jos este pentru un smartphone HUAWEI P10.
 - 1) Găsiți **Settings (Setări)** pe telefon.
 - 2) Alegeți **WLAN**.
 - 3) Atingeți **⋮** și alegeți **WLAN settings (Setări WLAN)**.

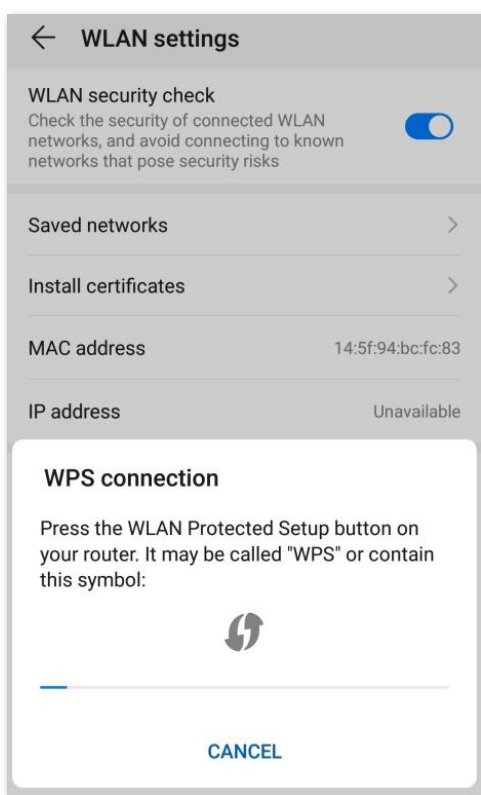


4) Alegeți WPS connection (Conexiune WPS).



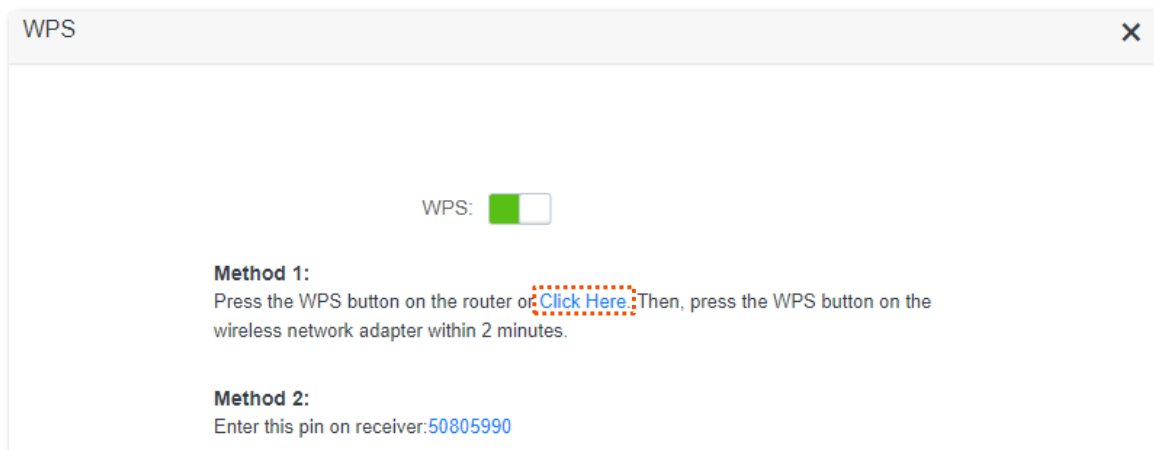
---Sfârșit


Așteptați un moment până când negocierea WPS este finalizată și telefonul inteligent este conectat la rețeaua Wi-Fi.

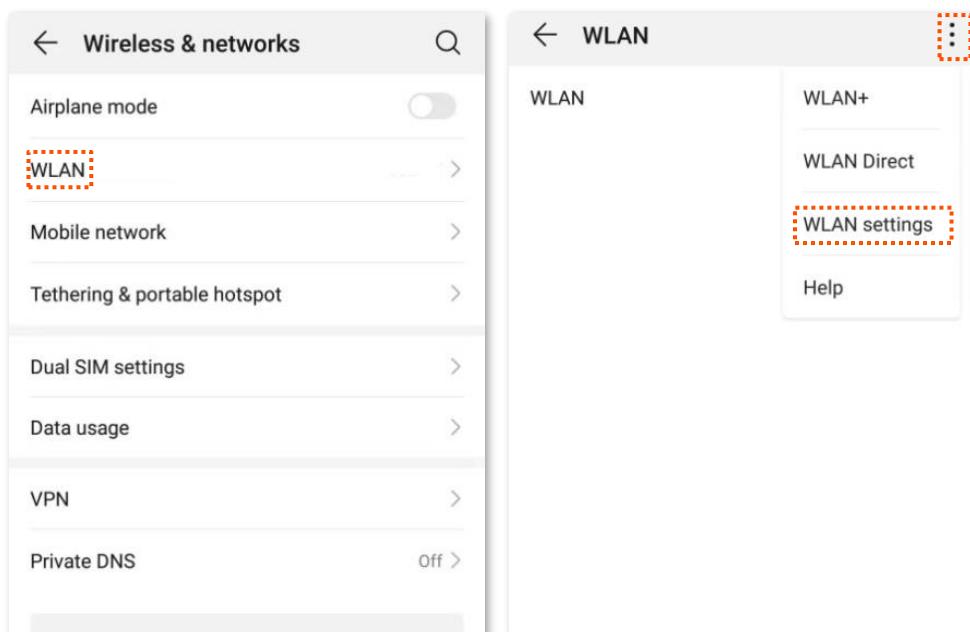


5.5.3 Conectați dispozitivele la rețeaua Wi-Fi prin interfața web de gestionare a routerului

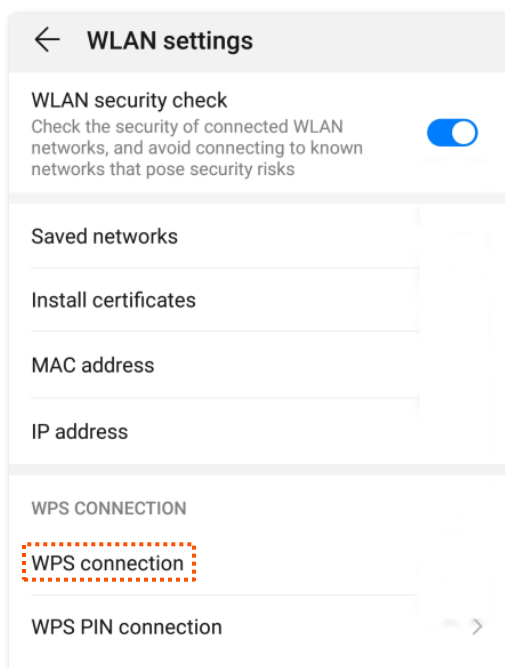
1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > WPS.**
3. Faceți clic pe textul albastru [Click Here \(Faceți clic aici\)](#) de sub **Method 1 (Metoda 1).**



4. Configurați funcția WPS pe dispozitivele dvs. fără fir **în decurs de maxim 2 minute.** Configurațiile pe diferite dispozitive pot diferi. Exemplificarea de mai jos este pentru un smartphone HUAWEI P10.
 - 1) Găsiți meniul **WLAN** din setările de sistem ale telefonului.
 - 2) Atingeți  și alegeți **WLAN settings (Setări WLAN).**

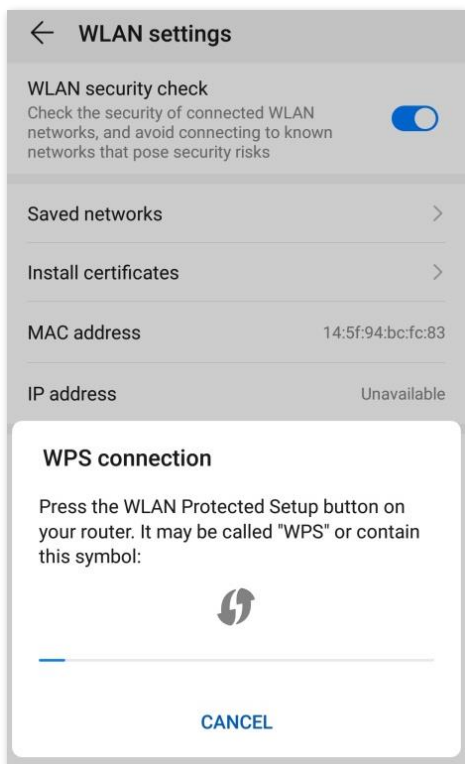


3) Alegeți WPS connection (Conexiune WPS).



---Sfârșit

Așteptați un moment până când negocierea WPS este finalizată și telefonul inteligent este conectat la rețeaua Wi-Fi.



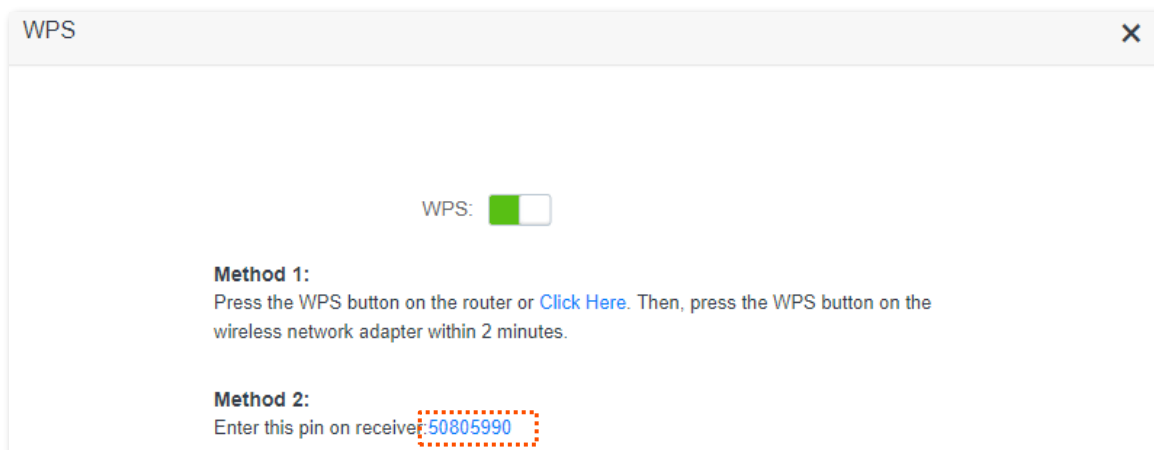
5.5.4 Conectați dispozitivele la rețeaua Wi-Fi folosind codul PIN afișat în interfața web de gestionare a ruterului



Este disponibil numai atunci când dispozitivele wireless, cum ar fi adaptoarele de rețea Wi-Fi, pot efectua negocieri WPS prin introducerea unui cod PIN. Vă rugăm să consultați ghidul de utilizare al adaptorului de rețea Wi-Fi pentru detalii de configurare.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **Wi-Fi Settings (Setări Wi-Fi) > WPS.**
3. Găsiți codul PIN afișat cu text albastru. Codul PIN este afișat sub **Method 2 (Metoda 2).**



4. Introduceți codul PIN pe dispozitivul client care poate efectua negocierea WPS utilizând codul PIN.

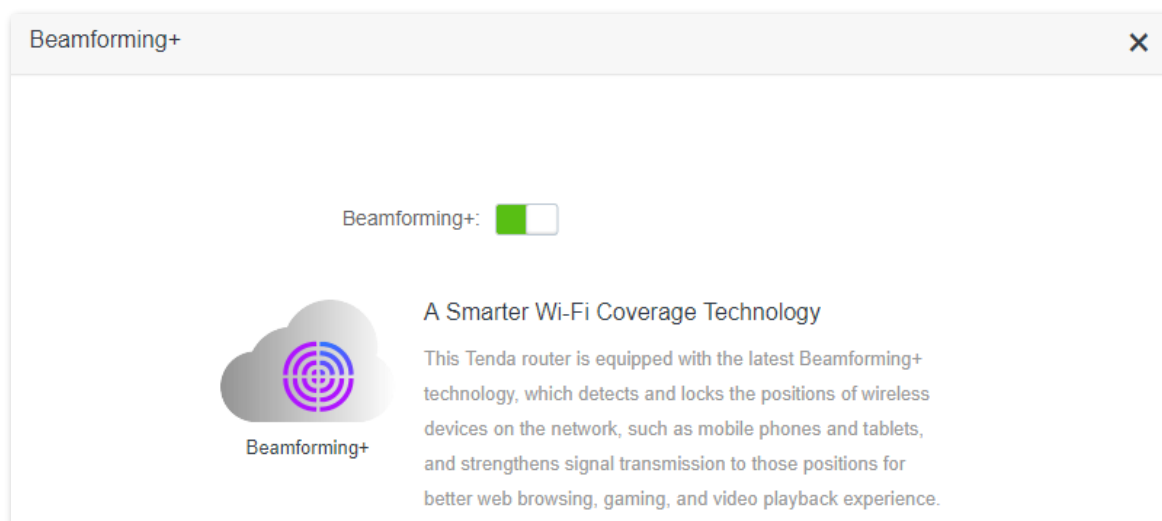
---Sfârșit

Așteptați un moment până când negocierea WPS este finalizată și dispozitivul client este conectat la rețeaua Wi-Fi.

5.6 Beamforming+

Beamforming+ este o tehnologie înscrisă în standardul IEEE 802.11ac. În mod tradițional, ruterul emite unde Wi-Fi (parte a spectrului radio) în toate direcțiile atunci când comunică date. Cu **Beamforming+**, ruterul transmite semnal radio în direcția clientului, creând astfel o comunicare wireless direcțională, mai puternică, mai rapidă și mai fiabilă. Această funcție este activată în mod implicit. Aceasta se realizează prin utilizarea mai multor antene pentru a crea un fascicul radio care se concentrează pe un dispozitiv specific, reducând interferențele și sporind eficiența transmisiei. **Beamforming+** este o îmbunătățire față de tehnologia tradițională Beamforming (fără +), având capacitatea de a ajusta în mod dinamic direcția semnalului în funcție de poziția și mișcarea dispozitivelor, ceea ce duce la o experiență de utilizare mai bună, rate de comunicare mai mari și o acoperire mai consistentă.

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Beamforming+**.



Următoarea figură arată transmisia prin Wi-Fi atunci când **Beamforming+** este activat.



Următoarea figură arată transmisia prin Wi-Fi atunci când **Beamforming +** este dezactivat.

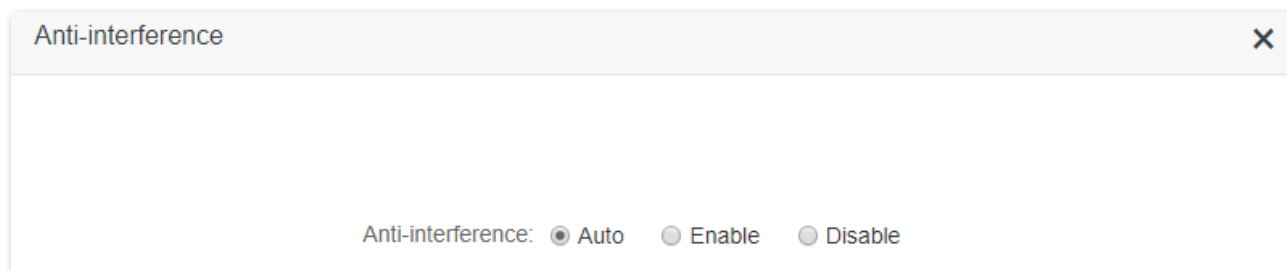


5.7 Anti-interferență

Când întâmpinați acces nesatisfăcător la rețeaua Wi-Fi și implicit la internet, puteți încerca să modificați setările de anti-interferență pentru îmbunătățirea comunicării radio.

Pentru a accesa pagina, [conectați-vă la interfața de utilizare web a ruterului](#) și navigați la **Wi-Fi Settings (Setări Wi-Fi) > Anti-interference (Anti-interferență)**.

Setarea implicită este **Auto**.



- **Auto:** Indică faptul că ruterul va regla automat sensibilitatea de recepție în funcție de interferența mediului actual. Este recomandat să păstrați **Auto**.
- **Enable (Activare):** Indică faptul că capacitatea de anti-interferență a ruterului se îmbunătățește, dar acoperirea rețelei Wi-Fi este redusă.
- **Disable (Dezactivare):** Indică faptul că acoperirea wireless a ruterului este îmbunătățită. Dacă interferențele din mediul de utilizare sunt puternice, se recomandă să selectați **Auto** sau **Enable (Activare)**.

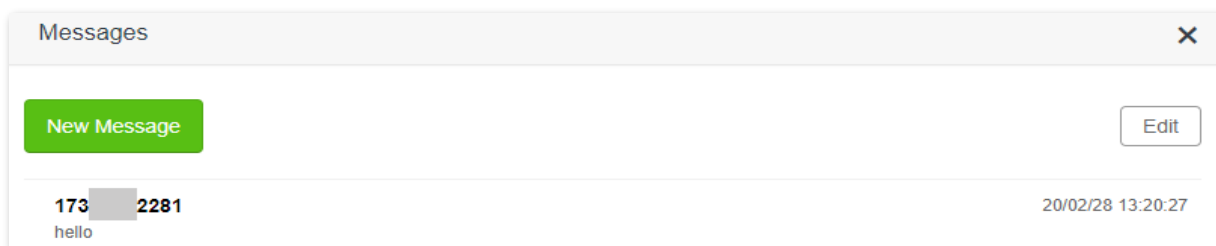
6 SMS

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

6.1 Gestionare mesaje SMS

Pe această pagină, puteți trimite, primi și șterge mesaje SMS direct din pagina web de gestionare a echipamentului Tenda.

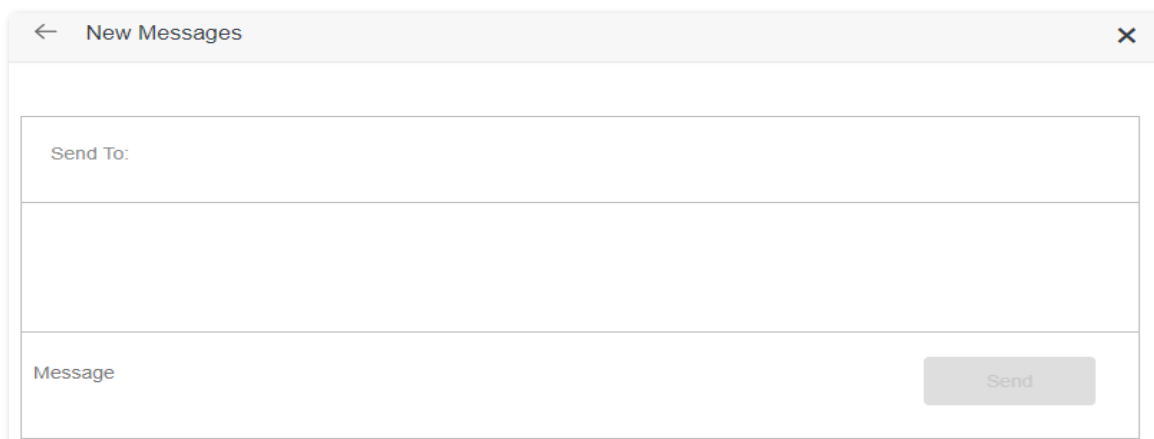
Pentru a accesa pagina, [conectați-vă la interfața web de gestionare](#) și navigați la **SMS > Messages (Mesaje)**.



6.1.1 Trimitere mesaje SMS

Trimitere un mesaj SMS către un număr de mobil

1. [Conectați-vă la interfața web de gestionare a routerului](#).
2. Navigați la **SMS > Messages (Mesaje)**.
3. Faceți clic pe **New Message (Mesaj nou)**.
4. Introduceți numărul telefonului mobil în câmpul **Send To (Trimitere către)**.
5. Introduceți conținutul mesajului în câmpul **Message (Mesaj)**, din partea de jos.

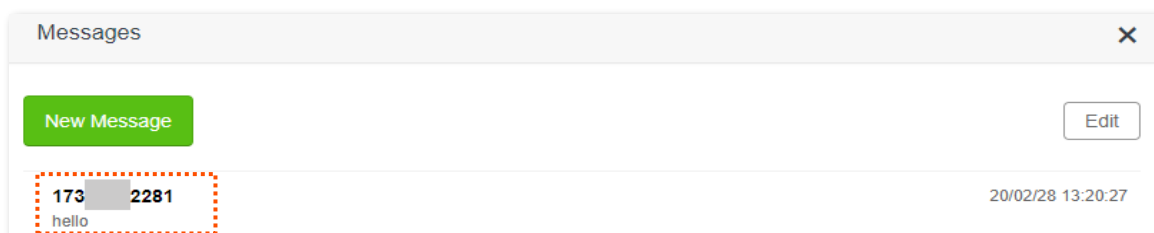


6. Faceți clic pe **Send (Trimiteți)** din colțul din dreapta jos.

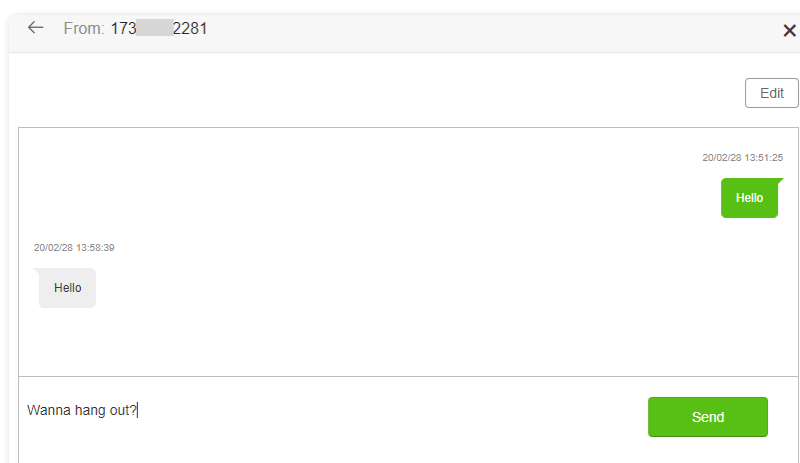
---Sfârșit

Trimitere mesaj SMS către un număr de mobil din istoricul conversațiilor

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **SMS > Messages (Mesaje)**.
3. Faceți clic pe numărul de mobil din istoricul mesajelor trimise anterior.



4. Apoi, în noua fereastră, introduceți conținutul mesajului în câmpul **Message (Mesaj)** din partea de jos.
5. Faceți clic pe **Send (Trimitere)**.

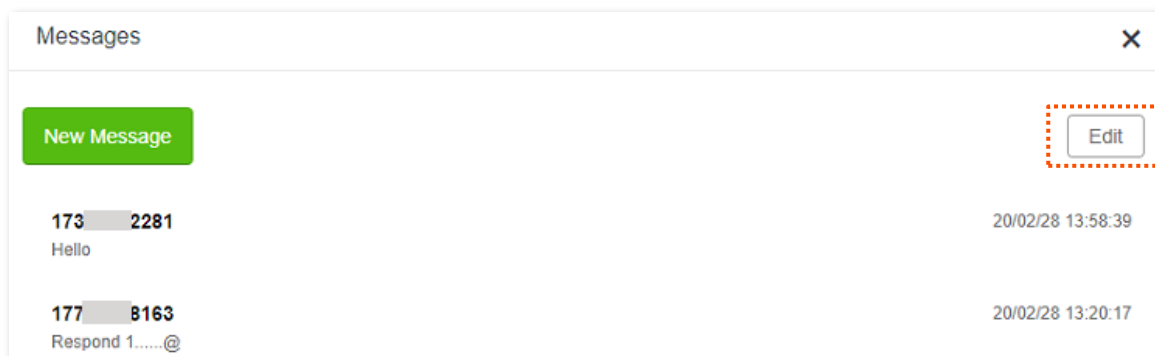



---Sfârșit

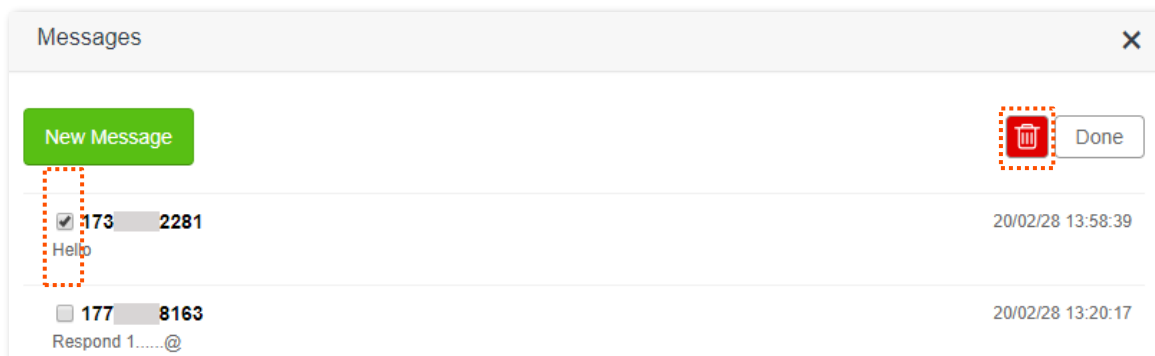
6.1.2 Ștergere mesaje SMS

Ștergerea tuturor mesajelor SMS selectate, după numărul de mobil

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **SMS > Messages (Mesaje)**.
3. Faceți clic pe butonul **Edit (Editați)** din colțul din dreapta sus.



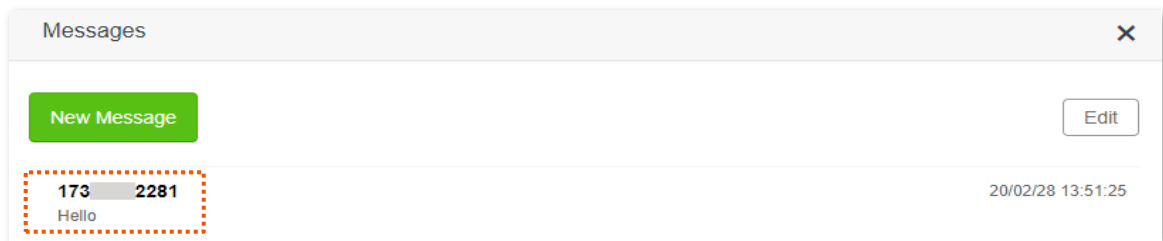
4. **Selectați** unul sau mai multe conversații din istoric, grupate după numărul de mobil.
5. Faceți clic pe butonul .



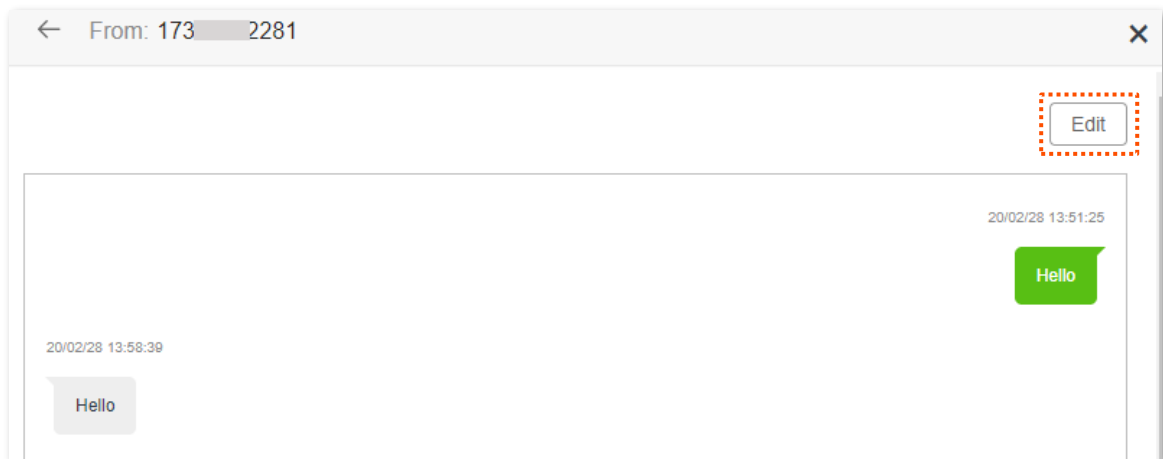
---Sfârșit

Ștergere anumite mesaje dintr-o conversație din istoric


1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **SMS > Messages (Mesaje)**.
3. Faceți clic pe numărul de mobil vizat din istoricul tuturor conversațiilor.

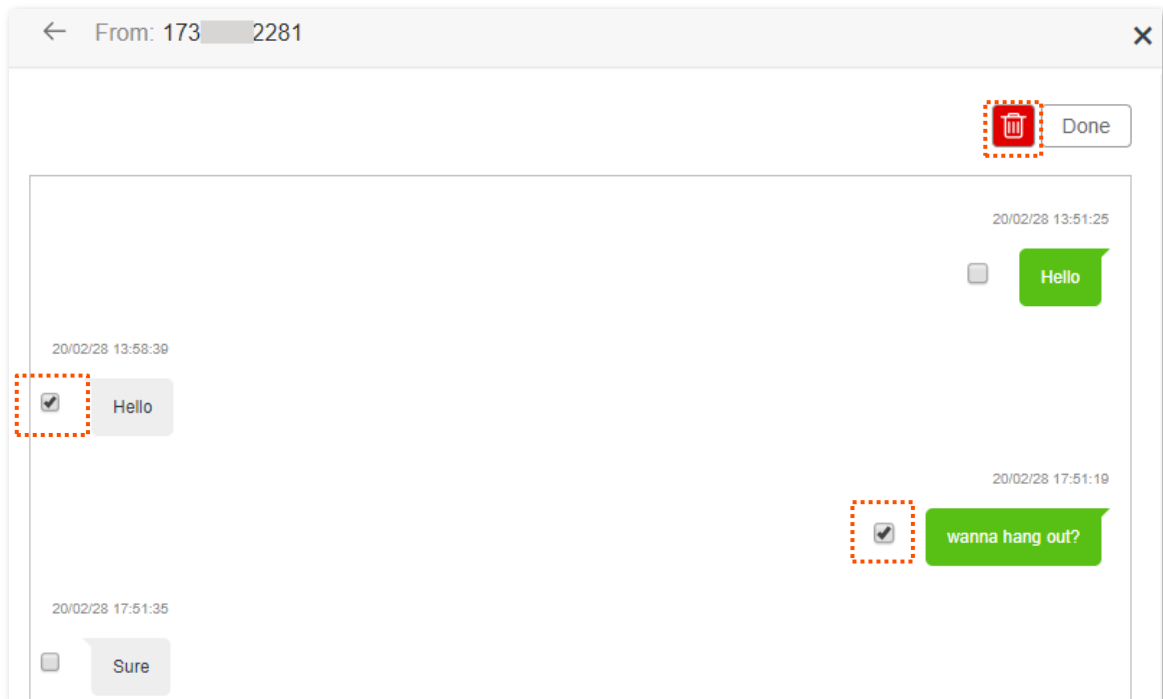


4. Faceți clic pe **Edit (Editare)**.



5. Selectați mesaje de șters.

6. Faceți clic pe butonul .



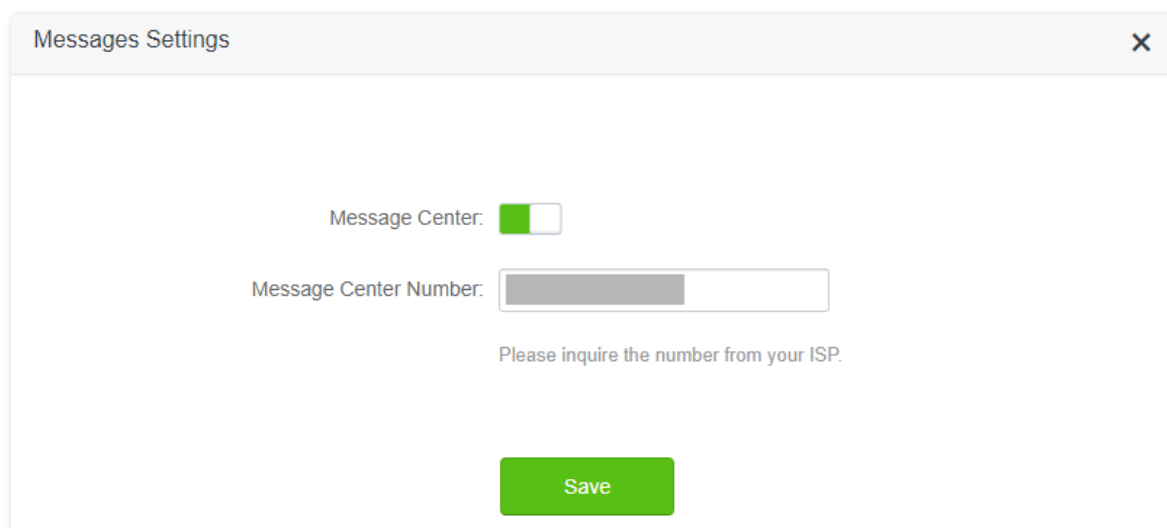
---Sfârșit

6.2 Setarea numărului centrului de mesagerie SMS

Numărul centrului de mesagerie SMS (SMS Center Number) este un număr de telefon asociat cu un serviciu de mesagerie text care este utilizat pentru a trimite și primi mesaje SMS. Acest număr este parte esențială a infrastructurii rețelei mobile, permițând mesajelor să fie ruteze între utilizatori prin intermediul operatorului de telecomunicații. Centrul de mesagerie SMS gestionează livrarea mesajelor, asigurându-se că acestea sunt transmise corect, chiar și în cazul în care destinatarul nu este disponibil la momentul trimiterii. Dacă un mesaj nu poate fi livrat imediat, centrul de mesagerie SMS îl va stoca temporar și va încerca să-l livreze mai târziu. Numărul centrului de mesagerie este adesea configurat automat pe telefoanele mobile, dar poate fi setat manual de utilizatori, în funcție de rețeaua mobilă folosită. Ruterul poate detecta automat numărul centrului de mesagerie după ce introduceți o cartelă SIM. Dacă întâmpinați probleme la trimiterea mesajelor SMS, vă recomandăm să întrebați ISP-ul dumneavoastră pentru numărul centrului de mesagerie SMS și să îl schimbați în interfața web de gestionare a routerului, dacă acesta este incorect.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **SMS > Message Settings (Setări mesaje)**.
3. Activați **Message Center (Centrul de mesagerie)**.
4. Introduceți numărul corect în **Message Center Number (Numărul al centrului de mesagerie)**.
5. Faceți clic pe **Save (Salvare)**.



The screenshot shows a window titled "Messages Settings" with a close button (X) in the top right corner. Inside the window, there is a "Message Center" toggle switch which is currently turned on (green). Below it is a "Message Center Number" input field, which is currently empty. Underneath the input field, there is a note that says "Please inquire the number from your ISP." At the bottom of the window, there is a green "Save" button.

---Sfârșit



Contactați ISP-ul dumneavoastră pentru numărul corect al centrului de mesagerie.

6.3 Solicitare informații trimițând comenzi USSD

Funcția **USSD** (Unstructured Supplementary Service Data) este un serviciu de comunicație utilizat în rețelele mobile care permite utilizatorilor să interacționeze în timp real cu furnizorii de servicii prin introducerea unor coduri scurte, de obicei în formatul *XXX#, pentru a accesa informații sau a efectua acțiuni, cum ar fi verificarea soldului contului, reîncărcarea creditului, activarea sau dezactivarea anumitor servicii, sau configurarea opțiunilor de rețea.



Aceste coduri sau comenzi sunt predeterminate. Puteți contacta ISP-ul dvs. pentru a găsi acele coduri sau comenzi specifice.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **SMS > USSD**.
3. Introduceți un **USSD CMD**, cum ar fi ***108#**.
4. Faceți clic pe **Send (Trimitere)**.

A screenshot of a web interface titled "USSD" in the top left corner. The interface contains a form with two main sections. The first section is labeled "USSD CMD:" and has a text input field containing the value "*108#". To the right of this input field is a green button with the text "Send" in white. The second section is labeled "USSD Read:" and has a large, empty rectangular box below it, intended for displaying the response from the USSD command.

---Sfârșit

Așteptați un moment, veți obține informațiile dorite pe care le doriți în caseta **USSD Read**.

7 Rețea Wi-Fi invitați

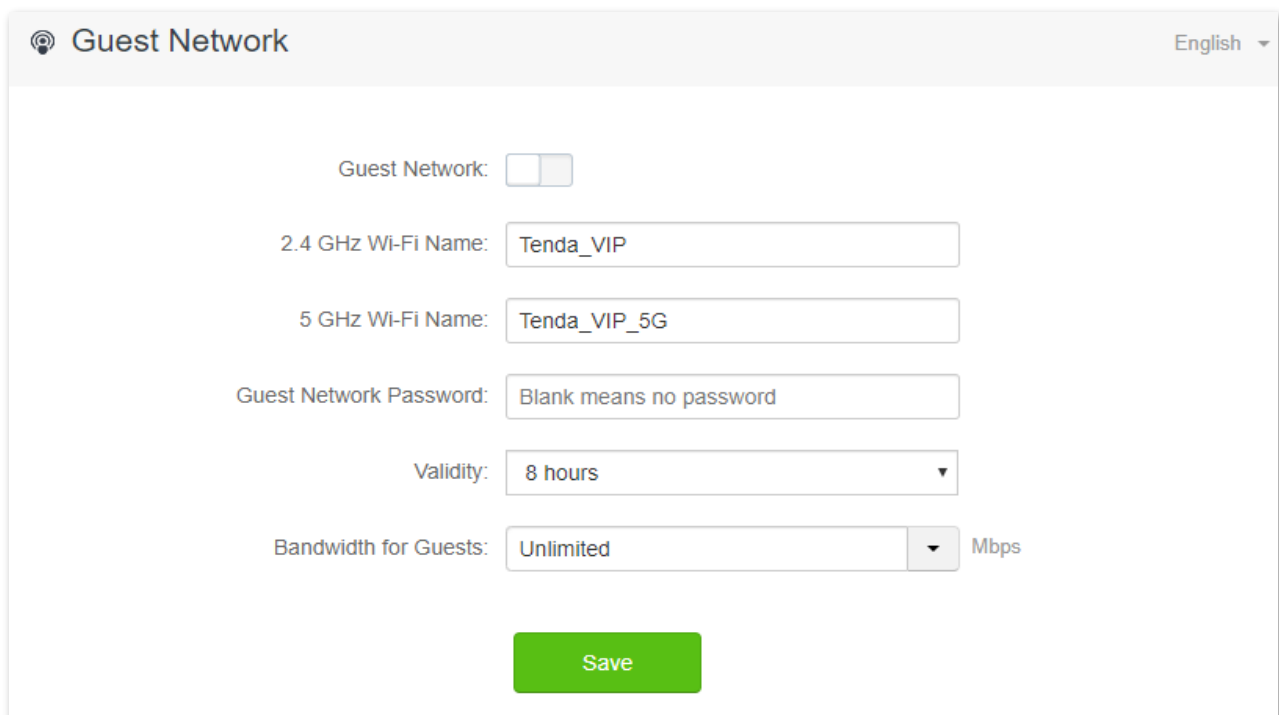
Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

7.1 Prezentare generală

În această secțiune, **Guest Network (Rețea invitați)**, puteți activa sau dezactiva rețeaua Wi-Fi, separată, pe altă clasă de IP, destinată oaspeților și puteți schimba numele și parola Wi-Fi, limita perioada de funcționare și rata maximă partajată cu toți utilizatorii acestei rețele.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Guest Network (Rețea invitați)**.

Această funcție este dezactivată implicit.



The screenshot shows the 'Guest Network' configuration page. At the top left is a Wi-Fi icon and the title 'Guest Network'. At the top right is a language dropdown menu set to 'English'. The main content area contains several settings:

- Guest Network:** A toggle switch that is currently turned off.
- 2.4 GHz Wi-Fi Name:** A text input field containing 'Tenda_VIP'.
- 5 GHz Wi-Fi Name:** A text input field containing 'Tenda_VIP_5G'.
- Guest Network Password:** A text input field containing 'Blank means no password'.
- Validity:** A dropdown menu set to '8 hours'.
- Bandwidth for Guests:** A dropdown menu set to 'Unlimited', with 'Mbps' indicated to the right.

At the bottom center, there is a green 'Save' button.

Descrierea parametrilor

Parametru	Descriere
Guest Network (Rețea invitați)	Folosit pentru a activa sau dezactiva funcția de rețea Wi-Fi destinată invitaților.
2.4 GHz Wi-Fi Name (Nume Wi-Fi 2,4 GHz)	Specificați numele Wi-Fi al rețelei de oaspeți a ruterului. În mod implicit, Tenda_VIP este pentru rețeaua Wi-Fi de 2,4 GHz și Tenda_VIP_5G pentru rețeaua Wi-Fi de 5 GHz.
5 GHz Wi-Fi Name (Nume Wi-Fi 5 GHz)	Puteți schimba SSID-urile (numele Wi-Fi) după cum este necesar. Pentru a distinge rețeaua oaspeților de rețeaua principală, vă recomandăm să setați diferite nume de rețea Wi-Fi.
Guest Network Password (Parola de rețea pentru oaspeți)	Specifică parola (chiar de conectare) pentru cele două rețele invitate ale ruterului.
Validity (Valabilitate)	Specifică valabilitatea rețelelor invitate. Rețelele Wi-Fi destinate invitaților va fi dezactivată automat după perioada de valabilitate. Se poate seta 4 ore, 8 ore sau permanent.
Bandwidth for Guests (Lățimea de bandă pentru oaspeți)	Vă permite să specificați "viteza" (rata) maximă de încărcare și descărcare pentru toate dispozitivele conectate la rețelele Wi-Fi pentru invitați. În mod implicit, lățimea de bandă nu este limitată.

7.2 Configurare Wi-Fi invitați

Scenariu: Un grup de prieteni, împreună cu copiii lor, vor vizita casa dvs. și vor sta aproximativ 8 ore.

Cerințe: Preveniți utilizarea rețelei Wi-Fi principale de către oaspeți, dar și afectarea conexiunii la internet a computerului de serviciu și mai ales evitați partajarea parolei personale pentru rețeaua Wi-Fi principală. De asemenea doriți să evitați ca aceștia sau copiii acestora să partajeze prin Chromecast sau AirPlay diverse videoclipuri pe TV.

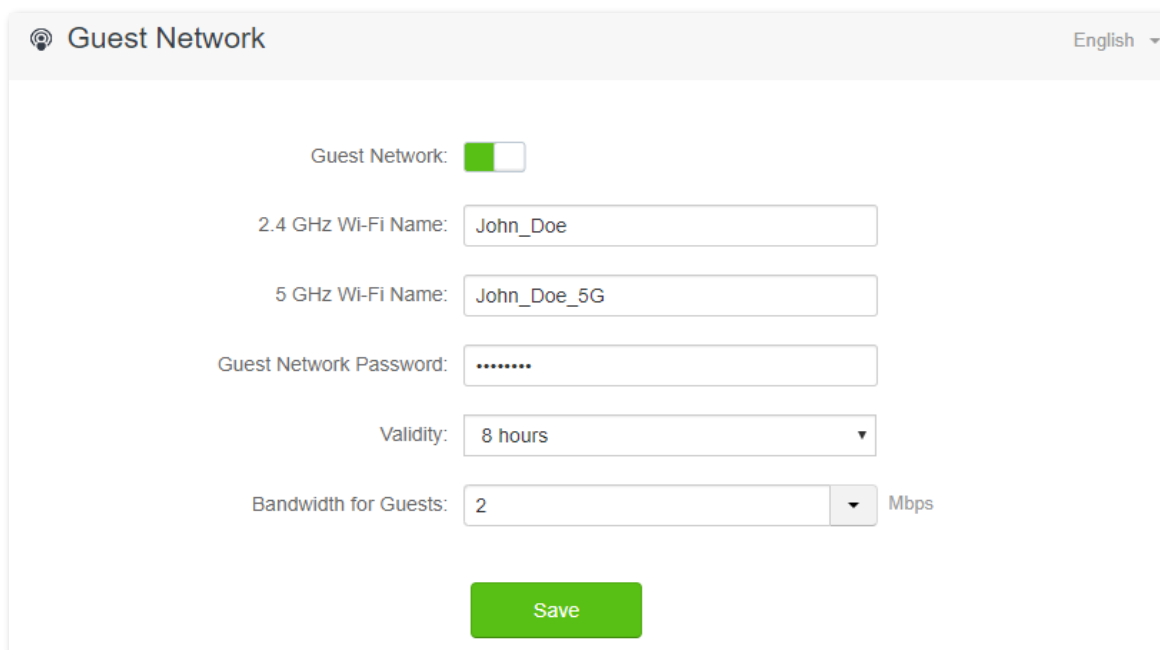
Soluție: Puteți configura funcția de rețea pentru oaspeți și le puteți permite oaspeților să folosească internetul.

Să presupunem că parametrii pe care urmează să îi setați pentru rețeaua Wi-Fi pentru oaspeți:

- Nume Wi-Fi pentru rețelele de 2,4 GHz și 5 GHz: John_Doe și John_Doe_5G
- Parola Wi-Fi pentru rețelele de 2,4 GHz și 5 GHz: Tenda_12345
- Lățimea de bandă partajată pentru oaspeți: 2 Mbps

Procedura de configurare:

1. [Conectați-vă la interfața web a routerului.](#)
2. Navigați la **Guest Network (Rețea invitați)**.
3. Permite cel **Guest Network (Rețea invitați)**.
4. Setați **2.4 GHz Wi-Fi Name (Nume Wi-Fi 2,4 GHz)**, adică **John_Doe** în acest exemplu.
5. Setați **5 GHz Wi-Fi Name (Nume Wi-Fi 5 GHz)**, adică **John_Doe_5G** în acest exemplu.
6. Setați **Guest Network Password (Parolă rețea invitați)**, adică **Tenda_12345** în acest exemplu.
7. Selectați o perioadă de valabilitate din **Validity (Valabilitate)** caseta drop-down, adică **8 ore** în acest exemplu.
8. Setați lățimea de bandă în caseta drop-down **Bandwidth for Guests (Lățime de bandă pentru oaspeți)**, adică **2**, ca exemplu.
9. Faceți clic pe **Save (Salvare)**.



The screenshot shows the 'Guest Network' configuration page. At the top, there is a title 'Guest Network' and a language dropdown set to 'English'. Below the title, there is a toggle switch for 'Guest Network' which is turned on. The configuration fields are as follows:

- 2.4 GHz Wi-Fi Name: John_Doe
- 5 GHz Wi-Fi Name: John_Doe_5G
- Guest Network Password: [masked with dots]
- Validity: 8 hours (dropdown menu)
- Bandwidth for Guests: 2 Mbps (dropdown menu)

At the bottom of the form, there is a green 'Save' button.

---Sfârșit

În cele 8 ore de la configurare, oaspeții își pot conecta dispozitivele wireless, cum ar fi smartphone-urile, la **John_Doe** sau **John_Doe_5G** pentru a accesa internetul și a se bucura de lățimea de bandă partajată de 2 Mbps.

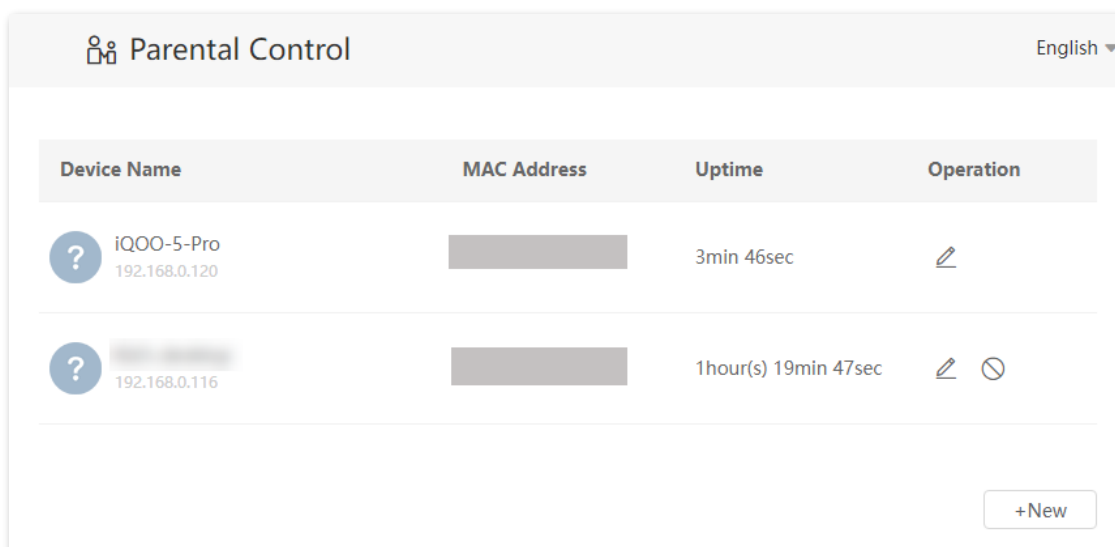
8 Control parental

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

8.1 Prezentare generală

Pe pagina de control parental, puteți vizualiza informațiile dispozitivelor online și puteți configura opțiunile de acces la internet ale acestora.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la pagina **Parental Control (Control parental)**.






The screenshot shows the 'Parental Control' web interface. At the top, there is a header with a home icon, the text 'Parental Control', and a language dropdown set to 'English'. Below the header is a table with the following columns: 'Device Name', 'MAC Address', 'Uptime', and 'Operation'. There are two rows of data. The first row shows a device named 'iQOO-5-Pro' with IP address '192.168.0.120', a greyed-out MAC address, and an uptime of '3min 46sec'. The second row shows a device with a greyed-out name and IP address '192.168.0.116', a greyed-out MAC address, and an uptime of '1hour(s) 19min 47sec'. Each row has an edit icon in the 'Operation' column. At the bottom right of the table area, there is a '+New' button.


Device Name	MAC Address	Uptime	Operation
iQOO-5-Pro 192.168.0.120	[Redacted]	3min 46sec	[Edit]
[Redacted] 192.168.0.116	[Redacted]	1hour(s) 19min 47sec	[Edit] [Stop]

Descrierea parametrilor

Parametru	Descriere
Device Name (Numele dispozitivului)	Specifică numele dispozitivului online.
MAC Address (Adresa MAC)	Specifică adresa MAC a dispozitivului online.
Uptime (Timp de funcționare)	Specifică durata online a dispozitivului.

Parametru	Descriere
Operation (Operațiune)	Faceți clic  pentru a configura regula de control parental pentru dispozitivul dorit. După ce ați configurat regula de control parental pentru dispozitiv, ar trebui să existe un buton  sau  , care este folosit pentru a activa sau dezactiva regula configurată.
+New (+Nou)	Faceți clic pe +New (+Nou) pentru a adăuga reguli de control parental aplicabile pentru alte dispozitive.

8.2 Configurare reguli control parental

Faceți clic pe  sau pe **+New (+Nou)** pentru a edita sau adăuga o regulă de control parental.

Parental Control
✕

Device Name:

MAC Address:

Internet Accessible At: ~

In: Every Day Specified Day

Sun. Mon. Tue. Wed.
 Thur. Fri. Sat.

Website Access Limit:

Access Control Mode: Blacklist Whitelist

Blocked Websites:

Enter website keywords separated by a comma. For example, eHow,google indicates that the eHow and Google websites are inaccessible.

Parametru	Descriere
Device Name (Numele dispozitivului)	Specifică numele dispozitivului căruia i se aplică regula de control parental.

Parametru	Descriere
MAC Address (Adresa MAC)	Specifică adresa MAC a dispozitivului căruia i se aplică regula de control parental.
Internet Accessible At (Acces la internet la)	Specifică intervalul orar în care dispozitivul poate accesa internetul.
In (în)	Specifică zilele în care regula intră în vigoare. Puteți seta Every Day (Zilnic) sau Specified Day (Zi specificată) opțiuni referitoare la zilele din săptămână pentru care se aplică regula.
Website Access Limit (Limitare acces site-uri)	Folosit pentru a activa sau dezactiva funcția de limitare a accesului la site-uri.
Access Control Mode (Mod control acces)	Când funcția de limitare a accesului la site-ul web este activată, sunt disponibile două moduri de control al accesului. <ul style="list-style-type: none"> - Blacklist (Listă neagră): dispozitivul este blocat să acceseze site-urile web specificate în regulă în perioada specificată, dar poate accesa alte site-uri web. Dispozitivul nu poate accesa internetul deloc în afara perioadei specificate. - Whitelist (Listă albă): dispozitivul poate accesa site-urile web specificate în regulă în perioada specificată, dar nu poate accesa alte site-uri web. Dispozitivul nu poate accesa internetul deloc în afara perioadei specificate.
Blocked Websites (Site-uri web blocate)	Specificați site-urile web pentru care dispozitivul are acces sau nu are acces sau i se permite să le acceseze în perioada specificată. În aceste liste puteți introduce cuvinte cheie, precum „Google”, astfel blocând toate domeniile care conțin „Google”. Dacă doriți blocarea în mod specific a unui site trebuie să tastați adresa completă, precum „ www.google.ro ”.
Unblocked Websites (Site-uri web deblocate)	

8.3 Exemplu de adăugare a unei reguli de control parental


Scenariu: Se apropie examenul final pentru copilul tău și vrei să-i restricționezi accesul la internet prin ruter.

Cerințe: Site-urile web, cum ar fi Facebook, Twitter, YouTube și Instagram, sunt inaccesibile între orele 8:00 și 22:00 în weekend, pentru computerul din camera copilului și nu poate accesa internetul deloc între 22:00 și 8:00.

Soluție: Puteți configura funcția de control parental pentru a atinge cerințele.

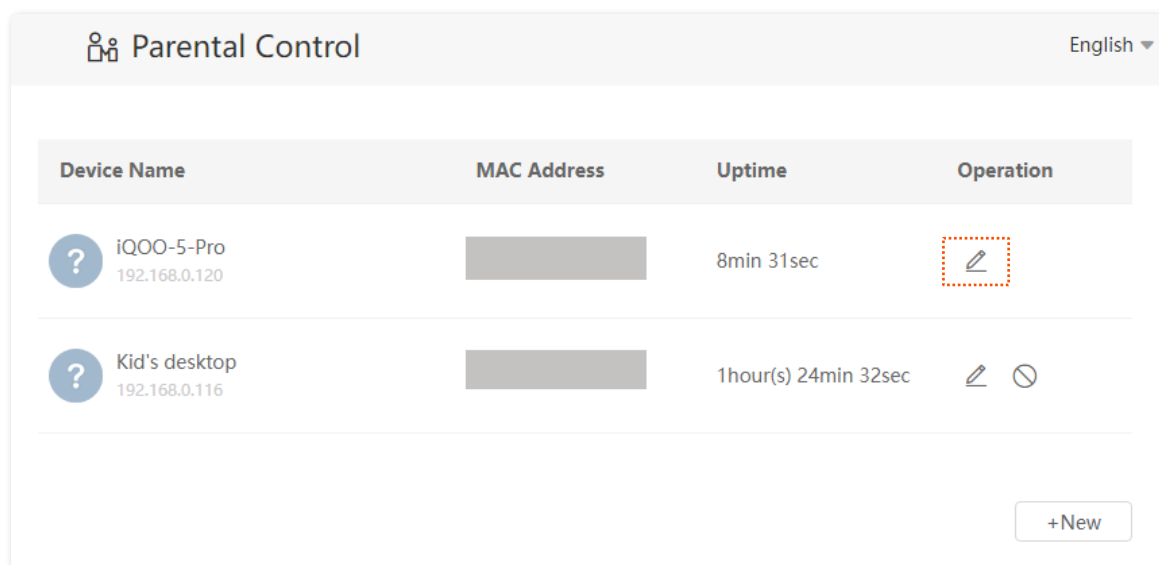
Configurare procedură:








1. [Conectați-vă la interfața web a routerului.](#)

2. Navigați la **Parental Control (Control parental)**.
3. Alegeți dispozitivul căruia i se va aplica regula și faceți clic pe  .



Dacă dispozitivul căruia i se aplică regula nu este online în acel moment, puteți face clic pe **+New (+Nou)** pentru a adăuga o regulă de control parental pentru dispozitiv.



Device Name	MAC Address	Uptime	Operation
 iQOO-5-Pro 192.168.0.120		8min 31sec	
 Kid's desktop 192.168.0.116		1hour(s) 24min 32sec	 

4. Specificați perioada în care site-urile web țintă nu pot fi accesate, perioadă care este **8:00-22:00** în acest exemplu.
5. Navigați la **Specified Day (Zi specificată)** și bifați zilele în care se aplică regula, care sunt **Sun. (Dum.)** și **Sat. (Sâm.)** în acest exemplu.
6. Activați **Website Access Limit (Limitare acces site-uri web)**.
7. Alegeți **Blacklist (Listă neagră)**.
8. Setati **Blocked Websites (Site-uri web blocate)**, și tastați cuvintele cheie, cu virgule între ele, **facebook, twitter, youtube, instagram**, ca exemplu.
9. Faceți clic **Save (Salvați)**.

Parental Control ✕

Device Name: Kid's desktop ✎

Internet Accessible At: 08:00 ~ 22:00

Every Day Mon. Tue. Wed. Thur.
 Fri. Sat. Sun.

Website Access Limit:

Access Control Mode: Blacklist Whitelist

Unblocked Websites: facebook,twitter,youtube,instagram

Enter website keywords separated by a comma. For example, eHow,google indicates that only the eHow and Google websites are accessible.

---Sfârșit

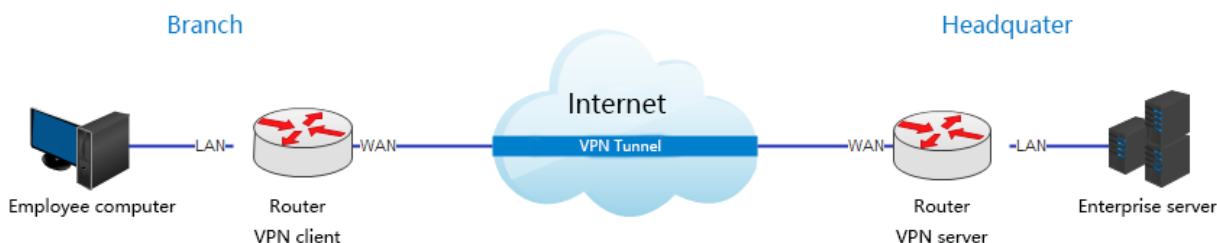
După finalizarea configurației, copilul dvs poate accesa orice site web, cu excepția Facebook, Twitter, YouTube și Instagram de la 8:00 la 22:00 în weekend și nu poate accesa internetul deloc între 22:00 și 8:00.

9 VPN

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

Un VPN (Virtual Private Network) este o tehnologie care creează o conexiune securizată și criptată între dispozitivul unui utilizator și o rețea sau server la distanță, prin intermediul internetului. Acesta permite utilizatorilor să acceseze resurse online în mod privat și să își ascundă adresa IP reală, oferind astfel un nivel suplimentar de securitate și confidențialitate. VPN-urile sunt frecvent utilizate pentru a proteja informațiile personale pe rețele Wi-Fi publice, pentru a accesa conținut restricționat geografic sau pentru a ocoli cenzura pe internet. Prin mascarea identității și criptarea datelor, VPN-urile protejează traficul de rețea împotriva interceptării de către terți sau atacuri cibernetice.

Topologia unei rețele VPN este prezentată mai jos.



9.1 Server PPTP

9.1.1 Prezentare generală

Această serie de routere poate funcționa ca un server PPTP și poate accepta conexiuni de la clienți PPTP.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **VPN > PPTP Server (Server PPTP)**. Această funcție este dezactivată implicit. Când este activată, pagina este afișată ca mai jos.

PPTP Server
✕

PPTP Server:

IP Address Pool: ~

MPPE Encryption:

User Name	Password	Connection Status	Operation
<input type="text"/>	<input type="text"/>	--	<input type="button" value="+New"/>

Descrierea parametrilor

Parametru	Descriere
PPTP Server (Server PPTP)	Folosit pentru a activa sau dezactiva serverul PPTP. Când este activat, ruterul funcționează ca un server PPTP, care poate accepta conexiunile de la clienții PPTP.
IP Address Pool (Pool de adrese IP)	Specifică intervalul intervalului de adrese IP în cadrul căruia serverul PPTP poate aloca clienților PPTP. Este recomandat să păstrați setările implicite.
MPPE Encryption (Criptare MPPE)	MPPE (Microsoft Point-to-Point Encryption) permite criptarea datelor pe 128 de biți. Setările de criptare ar trebui să fie aceleași între serverul PPTP și clienții PPTP. În caz contrar, comunicarea nu poate fi realizată în mod normal.
User Name (Nume de utilizator)	Specificați numele de utilizator VPN și parola, pe care utilizatorul VPN trebuie să le introducă atunci când face apeluri PPTP (conexiuni VPN).
Password (Parolă)	
Connection Status (Starea conexiunii)	Specifică starea conexiunii conexiunii VPN.
Operation (Operațiune)	<p>Operațiunile disponibile includ:</p> <p><input type="button" value="+New"/> : folosit pentru a adăuga noi conturi de utilizator PPTP.</p> <p>⊘ : folosit pentru a dezactiva contul de utilizator PPTP.</p> <p>☑ : folosit pentru a activa contul de utilizator PPTP.</p> <p>🗑️ : folosit pentru a șterge contul de utilizator PPTP.</p>

9.1.2 Permitearea utilizatorilor de pe internet să acceseze servicii din rețeaua locală

Scenariu: Ați configurat un server FTP în rețeaua locală (LAN) a ruterului.

Cerințe: Deschideți serverul FTP pentru utilizatorii de pe internet. Astfel, doriți să le permiteți să acceseze resursele serverului FTP, de pe internet, din afara rețelei locale.

Soluție: Puteți configura funcția server PPTP pentru a atinge cerințele. Să presupunem că:

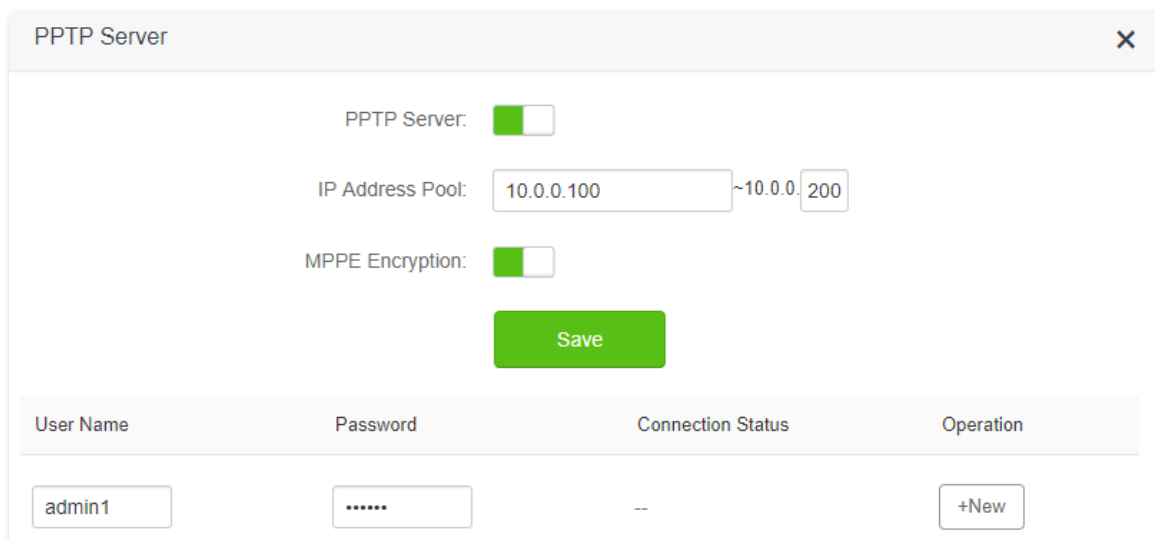
- Numele de utilizator și parola pe care serverul PPTP le atribuie clientului sunt ambele admin1.
- Adresa IP WAN a ruterului este 113.88.112.220.
- IP-ul local pentru serverul FTP este 192.168.0.136.
- Portul TCP a serverului FTP este 21.
- Numele de utilizator și parola de conectare FTP sunt ambele: JohnDoe.



Vă rugăm să vă asigurați că adresa IP WAN a ruterului este dintr-o rețea publică. Este posibil ca această funcție să nu funcționeze pe o gazdă cu o adresă IP a unei rețele private. Adresele IPv4 comune sunt clasificate în clasa A, clasa B și clasa C. Adresele IP private (adrese destinate pentru rețele locale LAN) din clasa A variază de la 10.0.0.0 la 10.255.255.255. Adresele IP private (adrese destinate pentru rețele locale LAN) din clasa B variază între 172.16.0.0-172.31.255.255. Adresele IP private (adrese destinate pentru rețele locale LAN) din clasa C variază de la 192.168.0.0-192.168.255.255.


Procedura de configurare:

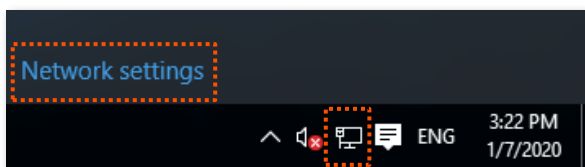
1. [Conectați-vă la interfața web a ruterului.](#)
2. Activați funcția **PPTP Server (Server PPTP)**.
 - 1) Navigați la **VPN > PPTP Server (Server PPTP)**.
 - 2) Activați **PPTP Server (Server PPTP)**.
 - 3) Activați **MPPE Encryption (Criptare MPPE)**, ceea ce înseamnă că cifra de criptare rămâne valoarea implicită „128”.
 - 4) Faceți clic pe **Save (Salvare)**.
3. Adăugați numele de utilizator și parola PPTP.
 - 1) Setati **User Name (Nume utilizator)** și **Password (Parolă)** pentru un utilizator PPTP, care sunt admin1 în acest exemplu.
 - 2) Faceți clic pe **+New (+ Nou)**.



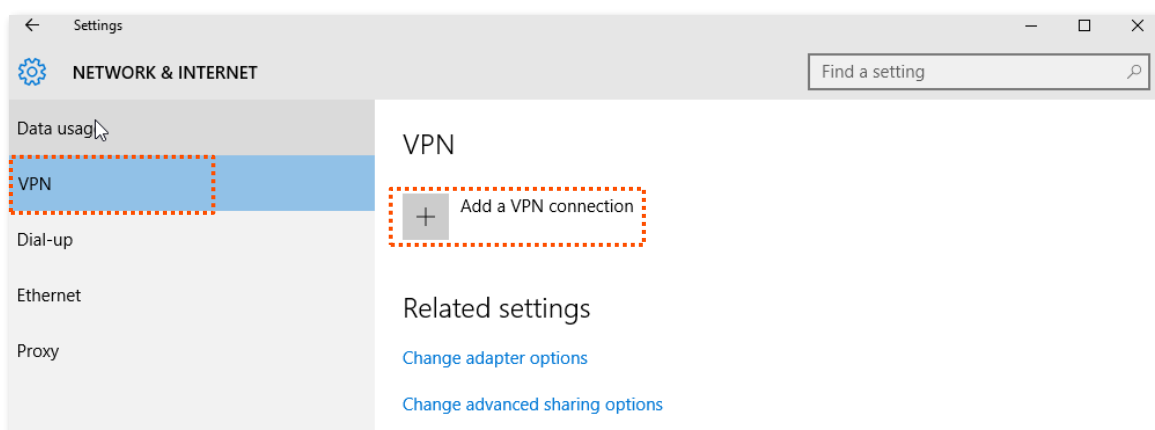
---Sfârșit

Când configurarea este finalizată, utilizatorii de internet pot accesa serverul FTP urmând acești pași, descriși pentru sistemul de operare **Microsoft Windows 10**, însă, în principiu, pașii se pot aplica pentru orice alt sistem de operare:

1. Faceți clic pe pictograma  din colțul din dreapta jos de pe desktop, apoi faceți clic pe **Network settings (Setări de rețea)**.

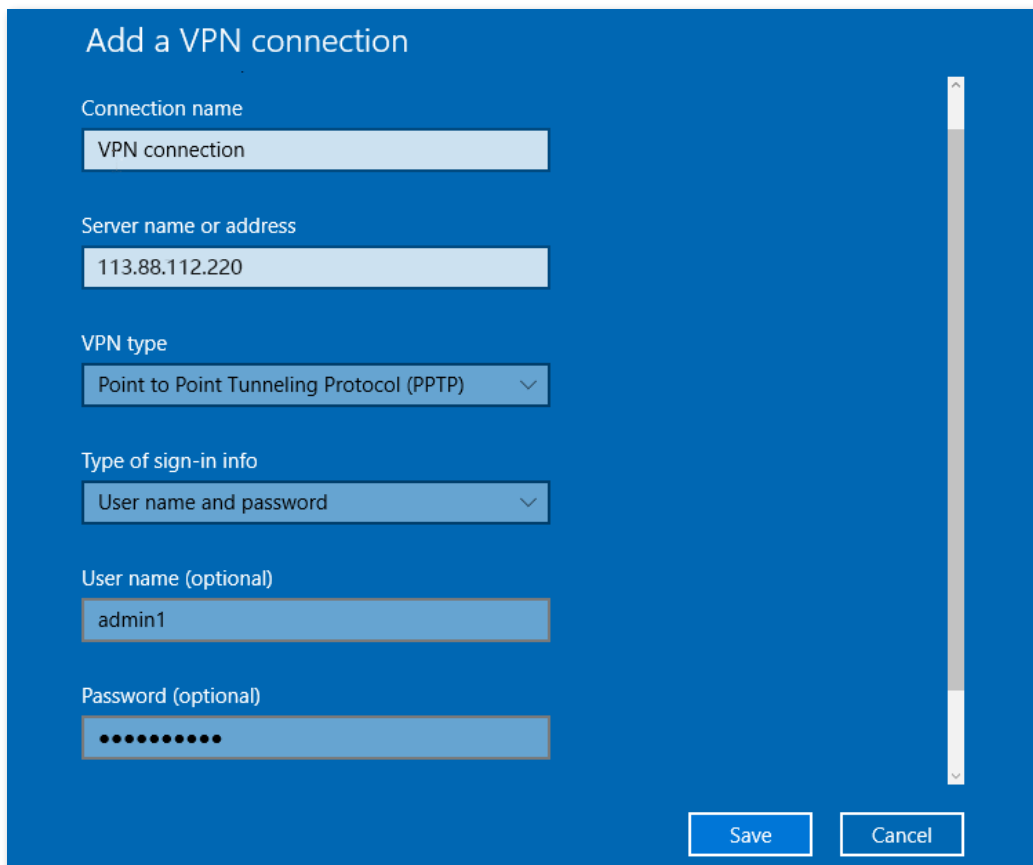


2. Alegeți **VPN** din partea stângă și faceți clic pe **Add a VPN connection (Adăugați o conexiune VPN)**.



3. În noua fereastră configurați parametrii VPN.
 - 1) Introduceți un nume pentru conexiune, cum ar fi **VPN connection (Conexiune VPN)**.

- 2) Introduceți adresa serverului, care este adresa IP publică a ruterului Tenda, fiind **113.88.112.220** în acest exemplu.
- 3) Selectați un **tip de VPN (VPN type)**, care este **Point to Point Tunneling Protocol (PPTP)** în acest exemplu.
- 4) Selectați un tip de informații de conectare, care sunt **User name and password (Nume de utilizator și parolă)** în acest exemplu.
- 5) Introduceți numele de utilizator și parola, care sunt ambele **admin1** în acest exemplu.
- 6) Faceți clic pe **Save (Salvare)**.

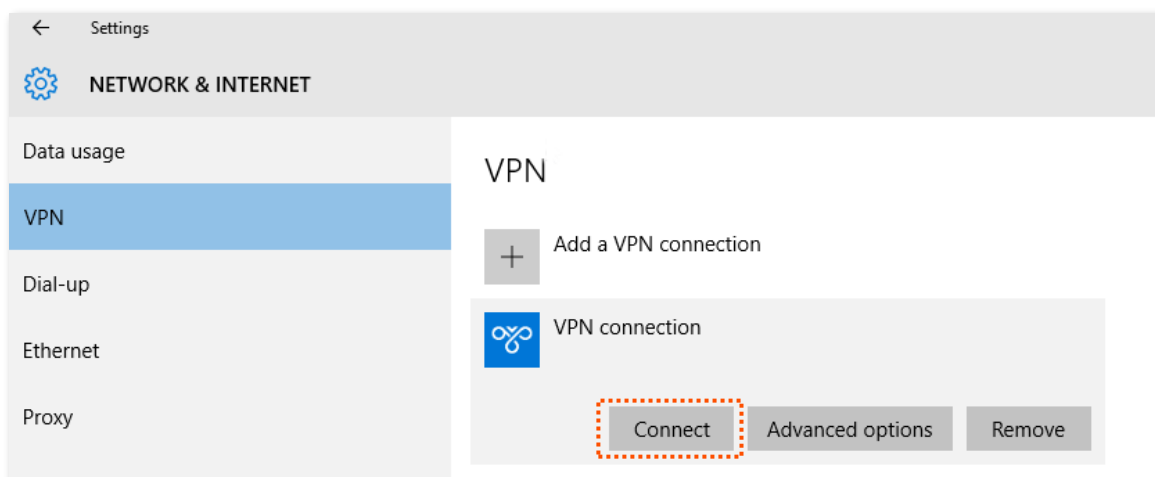



The screenshot shows the 'Add a VPN connection' dialog box. The fields are filled with the following information:

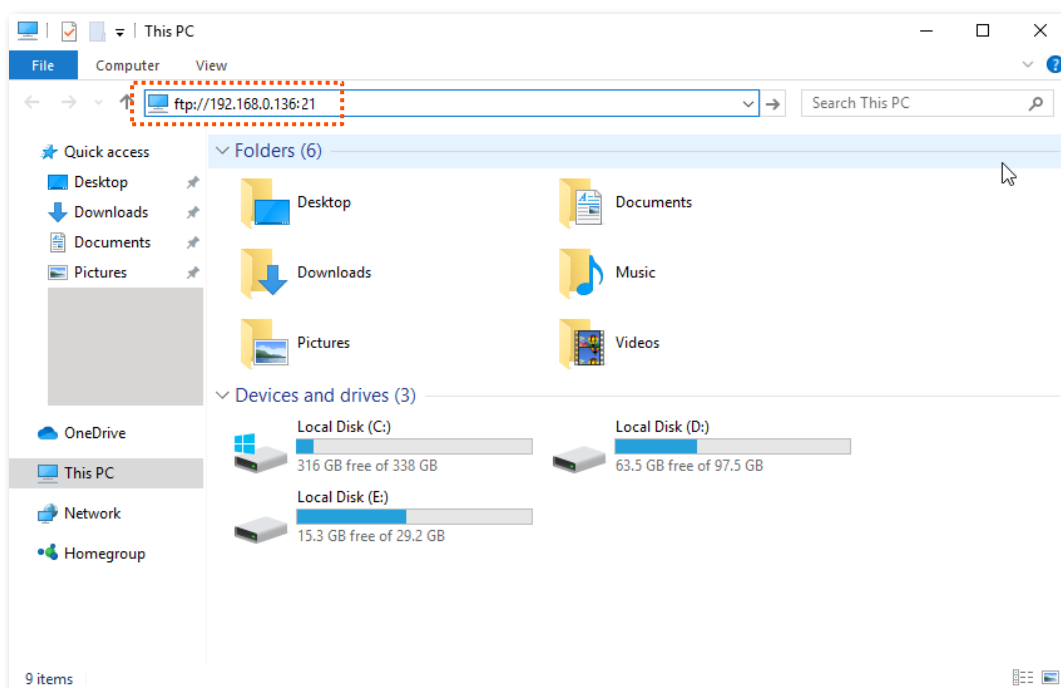
- Connection name: VPN connection
- Server name or address: 113.88.112.220
- VPN type: Point to Point Tunneling Protocol (PPTP)
- Type of sign-in info: User name and password
- User name (optional): admin1
- Password (optional): [Redacted]

Buttons: Save, Cancel

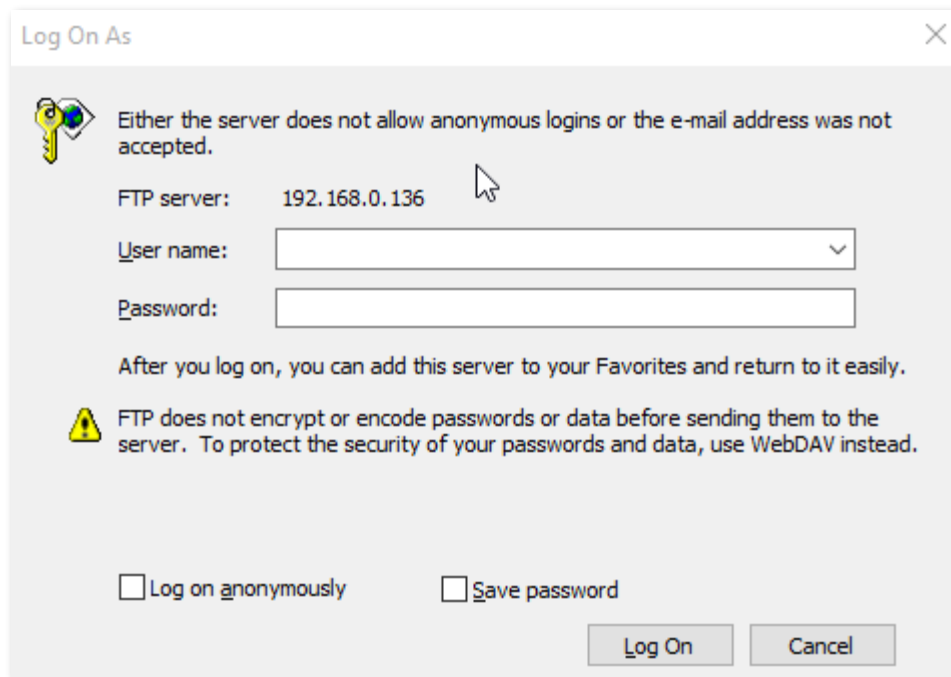
4. Găsiți conexiunea VPN adăugată și faceți clic pe **Connect (Conectare)**. Așteptați câteva momente pentru realizarea conexiunii.



5. Faceți clic pe pictograma  de pe desktop sau căutați **Explorer** și introduceți adresa în bara de adrese pentru a accesa serverul FTP, care este **ftp://192.168.0.136:21** în acest exemplu.



6. Introduceți numele de utilizator și parola pentru conectarea la serverul FTP, care sunt ambele **JohnDoe** în acest exemplu, și faceți clic pe **Log On (Conectare)**.



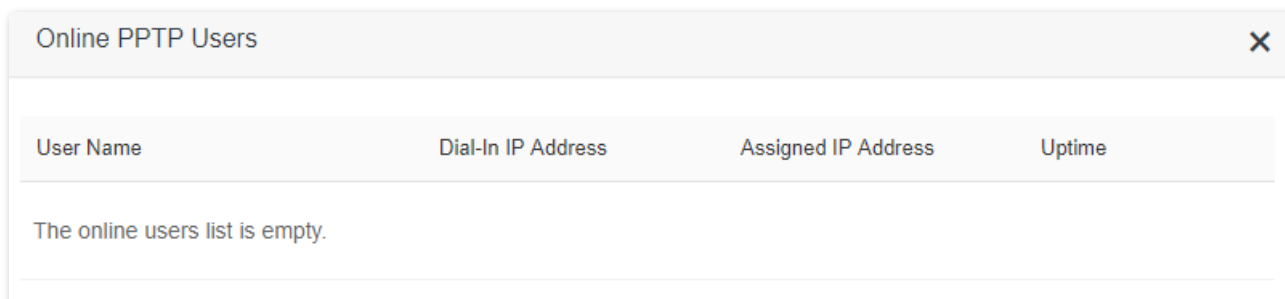
---Sfârșit

Efectuând pașii de mai sus, puteți accesa resursele de pe serverul FTP. Toate fișierele și folderele o să le vedeți în fereastra de **Explorer**. Bineînțeles, pentru accesarea serverului FTP puteți utiliza și alte programe destinate accesării serverelor FTP.

9.2 Vizualizare utilizatori PPTP conectați

Când funcția server PPTP este activată, puteți vizualiza informații detaliate despre clienții VPN care stabilesc conexiuni cu serverul PPTP configurat.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **VPN > Online PPTP Users (Utilizatori online PPTP)**.



User Name	Dial-In IP Address	Assigned IP Address	Uptime
The online users list is empty.			

Descrierea parametrilor

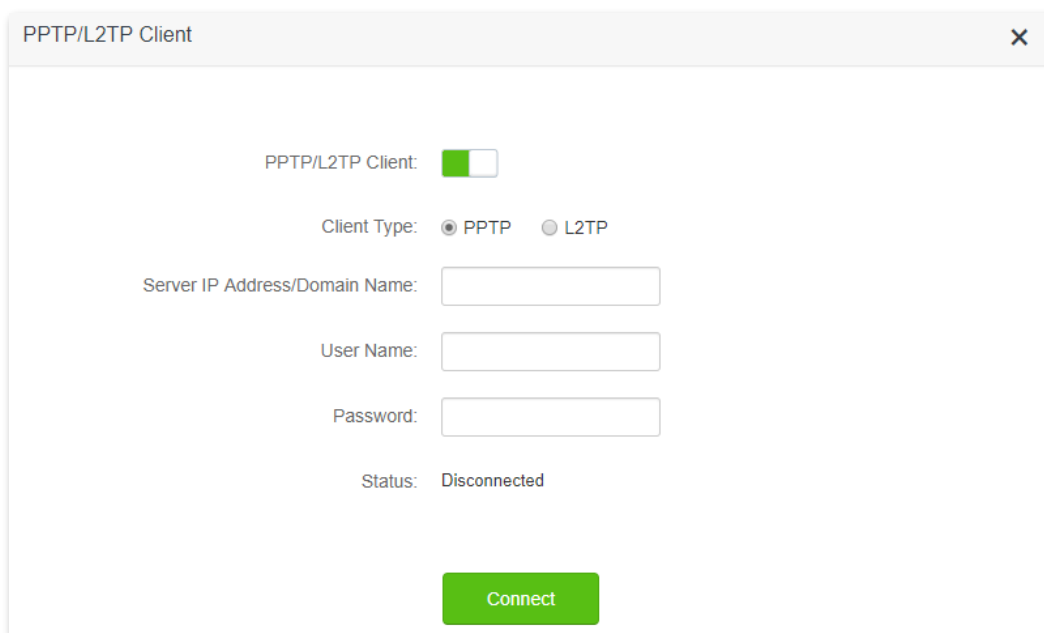
Parametru	Descriere
User Name (Nume de utilizator)	Specifică numele de utilizator VPN, pe care utilizatorul VPN îl folosește atunci când face apeluri PPTP (conexiune VPN).
Dial-In IP Address (Adresă IP de apelare)	Specifică adresa IP a clientului PPTP. Dacă clientul trece printr-un router atunci adresa IP va fi cea a portului WAN a ruterului din locația clientului conectat.
Assigned IP Address (Adresă IP atribuită)	Specifică adresa IP pe care serverul PPTP o atribuie clientului din IP Address Pool (Pool de adrese IP) .
Uptime (Timp de funcționare)	Specifică timpul online de când conexiunea VPN reușește.

9.3 Client PPTP/L2TP

9.3.1 Prezentare generală

Acest router poate funcționa ca client PPTP/L2TP și se poate conecta la servere PPTP/L2TP.

PPTP/L2TP este dezactivată implicit. Când este activată, pagina este afișată ca mai jos.



Descrierea parametrilor

Parametru	Descriere
PPTP/L2TP Client (Client PPTP/L2TP)	Folosit pentru a activa sau dezactiva funcția client PPTP/L2TP.
Client Type (Tipul de client)	Specifică tipul de client pe care ruterul îl servește, fie PPTP, fie L2TP. <ul style="list-style-type: none">- PPTP: când ruterul se conectează la un server PPTP, alegeți această opțiune.- L2TP: când ruterul se conectează la un server L2TP, alegeți această opțiune.
Server IP Address/Domain Name (Adresă IP/Numele de domeniu al serverului)	Specifică adresa IP sau numele de domeniu al serverului PPTP/L2TP la care se conectează ruterul.
User Name (Nume de utilizator)	Specificați numele de utilizator și parola de autentificare la serverul PPTP/L2TP.
Password (Parolă)	

Parametru	Descriere
Status (Stare)	Specifică starea conexiunii conexiunii VPN.

9.3.2 Conectare ruter la un server VPN

Scenariu: Fiind în departamentul IT și lucrând remote, administratorul de rețea supervisor, de la locul de muncă, vă oferă acces la resursele companiei prin VPN.

Cerințe: Doriți ca indiferent ce calculator din rețeaua de acasă folosiți, să aveți acces la fișierele și serverele companiei.

Soluție: Puteți configura funcția de client PPTP/L2TP pentru a atinge cerințele. Să presupunem că:

- Adresa IP publică a serverului VPN PPTP este 113.88.112.220.
- Utilizatorul și parola sunt ambele **admin1**.

Procedura de configurare:

1. [Conectați-vă la interfața web a routerului.](#)
2. Navigați la **VPN > PPTP/L2TP Client (Client PPTP/L2TP)**.
3. Activați **PPTP/L2TP Client (Client PPTP/L2TP)**.
4. Alegeți **PPTP** ca **tip de client (Client Type)**.
5. Introduceți, în **Server IP Address/Domain Name (Adresă IP server/Nume domeniu)**, IP-ul **113.88.112.220**, ca exemplu.
6. Introduceți **User Name (Nume utilizator)** și **Password (Parolă)**, care sunt ambele **admin1** în acest exemplu.
7. Faceți clic pe **Connect (Conectare)**.

PPTP/L2TP Client

PPTP/L2TP Client:

Client Type: PPTP L2TP

Server IP Address/Domain Name:

User Name:

Password:

Status: Disconnected

---Sfârșit

Când **Connected (Conectat)** este afișat în **Status (Stare)**, puteți accesa resursele rețelei locale de la serviciu prin VPN.

9.4 IPSec

9.4.1 Prezentare generală

Nu toate echipamentele din serie au această funcționalitate activă. Vă rugăm contactați departamentul suport tehnic Tenda sau citiți specificațiile tehnice aferente.

Exemplificările de mai jos se aplică pentru: Tenda 4G06 v3.0 și Tenda 4G03 v3.0

Acest router are funcționalitatea de VPN **IPSec**. VPN IPSec (Internet Protocol Security) este un protocol de securitate utilizat pentru a crea conexiuni VPN sigure prin criptarea și autentificarea datelor transmise între două dispozitive sau rețele. IPSec asigură confidențialitatea, integritatea și autenticitatea datelor, protejându-le împotriva interceptării și manipulării pe parcursul transmisiilor prin rețele nesigure, cum ar fi internetul. IPSec funcționează la nivelul rețelei (Layer 3) și poate fi utilizat pentru a securiza atât conexiunile site-to-site (între două rețele), cât și conexiunile remote access (între un dispozitiv individual și o rețea). IPSec utilizează două moduri principale de funcționare: **Tunnel Mode**, care criptează întregul pachet IP, și **Transport Mode**, care criptează doar porțiunea de date a pachetului. Este adesea combinat cu alte protocoale VPN, cum ar fi L2TP (Layer 2 Tunneling Protocol), pentru a oferi o securitate suplimentară.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **VPN > IPSec**. Această funcție este dezactivată implicit. Faceți clic pe **+New (+Nou)** pentru a configura funcția IPSec.



Descrierea parametrilor

Parametru	Descriere
Status (Stare)	Specifică starea funcției IPSec.
Connection Name (Numele conexiunii)	Specifică numele conexiunii IPSec.

Parametru	Descriere
Encapsulation Mode (Modul de încapsulare)	<p>Modurile de încapsulare IPSec (Encapsulation Modes) specifică modul în care datele sunt încapsulate și securizate atunci când sunt transmise printr-o conexiune IPSec:</p> <ul style="list-style-type: none"> - Transport (Transport Mode): Acest mod este utilizat, de obicei, între două dispozitive finale (gazde) sau între o gazdă și un gateway. În mod transport, doar porțiunea de date (payload-ul) din pachetul IP este criptată, în timp ce antetul original IP rămâne necriptat. Este mai potrivit pentru scenariile în care un singur dispozitiv trebuie să securizeze datele transmise, fără a modifica antetul de rutare. - Tunel (Tunnel Mode): Acest mod este utilizat, în general, între două gateway-uri de securitate (cum ar fi două routere sau firewall-uri) sau între un dispozitiv client și un gateway. În acest mod, întregul pachet IP, inclusiv antetul original, este criptat și încapsulat într-un nou pachet IP. Acesta este preferat în conexiunile site-to-site, deoarece ascunde informațiile de rutare și protejează întreaga structură a pachetului.
Protocol	<p>Specifică protocolul care oferă serviciul de securitate pentru IPSec.</p> <ul style="list-style-type: none"> - AH (Authentication Header): Este un protocol din cadrul IPSec care asigură integritatea și autenticitatea pachetelor IP, dar nu oferă criptare. AH protejează datele împotriva modificărilor în timpul transmisiei prin adăugarea unui antet de autentificare care include o semnătură digitală. Dacă un pachet este manipulat sau alterat în orice fel pe parcursul transmisiei, receptorul va detecta acest lucru și va respinge pachetul în timpul procesului de verificare a integrității. Cu toate acestea, AH nu protejează confidențialitatea datelor, deoarece nu criptează conținutul pachetului. - ESP (Encapsulating Security Payload): Este un protocol din IPSec care oferă atât criptare, cât și integritate. ESP criptează datele din pachet, asigurând confidențialitatea, astfel încât dacă un pachet este interceptat, atacatorul nu va putea accesa conținutul real. În plus, ESP verifică și integritatea pachetului, similar cu AH, pentru a se asigura că datele nu au fost modificate în timpul transmisiei. Datorită acestei combinații de funcții de securitate, ESP este folosit pe scară largă în produsele gateway și în scenariile care necesită un nivel ridicat de protecție a datelor. - AH+ESP: Aceasta indică utilizarea simultană a ambelor protocoale – AH pentru verificarea integrității și autenticității pachetului, și ESP pentru criptarea și verificarea suplimentară a datelor. Astfel, această combinație oferă atât protecție împotriva alterării datelor, cât și confidențialitate maximă.
Remote Gateway (Gateway de la distanță)	Specifică adresa IP sau numele de domeniu al gateway-ului peer al tunelului IPSec.
Operation (Operațiune)	<p>Operațiunile disponibile includ:</p> <p> : folosit pentru a adăuga o nouă conexiune IPSec.</p> <p> : folosit pentru a șterge o conexiune IPSec.</p>

9.4.2 Configurare conexiune IPSec

Când se apasă butonul **+New (+Nou)** pentru crearea unei noi conexiuni **IPSec**, atunci fereastra cu opțiunile aferente arată astfel:

← Add IPSec VPN

IPSec Status:

Mobile Data Options: Tunnel mode

Connection Name:

Negotiation Mode: Initiator

Protocol: ESP

Remote Gateway: URL

Local LAN IP/Prefix Length:

Remote LAN IP/Prefix Length:

Key Exchange Method: Auto (IKE)

Authentication Method: Pre-shared Key

Pre-shared Key:


DPD:

Show Advanced Settings ▾

Save

Descrierea parametrilor

Parametru	Descriere
IPSec Status (Stare IPSec)	Folosit pentru a activa sau dezactiva funcția IPSec.

Parametru	Descriere
Mobile Data Options (Opțiuni de date mobile)	<p>Modurile de încapsulare IPSec (Encapsulation Modes) specifică modul în care datele sunt încapsulate și securizate atunci când sunt transmise printr-o conexiune IPSec:</p> <ul style="list-style-type: none"> - Transport (Transport Mode): Acest mod este utilizat, de obicei, între două dispozitive finale (gazde) sau între o gazdă și un gateway. În mod transport, doar porțiunea de date (payload-ul) din pachetul IP este criptată, în timp ce antetul original IP rămâne necriptat. Este mai potrivit pentru scenariile în care un singur dispozitiv trebuie să securizeze datele transmise, fără a modifica antetul de rutare. - Tunel (Tunnel Mode): Acest mod este utilizat, în general, între două gateway-uri de securitate (cum ar fi două routere sau firewall-uri) sau între un dispozitiv client și un gateway. În acest mod, întregul pachet IP, inclusiv antetul original, este criptat și încapsulat într-un nou pachet IP. Acesta este preferat în conexiunile site-to-site, deoarece ascunde informațiile de rutare și protejează întreaga structură a pachetului.
Connection Name (Denumire conexiune)	<p>Specifică numele conexiunii IPSec.</p>
Negotiation Mode (Modul de negociere)	<p>Negotiation Mode (Modul de negociere) specifică rolul pe care un dispozitiv îl are în stabilirea conexiunii IPSec, în funcție de cine inițiază negocierea tunelului:</p> <ul style="list-style-type: none"> - Initiator (Inițiator): Acest dispozitiv este cel care pornește procesul de negociere și trimite prima solicitare de conectare către dispozitivul egal (peer). Inițiatorul începe configurarea tunelului IPSec prin trimiterea de cereri de conectare și propuneri de securitate, cum ar fi algoritmi de criptare și metode de autentificare. - Responder (Cel care răspunde): Acest dispozitiv așteaptă ca dispozitivul egal să trimită o solicitare de conectare. Când primește cererea de la inițiator, acesta răspunde și negociază parametrii tunelului IPSec pe baza propunerilor primite. <p> TIP</p> <p>Important: Nu setați ambele capete ale tunelului IPSec ca Responder, deoarece niciun dispozitiv nu va iniția solicitarea de conectare, ceea ce va face ca tunelul IPSec să eșueze în a se stabili. Un capăt trebuie să fie setat ca Initiator, iar celălalt ca Responder, pentru a asigura succesul negocierii și stabilirea conexiunii IPSec.</p>

Parametru	Descriere
Protocol	<p>Specifică protocolul care oferă serviciul de securitate pentru IPSec.</p> <ul style="list-style-type: none"> - AH (Authentication Header): Este un protocol din cadrul IPSec care asigură integritatea și autenticitatea pachetelor IP, dar nu oferă criptare. AH protejează datele împotriva modificărilor în timpul transmisiei prin adăugarea unui antet de autentificare care include o semnătură digitală. Dacă un pachet este manipulat sau alterat în orice fel pe parcursul transmisiei, receptorul va detecta acest lucru și va respinge pachetul în timpul procesului de verificare a integrității. Cu toate acestea, AH nu protejează confidențialitatea datelor, deoarece nu criptează conținutul pachetului. - ESP (Encapsulating Security Payload): Este un protocol din IPSec care oferă atât criptare, cât și integritate. ESP criptează datele din pachet, asigurând confidențialitatea, astfel încât dacă un pachet este interceptat, atacatorul nu va putea accesa conținutul real. În plus, ESP verifică și integritatea pachetului, similar cu AH, pentru a se asigura că datele nu au fost modificate în timpul transmisiei. Datorită acestei combinații de funcții de securitate, ESP este folosit pe scară largă în produsele gateway și în scenarii care necesită un nivel ridicat de protecție a datelor. - AH+ESP: Aceasta indică utilizarea simultană a ambelor protocole – AH pentru verificarea integrității și autenticității pachetului, și ESP pentru criptarea și verificarea suplimentară a datelor. Astfel, această combinație oferă atât protecție împotriva alterării datelor, cât și confidențialitate maximă.
Remote Gateway (Gateway la distanță)	Specifică adresa IP sau numele de domeniu al gateway-ului peer al tunelului IPSec.
Local LAN IP/Prefix Length (IP LAN local/Lungime prefix)	Specifică lungimea segmentului/prefixului de rețea a rețelei LAN a dispozitivului. De exemplu, dacă adresa IP a portului LAN al dispozitivului este 192.168.5.1 și masca de subrețea este 255.255.255.0, lungimea locală LAN/prefix poate fi 192.168.5.0/24.
Remote LAN IP/Prefix Length (IP LAN la distanță/Lungime prefix)	Specifică lungimea segmentului/prefixului de rețea a rețelei LAN a gateway-ului peer al tunelului IPSec. Dacă dispozitivul peer este o gazdă, acest parametru poate fi setat ca „adresa IP a dispozitivului/32”.

Parametru	Descriere
Key Exchange Method (Metoda de schimb de chei)	<p>Key Exchange Method (Metoda de schimb de chei) specifică modul în care cheile criptografice sunt schimbate pentru a securiza tunelul IPSec. În mod implicit, este selectată opțiunea Auto (IKE).</p> <ul style="list-style-type: none"> – Auto (IKE): Acest mod indică faptul că o Asociație de Securitate (SA) este configurată, întreținută și ștersă automat utilizând protocolul IKE (Internet Key Exchange). IKE gestionează schimbul de chei și negocierea parametrilor de securitate, reducând complexitatea configurării manuale și facilitând gestionarea conexiunilor IPSec. Cheile și parametrii de securitate sunt actualizați regulat pe durata ciclului de viață al SA, ceea ce asigură o securitate mai mare și o protecție continuă a datelor transmise. – Manual: Acest mod implică configurarea Asociației de Securitate (SA) prin specificarea manuală a algoritmilor și a cheilor de criptare și autentificare. Spre deosebire de modul automat, în acest caz SA nu are un ciclu de viață prestabilit și nu se actualizează automat, rămânând valabilă până când este modificată sau ștearsă manual. Aceasta poate crea riscuri de securitate, deoarece cheile nu sunt reînnoite automat, expunând tunelul la potențiale vulnerabilități. Modul manual este de obicei folosit doar în scopuri de testare sau configurare inițială.
Authentication Method (Metoda de autentificare)	Indică un șir de chei partajate negociat de părțile IPSec cu ceva timp în avans.
Pre-shared Key (Cheie pre-partajată)	Specifică cheia pre-partajată utilizată în timpul negocierii. Acest parametru trebuie să fie același cu cel al gateway-ului peer. Sunt permise maximum 128 de caractere.
DPD	<p>DPD (Dead Peer Detection) la IPSec este o funcție care monitorizează starea conexiunii IPSec și detectează dacă dispozitivul de la celălalt capăt al tunelului (peer) este activ și funcțional. DPD trimite periodic mesaje de control către peer pentru a verifica dacă acesta răspunde. Dacă peer-ul nu răspunde într-un anumit interval de timp, DPD presupune că tunelul a eșuat sau peer-ul nu mai este disponibil, și poate lua măsuri, cum ar fi închiderea tunelului sau reconectarea automată.</p> <p>Activarea DPD este importantă pentru a menține stabilitatea și securitatea tunelului IPSec, deoarece detectează rapid problemele de conectivitate și previne situațiile în care traficul este trimis pe o conexiune care nu mai este activă. În acest mod, dispozitivul știe când trebuie să restabilească conexiunea sau să înceteze trimiterea de date prin tunelul IPSec nevalid.</p>

Tot în aceeași fereastră faceți clic pe **Advanced (Avansat)** pentru a afișa parametrii avansați ai negocierii automate. Următoarele afișează pagina când sunt afișați parametrii avansați.

Phase 1

Exchange Mode:

Encryption Algorithm:

Integrity Algorithm:

Diffie-Hellman Group:

Local ID Type:

Remote ID Type:

Key Lifetime: s (Range: 600 to 604800)

Phase 2

Perfect Forward Secrecy:



Encryption Algorithm:

Integrity Algorithm:

Key Lifetime: s (Range: 600 to 604800)

Descrierea parametrilor

Parametru	Descriere
Exchange Mode (Modul de schimb)	<p>Specifică modul de schimb în IKE Phase 1 (Faza 1), care ar trebui să fie același cu cel al gateway-ului peer.</p> <ul style="list-style-type: none"> - Main (Principal): acest mod este modul principal. În acest mod, pachetele schimbate sunt uriașe pentru a oferi protecție identității, care este aplicabilă scenariilor în care protecția identității este riguroasă. - Aggressive (Agresiv): acest mod nu oferă protecție identității. În acest mod, pachetele schimbate sunt puține la număr și rata de negociere este mare, ceea ce este aplicabil scenariilor în care protecția identității este slabă.

Parametru	Descriere
Encryption Algorithm (Algoritm de criptare)	<p>Specifică algoritmul de criptare a sesiunii IKE.</p> <ul style="list-style-type: none"> - DES (Standard de criptare a datelor): o cheie de 56 de biți este utilizată pentru a cripta datele de 64 de biți. Ultimii 8 biți ai datelor pe 64 de biți sunt utilizați pentru verificarea parității. 3DES indică faptul că sunt folosite trei chei pe 56 de biți pentru criptare. - AES (Advanced Encryption Standard): AES 128/192/256 indică faptul că cheile de 128/192/256 de biți sunt folosite pentru criptare, respectiv.
Integrity Algorithm (Algoritm de integritate)	<p>Specifică algoritmul de verificare a sesiunii IKE.</p> <ul style="list-style-type: none"> - MD5 (Message Digest Algorithm): este generat un rezumat de mesaje pe 128 de biți pentru a preveni manipularea mesajelor. - SHA1 (Secure Hash Algorithm): se generează un rezumat al mesajelor pe 160 de biți pentru a preveni manipularea mesajelor, ceea ce duce la o securitate mai mare decât MD5.
Diffie-Hellman Group (Grupul Diffie-Hellman)	<p>Specifică informațiile de grup pentru algoritmul Diffie-Hellman pentru generarea unei chei de sesiune utilizată pentru a cripta un tunel IKE. Informațiile ar trebui să fie aceleași cu cele ale gateway-ului la distanță.</p>
Local ID Type (Tipul ID local)	<p>Specifică ID-ul gateway-ului local.</p> <ul style="list-style-type: none"> - IP Address (Adresă IP): ruterul utilizează adresa IP a portului WAN specificat pentru negocierea cu gateway-ul de la distanță. - FQDN: nume de domeniu complet calificat. Dacă selectați FQDN, trebuie să setați manual un șir de caractere, care ar trebui să fie identic cu ID-ul de la distanță. <p> TIP</p> <p>Local ID Type (Tipul ID local) și Remote ID Type (Tipul ID la distanță) ar trebui să fie aceleași. În astfel de circumstanțe, vi se recomandă să modificați Mode (Modul) la Aggressive (Agresiv).</p>
Remote ID Type (Tip ID telecomandă)	<p>Specifică ID-ul gateway-ului la distanță.</p> <ul style="list-style-type: none"> - IP Address (Adresă IP): În mod implicit, gateway-ul la distanță utilizează adresa IP WAN a ruterului pentru negociere. - FQDN: nume de domeniu complet calificat. Dacă selectați FQDN, trebuie să setați manual un șir de caractere, care ar trebui să fie identic cu ID-ul local. <p> TIP</p> <p>Local ID Type (Tipul ID local) și Remote ID Type (Tipul ID la distanță) ar trebui să fie aceleași. În astfel de circumstanțe, vi se recomandă să modificați Mode (Modul) la Aggressive (Agresiv).</p>
Key Lifetime (Ciclu cheie)	<p>Specifică ciclul de viață al IPSec SA.</p>

Parametru	Descriere
Perfect Forward Secrecy (Secretul de transmitere perfect)	<p>Această caracteristică generează o nouă cheie în IKE Faza II, care nu are legătură cu cheia generată în IKE Faza I, asigurând că cheia generată în Faza II este sigură chiar dacă cheia generată în IKE1 Phase 2 (Faza 2) este spartă.</p> <p>Cu Perfect Forward Secrecy (Secretul direct perfect dezactivat), generarea noii chei în IKE Faza II depinde de cheia din Faza I. Odată ce cheia generată în IKE Faza I este spartă, cheia generată în Faza II va suferi amenințări și va amenința în continuare securitatea comunicațiilor.</p>

10

Setări avansate

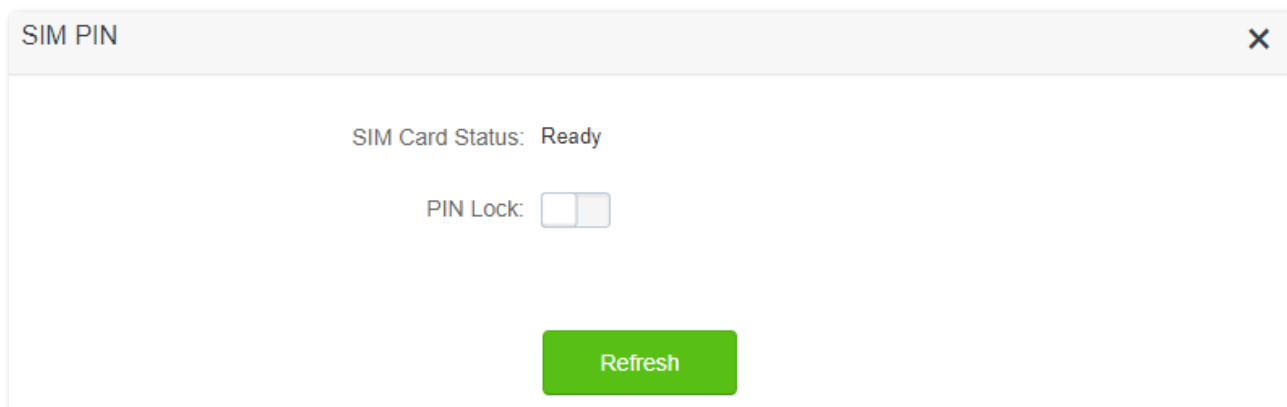
Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

10.1 PIN SIM

PIN-ul SIM este o măsură de protecție pentru a preveni utilizarea greșită a cartelei SIM. Dacă cartela SIM este blocată când o introduceți în router, vi se cere să o deblocați pentru acces la internet. De asemenea, puteți să activați blocarea PIN și să specificați un cod PIN pentru o cartelă SIM deblocată.

Pentru a accesa pagina de setări PIN SIM, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > SIM PIN (PIN SIM)**.

Când cartela SIM nu este setată cu codul PIN, pagina este afișată ca mai jos.



10.1.1 Deblocare cartelă SIM

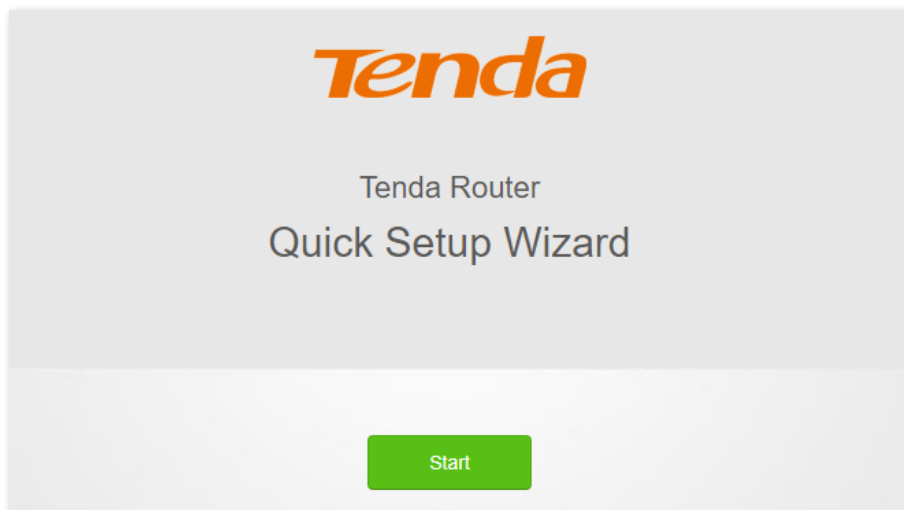
Dacă doriți să utilizați o cartelă SIM blocată pentru a accesa internetul, mai întâi trebuie să o deblocați.

Deblocare cartelă SIM în asistentul de configurare inițială

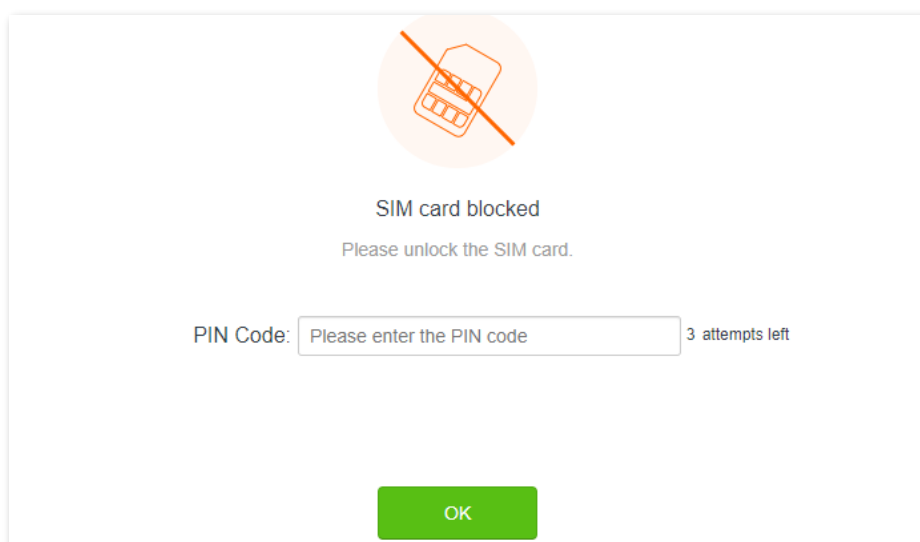
Când configurați ruterul pentru prima dată sau când ruterul este resetat, vi se solicită să deblocați cartela SIM în asistentul de configurare pas cu pas.

Procedura de configurare:

1. [Conectați-vă la interfața web a routerului.](#)
2. Faceți clic pe **Start**.



3. Introduceți **PIN Code (Codul PIN)** și faceți clic pe **OK**.



NOTE

Puteți încerca codul PIN doar de 3 ori. Dacă nu reușiți toate, trebuie să utilizați codul PUK pentru a reseta codul PIN. Contactați ISP-ul dvs. pentru codul PUK sau găsiți imprimată pe cartela mare care conținea cartela SIM decupată. În caz contrar, cartela SIM poate fi blocată definitiv după ce ați introdus codul PUK greșit de 10 ori.

4. Urmați pașii pentru a finaliza procesul de configurare.

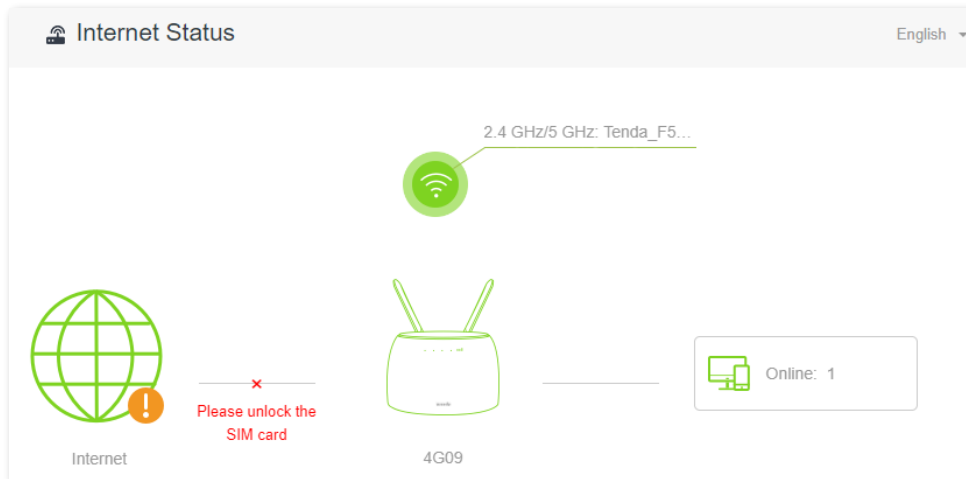
---Sfârșit

Deblocare SIM în interfața web de gestionare

De asemenea, puteți debloca cartela SIM atunci când puteți accesa deja interfața de utilizare web a ruterului.

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Clic pe **Please unlock the SIM card (Vă rugăm să deblocați cartela SIM)** sau navigați la **Advanced Settings (Setări avansate) > SIM PIN (PIN SIM)**.



3. Introduceți **PIN Code (Codul PIN)** și faceți clic pe **Save (Salvare)**.

NOTE

- Puteți încerca codul PIN doar de 3 ori. Dacă nu reușiți toate, trebuie să utilizați codul PUK pentru a reseta codul PIN. Contactați ISP-ul dvs. pentru codul PUK sau găsiți codul pe cartela mare sau în plicul în care a venit de la ISP. În caz contrar, cartela SIM poate fi blocată definitiv după ce ați introdus codul PUK greșit de 10 ori.
- Când opțiunea **Auto-unlock PIN (Deblocare automată PIN)** este activată, ruterul va debloca automat cartela SIM la fiecare repornire, însă codul PIN trebuie reintrodus după o resetare a echipamentului sau o reintroducere a cartelei SIM.

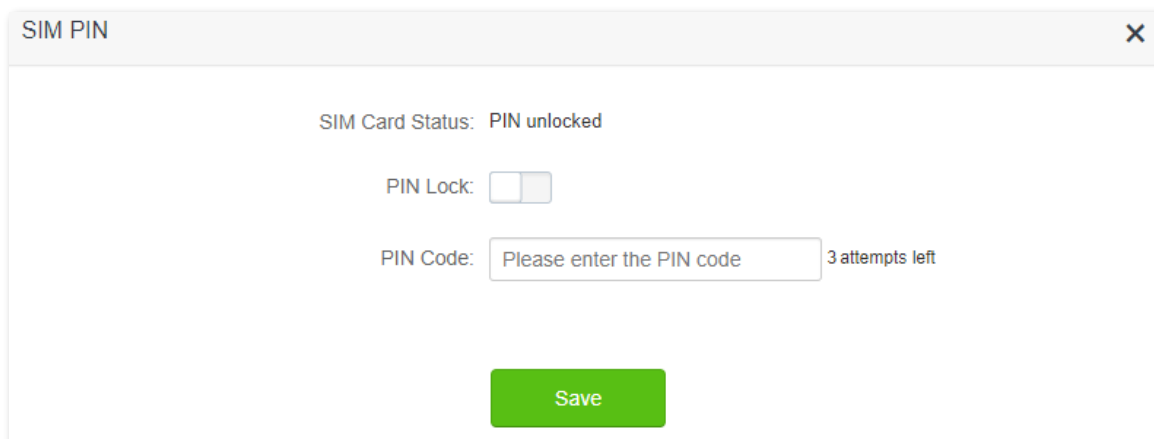
---Sfârșit

10.1.2 Dezactivare PIN pentru SIM

După ce blocarea PIN este dezactivată pentru cartela SIM, cartela SIM nu va fi protejată de blocarea PIN.

Procedura de configurare:

1. [Conectati-vă la interfața web a ruterului.](#)
2. Navigați la **Advanced Settings (Setări avansate) > SIM PIN (PIN SIM)**.
3. Dezactivați **PIN Lock (Blocare PIN)**.
4. Introduceți codul PIN în câmpul **PIN Code (Cod PIN)** și faceți clic pe **Save (Salvare)**.



---Sfârșit



Puteți încerca codul PIN doar de 3 ori. Dacă nu reușiți toate, trebuie să utilizați codul PUK pentru a reseta codul PIN. Contactați ISP-ul dvs. pentru codul PUK. În caz contrar, cartela SIM poate fi blocată definitiv după ce ați introdus codul PUK greșit de 10 ori.

10.1.3 Activare blocare cu PIN pentru cartela SIM

Puteți activa blocarea cartelei prin introducerea codului PIN. PIN-ul pentru SIM este o măsură de protecție pentru a preveni utilizarea greșită a cartelei SIM.

Procedura de configurare:

1. [Conectați-vă la interfața web a routerului.](#)
2. Activați **PIN Lock (Blocare PIN)**.
3. Introduceți **PIN Code (Cod PIN)** și faceți clic pe **Save (Salvare)**.

SIM PIN ✕

SIM Card Status: Ready

PIN Lock:

Auto-unlock PIN:

PIN Code: 3 attempts left



TIP

- Puteți încerca codul PIN doar de 3 ori. Dacă nu reușiți toate, trebuie să utilizați codul PUK pentru a reseta codul PIN. Contactați ISP-ul dvs. pentru codul PUK. În caz contrar, cartela SIM poate fi blocată definitiv după ce ați introdus codul PUK greșit de 10 ori.
- Când **Auto-unlock PIN (Deblocare automată PIN)** este activat, ruterul va debloca automat cartela SIM de fiecare dată când ruterul finalizează repornirea, însă codul PIN este încă necesar după resetarea generală a echipamentului sau după reintroducerea unei noi cartele SIM.

---Sfârșit

10.2 Date mobile

10.2.1 Prezentare generală

Puteți vizualiza și actualiza statisticile de utilizare a datelor mobile și puteți configura setările de utilizare a datelor, cum ar fi limită de utilizare a datelor și alertare.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Mobile Data (Date mobile)**.

Mobile Data
✕

Total Used: 0.261 MB Update

This usage statistic is for reference. You can send messages to your ISP to inquire the accurate usage statistic and update it here manually.

Data Limit:

The router automatically disconnects from the internet when the data limit is reached.

Monthly Allowance: GB ▾

Usage Alert: 80%

SMS Alert of Usage: Send Test Message

Note: This function may cause SMS charges.

Monthly Data Statistics:

Start Date:

Save

Descrierea parametrilor

Parametru	Descriere
Total Used (Total folosit)	<p>Specifică traficul total de date mobile care a fost utilizat. Puteți corecta valoarea cerând aceste informații de la ISP și apoi făcând clic Update (Actualizați) pentru a modifica manual.</p> <p>Când funcția Monthly Data Statistics (Statistică lunară a datelor) este activată, ruterul va șterge numărul la data specificată în Start Date (Data de începere).</p>
Data Limit (Limită de date)	Folosit pentru a activa sau dezactiva funcția de limitare a datelor. Când limita este atinsă, ruterul se va deconecta automat de la internet.
Monthly Allowance (Alocare lunară)	Specifică utilizarea maximă specifică a datelor permisă pentru fiecare lună.
Usage Alert (Alertă de utilizare)	Când procentul de trafic de date utilizat atinge limita, ruterul va trimite un mesaj SMS de alertă către un anumit număr de mobil.
SMS Alert of Usage (Alertă prin SMS pentru utilizare)	<p>Specifică numărul mobil pentru primirea mesajului SMS de alertă.</p> <p>Puteți face clic pe Send Test Message (Trimiteți mesaj de testare) pentru a testa numărul de mobil pe care l-ați introdus.</p>

Parametru	Descriere
Monthly Data Statistics (Statistici lunare de date)	Folosit pentru a activa sau dezactiva statisticile lunare de date. Când este activat, ruterul va reseta valoarea corespunzătoare traficului lunar total utilizat la data specificată în Start date (Data de începere) .
Start Date (Data de începere)	Specifică data la care ruterul șterge statisticile de date din ultima lună și începe să înregistreze în luna următoare.

10.2.2 Configurarea unei alerte pentru atingerea unei limite de trafic prin date mobile

Scenariu: Ați introdus o cartelă SIM în router pentru a oferi acces la internet mobil pentru smartphone, iPad și laptop.

Cerințe: Doriți să primiți o alertă de mesaj SMS pe smartphone și să vă pregătiți când utilizarea ajunge la o anumită valoare în fiecare lună.

Soluție: Puteți configura setările de date mobile pentru a îndeplini cerințele.

Să presupunem că:

- Trafic de date disponibil: 10 GB
- Data începerii înregistrării utilizării datelor: prima în fiecare lună
- Numărul de mobil pe care doriți să primiți alerta: 188****5555
- Procent alertă: 80%

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **Advanced Settings (Setări avansate) > Mobile Data (Date mobile)**.
3. Opțional, faceți clic pe **Update (Actualizare)** pentru a actualiza datele de utilizare curentă afișată la **Total Used (Total Utilizat)**.
4. Activați **Data Limit (Limită de date)**, introduceți **10** în Alocație lunară și alegeți **GB** în caseta derulantă.
5. Setati **Usage Alert (Alerta de utilizare)** la **80%**.
6. Introduceți **188****5555** în Alerta **SMS Alert of Usage (SMS de utilizare)**.
7. Activați **Monthly Data Statistics (Statisticile lunare ale)** datelor.
8. Introduceți **1** în **Start Date (Data de începere)** și faceți clic pe **Save (Salvare)**.

Mobile Data ✕

Total Used: 0.000 MB Update

This usage statistic is for reference. You can send messages to your ISP to inquire the accurate usage statistic and update it here manually.

Data Limit:

The router automatically disconnects from the internet when the data limit is reached.

Monthly Allowance: GB ▾

Usage Alert: 80%

SMS Alert of Usage: Send Test Message

Note: This function may cause SMS charges.

Monthly Data Statistics:

Start Date:

Save

---Sfârșit

După configurare este finalizat, veți primi un mesaj SMS când traficul de date a ajuns la 8 GB și nu puteți accesa internetul prin router când traficul de date a ajuns la 10 GB.



TIP

Dacă doriți să vă conectați din nou la internet după ce limita de date este atinsă, încercați următoarele metode:

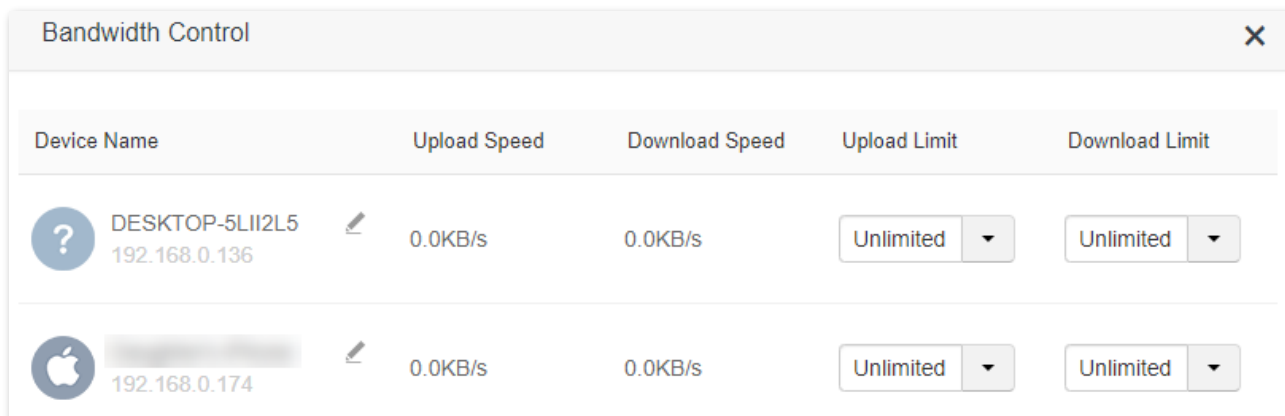
- Modificați **Total Usage (Utilizarea totală)** făcând clic pe **Update (Actualizare)**.
 - Dezactivați **Data Limit (Limita de date)**.
 - Navigați la **Internet Settings (Setări Internet)** și faceți clic pe **Connect (Conectare)** în partea de jos a paginii.
-




10.3 Controlul lăţimii de bandă

10.3.1 Prezentare generală


Prin configurarea acestei funcţii, puteţi limita viteza de încărcare şi descărcare a dispozitivelor conectate la router şi puteţi aloca lăţimea de bandă în mod rezonabil.

Pentru a accesa pagina, [conectaţi-vă la interfaţa web a ruterului](#) şi navigaţi la **Advanced Settings (Setări avansate) > Bandwidth Control (Controlul lăţimii de bandă)**.



Device Name	Upload Speed	Download Speed	Upload Limit	Download Limit
 DESKTOP-5LII2L5 192.168.0.136	0.0KB/s	0.0KB/s	Unlimited	Unlimited
  192.168.0.174	0.0KB/s	0.0KB/s	Unlimited	Unlimited

Descrierea parametrilor

Parametru	Descriere
Device Name (Numele dispozitivului)	Specifică numele şi adresa IP a dispozitivului. Puteţi face clic pe  pentru a modifica numele dispozitivului afişat în interfaţa ruterului. Schimbarea nu va afecta denumirea reală a dispozitivului..
Upload Speed (Viteza de încărcare)	Specifică rata actuală, în timp real, de încărcare şi descărcare a dispozitivului.
Download Limit (Limită de descărcare)	
Upload Limit (Limită de încărcare)	Specificaţi o limită maximă de rată de încărcare şi descărcare pentru dispozitiv. Puteţi face clic pe caseta derulantă pentru a alege o valoare prestabilită sau pentru a seta manual rata maximă.
Download Limit (Limită de descărcare)	

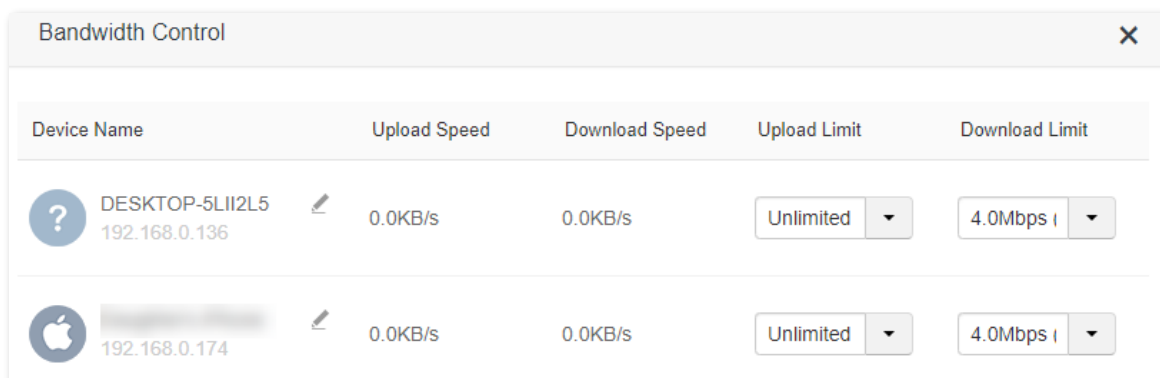
10.3.2 Limitare rată la încărcare și descărcare pentru dispozitivele conectate



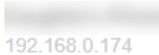
Scenariu: Doriți să alocați o lățime de bandă în mod egal tuturor dispozitivelor conectate și să aibă parte de videoclipuri 720p fluide.

Soluție: Configurați funcția de control a lățimii de bandă pentru a îndeplini cerințele.

Procedura de configurare:

1. [Conectați-vă la interfața web de gestionare.](#)
2. Navigați la **Advanced Settings (Setări avansate) > Bandwidth Control (Control lățime de bandă)**.
3. Localizați dispozitivele care trebuie controlate și setați **Download Limit (Limita de descărcare)** la **4.0 Mbps (For HD Video) (4,0 Mbps (pentru video HD))**.
4. Faceți clic pe **Save (Salvare)**.



Device Name	Upload Speed	Download Speed	Upload Limit	Download Limit
 DESKTOP-5LII2L5 192.168.0.136	0.0KB/s	0.0KB/s	Unlimited	4.0Mbps
  192.168.0.174	0.0KB/s	0.0KB/s	Unlimited	4.0Mbps

---Sfârșit

După configurare, cea mai mare rată (folosită și expresia “viteză”) pentru dispozitiv este de 4 Mbps (sau 512 KB/s) și poate fi satisfăcută cerința de videoclipuri 720p.

10.4 Aplicația Tenda WiFi de Android și iOS

Ruterul poate fi monitorizat și gestionat din aplicația **Tenda WiFi**, de Android și iOS. Cu această aplicație puteți să:

- Gestionați ruterul din rețeaua locală (LAN).
- Gestionați ruterul de pe internet, de oriunde.



Pentru a gestiona ruterul cu aplicația Tenda WiFi, urmați pașii de mai jos (Exemplu: iPhone).



TIP

Aplicația Tenda WiFi V4.0.1 este luată ca exemplu aici.

Procedura de configurare:

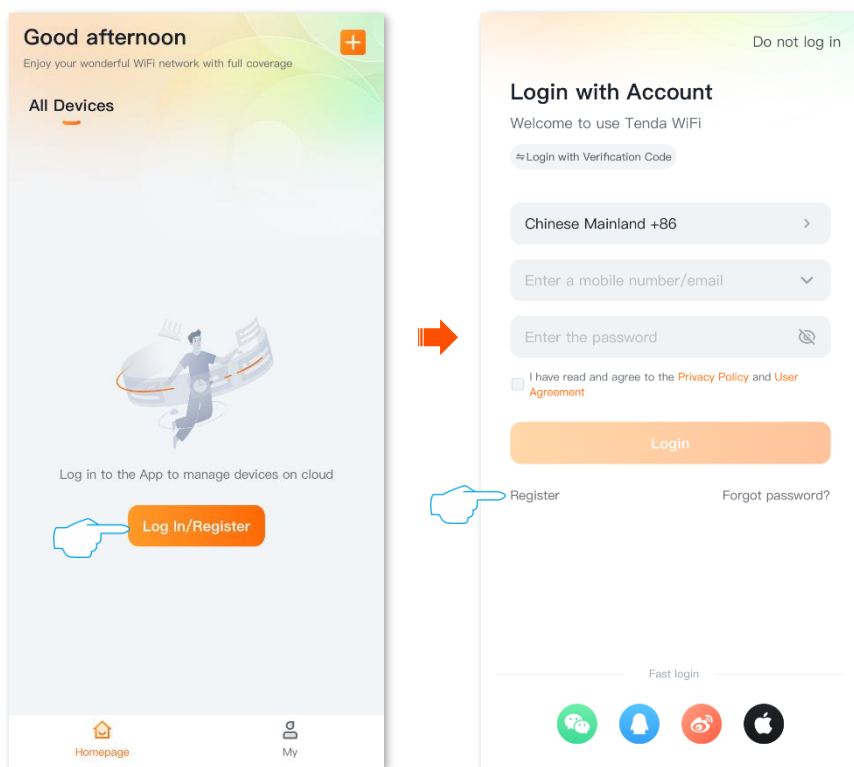
1. Conectați-vă smartphone-ul la internet și descărcați aplicația **Tenda WiFi** pe dispozitivul dvs. mobil scanând **codul QR** sau căutând **Tenda WiFi** în **Google Play** sau **App Store**.



Sau



2. **Opțional:** Rulați aplicația **Tenda WiFi** și clic **Log In/Register (Autentificare/Înregistrare)**. Faceți clic pe **Register (Înregistrare)** și apoi introduceți parametrii necesari pentru înregistrare.



3. Conectați-vă cu un cont înregistrat de Tenda WiFi.
4. În prima pagină a aplicației o să vedeți toate echipamentele Tenda detectate de Tenda WiFi. Dați clic pe pictograma echipamentului Tenda.
5. Apoi, logați-vă la interfața ruterului introducând parola de acces la interfața de gestionare.
6. Opțional, de pe telefon:
 - 1) Porniți un browser web pe smartphone-ul conectat la router și accesați din bara de adrese, nu câmpul căutare, <http://tendawifi.com> pentru a vă conecta la interfața web de gestionare a ruterului.
 - 2) Navigați la **Advanced Settings (Setări avansate) > Tenda WiFi App (Aplicația Tenda WiFi)**.
 - 3) Activați **Manage with Tenda WiFi App (Gestionare cu aplicația Tenda WiFi)**.
 - 4) Introduceți un cont înregistrat în aplicația Tenda WiFi în **Cloud Account (Contul cloud)**.
 - 5) Faceți clic pe **Save (Salvare)**.

Tenda WiFi App

Manage with Tenda WiFi App:

ID:

Cloud Account:

Save

Scan to download Tenda WiFi App.

---Sfârșit

Când configurarea este finalizată, vă puteți gestiona ruterul cu aplicația Tenda WiFi de pe smartphone-ul dvs. oriunde și oricând prin internet.

10.5 Modul repaus

Când modul de repaus este activat, ruterul își stinge indicatoarele LED și dezactivează rețeaua Wi-Fi în perioada specificată.

Pentru a accesa modul repaus, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Sleeping Mode (Modul Sleep)**.

Această funcție este dezactivată implicit. Când este activată, pagina este afișată ca mai jos.

Sleeping Mode

Sleeping Mode:

Sleeping Time: : : :

Delay: Delay enabling the Sleep mode when there is an online user.

Save

Descrierea parametrilor

Parametru	Descriere
Sleeping Mode (Modul Sleep)	Folosit pentru a activa sau dezactiva funcția de repaus. Când ruterul este în modul de repaus și doriți să utilizați rețeaua Wi-Fi, utilizați aplicația Tenda WiFi pentru a activa ruterul.
Sleeping Time (Timp de somn)	Specifică perioada în care ruterul se află în modul de repaus.
Delay (Întârziere)	Folosit pentru a activa sau dezactiva funcția Delay (Întârziere). <ul style="list-style-type: none">- Bifat: funcția este activată. În timpul perioadei de inactivitate, dacă există un utilizator conectat la router și traficul prin portul WAN al ruterului depășește 3 KB/s în 30 de minute, ruterul va întârzia intrarea în modul de repaus. Dacă nu există niciun utilizator conectat la router și traficul prin portul WAN al ruterului este mai lent de 3 KB/s în 3 minute, ruterul va intra în modul de repaus.- Debifat: funcția este dezactivată. Ruterul intră în modul de repaus în timpul perioadei de repaus.

10.6 Control indicatoare LED

Cu funcția de control LED, puteți controla starea indicatoarelor.


Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > LED Control (Control LED)**.

LED Control ✕

LED Control: Enable Disable Schedule

Save

Descrierea parametrilor

Parametru	Descriere
Enable (Permite)	Toți indicatorii LED rămân în starea lor normală.
Disable (Dezactivați)	Toți indicatorii LED sunt dezactivați.
Schedule (Programa)	Indicatoarele LED sunt oprite doar în perioada specificată.
	Este necesar doar când este selectat Schedule (Programare) .
	Specifică perioada în care indicatorii sunt opriți.
Turn Off During (Opriți în timpul)	 TIP Dacă ora de începere pe care o setați este mai mare decât ora de încheiere, programul începe de la ora de început până la ora de încheiere în a doua zi. De exemplu, dacă setați Turn Off During (Oprire în timpul) la 08:00~06:25 , aceasta indică faptul că programul începe de la 08:00 la 06:25 în a doua zi.

10.7 Filtru adresă MAC

10.7.1 Privire de ansamblu

Această funcție vă permite să blocați sau să filtrați accesul dispozitivelor client la rețeaua routerului și implicit la internet, pe baza adresei MAC a adaptorului de rețea utilizat de client. Adresele MAC pot fi adăugate fie pe o listă denumită **Blacklist (Listă neagră)**, care blochează accesul acelor dispozitive, fie pe una denumită **Whitelist (Listă albă)**, care permite accesul doar dispozitivelor incluse în listă, excluzându-le pe celelalte.

Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Filter MAC address (Filtru adresă MAC)**.

Descrierea parametrilor

Parametru	Descriere
MAC Address Filter Mode (Mod de filtrare a adresei MAC)	<p>Specifică modul de filtrare a adresei MAC.</p> <ul style="list-style-type: none">- Blacklist (Lista neagră): dispozitivele enumerate în listă, cu adresele MAC aferente, nu se pot conecta la rețeaua Wi-Fi sau prin cablu a ruterului și implicit nu pot accesa internetul.- Whitelist (Lista albă): numai dispozitivele enumerate în listă, cu adresele MAC aferente, se pot conecta la rețeaua Wi-Fi sau prin cablu a ruterului și implicit nu pot accesa internetul. Rețineți că unele dispozitive pot schimba aleatoriu adresa MAC a adaptorului de rețea (pe cablu sau Wi-Fi). Schimbarea adresei MAC de către dispozitivul client, cunoscută și sub numele de „MAC spoofing”, permite unui dispozitiv să își modifice adresa MAC pentru a se prezenta cu o identitate diferită. Așadar, puteți folosi acest mod de filtrare, utilizând Whitelist (Listă albă), pentru a permite accesul la rețea doar a adreselor MAC eligibile și de încredere.

Parametru	Descriere
Blacklisted Device (Dispozitiv pe lista neagră)	Specificați numele sau orice remarcă considerați pentru dispozitiv.
Whitelisted Device (Dispozitiv inclus pe lista albă)	
MAC Address (Adresă MAC)	Specifică adresele MAC ale dispozitivelor adăugate în listă.
Operation (Operațiune)	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Folosit pentru a adăuga dispozitive noi, mai exact adrese MAC noi, la Whitelist (Lista neagră) sau la Blacklist (Lista albă).</p> </div> </div> <div style="margin-top: 10px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Folosit pentru a elimina dispozitive, mai exact adresele MAC ale acestora, Whitelist (Lista neagră) sau la Blacklist (Lista albă)</p> </div> </div> </div>
Add all online devices to the whitelist (Adăugați toate dispozitivele online la lista albă)	<p>Este disponibil atunci când setați Whitelist (Lista albă) pentru prima dată. Făcând clic pe acest text albastru, Add all online devices to the whitelist (Adăugați toate dispozitivele online la lista albă), puteți adăuga toate dispozitivele conectate în prezent la Whitelist (Lista albă).</p>

10.7.2 Permiteți numai dispozitivului specificat să acceseze internetul

Scenariu: Wi-Fi-ul din casă este folosit neadecvat de dispozitive necunoscute.

Cerințe: Permiteți accesul la internet numai anumitor dispozitive ale membrilor familiei.

Soluție: Puteți configura funcția de filtrare a adresei MAC pentru a atinge cerințele.

Să presupunem că:

Dispozitivul	Adresa MAC	Stare
Propriul telefon	8C: EC:4B:B3:04:92	Conectat
Kid 1's phone	94:C6:91:29:C2:12	Deconectat
Telefonul copilului 2	98:9 C:57:19:D0:1B	Deconectat

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **Advanced Settings (Setări avansate) > Filter MAC Address (Filtru adresă MAC).**
3. Setați **MAC Address Filter Mode (Mod filtrare adresă MAC)** la **Whitelist (Lista albă).**

4. Opțional, introduceți numele dispozitivului în câmpul **Whitelist Device (Dispozitiv Lista albă)**, care este **Kid 1's phone** în acest exemplu.
5. Introduceți **MAC Address (Adresa MAC)** a dispozitivului, care este **94:C6:91:29:C2:12** în acest exemplu.
6. Clic pe **+Add (+Adăugați)**.

Filter MAC Address

MAC Address Filter Mode: Blacklist(To disallow listed devices to access the internet)
 Whitelist(To allow only the listed devices to access the internet)

Whitelisted Device	MAC Address	Operation
<input type="text" value="Kid 1's phone"/>	<input type="text" value="94:C6:91:29:C2:12"/>	<input type="button" value="+ Add"/>
Unknown	8C:EC:4B:B3:04:92	<input type="button" value="🗑"/>

7. Repetați **4** până la **6** pentru a adăuga toate telefoanele la Whitelist (Lista albă).
8. Faceți clic pe **Save (Salvare)**.

Filter MAC Address

MAC Address Filter Mode: Blacklist(To disallow listed devices to access the internet)
 Whitelist(To allow only the listed devices to access the internet)

Whitelisted Device	MAC Address	Operation
<input type="text" value="Kid 2's phone"/>	<input type="text" value="98:9C:57:19:D0:1B"/>	<input type="button" value="+ Add"/>
Kid 1's phone	94:C6:91:29:C2:12	<input type="button" value="🗑"/>
Unknown	8C:EC:4B:B3:04:92	<input type="button" value="🗑"/>

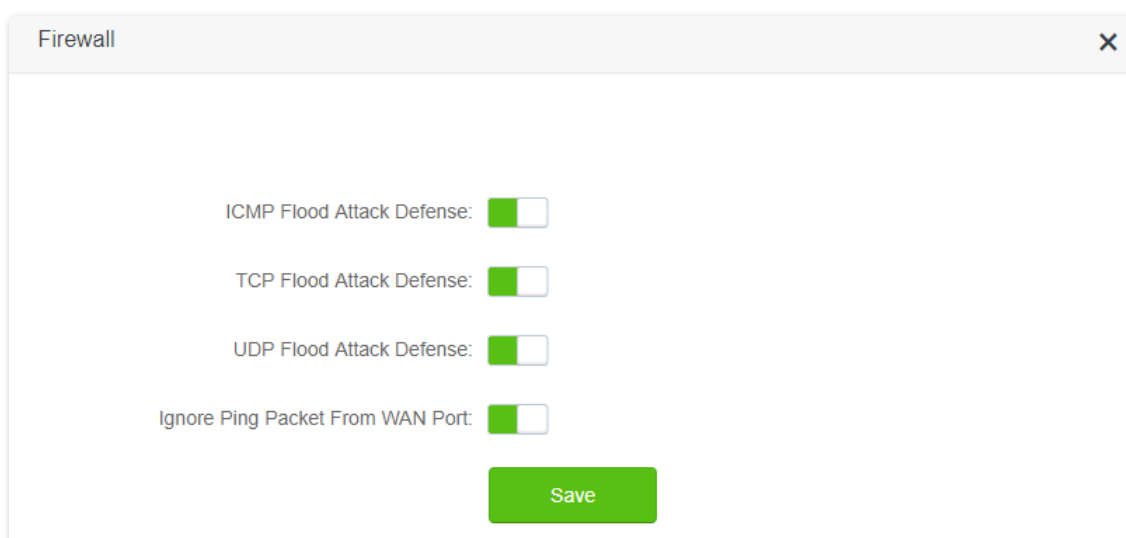
---Sfârșit

Când configurarea este finalizată, doar cele trei dispozitive adăugate pot accesa internetul prin ruter.

10.8 Firewall

Funcția de firewall ajută ruterul să detecteze și să apere împotriva unor atacuri cibernetice de tip ICMP Flood, TCP Flood și UDP Flood și să ignore pachete Ping către WAN. Este recomandat să păstrați setările implicite.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Firewall**.



Descrierea parametrilor

Parametru	Descriere
ICMP Flood Attack Defense (Apărare împotriva atacurilor de tip ICMP Flood)	ICMP flood este un tip de atac de tip Denial of Service (DoS) care folosește protocolul ICMP (Internet Control Message Protocol) pentru a inunda un dispozitiv sau o rețea cu un volum mare de pachete ICMP, în special mesaje Echo Request (cunoscut și ca pachete "ping"). Atacatorul trimite un număr mare de astfel de pachete către o țintă, copleșind resursele dispozitivului sau ale rețelei și făcându-le incapabile să proceseze traficul legitim. Scopul unui ICMP flood este de a satura lățimea de bandă și resursele de procesare ale serverului sau routerului atacat, rezultând într-o performanță scăzută sau chiar întreruperea totală a serviciului. Acest tip de atac este simplu de executat, dar poate fi contracarat prin măsuri de securitate precum filtrarea traficului ICMP sau limitarea ratei de răspuns.

Parametru	Descriere
TCP Flood Attack Defense (Apărare împotriva atacurilor de tip TCP Flood)	TCP flood este un tip de atac Denial of Service (DoS) în care un atacator trimite un volum mare de pachete TCP către un server sau o rețea, cu scopul de a satura resursele acestora și de a le face indisponibile pentru utilizatorii legitimi. Aceste pachete sunt, de obicei, fie pachete de inițializare SYN (într-un atac SYN flood), fie alte tipuri de pachete TCP, care forțează serverul să deschidă și să mențină conexiuni inutile, consumând resursele de procesare și lățimea de bandă. Atacul TCP flood exploatează modul în care funcționează protocolul TCP, care necesită stabilirea unei conexiuni în trei pași (handshake). Atacatorul trimite o cantitate mare de cereri de conexiune (SYN), dar nu finalizează handshake-ul, lăsând serverul să aștepte finalizarea fiecărei conexiuni. Acest lucru duce la un consum excesiv de resurse, afectând performanța ruterului sau serverelor din rețea și provocând întreruperea serviciului.
UDP Flood Attack Defense (Apărare împotriva atacurilor de tip UDP Flood)	UDP flood este un tip de atac Denial of Service (DoS) în care un atacator trimite un volum mare de pachete UDP (User Datagram Protocol) către o țintă, cum ar fi un server sau o rețea, cu scopul de a satura resursele și de a le face indisponibile pentru utilizatorii legitimi. Deoarece protocolul UDP este nesecurizat și nu necesită stabilirea unei conexiuni, acest tip de atac este deosebit de eficient în inundarea rețelei sau a serverului cu trafic inutil. Într-un atac UDP flood, serverul țintă încearcă să proceseze și să răspundă pachetelor UDP, dar datorită numărului mare de pachete primite, poate deveni suprasolicitat și incapabil să răspundă traficului legitim. Deoarece UDP nu are un mecanism de verificare a conexiunilor, serverul trebuie să trateze fiecare pachet ca o solicitare validă, consumând astfel resursele rețelei și lățimea de bandă.
Ignore Ping Packet From WAN Port (Ignorare pachete pe WAN)	Când este activat, ruterul ignoră automat ping-ul către WAN-ul său de la gazdele de pe internet și se împiedică să fie expus, prevenind în același timp atacurile ping externe.

10.9 Actualizare ISP

Pe această pagină, **ISP Update (Actualizare ISP)**, puteți actualiza informațiile ISP pentru a obține o experiență mai bună de utilizare. Când apare problema de compatibilitate a ISP-ului sau nepotrivirea APN-ului la introducerea unei cartele SIM, puteți încerca să utilizați această funcție pentru a rezolva problema.

De reținut faptul că puteți seta manual un APN, dacă APN-ul nu este configurat automat la introducerea unei cartele SIM. Setarea APN-ului se face în Internet Settings (Setări Internet). Pentru crearea unui APN citiți [secțiunea 4.1.2](#).

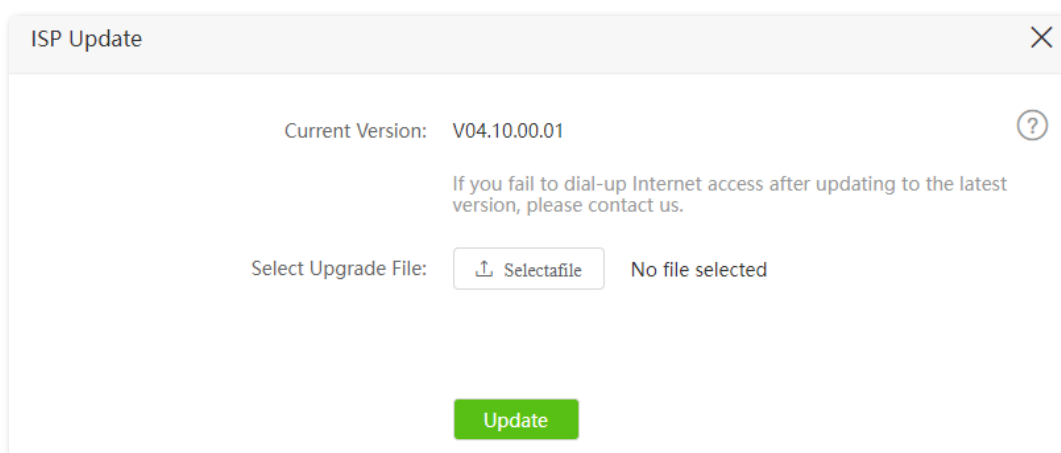


Pentru a preveni deteriorarea ruterului:

- Asigurați-vă că fișierul de actualizare este aplicabil ruterului.
- Când actualizați informațiile ISP, nu opriți ruterul.

Procedura de configurare:

1. Accesați www.tendacn.com/ro și căutați modelul de echipament. Apoi accesați secțiunea Services (Servicii) sau Download (Descărcări) și descărcați un fișier cu denumirea „IPS Update”. **Citiți cu atenție notele aferente fișierului.** Descărcați fișierul și dezarhivați-l.
2. [Conectați-vă la interfața web a ruterului.](#)
3. Navigați la **Advanced Settings (Setări avansate) > ISP Update (Actualizare ISP).**
4. Faceți clic pe **Select a file (Selectare fișier)**. Selectați și încărcați fișierul de actualizare care a fost descărcat la pasul 1 și faceți clic pe **Update (Actualizare)**.



---Sfârșit

Așteptați un moment până când procesul în curs se termină. Conectați-vă din nou la interfața web a ruterului și verificați dacă actualizarea a avut succes pe baza informației de la câmpul **Current Version (Versiune curentă)** de pe pagina de meniu **ISP Update (Actualizare ISP)**.

10.10 Rutare statică



10.10.1 Prezentare generală

Rutarea statică pe un router Tenda permite configurarea manuală a unor rute fixe pentru direcționarea traficului de rețea către anumite destinații IP. Aceasta înseamnă că administratorul rețelei introduce manual adresele IP ale rețelelor de destinație și gateway-urile prin care traficul trebuie direcționat, fără a utiliza un protocol dinamic de rutare, cum ar fi RIP sau OSPF. Rutarea statică este utilă în rețele mici sau în cazuri unde administratorul dorește să aibă un control strict asupra căilor de comunicație între rețele. Deși mai puțin flexibilă decât rutarea dinamică, este mai sigură și nu consumă resurse pentru calcularea constantă a rutelor optime.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Static Route (Rutare statică)**.

Destination Network	Subnet Mask	Gateway	Port	Operation
<input type="text"/>	<input type="text"/>	<input type="text"/>	WAN	+ Add
0.0.0.0	0.0.0.0	192.168.96.1	WAN1	System
192.168.0.0	255.255.255.0	0.0.0.0	br0	System
192.168.96.0	255.255.255.0	0.0.0.0	WAN1	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System

Descrierea parametrilor

Parametru	Descriere
Destination Network (Rețeaua de destinație)	<p>Specifică adresa IP a rețelei de destinație.</p> <p>Când Rețeaua de destinație și Masca de subrețea sunt ambele 0.0.0.0, aceasta indică faptul că aceasta este ruta implicită.</p> <p> TIP</p>
Subnet Mask (Masca de subrețea)	<p>Când ruta pachetelor nu poate fi găsită în tabelul de rutare, ruterul va redirecționa pachetele folosind ruta implicită.</p> <p>Specifică masca de subrețea a rețelei de destinație.</p>
Gateway (Gateway)	<p>Specifică adresa IP a următorului hop, care poate fi un alt ruter, switch, nod, gateway, după ce pachetul de date iese din interfața ruterului.</p> <p>0.0.0.0 indică faptul că rețeaua de destinație este conectată direct la ruter.</p>
WAN	<p>Specifică interfața din care iese pachetul.</p>
Operation (Operațiune)	<p><input type="button" value="+ Add"/> : folosit pentru a adăuga o regulă de rută statică.</p> <p> : folosit pentru a șterge o regulă de rută statică.</p>

10.10.2 Adăugați o regulă de rutare statică

Scenariu: Aveți un ruter Tenda 4G09 și alte două rutere. *Router1* este conectat la internet și serverul său DHCP este activat. *Router2* este conectat la un intranet și serverul său DHCP este dezactivat.

Cerințe: Doriți a accesa atât internetul, cât și intranetul în același timp.

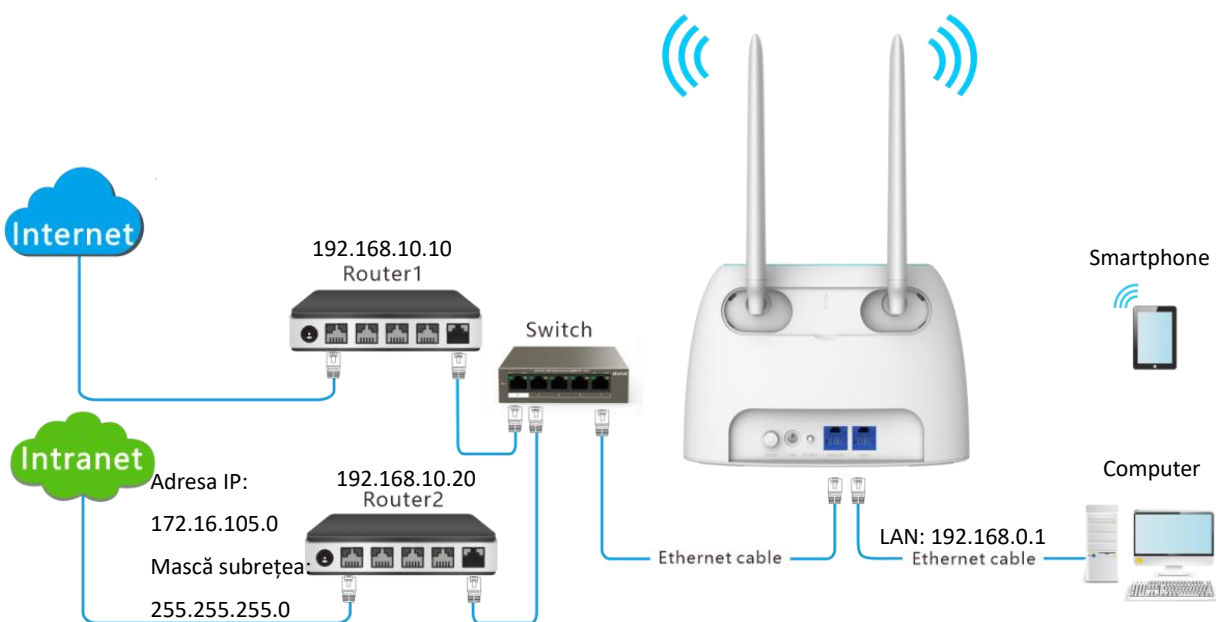
Soluție: Puteți configura funcția de rută statică pentru a îndeplini cerințele.

Să presupunem că adresele IP LAN (rețea locală), clasă C privată (locală), ale acestor dispozitive sunt:

- 4G09: 192.168.0.1
- Router1: 192.168.10.10
- Router2: 192.168.10.20

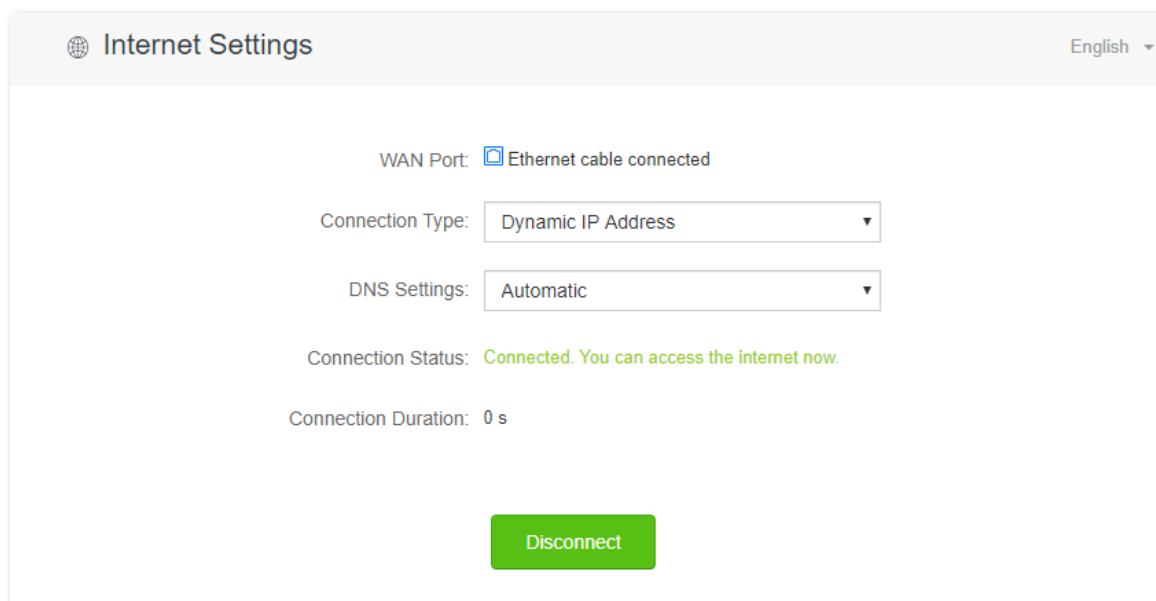
Informațiile despre intranet:

- Adresa IP clasă B, privată (locală): 172.16.105.0
- Mască de subrețea: 255.255.255.0



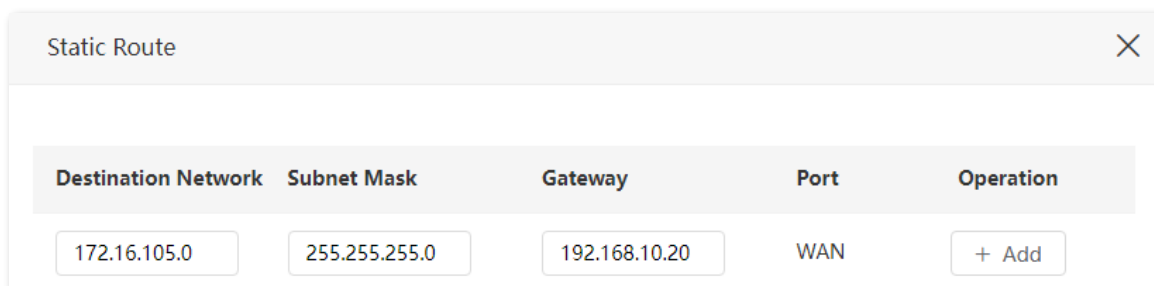
Procedura de configurare:

1. [Conectati-vă la interfața web a ruterului.](#)
2. Consultați secțiunea din acest manual [Acces la internet cu o adresă IP dinamică](#) pentru a configura accesul la internet.



3. Adăugați o regulă de rută statică.

- 1) Navigați la **Advanced Settings (Setări avansate) > Static Route (Rutare statică)**.
- 2) Introduceți adresa IP a rețelei de destinație, care este **172.16.105.0** în acest exemplu.
- 3) Introduceți masca de subrețea a rețelei de destinație, care este **255.255.255.0** în acest exemplu.
- 4) Introduceți adresa IP de intrare a următorului *hop*, care este **192.168.10.20** în acest exemplu.
- 5) Clic **+Add (+ Adăugați)**.



---Sfârșit

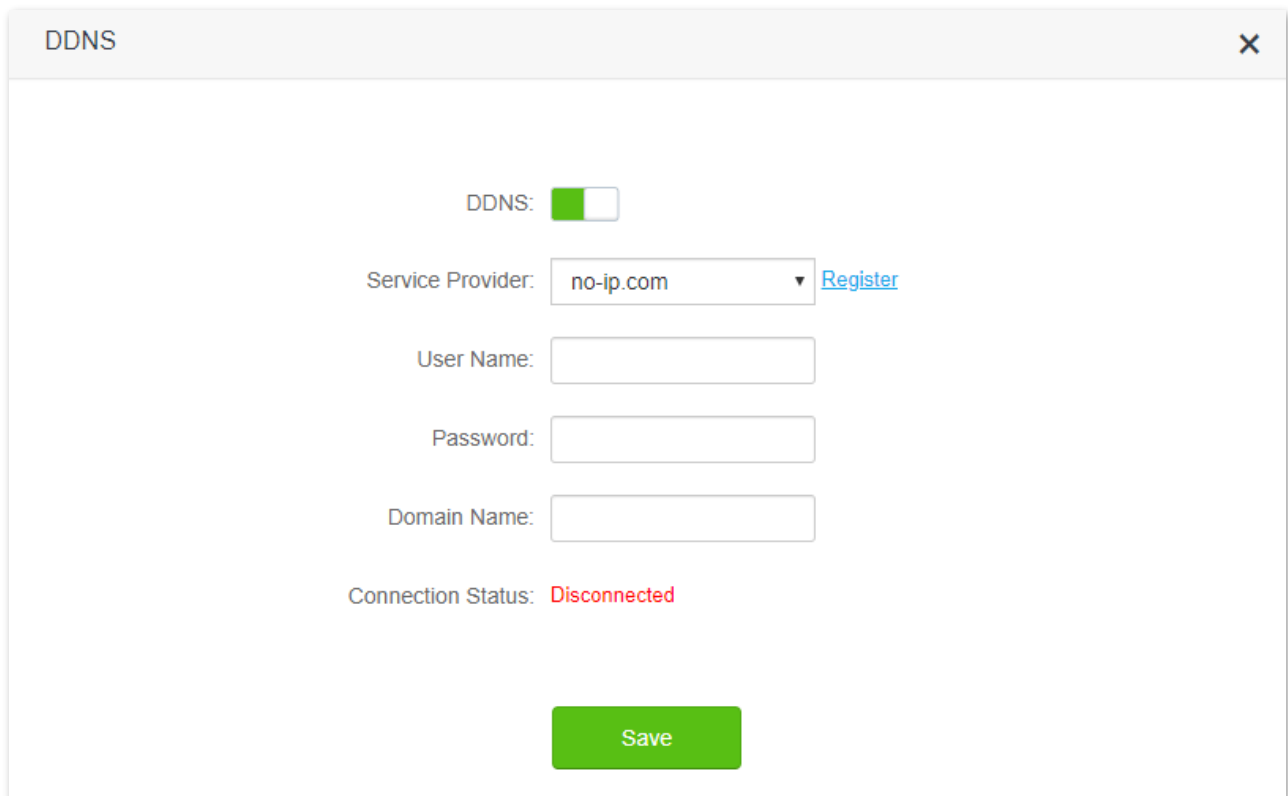
Când configurarea este finalizată, puteți accesa atât internetul, cât și intranetul prin 4G09 în același timp.

10.11 DDNS

10.11.1 Prezentare generală

DDNS (Dynamic Domain Name System) este un serviciu care actualizează automat și în timp real înregistrările DNS ale unui domeniu atunci când adresa IP publică a dispozitivului sau rețelei se schimbă. Acest lucru este util în special pentru utilizatorii cu conexiuni de internet care au adrese IP dinamice, adică IP-ul public al ruterului lor se schimbă periodic. În mod obișnuit, DNS leagă un nume de domeniu de o adresă IP fixă. În cazul DDNS, dacă adresa IP a ruterului sau serverului se schimbă, serviciul DDNS actualizează înregistrările DNS astfel încât domeniul să fie întotdeauna asociat cu adresa IP corectă. Acest lucru permite accesul continuu la servere de acasă, camere IP, sau alte dispozitive care necesită o conexiune constantă, chiar și atunci când IP-ul public se schimbă.

Pentru a accesa pagina de meniu **DDNS**, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > DDNS**.



The screenshot shows a web interface window titled "DDNS" with a close button (X) in the top right corner. The main content area contains the following elements:

- A toggle switch labeled "DDNS:" which is currently turned on (green).
- A "Service Provider:" dropdown menu showing "no-ip.com" with a "Register" link to its right.
- Input fields for "User Name:", "Password:", and "Domain Name:".
- A "Connection Status:" label with the text "Disconnected" in red.
- A green "Save" button at the bottom center.

Descrierea parametrilor

Parametru	Descriere
DDNS	Folosit pentru a activa sau dezactiva funcția DDNS.
Service Provider (Furnizor de servicii)	Selectați unul dintre furnizorii de servicii DDNS predefiniți. Puteți apăsa textul albastru Register (înregistrare) pentru a vă crea un cont pe site-ul furnizorului de servicii DDNS.
User Name (Nume de utilizator)	Specificați numele de utilizator și parola înregistrate pe site-ul web al unui furnizor de servicii DDNS pentru a vă conecta la serviciul DDNS.
Password (Parolă)	
Domain Name (Nume de domeniu)	Specificați numele de domeniu înregistrat pe site-ul furnizorului de servicii DDNS. Dacă acest câmp este vizibil după ce a fost ales un anume furnizor de servicii, atunci nu este necesară introducerea unui domeniu.
Connection Status (Starea conexiunii)	Specifică starea curentă a conexiunii a serviciului DDNS.

10.11.2 Accesarea de pe internet a unui server din rețeaua locală folosind un nume de domeniu

Scenariu: Ați configurat un server FTP pe un server din rețeaua locală (LAN).

Cerințe: Doriți să permiteți accesul de pe internet la serverul serverul FTP pentru membrii familiei care nu sunt acasă.

Soluție: Puteți configura funcțiile din meniul **DDNS** plus redirectionarea unui port TCP din meniul **Virtual Server (Server virtual)** pentru a atinge cerințele.

Să presupunem că informațiile serverului FTP sunt:

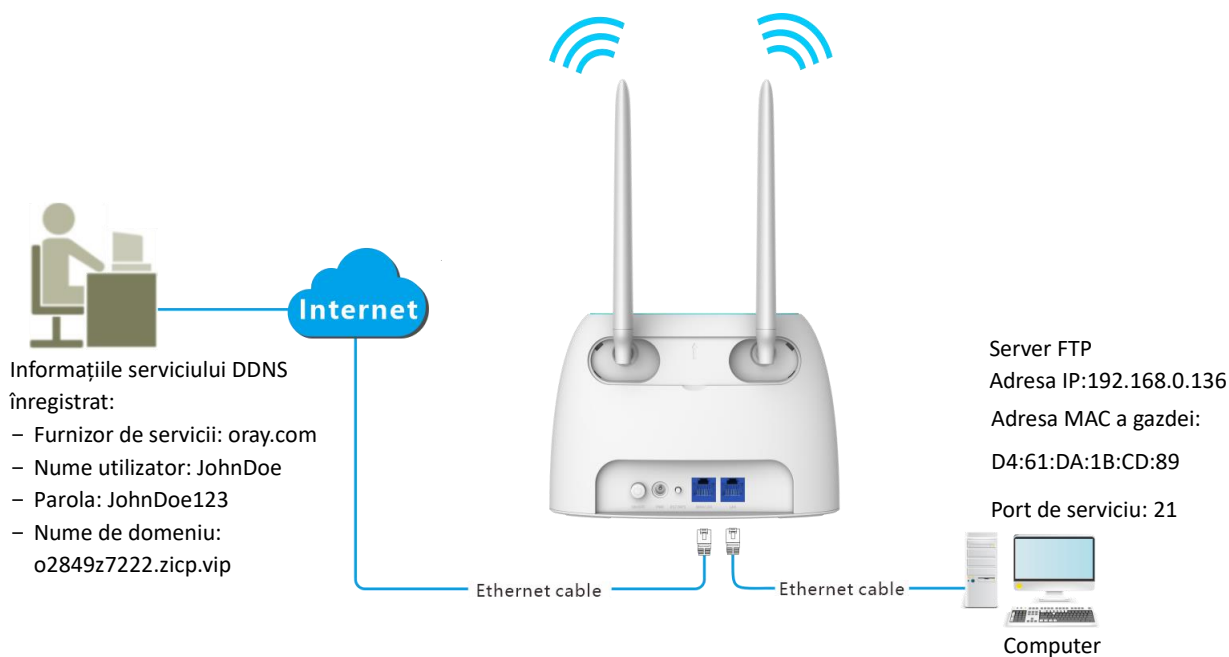
- Adresa IP din rețeaua locală: 192.168.0.136
- Adresa MAC a gazdei: D 4:61:DA:1B:CD:89
- Port TCP pentru serviciul FTP: 21

Informațiile despre serviciul DDNS înregistrat:

- Furnizor de servicii: oray.com
- Nume utilizator: JohnDoe
- Parola: JohnDoe123
- Nume de domeniu: o2849z7222.zicp.vip

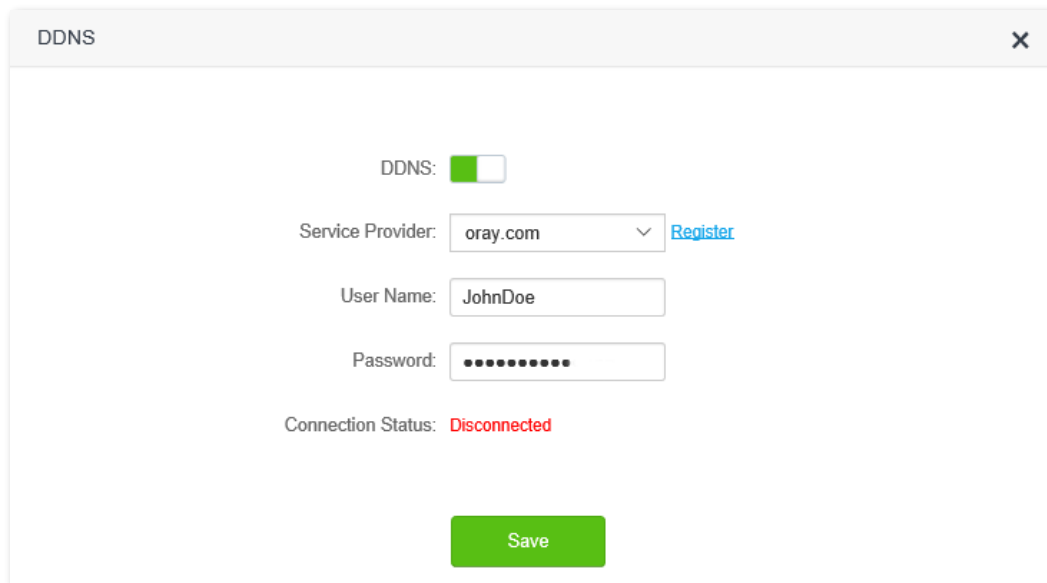


Vă rugăm să vă asigurați că ruterul obține o adresă IP publică. Pentru a afla care e adresa IP publică puteți accesa <https://whatismyipaddress.com/> de pe un dispozitiv conectat la ruterul Tenda. Este posibil ca această funcție să nu funcționeze pe o gazdă cu o adresă IP a unei rețele private sau o adresă IP intranet atribuită de ISP-uri care încep cu 100. Adresele IPv4 comune sunt clasificate în clasa A, clasa B și clasa C. Adresele IP private ale clasa A variază de la 10.0.0.0 la 10.255.255.255. Adresele IP private din clasa B variază între 172.16.0.0-172.31.255.255. Adresele IP private din clasa C variază de la 192.168.0.0-192.168.255.255.



Procedura de configurare:

1. [Conectati-vă la interfața web de gestionare a ruterului.](#)
2. Configurați funcția DDNS.
 - 1) Navigați la **Advanced Settings (Setări avansate) > DDNS.**
 - 2) Activați funcția **DDNS.**
 - 3) Alegeți un furnizor de servicii, care este **oray.com** în acest exemplu.
 - 4) Introduceți numele de utilizator și parola, care sunt **JohnDoe** și **JohnDoe123** în acest exemplu.
 - 5) Faceți clic pe **Save (Salvare).**

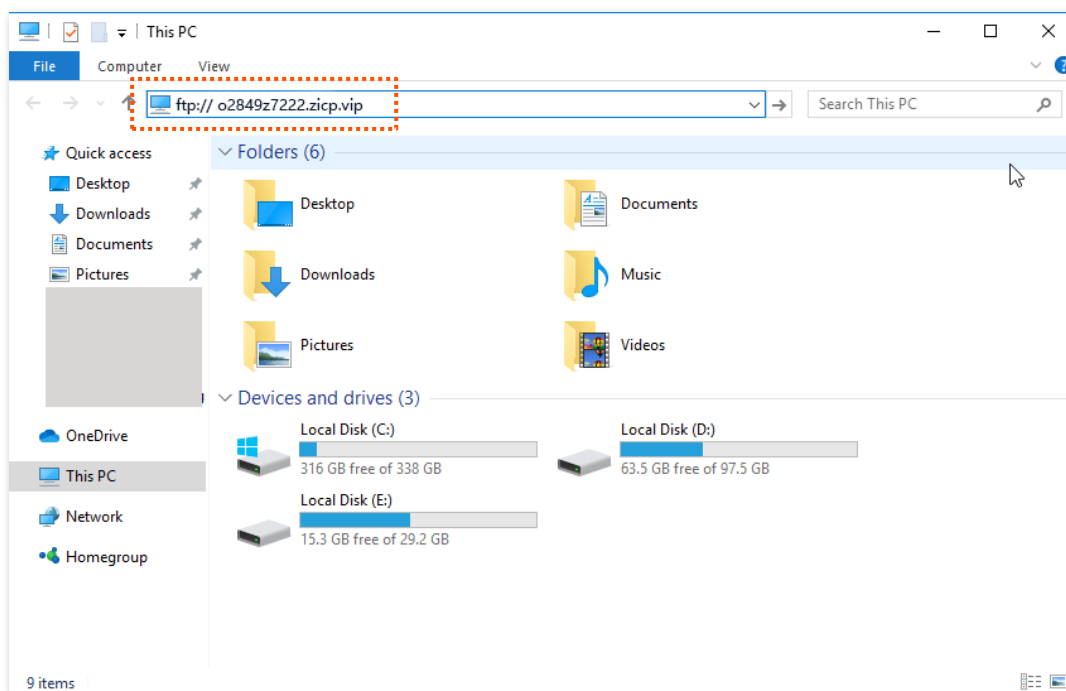


Așteptați un moment. Când starea conexiunii devine **Connected (Conectată)**, configurațiile reușesc.

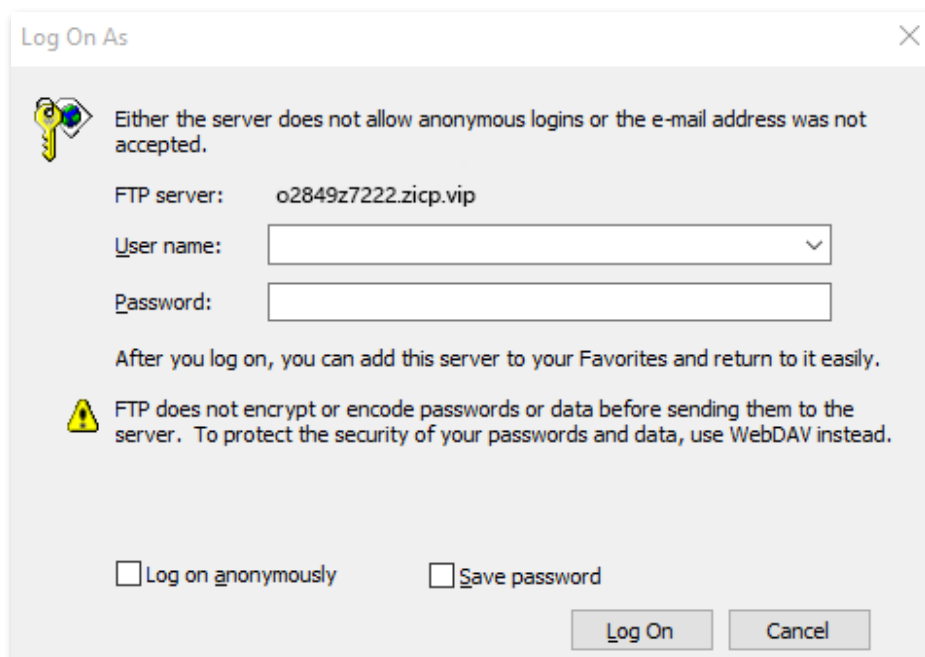
3. Apoi trebuie să configurați redirecționarea portului 21 pe TCP de la și către IP-ul local al serverului FTP și IP-ul public al ruterului. Această redirecționare se face în meniul **Virtual Server (Server virtual)**, consultați secțiunea din acest manual [Redirecționare porturi TCP și UDP](#).

---Sfârșit

Când configurarea este finalizată, utilizatorii de pe internet pot accesa serverul FTP vizitând „Nume protocol al stratului aplicației serviciului intranet://numele domeniului:numărul portului TCP pe WAN”, de exemplu, adresa **ftp://o2849z7222.zicp.vip:21**.



Introduceți numele de utilizator și parola pentru a accesa resursele de pe serverul FTP.



După configurații, dacă utilizatorii de internet tot nu pot accesa serverul FTP, încercați următoarele metode:

- Asigurați-vă că ați configurat redirectionarea portului 21 pe TCP de la și către IP-ul local al serverului FTP și IP-ul public al ruterului. Această redirectionare se face în meniul **Virtual Server (Server virtual)**.
- Configurați corespunzător sau chiar închideți firewall-ul, antivirusul și alți agenți de securitate pe gazda serverului FTP și încercați din nou.

10.12 Redirecționare porturi TCP și UDP din meniul Server virtual

10.12.1 Prezentare generală

În meniul **Virtual Server (Server virtual)** se permite redirecționarea porturilor TCP/UDP. Astfel, se permite direcționarea traficului din exterior (internet) către un anumit dispozitiv din rețeaua locală (LAN) pe baza unui port virtual, fie că este pe TCP sau UDP, specific. Aceasta este utilizată, de exemplu, pentru a permite accesul extern la un server web, o cameră de supraveghere IP sau o aplicație de gaming care rulează în rețeaua de acasă. TCP și UDP sunt protocoalele utilizate pentru stabilirea conexiunilor și transferul datelor între dispozitivele conectate. TCP (Transmission Control Protocol) e un protocol orientat pe conexiune care asigură livrarea corectă a datelor, verificând fiecare pachet și retransmițându-l dacă este pierdut și este utilizat în aplicații unde integritatea datelor este critică, cum ar fi navigarea web și transferurile de fișiere. UDP (User Datagram

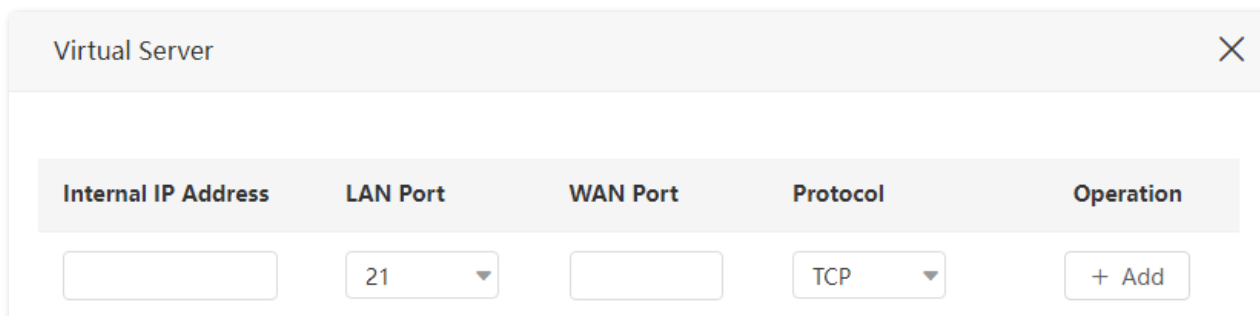
Protocol) este un protocol care trimite datele fără confirmarea de primire și este folosit acolo unde viteza este mai importantă decât acuratețea, cum ar fi streamingul video, VoIP și gaming online.

Porturile sunt numerotate de la 0 la 65535 și sunt împărțite, în general, în trei mari categorii:

- **Porturi bine cunoscute (Well-Known Ports)** cu intervalul 0 – 1023 și sunt rezervate pentru protocoale și servicii de bază, precum porturile 80 (HTTP), 443 (HTTPS), 25 (SMTP pentru trimiterea e-mailurilor), 21 (FTP File Transfer Protocol) etc.
- **Porturi înregistrate (Registered Ports)** cu intervalul 1024 – 49151 și sunt utilizate de aplicațiile și serviciile care necesită un port specific pentru comunicare, dar care nu fac parte din protocoalele de bază ale internetului, precum porturile 3306 (MySQL), 8080 (HTTP alternativ), 3389 (Remote Desktop Protocol) etc.
- **Porturi dinamice sau private (Dynamic/Private Ports)** cu interval 49152 – 65535 și sunt folosite de aplicații pentru sesiuni temporare, când nu este necesar un port dedicat permanent.



Pentru a accesa pagina, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Virtual Server (Server virtual)**.

În mod implicit nu există nicio regulă în listă. Toate regulile create aici se aplică pentru ambele conexiuni la internet, rețea externă, fie prin date mobile, fie prin cablu Ethernet.



Internal IP Address	LAN Port	WAN Port	Protocol	Operation
<input type="text"/>	21	<input type="text"/>	TCP	+ Add

Descrierea parametrului

Parametru	Descriere
Internal IP Address (Adresă IP internă)	Specifică adresa IP a serverului din rețeaua locală (LAN) a ruterului.
LAN Port (Port LAN)	Specifică numărul portului TCP/UDP al serverului din rețeaua locală (LAN). Puteți fie să alegeți un număr de port de serviciu în caseta derulantă, fie să introduceți manual un număr de port de serviciu. LAN Port (Port LAN) poate fi diferit de WAN Port (Port WAN) .
WAN Port (Port WAN)	Specifică portul TCP/UDP public, de pe ieșirea WAN (externă, publică) a ruterului. WAN nu se referă la portul RJ-45 WAN de pe ruter, ci la conexiunea externă, la internet, fie că este prin date mobile, fie că este prin cablu Ethernet prin portul RJ-45 WAN. LAN Port (Port LAN) poate fi diferit de WAN Port (Port WAN) .
Protocol	Specifică protocolul nivelului de transport al serviciului TCP , UDP sau TCP&UDP . Dacă nu sunteți sigur de acest parametru, se recomandă TCP&UDP .
Operation (Operațiune)	Operațiunile disponibile includ:  : folosit pentru a adăuga o nouă regulă de redirectionare de porturi.  : folosit pentru a șterge o regulă din listă.

10.12.2 Permitearea accesării unui server FTP din rețeaua locală de către utilizatori de pe internet

Scenariu: Ați configurat un server FTP pe un server din rețeaua locală (LAN).

Cerințe: Doriți ca fișierele de pe serverul FTP să fie accesate de către utilizatori de pe internet și astfel să permiteți membrilor familiei care nu sunt acasă să acceseze resursele serverului FTP de oriunde.

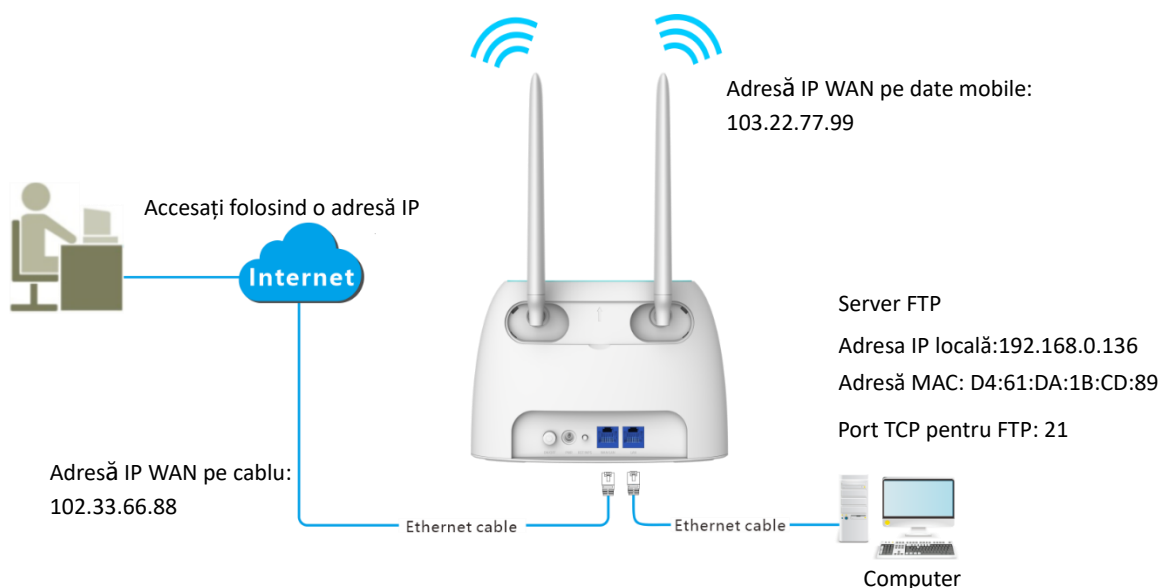
Soluție: Puteți configura o redirectionare a unui port TCP în meniul **Virtual Server (Server virtual)** dar și atribuirea unui IP fix pentru serverul FTP din rețeaua locală, în meniul **DHCP Reservation (Rezervare DHCP)**.

Să presupunem că informațiile serverului FTP includ:

- Adresa IP din rețeaua locală: 192.168.0.136
- Adresă MAC: D4:61:DA:1B:CD:89
- Port TCP server FTP: 21
- Adresele IP WAN (publice) pentru ruter: 102.33.66.88 pe cablu și 103.22.77.99 pe date mobile.



- Vă rugăm să vă asigurați că ruterul obține o adresă IP publică. Este posibil ca această funcție să nu funcționeze pe o gazdă cu o adresă IP a unei rețele private sau o adresă IP intranet atribuită de ISP-uri care încep cu 100. Adresele IPv4 comune sunt clasificate în clasa A, clasa B și clasa C. Adresele IP private ale clasa A variază de la 10.0.0.0 la 10.255.255.255. Adresele IP private din clasa B variază între 172.16.0.0-172.31.255.255. Adresele IP private din clasa C variază de la 192.168.0.0-192.168.255.255.
- ISP-urile pot bloca accesarea serviciilor web neraportate cu portul implicit 80. Prin urmare, atunci când numărul implicit al portului LAN este 80, vă rugăm să îl schimbați manual cu un număr de port neobișnuit (1024-65535), cum ar fi 9999.
- **LAN Port (Port LAN)** poate fi diferit de **WAN Port (Port WAN)**.

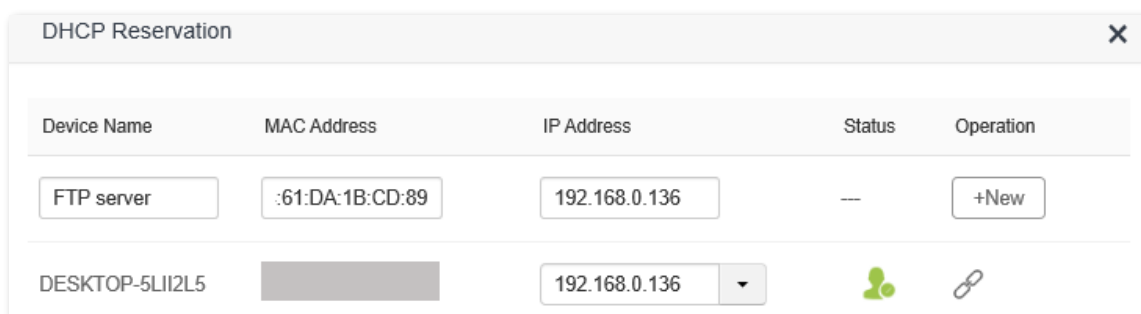


Procedura de configurare:

1. [Conectati-vă la interfața web de gestionare a ruterului.](#)
2. Pentru a adăuga regula de redirecționare a portului 21:
 - 1) Navigați la **Advanced Settings (Setări avansate) > Virtual Server (Server virtual)**.
 - 2) Introduceți **Internal IP Address (Adresa IP internă)**, care este **192.168.0.136** în acest exemplu.
 - 3) Alegeți un **LAN Port (Port LAN)** din caseta derulantă, care este **21** în acest exemplu.
 - 4) Alegeți un protocol, care este **TCP&UDP** în acest exemplu.
 - 5) Faceți clic pe **+New (+Nou)**.

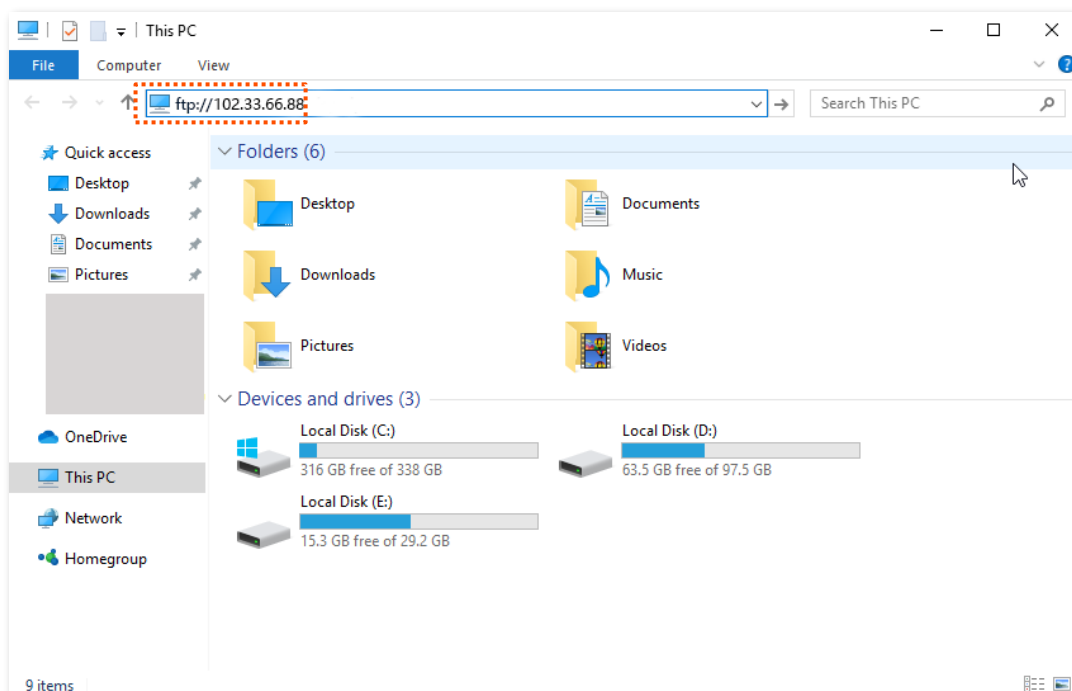
Internal IP Address	LAN Port	WAN Port	Protocol	Operation
192.168.0.136	21	21	TCP&UDP	+New

3. Atribuiți o adresă IP fixă gazdei unde se află serviciul FTP.
 - 1) Navigați la **System Settings (Setări sistem) > DHCP Reservation (Rezervare DHCP)**.
 - 2) Tastați o denumire sau orice remarcă în câmpul **Device Name (Nume dispozitiv)** pentru gazda serviciului FTP, care este **FTP server** în acest exemplu.
 - 3) Introduceți adresa MAC a adaptorului de rețea a gazdei serviciului FTP în câmpul **MAC Address (Adresă MAC)**, care este **D4: 61:DA:1B:CD:89** în acest exemplu.
 - 4) Introduceți o adresă IP la câmpul **IP Address (Adresă IP)** aferent gazdei serviciului FTP, care este **192.168.0.136** în acest exemplu.
 - 5) Faceți clic pe **+New (+Nou)**.

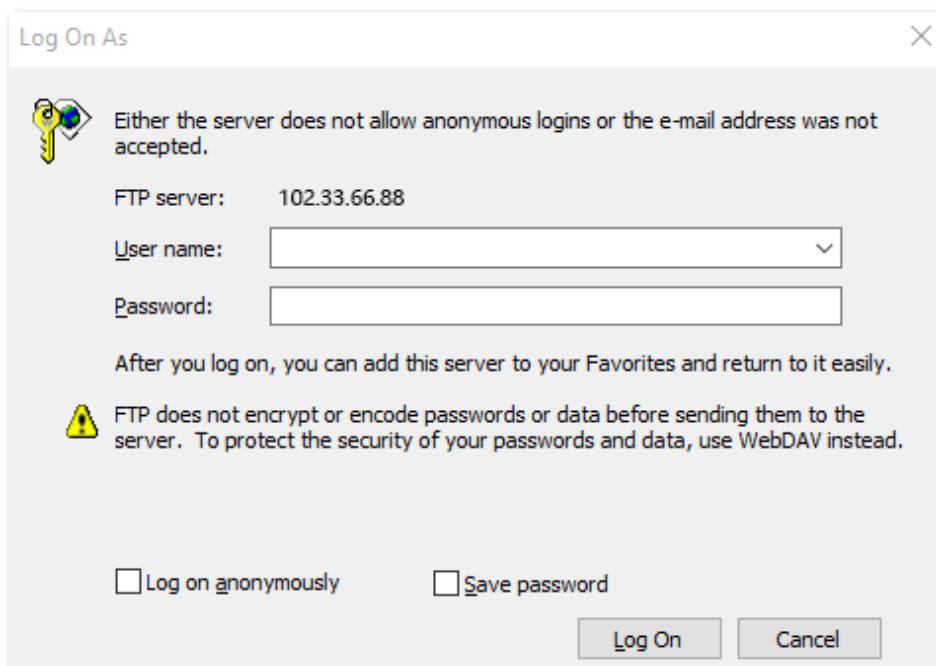


---Sfârșit

Când configurarea este finalizată, utilizatorii de pe internet pot accesa serverul FTP accesând „Nume protocolul stratului aplicației serviciului intranet://adresa IP WAN a routerului:numărul portului WAN”. În acest exemplu, adresa este **ftp://102.33.66.88:21**, însă se poate accesa și prin IP-ul public prin date mobile, anume **ftp://103.22.77.99:21**. Puteți găsi adresa IP WAN a ruterului în secțiunea din manual [Vizualizare informații despre sistem](#).



Apoi, introduceți numele de utilizator și parola pentru a accesa resursele de pe serverul FTP. Aceste credențiale au fost create în prealabil pe serverul FTP.



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 102.33.66.88

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

Log on anonymously Save password

Log On Cancel

Dacă doriți să accesați serverul folosind un nume de domeniu, în loc de un IP, consultați secțiunea din manual [Accesarea de pe internet a unui server din rețeaua locală folosind un nume de domeniu](#).



După configurații, dacă utilizatorii de internet tot nu pot accesa serverul FTP, încercați următoarele metode:

- Asigurați-vă că numărul portului LAN configurat în funcția de Virtual Server (Server virtual) este același cu numărul portului de serviciu setat pe server.
- Configurați corespunzător sau chiar închideți firewall-ul, antivirusul și alți agenți de securitate pe gazda serverului FTP și încercați din nou.

10.13 DMZ

10.13.1 Prezentare generală

O gazdă DMZ pe o rețea LAN nu are restricții în comunicarea cu internetul. Este util pentru a obține o experiență mai bună și mai fluidă în conferințe video și jocuri online. De asemenea, puteți seta gazda unui server din LAN ca gazdă DMZ atunci când aveți nevoie să accesați serverul de pe internet.



- O gazdă DMZ nu este protejată de firewall-ul ruterului. Un hacker poate folosi gazda DMZ pentru a vă ataca rețeaua locală. Prin urmare, activați funcția DMZ numai atunci când este necesar.
- Software-ul antivirus și firewall-ul de pe sistemul de operare al computerului pot cauza unele blocări ale funcției. Configurați-le corespunzător sau dezactivați-le când utilizați funcția DMZ.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > DMZ Host (Gazdă DMZ)**.

DMZ Host

DMZ Host:

DMZ Host IP Address: 192.168.0.

Save

Descrierea parametrului

Parametru	Descriere
DMZ Host (Gazdă DMZ)	Folosit pentru a activa sau dezactiva funcția DMZ.
DMZ Host IP Address (Adresa IP a gazdei DMZ)	Specifică adresa IP a gazdei care urmează să fie setată ca gazdă DMZ.

10.13.2 Permiteți utilizatorilor de internet să acceseze resursele LAN

Scenariu: Ați configurat un server FTP în rețeaua locală (LAN).

Cerințe: Doriți să deschideți serverul FTP pentru utilizatorii de internet și să permiteți membrilor familiei care nu sunt acasă să acceseze resursele serverului FTP de pe internet.

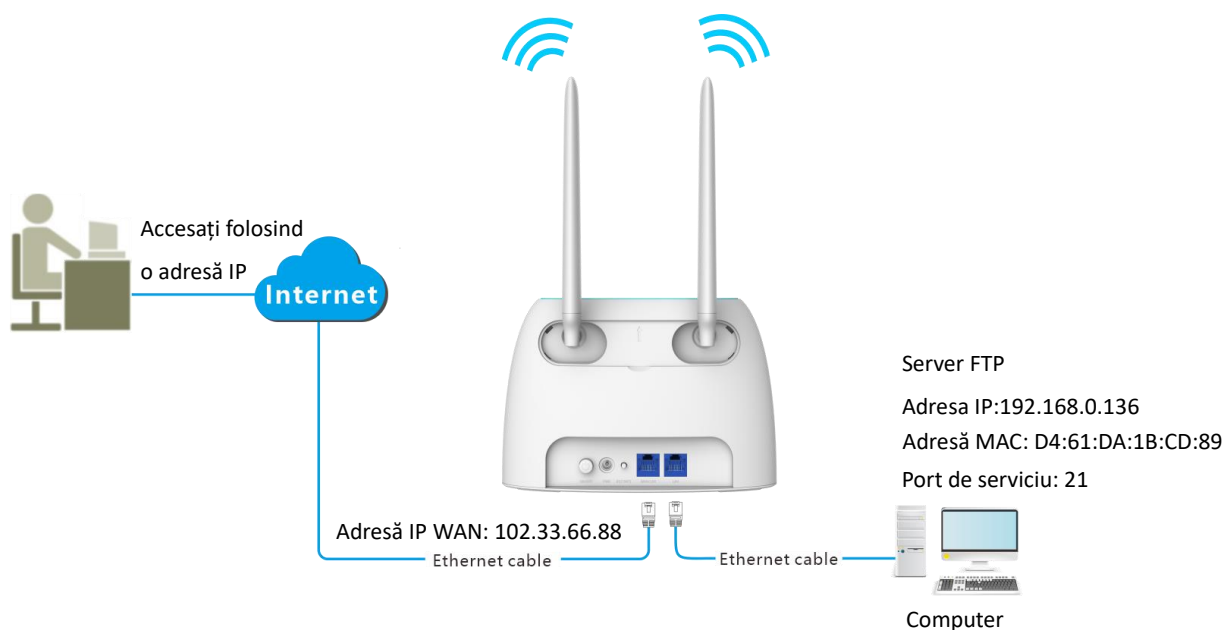
Soluție: Puteți configura funcția gazdă DMZ și apoi atribui o adresă fixă gazdei serverului FTP pentru a îndeplini cerințele.

Să presupunem că informațiile serverului FTP includ:

- Adresa IP: 192.168.0.136
- Adresă MAC: D 4:61:DA:1B:CD:89
- Port TCP pentru serverul FTP: 21
- Adresa WAN a ruterului: 102.33.66.88.



Vă rugăm să vă asigurați că ruterul obține o adresă IP publică. Este posibil ca această funcție să nu funcționeze pe o gazdă cu o adresă IP a unei rețele private sau o adresă IP intranet atribuită de ISP-uri care încep cu 100. Adresele IPv4 comune sunt clasificate în clasa A, clasa B și clasa C. Adresele IP private ale clasa A variază de la 10.0.0.0 la 10.255.255.255. Adresele IP private din clasa B variază între 172.16.0.0-172.31.255.255. Adresele IP private din clasa C variază de la 192.168.0.0-192.168.255.255.



Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Setati funcția **DMZ Host (Gazdă DMZ)**.
 - 1) Navigați la **Advanced Settings (Setări avansate) > DMZ Host (Gazdă DMZ)**.
 - 2) Activați **DMZ Host (Gazdă DMZ)**.

- 3) Introduceți adresa IP a gazdei, care este **192.168.0.136** în acest exemplu.
- 4) Faceți clic pe **Save (Salvare)**.

3. Atribuiți o adresă IP fixă gazdei unde se află serverul FTP.
- 1) Navigați la **System Settings (Setări sistem) > DHCP Reservation (Rezervare DHCP)**.
 - 2) Introduceți o denumire la **Device Name (Nume de dispozitiv)**, care este **FTP server** în acest exemplu.
 - 3) Introduceți MAC-ul adaptorului de rețea a gazdei unde se află serverul FTP în câmpul **MAC Address (Adresa MAC)**, care este **D4: 61:DA:1B:CD:89** în acest exemplu.
 - 4) Introduceți adresa IP rezervată pentru gazda serverului, care este **192.168.0.136** în acest exemplu.
 - 5) Faceți clic pe **+New (+Nou)**.

Device Name	MAC Address	IP Address	Status	Operation
FTP server	61:DA:1B:CD:89	192.168.0.136	--	+New
DESKTOP-5LII2L5		192.168.0.136		

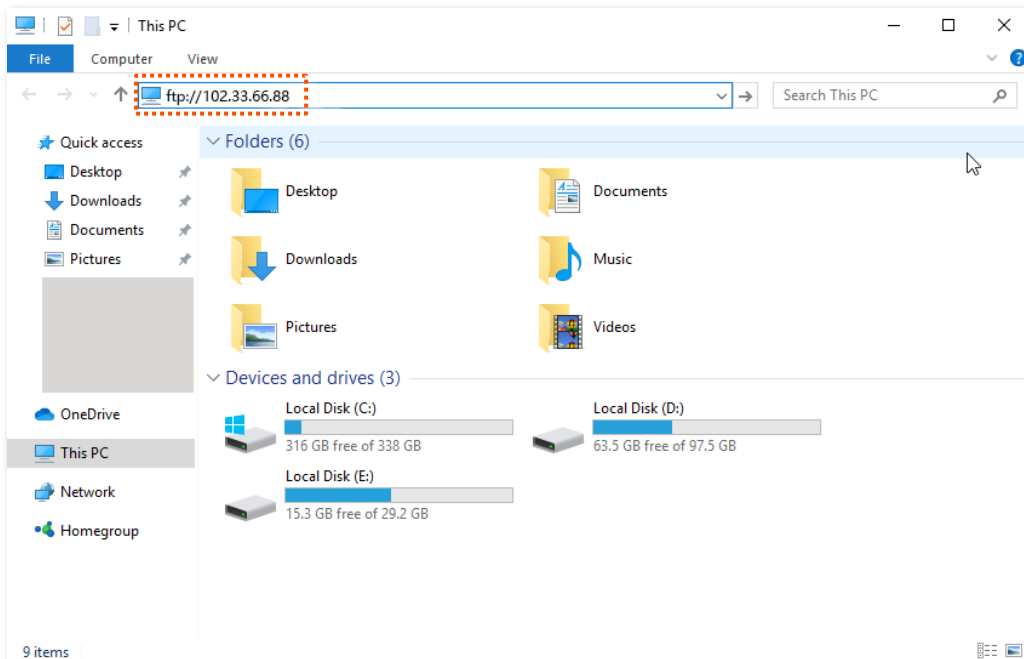
----Sfârșit

Când configurațiile sunt finalizate, utilizatorii de pe internet pot accesa gazda DMZ vizitând „Nume protocolul stratului aplicației serviciului://Adresa IP WAN a routerului:numărul portului serviciului intranet”.

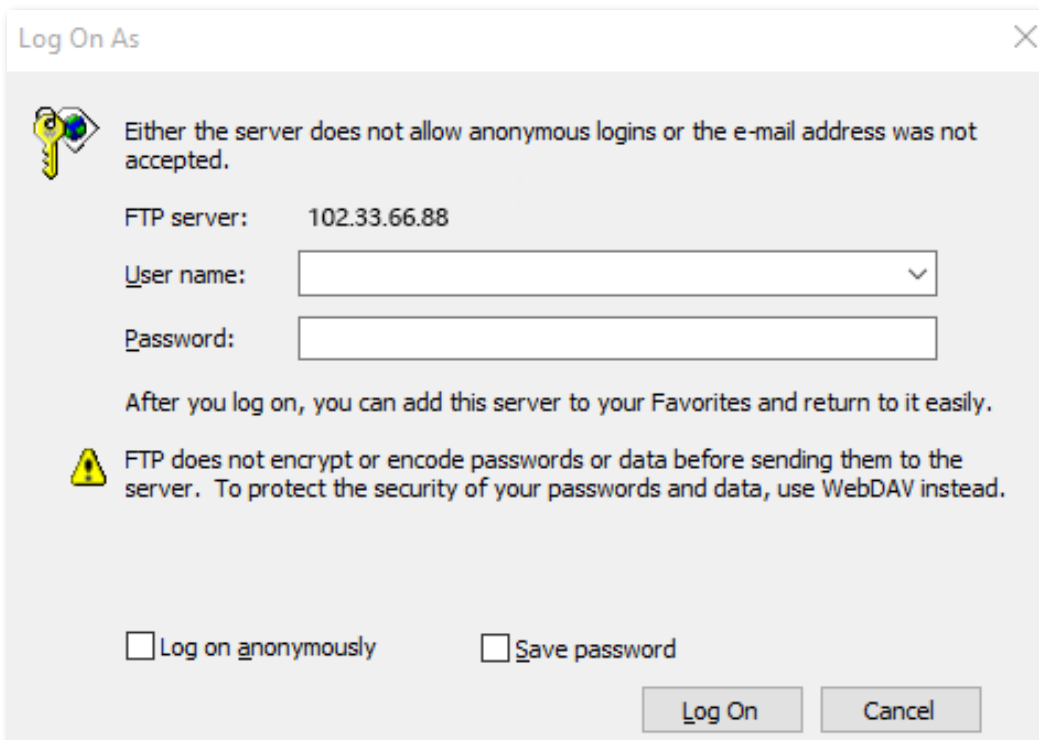
În acest exemplu, adresa este „**ftp://102.33.66.88:21**”. Puteți găsi adresa IP WAN a ruterului în [Vizualizare informații despre sistem](#).



Când numărul implicit al portului de serviciu intranet este 80, vă rugăm să schimbați numărul portului de serviciu cu unul neobișnuit (1024-65535), cum ar fi 9999.



Introduceți numele de utilizator și parola pentru a accesa resursele de pe serverul FTP. Aceste credențiale au fost create pe serverul FTP.



Dacă doriți să accesați serverul folosind un nume de domeniu, în loc de un IP, consultați secțiunea din manual [Accesarea de pe internet a unui server din rețeaua locală folosind un nume de domeniu](#).



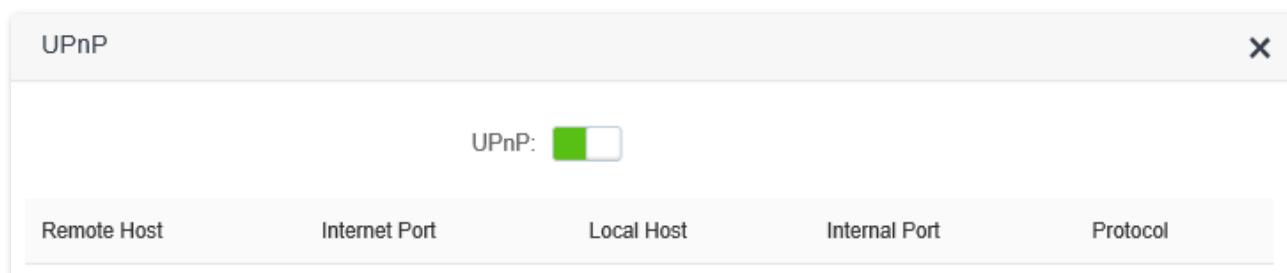
După configurații, dacă utilizatorii de internet încă nu pot accesa serverul FTP, închideți firewall-ul, software-ul antivirus și agenții de securitate de pe gazda serverului FTP și încercați din nou.

10.14 UPnP

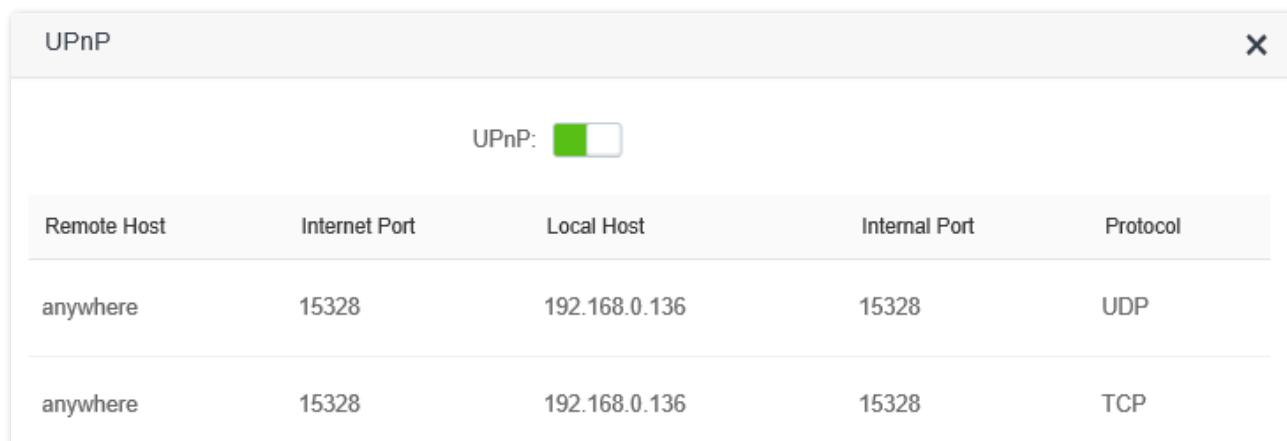
UPnP este prescurtarea pentru Universal Plug and Play. Această funcție permite deschiderea automată a portului ruterului pentru programele bazate pe UPnP. Este folosit în general pentru programe P2P, cum ar fi BitComet și AnyChat.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > UPnP**.

Această funcție este activată în mod implicit.



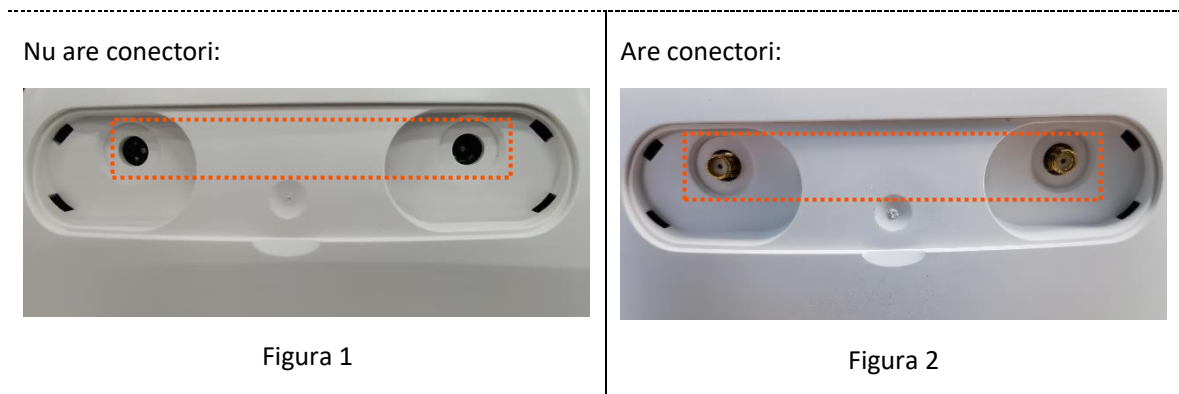
Cu funcția UPnP activată, puteți găsi informațiile de redirectionare automată a porturilor TCP și UDP, pe această pagină, atunci când programele conforme trimit cereri.



10.15 Setări antene

Această secțiune se aplică numai pentru 4G03.

Meniul **Antenna Setting (Setări antene)** este activ pentru echipamentele care nu vin cu o antenă externă în pachet dar au conectori SMA de conectare a unor antene pentru conectare la rețelele celulare. De exemplu, pentru modelul 4G03 care acceptă instalarea antenei externe se observă conectorii SMA (figura 2) după scoaterea capacului, alte versiuni de 4G03 (vândute în anumite regiuni sau cu anumite versiuni hardware) nu permit montarea unor antene externe, neavând conectorii necesari (figura 1).



Vă rugăm să îndepărtați ușor capacul care acoperă conectorii de antene pentru a evita deteriorarea ruterului. Contactați suportul nostru tehnic dacă mai aveți întrebări despre instalarea antenelor externe.

Dacă ruterul acceptă instalarea antenei externe și funcția de setare a puterii, consultați următorul conținut.

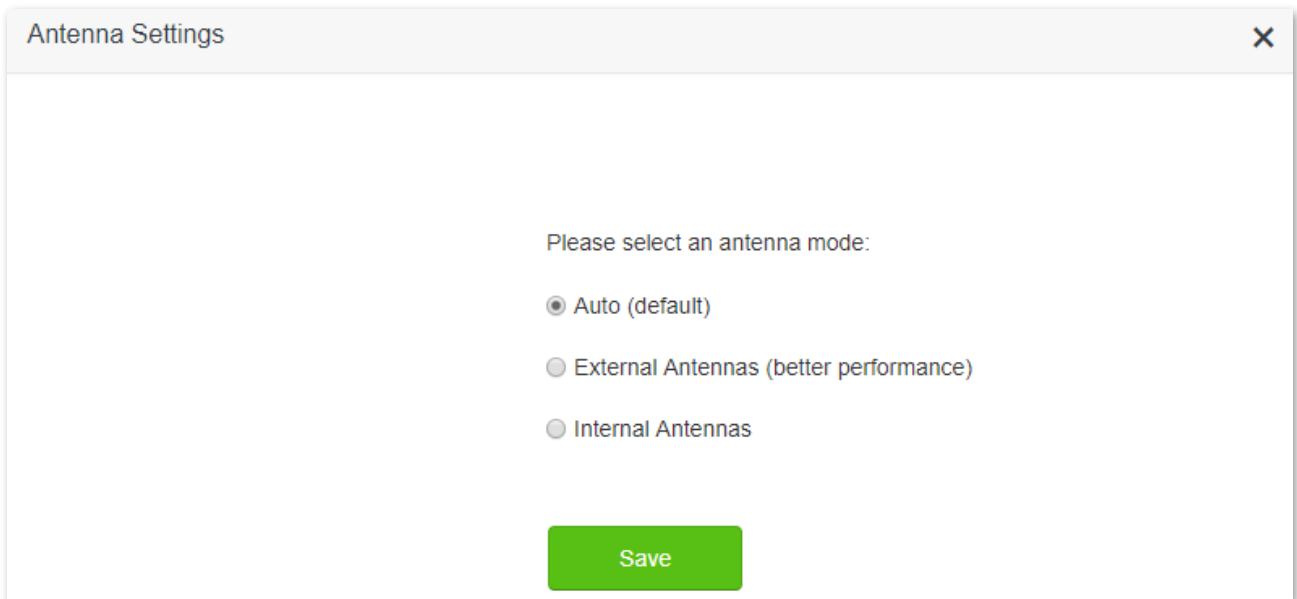


- Antenele externe nu sunt incluse în pachetul 4G03 și trebuie să le achiziționați separat.
- Antenele externe pot permite ruterului să primească semnal 3G/4G de la o distanță mai mare.
- De reținut că 4G03 are antene interne pentru comunicarea cu rețelele 4G/3G.

Trei moduri sunt disponibile în **Antenna Setting (Setări antene)**.

- **Auto (default) (Auto (implicit))**: ruterul comută automat între antene interne și externe, în funcție de instalarea antenelor externe. Când sunt instalate antene externe, ruterul acordă prioritate antenelor externe.
- **External Antennas (better performance) (Antene externe (performanță mai bună))**: ruterul primește și transmite semnal 4G prin antene externe. În modul router wireless, setarea nu funcționează.
- **Internal Antennas (Antene interne)**: ruterul primește și transmite semnal 4G sau oferă rețea Wi-Fi numai prin antenenele interne.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **Advanced Settings (Setări avansate) > Antennas Settings (Setări antene)**. Alegeți modul potrivit după cum este necesar.



Antenna Settings X

Please select an antenna mode:

- Auto (default)
- External Antennas (better performance)
- Internal Antennas

Save

11

Setări de sistem

Acest ghid este doar pentru referință și nu implică faptul că produsul acceptă toate funcțiile din ghid. Funcțiile acceptate de modele diferite sau versiuni diferite ale aceluiași model pot diferi. Interfața web reală prevalează. Pentru descrierea meniurilor și opțiunilor se folosesc termeni în română și engleză.

11.1 Setări LAN

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > LAN Settings (Setări LAN)**.

Pe această pagină, puteți să:

- Schimbați adresa IP și masca de subrețea a ruterului pentru rețeaua locală (LAN).
- Modificați parametrii serverului DHCP ai ruterului.

Serverul DHCP poate atribui automat adresa IP, masca de subrețea, gateway-ul și alte informații clienților aflați în rețeaua locală (LAN). Dacă dezactivați această funcție, trebuie să configurați manual informațiile despre adresa IP de pe client pentru a accesa internetul. Nu dezactivați funcția serverului DHCP decât dacă este necesar.

- Configurați informațiile DNS alocate clienților din rețeaua locală (LAN).

LAN Settings

LAN IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

DHCP Server:



IP Address Range: 192.168.0.100 ~ 200

Lease Time: 1 day

DNS Settings:

Save

Descrierea parametrilor

Parametru	Descriere
LAN IP Address (Adresă IP LAN)	Specifică adresa IP a ruterului din rețeaua locală (LAN), care este și adresa IP de acces al interfeței, paginii web de gestionare a ruterului. Rețineți că dacă schimbați clasa acestui IP o să schimbați și clasa IP atribuită clienților din rețeaua locală.
Subnet Mask (Masca de subrețea)	Specifică masca de subrețea, utilizată pentru a identifica intervalul de adrese IP a rețelei locale. Rețineți că acest parametru va fi atribuit și clienților din rețeaua locală.
DHCP Server (Server DHCP)	Folosit pentru a activa sau dezactiva serverul DHCP. Odată activat, serverul DHCP atribuie automat parametri necesari conectării clienților din rețeaua locală (LAN), cum ar fi adresa IP, masca de subrețea și adresa gateway-ului dispozitivului terminal. Se recomandă ca această funcție să fie activată.
IP Address Range (Interval de adrese IP)	Specifică intervalul de adrese IP care pot fi atribuite dispozitivelor conectate la ruter. Intervalul implicit este de la 192.168.0.100 la 192.168.0.200. Este necesar doar când DHCP Server (Serverul DHCP) este activat.
Lease Time (Timp de închiriere)	Specifică durata validă a adresei IP care este atribuită unui client. Este necesar doar când DHCP Server (Serverul DHCP) este activat. Când durata de închiriere ajunge la jumătate, clientul va trimite o solicitare DHCP serverului DHCP pentru reînnoire. Dacă reînnoirea reușește, contractul de închiriere este reînnoit în funcție de momentul cererii de reînnoire. Dacă reînnoirea eșuează, procesul de reînnoire se repetă din nou la 7/8 din perioada de închiriere. Dacă are succes, contractul de închiriere se reînnoiește în funcție de momentul cererii de reînnoire. Dacă tot eșuează, clientul trebuie să solicite din nou informații despre adresa IP după expirarea contractului de închiriere. Se recomandă valoarea implicită.
DNS Settings (Setări DNS)	Se activează sau dezactivează alocarea unor DNS-uri atribuite clienților din rețeaua locală. Când este dezactivat, adresa IP LAN a ruterului este utilizată ca adresă DNS a clientului. Când este activat, Primary DNS (DNS primar) trebuie setat, iar Secondary DNS (DNS secundar) este opțional. Este necesar doar când DHCP Server (Serverul DHCP) este activat.  TIP Acest router are funcția de proxy DNS.
Primary DNS Server (Server DNS primar)	Se setează adresa DNS primară care este atribuită clienților din rețeaua locală. Îl puteți seta, dacă este necesar, cu DNS-uri publice precum 1.1.1.1 sau 8.8.8.8. Este necesar doar când DNS Settings (Setările DNS) sunt activate.  TIP Asigurați-vă că serverul DNS principal este adresa IP a serverului DNS sau a proxy-ului DNS corect. În caz contrar, este posibil să nu reușiți să accesați internetul.

Parametru	Descriere
Secondary DNS Server (Server DNS secundar)	Se setează adresa DNS secundară atribuită clienților din rețeaua locală. Este un câmp opțional și este lăsat necompletat în mod implicit. Îl puteți seta, dacă este necesar, cu DNS-uri publice precum 1.1.1.1 sau 8.8.8.8.

11.2 Rezervare DHCP

11.2.1 Prezentare generală





Prin intermediul funcției de rezervare DHCP, clienții specificați pot obține întotdeauna aceeași adresă IP atunci când se conectează la router, asigurându-se că serviciile din meniurile Virtual Server (Server virtual), DDNS, DMZ Host (Gazdă DMZ) și altele pot funcționa normal. Această funcție are efect numai atunci când funcția de server DHCP a ruterului este activată.

Atribuirea unei adrese IP fixe se face pe baza adresei MAC a adaptorului de rețea prin care dispozitivul client se conectează.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > DHCP Reservation (Rezervare DHCP)**.

Descrierea parametrilor

Parametru	Descriere
Device Name (Numele dispozitivului)	Puteți specifica numele dispozitivului client pentru care se adaugă rezervarea de IP. Se poate adăuga orice remarcă considerați necesară.
MAC Address (Adresa MAC)	Specificați adresa MAC a clientului.
IP Address (Adresa IP)	Specificați adresa IP din rețeaua locală (LAN) rezervată clientului.
Status (Stare)	Specifică dacă clientul este online sau nu.

Parametru	Descriere
	Opțiunile disponibile includ:
	 : folosit pentru a adăuga o nouă regulă de rezervare DHCP.
Operation (Operațiune)	 : folosit pentru a lega adresa MAC de adresa IP fixă.
	 : folosit pentru a deconecta adresa MAC de adresa IP rezervată.
	 : folosit pentru a șterge regula de rezervare DHCP.

11.2.2 Atribuirea unei adrese IP fixe unui client din rețeaua locală

Scenariu: Ați configurat un server FTP în rețeaua locală (LAN).

Cerințe: Atribuiți o adresă IP fixă gazdei serverului FTP și preveniți eșecul accesului la serverul FTP din cauza schimbării adresei IP.

Soluție: Puteți configura funcția de rezervare DHCP pentru a îndeplini cerințele.

Să presupunem că informațiile serverului FTP includ:

- Adresa IP dorită pentru gazda FTP-ului: 192.168.0.136
- Adresa MAC a gazdei FTP-ului: D4:61:DA:1B:CD:89

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **System Settings (Setări sistem) > DHCP Reservation (Rezervare DHCP)**.
3. Opțional, introduceți o denumire sau orice remarcă în **Device Name (Numele dispozitivului)** pentru gazdă.
4. La **MAC Address (Adresa MAC)** introduceți adresa MAC a gazdei serviciului FTP **D4:61:DA:1B:CD:89**, ca exemplu.
5. La **IP Address (Adresa IP)** introduceți IP-ul pe care doriți să-l rezervați gazdei FTP-ului, care este **192.168.0.136** în acest exemplu.
6. Faceți clic pe **+New (+Nou)**.



Device Name	MAC Address	IP Address	Status	Operation
FTP server	:61:DA:1B:CD:89	192.168.0.136	---	+New

---Sfârșit

Când configurarea este finalizată, pagina este afișată ca mai jos, iar gazda serverului FTP primește întotdeauna aceeași adresă IP atunci când se conectează la router, care este 192.168.0.136 în acest exemplu.



Device Name	MAC Address	IP Address	Status	Operation
Optional	<input type="text"/>	<input type="text"/>	—	+New
DESKTOP-5LII2L5	<input type="text"/>	192.168.0.135		
FTP server	D4:61:DA:1B:CD:89	192.168.0.136		

11.3 Setări WAN

În meniul **WAN Parameters (Parametri WAN)**, puteți verifica și modifica valoarea MTU, modul de comunicare și rata maximă pe portul Ethernet RJ-45 în modul WAN, adresa MAC, numele serviciului și numele serverului.

11.3.1 Modificați valoarea MTU

Maximum Transmission Unit (MTU) este cel mai mare pachet de date transmis de un dispozitiv de rețea. Când tipul de conexiune este PPPoE, valoarea MTU implicită este 1480. Când tipul de conexiune este adresa IP dinamică sau adresa IP statică, valoarea MTU implicită este 1500. Nu modificați valoarea decât dacă este necesar. Dacă aveți nevoie, vă rugăm să consultați următoarele instrucțiuni.

Pentru a accesa pagina, [conectați-vă la interfața de utilizare web a ruterului](#) și navigați la **System Settings (Setări de sistem) > WAN Settings (Setări WAN)**.

WAN Settings

MTU: 1480

Speed: 1000 Mbps auto-negotiation

MAC Address: Default

Service Name: Default

Server Name: Default

Save

În general, se recomandă valoarea implicită. Încercați să modificați valoarea MTU atunci când:

- Nu puteți accesa anumite site-uri web sau site-uri web criptate, cum ar fi site-urile de e-banking sau PayPal.
- Nu puteți primi și trimite e-mailuri sau accesați un server FTP sau POP.

Puteți încerca să reduceți treptat valoarea MTU de la 1500 până când problema este rezolvată, intervalul recomandat este de la 1400 la 1500.

Descrierea aplicației MTU

MTU	Aplicație
1500	Este folosit în mod obișnuit pentru conexiuni dial-up non-ADSL și non-VPN.
1492, 1480	Este folosit pentru conexiunile dial-up ADSL.
1472	Este valoarea maximă pentru comanda ping. Un pachet cu o dimensiune mai mare este fragmentat.
1468	Este folosit pentru conexiuni DHCP.
1436	Este folosit pentru conexiuni VPN sau PPTP.

11.3.2 Modificare rată și mod de comunicare pe WAN

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > WAN Settings (Setări WAN)**.

Când cablul Ethernet este intact și conectat corect la portul Ethernet RJ-45 WAN, dar mesajul **Ethernet cable disconnected (Cablu Ethernet deconectat)** este încă afișat pe pagina **Internet Settings (Setări Internet)**, puteți încerca să schimbați **Speed (Viteza)** la **10 Mbps FDX** sau **10 Mbps HDX** pentru a rezolva problema. În caz contrar, păstrați setările implicite.

WAN Settings
✕

MTU:

Speed:

1000 Mbps auto-negotiation

10 Mbps FDX

10 Mbps HDX

100 Mbps FDX

100 Mbps HDX

MAC Address: Default:

Service Name: Keep the default unless necessary

Server Name: Keep the default unless necessary

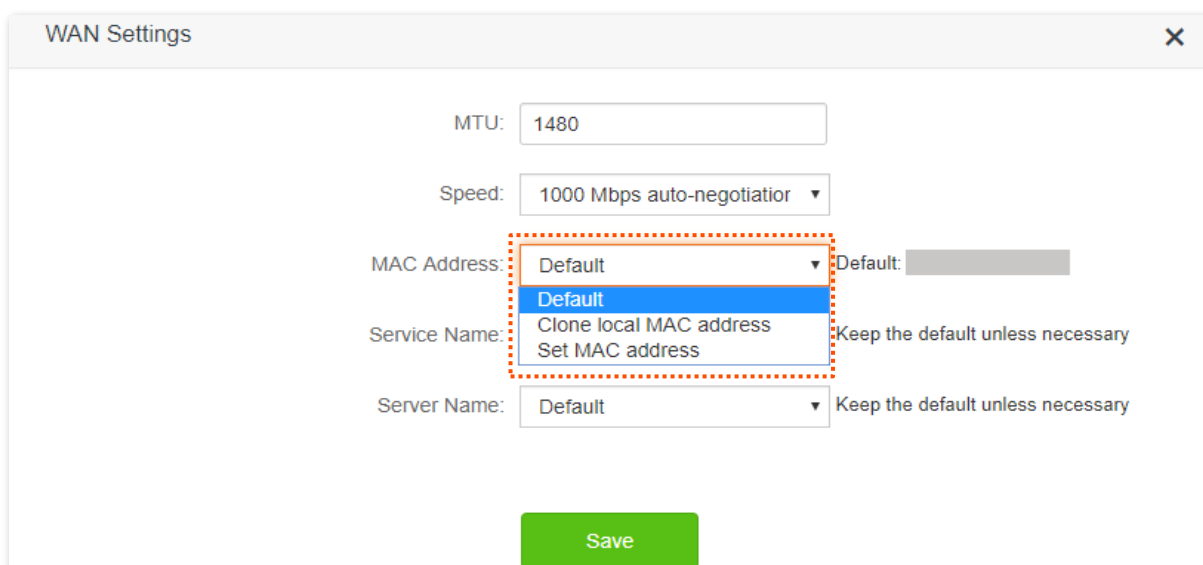
Descrierea parametrilor

Oțiunile din Speed (Viteză)	Descriere
1000 Mbps auto-negotiation (Auto-negociere 1000 Mbps)	Indică faptul că rata maximă la trimitere (și aceeași la primire) este de 1000 Mbps și modul duplex sunt determinate prin negociere cu celălalt dispozitiv de la capătul cablului.
10 Mbps FDX	Indică faptul că portul WAN funcționează la rata maximă de 10 Mbps la trimitere (și aceeași la primire), iar portul poate primi și trimite pachete de date în același timp, modul full-duplex (FDX).
10 Mbps HDX	Indică faptul că portul WAN funcționează la rata maximă de 10 Mbps la trimitere (și aceeași la primire), dar portul poate primi sau trimite pachete de date numai alternativ, pe rând trimite, apoi primește, modul half-duplex (HDX).
100 Mbps FDX	Indică faptul că portul WAN funcționează la rata maximă de 100 Mbps la trimitere (și aceeași la primire), iar portul poate primi și trimite pachete de date în același timp, modul full-duplex (FDX).
100 Mbps HDX	Indică faptul că portul WAN funcționează la rata maximă de 100 Mbps la trimitere (și aceeași la primire), dar portul poate primi sau trimite pachete de date numai alternativ, pe rând trimite, apoi primește, modul half-duplex (HDX).

11.3.3 Schimbare adresă MAC pe portul WAN

Dacă tot nu puteți accesa internetul după finalizarea [Accesului la internet prin cablu Ethernet](#), ar putea fi rezultatul configurației ISP-ului de a lega informațiile contului de internet cu o adresă MAC fixă. În acest caz, puteți clona și modifica adresa MAC a ruterului pentru a rezolva problema.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > WAN Settings (Setări WAN)**.



The screenshot shows the WAN Settings configuration page. The fields are as follows:

- MTU: 1480
- Speed: 1000 Mbps auto-negotiator
- MAC Address: Default (dropdown menu is open, showing options: Default, Clone local MAC address, Set MAC address)
- Service Name: Clone local MAC address (with a note: Keep the default unless necessary)
- Server Name: Default (with a note: Keep the default unless necessary)

A green Save button is located at the bottom center of the form.

- **Default (Implicit):** Păstrați valoarea din fabrică a adresei MAC.
- **Clone local MAC address (Clonează adresa MAC locală):** Setează adresa MAC a ruterului aceeași cu cea a dispozitivului care accesează pagina de gestionare a ruterului.
- **Set MAC address (Setați adresa MAC):** Setați manual o adresă MAC.

NOTE

Vă rugăm să vă asigurați că adresa MAC clonată este cea a computerului sau a ruterului care este deja capabil să acceseze internetul.

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului](#).
2. Navigați la **System Settings (Setări sistem) > WAN Settings (Setări WAN)**.
3. Faceți clic pe caseta derulantă din **MAC Address (Adresă MAC)**, alegeți **Clone local MAC address (Clonează adresa MAC locală)** sau **Set MAC address (Setați adresa MAC)** și introduceți adresa MAC dorită.
4. Faceți clic pe **Save (Salvare)**.

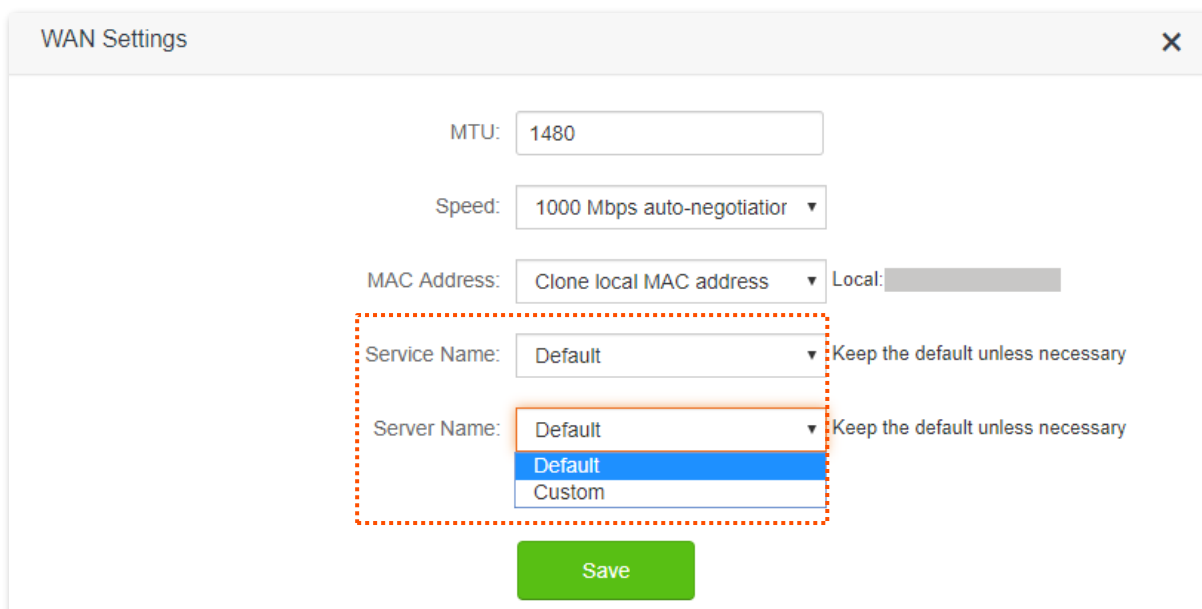
---Sfârșit

11.3.4 Schimbați numele serviciului și numele serverului

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > WAN Settings (Setări WAN)**.

Când setați conexiunea la internet prin cablu Ethernet conectat la portul RJ-45 marcat WAN, din meniul **Internet Settings (Setări Internet) > Failover**, atunci în unele cazuri pentru anumiți furnizori de internet să fie nevoie să modificați valorile din **Service Name (Nume serviciu)** și **Server Name (Nume server)**. De obicei se modifică aceste valori atunci când tipul de conexiune la internet, prin cablu, este **PPPoE**.

Dacă obțineți numele serviciului și serverului de la ISP-ul dvs. la achiziționarea serviciului de bandă largă, le puteți modifica pe această pagină după finalizarea setărilor de internet. În caz contrar, păstrați setările implicite.



The screenshot displays the WAN Settings configuration page. The fields are as follows:

- MTU: 1480
- Speed: 1000 Mbps auto-negotiator
- MAC Address: Clone local MAC address
- Service Name: Default (Keep the default unless necessary)
- Server Name: Default (Keep the default unless necessary)

The 'Server Name' dropdown menu is open, showing 'Default' and 'Custom' options. A green 'Save' button is located at the bottom of the form.

11.4 Setări de timp

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > Time Settings (Setări oră)**.

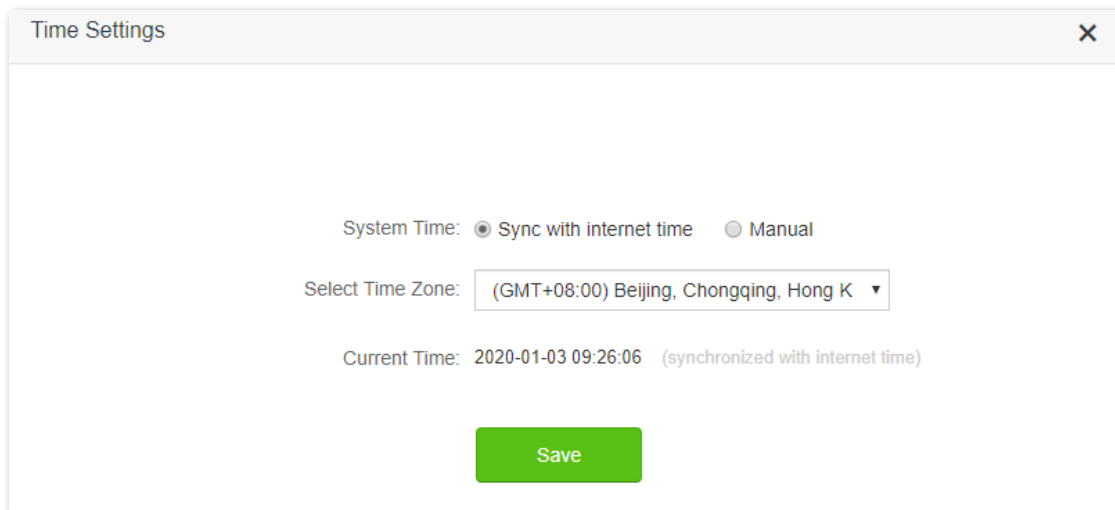
Puteți modifica setările de timp pe această pagină. Funcționarea funcțiilor bazată pe timp necesită un timp precis al sistemului. Data și ora de sistem poate fi sincronizată cu internetul sau setată manual. Implicit, este sincronizat cu internetul.

11.4.1 Sincronizare timp sistem cu timpul de pe internet

Dacă la **System Time (Timp sistem)** selectați **Sync with internet time (Sincronizare cu timpul de pe internet)**, ruterul își va sincroniza automat data și ora cu un server NTP de pe internet atunci când are conexiune la internet. De asemenea, e important să alegeți fusul orar în **Select Time Zone (Selectare fus orar)**.

Anul, luna, ziua, ora, minutul și secunda sistemului sunt afișate la **Current Time (Timp curent)**.

La final apăsați **Save (Salvare)**.



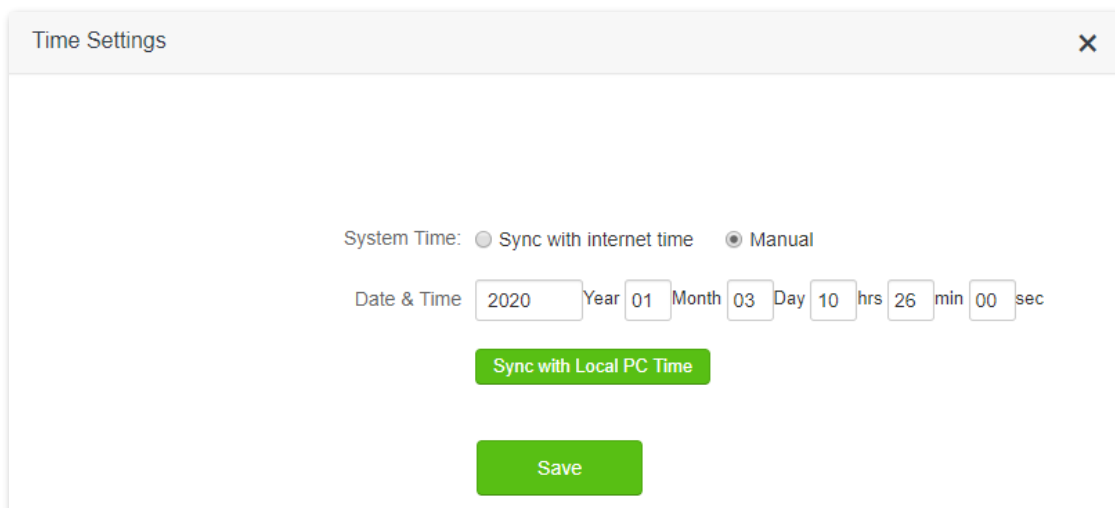
The screenshot shows a 'Time Settings' window with the following elements:

- System Time:** Two radio buttons are present. The first, labeled 'Sync with internet time', is selected. The second, labeled 'Manual', is unselected.
- Select Time Zone:** A dropdown menu is open, showing '(GMT+08:00) Beijing, Chongqing, Hong K' as the selected option.
- Current Time:** The text '2020-01-03 09:26:06' is displayed, followed by '(synchronized with internet time)' in a smaller font.
- Save Button:** A green rectangular button with the text 'Save' is centered at the bottom of the window.

11.4.2 Setare manuală a datei și orei

Când **System Time (Timp sistem)** este setat pe **Manual**, puteți introduce ora dorită sau puteți sincroniza ora de sistem a ruterului cu dispozitivul care configurează ruterul. În plus, trebuie să corectați de fiecare dată când reporniți ruterul pentru a asigura acuratețea timpului sistemului.

Pentru sincronizarea datei și orei sistemului cu calculatorul conectat la interfața web de gestionare atunci apăsați **Sync with Local PC Time (Sincronizare cu timp PC)** și dați **Save (Salvare)**.



The screenshot shows the 'Time Settings' window with the following elements:

- System Time:** Two radio buttons are present. The first, labeled 'Sync with internet time', is unselected. The second, labeled 'Manual', is selected.
- Date & Time:** A series of input fields for manual time setting: '2020' (Year), '01' (Month), '03' (Day), '10' (hrs), '26' (min), and '00' (sec).
- Sync with Local PC Time Button:** A green rectangular button with the text 'Sync with Local PC Time' is positioned below the date and time fields.
- Save Button:** A green rectangular button with the text 'Save' is centered at the bottom of the window.

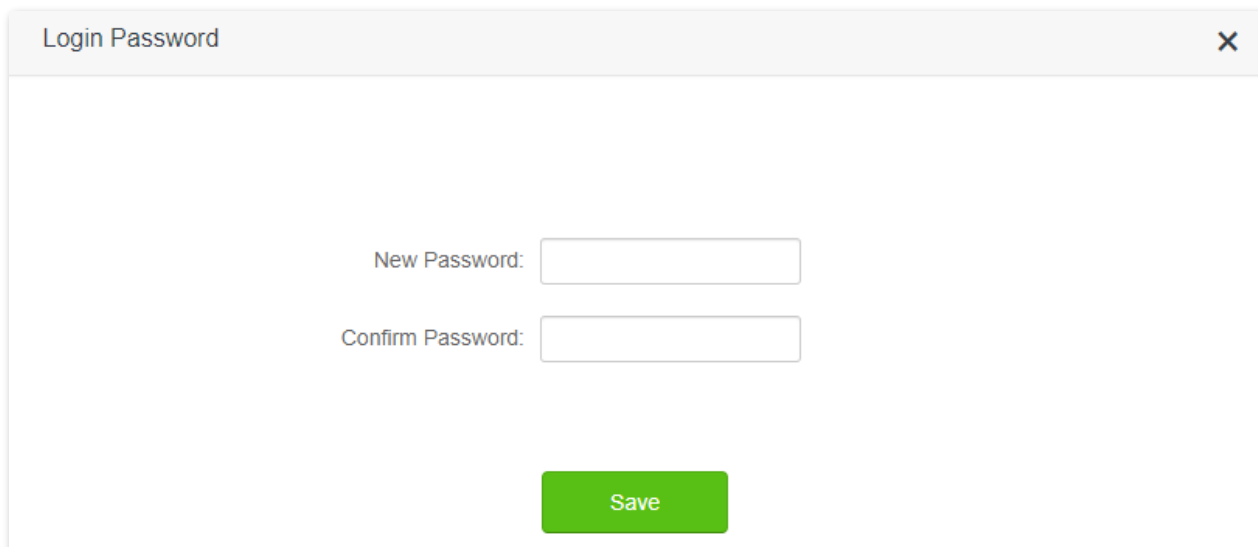
11.5 Parola de conectare la interfața de gestionare

Pentru a asigura securitatea rețelei, se recomandă o parolă de conectare la interfața de gestionare a ruterului. O parolă de conectare constând din mai multe tipuri de caractere, cum ar fi litere mari și litere mici, aduce o securizare mai mare echipamentului și implicit rețelelor create.

Când utilizați ruterul pentru prima dată, și deschideți configuratorul rapid pas cu pas, nu este necesară nicio parolă. Ulterior, în acel configurator pas cu pas, după setarea conexiunii la internet, la ultimul pas unde setați rețeaua Wi-Fi, aveți și o secțiune care permite crearea unei parole de acces la interfața de gestionare.

Pentru a accesa pagina de schimbare sau crearea a unei parole de conectare la interfața de gestionare, [conectați-vă la interfața web a routerului](#) și navigați la **System Settings (Setări sistem) > Login Password (Parolă de conectare)**.

Dacă nu aveți setată o parolă de acces a interfeței de gestionare pagina va arăta ca mai jos, în care trebuie să creați o parolă introducând aceeași în **New Password (Parolă nouă)** și aceeași în **Confirm Password (Confirmare parolă)**.



The screenshot shows a web form titled "Login Password" with a close button in the top right corner. The form contains two text input fields: "New Password:" and "Confirm Password:". Below these fields is a green "Save" button.

Dacă ați setat deja o parolă de conectare, puteți schimba parola pe această pagină. Astfel, introduceți parola actuală în **Old Password (Parolă veche)** și noua parolă pe care o doriți, de două ori în **New Password (Parolă nouă)** și în **Confirm Password (Confirmare parolă)**. Puteți da clic pe fiecare câmp pentru a vedea în clar parolele introduse.

Login Password ✕

Old Password:

New Password:

Confirm Password:



TIP

Dacă uitați parola de conectare și nu vă puteți conecta la interfața web a routerului, consultați secțiunea din manual despre [resetarea ruterului](#) pentru a restabili la setările din fabrică și conectați-vă la interfața web fără parolă.

Această parolă de conectare la interfața web se va folosi și atunci când accesați echipamentul cu aplicația **Tenda WiFi** (Android & iOS) pentru gestionarea de pe un smartphone.

11.6 Repornire și resetare

11.6.1 Repornire ruter

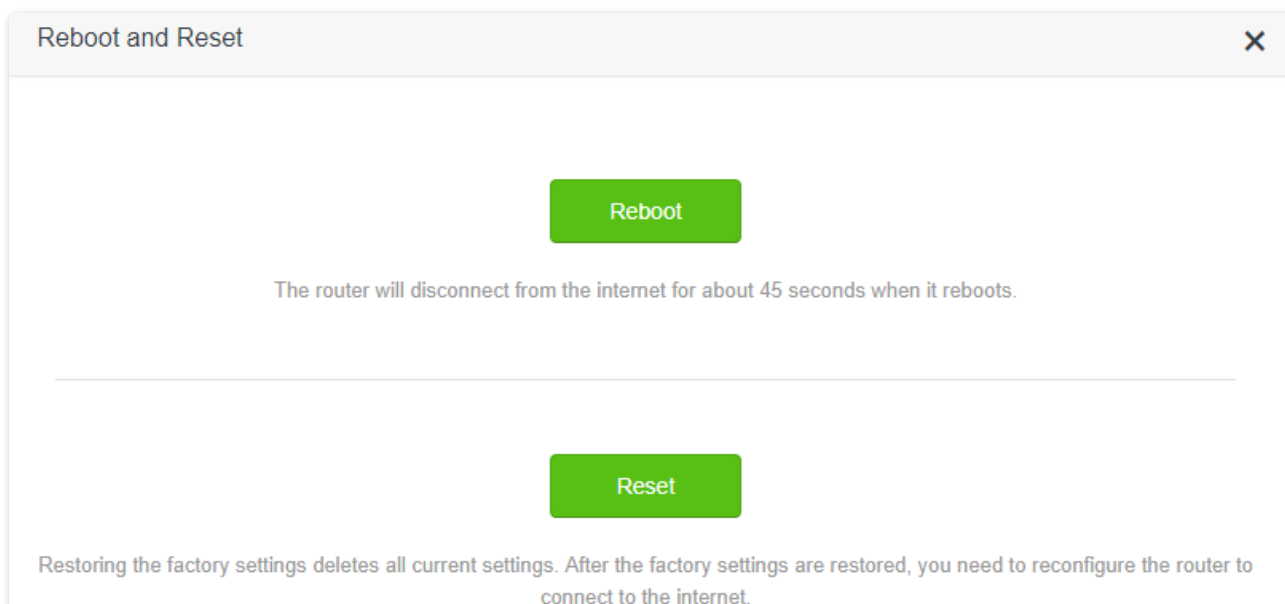
Dacă vreun parametru nu are efect sau ruterul nu funcționează corect, puteți încerca să reporniți ruterul.



TIP

Repornirea ruterului va deconecta toate conexiunile la ruter.

Pentru a reporni routerul, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări sistem) > Reboot and Reset (Repornire și resetare)**. Faceți clic pe **Reboot (Reporniți)** pentru a reporni ruterul.



Așteptați câteva momente până când procesul în curs se termină.

11.6.2 Resetare ruter

Dacă nu sunteți sigur de ce internetul este inaccesibil sau uitați parola de conectare la interfața de gestionare, puteți reseta ruterul.



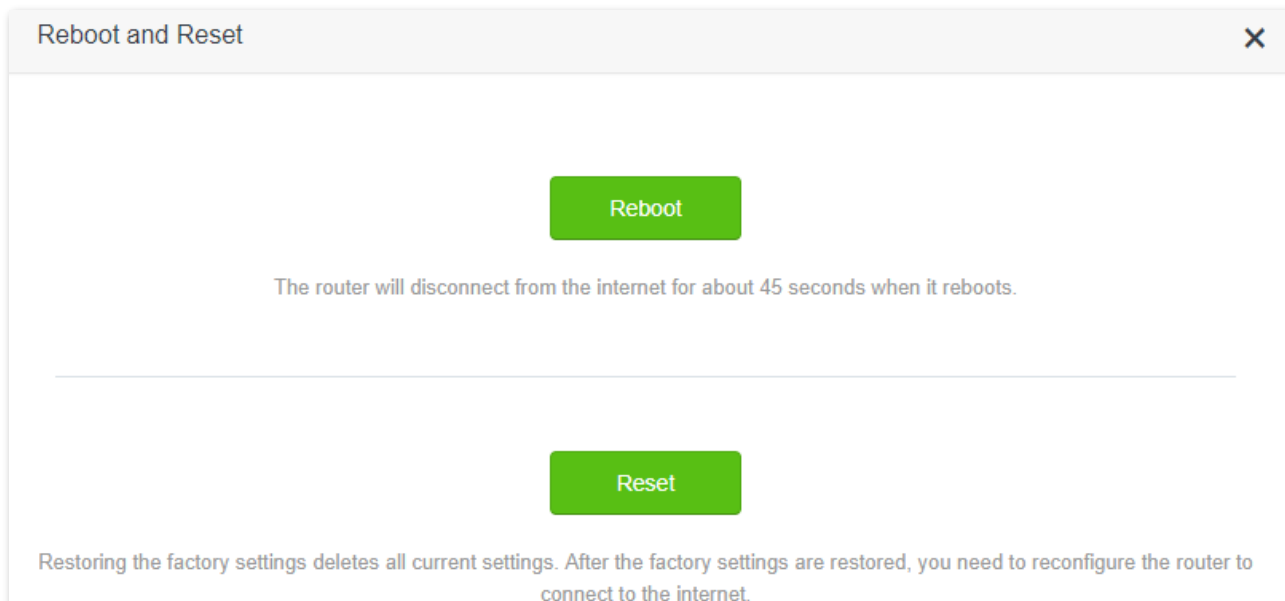
- Resetarea ruterului nu este recomandată decât dacă nu puteți găsi o soluție pentru problema curentă. Trebuie să reconfigurați ruterul după ce este resetat.
- Asigurați-vă că sursa de alimentare a ruterului este normală atunci când ruterul este resetat. În caz contrar, ruterul ar putea fi deteriorat.
- Adresa IP implicită de conectare este 192.168.0.1 după resetare și nu este necesară nicio parolă.

Resetare utilizând butonul fizic de resetare

Țineți apăsat butonul **RST/WPS** pe spatele echipamentului Tenda timp de aproximativ **8 secunde** și eliberați când toate indicatoarele LED clipește o dată. Ruterul este resetat și restaurat la setările din fabrică. Procesul poate dura câteva minute.

Resetare din pagina web de gestionare

Pentru a seta routerul, [conectați-vă la interfața web de gestionare a ruterului](#) și navigați la **System Settings (Setări sistem) > Reboot and Reset (Repornire și resetare)** și faceți clic pe butonul verde **Reset (Resetează)**.



Așteptați un moment până când procesul în curs se termină.

11.7 Actualizare firmware

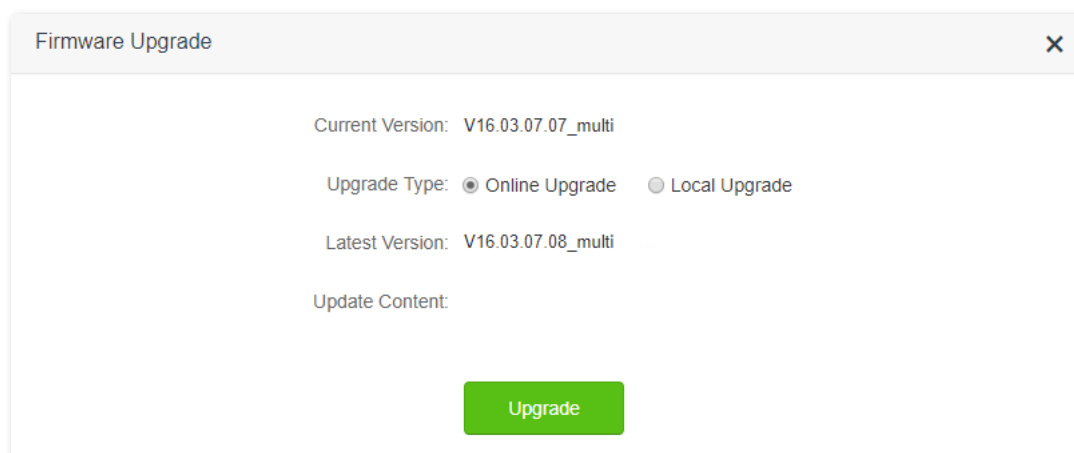
Această funcție permite ruterului să obțină cele mai recente funcții dar și performanțe mai stabile și corectarea eventualelor bug-uri detectate. Se recomandă ca ruterul să folosească cea mai recentă versiune de firmware. Pe această pagină, puteți configura actualizarea firmware-ului online și actualizarea firmware-ului local.

11.7.1 Upgrade online

Când ruterul este conectat la internet, detectează automat dacă există un firmware nou și afișează informațiile detectate pe pagină. Puteți alege dacă să faceți upgrade la cel mai recent firmware.

Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **System Settings (Setări sistem) > Firmware Upgrade (Actualizare firmware).**
3. La **Upgrade Type (Tip upgrade)** asigurați-vă că e selectat **Online Upgrade (Upgrade online).**
4. Așteptați până când este detectată o nouă versiune de firmware, informație afișată la **Latest Version (Ultima versiune).**



5. Pentru începerea procesului de descărcare a firmware-ului de pe serverele Tenda și actualizare efectivă a echipamentului faceți clic pe butonul verde **Update (Actualizare).**

---Sfârșit

Așteptați un moment până când procesul în curs se termină. [Conectați-vă din nou la interfața web a routerului.](#) Navigați la **System Settings (Setări sistem) > System Status (Stare sistem)** și verificați dacă actualizarea a reușit, verificând informația de la câmpul **Firmware Version (Versiune firmware).**

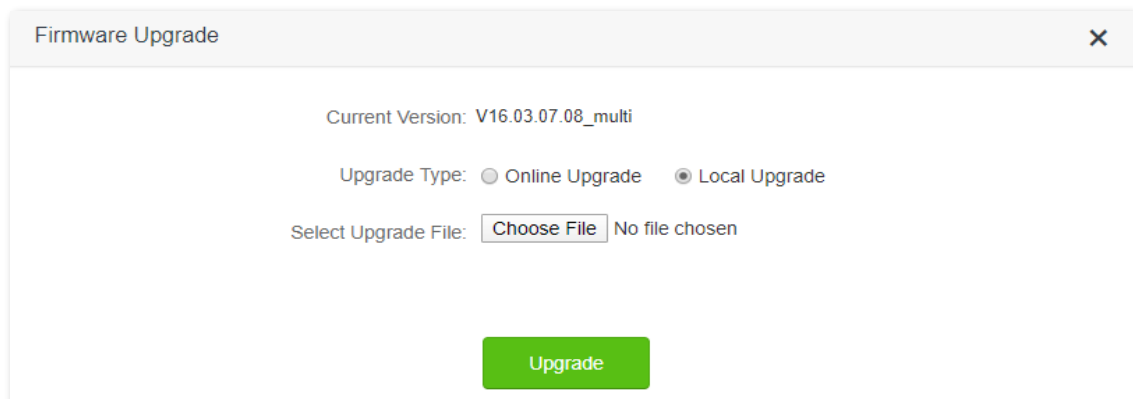
11.7.2 Upgrade local



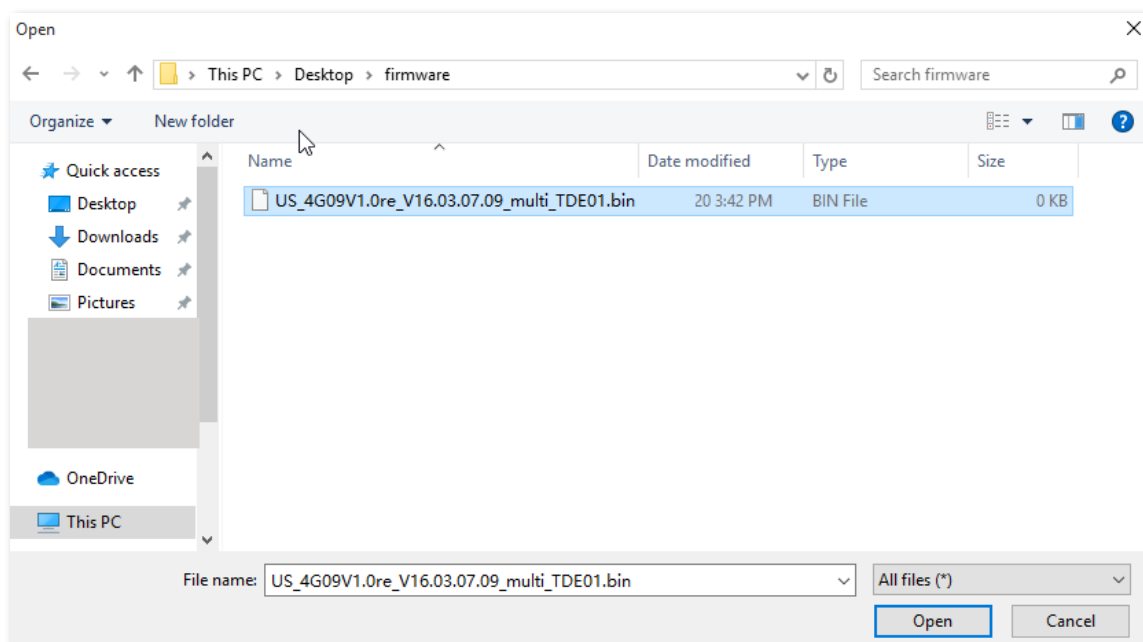
Pentru a preveni deteriorarea ruterului:

- Asigurați-vă că firmware-ul este aplicabil ruterului.
- Este recomandat să actualizați firmware-ul conectând un calculator la un port LAN și efectuând actualizarea din pagina locală web de gestionare a echipamentului Tenda.
- Când actualizați firmware-ul nu opriți ruterul.

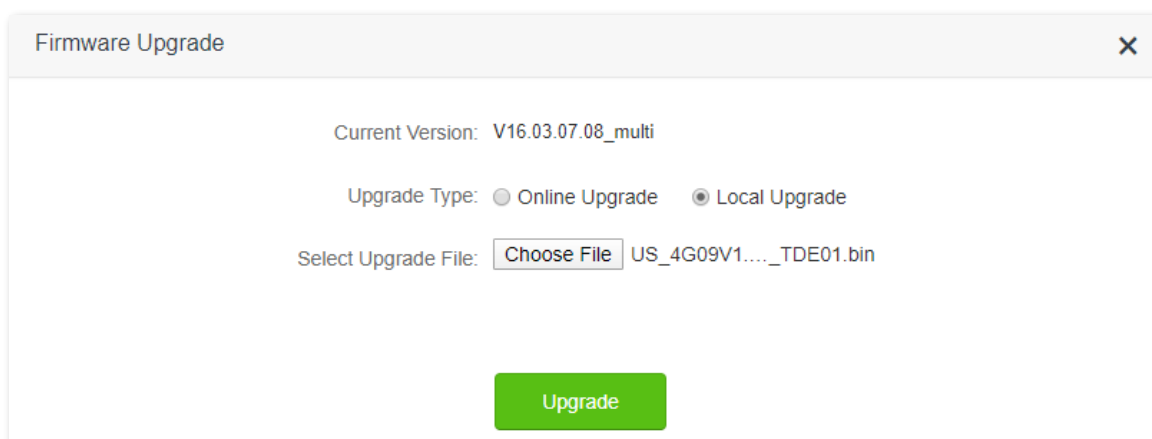
1. Aflați versiunea hardware a echipamentului și modelul. Aceste informații se află accesând pagina web de gestionare a ruterului, apoi meniul **System Settings (Setări de sistem) > System Status (Stare sistem) > Information (Informații)**. Modelul se află scris pe [eticheta de pe spatele echipamentului](#).
2. Accesați www.tendacn.com/ro. Căutați modelul de echipament. Apoi accesați secțiunea Downloads (Descărcări) sau Services (Servicii) și căutați ultima versiune de firmware aplicabilă **versiunii hardware** (v3.0, v2.0 etc.) a echipamentului.
3. **Citiți cu atenție notele din pagina de descărcare a firmware-ului**. Descărcați pe computerul local și dezarhivați-l.
4. [Reconectați-vă la interfața web de gestionare a routerului](#).
5. Navigați la **System Settings (Setări sistem) > Firmware Upgrade (Actualizare firmware)**.
6. Alegeți **Local Upgrade (Upgrade local)**.
7. Faceți clic pe **Choose File (Alegeți fișier)**.



8. Căutați fișierul firmware cu extensia **.bin**, descărcat și dezarhivat anterior, și faceți clic pe **Open (Deschidere)**.



9. Apoi, faceți clic pe **Upgrade (Upgrade)**.



---Sfârșit

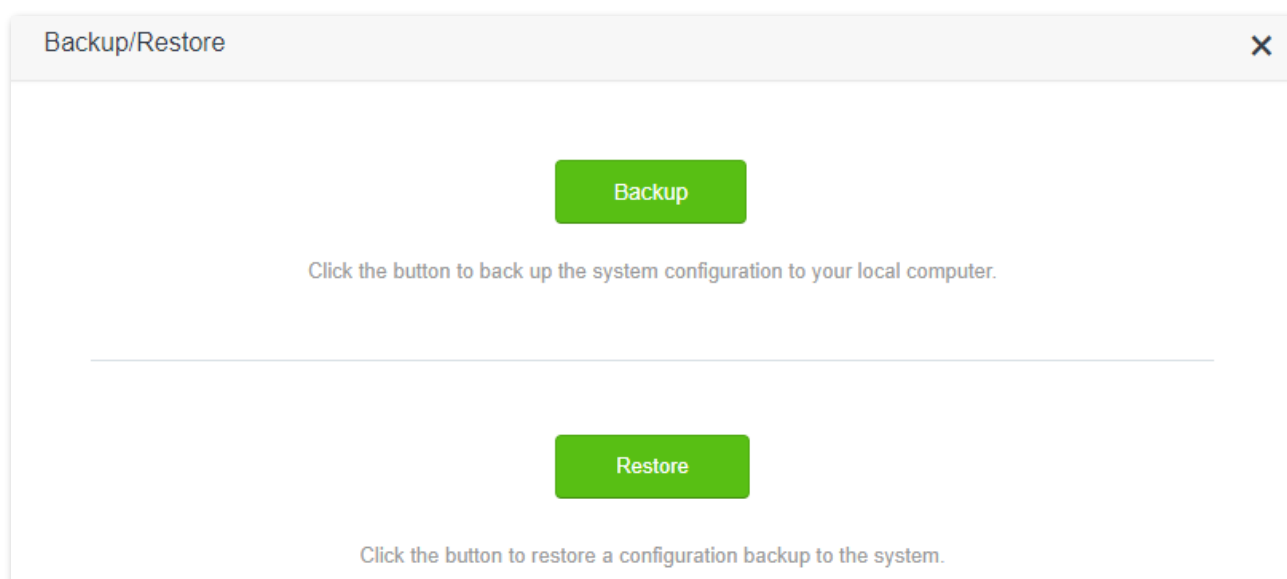
Așteptați un moment până când procesul în curs se termină. [Conectați-vă din nou la interfața routerului](#). Navigați la **System Settings (Setări sistem) > System Status (Stare sistem)** și verificați dacă actualizarea a reușit, verificând informația de la **Firmware Version (Versiunea de firmware)**.

11.8 Backup și restaurare configurații

În acest meniu, puteți face copii de rezervă ale configurațiilor curente ale ruterului, pe computer. Vă recomandăm să faceți o copie de rezervă a configurației după ce setările ruterului sunt modificate semnificativ și ruterul funcționează într-o stare bună.

După ce resetați ruterul la setările din fabrică sau actualizați versiunea de firmware, puteți utiliza această funcție pentru a restabili configurațiile pentru care s-a făcut backup.

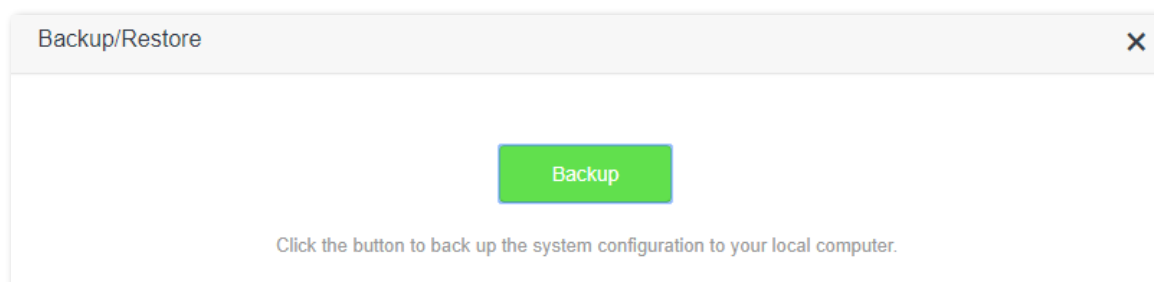
Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări sistem) > Backup/Restore (Backup/Restaurare)**.



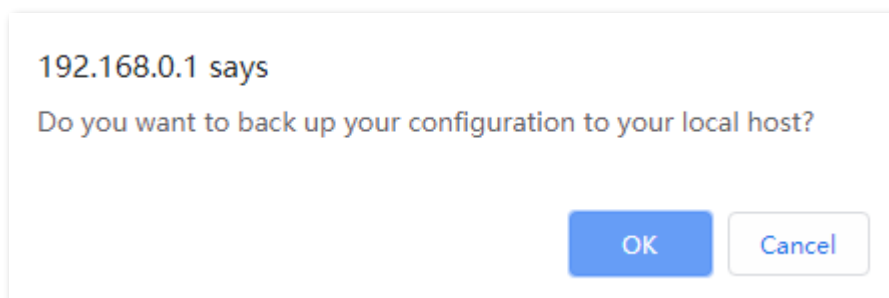
11.8.1 Salvarea locală a configurațiilor ruterului

Pentru a face o copie de rezervă cu configurațiile ruterului, urmați pașii:

1. [Conectați-vă la interfața web de gestionare a routerului.](#)
2. Navigați la **System Settings (Setări sistem) > Backup/Restore (Backup/Restaurare)**.
3. Faceți clic pe **Backup**.



4. Faceți clic pe **OK** în fereastra pop-up.



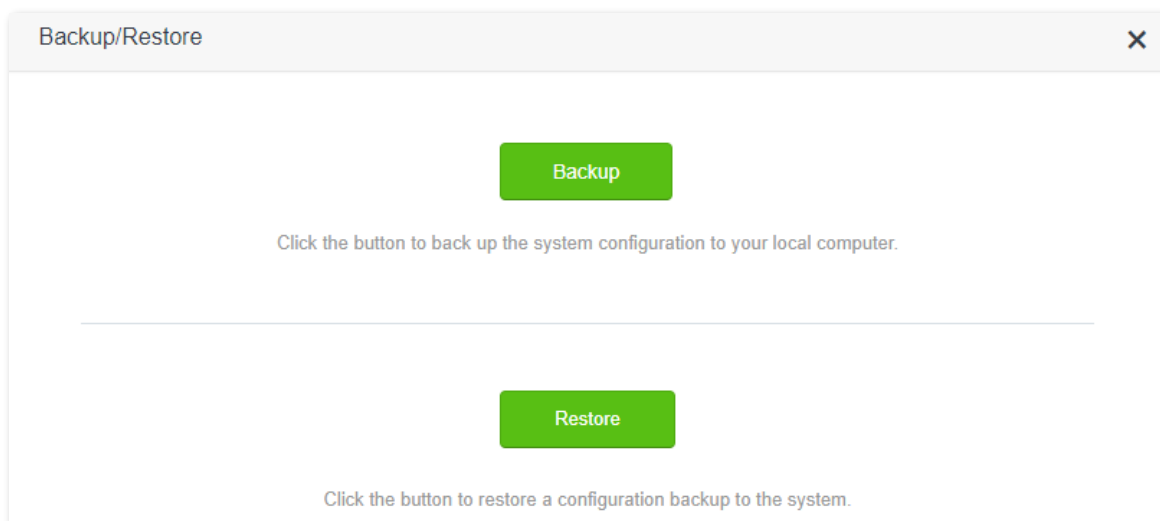
---Sfârșit

Un fișier denumit **RouterCfm.cfg** va fi descărcat pe calculatorul local.

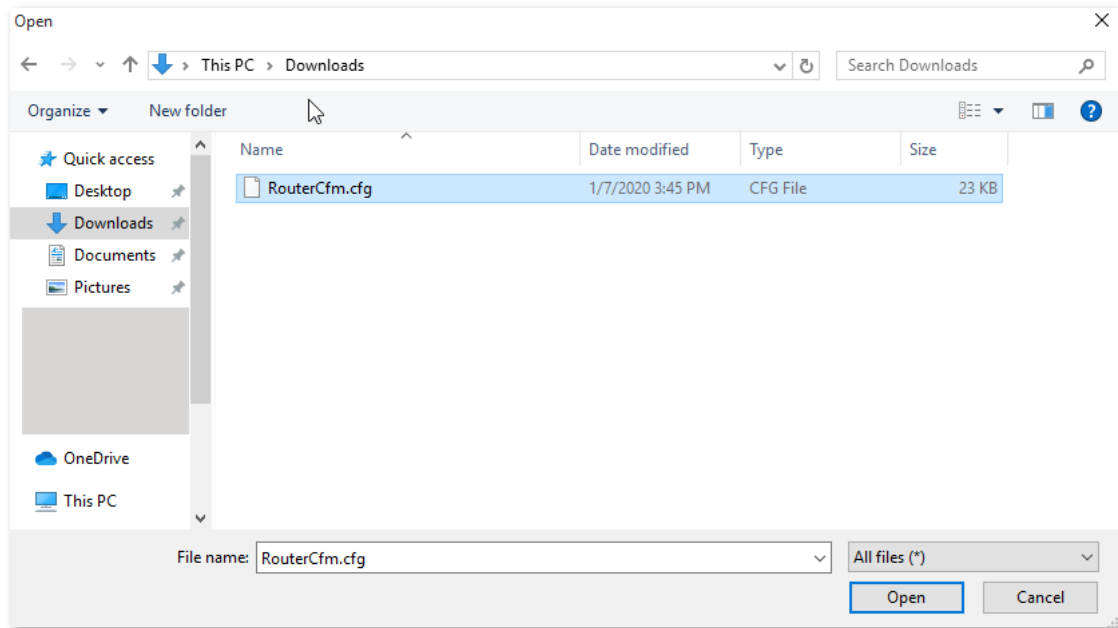
11.8.2 Restaurarea configurațiilor anterior salvate

Pentru a restabili configurațiile anterioare ale routerului, urmați pașii:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **System Settings (Setări sistem) > Backup/Restore (Backup/Restaurare)**.
3. Faceți clic pe **Restore (Restaurare)**.



4. Alegeți un fișier de configurare (extensia: .cfg) anterior salvat pentru a fi restaurat și faceți clic pe **Open (Deschidere)**.



---Sfârșit

Așteptați un moment până când procesul în curs se termină, iar ruterul restabilește setările anterioare.

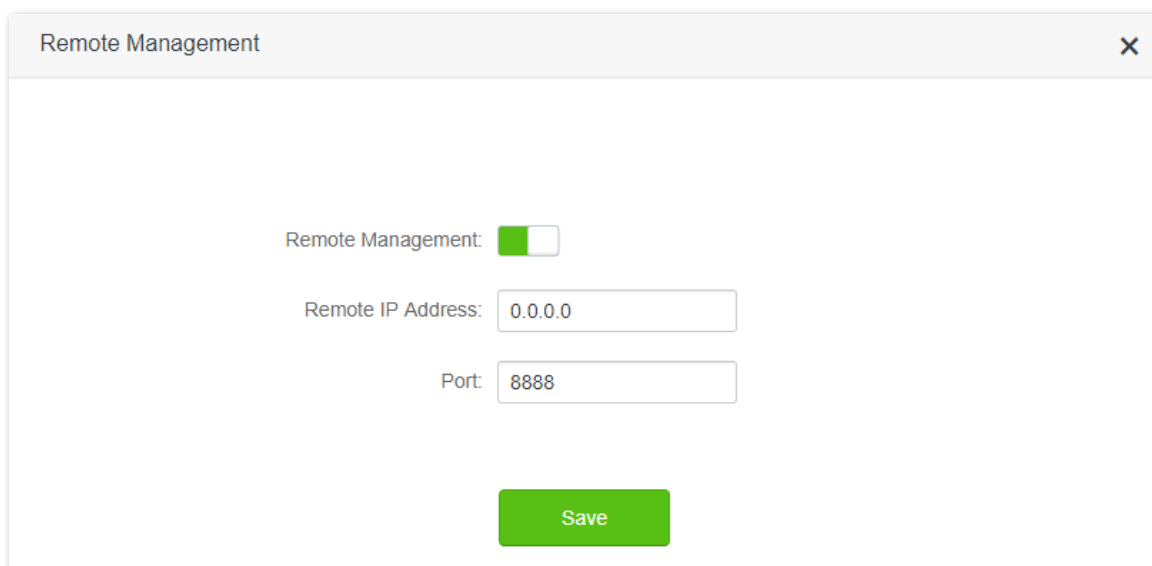
11.9 Accesare interfață web de gestionare din afara rețelei locale

11.9.1 Prezentare generală

În general, interfața de utilizare web a ruterului poate fi accesată numai de pe dispozitivele din rețeaua locală, care sunt conectate la router printr-un port LAN sau prin Wi-Fi, însă aveți și posibilitatea de a accesa pagina web de gestionare a ruterului din afara rețelei interne, de pe internet, de oriunde, accesând din browser adresa publică.


Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > Remote Management (Management de la distanță)**.

Implicit, această funcție este dezactivată. Când această funcție este activată, pagina este afișată ca mai jos.



Descrierea parametrului

Parametru	Descriere
Remote Management (Management de la distanță)	Folosit pentru a activa sau dezactiva funcția de accesa a paginii web de gestionare a ruterului din afara rețelei locale.

Parametru	Descriere
Remote IP Address (Adresă IP de la distanță)	<p>Specifică adresa IP a gazdei care poate accesa de la distanță interfața web a ruterului.</p> <ul style="list-style-type: none"> - 0.0.0.0: indică faptul că gazdele cu orice adresă IP de pe internet pot accesa interfața de utilizare web a ruterului. Nu este recomandat pentru securitate. - O altă adresă IP specificată: numai gazda cu adresa IP specificată poate accesa de la distanță interfața web a ruterului. Asigurați-vă că adresa IP este o adresă IP publică.
Port	<p>Specifică numărul portului TCP a ruterului care este deschis pentru management de la distanță. Schimbați-l după cum este necesar.</p> <p> TIP</p> <ul style="list-style-type: none"> - Porturile de la 1 la 1024 sunt de obicei ocupate de servicii standard. Este recomandat să introduceți un număr de port de la 1025 la 65535 pentru a preveni conflictele. - Gestionarea de la distanță poate fi realizată accesând „http://adresa IP WAN a ruterului:numărul portului TCP”. Dacă funcția gazdă DDNS este activată, interfața de utilizare web poate fi accesată și prin „http://numele de domeniu al portului WAN al ruterului:numărul portului TCP”. - De exemplu, dacă portul setat este 8888 și la Remote IP Address (Adresă IP de la distanță) este 0.0.0.0 iar IP-ul public al ruterului este 88.80.78.56 atunci din bara de adrese a unui browser de pe orice dispozitiv de pe internet, interfața de gestionare se poate accesa cu adresa http://88.80.78.56:8888. După, este nevoie să fie introdusă parola de acces la interfața de gestionare.

11.9.2 Exemplu de configurare a accesului la interfața web de la un IP public specificat

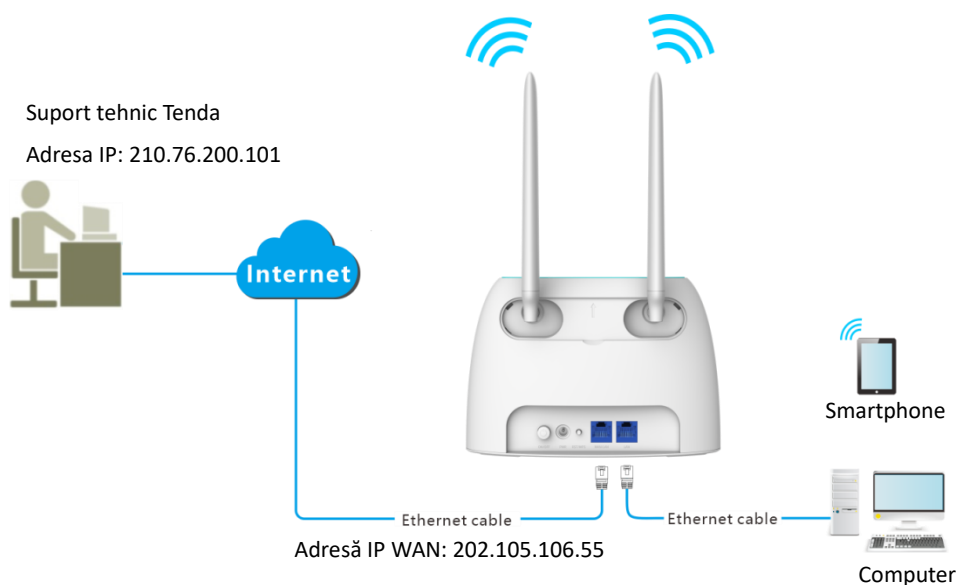
Scenariu: Întâmpinați o problemă la configurarea ruterului.

Cerințe: Solicitați asistență tehnică Tenda să vă ajute să configurați ruterul, de la distanță.

Soluție: Puteți configura funcția de gestionare la distanță pentru a atinge cerințele.

Să presupunem că:

- Adresa IP publică a suportului tehnic Tenda: 210.76.200.101
- Adresa WAN a ruterului, adresa IP publică: 202.105.106.55



Procedura de configurare:

1. [Conectați-vă la interfața web a ruterului.](#)
2. Navigați la **System Settings (Setări sistem) > Remote Management (Gestionare la distanță)**.
3. Activați **Remote Management (Managementul de la distanță)**.
4. Introduceți adresa IP care poate accesa interfața web de la distanță, care este **210.76.200.101** în acest exemplu.
5. Faceți clic pe **Save (Salvare)**.

Remote Management ✕

Remote Management:

Remote IP Address:

Port:

---Sfârșit

Când configurațiile sunt finalizate, asistența tehnică Tenda poate accesa și gestiona interfața web a ruterului vizitând „<http://202.105.106.55:8888>” pe computer. Va fi necesar să comunicați [parola de autentificare la interfața web de gestionare](#).

11.10 Starea sistemului

Pe această pagină, puteți găsi informațiile de bază despre ruter precum versiunea de firmware și hardware, starea WAN, starea LAN, starea Wi-Fi și starea IPv6.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > System Status (Stare sistem)**.

11.10.1 Informații de bază

În secțiunea **Information (Informații)** puteți vizualiza informațiile de bază ale ruterului, cum ar fi timpul de sistem, perioada neîntreruptă de funcționare și versiunea de firmware și versiunea hardware.

Information

System Time: 2020-02-25 16:31:20

Uptime: 1 hour(s) 28 min 21 s

Firmware Version: V16.03.07.08_multi

Hardware Version: V1.0

Descrierea parametrului

Parametru	Descriere
System Time (Ora sistemului)	Specifică data și ora de sistem a ruterului.
Uptime (Timp de funcționare)	Specifică timpul de funcționare al ruterului de când este pornit.
Firmware Version (Versiune de firmware)	Specifică versiunea de firmware a ruterului.
Hardware Version (Versiune hardware)	Specifică versiunea hardware a ruterului.

11.10.2 Starea conexiunilor

3G/4G

În această secțiune, puteți vizualiza informațiile despre cartela SIM și rețeaua 3G/4G.

3G/4G

SIM Card Status: Ready

Connection Status: Connected

Signal Strength: Excellent

ISP: ██████████

Mobile Network: 4G

Statistics: 0.438MB

Upload Speed: 0.0KB/s

Download Speed: 0.0KB/s

IP Address: 10.136.116.154

Subnet Mask: 255.255.255.252

Default Gateway: 10.136.116.153

Primary DNS: 120.80.80.80

Secondary DNS: 221.5.88.88

MAC Address: ██████████

Descrierea parametrului

Parametru	Descriere
SIM Card Status (Starea cartelei SIM)	Specifică starea cartelei SIM introduse în ruter.
Connection Status (Starea conexiunii)	Specifică starea conexiunii la internet a rețelei mobile 3G/4G.
Signal Strength (Puterea semnalului)	Puterea semnalului rețelei mobile 3G/4G, anume excelentă, medie și suficientă.
ISP	Specifică numele ISP (furnizorul de servicii Internet) al cartelei SIM.

Parametru	Descriere
Mobile Network (Rețea mobilă)	Specifică tipul curent de generație de tehnologie pentru rețelele mobile de comunicație.
Statistics (Statistici)	Specifică traficul de date al cartelei SIM care a fost utilizată.
Upload Speed (Viteza de încărcare)	Specifică rata de încărcare a rețelei mobile a ruterului.
Download Speed (Viteza de descărcare)	Specifică rata de descărcare a rețelei mobile a ruterului.
IP address (Adresa IP)	Specifică adresa IP a ruterului obținută de la ISP, fiind de obicei o adresă IP publică.
Subnet Mask (Masca de subrețea)	Specifică masca de subrețea a rețelei mobile.
Default Gateway (Gateway implicit)	Specifică adresa IP a gateway-ului prin care ruterul se conectează.
Primary DNS (DNS primar)	Specifică adresa IP a serverelor DNS primare și secundare obținute.
Secondary DNS (DNS secundar)	
MAC Address (Adresa MAC)	Specifică adresa MAC a adaptorului pentru pentru rețelele mobile de comunicație de pe ruter.

Stare WAN

În această secțiune, puteți vizualiza informațiile portului Ethernet RJ-45 marcat WAN, inclusiv tipul conexiunii, starea conexiunii și durata conexiunii și așa mai departe.

WAN Status	
Connection Type:	Dynamic IP Address
Connection Status:	Connected
Connection Duration:	2 hour(s) 29 min 38 s
IP Address:	172.16.20.80
Subnet Mask:	255.255.255.0
Default Gateway:	172.16.20.20
Primary DNS:	8.8.8.8
Secondary DNS:	3.3.3.3
MAC Address:	[REDACTED]

Descrierea parametrului

Parametru	Descriere
Connection Type (Tip conexiune)	Specifică tipul de conexiune IPv4 al portului WAN. Fie este IP dinamic, static sau PPPoE.
Connection Status (Starea conexiunii)	Specifică starea conexiunii la internet a portului WAN.
Connection Duration (Conexiune Duration)	Specifică durata de când ruterul este conectat la internet.
IP address (Adresa IP)	Specifică adresa IP WAN a ruterului.
Subnet Mask (Masca de subrețea)	Specifică masca de subrețea WAN a ruterului.
Default Gateway (Gateway implicit)	Specifică adresa IP a gateway-ului la care ruterul se conectează.
Primary DNS (DNS primar)	Specifică adresa IP a serverelor DNS primare și secundare oferite ruterului.
Secondary DNS (DNS secundar)	
MAC Address (Adresa MAC)	Specifică adresa MAC WAN a ruterului.

11.10.3 Stare LAN

În această secțiune, puteți vizualiza informații, cum ar fi adresa IPv4, masca de subrețea și adresa MAC pentru ruter, dar din rețeaua locală (internă).

LAN Status
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
MAC Address: <input type="text"/>

Descrierea parametrului

Parametru	Descriere
IP Address (Adresa IP)	Specifică adresa IP locală (LAN) a ruterului.
Subnet Mask (Masca de subrețea)	Specifică masca de subrețea LAN a ruterului.
MAC Address (Adresa MAC)	Specifică adresa MAC LAN a ruterului.

11.10.4 Stare Wi-Fi

În această secțiune, puteți vizualiza informațiile rețelelor Wi-Fi de 2,4 GHz și 5 GHz, inclusiv starea conexiunii, vizibilitatea, numele și modul de criptare și așa mai departe.

Wi-Fi Status

2.4 GHz Wi-Fi Network: Visible

2.4 GHz Wi-Fi Name: Tenda_F5E8B0

Encryption Mode: None

Channel:

Bandwidth: 20

MAC Address:

5 GHz Wi-Fi Network: Visible

5 GHz Wi-Fi Name: Tenda_F5E8B0

Encryption Mode: None

Channel:

Bandwidth: 80

MAC Address:

Descrierea parametrului

Parametru	Descriere
2.4 GHz Wi-Fi Network (Rețea Wi-Fi de 2,4 GHz)	Se specifică dacă rețeaua Wi-Fi corespunzătoare este activată sau dezactivată și vizibilitatea rețelei Wi-Fi.
5 GHz Wi-Fi Network (Rețea Wi-Fi de 5 GHz)	
2.4 GHz Wi-Fi Name (Nume Wi-Fi 2,4 GHz)	Se specifică numele Wi-Fi de 2,4 GHz și pe 5 GHz emise de ruter.
5 GHz Wi-Fi Name (Nume Wi-Fi 5 GHz)	
Encryption Mode (Mod de criptare)	Specifică modul de criptare al rețelei Wi-Fi respective.
Channel (Canal)	Specifică canalul în care funcționează rețeaua Wi-Fi respectivă.

Parametru	Descriere
Bandwidth (Lățimea de bandă)	Specifică lățimea canalului a rețelei Wi-Fi respective.
MAC Address (Adresa MAC)	Specifică adresa MAC a rețelei Wi-Fi respective.

11.10.5 Stare IPv6

Această secțiune este afișată numai când funcția IPv6 este activată. Puteți vizualiza informațiile conexiunii IPv6, inclusiv tipul conexiunii, adresa IPv6 WAN și adresa IPv6 LAN.

IPv6 Status	
Connection Type:	DHCPv6
IPv6 WAN Address:	2408:805f:e206:23a3:78ed:cbff:fe25:1627/64 fe80::78ed:cbff:fe25:1627/64 fe80::522b:73ff:fe5:e8b9/64
Default IPv6 Gateway:	fe80::50b3:fff7:3ee5:8840
Primary IPv6 DNS:	2408:805d:8::
Secondary IPv6 DNS:	2408:805c:4008::
IPv6 LAN Address:	fec0::522b:73ff:fe5:e8b0/64 fe80::522b:73ff:fe5:e8b0/64

Descrierea parametrului

Parametru	Descriere
Connection Type (Tip conexiune)	Specifică tipul de conexiune IPv6 a ruterului.
IPv6 WAN Address (Adresă WAN IPv6)	Specifică adresa IPv6 WAN a ruterului. După ce funcția IPv6 este configurată, portul WAN al ruterului obține o adresă IPv6 unicast globală sau o adresă de tunel.
Default IPv6 Gateway (Gateway IPv6 implicit)	Specifică adresa serverului DNS principal al rețelei IPv6.
Primary IPv6 DNS (DNS IPv6 primar)	
Secondary IPv6 DNS (DNS IPv6 secundar)	Specifică adresa serverului DNS principal și secundar al rețelei IPv6.

Parametru	Descriere
IPv6 LAN Address (Adresă LAN IPv6)	Specifică adresa IPv6 LAN (rețea locală) a ruterului. După ce funcția IPv6 este configurată, portul LAN al ruterului obține o adresă IPv6 unicast globală sau o adresă de tunel și o adresă locală de legătură.

11.11 Jurnal de sistem

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > System Log (Jurnal de sistem)**.

Această funcție înregistrează toate evenimentele cheie care apar după pornirea ruterului. Dacă întâmpinați o eroare în rețea, puteți apela la jurnalele de sistem pentru a afla care este cauza problemei.

Dacă este necesar, puteți, de asemenea, să exportați jurnalele de sistem pe computerul dvs. local făcând clic pe **Export**.

System Log ×

Note: If the router is not connected to the internet, the default logging time is 2000-X-X XX:XX:XX.

Number	Time	Type	Log Content
1	2020-01-03 15:20:11	system	WiFi Configuration Start
2	2020-01-03 15:20:01	system	2.4G MAIN WIFI UP
3	2020-01-03 15:19:59	system	WiFi Basic Set
4	2020-01-03 15:19:57	system	WiFi Configuration Start
5	2020-01-03 15:19:51	system	WiFi Basic Set
6	2020-01-03 15:19:17	system	WiFi Configuration Start
7	2020-01-03 15:19:16	system	2.4G MAIN WIFI DOWN
8	2020-01-03 15:19:15	system	WiFi Basic Set
9	2020-01-03 15:19:03	system	LAN1 up
10	2020-01-03 15:16:06	system	LAN1 down

Export << < > >>



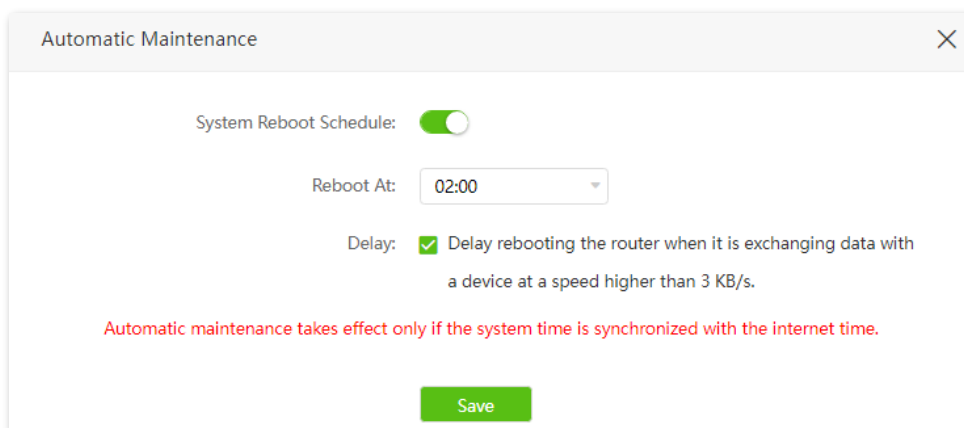
TIP

Repornirea ruterului va șterge toate jurnalele de sistem anterioare.

11.12 Întreținere și repornire automată


O întreținere automată vă permite să reporniți în mod regulat ruterul. Ajută la îmbunătățirea stabilității și a duratei de viață a ruterului dar și evitarea erorilor în buclă. Această funcție este activată implicit.

Pentru a accesa pagina, [conectați-vă la interfața web a ruterului](#) și navigați la **System Settings (Setări de sistem) > Automatic Maintenance (Întreținere automată)**.



Descrierea parametrului

Parametru	Descriere
System Reboot Schedule (Programul de repornire a sistemului)	Folosit pentru a activa sau dezactiva funcția de repornire automată.
Reboot At (Reporniți la)	Specifică ora la care ruterul repornește automat în fiecare zi.
Delay (Întârziere)	<p>Folosit pentru a activa sau dezactiva funcția de întârziere.</p> <ul style="list-style-type: none">- Bifat: funcția este activată. Când se apropie timpul de repornire, dacă există un utilizator conectat la router și traficul prin portul WAN al ruterului depășește 3 KB/s în 30 de minute, ruterul va întârzi repornirea. Dacă există un utilizator conectat la router și traficul prin portul WAN nu depășește 3 KB/s în 30 de minute sau nu există niciun utilizator conectat la router și traficul prin portul WAN al ruterului este mai lent de 3 KB/ În decurs de 3 minute, ruterul se va reporni automat.- Debifat: funcția este dezactivată. Ruterul repornește la ora setată.


 **TIP**

Când funcția de programare a repornirii sistemului este activată, ruterul detectează continuu traficul prin portul WAN în decurs de 2 ore de la ora de repornire specificată și repornește când este îndeplinită cerințele de trafic.

Anexe

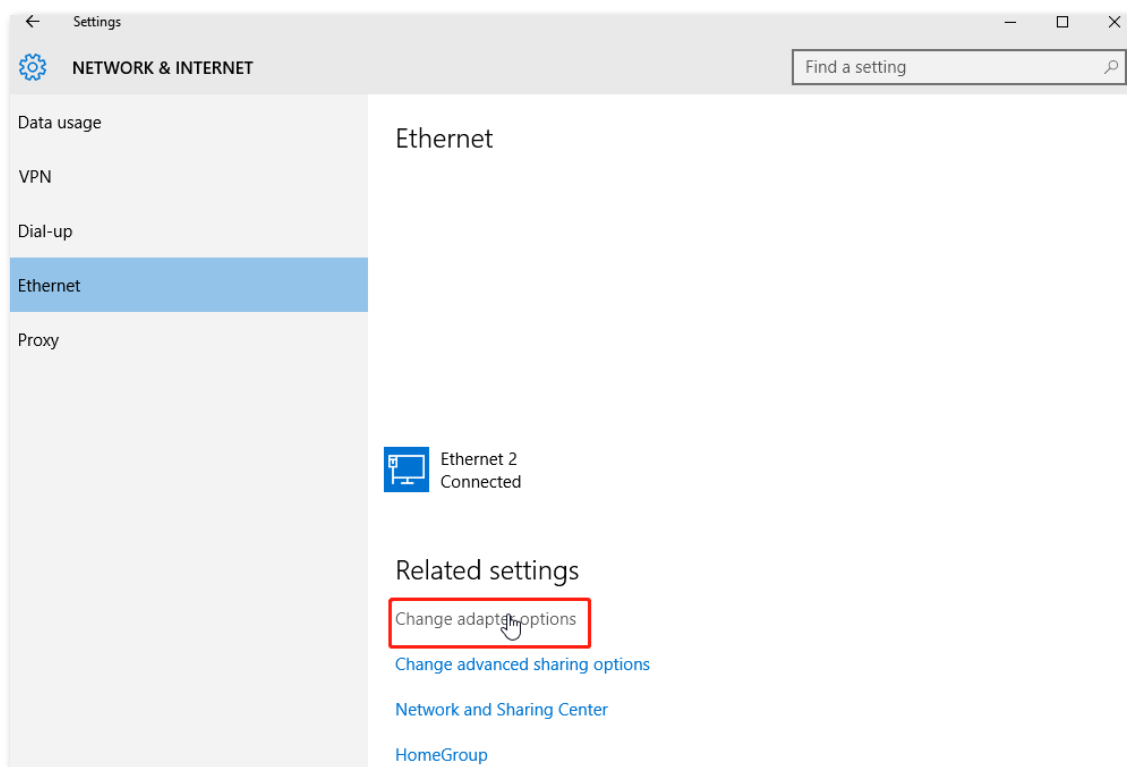
A.1 Configurarea computerului pentru a obține automat o adresă IPv4

Sistemul de operare **Windows 10** de la Microsoft este folosit pentru ilustrare. Un computer cu un adaptor de rețea cu fir este folosit ca exemplu pentru a descrie procedurile. Procedurile pentru configurarea computerelor instalate cu un adaptor de rețea Wi-Fi sunt similare.

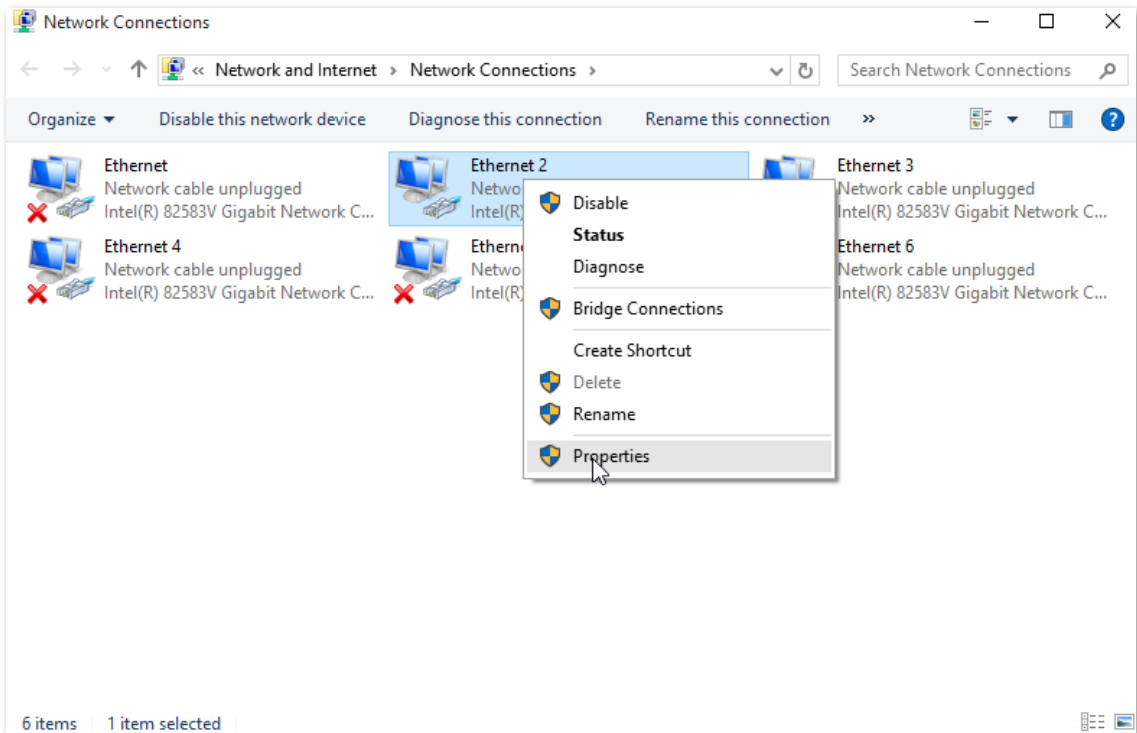
1. Faceți clic pe  în colțul din dreapta jos al desktopului și alegeți **Network settings (Setări de rețea)**.



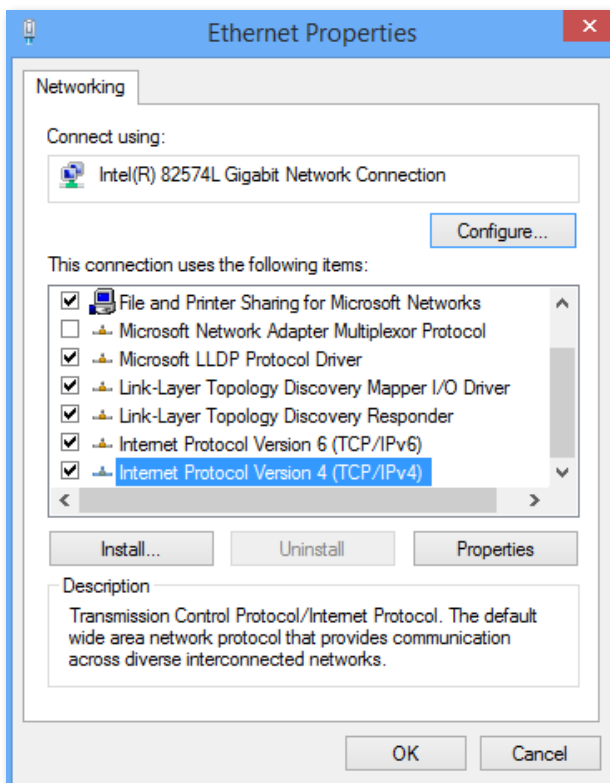
2. Faceți clic pe **Change adapter options (Schimbați opțiunile adaptorului)**.



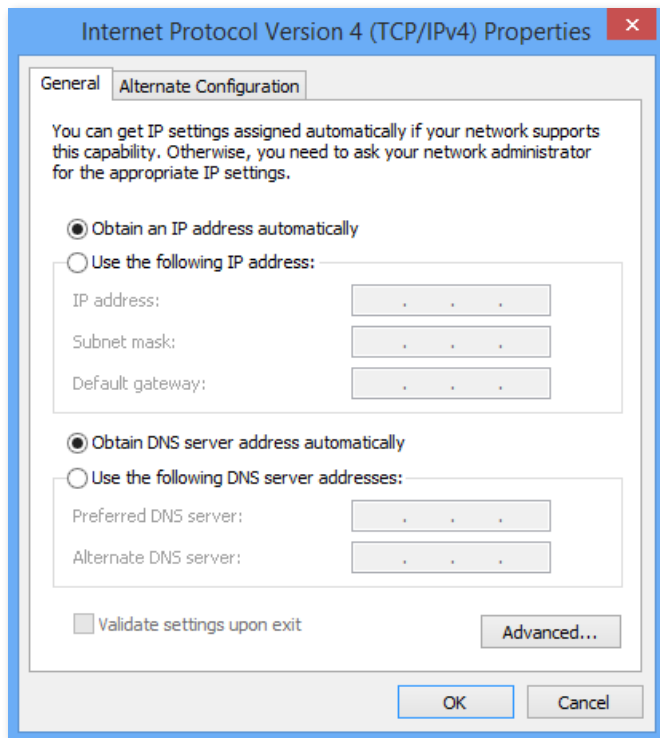
3. Faceți clic dreapta pe conexiunea care este conectată, apoi faceți clic pe **Properties (Proprietăți)**.



4. Faceți dublu clic pe **Internet Protocol Version 4 (TCP/IPv4)**.



5. Selectați **Obtain an IP address automatically (Obține automat o adresă IP)** și **Obtain DNS server address automatically (Obține automat adresa serverului DNS)** și faceți clic pe **OK**.



6. Faceți clic pe **Close (Închidere)** în fereastra **Ethernet Properties (Proprietăți Ethernet)**.

---Sfârșit

A.2 Acronime și abrevieri

Acronim sau abreviere	Denumire completă și explicare
AES	AES (Advanced Encryption Standard) este un algoritm de criptare simetrică utilizat pentru a securiza datele
BR	BR (Border Relay) sau releu de frontieră este un dispozitiv de rețea care funcționează la marginea (frontiera) unei rețele, permițând comunicarea între rețele diferite. Acesta poate media traficul între rețele locale și rețele externe sau între rețele private și internet. În funcție de configurație, releul de frontieră poate gestiona traducerea adreselor IP (NAT), rutarea pachetelor, securitatea traficului și alte funcții de interconectare între diferite tipuri de rețele sau segmente de rețea.
CE	CE (Customer Edge) sau marginea clientului reprezintă echipamentul de rețea situat la granița rețelei unui client, conectând rețeaua privată a acestuia cu rețeaua furnizorului de servicii (ISP sau provider de rețea). Dispozitivele CE sunt, de obicei, routere sau switch-uri gestionate de client și sunt responsabile pentru interfațarea cu rețeaua furnizorului, printr-un echipament de tip PE (Provider Edge) situat pe marginea rețelei providerului.
DDNS	DDNS (Dynamic Domain Name System) este un serviciu care actualizează automat înregistrările DNS ale unui nume de domeniu atunci când adresa IP asociată acestuia se schimbă.
DHCP	DHCP (Dynamic Host Configuration Protocol) este un protocol de rețea care alocă automat adrese IP și alte configurații de rețea dispozitivelor dintr-o rețea, permițându-le să comunice eficient. Atunci când un dispozitiv se conectează la rețea, serverul DHCP îi atribuie automat o adresă IP, gateway-ul implicit, adresa serverului DNS și alte informații necesare pentru a se conecta la internet sau la alte dispozitive din rețea, fără ca utilizatorul să configureze manual aceste setări.
DMZ	DMZ (Demilitarized Zone) este o zonă separată într-o rețea de calculatoare care adaugă un nivel suplimentar de securitate între rețeaua internă și internet. DMZ găzduiește servere sau servicii publice (cum ar fi servere web, de e-mail sau FTP), izolându-le de rețeaua internă protejată.
DNS	DNS (Domain Name System) este un sistem care traduce numele de domenii ușor de utilizat în adrese IP, permițând astfel accesarea resurselor de pe internet.
GMT	GMT (Greenwich Mean Time) este un standard de timp care reprezintă ora medie la Observatorul Regal de la Greenwich, în Londra, și servește drept referință pentru fuserile orare din întreaga lume.
IKE	IKE (Internet Key Exchange) este un protocol folosit pentru a negocia și stabili parametrii de securitate, inclusiv autentificarea și schimbul de chei, între două entități care doresc să comunice securizat prin intermediul rețelelor.

Acronim sau abreviere	Denumire completă și explicare
IP	IP (Internet Protocol) este un protocol fundamental care reglează modul în care datele sunt transmise prin rețelele de calculatoare, inclusiv internetul, și se ocupă de adresarea și rutarea pachetelor de date între dispozitive. Există două versiuni principale ale IP: IPv4, care folosește adrese de 32 de biți (ex: 192.168.1.1), și IPv6, care folosește adrese de 128 de biți pentru a permite un număr mai mare de adrese unice.
IPTV	IPTV (Internet Protocol Television) este o tehnologie care permite livrarea de programe de televiziune și conținut video prin intermediul internetului, în loc de metodele tradiționale, cum ar fi cablul sau satelitul. IPTV folosește protocoale de rețea pentru a transmite fluxuri video, permițând utilizatorilor să vizioneze emisiuni live, să acceseze filme la cerere și să utilizeze servicii interactive, toate prin intermediul unei conexiuni broadband.
IPv4	Internet Protocol Versiunea 4
IPv6	Internet Protocol Versiunea 6
ISP	ISP (Internet Service Provider) este o companie sau organizație care oferă acces la internet și servicii asociate. ISP-urile pot oferi conexiuni de internet prin diverse tehnologii, inclusiv linii telefonice, cablu, fibră optică sau satelit, și sunt esențiale pentru conectarea utilizatorilor finali la rețeaua globală a internetului.
L2TP	L2TP (Layer 2 Tunneling Protocol) este un protocol de tunelare utilizat pentru a crea conexiuni securizate între două puncte pe internet, permițând transportul datelor prin intermediul unor rețele necontrolate. L2TP nu oferă criptare sau autentificare de sine stătătoare, dar este adesea combinat cu protocoale de securitate, cum ar fi IPsec, pentru a asigura confidențialitatea și integritatea datelor. Acest protocol este utilizat frecvent în rețelele VPN (Virtual Private Network) pentru a permite utilizatorilor să acceseze rețele private prin conexiuni publice.
LAN	LAN (Local Area Network) este o rețea locală de dispozitive care acoperă o zonă limitată, internă, cum ar fi o clădire, un birou sau un campus, și permite conectarea dispozitivelor, precum calculatoare, imprimante și servere, pentru a partaja resurse și a comunica între ele.
MAC	MAC (Media Access Control) se referă la o adresă unică atribuită fiecărui adaptor de rețea care utilizează protocoale de comunicație la nivelul legăturii de date, precum plăci Ethernet sau Wi-Fi. Această adresă, formată din 48 de biți, este utilizată pentru a identifica în mod unic un dispozitiv într-o rețea locală (LAN) și este esențială pentru gestionarea comunicării între dispozitivele conectate.

Acronim sau abreviere	Denumire completă și explicare
MTU	<p>MTU (Maximum Transmission Unit) este dimensiunea maximă a unui pachet de date care poate fi transmis printr-o rețea sau un protocol de comunicație specificat, fără a fi fragmentat. De obicei, MTU este exprimată în octeți și poate varia în funcție de tehnologia utilizată; de exemplu, valoarea standard pentru Ethernet este de 1500 de octeți. Stabilirea unei valori adecvate a MTU este importantă pentru a optimiza performanța rețelei, deoarece o MTU prea mică poate duce la o creștere a numărului de pachete și, implicit, la o utilizare mai mare a resurselor de rețea, în timp ce o MTU prea mare poate provoca probleme de fragmentare a datelor și întârzieri în transmisie.</p>
PIN	<p>PIN (Personal Identification Number) este un cod numeric utilizat pentru a autentifica utilizatorii și pentru a proteja accesul la conturi, dispozitive sau servicii, cum ar fi cardurile de credit, telefoanele mobile sau aplicațiile online. De obicei, un PIN are între 4 și 6 cifre, dar poate fi mai lung, și este ales de utilizator pentru a asigura un nivel de securitate. Utilizarea unui PIN ajută la prevenirea accesului neautorizat și la protejarea informațiilor personale.</p>
PPPoE	<p>PPPoE (Point-to-Point Protocol over Ethernet) este un protocol de rețea care combină caracteristicile PPP (Point-to-Point Protocol) cu Ethernet, permițând conectarea dispozitivelor de la utilizatori finali la un ISP (Internet Service Provider) prin intermediul unei conexiuni Ethernet. PPPoE este utilizat frecvent în rețelele DSL (Digital Subscriber Line) și facilitează autentificarea utilizatorilor printr-un nume de utilizator și o parolă, gestionând și controlând conexiunea la internet. De asemenea, acest protocol permite crearea de sesiuni separate pentru utilizatori, oferind funcționalități precum autentificarea, criptarea și compresia datelor.</p>
PPTP	<p>PPTP (Point-to-Point Tunneling Protocol) este un protocol de tunelare utilizat pentru a crea conexiuni VPN (Virtual Private Network) între un client și un server, permițând utilizatorilor să acceseze rețele private prin internet. PPTP funcționează prin encapsularea datelor PPP (Point-to-Point Protocol) în pachete IP, facilitând astfel transportul acestora prin rețelele publice. Deși PPTP este ușor de configurat și oferă viteze rapide, este considerat mai puțin sigur comparativ cu alte protocoale VPN moderne, deoarece utilizează metode de criptare care pot fi vulnerabile la atacuri. Din acest motiv, utilizatorii care prioritizează securitatea sunt adesea sfătuiți să opteze pentru protocoale mai avansate, cum ar fi L2TP, IPSec sau OpenVPN.</p>
PUK	<p>PUK (Personal Unblocking Key) este un cod numeric utilizat pentru deblocarea unui telefon mobil sau a unui card SIM după ce acesta a fost blocat din cauza introducerii incorecte repetate a codului PIN (Personal Identification Number). PUK-ul este de obicei format din 8 cifre și este furnizat de operatorul de telecomunicații atunci când utilizatorul achiziționează un card SIM. Utilizatorii trebuie să introducă corect PUK-ul pentru a debloca SIM-ul și a restabili accesul la serviciile de telefonie mobilă. Dacă PUK-ul este introdus incorect de mai multe ori, cardul SIM poate fi blocat permanent, necesitând înlocuirea acestuia.</p>

Acronim sau abreviere	Denumire completă și explicare
SIM	<p>SIM (Subscriber Identity Module) este un microcip utilizat în telefoanele mobile și alte dispozitive conectate la rețelele de telecomunicații pentru a stoca informații esențiale despre abonat, inclusiv numărul de telefon, datele de autentificare și informațiile de rețea. SIM-ul permite utilizatorului să se conecteze la rețeaua mobilă a operatorului, permițând efectuarea de apeluri, trimiterea de mesaje text și accesul la internet. Există mai multe tipuri de SIM-uri, inclusiv SIM-uri standard, mini-SIM, micro-SIM și nano-SIM, care diferă în dimensiune și formă. De asemenea, există SIM-uri virtuale (eSIM) care nu necesită un suport fizic și sunt integrate direct în dispozitive. SIM-urile contribuie la securitatea rețelei, având caracteristici de criptare pentru a proteja datele utilizatorului.</p>
SMS	<p>SMS (Short Message Service) este un serviciu de comunicație care permite trimiterea și primirea de mesaje text scurte între telefoane mobile și alte dispozitive compatibile. Un mesaj SMS poate avea o lungime de până la 160 de caractere, deși mesajele mai lungi sunt împărțite în mai multe părți. SMS-ul este utilizat pe scară largă pentru comunicarea rapidă și eficientă, permițând utilizatorilor să transmită mesaje instantanee fără a fi nevoie de o conexiune de internet. De asemenea, este folosit pentru notificări, alerte, servicii de autentificare în doi pași dar și comunicări de marketing.</p>
SSID	<p>SSID (Service Set Identifier) este un nume unic care identifică o rețea wireless (Wi-Fi) și permite utilizatorilor să o găsească și să se conecteze la ea. SSID-ul poate conține până la 32 de caractere și este transmis de ruterul wireless în timpul scannării rețelei, astfel încât dispozitivele să îl poată recunoaște.</p>
TCP	<p>TCP (Transmission Control Protocol) este un protocol de comunicație fundamental în cadrul suitei de protocoale internet (Internet Protocol Suite) care asigură transferul fiabil de date între dispozitive pe rețea. TCP oferă următoarele caracteristici cheie:</p> <ul style="list-style-type: none"> • Garantează livrarea pachetelor de date prin retransmiterea acestora în cazul în care nu sunt primite sau sunt corupte. • Reglează rata de transmitere a datelor între sursă și destinație pentru a preveni supraîncărcarea rețelei. • Monitorizează starea rețelei și ajustează rata de trimitere a datelor pentru a minimiza congestia. • Împarte mesajele mari în segmente mai mici, facilitând transmiterea acestora prin rețea. • Asigură că pachetele sunt reconstituite în ordinea corectă la destinație, chiar dacă sunt primite într-o ordine diferită. <p>Datorită acestor caracteristici, TCP este utilizat pe scară largă în aplicații care necesită o livrare fiabilă a datelor, cum ar fi navigarea pe internet, e-mailul și transferurile de fișiere.</p>

Acronim sau abreviere	Denumire completă și explicare
UDP	<p>UDP (User Datagram Protocol) este un protocol de comunicație din cadrul suitei de protocoale internet (Internet Protocol Suite) care permite transmiterea rapidă de date între dispozitive, fără a oferi garanții de livrare sau de ordine a pachetelor. UDP are următoarele caracteristici principale:</p> <ul style="list-style-type: none"> • UDP nu stabilește o conexiune între sursă și destinație înainte de a trimite datele, ceea ce îl face mai rapid decât TCP. • UDP nu asigură că pachetele de date ajung la destinație; pachetele pot fi pierdute sau deteriorate fără a fi retransmise. • UDP nu reglează rata de trimitere a datelor, ceea ce înseamnă că poate provoca congestiunea rețelei. • UDP împarte datele în unități numite "datagramuri", care sunt transmise independent unele de altele. • Datorită lipsei caracteristicilor de fiabilitate, UDP este adesea folosit în aplicații care necesită o latență scăzută și unde pierderea unor pachete nu este critică, cum ar fi streamingul video, jocurile online și apelurile VoIP. <p>În general, UDP este preferat în situațiile în care viteza și eficiența sunt mai importante decât fiabilitatea completă a livrării datelor.</p>
UPnP	<p>UPnP (Universal Plug and Play) este un set de protocoale care permite dispozitivelor conectate la rețea să se descopere și să comunice între ele automat, facilitând configurarea și utilizarea serviciilor de rețea fără intervenție manuală.</p>
USSD	<p>USSD (Unstructured Supplementary Service Data) este un protocol de comunicație utilizat în rețelele mobile pentru a permite interacțiuni în timp real între utilizatori și serviciile de rețea, fără a necesita o conexiune de date. USSD este adesea folosit pentru a accesa servicii precum verificarea soldului contului, reîncărcarea creditului, activarea sau dezactivarea serviciilor și alte aplicații bazate pe text, prin intermediul unor coduri scurte (de obicei în formatul *123#). Aceste interacțiuni sunt rapide și se desfășoară în timp real, oferind utilizatorilor un mod simplu și eficient de a accesa informații și servicii.</p>
WAN	<p>WAN (Wide Area Network) este o rețea de calculatoare care acoperă o zonă geografică extinsă, cum ar fi orașe, țări sau chiar continente, și permite conectarea mai multor rețele locale (LAN-uri) între ele. WAN-urile sunt utilizate pentru a facilita comunicarea și schimbul de date între organizații, sucursale sau utilizatori care se află la distanțe mari. Aceste rețele folosesc diferite tehnologii de comunicație, cum ar fi linii dedicate, conexiuni prin satelit, fibra optică sau rețele mobile, și sunt esențiale pentru suportul aplicațiilor de afaceri, colaborare și acces la internet la scară largă.</p>

Acronim sau abreviere	Denumire completă și explicare
WISP	<p>WISP (Wireless Internet Service Provider) este un furnizor de servicii de internet care utilizează tehnologia wireless pentru a oferi acces la internet utilizatorilor finali, de obicei în zone rurale sau greu accesibile, unde infrastructura tradițională de cablu sau fibră optică nu este disponibilă sau este costisitoare de implementat. WISP-urile folosesc echipamente wireless, cum ar fi antene și routere, pentru a transmite semnale de internet de la un punct de acces centralizat către clienți, care pot fi case sau afaceri.</p> <p>WISP se folosește și pentru denumirea modului de rutare cu conectare la rețeaua externă/ISP prin Wi-Fi și nu prin cablu cum se furnizează în majoritatea cazurilor.</p>
WPA-PSK	<p>WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) este un protocol de securitate pentru rețelele wireless care utilizează o cheie pre-partajată (PSK) pentru autentificare și criptarea datelor transmise între dispozitive. WPA-PSK este o soluție accesibilă și eficientă pentru protejarea rețelelor Wi-Fi, deoarece permite utilizatorilor să seteze o parolă care este utilizată pentru a conecta dispozitivele la rețea.</p>