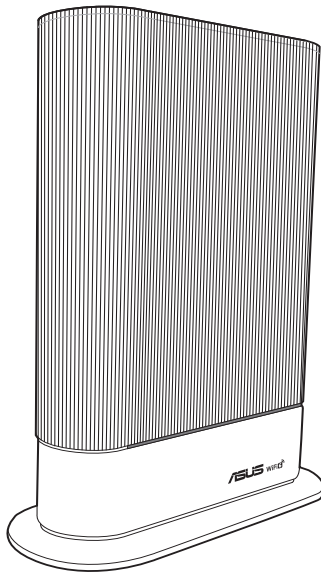


Guia de l'usuari

RT-AX59U

Encaminador Wi-Fi de banda dual



CL22545

Primera edició

Octubre de 2023

Copyright © 2023 ASUSTeK Computer Inc. Tots els drets reservats.

No es permet reproduir, transmetre, transcriure, emmagatzemar en un sistema de recuperació ni traduir a un altre idioma de cap manera ni per cap mitjà cap part d'aquest manual, incloent-hi els productes i el software que s'hi descriuen, excepte la documentació que el comprador conserva com a còpia de seguretat, sense el permís per escrit explícit d'ASUSTek Computer Inc. ("ASUS").

La garantia o servei del producte no s'estendrà si: (1) el producte es repara, es modifica o s'altera, a no ser que aquesta reparació, modificació o alteració hagi estat autoritzada per escrit per ASUS, o (2) el número de sèrie del producte s'ha alterat o esborrat del tot.

ASUS PROPORCIONA AQUEST MANUAL "TAL QUAL" SENSE CAP TIPUS DE GARANTIA, NI EXPLÍCITA NI IMPLÍCITA; AIXÒ INCLOU, SENSE LIMITAR-S'HI, LES GARANTIES IMPLÍCITES O LES CONDICIONS DE COMERCIALIZACIÓ O D'ADEQUACIÓ A UN PROPÒSIT PARTICULAR. ASUS, ELS SEUS GERENTS, DIRECTIUS, TREBALLADORS I AGENTS NO SERAN MAI RESPONSABLES DE CAP DANY INDIRECTE, ESPECIAL, FORTUÏT O CONSEQÜENT (INCLOENT-HI DANYS PER PÈRDUA DE BENEFICIS, PÈRDUA DE NEGOCI, PÈRDUA D'ÚS O DE DADES, INTERRUPCIÓ DE L'ACTIVITAT COMERCIAL O D'ALTRES TIPUS), FINS I TOT SI S'HA AVISAT A ASUS DE LA POSSIBILITAT DE QUE ES PRODUÏXIN AQUESTS DANYS COM A CONSEQÜÈNCIA D'UN DEFECTE O D'UN ERROR AL MANUAL O AL PRODUCTE.

LES ESPECIFICACIONS I LA INFORMACIÓ D'AQUEST MANUAL S'OFEREIXEN ÚNICAMENT AMB FINALITAT INFORMATIVA, PODEN INTRODUIR-S'HI CANVIS EN QUALSEVOL MOMENT SENSE AVISAR I NO HAN D'INTERPRETAR-SE COM A UN COMPROMÍS PER PART D'ASUS. ASUS NO ASSUMEIX CAP OBLIGACIÓ NI CAP RESPONSABILITAT PELS ERRORS O LES IMPRECISSIONS QUE PUGUIN HAVER-HI EN AQUEST MANUAL, INCLOSOS ELS PRODUCTES I EL SOFTWARE QUE S'HI DESCRUIEN.

Els productes i els noms corporatius d'aquest manual poden ser marques comercials registrades o no ser-ho o poden tenir drets de còpia o no tenir-ne i s'utilitzen exclusivament amb finalitats d'identificació o d'explicació i en benefici dels propietaris, sense cap intenció de cometre cap infracció.

Índex

1	Informació sobre el wireless router	
1.1	Benvingut/da!.....	7
1.2	Contingut del paquet	7
1.3	El wireless router	8
1.4	Ubicació del wireless router	10
1.5	Requisits de configuració.....	11
2	Primers passos	
2.1	Configuració del router.....	12
	A. Connexió amb fil	12
	B. Connexió wireless.....	13
2.2	Configuració ràpida d'Internet (QIS) mitjançant la detecció automàtica	15
2.3	Connexió a la xarxa wireless	18
3	Configuració General i Configuració Avançada	
3.1	Inici de sessió a la interfície gràfica (GUI) en línia.....	19
3.2	QoS adaptativa.....	21
3.3	Administració	22
	3.3.1 Mode de funcionament.....	22
	3.3.2 Sistema.....	23
	3.3.3 Actualització del firmware	24
	3.3.4 Restablir/desar/pujar la configuració	25
3.4	AiCloud 2.0	26
	3.4.1 Disc al núvol.....	27
	3.4.2 Accés intel·ligent	29
	3.4.3 Sincronització iCloud.....	30
3.5	AiMesh	31
	3.5.1 Abans de la configuració.....	31
	3.5.2 Passos per a la configuració de l'AiMesh	31
	3.5.3 Solució de problemes.....	34
	3.5.4 Reubicació	35
	3.5.5 Preguntes freqüents (PF)	36

Índex

3.6	AiProtection	37
	3.6.1 Configuració d'Aiprotection.....	38
	3.6.2 Bloqueig de llocs maliciosos.....	40
	3.6.3 IPS bidireccional	41
	3.6.4 Prevenció i bloqueig de dispositius infectats	42
3.7	Firewall	43
	3.7.1 General.....	43
	3.7.2 Filtre d'URL.....	43
	3.7.3 Filtre de paraules clau.....	44
	3.7.4 Filtre de serveis de la xarxa.....	45
3.8	Xarxa per a convidats	46
3.9	IPv6	48
3.10	LAN	49
	3.10.1 IP de LAN.....	49
	3.10.2 Servidor DHCP.....	50
	3.10.3 Encaminament.....	52
	3.10.4 IPTV	53
3.11	Mapa de la xarxa	54
	3.11.1 Configuració dels paràmetres de seguretat wireless	56
	3.11.2 Gestió dels clients de la xarxa.....	57
	3.11.3 Supervisió del dispositiu USB.....	58
3.12	Controls parentals	60
3.13	Smart Connect	63
	3.13.1 Configuració d'Smart Connect.....	63
3.14	Registre del sistema	65
3.15	Analitzador de trànsit	66
3.16	Aplicació USB	68
	3.16.1 Ús de l'AiDisk.....	69
	3.16.2 Ús del Servers Center.....	71
	3.16.3 3G/4G	76

Índex

3.17	VPN.....	77
	3.17.1 Servidor de VPN.....	77
	3.17.2 VPN Fusion.....	78
	3.17.3 Instant Guard.....	79
3.18	WAN.....	80
	3.18.1 Internet Connection (Connexió a Internet).....	80
	3.18.2 WAN dual.....	83
	3.18.3 Activació de ports.....	84
	3.18.4 Servidor virtual/reenviament de port.....	86
	3.18.5 DMZ.....	89
	3.18.6 DDNS.....	90
	3.18.7 Pas NAT.....	91
3.19	Wireless.....	92
	3.19.1 General.....	92
	3.19.2 WPS.....	94
	3.19.3 Bridge.....	96
	3.19.4 Filtre wireless MAC.....	98
	3.19.5 Configuració de RADIUS.....	99
	3.19.6 Professional.....	100
4	Utilitats	
4.1	Device Discovery.....	103
4.2	Firmware Restoration.....	104
4.3	Configuració del servidor d'impresió.....	105
	4.3.1 ASUS EZ Printer Sharing.....	105
	4.3.2 Ús de LPR per compartir impressora.....	109
4.4	Download Master.....	114
	4.4.1 Configuració dels paràmetres de baixada de Bit Torrent.....	115
	4.4.2 Configuració d'NZB.....	116

5	Solució de problemes	
5.1	Solució de problemes bàsics.....	117
5.2	Preguntes freqüents (PF)	119
	Apèndix	
	Servei i assistència tècnica	138

1 Informació sobre el wireless router

1.1 Benvingut/da!

Gràcies per comprar un wireless router ASUS RT-AX59U.

Aquest modern encaminador disposa de banda dual de 2,4 GHz i 5 GHz per a una transmissió en continu d'alta definició sense fil amb una qualitat inigualable; servidor d'SMB, servidor d'AV UPnP i servidor FTP per a ús compartit de fitxers 24/7, ofereix capacitat per a 300 000 sessions i incorpora la tecnologia ASUS Green Network, una solució que permet estalviar fins a un 70 % d'energia.

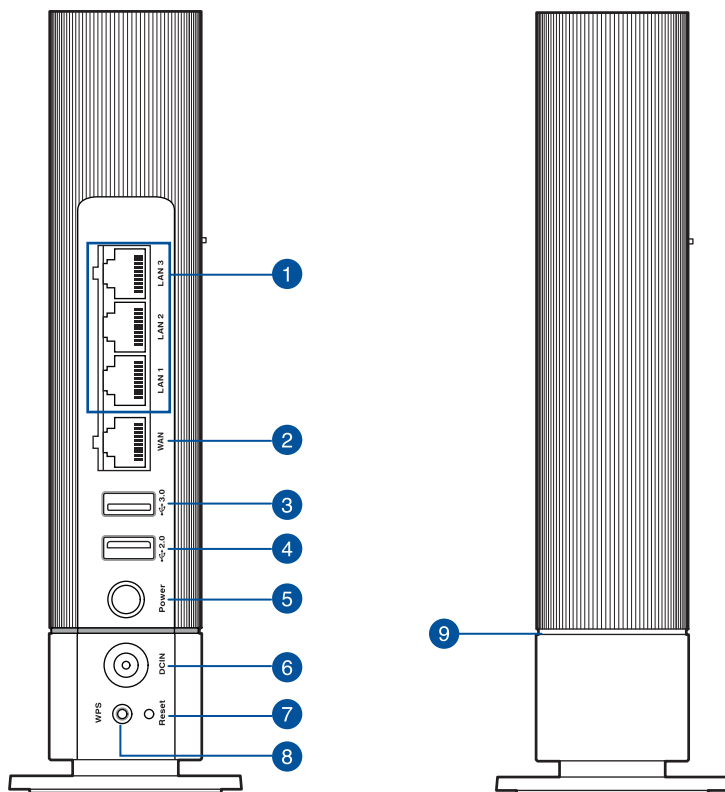
1.2 Contingut del paquet

- | | |
|--|--|
| <input checked="" type="checkbox"/> Wireless router RT-AX59U | <input checked="" type="checkbox"/> Adaptador de CA |
| <input checked="" type="checkbox"/> Cable de xarxa (RJ-45) | <input checked="" type="checkbox"/> Guia d'inici ràpid |

NOTES:

- Si manca cap article o bé en detecteu cap desperfecte, poseu-vos en contacte amb ASUS per obtenir informació i assistència tècnica. Consulteu la llista de telèfons de suport d'ASUS que trobareu al darrere d'aquest manual.
 - Conserveu el material d'emalatge original per si us cal cap reparació o substitució en garantia en el futur.
-

1.3 El wireless router



-
- 1 Ports LAN 1-3**
Connecteu els cables de xarxa en aquests ports per establir una connexió LAN.

 - 2 Port WAN (Internet)**
Connecteu un cable de xarxa en aquest port per establir una connexió WAN.

 - 3 Port USB 3.2 Gen 1**
Introduïu en aquest port un dispositiu compatible amb USB 3.2 Gen 1, com ara un disc dur USB, una unitat flaix USB, un telèfon intel·ligent o una impressora.

 - 4 Port USB 2.0**
Introduïu en aquest port un dispositiu compatible amb USB 2.0, com ara un disc dur USB, una unitat flaix USB, un telèfon intel·ligent o una impressora.
-

-
- 5 Botó d'encendre**
Premeu aquest botó per encendre o apagar el sistema.
-
- 6 Port Power (DCIN)**
Inseriu l'adaptador de CA inclòs en aquest port i connecteu el router a la xarxa elèctrica.
-
- 7 Botó Reset**
Aquest botó reinicialitza o restableix el sistema a la configuració original de fàbrica.
-
- 8 Botó WPS**
Mantingueu premut el botó per iniciar l'assistent WPS.
-
- 9 Indicador LED**
- Blau fix: Podeu començar a configurar l'RT-AX59U
 - Blanc fix: L'RT-AX59U està en línia i funciona correctament
 - Vermell fix: L'RT-AX59U no té connexió a Internet
El node està desconnectat de l'encaminador
 - Groc fix: El senyal entre l'encaminador RT-AX59U i el node és dèbil
-

NOTES:

- Feu servir exclusivament l'adaptador subministrat. L'ús d'altres adaptadors pot malmetre el dispositiu.
- **Especificacions:**

Adaptador l'alimentació de CC	Sortida de CC: +12 V amb corrent de 2,5 A		
Temperatura de funcionament	0~40°C	Emmagatzematge	0~70°C
Humitat de funcionament	50~90%	Emmagatzematge	20~90%

1.4 Ubicació del wireless router

Per a la millor una transmissió wireless òptima entre el wireless router i els dispositius wireless connectats, comproveu que:

- Col·loqueu el wireless router en un lloc centralitzat per aconseguir que tots els dispositius de xarxa tinguin cobertura wireless.
- Manteniu el dispositiu allunyat d'obstacles metàl·lics i de la llum del sol directa.
- Manteniu el dispositiu allunyat de dispositius de Wi-Fi exclusius per a 802.11 g o 20 MHz, perifèrics d'ordinador de 2,4 GHz, dispositius Bluetooth, telèfons wireless, transformadors, motors d'alt rendiment, llums fluorescents, forns microones, neveres i altres equips industrials per evitar interferències o interrupcions del senyal.
- Actualitzeu-lo sempre al firmware més recent. Visiteu el web d'ASUS a <http://www.asus.com> per obtenir les darreres actualitzacions del firmware.
- Per garantir el millor senyal sense fil, orienteu les quatre antenes extraïbles tal com veieu al diagrama inferior.



1.5 Requisits de configuració

Per configurar la xarxa wireless, necessiteu un ordinador amb les característiques del sistema següents:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Capacitat wireless IEEE 802.11 a/b/g/n/ac/ax
- Un servei de TCP/IP instal·lat
- Navegador web, com ara: Internet Explorer, Firefox, Safari o Google Chrome

NOTES:

- Si l'ordinador no té capacitats integrades de funcionament wireless, instal·leu un adaptador de WLAN IEEE 802.11 a/b/g/n/ac/ax a l'ordinador per connectar-lo a la xarxa.
- Amb aquesta tecnologia de dual banda, el wireless router admet simultàniament senyals wireless de 2,4 GHz i 5 GHz. Això us permet fer activitats que demanin l'ús d'Internet, com ara navegar o fer servir el correu electrònic amb la banda de 2,4 GHz i, simultàniament, transmetre en streaming fitxers d'àudio i vídeo en alta definició, com ara pel·lícules o música, amb la banda de 5 GHz.
- No tots els dispositius IEEE 802.11n que voleu connectar a la xarxa són compatibles amb la banda de 5 GHz. Consulteu el manual del dispositiu per veure'n les especificacions.
- Els cables Ethernet RJ-45 que utilitzeu per connectar els dispositius de xarxa no han de superar els 100 metres.

IMPORTANT!

- Alguns adaptadors wireless poden tenir problemes de connectivitat a AP Wi-Fi 802.11ax.
- En aquest cas, haureu d'actualitzar el controlador a la versió més recent. Consulteu el lloc web de suport oficial del fabricant per obtenir controladors de software, actualitzacions i altra informació relacionada.
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/>

2 Primers passos

2.1 Configuració del router

IMPORTANT!

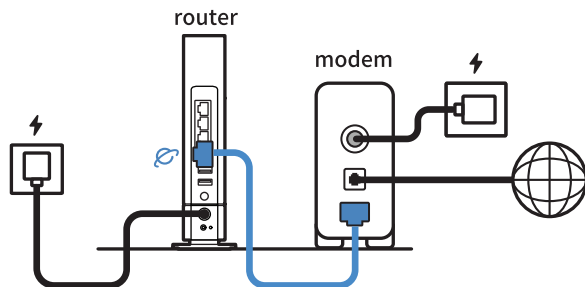
- Utilitzeu una connexió amb fil quan configureu el wireless router per evitar possibles problemes de configuració.
 - Abans de configurar el wireless router ASUS, seguiu aquestes instruccions:
 - Si substituïu un router existent, desconnecteu-lo de la xarxa.
 - Desconnecteu els cables/fils del mòdem que feu servir en aquest moment. Si el mòdem té una bateria auxiliar, traieu-la.
 - Reinicieu el mòdem per cable i l'ordinador (recomanat).
-

A. Connexió amb fil

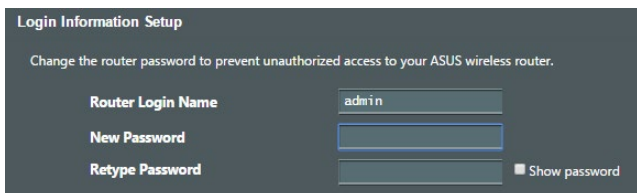
NOTA: Podeu utilitzar un cable pla o un cable trenat per a la connexió amb fil.

Per configurar el wireless router mitjançant una connexió amb fil.

1. Prepareu l'encaminador d'ASUS i engegueu-lo.



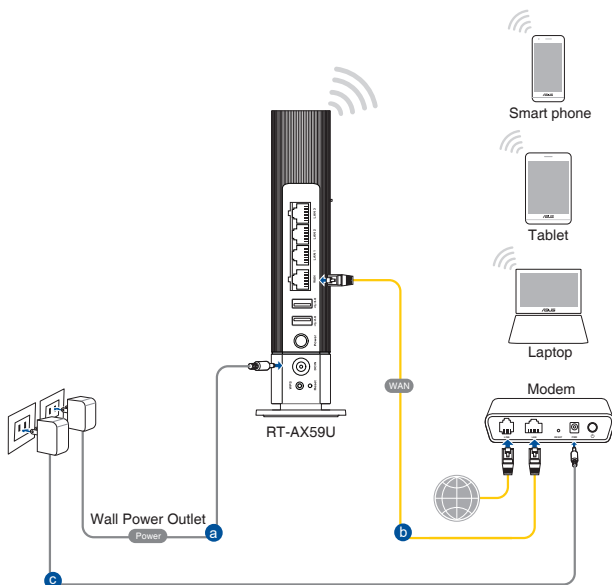
2. La interfície gràfica (GUI) en línia s'inicia automàticament en obrir un navegador web. Si no s'inicia automàticament, introduïu <http://www.asusrouter.com>.
3. Configureu una contrasenya per evitar accessos no autoritzats al router.



B. Connexió wireless

Per configurar el wireless router mitjançant una connexió wireless:

1. Endolleu el router a una presa de corrent i enceneu-lo.



2. Connecteu-vos al nom de la xarxa (SSID) que apareix a l'etiqueta del producte que trobareu a la part de darrere del router. Per millorar la seguretat de la xarxa, canvieu a un SSID únic i assigneu una contrasenya.



Nom de Wi-Fi (SSID): ASUS_XX

* **XX** es refereix als dos últims díigits de l'adreça MAC de 2,4 GHz. La trobareu a l'etiqueta del darrere del ASUS router.

3. En establir la connexió, la interfície gràfica (GUI) en línia s'inicia automàticament en obrir un navegació web. Si no s'inicia automàticament, introduïu <http://www.asusrouter.com>.
4. Configureu una contrasenya per evitar accessos no autoritzats al router.

NOTES:

- Per obtenir més informació sobre la connexió a una xarxa wireless, consulteu el manual de l'usuari de l'adaptador WLAN.
- Per configurar els paràmetres de seguretat de la xarxa, consulteu l'apartat **3 Configuració dels paràmetres de seguretat wireless** d'aquest manual d'usuari.

Login Information Setup

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

Router Login Name: admin

New Password: [Empty field]

Retype Password: [Empty field] Show password

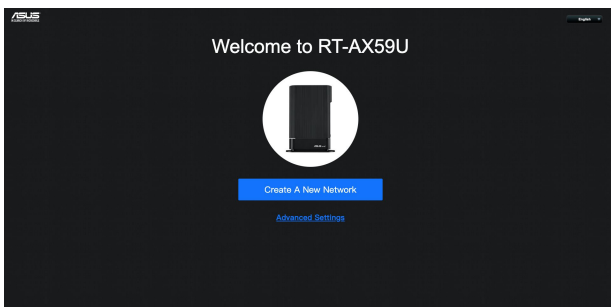
2.2 Configuració ràpida d'Internet (QIS) mitjançant la detecció automàtica

La funció de Configuració ràpida d'Internet (Quick Internet Setup, QIS) permet una configuració ràpida de la connexió a Internet.

NOTA: Quan configureu la connexió a Internet per primera vegada, premeu el botó Reset del wireless router per restablir-ne la configuració predeterminada.

Per utilitzar la funció QIS amb detecció automàtica:

1. Obriu un navegador web. S'hauria d'obrir l'assistent de configuració d'ASUS (configuració ràpida d'Internet). Si no s'obre, introduïu <http://www.asusrouter.com> manualment.

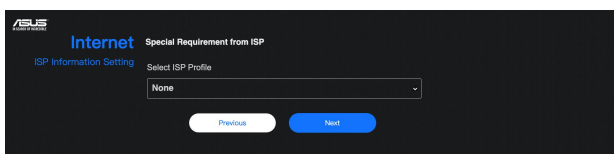
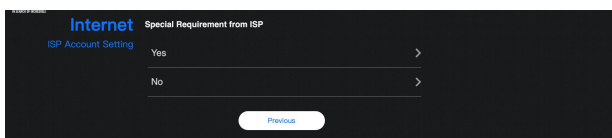


2. El wireless router detecta automàticament si el tipus de connexió del proveïdor de serveis d'Internet (ISP) és **IP dinàmic, PPPoE, PPTP i L2TP**. Introduïu la informació necessària per al tipus de connexió del proveïdor de serveis d'Internet (ISP).

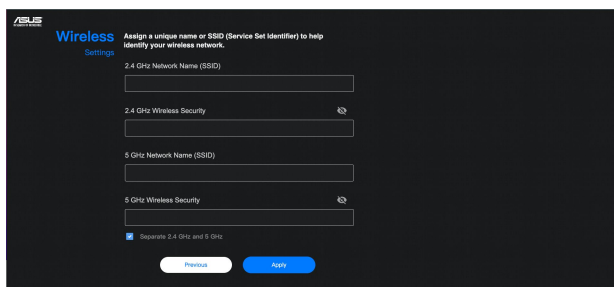
IMPORTANT! Demaneu la informació necessària sobre el tipus de connexió a Internet al vostre proveïdor de serveis d'Internet (ISP).

NOTES:

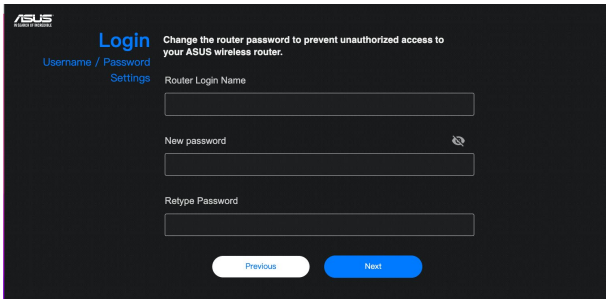
- La detecció automàtica del tipus de connexió del proveïdor de serveis d'Internet (ISP) es produeix quan es configura el wireless router per primera vegada o quan es restableixen els paràmetres predeterminats del wireless router (reset).
 - Si la funció de QIS no pot detectar el tipus de connexió a Internet, premeu **Passa a la configuració manual** i configureu manualment els paràmetres de la connexió.
-



3. Assigneu el nom de la xarxa wireless (SSID) i la clau de seguretat de la connexió wireless de 2,4 GHz i 5 GHz. Quan acabeu, premeu **Aplicar**.



4. A la pàgina **Configuració de la informació d'inici de sessió**, canvieu la contrasenya d'inici de sessió del router per evitar accessos no autoritzats al wireless router.





The screenshot shows the ASUS wireless router login page. At the top left is the ASUS logo. The main heading is "Login" in blue. Below it, there are links for "Username / Password" and "Settings". The primary instruction is "Change the router password to prevent unauthorized access to your ASUS wireless router." The form contains three input fields: "Router Login Name", "New password" (with a password strength indicator icon), and "Retype Password". At the bottom, there are two buttons: "Previous" (white) and "Next" (blue).

NOTA: El nom d'usuari i la contrasenya del wireless router és diferent del nom de la xarxa (SSID) de 2,4 GHz/5 GHz i la clau de seguretat. El nom d'usuari i la contrasenya d'inici de sessió del wireless router us permeten iniciar la sessió a la interfície gràfica (GUI) en línia del wireless router per configurar els paràmetres del wireless router. Amb el nom de la xarxa de 2,4 GHz/5 GHz (SSID) i la clau de seguretat, els dispositius Wi-Fi poden iniciar la sessió i connectar-se a la xarxa de 2,4 GHz/5 GHz.

2.3 Connexió a la xarxa wireless

Després de configurar el wireless router amb la funció QIS, podreu connectar l'ordinador o altres dispositius intel·ligents a la xarxa wireless.

Per connectar-vos a la vostra xarxa:

1. A l'ordinador, premeu la icona de la xarxa  de l'àrea de notifikacions per mostrar les xarxes wireless disponibles.
2. Seleccioneu la xarxa wireless a la qual voleu connectar-vos i premeu **Connectar**.
3. Si es tracta d'una xarxa wireless protegida per contrasenya, potser necessitareu la clau de seguretat; introduïu-la i premeu **D'acord**.
4. Espereu fins que l'ordinador estableixi la connexió a la xarxa wireless correctament. Es mostra l'estat de la connexió i la icona de la xarxa mostra l'estat de connectada .

NOTES:

- Als capítols següents trobareu més informació sobre la configuració de la xarxa wireless.
 - Al manual de l'usuari del dispositiu trobareu més informació sobre la connexió a la xarxa wireless.
-

3 Configuració General i Configuració Avançada

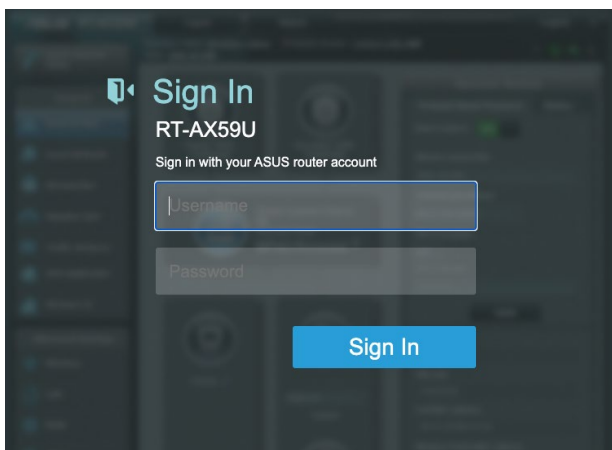
3.1 Inici de sessió a la interfície gràfica (GUI) en línia

L'encaminador sense fil ASUS inclou una interfície d'usuari gràfica (GUI) en línia molt intuïtiva que us permet configurar fàcilment diverses funcions mitjançant un navegador web, com ara Internet Explorer, Firefox, Safari o Google Chrome.

NOTA: Les funcions poden variar en funció de la versió de firmware.

Per entrar a la interfície gràfica (GUI) en línia:

1. Introduïu al navegador web l'adreça IP per defecte del wireless router: <http://www.asusrouter.com>.
2. A la pàgina d'inici de sessió, introduïu el nom d'usuari (**admin**) i la contrasenya que heu fet servir a **2.2 Configuració ràpida d'Internet (QIS) mitjançant la detecció automàtica**.



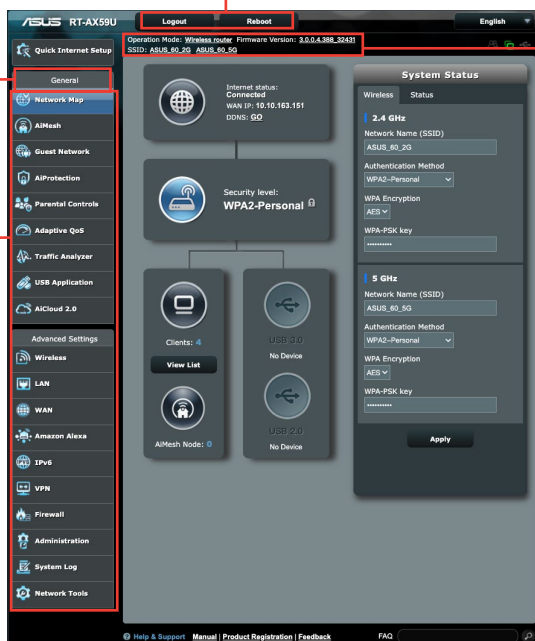
3. Ara podeu utilitzar la GUI en línia per configurar diversos paràmetres del wireless router ASUS.

Principals botons de comandament

QIS - Assistent de connexió intel·ligent

Panell de navegació

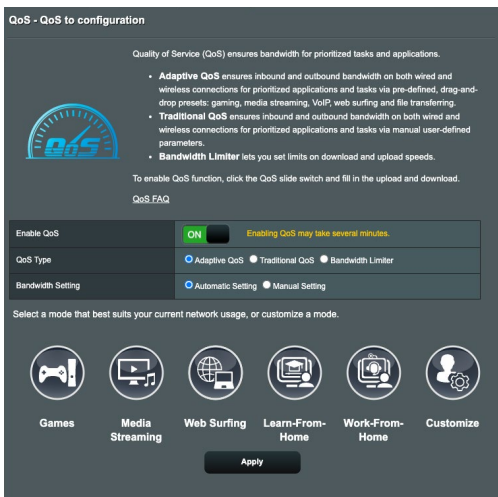
Bàner informatiu



NOTA: Quan iniciu la sessió a la interfície gràfica (GUI) en línia per primera vegada, s'obrirà automàticament la pàgina de configuració ràpida d'Internet (QIS).

3.2 QoS adaptativa

Aquesta funció garanteix l'ample de banda per a tasques i aplicacions prioritzades.



Per activar la funció QoS adaptativa:

1. Des del tauler de navegació, aneu a **General > QoS adaptativa > QoS**.
2. Des de la subfinestra **Enable QoS (Activar QoS)**, premeu **ON** per activar-la.
3. Seleccioneu el tipus de QoS (QoS Adaptativa, QoS Tradicional o Limita l'amplada de banda) per a la vostra configuració.

NOTA: A la QoS trobareu la definició dels tipus de QoS.

4. Feu clic a **Automatic Setting (Configuració automàtica)** perquè s'estableixi automàticament l'amplada de banda òptima o a **Manual Setting (Configuració manual)** per establir manualment l'amplada de banda de pujada i baixada.

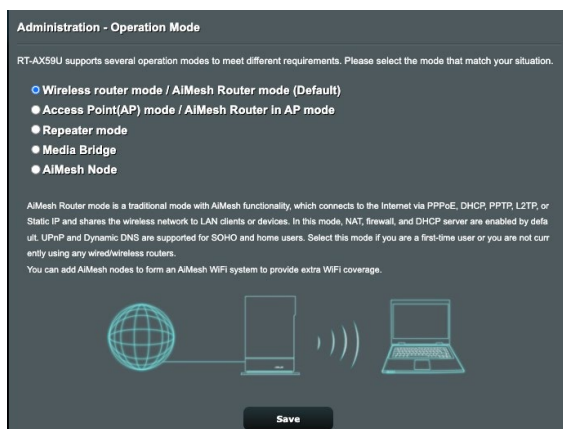
NOTA: Demaneu la informació de l'amplada de banda al vostre proveïdor de serveis d'internet (ISP). També podeu accedir a <http://speedtest.net> per saber quina amplada de banda teniu.

5. Premeu **Aplicar**.

3.3 Administració

3.3.1 Mode de funcionament

La pàgina de mode de funcionament us permet seleccionar el mode apropiat per a la xarxa.



Per configurar el mode de funcionament:

1. Des del tauler de navegació, aneu a **Configuració avançada** > **Administració** > **Mode de funcionament**.
2. Seleccioneu un dels modes de funcionament següents:
 - **Mode de wireless router / Mode de encaminador AiMesh (predeterminat):** Al mode de wireless router, l'equip es connecta a Internet i ofereix accés a Internet als dispositius disponibles a la seva pròpia xarxa local.
 - **Mode de punt d'accés (AP) / Encaminador AiMesh ai mode de punt d'accés (AP):** En aquest mode, el router crea una nova xarxa wireless en una xarxa existent.
 - **Mode de repetidor:** Al mode de repetidor, el RT-AX59U es connecta sense fil a una xarxa sense fil existent per ampliar la cobertura sense fil. En aquest mode es desactiven les funcions de tallafoc, ús compartit d'IP i NAT.
 - **Pont multimèdia:** Aquesta configuració exigeix dos encaminadors sense fil. El segon encaminador s'utilitza com a pont multimèdia per connectar-hi diversos dispositius, com ara televisors intel·ligents i consoles de videojoc a través d'ethernet.

- **Node AiMesh:** Aquesta configuració exigeix com a mínim dos encaminadors ASUS compatibles amb AiMesh. Activeu el node AiMesh i inicieu la sessió a la interfície de l'usuari en línia de l'encaminador AiMesh per cercar nodes AiMesh disponibles a prop per afegir-los al vostre sistema AiMesh. El sistema AiMesh permet cobrir tota la llar i ofereix gestió centralitzada.

3. Premeu **Desa**.

NOTA: El router es reinicia en canviar de mode.

3.3.2 Sistema

La pàgina **Sistema** us permet configurar els paràmetres del wireless router.

Per configurar els paràmetres del sistema:

1. Des del tauler de navegació, aneu a **Configuració avançada > Administració > Sistema**.
2. Podeu configurar els paràmetres següents:
 - **Canviar la contrasenya d'accés de l'encaminador:** Podeu canviar la contrasenya i el nom d'inici de sessió del wireless router i introduir-ne de nous.
 - **Zona horària:** Seleccioneu la zona horària de la vostra xarxa.
 - **Servidor NTP:** El wireless router pot accedir a un NTP (protocol horari de la xarxa, de l'anglès Network time Protocol) per sincronitzar l'hora.
 - **Habilitar Telnet:** Premeu **Sí** per habilitar els servei de telnet a la xarxa. Premeu **No** per inhabilitar els serveis de telnet.
 - **Mètode d'autenticació:** Podeu seleccionar els protocols HTTP, HTTPS o tots dos per protegir l'accés al router.
 - **Habilitar l'accés web des de la WAN:** Seleccioneu **Sí** perquè els dispositius externs a la xarxa puguin accedir als paràmetres de la GUI del wireless router. Seleccioneu **No** per impedir-ne l'accés.
 - **Admet només les adreces IP indicades:** Premeu **SÍ** si voleu especificar les adreces IP dels dispositius que poden accedir als paràmetres de la GUI de l'encaminador sense fil des de la WAN.
 - **Llista de clients:** Introduïu les adreces IP WAN dels dispositius de xarxa que poden accedir als paràmetres del wireless router. Aquesta llista es farà servir si heu seleccionat **Sí** per a l'opció **Permet només IP específiques**.

3. Premeu **Aplicar**.

3.3.3 Actualització del firmware

NOTA: Descarregueu el firmware més recent del llocs web d'ASUS a <http://www.asus.com>.

Per actualitzar el firmware:

1. Des del tauler de navegació, aneu a **Configuració avançada > Administració > Actualització del firmware**.
2. Al camp **Fitxer de firmware nou** o **Nou microprogramari del mòdem**, premeu **Cercar** i trieu el fitxer que heu baixat.
3. Premeu **Pujar**.

NOTES:

- Quan el procés d'actualització finalitzi, espereu que el sistema es reiniciï.
 - Si el procés d'actualització falla, el wireless router entra automàticament en mode rescat i el llum indicador d'alimentació del tauler frontal parpelleja lentament. Per recuperar o restablir el sistema, consulteu l'apartat **4.2 Restabliment del firmware**.
-

3.3.4 Restablir/desar/pujar la configuració

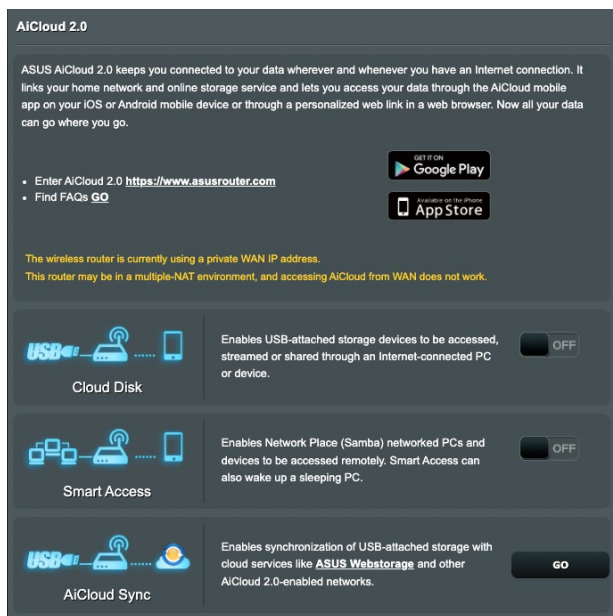
Per restablir, desar o pujar els paràmetres del wireless router:

1. Des del tauler de navegació, aneu a **Configuració avançada > Administració > Restablir/desar/pujar la configuració**.
2. Seleccioneu la tasca que voleu realitzar:
 - Per restablir els paràmetres predeterminats de fàbrica, premeu **Restablir** i **Acceptar** al missatge de confirmació.
 - Per desar la configuració actual del sistema, premeu **Desar**, aneu a la carpeta de destí del fitxer i premeu **Desar**.
 - Per restablir els paràmetres d'un fitxer de configuració del sistema, premeu **Cercar** per localitzar el fitxer i feu clic a **Pujar**.

IMPORTANT! Si es produeix cap problema, carregueu la darrera versió de firmware i configureu paràmetres nous. No restabliu la configuració predeterminada del router.

3.4 AiCloud 2.0

L'AiCloud 2.0 és una aplicació de servei al núvol que permet desar, sincronitzar, compartir i accedir als fitxers.



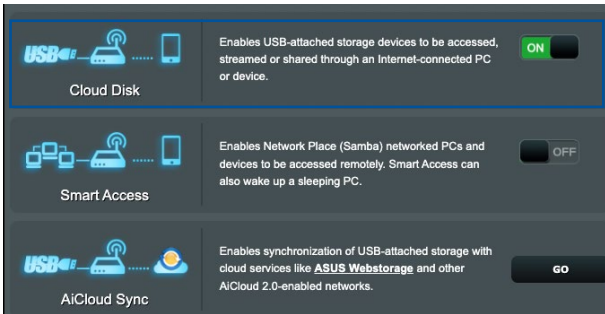
Per utilitzar l'AiCloud:

1. Des del Google Play Store o l'Apple Store, baixeu i instal·leu l'app ASUS AiCloud al dispositiu intel·ligent.
2. Connecteu el dispositiu intel·ligent a la xarxa. Seguiu les instruccions per completar el procés de configuració de l'AiCloud.

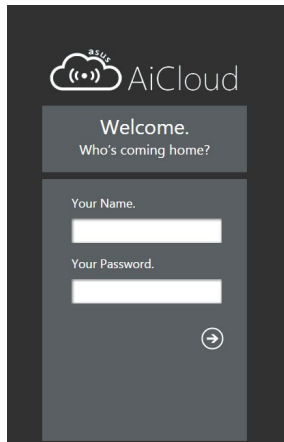
3.4.1 Disc al núvol

Per crear un disc al núvol

1. Inserir un dispositiu d'emmagatzematge USB al wireless router.
2. Activeu **Disc al núvol**.

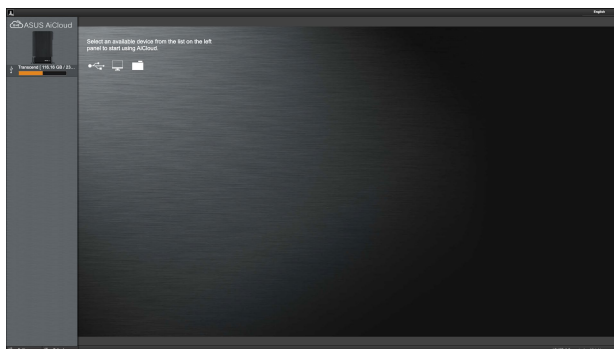


3. Aneu a <http://www.asusrouter.com> i introduïu el compte i la contrasenya d'inici de sessió al router. Per a una millor experiència d'usuari, us recomanem utilitzar el **Google Chrome** o el **Firefox**.



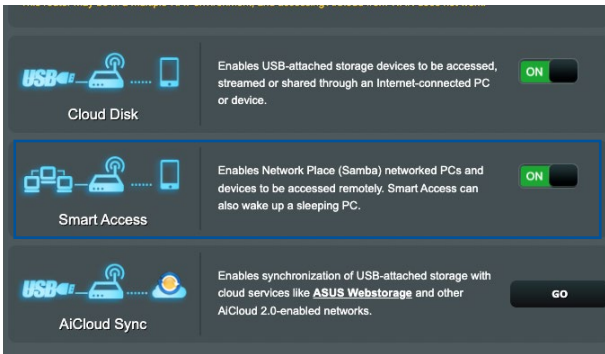
4. Ara ja podeu accedir als fitxers del disc al núvol des dels dispositius connectats a la xarxa.

NOTA: Quan accediu als dispositius connectats a la xarxa, haureu d'introduir manualment el nom d'usuari i la contrasenya del dispositiu, que no es desen a l'iCloud per motius de seguretat.



3.4.2 Accés intel·ligent

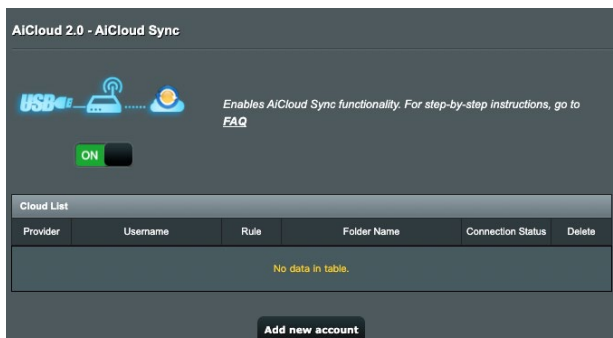
La funció d'accés intel·ligent us permet accedir fàcilment a la xarxa domèstica a través del nom de domini del router.



NOTES:

- Podeu crear un nom de domini per al router amb l'ASUS DDNS. Trobareu més informació a l'apartat **3.18.6 DDNS**.
 - De forma predeterminada, l'AiCloud 2.0 ofereix una connexió HTTPS segura. Introduïu [https://\[elvostrenomASUSDDNS\].asuscomm.com](https://[elvostrenomASUSDDNS].asuscomm.com) per a un disc al núvol del tot segur i l'ús de l'accés intel·ligent.
-

3.4.3 Sincronització AiCloud



Per utilitzar la sincronització AiCloud:

1. Executeu l'AiCloud, premeu **Sincronització AiCloud > Go (Executa)**.
2. Seleccioneu **Activar** per activar la sincronització AiCloud.
3. Premeu **Afegir compte nou**.
4. Introduïu la contrasenya de WebStorage d'ASUS i seleccioneu el directori que voleu sincronitzar amb el WebStorage.
5. Premeu **Aplicar**.

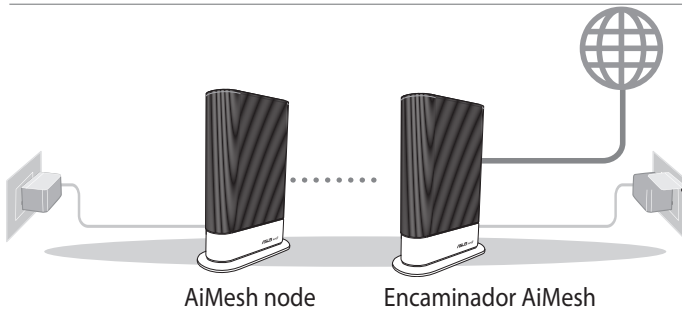
3.5 AiMesh

3.5.1 Abans de la configuració

Preparació per configurar un sistema de wifi AiMesh

1. Dos (2) encaminadors ASUS (models compatibles amb AiMesh: <https://www.asus.com/AiMesh/>).
2. Assigneu-ne un com a encaminador AiMesh i l'altre com a node AiMesh.

NOTA: Si teniu diversos encaminadors AiMesh, us recomanem que utilitzeu l'encaminador amb les especificacions més altes com al vostre encaminador AiMesh i els altres com a nodes AiMesh.



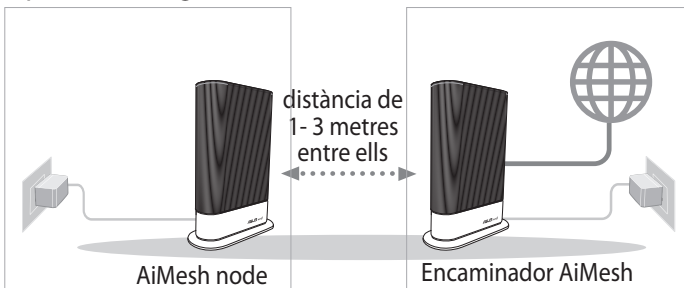
3.5.2 Passos per a la configuració de l'AiMesh

Preparació

Col·loqueu l'encaminador i el node AiMesh a una distància de 1-3 metres entre ells durant el procés de configuració.

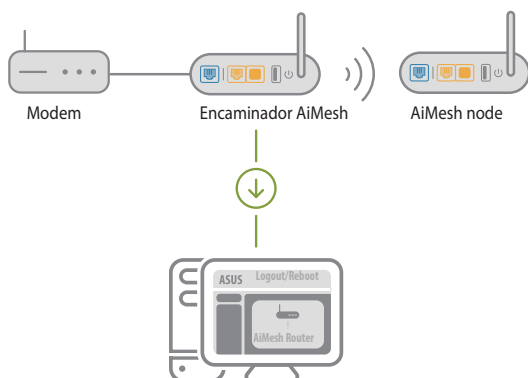
AiMesh node

Estat per defecte de fàbrica. Mantingueu l'aparell connectat i en espera per a la configuració del sistema AiMesh.



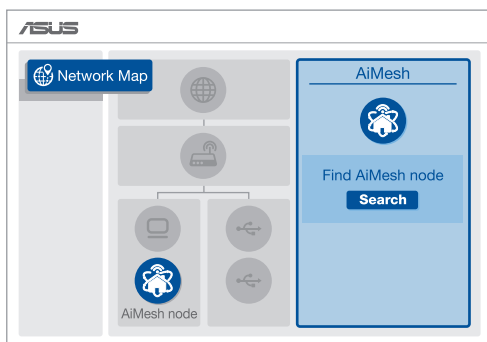
Encaminador AiMesh

- 1) Consulteu la **Quick Start Guide (Guia d'inici ràpid)** de l'altre encaminador per connectar l'encaminador AiMesh al PC i al mòdem, i seguidament iniciar la sessió a la interfície gràfica (GUI) en línia.



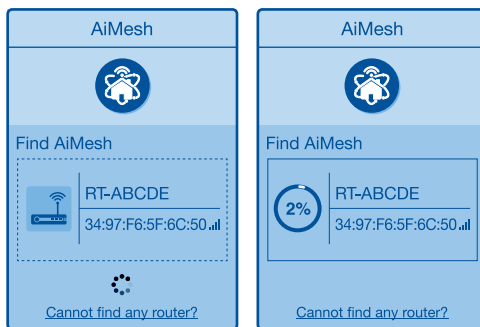
- 2) Aneu a la pàgina Mapa de la xarxa, feu clic a la icona d'AiMesh i, a continuació, cerqueu el node AiMesh estès.

NOTA: Si no hi trobeu la icona d'AiMesh, feu clic a la versió de microprogramari i actualitzeu el microprogramari.

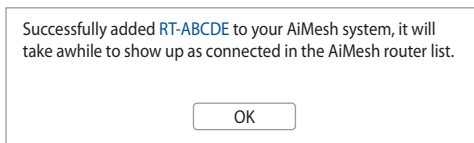


- 3) Feu clic a **Search (Cerca)** per cercar automàticament el vostre node AiMesh. Quan el node AiMesh aparegui en aquesta pàgina, feu-hi clic per afegir-lo al sistema AiMesh.

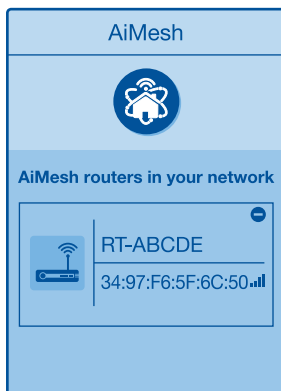
NOTA: Si no trobeu el node AiMesh, aneu a **TROUBLE SHOOTING (SOLUCIÓ DE PROBLEMES)**.



- 4) Quan la sincronització s'ha completat, apareix un missatge.



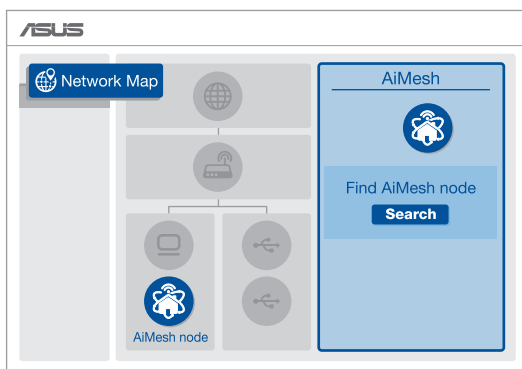
- 5) Enhorabona! La pàgina següent es mostra quan s'ha afegit un node AiMesh amb èxit a la xarxa AiMesh.



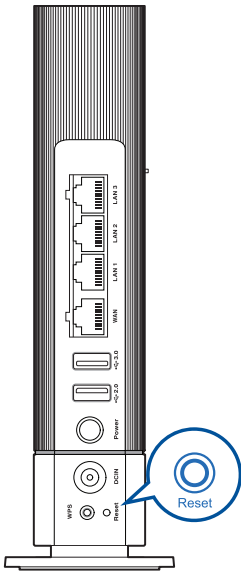
3.5.3 Solució de problemes

Si l'encaminador AiMesh no troba un node AiMesh a prop o la sincronització ha fallat, reviseu els paràmetres següents i torneu-ho a provar.

- 1) Apropieu el node AiMesh a l'encaminador AiMesh, si és possible. Ha d'estar a una distància d'entre 1 i 3 metres.
- 2) Comproveu que el node AiMesh està encès.
- 3) Comproveu que el node AiMesh té el microprogramari compatible amb AiMesh actualitzat.
 - i. Descarregueu el microprogramari compatible amb AiMesh de: <https://www.asus.com/AiMesh/>.
 - ii. Enceneu el node AiMesh i connecteu-lo a l'ordinador amb un cable de xarxa.
 - iii. Executeu la interfície gràfica (GUI) en línia. Se us redirigirà a l'assistent de configuració d'ASUS. Si no és així, aneu a <http://www.asusrouter.com>.
 - iv. Aneu a **Administration > Firmware Upgrade (Administració > Actualització del microprogramari)**. Feu clic a **Seleccionar arxiu** i carregueu el microprogramari compatible amb AiMesh.
 - v. Quan hàgiu descarregat el microprogramari, aneu a la pàgina Mapa de la xarxa per confirmar si ha aparegut la icona d'AiMesh.



- vi. Premeu el botó de reinicialització del vostre node AiMesh durant 5 segons com a mínim. Deixeu anar el botó de reinicialització quan el LED d'alimentació parpellegi lentament.



3.5.4 Reubicació

El millor rendiment:

Col·loqueu el node i l'encaminador AiMesh al millor lloc.

NOTES:

- Per minimitzar les interferències, allunyeu els encaminadors de dispositius com ara telèfons sense fil, dispositius Bluetooth i forns microones.
 - Us recomanem que col·loqueu els encaminadors en llocs oberts i espaiosos.
-



3.5.5 Preguntes freqüents (PF)

P1: L'encaminador AiMesh admet el mode de punt d'accés?

A: Sí. Podeu configurar l'encaminador AiMesh en mode d'encaminador o en mode de punt d'accés. Aneu a la GUI en línia (<http://www.asusrouter.com>) i accediu a la pàgina **Administració > Operation Mode (Mode de funcionament)**.

P2: Puc configurar la connexió amb fil entre encaminadors AiMesh (retorn d'Ethernet)?

A: Sí. El sistema AiMesh admet les connexions amb i sense fil entre l'encaminador AiMesh i el node per maximitzar el rendiment i l'estabilitat. L'AiMesh analitza la potència del senyal sense fil per a totes les bandes de freqüència disponibles i determina automàticament si és millor una connexió amb fil o sense fil com a xarxa troncal de connexió entre encaminadors.

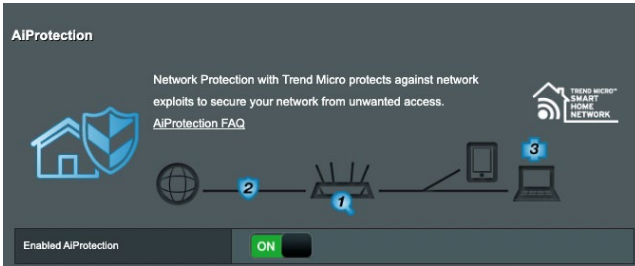
- 1) Seguiu els passos de la configuració per establir una connexió entre l'encaminador AiMesh i el node a través del wifi en primer lloc.
- 2) Col·loqueu el node al lloc ideal per maximitzar la cobertura. Col·loqueu un cable d'Ethernet del port LAN de l'encaminador AiMesh al port WAN del node AiMesh.



- 3) El sistema AiMesh seleccionarà automàticament el millor camí per a la transmissió de dades, amb o sense fil.

3.6 AiProtection

AiProtection supervisa el dispositiu en temps real per detectar software maliciós (malware), software espia i accessos no desitjats. També filtra els llocs web i les app no desitjades i us permet configurar durant quant de temps d'accés a Internet per a un dispositiu connectat.



3.6.1 Configuració d'Aiprotection

La AiProtection evita el mal ús de la xarxa i la protegeix d'accessos no autoritzats.

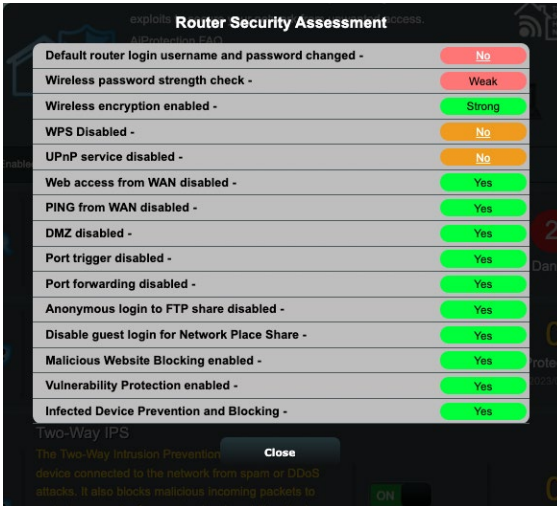
The screenshot displays the AiProtection control panel. At the top, it states 'Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access.' Below this is a diagram of a network setup with three numbered steps: 1. Router, 2. Internet, and 3. Connected devices. The main interface features a toggle for 'Enabled AiProtection' which is currently turned 'ON'. Below this are four security modules, each with a description, a status toggle, and a protection level indicator:

- Router Security Assessment**: Includes a 'Scan' button. The status is 'Danger' (indicated by a red '2').
- Malicious Sites Blocking**: The status toggle is 'ON'. The protection level is 'Protection' (indicated by a yellow '0').
- Two-Way IPS**: The status toggle is 'ON'. The protection level is 'Protection' (indicated by a yellow '0').
- Infected Device Prevention and Blocking**: The status toggle is 'ON'. The protection level is 'Protection' (indicated by a yellow '0').

Per configurar la Aiprotection de la xarxa:

1. Des del tauler de navegació, aneu a **General > AiProtection**.
2. A la pàgina principal d'AiProtection, premeu **Protecció de la xarxa**.
3. A la Protecció de la xarxa, premeu **Escanejar**.

Els resultats de la cerca es mostren a la pàgina **Router Security Assessment (Avaluació de seguretat de l'encaminador)**.



IMPORTANT! Els elements que es marquen amb el text **Sí** a la pàgina **Avaluació de la seguretat del router** es consideren que tenen un estat segur.

4. (Opcional) Des de la pàgina **Avaluació de la seguretat del router** podeu configurar manualment els elements que es marquen amb el text **No**, **Dèbil** o **Molt dèbil**. Per fer-ho:
 - a. Feu clic a un element per accedir a la pàgina de configuració d'aquest element.
 - b. Des de la pàgina de paràmetres de seguretat de l'element en qüestió, apliqueu els paràmetres i els canvis necessaris i premeu **Aplificar** quan acabeu.
 - c. Torneu a la pàgina d'**Avaluació de la seguretat del router** i premeu **Tancar** per tancar-la.
5. Feu clic a **OK (Acceptar)** al missatge de confirmació.

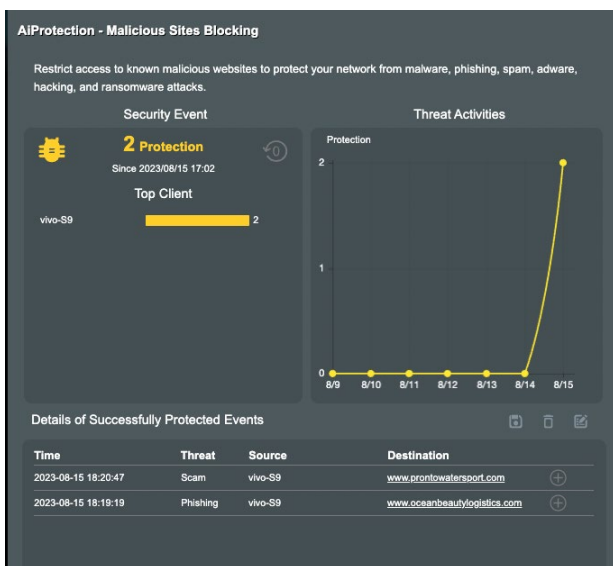
3.6.2 Bloqueig de llocs maliciosos

Aquesta funció restringeix l'accés de llocs web maliciosos a la base de dades al núvol per garantir una protecció continuada.

NOTA: Aquesta funció s'activa automàticament en executar l'Escaneig de punts febles del router.

Per activar el bloqueig de llocs maliciosos:

1. Des del tauler de navegació, aneu a **General > AiProtection**.
2. A la pàgina principal d'AiProtection, premeu **Bloqueig de llocs maliciosos**.



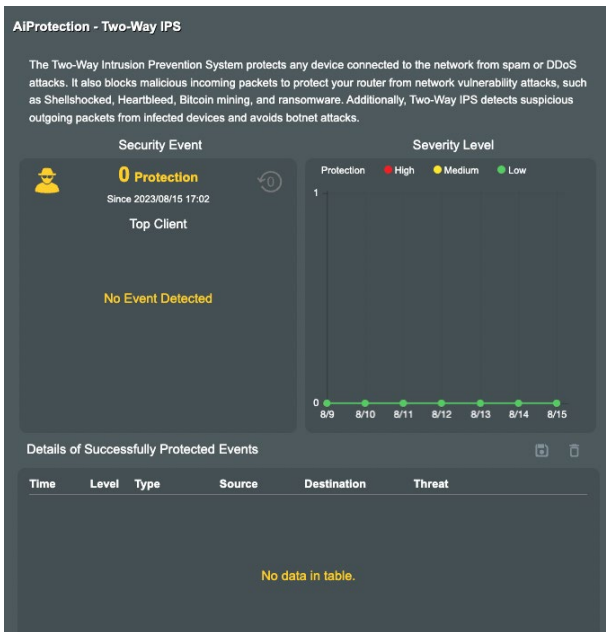
3.6.3 IPS bidireccional

Aquesta funció resol vulnerabilitats habituals de la configuració de l'encaminament.

NOTA: Aquesta funció s'activa automàticament en executar l'Escaneig de punts febles del router.

Per activar l'IPS bidireccional:

1. Des del tauler de navegació, aneu a **General > AiProtection**.
2. A la pàgina principal d'AiProtection, premeu **IPS bidireccional**.



3.6.4 Previsió i bloqueig de dispositius infectats

Aquesta funció evita que dispositius infectats puguin comunicar informació personal o passar virus a altres parts.

NOTA: Aquesta funció s'activa automàticament en executar l'Escaneig de punts febles del router.

Per activar la previsió i bloqueig de dispositius infectats:

1. Des del tauler de navegació, aneu a **General > AiProtection**.
2. A la pàgina principal d'AiProtection, premeu **Previsió i bloqueig de dispositius infectats**.

Per configurar les preferències de les alertes:

1. Des de la subfinestra de Previsió i bloqueig de dispositius infectats, premeu **Preferències de les alertes**.
2. Seleccioneu o introduïu el proveïdor de correu, el compte de correu electrònic i la contrasenya i, seguidament, premeu **Aplicar**.



3.7 Firewall

El wireless router pot fer de firewall de hardware per a la xarxa.

NOTA: La funció de firewall està habilitada per defecte.

3.7.1 General

Per configurar els paràmetres bàsics del firewall:


1. Des del tauler de navegació, aneu a **Configuració avançada > Firewall > General**.
2. Al camp **Habilitar firewall**, seleccioneu **Sí**.
3. A **Habilitar protecció DoS**, seleccioneu **Sí** per protegir la xarxa d'atacs de DoS (Denial of Service), tot i que això pot afectar el rendiment del router.
4. També podeu controlar els paquets intercanviats entre la connexió LAN i WAN. Al tipus de paquets registrats, seleccioneu **Perduts, Acceptats** o **Tots dos**.
5. Premeu **Aplicar**.

3.7.2 Filtre d'URL

Podeu especificar paraules clau o adreces web per impedir l'accés a URL específiques.

NOTA: El filtre d'URL està basat en una consulta DNS. Si un client de xarxa ja ha accedit a un lloc web, com ara `http://www.abcxxx.com`, aquest lloc web no es bloquejarà (la memòria cau DNS del sistema emmagatzema els llocs web que s'han visitat anteriorment). Per resoldre aquest problema, esborreu la memòria cau DNS abans de configurar el filtre d'URL.

Per configurar un filtre d'URL:

1. Des del tauler de navegació, aneu a **Configuració avançada > Firewall > Filtre d'URL**.
2. Al camp **Habilitar filtre d'URL**, seleccioneu **Habilitat**.
3. Introduïu una URL i, a continuació, feu clic al botó .
4. Premeu **Aplicar**.

3.7.3 Filtre de paraules clau

El filtre de paraules clau bloqueja l'accés a les pàgines web que contenen paraules clau específiques.

Firewall - Keyword Filter

Keyword Filter allows you to block the clients' access to webpages containing the specified keywords.

Limitations of the filtering function :

1. Compressed webpages that use HTTP compression technology cannot be filtered. [See here for more details.](#)
2. Https webpages cannot be filtered.


Basic Config

Enable Keyword Filter Enabled Disabled

Keyword Filter List (Max Limit : 64)

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

Per configurar un filtre de paraules clau:

1. Des del tauler de navegació, aneu a **Configuració avançada > Firewall > Filtre de paraules clau.**
2. Al camp **Habilitar filtre de paraules clau**, seleccioneu **Habilitat.**
3. Introduïu una paraula o frase i premeu el botó .
4. Premeu **Aplicar.**

NOTES:

- El filtre de paraules clau està basat en una consulta DNS. Si un client de xarxa ja ha accedit a un lloc web, com ara <http://www.abcxxx.com>, aquest lloc web no es bloquejarà (la memòria cau DNS del sistema emmagatzema els llocs web que s'han visitat anteriorment). Per resoldre aquest problema, esborreu la memòria cau DNS abans de configurar el filtre de paraules clau.
- Les pàgines web comprimides amb la compressió HTTP no poden filtrar-se. Les pàgines HTTP tampoc poden bloquejar-se amb un filtre de paraules clau.

3.7.4 Filtre de serveis de la xarxa

El filtre de serveis de la xarxa bloqueja els intercanvis de paquets de LAN a WAN i restringeix l'accés dels clients de la xarxa a serveis web específics, com ara Telnet o FTP.

Firewall - Network Services Filter

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

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

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

Network Services Filter

Enable Network Services Filter Yes No

Filter table type

Well-Known Applications

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

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

Date to Enable LAN to WAN Filter Sat Sun

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

Filtered ICMP packet types

Network Services Filter Table (Max Limit : 32)

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

No data in table.

Apply

Per configurar un filtre de serveis de la xarxa:

1. Des del tauler de navegació, aneu a **Configuració avançada > Firewall > Filtre de serveis** de la xarxa.
2. Al camp **Habilitar filtre de serveis de la xarxa**, seleccioneu.
3. Seleccioneu el tipus de taula de filtres. **Llista negra** bloqueja els serveis de la xarxa especificats. **Llista blanca** limita l'accés només als serveis de la xarxa especificada.
4. Especifiqueu el dia i l'hora en què els filtres estaran actius.
5. Per especificar el serveis de xarxa que voleu filtrar, introduïu l'adreça IP d'origen, l'adreça IP de destinació, l'interval de ports i el protocol. Feu clic al botó **+**.
6. Premeu **Aplicar**.

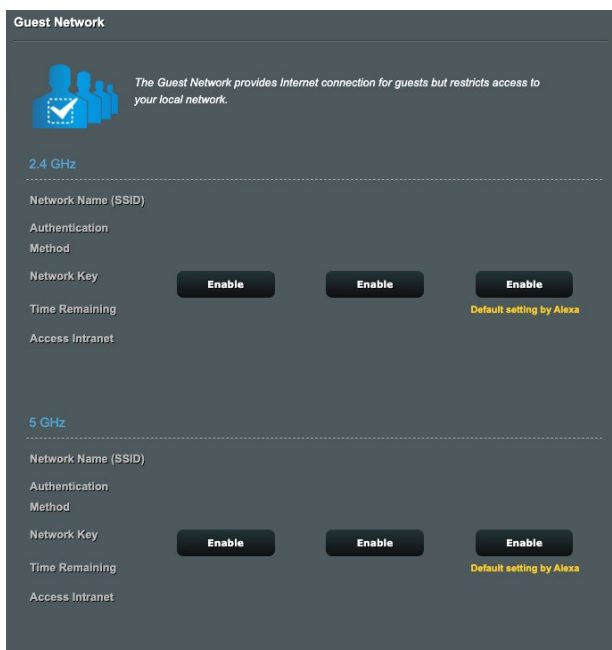
3.8 Xarxa per a convidats

La xarxa per a convidats ofereix als visitats accés temporal via Internet a SSID o xarxes separades sense haver de donar-los accés a la vostra xarxa privada.

NOTA: RT-AX59U admet fins a sis SSIDs (tres SSID de 2,4 GHz i tres SSID de 2,4 GHz).

Per crear una xarxa de convidats:

1. Des del tauler de navegació, aneu a **General > Xarxa de convidats**.
2. A la pantalla Xarxa de convidat, seleccioneu la banda de freqüència de 2,4 GHz o 5 GHz per a la xarxa de convidats que voleu crear.
3. Premeu **Habilitar**.

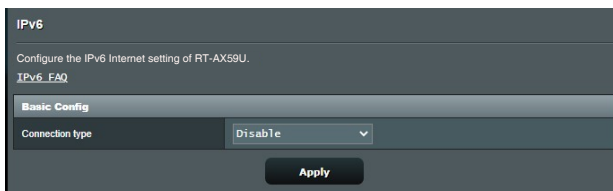


The screenshot shows the 'Guest Network' configuration page. At the top, there is a blue icon of three people and a checkmark, with the text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' Below this, there are two sections for configuring the network: '2.4 GHz' and '5 GHz'. Each section includes fields for 'Network Name (SSID)', 'Authentication Method', and 'Network Key'. The 'Network Key' field has three 'Enable' buttons. Below these fields, there are 'Time Remaining' and 'Access Intranet' options. A yellow note indicates 'Default setting by Alexa'.

4. Per canviar les opcions d'un convidat, feu clic a les opcions que voleu modificar. Feu clic a **Remove (Elimina)** per eliminar les opcions de configuració del convidat.
5. Al camp Nom de la xarxa (SSID), poseu un nom a la xarxa temporal wireless.
6. Seleccioneu un Mètode d'autenticació.
7. Si seleccioneu un mètode d'autenticació WPA, seleccioneu un xifratge WPA.
8. Especifiqueu el Temps d'accés o seleccioneu **Il·limitat**.
9. Seleccioneu **Inhabilitar** o **Habilitar** a l'element Accés a la Intranet.
10. Quan acabeu, premeu **Aplicar**.

3.9 IPv6

El wireless router admet IPv6, un sistema compatible amb més adreces IP. Aquest estàndard encara no està disponible a tot arreu. Demaneu al vostre proveïdor de serveis d'Internet (ISP) si el servei que us ofereix és compatible amb IPv6.



Per configurar l'IPv6:

1. Des del tauler de navegació, aneu a **Configuració avançada > IPv6**.
2. Seleccioneu el **tipus de Connexió**. Les opcions de configuració varien en funció del tipus de connexió seleccionat.
3. Introdueix els paràmetres de DNS i LAN d'IPv6.
4. Premeu **Aplicar**.

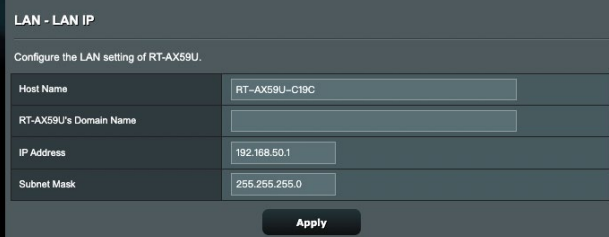
NOTA: Demaneu al vostre proveïdor de serveis d'Internet (ISP) informació específica d'IPv6 per al vostre servei d'Internet.

3.10 LAN

3.10.1 IP de LAN

La pantalla IP de LAN permet modificar la configuració IP de la xarxa LAN del wireless router.

NOTA: Qualsevol canvi que es realitzi a l'adreça IP de la xarxa LAN apareixerà a la configuració de DHCP.



LAN - LAN IP	
Configure the LAN setting of RT-AX59U.	
Host Name	RT-AX59U-C19C
RT-AX59U's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0
Apply	

Per modificar la configuració de la IP de la xarxa LAN:

1. Des del tauler de navegació, aneu a **Configuració avançada > LAN > IP de LAN.**
2. Modifiqueu l'**Adreça IP** i la **Màscara de subxarxa.**
3. Quan acabeu, premeu **Aplicar.**

3.10.2 Servidor DHCP

El wireless router utilitza el protocol DHCP per assignar adreces IP automàticament a la xarxa. Podeu especificar l'interval d'adreces IP i el temps d'arrendament per als clients de la xarxa.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. RT-AX59U supports up to 253 IP addresses for your local network.
[Manually Assigned IP around the DHCP list FAQ](#)

Basic Config

Enable the DHCP Server Yes No

RT-AX59U's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time (seconds)

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

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

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

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

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

No data in table.

Per configurar el servidor DHCP:

1. Des del tauler de navegació, aneu a **Configuració avançada > LAN > Servidor DHCP**.
2. Al camp **Habilitar el servidor DHCP**, marqueu **Sí**.
3. Al quadre de text **RT-AX59U de videojocs TUF's Nom de domini**, introduïu un nom de domini per al wireless router.
4. Al camp **Adreça inicial de pool d'IP**, introduïu l'adreça IP inicial.
5. Al camp **Adreça final de pool d'IP**, introduïu l'adreça IP final.

6. Al camp **Temps d'arrendament (segons)**, especifiqueu en segons quan caduca una adreça IP assignada. Quan s'esgota el límit temporal, el servidor DHCP assigna una nova adreça IP.

NOTES:

- Us recomanem que, quan especifiqueu un interval d'adreces IP, utilitzeu el format d'adreça IP 192.168.50.xxx (en què xxx pot ser qualsevol número entre 2 i 254).
 - L'adreça inicial del pool d'IP no pot ser més gran que la final.
-
7. A la secció **Configuració de DNS i WINS de Servidor**, introduïu l'adreça IP del servidor WINS i el servidor de DNS, si és necessari.
 8. El wireless router també pot assignar manualment adreces IP als dispositius de la xarxa. Al camp **Habilitar assignació manual**, seleccioneu **Sí** per assignar una adreça IP a adreces MAC específiques de la xarxa. Es poden afegir fins a 32 adreces MAC a la llista DHCP per a l'assignació manual.

3.10.3 Encaminament

Si la xarxa utilitza més d'un wireless router, podeu configurar una taula d'encaminament per compartir el mateix servei d'Internet.

NOTA: Us recomanem que no canvieu la configuració d'encaminament predeterminada a no ser que tingueu coneixements avançats sobre les taules d'encaminament.

LAN - Route

This function allows you to add routing rules into RT-AX59U. It is useful if you connect several routers behind RT-AX59U to share the same connection to the Internet.

Basic Config

Enable static routes Yes No



Static Route List (Max Limit : 32)

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

No data in table.

Apply

Per configurar la taula d'encaminament LAN:

1. Des del tauler de navegació, aneu a **Configuració avançada > LAN > Encaminament**.
2. Al camp **Habilitar encaminament estàtic**, seleccioneu **Sí**.
3. A la **Llista d'encaminament estàtic**, introduïu la informació de xarxa d'altres punts d'accés o nodes. Premeu el botó **Afegir**  o **Eliminar**  per afegir o suprimir un dispositiu de la llista.
4. Premeu **Aplicar**.

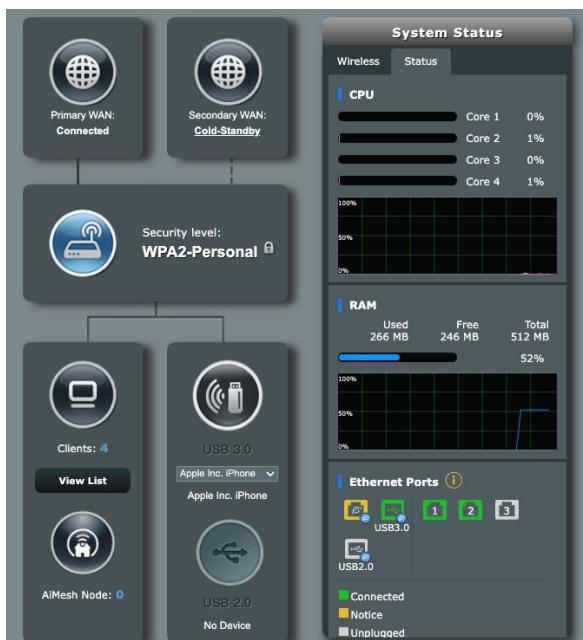
3.10.4 IPTV

El wireless router admet la connexió als serveis IPTV mitjançant un proveïdor de serveis d'Internet (ISP) o una xarxa LAN. La IPTV ofereix els paràmetres de configuració necessaris per configurar IPTV, VoIP, multidifusió i UDP per al vostre servei. Poseu-vos en contacte amb el vostre proveïdor de serveis d'Internet (ISP) per obtenir informació específica sobre el vostre servei.

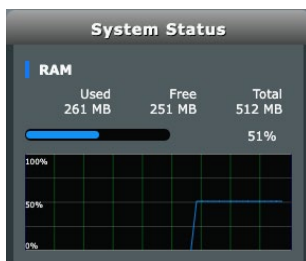
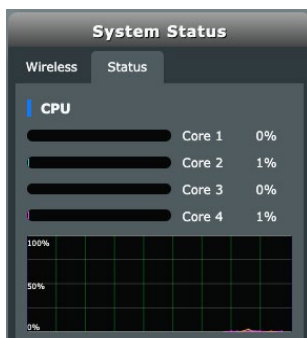
LAN - IPTV	
To watch IPTV, the WAN port must be connected to the Internet. Please go to WAN - Dual WAN to confirm that WAN port is assigned to primary WAN.	
LAN Port	
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾
Special Applications	
Use DHCP routes	Microsoft ▾
Enable multicast routing	Disable ▾
Enable efficient multicast forwarding (IGMP Snooping)	Disable ▾
UDP Proxy (Udpxy)	0
Apply	

3.11 Mapa de la xarxa

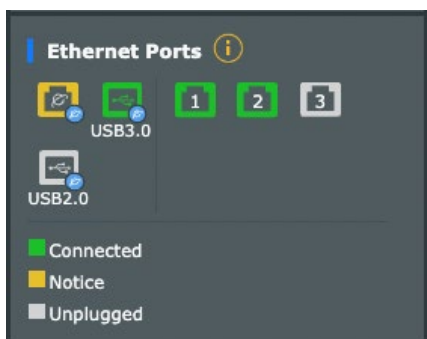
El Network Map (Mapa de la xarxa) us permet configurar les opcions de seguretat de la xarxa, gestionar els clients de la xarxa i supervisar el dispositiu USB.



Podeu controlar l'estat de la CPU de cada nucli, l'estat d'ús de la memòria RAM i l'estat dels ports Ethernet. A continuació, trobareu un exemple de l'estat d'ús de la CPU, la RAM i els ports Ethernet.



Estat del port: Us permet verificar l'estat dels ports d'Ethernet i els ports USB.



3.11.1 Configuració dels paràmetres de seguretat wireless

Per protegir la xarxa wireless contra accessos no autoritzats, haureu de configurar els paràmetres de seguretat.

Per configurar els paràmetres de seguretat wireless:

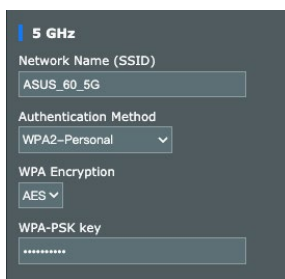
1. Des del tauler de navegació, aneu a **General > Mapa de la xarxa**.
2. A la pantalla Mapa de la xarxa i sota **Estat del sistema**, podeu configurar els paràmetres de seguretat wireless (p. ex. SSID, nivell de seguretat i paràmetres de xifratge).

NOTA: Podeu configurar diferents paràmetres de seguretat wireless per a les bandes de 2,4 GHz i 5 GHz.

Paràmetres de seguretat de 2,4 GHz



Paràmetres de seguretat de 5 GHz



3. Al camp **Nom de la xarxa (SSID)**, introduïu un nom únic per a la xarxa wireless.
4. A la llista desplegable **Authentication Method (Mètode d'autenticació)**, seleccioneu el mètode de xifratge de la xarxa wireless.

Si seleccioneu WPA-Personal o WPA-2 Personal com a mètode d'autenticació, introduïu la clau de WPA-PSK o la clau d'accés de seguretat.

IMPORTANT! L'estàndard IEEE 802.11n/ac prohibeix l'ús d'altres velocitats amb WEP o WPA-TKIP per a emissió única. Si utilitzeu aquests mètode de xifratge, la velocitat de les dades baixarà a la connexió de 54 Mbps de l'estàndard IEEE 802.11g.

5. Quan acabeu, premeu **Aplicar**.

3.11.2 Gestió dels clients de la xarxa



Per gestionar els clients de la xarxa:

1. Des del tauler de navegació, aneu a **General > Mapa de la xarxa**.
2. A la pantalla **Mapa de la xarxa**, seleccioneu la icona **Clients** per mostrar la informació del client de la xarxa.
3. Feu clic a **Mostrar llista** sota la icona **Clients** per mostrar tots els clients.
4. Per blocar l'accés d'un client a la vostra xarxa, seleccioneu el client i premeu icona del candau obert.

Internet	Icon	Clients Name	Client IP address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
Internet	🌐	Shenzhen Qihu Intelligent Techn	192.168.50.71	Static	B0:59:47:2F:66:A8	72	1	05:11:39
Internet	📺	MacBook-Air-M1	192.168.50.190	BRCP	50:ED:3C:03:82:D7	1201	6	05:07:26
Internet	👤	vivo-S9	192.168.50.196	BRCP	EA:D0:66:DC:7F:28	600	600	01:22:01
Internet	📺	REALTEK SEMICONDUCTOR CORP	192.168.50.209	BRCP	00:ED:4C:68:01:A2	-	-	-

3.11.3 Supervisió del dispositiu USB

El wireless router ASUS inclou un port USB per connectar-hi un dispositiu USB o una impressora USB que us permetran compartir fitxers i compartir la impressora amb els clients de la vostra xarxa.



NOTES:

- Per utilitzar aquesta funció, haureu de connectar un dispositiu d'emmagatzematge USB, com ara un disc dur USB o una unitat de memòria USB, al port USB 3.0/2.0 del darrere del wireless router. Comproveu que el dispositiu d'emmagatzematge USB està correctament formatat i particionat. Consulteu la Llista de compatibilitat de disc Plug-n-Share a <http://event.asus.com/networks/disksupport>
- Els ports USB admeten dos unitats d'USB o una impressora i una unitat d'USB simultàniament.

IMPORTANT! Abans haureu de crear un compte compartit i definir-ne els permisos i els drets d'accés perquè altres clients de la xarxa puguin accedir al dispositiu USB mitjançant una utilitat de client d'FTP pròpia o de tercers, Servers Center, Samba o AiCloud Per obtenir més informació, consulteu l'apartat **3.16 Aplicació USB i 3.4 AiCloud 2.0** en aquest manual de l'usuari.

Per supervisar el dispositiu USB:

1. Des del tauler de navegació, aneu a **General > Mapa de la xarxa**.
2. A la pantalla Mapa de la xarxa, seleccioneu la icona **Estat del disc USB** per mostrar la informació del dispositiu USB.
3. Al camp Assistent AiDisk, premeu **ENDAVANT** per configurar un servidor FTP per a l'ús compartit de fitxers per Internet.


NOTES:

- Per obtenir més informació, consulteu l'apartat **3.16.2 Ús del Servers Center** d'aquest manual de l'usuari.
- El wireless router és compatible amb la majoria de dispositius de memòria i discs durs USB (fins a 4 TB de mida) i permet l'accés de lectura i d'escriptura per a FAT16, FAT32, NTFS i HFS+.

Extracció segura del disc USB

IMPORTANT! L'extracció incorrecta del disc USB pot provocar errors a les dades.

Per extreure el disc USB d'una manera segura:

1. Des del tauler de navegació, aneu a **General > Mapa de la xarxa**.
2. A la cantonada superior dreta, premeu  > **Expulsar disc USB**. Si expulseu el disc USB correctament, mostra l'estat **Desmuntat**.



3.12 Controls parentals

El controls parental us permet controlar el temps d'accés a Internet o establir el límit de temps d'ús de la xarxa d'un client.

Per activar l'Controls parentals:

Des del tauler de navegació, aneu a **General > Controls parentals**.

Parental Controls - Web & Apps Filters

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

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

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

Web & Apps Filters ON

Client List (Max Limit : 64)


<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	<input type="text"/>	<ul style="list-style-type: none"><input type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.<input type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.<input type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	<input type="button" value="+"/>

No data in table.

Filtres d'apps i webs

Els filtres d'apps i webs són una funció dels Controls Parentals que us permeten bloquejar l'accés a llocs webs o aplicacions no desitjats.

Per configurar els filtres d'apps i webs:

1. Des del tauler de navegació, aneu a **General > Controls parentals > Filtres d'apps i webs**.
2. Des de la subfinestra de **filtres d'apps i webs**, premeu **Activar**.
3. Quan aparegui el missatge que us demana que accepteu el Contracte de llicència de l'usuari final (EULA), premeu **Hi estic d'acord** per continuar.
4. Des de la columna **Llista de clients**, introduïu el nom del client o seleccioneu-lo de la llista desplegable.
5. A la columna **Categoria de contingut**, seleccioneu els filtres de les quatre categories principals: **Contingut per a adults, missatgeria instantània i comunicació, P2P i transferències de fitxers, i streaming i entreteniment**.
6. Premeu  per afegir el perfil del client.
7. Premeu **Aplicar** per desar els paràmetres.

Planificació temporal

La planificació temporal permet establir un límit de temps d'ús de la xarxa per al client.

NOTA: Comproveu que l'hora del sistema està sincronitzada amb la del servidor d'NTP.

Parental Controls - Time Scheduling

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

Enable block all devices

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

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

Note:
1. Please disable NAT Acceleration for more precise scheduling control.

Enable Time Scheduling

System Time **Tue, Aug 15 18:24:45 2023**

Client List (Max Limit : 64)

Select all	Client Name (MAC Address)	Time Management	Add / Delete
Time	<input type="text"/>	-	<input type="button" value="+"/>

No data in table.

Per configurar la planificació temporal:

1. Des del tauler de navegació, aneu a **General > Controls parents > Planificació temporal**.
2. Des de la subfinestra **Activar planificació temporal**, premeu **Activar**.
3. A la columna **Nom del Client**, introduïu el nom del client o seleccioneu-lo de la llista desplegable.

NOTA: També podeu introduir l'adreça MAC del client a la columna Adreça MAC del client. Comproveu que el nom del client no conté espais ni caràcters especials perquè poden provocar problemes de funcionament al router.

4. Premeu per afegir el perfil del client.
5. Premeu **Aplicar** per desar els paràmetres.

3.13 Smart Connect

Smart Connect està dissenyat per redirigir els clients automàticament a una de les tres ràdios (2,4 GHz i 5 GHz) per maximitzar el rendiment total de la xarxa sense fil.

3.13.1 Configuració d'Smart Connect

Podeu activar l'Smart Connect des de la interfície d'usuari en línia mitjançant un d'aquests dos procediments:

- **Mitjançant la pantalla de la xarxa sense fil**
 1. Al navegador web, introduïu manualment l'adreça IP per defecte de l'encaminador sense fil: <http://www.asusrouter.com>.
 2. A la pàgina d'inici de sessió, introduïu el nom d'usuari predeterminat (**admin**) i la contrasenya (**admin**) i feu clic a **OK(D'acord)**. La pàgina de QIS s'inicia automàticament.
 3. Des del tauler de navegació, aneu a **Configuració avançada > Wireless (Sense fil) > General (General)**.
 4. Desplaceu el control lliscant a **ON (Activat)** al camp **Enable Smart Connect (Activar Smart Connect)**. Aquesta funció connecta automàticament els clients de la xarxa a la banda apropiada per a una velocitat òptima.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input checked="" type="checkbox"/> ON
Smart Connect	Dual-Band Smart Connect (2.4 GHz and 5 GHz) ▾
2.4/5 GHz	
Network Name (SSID)	ASUS_60_2G
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto ▾ <input checked="" type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable ▾ <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check FAQ</small>
WiFi Agile Multiband	Enable ▾
Target Wake Time	Disable ▾
Authentication Method	WPA2-Personal ▾ ⓘ
WPA Encryption	AES ▾
WPA Pre-Shared Key	0933699365
Protected Management Frames	Disable ▾
Group Key Rotation Interval	3600
2.4 GHz	
Channel bandwidth	20/40 MHz ▾
Control Channel	Auto ▾ <small>Current Control Channel: 6</small> <input type="checkbox"/> Auto select channel including channel 12, 13
Extension Channel	Auto ▾
5 GHz	
Channel bandwidth	20/40/80 MHz ▾ <input type="checkbox"/> Enable 160 MHz
Control Channel	Auto ▾ <small>Current Control Channel: 112</small> <input checked="" type="checkbox"/> Auto select channel including DFS channels
Extension Channel	Auto ▾

Apply

3.14 Registre del sistema

El Registre del Sistema conté les activitats que s'han registrat de la xarxa.

NOTA: El registre del sistema es restableix (reset) en reiniciar i en apagar el router.

Per veure el registre del sistema:

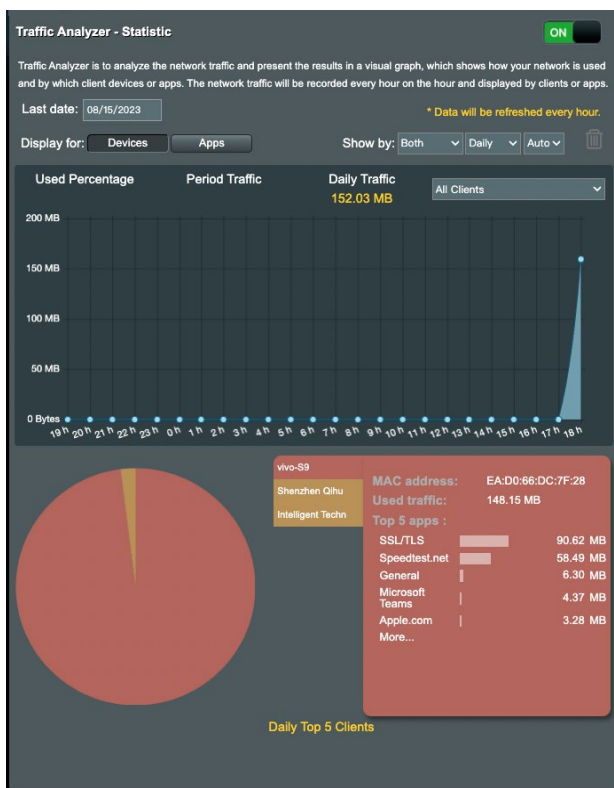
1. Des del tauler de navegació, aneu a **Configuració avançada** > **Registre del sistema**.
2. Podeu veure les activitats de la xarxa en qualsevol de les pestanyes següents:
 - Registre general
 - Registre wireless
 - Arrendaments DHCP
 - IPv6
 - Taula d'encaminaments
 - Reenviament de port
 - Connexions

The screenshot displays the 'System Log - General Log' interface. At the top, it states 'This page shows the detailed system's activities.' Below this, there are summary statistics: 'System Time' is 'Tue, Aug 15 19:09:24 2023', and 'Uptime' is '0 days 2 hour(s) 6 minute(s) 25 seconds'. A 'Remote Log Server' field is set to '514', with a note: '* The default port is 514. If you reconfigured the port number, please make sure that the remote log server or IoT devices' settings match your current configuration.' There are 'Apply', 'Clear', and 'Save' buttons. The main area contains a log of system events:

```
Aug 15 18:51:49 miniupnpd[13959]: shutting down MiniUPnPd
Aug 15 18:51:49 WEBDAV server: daemon is started
Aug 15 18:51:49 : it is advised to use network interface name instead of 192.168.50.1/255.255.255.0
Aug 15 18:51:49 miniupnpd[13986]: HTTP listening on port 41569
Aug 15 18:51:49 miniupnpd[13986]: Listening for NAT-PMP/PCP traffic on port 5351
Aug 15 18:51:50 avahi-daemon[13981]: Alias name "RT-AX59U" successfully established.
Aug 15 18:51:50 avahi-daemon[13981]: Alias name "findasus" successfully established.
Aug 15 18:52:14 hotplug: add net eth2.
Aug 15 18:52:14 hotplug: add net eth2.
Aug 15 18:52:14 hotplug: set net eth2.
Aug 15 18:52:14 hotplug: set net eth2.
Aug 15 18:54:31 kernel: nvram_free: 1538(httppd) nvram_idx(1 / 2)
Aug 15 18:54:31 rc_services: httpd 1538(notify) rc restart firewall
Aug 15 18:54:31 rc_services: httpd 1538(notify) rc restart firewall
Aug 15 18:54:31 rc_services: waiting "restart firewall" via httpd ...
Aug 15 18:54:33 kernel: nvram_free: 1(init) nvram_idx(0 / 2)
Aug 15 18:54:36 kernel: nvram_free: 1(init) nvram_idx(1 / 2)
Aug 15 19:06:30 kernel: 7986@C15L2ra0,PeerGroupMsg2Action() 7169: AP SETKEYS DONE - ARMMap=WPA2-Persona
Aug 15 19:06:33 kernel: 7986@C15L2ra0,PeerGroupMsg2Action() 7169: AP SETKEYS DONE - ARMMap=WPA2-Persona
Aug 15 19:06:33 kernel: 7986@C15L2ra0,PeerGroupMsg2Action() 7169: AP SETKEYS DONE - ARMMap=WPA2-Persona
Aug 15 19:08:19 kernel: nvram_free: 1538(httppd) nvram_idx(0 / 2)
Aug 15 19:08:19 rc_services: httpd 1538(notify) rc ipsec_start
Aug 15 19:08:22 kernel: nvram_free: 1(init) nvram_idx(1 / 2)
Aug 15 19:08:22 ipsec: CA files are generated properly.
Aug 15 19:08:27 kernel: nvram_free: 1(init) nvram_idx(0 / 2)
Aug 15 19:08:31 BODP1: fun bitmap = 52*
```

3.15 Analitzador de trànsit

Traffic Analyzer us ofereix una visió general d'allò que passa a la xarxa diàriament, setmanalment o mensualment. Us permet consultar ràpidament l'amplada de banda de cada usuari o el dispositiu o l'aplicació que es fa servir de forma que us ajuda a reduir els colls d'ampolla de la connexió a Internet. També és una forma òptima de supervisar l'ús o les activitats d'internet dels usuaris.



Per configurar Traffic analyzer:

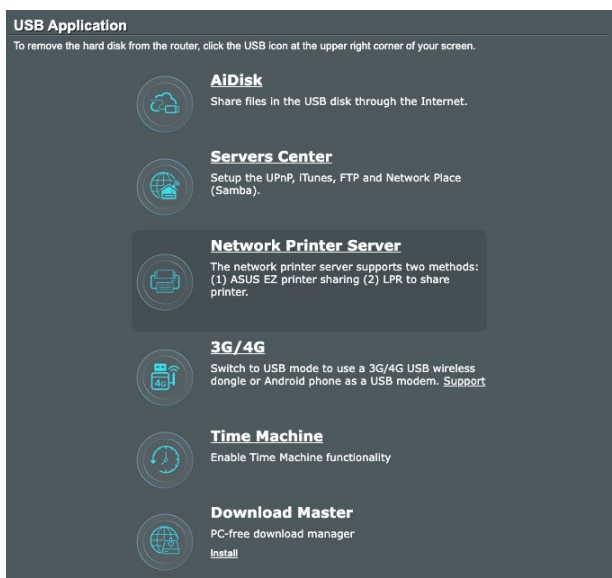
1. Al tauler de navegació, aneu a **General > Traffic Analyzer (Analitzador de trànsit)**.
2. A la pàgina principal de l'**Traffic Analyzer (Analitzador de trànsit)**, activeu les estadístiques de l'analitzador de trànsit.

3. Seleccioneu la data per a la qual voleu veure el gràfic.
4. Al camp **Display for (Visualitzar per)** a, seleccioneu l'encaminador o les aplicacions per mostrar-ne la informació de trànsit.
5. Al camp **Mostrar en**, seleccioneu com voleu mostrar la informació de trànsit.

3.16 Aplicació USB

La funció Aplicacions USB inclou els menús subordinats de: AiDisk, Servers Center, Servidor de la impressora de xarxa i Download Master.

IMPORTANT! Per utilitzar les funcions del servidor, haureu d'inserir un dispositiu de memòria USB (p. ex. un disc dur USB o una unitat de memòria USB) al port USB 3.0 que hi ha darrere del wireless router. Comproveu que el dispositiu d'emmagatzematge USB està correctament formatat i particionat. Al lloc web d'ASUS (<http://event.asus.com/2009/networks/disksupport/>) trobareu la taula de compatibilitat de sistemes de fitxers.



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

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

3.16.1 Ús de l'AiDisk

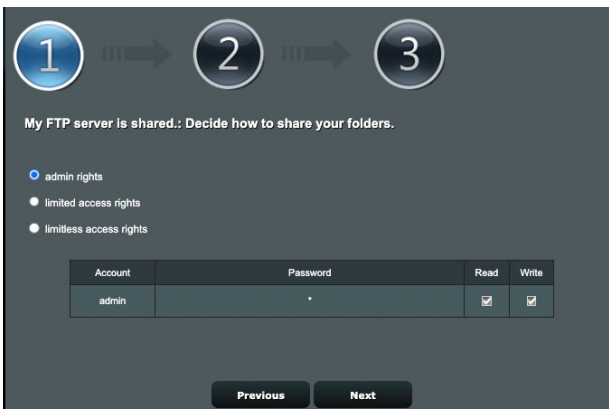
L'AiDisk us permet compartir els fitxers emmagatzemats en un dispositiu USB connectat a través d'Internet. L'AiDisk també us ajuda a configurar el DDNS d'ASUS i un servidor d'FTP.

Per utilitzar l'AiDisk:

1. Des del tauler de navegació, aneu a **General > Aplicació USB** i, seguidament, premeu la icona **AiDisk**.
2. Des de la pantalla Benvingut a l'assistent d'AiDisk, premeu **Endavant**.



3. Seleccioneu els drets d'accés que voleu assignar als clients que accedeixen a les dades compartides.



4. Creeu el nom del domini mitjançant els serveis de DDNS d'ASUS, llegiu les Condicions del servei i, seguidament, seleccioneu **Utilitzaré el servei i accepto les Condicions del servei** i introduïu el nom del domini. Quan acabeu, premeu **Següent**.



1 → 2 → 3

Create your domain name via the ASUS DDNS services.

I will use the service

Key in the name .asuscomm.com

Disable DDNS.

Previous Next

Podeu seleccionar **Omet la configuració de DDNS d'ASUS** i, a continuació, premeu **Següent** per ometre la configuració de DDNS.

5. Premeu **Finalitzar** per completar la configuració.
6. Per accedir al lloc d'FTP que heu creat, inicieu un navegador web o una utilitat de client d'FTP de tercers i introduïu l'enllaç ftp (**ftp://<domain name>.asuscomm.com**) que heu creat.

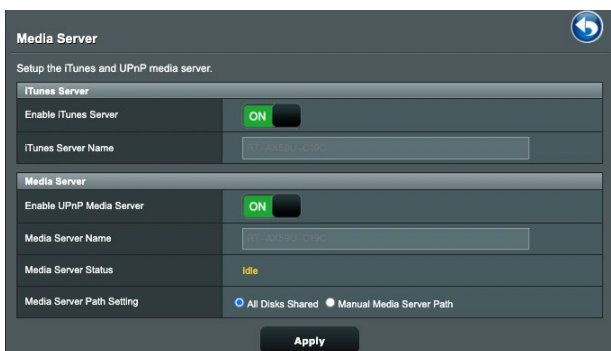
3.16.2 Ús del Servers Center

Servers Center us permet compartir els fitxers multimèdia des del disc USB a través d'un directori de servidor multimèdia, un servei d'ús compartit Samba o un servei d'ús compartit per FTP. També podeu configurar altres paràmetres per al disc USB al Servers Center.

Ús del servidor multimèdia

El wireless router permet que els dispositius compatibles amb UPnP accedeixin als fitxers multimèdia del disc USB connectat al wireless router.

NOTA: Abans d'utilitzar la funció Servidor multimèdia de UPnP, connecteu el dispositiu a la xarxa de l'encaminador.

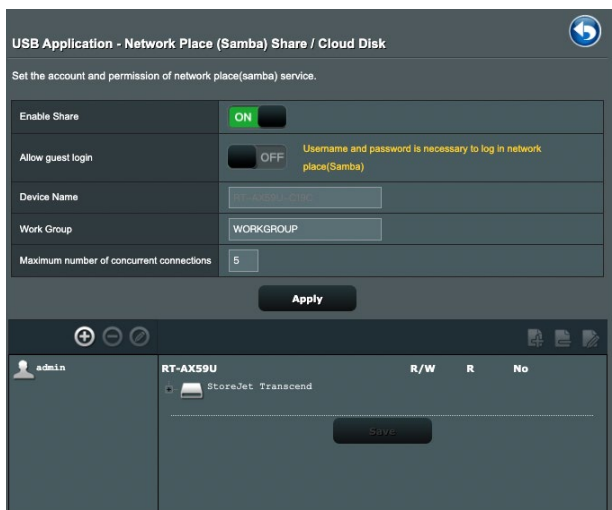


Des del tauler de navegació, aneu a **General > Aplicació USB > Multimèdia Servidors**. Consulteu la informació següent sobre els camps:

- **Activar servidor d'iTunes:** Seleccioneu ON/OFF per activar o desactivar el servidor d'iTunes.
- **Activa servidor multimèdia UPnP:** Seleccioneu ON/OFF per activar o desactivar el servidor multimèdia UPnP.
- **Estat del servidor multimèdia:** Mostra l'estat del servidor multimèdia.
- **Configuració del camí del servidor multimèdia:** seleccioneu **Tots els discs compartits** o **Camí del servidor multimèdia manual**.

Ús del servei d'ús compartit de llocs de la xarxa (Samba)

El servei d'ús compartit de llocs de la xarxa (Samba) permet configurar els comptes i els permisos del servei Samba.




Per utilitzar l'ús compartit Samba:

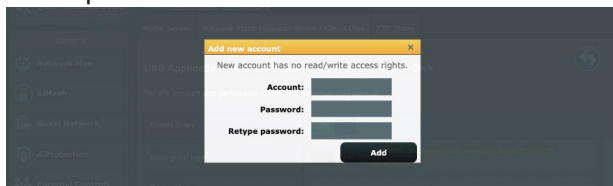
1. Des del tauler de navegació, aneu a **General > Aplicació USB > Ús compartit de llocs de la xarxa (Samba) / disc al núvol**.

NOTA: El servei d'ús compartit de llocs de la xarxa (Samba) està habilitat per defecte.


2. Seguiu els passos següents per afegir, eliminar o modificar un compte.

Per crear un compte nou:

- a) Premeu  per afegir un compte nou.
- b) Als camps **Compte** i **Contrasenya**, introduïu el nom i la contrasenya del client de la xarxa. Torneu a introduir la contrasenya per confirmar-la. Premeu **Afegir** per afegir el compte a la llista.

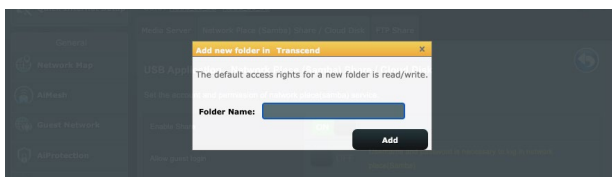


Per eliminar un compte existent:

- a) Seleccioneu el compte que voleu eliminar.
- b) Premeu .
- c) Quan se us demani, premeu **Eliminar** per confirmar la supressió d'un compte.

Per afegir una carpeta:

- a) Premeu .
- b) Introduïu el nom de la carpeta i premeu **Afegir**. La carpeta que heu creat s'afegirà a la llista de carpetes.



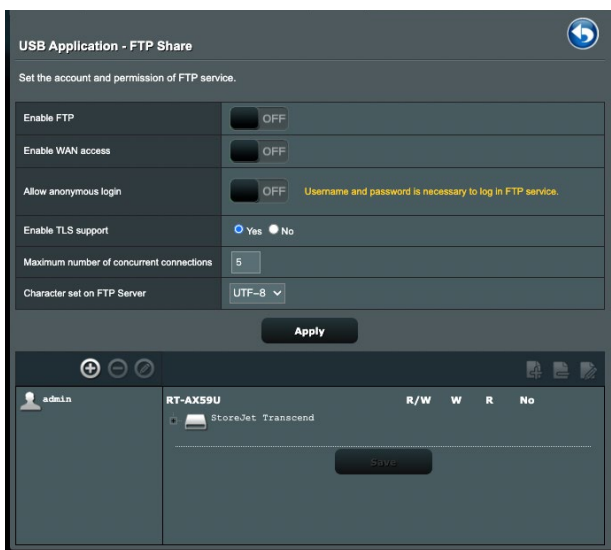
3. A la llista de carpetes, seleccioneu el tipus de permís d'accés que voleu assignar a carpetes específiques:
 - **L/E**: seleccioneu aquesta opció per donar accés de lectura i d'escriptura.
 - **L**: seleccioneu aquesta opció per donar accés només de lectura.
 - **No**: seleccioneu aquesta opció si no voleu compartir una carpeta de fitxers específica.
4. Premeu **Aplicar** per aplicar els canvis.

Ús del servei d'ús compartit per FTP

L'ús compartit per FTP permet que un servidor d'FTP comparteixi fitxers des del disc USB a altres dispositius mitjançant la xarxa d'àrea local o mitjançant Internet.

IMPORTANT!

- Extraieu el disc USB de forma segura. L'extracció incorrecta del disc USB pot provocar errors a les dades.
- Per extraure el disc USB de forma segura, consulteu la secció **Extracció segura del disc USB** sota l'apartat **3.11.3 Supervisió del dispositiu USB**.



Per utilitzar el servei d'ús compartit d'FTP:

NOTA: Comproveu que heu configurat el servidor d'FTP a través d'AiDisk. Per obtenir més informació, consulteu l'apartat **3.16.1 Ús de l'AiDisk**.

1. Des del tauler de navegació, aneu a **General > Aplicació USB > Ús compartit d'FTP**.
2. A la llista de carpetes, seleccioneu el tipus de drets d'accés que voleu assignar a carpetes específiques:
 - **L/E:** seleccioneu aquesta opció per assignar accés de lectura/ escriptura per a una carpeta específica.
 - **E:** seleccioneu aquesta opció per assignar accés d'escriptura per a una carpeta específica.
 - **L:** seleccioneu aquesta opció per assignar permís de lectura per a una carpeta específica.
 - **No:** Seleccioneu aquesta opció si no voleu compartir una carpeta específica.
3. Si ho preferiu, podeu establir el camp **Allow anonymous login (Permet inici de sessió anònim)** en **ON (Actiu)**.
4. Al camp **Maximum number of concurrent connections (Nombre màxim de connexions simultànies)**, introduïu el nombre de dispositius que poden connectar-se simultàniament al servidor FTP d'ús compartit.
5. Premeu **Aplicar** per confirmar els canvis.
6. Per accedir al servidor d'FTP, introduïu l'enllaç d'ftp **ftp://<hostname>.asuscomm.com** i el nom d'usuari i la contrasenya en un navegador web o una utilitat d'FTP de tercers.

3.16.3 3G/4G

Podeu connectar mòdems USB de 3G/4G al RT-AX59U per permetre l'accés a Internet.

NOTA: Per accedir a una llista de mòdem USB verificats, visiteu: <http://event.asus.com/2009/networks/3gsupport/>.

Per configurar l'accés a Internet 3G/4G:

1. Des del tauler de navegació, aneu a **General > Aplicació USB > 3G/4G**.
2. Al camp **Activar mòdem USB**, seleccioneu **Sí**.
3. Configureu el següent:
 - **Ubicació:** seleccioneu la ubicació del proveïdor de serveis 3G/4G de la llista desplegable.
 - **ISP:** seleccioneu el vostre proveïdor de serveis d'Internet (ISP) de la llista desplegable.
 - **Servei d'APN (Nom del punt d'accés), opcional:** posa't en contacte amb el proveïdor de serveis de 3G/4G per obtenir més informació.
 - **Número d'accés i codi PIN:** el número d'accés del proveïdor de 3G/4G i el codi PIN de connexió.

NOTA: El codi PIN pot variar en funció del proveïdor.

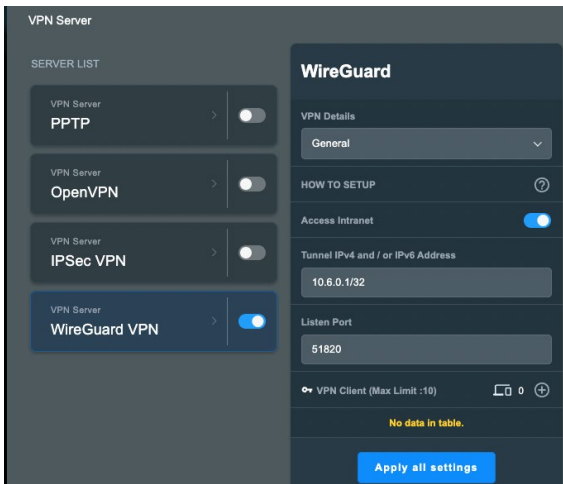
- **Nom d'usuari/contrasenya:** el proveïdor de la xarxa de 3G/4G us donarà el nom d'usuari i la contrasenya.
 - **Adaptador USB:** seleccioneu el vostre adaptador USB de 3G/4G de la llista desplegable. Si no sabeu quin és el model del vostre adaptador USB o no el trobeu a la llista, seleccioneu **Auto**.
4. Premeu **Aplicar**.

NOTA: El router es reiniciarà per aplicar la configuració.

3.17 VPN

VPN (Virtual Private Network) ofereix una comunicació segura a un ordinador remot o a una xarxa remota utilitzant una xarxa pública, com ara internet.

NOTA: Abans d'establir una connexió de VPN, necessitareu l'adreça IP o el nom del domini del servidor de VPN al qual proveu d'accedir.



3.17.1 Servidor de VPN


Per configurar l'accés a un servidor de VPN:

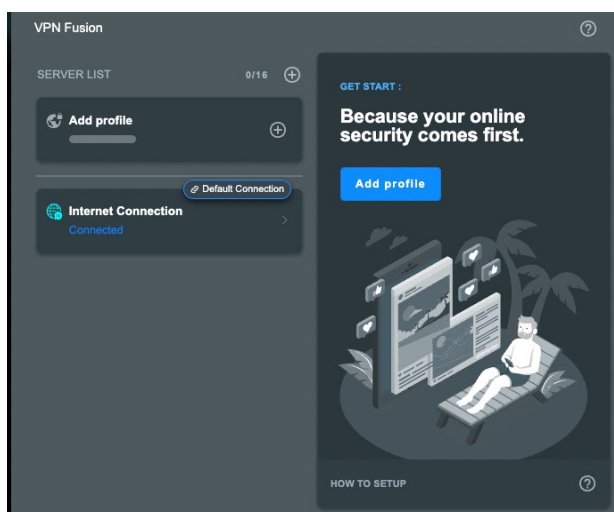
1. Des del tauler de navegació, aneu a **Configuració avançada > VPN Server (Servidor VPN)**.
2. Al camp **PPTP**, premeu **ON (Activat)**.
3. A la llista desplegable **VPN Details (Detalls de la VPN)**, seleccioneu **Advanced Settings (Configuració avançada)** si voleu configurar els paràmetres avançats de la VPN, com ara l'assistència per a la difusió, l'autenticació, l'encryptació MPPE i el rang d'adreces IP del client.
4. Al camp **Network Place (Samba) Support (Assistència de lloc de xarxa, Samba)**, premeu **ON (Activat)**.
5. Introduïu el nom d'usuari i la contrasenya per accedir al servidor de VPN. Premeu el botó **[+]**.
6. Premeu **Apply all settings (Aplica tots els paràmetres)**.

3.17.2 VPN Fusion

VPN Fusion us permet connectar-vos a diversos servidors VPN simultàniament i assignar els vostres dispositius de client perquè es connectin a a diferents túnels VPN. Alguns dispositius, com els descodificadors d'Internet, les Smart TV i els reproductors de Blu-ray no són compatibles amb el programari de VPN. Aquesta funció permet l'accés a la VPN als dispositius de la xarxa domèstica sense haver d'instal·lar programari per a VPN, mentre que el vostre smartphone segueix connectat a internet, no a la VPN. Per al Gamer, la connexió VPN contraresta els atacs de DDoS per evitar que el joc de PC o d'streaming es desconnecti dels servidors del joc. Establir una connexió VPN pot ser tan senzill com canviar la vostra adreça IP a la regió en que es troba el servidor del joc per millorar el temps de ping al servidor.

Per començar, seguïu els passos següents:

1. Feu clic al signe  que hi ha al costat de la **Server List (Llista de servidors)** o **Afegeix un perfil** per afegir un túnel de VPN nou.
2. Activeu la connexió VPN que heu creat a la llista de servidors.



3.17.3 Instant Guard

Instant Guard executa el vostre servidor VPN privat al vostre propi encaminador. Si feu servir un túnel VPN, totes les vostres dades passen a través del servidor. Amb Instant Guard, teniu el control total del vostre propi servidor i, per tant, es converteix en la solució més segura possible.

The screenshot shows the 'Instant Guard' configuration page. At the top, there is a title 'Instant Guard' and a descriptive paragraph: 'Instant Guard allows you to create a VPN tunnel with just one click via the ASUS Router app. You can monitor who's connected to your VPN Server with Instant Guard app.' Below this is a 'Basic Config' section with four rows: 'Instant Guard' with a green 'ON' toggle switch, 'Server IP Address' with a '-' sign, 'System Log' with a 'Check log' button, and 'Client will use VPN to access' with radio buttons for 'Internet only' (selected) and 'Internet and local network'. A note below the radio buttons states: 'The access setting will be applied to both IPsec VPN and Instant Guard.' Below the 'Basic Config' section is a 'Connection Status' section with a table header containing 'Remote IP', 'Client status', 'Access time', 'Device', and 'PSKRAUHTIME'. The table body is empty, with a message 'No data in table.' centered below the header.

Instant Guard				
Instant Guard allows you to create a VPN tunnel with just one click via the ASUS Router app. You can monitor who's connected to your VPN Server with Instant Guard app.				
Basic Config				
Instant Guard	<input checked="" type="checkbox"/> ON			
Server IP Address	-			
System Log	<input type="button" value="Check log"/>			
Client will use VPN to access	<input checked="" type="radio"/> Internet only <input type="radio"/> Internet and local network <small>The access setting will be applied to both IPsec VPN and Instant Guard.</small>			
Connection Status				
Remote IP	Client status	Access time	Device	PSKRAUHTIME
No data in table.				

3.18 WAN

3.18.1 Internet Connection (Connexió a Internet)

La pantalla de connexió a Internet permet configurar els paràmetres de diversos tipus de connexió WAN.

The screenshot shows the 'WAN - Internet Connection' configuration page. It is divided into several sections: 'Basic Config', 'WAN IP Setting', and 'WAN DNS Setting'. In the 'Basic Config' section, 'WAN Connection Type' is set to 'Static IP', 'Enable WAN' is checked, 'Enable NAT' is checked, 'Enable UPnP' is checked, and 'Enable WAN Aggregation' is unchecked. The 'WAN IP Setting' section shows 'IP Address' as 10.10.163.151, 'Subnet Mask' as 255.255.255.0, and 'Default Gateway' as 10.10.163.1. The 'WAN DNS Setting' section shows 'Filter Mode' as 'Fast DNS', 'Service Name' as 'Google', and 'DNS Server' as '8.8.8.8, 8.8.4.4'. There is an 'Assign' button next to the DNS server information. Other options include 'Forward local domain queries to upstream DNS' (checked), 'Enable DNS Rebind protection' (checked), 'Enable DNSSEC support' (checked), 'Prevent client auto DoH' (set to 'Auto'), and 'DNS Privacy Protocol' (set to 'None').

WAN - Internet Connection	
RT-AX59U supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.	
Configure the Ethernet WAN settings of RT-AX59U.	
Basic Config	
WAN Connection Type	Static IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP <small>UPnP FAQ</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 3 port to your modem's LAN ports (ensure you use two cables with the same specification). WAN Aggregation FAQ</small>
WAN IP Setting	
IP Address	10.10.163.151
Subnet Mask	255.255.255.0
Default Gateway	10.10.163.1
WAN DNS Setting	
DNS Server	Filter Mode: Fast DNS Service Name: Google DNS Server: 8.8.8.8, 8.8.4.4 <small>Assign a DNS service to improve security, block advertisement and gain faster performance.</small> Assign
Forward local domain queries to upstream DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable DNS Rebind protection	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable DNSSEC support	<input checked="" type="radio"/> Yes <input type="radio"/> No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

Per configurar els paràmetres de la connexió WAN:

1. Des del tauler de navegació, aneu a **Configuració avançada > WAN > Connexió a Internet**.
2. Configureu els següents paràmetres. Quan acabeu, premeu **Aplicar**.

- **Tipus de connexió WAN:** Seleccioneu el vostre tipus de proveïdor de serveis d'Internet. Les opcions són: **Automatic IP, PPPoE, PPTP, L2TP** o **IP fixa**. Poseu-vos en contacte amb el vostre proveïdor de serveis d'Internet (ISP) si el router no pot obtenir una adreça IP vàlida o si no sabeu quin és el vostre tipus de connexió WAN.
- **Habilitar WAN:** Seleccioneu **Sí** per permetre l'accés a Internet del router. Seleccioneu **No** per inhabilitar l'accés a Internet.
- **Habilitar NAT:** NAT (traducció d'adreces de la xarxa, de l'anglès Network Address Translation) és un sistema que utilitza una IP pública (WAN IP) per oferir accés a Internet als clients de la xarxa amb una adreça IP privada en una xarxa LAN. L'adreça IP privada de cada client de la xarxa es desa en una taula de NAT i s'utilitza per encaminar els paquets de dades d'entrada.
- **Habilitar UPnP:** UPnP (Universal Plug and Play) permet controlar diversos dispositius (p. ex. routers, televisions, sistemes estèreo, consoles de jocs i telèfon mòbil) mitjançant una xarxa basada en IP amb o sense un control central a través d'una passarel·la. UPnP connecta ordinadors amb tot tipus de factors de forma i ofereix una xarxa uniforme per a la configuració remota i la transferència de dades. UPnP permet detectar automàticament un dispositiu de xarxa nou. Després de connectar-se a la xarxa, els dispositius poden configurar-se de forma remota per a aplicacions de P2P, jocs interactius, videoconferències i servidors web o intermediaris. A diferència del reenviament de port, que implica la configuració manual dels paràmetres dels ports, l'UPnP configura automàticament el router perquè accepti les connexions d'entrada i les peticions directes a un ordinador específic de la xarxa local.
- **Connectar a servidor de DNS:** Permet que el router obtingui automàticament l'adreça IP de DNS del proveïdor de serveis d'Internet (ISP). Un DNS és un amfitrió d'Internet que tradueix els noms d'Internet a adreces IP numèriques.

- **Autenticació:** Alguns proveïdors de serveis d'Internet (ISP) especifiquen aquest element. Consulteu-los al vostre proveïdor de serveis d'Internet (ISP) i introduïu la informació necessària.
- **Nom de l'amfitrió:** Aquest camp permet introduir el nom de l'amfitrió del router. Sol ser un requisit especial del proveïdor de serveis d'Internet (ISP). Si el vostre proveïdor de serveis d'Internet (ISP) ha assignat un nom d'amfitrió al vostre equip, introduïu-lo aquí.
- **Adreça MAC:** L'adreça MAC (Media Access Control) és un identificador únic per al vostre dispositiu de xarxa. Alguns proveïdors de serveis d'Internet (ISP) supervisen l'adreça MAC dels dispositius de xarxa que es connecten al seu servei i rebutgen qualsevol dispositiu no reconegut que provi de connectar-se. Per evitar els problemes de connexió degut a una adreça MAC no registrada, podeu:
 - Poseu-vos en contacte amb el vostre proveïdor de serveis d'Internet (ISP) i actualitzeu l'adreça MAC associada amb el servei de l'ISP.
 - Cloneu o canvieu l'adreça MAC del wireless router ASUS en funció de l'adreça MAC de l'anterior dispositiu de xarxa reconegut per l'ISP.
- **Freqüència de consulta DHCP:** Canvia l'interval de detecció de DHCP per evitar carregar excessivament el servidor de DHCP.

3.18.2 WAN dual

La WAN dual us permet seleccionar dues connexions d'ISP al router, una WAN primària i una WAN secundària.

- **Mode de commutació per error:** Seleccioneu aquest mode per utilitzar la WAN secundària com a accés a la xarxa en cas de fallada.
- **Mode d'equilibri de càrregues:** Seleccioneu aquest mode per optimitzar l'amplada de banda, minimitzar el temps de resposta i evitar sobrecàrregues de dades per a les connexions WAN primàries i secundàries.

WAN - Dual WAN

RT-AX59U provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)

To enable WAN Aggregation go to the [WAN-Internet Connection](#) page.

Basic Config

Enable Dual WAN	<input checked="" type="checkbox"/> ON
Primary WAN	WAN
Secondary WAN	USB
Dual WAN Mode	Fail Over <input checked="" type="checkbox"/> Allow fallback

Auto Network Detection

Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.

Detect Interval	Every 3 seconds
Fallover Trigger Condition	When the current WAN fails 2 continuous times, fallover to Secondary WAN
Fallback Trigger Condition	When the Primary WAN is detected to have an active internet connection using a physical cable for 4 continuous times, fallback to the Primary WAN.
Network Monitoring	<input type="checkbox"/> DNS Query <input type="checkbox"/> Ping

Apply

3.18.3 Activació de ports

L'activació d'un interval de ports obre un port d'entrada predeterminat durant un període de temps limitat cada vegada que un client de la xarxa LAN estableix una connexió de sortida en un port especificat. L'activació de ports s'utilitza en els escenaris següents:

- Quan hi ha més d'un client local que demana un reenviament de port per a la mateixa aplicació en un moment diferent.
- Quan una aplicació demana ports d'entrada específics que no coincideixen amb els ports de sortida.

WAN - Port Trigger

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

[Port Trigger FAQ](#)

Basic Config

Enable Port Trigger Yes No



Well-Known Applications

Trigger Port List (Max Limit : 32)

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

Per configurar l'activació de ports:

1. Des del tauler de navegació, aneu a **Configuració avançada > WAN > Activació de ports**.
2. Al camp **Enable Port Trigger (Habilitar activació de ports)**, marqueu **Yes (Sí)**.
3. Al camp **Well-Known Applications (Aplicacions conegudes)**, seleccioneu jocs i serveis web populars per afegir-los a la llista d'activació de ports.
4. A la taula **Trigger Port List (Llista de port d'activació)**, introduïu la informació següent:
 - **Descripció:** Introduïu un nom o una descripció breu per al servei.

- **Port d'activació:** Especifiqueu el port activat per obrir el port d'entrada.
 - **Protocol:** Seleccioneu el protocol: TCP o UDP.
 - **Port d'entrada:** Especifiqueu un port d'entrada per rebre dades d'entrada d'Internet.
5. Premeu el botó **Add (Afegir)**  per introduir la informació d'activació de port a la llista. Premeu el botó **Delete (Eliminar)**  per eliminar una entrada d'activació de port de la llista.
 6. Quan acabeu, premeu **Aplicar**.

NOTES:

- Quan us connecteu a un servidor IRC, un equip client estableix una connexió de sortida utilitzant l'interval de ports d'activació 66660-7000. El servidor IRC verifica el nom d'usuari i estableix una connexió nova amb l'equip del client mitjançant un port d'entrada.
 - Si es deshabilita l'activació de ports, el router atura la connexió perquè no pot determinar quin equip demana accés a IRC. Si s'habilita l'activació de ports, el router assigna un port d'entrada per rebre les dades d'entrada. El port d'entrada es tanca quan passa el període de temps especificat perquè el router no sap segur en quin moment deixa d'utilitzar-se l'aplicació.
 - L'activació de ports permet que només un client de la xarxa utilitzi un servei concret i un port d'entrada específic alhora.
 - No podeu utilitzar la mateixa aplicació per activar un port en més d'un equip alhora. el router només reenviarà el port al darrer equip per enviar al router una sol·licitud d'activació.
-

3.18.4 Servidor virtual/reenviament de port

El reenviament de port és un mètode per dirigir el trànsit de la xarxa des d'Internet a un port específic o un interval específic de ports a un dispositiu o a un número de dispositius de la xarxa local. Configurar el reenviament de port al router permet que equips externs a la xarxa puguin accedir a serveis específics que ofereix un equip de la vostra xarxa.

WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.

If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port blank.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with RT-AX59U's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with RT-AX59U's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

Basic Config

Enable Port Forwarding ON

Port Forwarding List (Max Limit : 64)

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



[Add profile](#)

Per configurar el reenviament de port:

1. Des del tauler de navegació, aneu a **Configuració avançada > WAN > Servidor virtual / reenviament de port.**
2. Al camp **Enable Port Forwarding (Activa reenviament de ports)**, marqueu **Yes (Sí)**.
3. Fes clic a **Afegir perfil** i introdueix la següent informació a la taula **Llista de Redirecció de Ports**:
 - **Nom del servei:** Introduïu el nom del servei.
 - **Protocol:** Seleccioneu el protocol. No no n'esteu segur, seleccioneu **TOTS DOS**.
 - **Port Extern:** El Port Extern accepta els següents formats:
 - 1) Rangs del port utilitzant els dos punts (":") entre el port inicial i el final, com ara 300:350.
 - 2) Ports únics utilitzant la coma (",") entre els ports individuals, com ara 566, 789.

- 3) Una combinació de rangs de ports i rangs únics utilitzant dos punts (":") i comes (",") com ara 1015:1024, 3021.
- **IP local (Adreça IP d'Internet):** Introduïu l'adreça IP de la LAN del client.

NOTA: Utilitzeu una adreça IP estàtica per al client local perquè el reenviament de port funcioni correctament. Consulteu l'apartat **3.10 LAN** per obtenir més informació.

- **Port local (Port d'Internet):** Introduïu un port específic per rebre els paquets reenviats. Deixeu aquest camp en blanc si voleu que els paquets d'entrada es redirigeixin a l'interval de ports especificat.
 - **Source IP (Adreça IP):** si vols obrir el teu port per a una adreça IP específica, introdueix la direcció IP que vols especificar al camp Adreça IP.
4. Premeu el botó **Add (D'Afegir)**  per introduir la informació d'activació de port de la llista. Premeu el botó de **Delete (Suprimir)**  per eliminar una entrada d'activació de port de la llista.
5. Quan acabeu, premeu **Aplicar**.

Per comprovar si el reenviament de port s'ha configurat correctament:

- Comproveu que el servidor o l'aplicació estan configurats i en execució.
- Necessitareu un client extern a la LAN amb accés a Internet (conegut com a "client d'Internet"). Aquest client no ha d'estar connectat al router ASUS.
- Al client d'Internet, utilitzeu l'adreça IP de la WAN del router per accedir al servidor. Si el reenviament de port s'ha configurat correctament, hauríeu de poder accedir als fitxers o a les aplicacions.

Diferències entre l'activació de ports i el reenviament de port:

- L'activació de ports funciona sense configurar una adreça IP específica per a la xarxa LAN. A diferència del reenviament de port, que requereix una adreça IP de LAN estàtica, l'activació de ports permet el reenviament de port dinàmic mitjançant el router. Els intervals de ports predeterminats estan configurats per acceptar les connexions d'entrada durant un període de temps limitat. L'activació de ports permet que diversos equips executin aplicacions que normalment demanen un reenviament manual dels mateixos ports a cada ordinador de la xarxa.
- L'activació de ports és més segura que el reenviament de port perquè els ports d'entrada no estan oberts tot el temps. Només s'obren quan una aplicació estableix una connexió de sortida mitjançant el port d'activació.

3.18.5 DMZ

La DMZ (zona desmilitaritzada de la xarxa) virtual exposa un client a Internet i, d'aquesta manera, permet que aquest client rebi tots els paquets d'entrada dirigits a la vostra LAN.

El trànsit d'entrada procedent d'Internet normalment es rebutja i s'encamina a un client específic només si s'ha configurat el reenviament de port o una activació de port a la xarxa. En una configuració de DMZ, un client de la xarxa rep tots els paquets d'entrada.

Configurar DMZ en una xarxa és útil quan necessiteu els ports d'entrada oberts o quan voleu allotjar un domini, web o servidor de correu.

PRECAUCIÓ: L'obertura a Internet de tots els ports d'un client fa que la xarxa sigui vulnerable als atacs exteriors. Heu de ser conscients dels riscos de seguretats que comporta l'ús de la DMZ.

Per configurar la DMZ:

1. Des del tauler de navegació, aneu a **Configuració avançada > WAN > DMZ**.
2. Configureu els paràmetres següents. Quan acabeu, premeu **Aplicar**.
 - **Adreça IP de l'estació exposada:** Introduïu l'adreça IP de la LAN del client que oferirà el servei de DMZ i estarà exposat a Internet. Comproveu que el client del servidor té una adreça IP estàtica.

Per suprimir la DMZ:

1. Elimineu l'adreça IP de la LAN del client del quadre de text **Adreça IP de l'estació exposada**.
2. Quan acabeu, premeu **Aplicar**.

3.18.6 DDNS

La configuració de la DDNS (Dynamic DNS) us permet accedir al router des de l'exterior de la xarxa mitjançant el servei DDNS d'ASUS o un altre servei de DDNS.

WAN - DDNS	
<p>DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.</p> <p>If you cannot use ASUS DDNS services, please go to https://plookup.asus.com/nslookup.php to reach your internet IP address to use this service.</p> <p>The wireless router currently uses a private WAN IP address. This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.</p>	
Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	WWW.ASUS.COM
Host Name	Key in the name .asuscomm.com
DDNS Status	Inactive
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None
Apply	

Per configurar la DDNS:

1. Des del tauler de navegació, aneu a **Configuració avançada > WAN > DDNS**.
2. Configureu els següents paràmetres. Quan acabeu, premeu **Aplicar**.
 - **Habilita el client de DDNS:** Habiliteu el DDNS per accedir al router ASUS pel noms de DNS, enlloc d'utilitzar l'adreça IP de la WAN.
 - **Nom de servidor i amfitrió:** Seleccioneu DDNS ASUS o un altre DDNS. Si voleu utilitzar el DDNS ASUS, introduïu el nom d'amfitrió en format xxx.asuscomm.com (xxx correspon al vostre nom d'amfitrió).
 - Si voleu utilitzar un servei de DDNS, premeu PROVA GRATUÏTA i registreu-vos en línia. Ompliu els camps Nom d'usuari o Adreça electrònica i Contrasenya o Clau de DDNS.
 - **Habilita comodí:** Habiliteu el comodí si el vostre servei de DDNS el demana.

NOTES:

El servei de DDNS no funciona en aquests casos:

- Quan el wireless router utilitza una adreça IP WAN privada (192.168.x.x, 10.x.x.x o 172.16.x.x), que s'indica amb un text en groc.
 - Quan el router es troba en una xarxa que utilitza múltiples taules NAT.
-

3.18.7 Pas NAT

Pas NAT permet que la xarxa privada virtual (VPN) passi a través del router i arribi als clients de la xarxa. Pas PPTP, pas L2TP, pas IPsec i pas RTSP estan habilitats per defecte.

Per habilitar/inhabilitar la configuració de pas NAT, aneu a **Configuració avançada > WAN > Pas NAT**. Quan acabeu, premeu **Aplicar**.

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

Apply

3.19 Wireless

3.19.1 General

La General us permet configurar els paràmetres wireless bàsics.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect OFF

2.4 GHz

Network Name (SSID) ASUS_80_2G

Hide SSID Yes No

Wireless Mode Auto big Protection Disable 11b

802.11ax / WiFi 6 mode Enable If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: [FAQ](#)

WiFi Agile Multiband Enable

Target Wake Time Disable

Channel bandwidth 20/40 MHz

Control Channel Auto Current Control Channel: 6
 Auto select channel including channel 12, 13

Extension Channel Auto

Authentication Method WPA2-Personal

WPA Encryption AES

WPA Pre-Shared Key 093369365

Protected Management Frames Disable

Group Key Rotation Interval 3600

5 GHz

Network Name (SSID) ASUS_80_5G

Hide SSID Yes No

Wireless Mode Auto

802.11ax / WiFi 6 mode Enable If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: [FAQ](#)

WiFi Agile Multiband Enable

Target Wake Time Disable

Channel bandwidth 20/40/80 MHz Enable 160 MHz

Per configurar els paràmetres wireless bàsics:

1. Des del tauler de navegació, aneu a **Configuració avançada > Wireless > General**.
2. Seleccioneu la banda de freqüència de 2,4 GHz o 5 GHz per a la xarxa sense fil.
3. Si voleu fer servir la funció Smart Connect, llisqueu el controlador del camp **Enable Smart Connect (Activar Smart Connect)** a la posició **ON**. Aquesta funció connecta

automàticament els clients de la xarxa a la banda apropiada (2,4 GHz o 5 GHz) per a una velocitat òptima.

4. Especifiqueu un nom únic amb un màxim de 32 caràcters per a l'SSID (Service Set Identifier, identificador de conjunt de serveis) o el nom de la xarxa per identificar la xarxa sense fil. Els dispositius Wi-Fi podran identificar i connectar-se a la xarxa sense fil amb l'SSID assignat. Els SSID del bàner informatiu s'actualitzen quan es desen els nous SSID als paràmetres.

NOTA: Podeu assignar SSID únics per a les bandes de freqüència de 2,4 GHz i 5 GHz.

5. Al camp **Ocultar SSID**, seleccioneu **Sí** per evitar que altres dispositius wireless puguin detectar el vostre SSID. Si activeu aquesta funció, haureu d'introduir l'SSID manualment al dispositiu wireless per accedir a la xarxa wireless.
6. Al camp **Wireless Mode (Mode sense fil)**, seleccioneu alguna d'aquestes opcions de mode sense fil per determinar els tipus de dispositius sense fil que poden connectar-se a l'encaminador sense fil.
 - **Auto:** Seleccioneu **Auto** perquè puguin connectar-se al wireless router els dispositius de 802.11ac, 802.11n, 802.11g i 802.11b.
 - **Només N:** Seleccioneu **N only (Només N)** per maximitzar el rendiment sense fil N. Aquesta opció evita que els dispositius de 802.11g i 802.11b puguin connectar-se a l'encaminador sense fil.
 - **Tradicional:** Seleccioneu **Tradicional** perquè puguin connectar-se al wireless router els dispositius de 802.11b/g/n. Recordeu que el hardware compatible de forma nativa amb 802.11n, només s'executarà a una velocitat màxima de 54 Mbps.
7. Al camp Control Channel (Canal de control), seleccioneu el canal operatiu per a l'encaminador sense fil. Seleccioneu **Auto** perquè l'encaminador sense fil pugui seleccionar automàticament el canal amb menys interferències.
8. Seleccioneu l'amplada de banda de canal per permetre velocitats de transmissió més altes.
9. Seleccioneu el mètode d'autenticació.
10. Quan acabeu, premeu **Aplicar**.

3.19.2 WPS

WPS (configuració protegida per WiFi, de l'anglès WiFi Protected Setup) és un estàndard de seguretat wireless que permet connectar fàcilment dispositius a una xarxa wireless. Podeu configurar la funció WPS mitjançant el botó WPS o el codi PIN.

NOTA: Comproveu que els dispositius són compatibles amb WPS.

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/> ON
Current Frequency	2.4 GHz / 5 GHz
Connection Status	Idle / Idle
Configured	Yes / Yes <input type="button" value="Reset"/> Pressing the reset button resets the network name (SSID) and WPA encryption key.
AP PIN Code	<input type="text" value="05477616"/>

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: Push button Client PIN Code

Per activar la WPS a la vostra xarxa wireless:

1. Des del tauler de navegació, aneu a **Configuració avançada > Wireless > WPS**.
2. Al camp **Activar WPS**, desplaceu el botó lliscant cap a **Activar**.
3. WPS fa servir 2,4 GHz de forma predeterminada. Si voleu canviar la freqüència a 5 GHz, trieu **Desactivat** per a la funció WPS, premeu **Canviar freqüència** al camp **Freqüència actual** i torneu a triar **Activar** per a la WPS.

NOTA: WPS admet l'autenticació mitjançant sistema obert, WPA/WPA2/WPA3-Personal. WPS no admet xarxes wireless que facin servir un mètode de xifratge de clau compartida, WPA-Enterprise, WPA2-Enterprise i RADIUS.

4. Al camp del mètode WPS, seleccioneu **Botó pulsador** o **Codi PIN de client**. Si trieu **Botó pulsador**, aneu al pas 5. Si trieu **Codi PIN de client**, aneu al pas 6.
5. Per configurar la WPS mitjançant el botó de WPS del router, seguiu aquests passos:
 - a. Premeu **Inici** o premeu el botó de WPS del darrere del wireless router.
 - b. Premeu el botó de WPS del dispositiu wireless. Normalment s'identifica amb el logotip de WPS.

NOTA: Reviseu el dispositiu wireless o consulteu-ne el manual de l'usuari per saber on és el botó de WPS.

- c. El wireless router cercarà els dispositius de WPS disponibles. Si el wireless router no troba cap dispositiu de WPS, passarà al mode d'espera.
6. Per configurar la WPS amb el codi PIN del client, seguiu aquests passos:
 - a. Cerqueu el codi PIN de la WPS al manual de l'usuari del dispositiu wireless o al propi dispositiu.
 - b. Introduïu el codi PIN del client al quadre de text.
 - c. Premeu **Inici** perquè el wireless router entri en mode de monitoratge WPS. Els llums indicadors del router parpellegen ràpidament tres cops abans de completar la configuració de la WPS.

3.19.3 Bridge

Bridge o WDS (sistema de distribució wireless, de l'anglès Wireless Distribution System) permet que el wireless router ASUS es connecti a un altre punt d'accés wireless de forma exclusiva i evita que altres dispositius wireless o estacions puguin accedir al wireless router ASUS. També es pot considerar com a un repetidor wireless ja que el wireless router ASUS es comunica amb un altre punt d'accés i amb altres dispositius wireless.

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your RT-AX59U to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

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

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

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

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

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

Basic Config

2.4 GHz MAC	<input type="text" value="C8:7F:54:22:C1:9C"/>
5 GHz MAC	<input type="text" value="CA:7F:54:32:C1:9C"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)

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

Per configurar el wireless bridge:

1. Des del tauler de navegació, aneu a **Configuració avançada > Wireless > WDS**.
2. Seleccioneu la banda de freqüència del wireless bridge.


3. Al camp **Mode AP**, seleccioneu una de les opcions següents:
 - **Només AP**: Desactiva la funció wireless bridge.
 - **Només WDS**: Permet la funció wireless bridge però evita que altres dispositius wireless o estacions es connectin al router.
 - **HÍBRID**: Permet la funció wireless bridge i permet que altres dispositius wireless o estacions es connectin al router.

NOTA: En mode híbrid, els dispositius wireless connectats al wireless router ASUS només rebran la meitat de la velocitat de connexió del punt d'accés.

4. Al camp **Connectar als AP de la llista**, premeu **Sí** si voleu connectar-vos a un punt d'accés (AP) de la llista d'AP remots.
5. De forma predeterminada, el canal de control del pont sense fil s'estableix en **Auto** perquè l'encaminador pugui seleccionar automàticament el canal amb menys interferències.

Podeu modificar el **Control Channel (Canal de control)** a la **Advanced Settings (Configuració avançada) > Wireless (Sense fil) > General**.

NOTA: La disponibilitat de canals varia en funció del país o de la regió.

6. A la llista d'AP remots, introduïu una adreça MAC i premeu el botó **Afegir**  per introduir l'adreça MAC d'altres punts d'accés disponibles.

NOTA: Qualsevol punt d'accés afegit a la llista ha d'estar al mateix canal de control que el wireless router ASUS.

7. Premeu **Aplicar**.

3.19.4 Filtre wireless MAC

El filtre wireless MAC ofereix control sobre els paquets que es transmeten a una adreça MAC (control de l'accés dels mitjans, de l'anglès Media Access Control) especificada a la xarxa wireless.

Wireless - Wireless MAC Filter


Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

Basic Config

Band	2.4 GHz
Enable MAC Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No

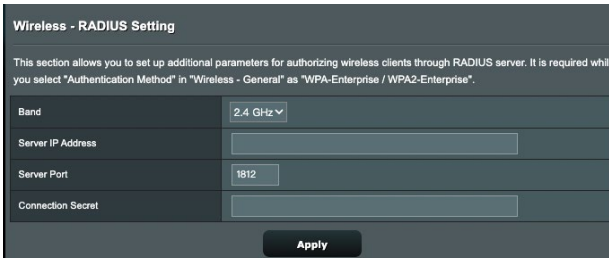
Apply

Per configurar el filtre wireless MAC:

1. Des del tauler de navegació, aneu a **Configuració avançada > wireless > Filtre wireless MAC**.
2. Seleccioneu la banda de freqüència.
3. Marqueu **Sí** al camp **Activar filtre MAC**.
4. A la llista desplegable **Mode de filtre MAC**, seleccioneu **Acceptar** o **Rebutjar**.
 - Seleccioneu **Acceptar** perquè els dispositius de la llista de filtres MAC puguin accedir a la xarxa wireless.
 - Seleccioneu **Rebutjar** perquè els dispositius de la llista de filtres MAC no puguin accedir a la xarxa wireless.
5. A la llista de filtres MAC, premeu el botó **Afegir**  i introduïu l'adreça MAC del dispositiu wireless.
6. Premeu **Aplicar**.

3.19.5 Configuració de RADIUS

La funció RADIUS (servei d'usuari de marcatge d'autenticació remota, de l'anglès Remote Authentication Dial In User Service) ofereix una capa addicional de seguretat quan es tria WPA-Enterprise, WPA2-Enterprise o Radius amb 802.1x com a mode d'autenticació.



Wireless - RADIUS Setting	
This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".	
Band	2.4 GHz ▾
Server IP Address	<input type="text"/>
Server Port	1812
Connection Secret	<input type="text"/>
Apply	

Per configurar la funció RADIUS wireless:

1. Confirmeu que el mode d'autenticació del wireless router és WPA-Enterprise, WPA2-Enterprise.

NOTA: Aneu a l'apartat **3.19.1 General** per configurar el mode d'autenticació del wireless router.

2. Des del tauler de navegació, aneu a **Configuració avançada > Wireless > Configuració de RADIUS**.
3. Seleccioneu la banda de freqüència.
4. Al camp **Adreça IP del servidor**, introduïu l'adreça IP del servidor RADIUS.
5. Al camp **Server Port (Port del servidor)**, introduïu el port del servidor.
6. Al camp **Secret de connexió**, introduïu la contrasenya que s'utilitzarà per accedir al servidor RADIUS.
7. Premeu **Aplicar**.

3.19.6 Professional

La pantalla Professional ofereix opcions de configuració avançades.

NOTA: Us recomanem que empreu els valors predeterminats d'aquesta pàgina.

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

Apply

A la pantalla **Configuració professional**, podeu configurar el següent:

- **Banda:** Seleccioneu la banda de freqüència de la configuració professional.
- **Activar ràdio:** Seleccioneu **Sí** per activar la xarxa wireless. Seleccioneu **No** per desactivar la xarxa wireless.
- **Habilitar planificador wireless:** Seleccioneu **Yes (Sí)** per activar i configurar el planificador sense fil. Seleccioneu **No** per desactivar la planificador wireless.
 - **Data per activar emissions de xarxa wifi (entre setman):** Podeu especificar els dies entre setmana que voleu activar la xarxa sense fil.
 - **Hora del dia per activar emissions de xarxa wifi:** Podeu

especificar un interval de temps en què s'activarà la xarxa sense fil durant la setmana.

- **Data per activar emissions de xarxa wifi (cap de setmana):** Podeu especificar els dies de cap de setmana que voleu activar la xarxa sense fil.
- **Hora del dia per activar emissions de xarxa wifi:** Podeu especificar un interval de temps en què s'activarà la xarxa sense fil durant el cap de setmana.
- **Establir AP Aïllat:** L'element Set AP isolated (**Establir AP aïllat**) evita que els dispositius sense fils de la xarxa puguin comunicar-se entre ells. Aquesta funció és útil si teniu molts convidats que entren i surten de la vostra xarxa amb freqüència. Seleccioneu **Yes (Sí)** per activar aquesta funció o seleccioneu **No** per desactivar-la.
- **Assistent d'Itinerància:** A les configuracions de xarxa amb múltiples repetidors sense fil, punts o accessos, els clients sense fil normalment no poden connectar-se automàticament als punts d'accés disponibles perquè segueixen connectats a l'encaminador sense fil principal. Activeu aquesta opció perquè el client es desconnecti de l'encaminador sense fil principal i es connecti a un senyal més potent, si la potència del senyal es troba per sota d'un llindar específic.
- **Habilita l'escolta d'IGMP:** Activar aquesta funció permet controlar l'IGMP (Internet Group Management Protocol) entre dispositius i optimitza el trànsit de multidifusió sense fil.
- **Velocitat multidifusió (Mbps):** Seleccioneu la velocitat de transmissió de multidifusió o premeu **Desactivar** per desactivar la transmissió individual simultània.
- **Tipus de preàmbul:** El Tipus de preàmbul defineix la durada de temps que dedica l'encaminador al CRC (control de redundància cíclica, de l'anglès Cyclic Redundancy Check). CRC és un mètode que permet detectar errors durant la transmissió de dades. Seleccioneu **Short (Breu)** per a una xarxa sense fil amb molt trànsit. Seleccioneu **Long (Llarg)** si la vostra xarxa sense fil consta de dispositius sense fil més antics o heretats.
- **AMPDU RTS:** Activar aquesta funció permet crear un grup de trames abans de transmetre'ls i fer servir RTS per a cada AMPDU en la comunicació entre dispositius 802.11g i 802.11b.
- **Llindar d'RTS:** Seleccioneu un valor baix per a RTS (sol·licitud d'enviament, de l'anglès Request to Send) per millorar la comunicació wireless en una xarxa ocupada i sorollosa amb molt

tràfic i molts dispositius wireless.

- **Interval de DTIM:** L'interval de DTIM (missatge d'indicació de trànsit d'enviament, de l'anglès Delivery Traffic Indication Message) o la velocitat del senyal de dades (de l'anglès Data Beacon Rate) es refereixen a l'interval de temps abans d'enviar un senyal a un dispositiu wireless en mode de repòs indicant que hi ha un paquet de dades que espera per ser enviat. El valor predeterminat és de tres mil·lisegons.
- **Interval de senyal:** L'interval de senyal és el temps entre un DTIM i el següent. El valor predeterminat és de 100 mil·lisegons. Baixeu el valor de l'interval de senyal per a una connexió wireless inestable o per a dispositius en itinerància.
- **Habilitar TX Bursting:** Habilitar TX Bursting millora la velocitat de transmissió entre el wireless router i dispositius 802.11g.
- **Habilitar WMM APSD:** Habilitar WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) per millorar la gestió energètica entre dispositius wireless. Seleccioneu **Deshabilitar** per apagar WMM APSD.
- **Optimitza l'agrupació AMPDU:** Optimitzeu el nombre màxim d'MPDU en un AMPDU i eviteu que els paquets es perdin o es malmetin durant la transmissió als canals sense fils propensos a errors.
- **Turbo QAM:** Activar aquesta funció permet utilitzar 256-QAM (MCS 8/9) a la banda de 2,4 GHz per millorar el rang i el rendiment en aquesta freqüència.
- **Equitat en el temps d'emissió:** Amb l'equitat en el temps d'emissió, la velocitat de la xarxa no ve determinada pel trànsit més lent. Si s'assigna el temps de forma equitativa entre els clients, l'equitat en el temps d'emissió permet que totes les transmissions es transmetin a la seva màxima velocitat potencial.
- **Formació explícita de feixos:** L'adaptador WLAN del client i l'encaminador admeten la tecnologia de formació de feixos. Aquesta tecnologia permet que aquests dispositius es comuniquin entre si l'estimació de canal i l'objectiu del redireccionament per millorar la velocitat de baixada i de pujada.
- **Formació universal de feixos:** Per als adaptadors de xarxa sense fil antics que no admeten la formació de feixos, l'encaminador estima el canal i determina l'objectiu del redireccionament per millorar la velocitat de baixada.

4 Utilitats

NOTES:

- Descarregueu i instal·leu les utilitats del wireless router des del lloc web d'ASUS:
 - Device Discovery versió 1.4.7.1 a <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
 - Firmware Restoration versió 1.9.0.4 a <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Windows Printer Utility versió 1.0.5.5 a <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
 - Les utilitats no són compatibles amb el sistema operatiu del Mac.
-

4.1 Device Discovery

Device Discovery és una utilitat WLAN d'ASUS que detecta un dispositiu de wireless router ASUS i us permet configurar els paràmetres de la xarxa wireless.

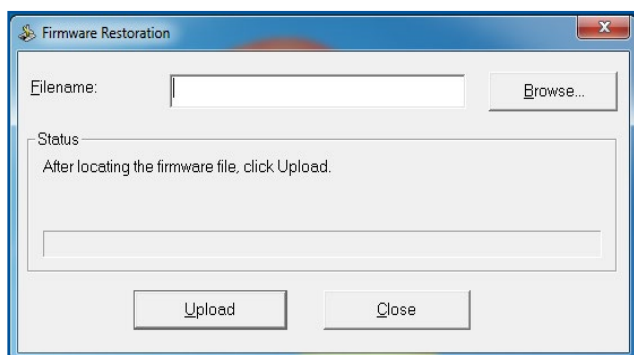
Per executar la utilitat Device Discovery:

- Des de l'escriptori de l'ordinador, premeu **Inicia > Tots els programes > Utilitat ASUS > ASUS Wireless router > Device Discovery**.

NOTA: Si configureu el mode de punt d'accés al router, haureu d'utilitzar Device Discovery per obtenir l'adreça IP del router.

4.2 Firmware Restoration

La utilitat Firmware Restoration s'utilitza quan el wireless router ASUS falla durant el procés d'actualització del firmware. Carrega el firmware que l'usuari especifica. El procés triga uns 3 o 4 minuts.



IMPORTANT! Executeu el mode rescat al router abans de fer servir la utilitat Firmware Restoration.

NOTA: Aquesta funció no és compatible amb el sistema operatiu del Mac.

Per executar el mode de rescat i utilitzar la utilitat Firmware Restoration:

1. Desendolheu el wireless router de la font d'alimentació.
2. Premeu el botó Reset del darrere i simultàniament torneu a endollar el wireless router a la font d'alimentació. Deixeu anar el botó Reset quan el llum d'alimentació del tauler frontal parpellegi lentament, que indica que el wireless router està en mode de rescat.

3. Establiu una IP estàtica al vostre ordinador i feu servir les dades següents per configurar els paràmetres de TCP/IP:

Adreça IP: 192.168.1.x

Màscara de subxarxa: 255.255.255.0

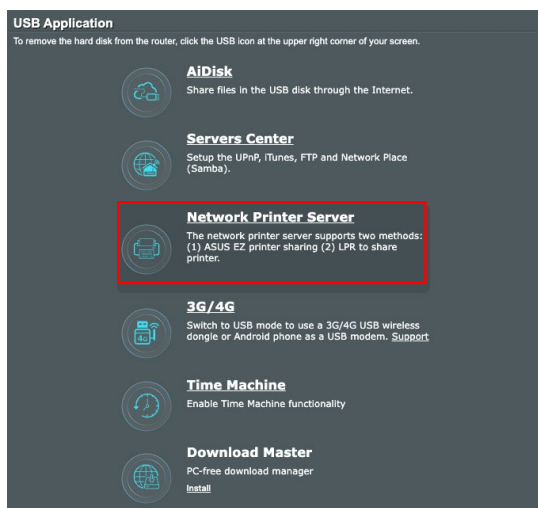
4. Des de l'escriptori de l'ordinador, premeu **Inicia > Tots els programes > Utilitat ASUS RT-AX59U Wireless router > Firmware Restoration**.
5. Especifiqueu un fitxer de firmware i premeu **Pujar**.

NOTA: Aquesta no és una utilitat d'actualització de firmware i no pot utilitzar-se en un wireless router ASUS que funcioni. Les actualitzacions de firmware normals han d'executar-se a través de la interfície web. Consulteu el **Capítol 3: Configuració General i Configuració Avançada** per obtenir més informació.

4.3 Configuració del servidor d'impressió

4.3.1 ASUS EZ Printer Sharing

La utilitat ASUS EZ Printing Sharing us permet connectar una impressora USB al port USB del wireless router i configurar el servidor d'impressió. D'aquesta manera, els clients de la xarxa podran imprimir i escanejar fitxers remotament.



NOTA: La funció de servidor d'impressió és compatible amb els sistemes operatius Windows® 7, Windows® 8, Windows® 8.1, Windows® 10 i Windows® 11.

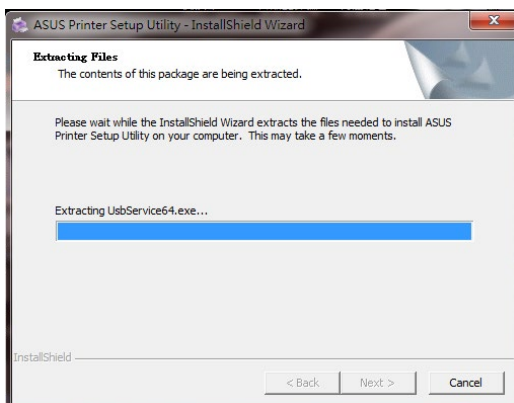
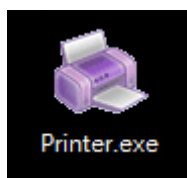
Per configurar el mode d'ús compartit de la impressora EZ:

1. Des del tauler de navegació, aneu a **General > Aplicació USB > Servidor d'impressió en xarxa**.
2. Premeu **Baixar ara** per baixar la utilitat d'impressora en xarxa.

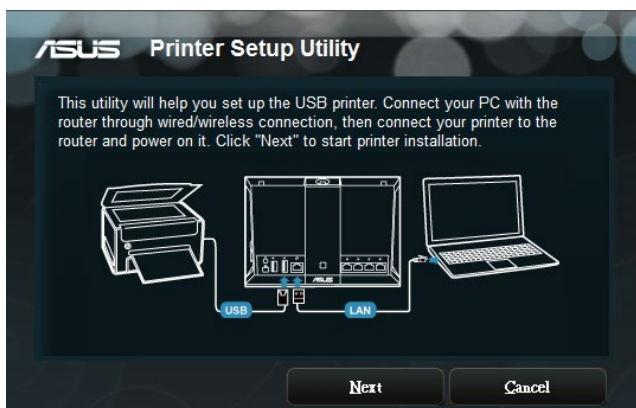


NOTA: La utilitat d'impressora en xarxa només és compatible amb els sistemes operatius Windows® 7, Windows® 8, Windows® 8.1, Windows® 10 i Windows® 11. Per instal·lar aquesta utilitat en un Mac OS, seleccioneu **Utilitza el protocol LPR per compartir la impressora**.

3. Descomprimiu el fitxer que heu baixat i premeu la icona de la impressora per executar el programa de configuració de la impressora en xarxa.



4. Seguiu les instruccions en pantalla per configurar el hardware i premeu **Següent**.

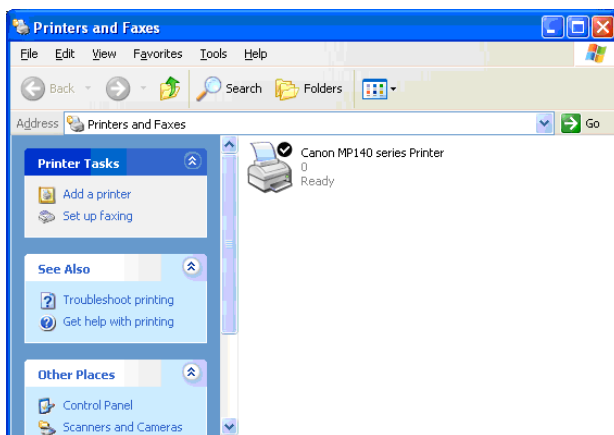


5. Espereu uns minuts que acabi la configuració inicial. Feu clic a **Següent**.
6. Feu clic a **Finalitzar** per completar la instal·lació.

7. Seguiu les instruccions del Windows® OS per instal·lar el controlador de la impressora.



8. Quan completeu la instal·lació del controlador de la impressora, la podran fer servir els clients de la xarxa.



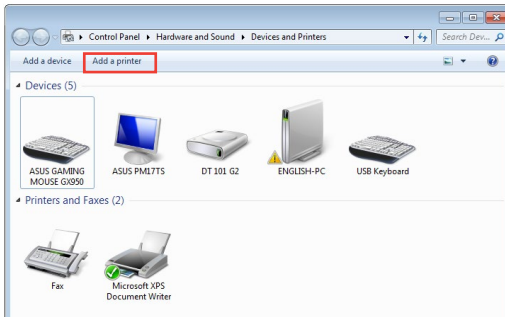
4.3.2 Ús de LPR per compartir impressora

Podeu compartir la impressora amb ordinadors amb el sistema operatiu Windows® i MAC utilitzant l'LPR/LPD (Line Printer Remote/Line Printer Daemon).

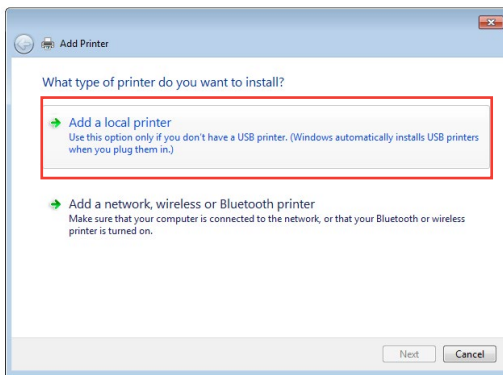
Ús compartit de la impressora LPR

Per compartir la impressora LPR:

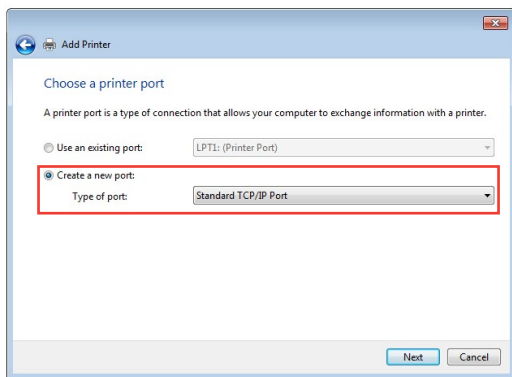
1. Des de l'escriptori del Windows®, premeu **Inicia > Dispositius i impressores > Afegeix una impressora** per executar l'**Auxiliar d'addició d'impressores**.



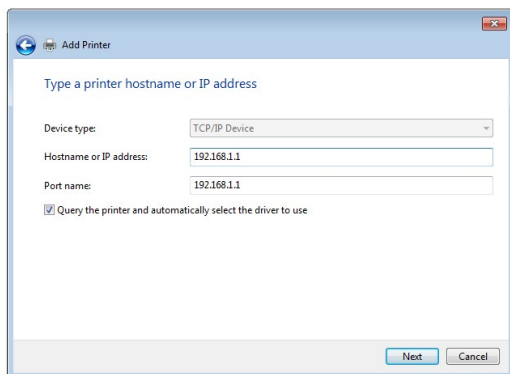
2. Seleccioneu **Afegeix una impressora local** i seguidament feu clic a **Següent**.



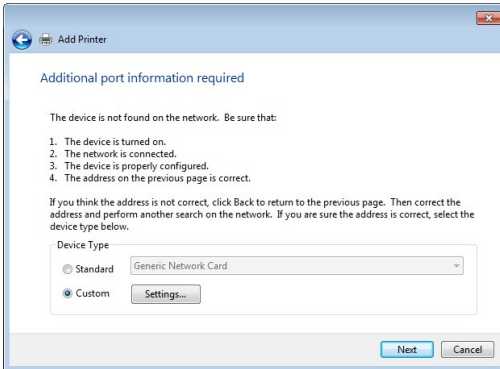
3. Seleccioneu **Crea un port nou** i establiu el **Tipus de port** en **Port TCP/IP estàndard**. Premeu **Següent**.



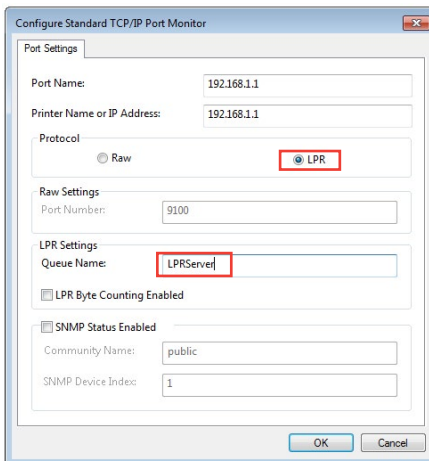
4. Al camp **Nom d'amfitrió o adreça IP**, introduïu l'adreça IP del wireless router i premeu **Següent**.



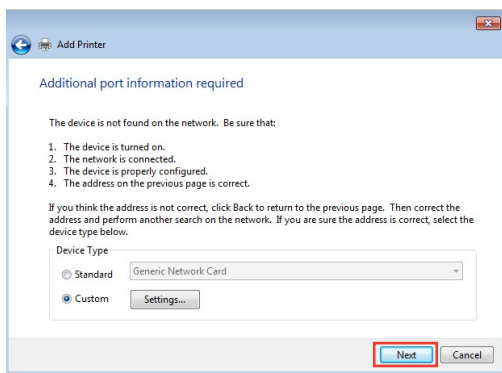
5. Seleccione **Personalitzat** i, seguidament, **Configuració**.



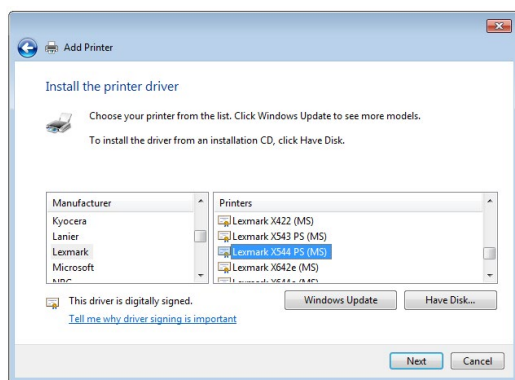
6. Establiu el **Protocol** en **LPR**. Al camp **Nom de la cua**, introduïu **ServidorLPR** i premeu **D'acord** per continuar.



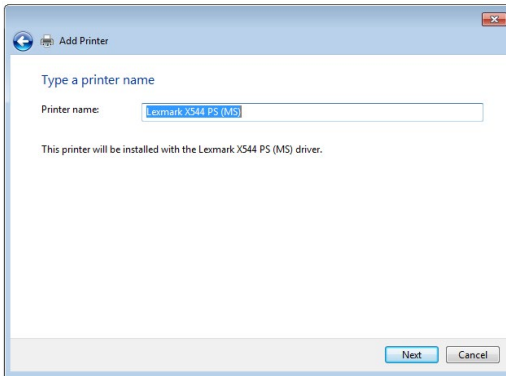
7. Premeu **Següent** per acabar de configurar el port TCP/IP estàndard.



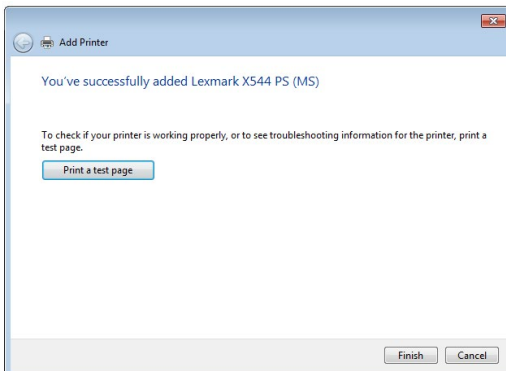
8. Instal·leu el controlador de la impressora des de la llista de models dels proveïdors. Si la vostra impressora no apareix a la llista, premeu **Tinc un disc** per instal·lar manualment els controladors de la impressora des d'un CD-ROM o un fitxer.



9. Premeu **Següent** per acceptar el nom predeterminat de la impressora.



10. Feu clic a **Finalitzar** per completar la instal·lació.



4.4 Download Master

Download Master és una utilitat que us ajuda a descarregar fitxers fins i tot quan el portàtil o altres dispositius està apagat.

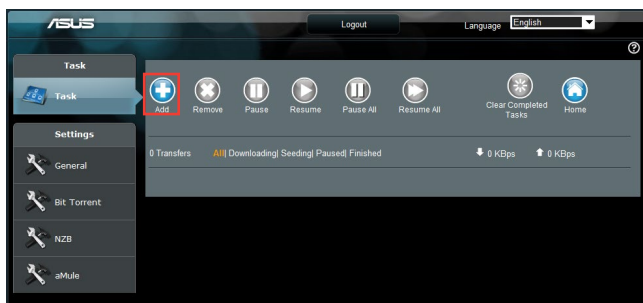
NOTA: Per utilitzar la utilitat Download Master, necessiteu tenir un dispositiu USB connectat al wireless router.

Per utilitzar Download Master:

1. Premeu **General > Aplicació USB > Download Master** per baixar i instal·lar la utilitat automàticament.

NOTA: Si teniu més d'una unitat USB, seleccioneu el dispositiu USB al qual voleu baixar els fitxers.

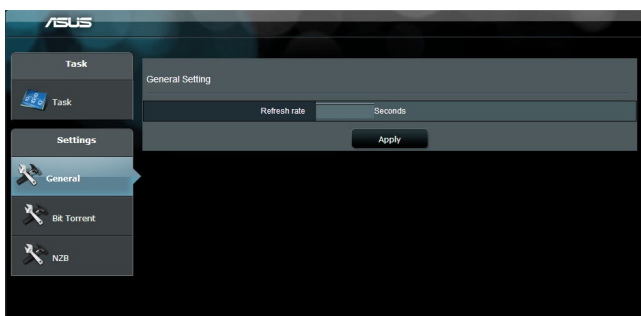
2. Després de finalitzar el procés de baixada, premeu la icona del Download Master per començar a utilitzar la utilitat.
3. Premeu **Afegir** per afegir una tasca de baixada.



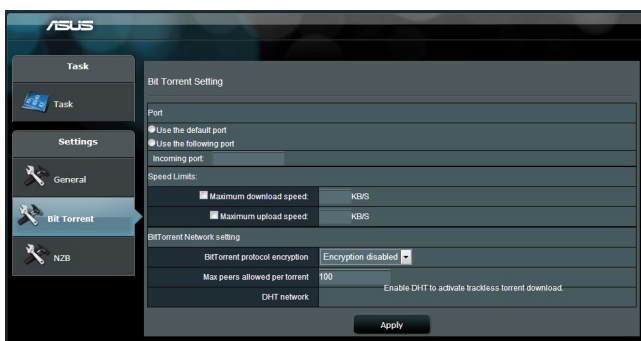
4. Seleccioneu un tipus de baixada, com ara BitTorrent, HTTP o FTP. Introduïu un fitxer de torrent o una URL per iniciar la baixada.

NOTA: Per a més informació sobre el Bit Torrent, consulteu l'apartat **4.4.1 Configuració dels paràmetres de baixada de Bit Torrent**.

- Utilitzeu el tauler de navegació per a la configuració avançada.



4.4.1 Configuració dels paràmetres de baixada de Bit Torrent

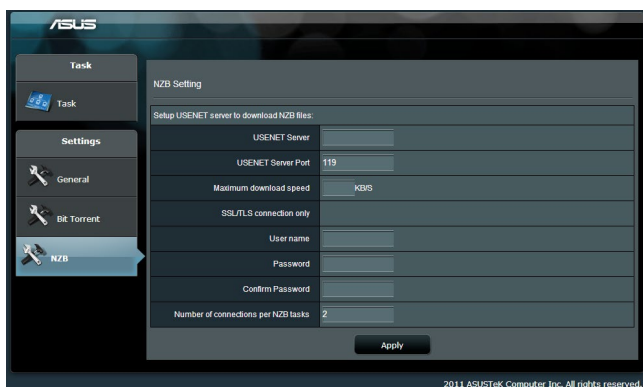


Per configurar els paràmetres de baixada de Bit Torrent

- Des del tauler de navegació de Download Master, premeu **Bit Torrent** per executar la pàgina **Configuració de Bit Torrent**.
- Seleccioneu un port específic per a la baixada.
- Per evitar la congestió de la xarxa, **Speed Limits (Límits de velocitat)** permet limitar les velocitats màximes de pujada i baixada.
- Podeu limitar el nombre màxim d'homòlegs admesos i habilitar o deshabilitar el xifratge de fitxers durant les baixades.

4.4.2 Configuració d'NZB

Podeu configurar un servidor USENET per baixar fitxers NZB. Introduïu els paràmetres de configuració d'USENET i premeu **Aplicar**.



5 Solució de problemes

Aquest capítol ofereix solucions per als possibles problemes que poden aparèixer amb el router. Si us trobeu amb algun problema que no apareix en aquest capítol, visiteu el lloc web de suport tècnic d'ASUS a: <https://www.asus.com/support/> per obtenir més informació sobre el producte i les dades de contacte del suport tècnic d'ASUS.

5.1 Solució de problemes bàsics

Si teniu cap problema amb el router, seguiu aquests passos bàsics abans de buscar altres solucions.

Actualització del firmware a la versió més recent.

1. Executeu la interfície gràfica (GUI) en línia. Aneu a **Configuració avançada > Administració > Actualització del firmware**. Premeu **Comprovar** per consultar el firmware més recent disponible.
2. Si hi ha firmware més recent, visiteu el lloc web internacional d'ASUS a https://rog.asus.com/networking/rog-rapture-RT-AX59U-model/helpdesk_download per baixar el firmware més recent.
3. Des de la pàgina **Actualització de firmware**, premeu **Cercar** per cercar el fitxer de firmware.
4. Premeu Pujar per actualitzar el firmware.

Reinicieu la vostra xarxa en aquest ordre:

1. Apagueu el mòdem.
2. Desendolleu el mòdem.
3. Apagueu el router i els ordinadors.
4. Endolleu el mòdem.
5. Enceneu el mòdem i espereu 2 minuts.
6. Enceneu el router i espereu 2 minuts.
7. Enceneu els ordinadors.

Comproveu si els cables d'Ethernet estan ben endollats.

- Si el cable d'Ethernet que connecta el router amb el mòdem està ben endollat, el llum de WAN està encès.
- Si el cable d'Ethernet que connecta l'ordinador que està encès amb el router està ben endollat, el llum de LAN corresponent està encès.

Comproveu si la configuració wireless del vostre ordinador coincideix amb la del router.

- Quan connecteu l'ordinador al wireless routers, comproveu que l'SSID (nom de la xarxa wireless), el mètode d'encryptació i la contrasenya són correctes.

Comproveu si la configuració de xarxa és correcta.

- Tots els clients de la xarxa han de tenir una adreça IP vàlida. ASUS recomana utilitzar el servidor de DHCP del wireless router per assignar adreces IP als ordinadors de la xarxa.
- Alguns proveïdors de servei de mòdem per cable exigeixen l'ús de l'adreça MAC de l'ordinador inicialment registrat en aquest compte. Podeu veure l'adreça MAC a la interfície gràfica (GUI) en línia, aneu a la pàgina **Mapa de la xarxa > Clients** i passeu el punter del ratolí per sobre del vostre dispositiu a **estat del Client**.

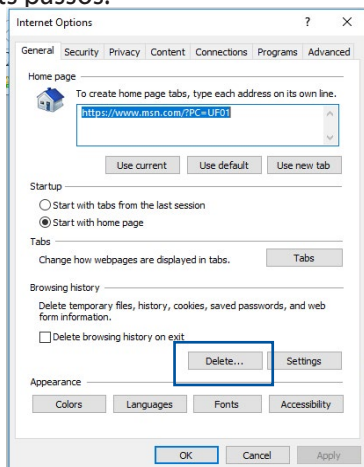


5.2 Preguntes freqüents (PF)

No puc accedir a la GUI del router amb un navegador web

- Si l'ordinador està connectat per cable, comproveu la connexió per cable Ethernet i si el llum està encès o apagat amb les instruccions de l'apartat anterior.
- Comproveu que feu servir la informació correcta per a l'inici de la sessió. El nom d'inici de sessió predeterminat de fàbrica i la contrasenya són "admin/admin". Comproveu que la tecla Bloq Maj està desactivada quan introduïu la informació d'inici de la sessió.
- Esborreu les cookies i els fitxers del navegador web. Per a l'Internet Explorer, seguiu aquests passos:

1. Obriu l'Internet Explorer i premeu **Eines > Opcions d'Internet**.
2. A la **General**, sota **Historial de navegació**, premeu **Suprimeix...**, seleccioneu **Fitxers temporals d'Internet i fitxers de llocs web i Cookies i dades de llocs web** i premeu **Suprimir**.



NOTES:

- Les ordres per suprimir les cookies i els fitxers varien en funció del navegador.
- Deshabiliteu la configuració del servidor intermediari, cancel·leu la connexió amb marcatge i configureu els paràmetres de TCP/IP per obtenir automàticament les adreces IP. Per obtenir més informació, consulteu el Capítol 1 d'aquest manual de l'usuari.
- Heu d'utilitzar cables Ethernet amb classificació CAT5e o CAT6.

El client no pot establir una connexió per xarxa wireless amb el router.

NOTA: Si teniu problemes per connectar-vos a la xarxa de 5 GHz, comproveu que el vostre dispositiu wireless és compatible amb la connexió de 5 GHz o que admet la banda dual.

- **Fora d'abast:**
 - Apropieu el router al client wireless.
 - Proveu d'ajustar la direcció de les antenes del router, segons les instruccions de l'apartat **1.4 Com col·locar el wireless router**.
- **El servidor de DHCP s'ha deshabilitat:**
 1. Executeu la interfície gràfica (GUI) en línia. Aneu a **General > Mapa de la xarxa > Clients** i cerqueu el dispositiu que voleu connectar al router.
 2. Si no trobeu el dispositiu al **Mapa de la xarxa**, aneu a **Configuració avançada > LAN > Servidor DHCP**, llista de **Configuració bàsica**, seleccioneu **Sí** a **Habilitar el servidor DHCP**.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and inform the client of the DNS server IP and default gateway IP. RT-AX59U supports up to 253 IP addresses for your local network.
[Manually Assigned IP around the DHCP list FAQ](#)

Basic Config

Enable the DHCP Server Yes No

RT-AX59U's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time (seconds)

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

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

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

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

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>
No data in table.				

- L'SSID s'ha ocultat. Si el dispositiu detecta els SSID d'altres routers però no detecta l'SSID del vostre router, aneu a **Configuració avançada > Wireless > General**, seleccioneu **No a Amaga SSID** i seleccioneu **Auto a Canal de control**.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
2.4 GHz	
Network Name (SSID)	ASUS_60_2G
Hide SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> big Protection <input checked="" type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ</small>
WiFi Agile Multiband	Enable
Target Wake Time	Disable
Channel bandwidth	20/40 Mhz
Control Channel	Auto <small>Current Control Channel: 6</small> <input type="checkbox"/> Auto select channel including channel 12, 13
Extension Channel	Auto

- Si utilitzeu un adaptador LAN wireless, comproveu si el canal wireless que utilitzeu és correcte per als canals disponibles a la vostra regió/país. Si no ho és, ajusteu el canal, l'ample de banda del canal i el mode wireless.
- Si encara no us podeu connectar al wireless router, restabliu la configuració predeterminada defecte de fàbrica del router. A la GUI del router, premeu **Administració > Restablir/desar/ pujar la configuració i Restablir**.

Administration - Firmware Upgrade

Note:

1. The latest firmware version includes updates from the previous version.
2. Configuration parameters will keep their settings during the firmware update process.
3. In case the upgrade process fails, RT-AX59U enters the emergency mode automatically. The LED signals at the front of RT-AX59U will indicate such a situation. Please visit [ASUS Download Center](#) to download ASUS Firmware Restoration utility for a manual update. Check on [FAQ](#) for more instructions.
4. Get the latest firmware version from the [ASUS Support site](#)

Auto Firmware Upgrade	
Auto Firmware Upgrade	<input type="checkbox"/> OFF
Firmware Version	
Signature version	2.366 Updated : 2023/08/15 17:05 <input type="button" value="Check"/>
Check Update	<input type="checkbox"/> I would like to retrieve beta firmware. <input type="button" value="Check"/>
AI Mesh router	
RT-AX59U	Current Version : 3.0.0.4.388_32431-g57f676 Manual firmware update : Upload

Note: A manual firmware update will only update selected AI Mesh routers / nodes, when using the AI Mesh system. Please make sure you are uploading the correct AI Mesh firmware version to each applicable router / node.

No hi ha accés a Internet.

- Comproveu si el router pot connectar-se a l'adreça IP de la WAN del vostre proveïdor de serveis d'Internet (ISP). Per fer-ho, obriu la interfície gràfica (GUI) en línia i aneu a **General > Mapa de la xarxa** i reviseu l'**Estat d'Internet**.
- Si el router no pot connectar-se a l'adreça IP de la WAN del proveïdor de serveis d'Internet (ISP), proveu de reiniciar la xarxa segons les instruccions de la secció **Reinicieu la xarxa en l'ordre següent** sota l'apartat **Solució de problemes bàsics**.



- El dispositiu s'ha bloquejat amb la funció de Control parental. Aneu a **General > Controls Parentals** i comproveu si el dispositiu és a la llista. Si el dispositiu apareix sota **Nom del client**, elimineu-lo amb el botó **Suprimir** o ajusteu la Configuració d'administració del temps.
- Si encara no hi ha accés a internet, proveu de reiniciar l'ordinador i comproveu l'adreça IP de la xarxa i l'adreça de la passarel·la.
- Comproveu els indicadors d'estat del mòdem ADSL i el wireless router. Si el llum de la WAN del wireless router no està encès, comproveu que tots els cables estan ben endollats.

Heu oblidat l'SSID (nom de la xarxa) o la contrasenya de la xarxa

- Configureu un SSID i una clau de xifratge noves mitjançant una connexió amb fil (cable d'Ethernet). Obriu la interfície gràfica (GUI) en línia, aneu a **Mapa de la xarxa**, premeu la icona del router, introduïu un SSID i una clau de xifratge nous i premeu **Aplicar**.
- Reinicieu el router als paràmetres predeterminats. Obriu la interfície gràfica (GUI) en línia, aneu a **Administració > Restablir/desar/pujar la configuració** i premeu **Restablir**. El compte i la contrasenya predeterminats d'inici de sessió són tots dos "admin".

Com restablir la configuració predeterminada de l'sistema?

Aneu a **Administració > Restablir/desar/pujar la configuració** i premeu **Restablir**.

Els següents són els paràmetres per defecte de fàbrica:

Nom d'usuari:	admin
Contrasenya:	admin
Activa DHCP :	Sí (si el cable WAN està endollat)
Adreça IP	http://www.asusrouter.com (o 192.168.50.1)
El nom del domini:	(Blank)
Màscara de subxarxa:	255.255.255.0
Servidor DNS 1:	192.168.50.1
Servidor DNS 2:	(Blank)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz):	ASUS_XX_5G

L'actualització del firmware ha fallat.

Obriu el mode de rescat i executeu la utilitat Firmware Restoration. Consulteu l'apartat **4.2 Firmware Restoration** per saber com funciona la utilitat Firmware Restoration.

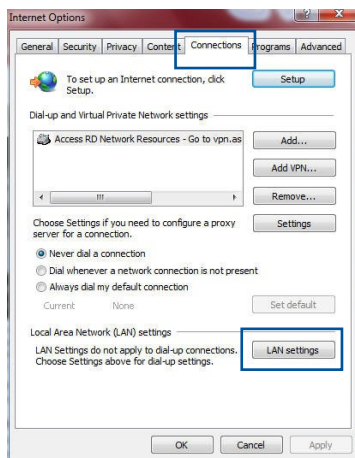
No es pot accedir a la interfície gràfica (GUI) en línia.

Abans de configurar el wireless router, seguïu els passos d'aquesta secció per a l'ordinador amfitrió i els clients de la xarxa.

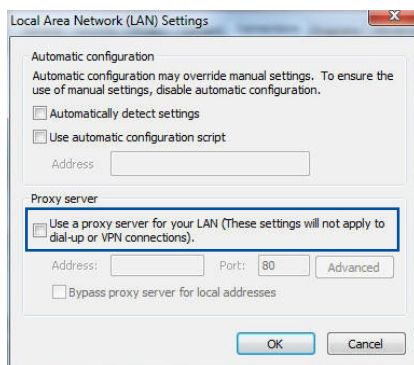
A. Deshabiliteu el servidor intermediari, si està habilitat.

Windows®

1. Premeu **Inicia** > **Internet Explorer** per executar el navegador.
2. Premeu **Eines** > **Opcions d'Internet** > **Connexions** > **Configuració de LAN**.

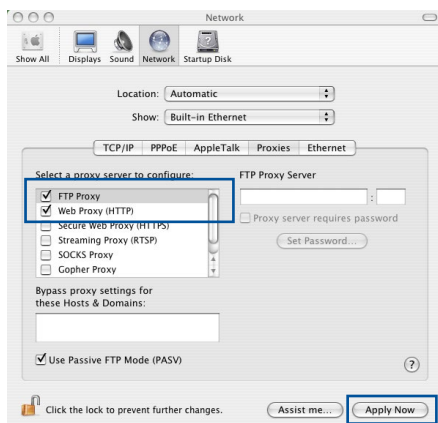


3. A la pantalla de configuració de la LAN, desmarqueu **Utilitza un servidor intermediari per a la LAN**.
4. Premeu **D'acord** quan acabeu.



MAC OS

1. Des del Safari, premeu **Safari > Preferències > Avançades > Canviar la configuració...**
2. A la pantalla de xarxa, desmarqueu **Servidor intermediari d'FTP i Servidor intermediari de web (HTTP)**.
3. Quan acabeu, premeu **Aplicar ara**.

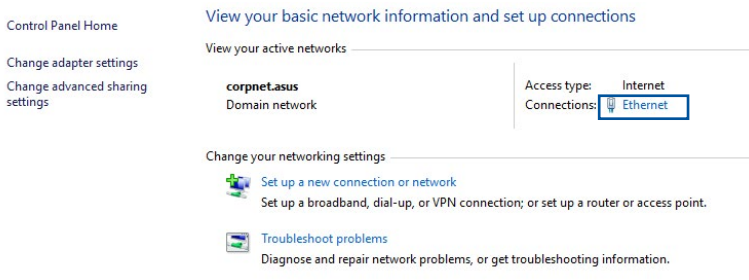


NOTA: Consulteu la funció d'ajuda del vostre navegador per saber com desactivar el servidor intermediari.

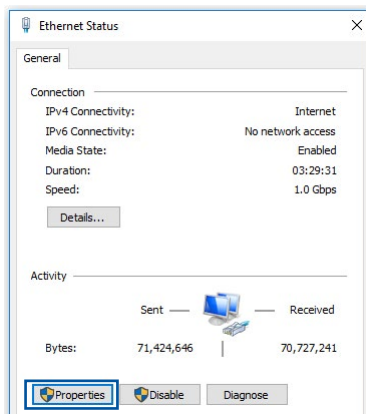
B. Configureu els paràmetres de TCP/IP per obtenir automàticament una adreça IP.

Windows®

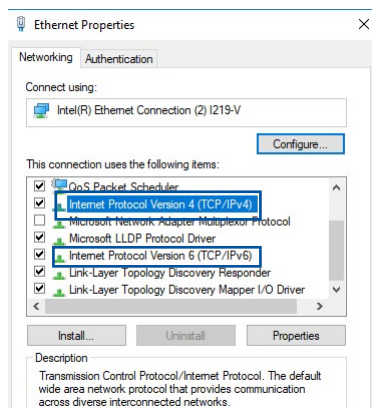
1. Premeu **Inicia > Tauler de control > Centre de xarxes i de recursos compartits**, premeu la connexió de xarxa per veure'n la finestra d'estat.



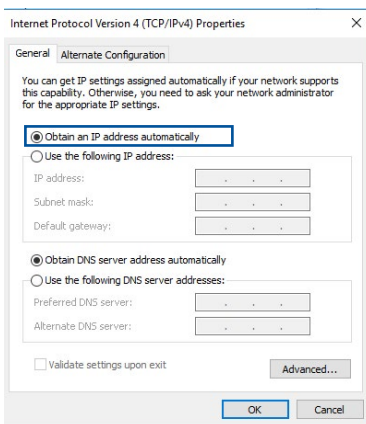
2. Premeu **Propietats** per veure la pantalla de Propietats d'Ethernet.




3. Seleccioneu **Versió 4 de protocol d'Internet (TCP/IPv4)** o **Versió 6 de protocol d'Internet (TCP/IPv6)** i premeu **Propietats**.

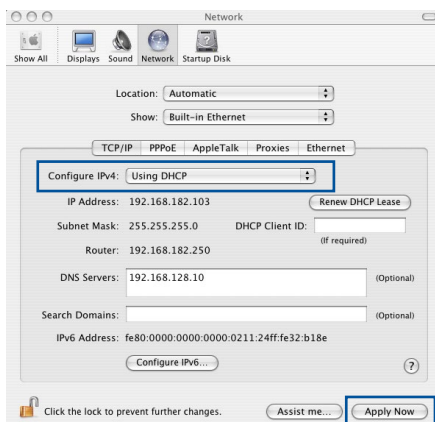


4. Per obtenir la configuració IP IPv4 automàticament, marqueu **Obtén l'adreça IP automàticament**.
Per obtenir la configuració IP IPv6 automàticament, marqueu **Obtén l'adreça IPv6 automàticament**.
5. Premeu **D'acord** quan acabeu.



MAC OS

1. Premeu la icona d'Apple  de la part superior esquerra de la pantalla.
2. Premeu **Preferències del sistema > Xarxa > Configurar...**
3. A la **TCP/IP**, seleccioneu **Amb DHCP** a la llista desplegable **Configurar IPv4**.
4. Quan acabeu, premeu **Aplicar ara**.

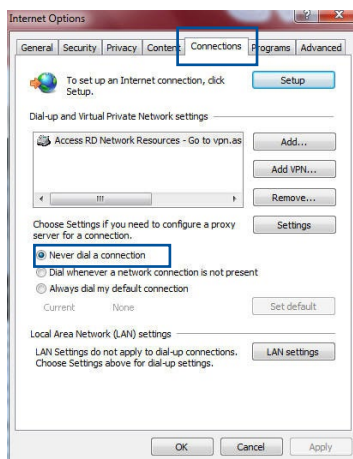


NOTA: Consulteu la funció d'ajuda i assistència tècnica del vostre sistema operatiu per obtenir informació sobre la configuració TCP/IP de l'equip.

C. Deshabiliteu la connexió de marcatge, si està habilitada.

Windows®

1. Premeu **Inicia > Internet Explorer** per executar el navegador.
2. Premeu **Eines > Opcions d'Internet > Connexions**.
3. Marqueu **No marquis mai una connexió**.
4. Premeu **D'acord** quan acabeu.



NOTA: Consulteu la funció d'ajuda del vostre navegador per saber com desactivar el marcatge directe.

Appendix

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Servei i assistència tècnica

Visiteu el nostre lloc web en diversos idiomes a
<https://www.asus.com/support>.

