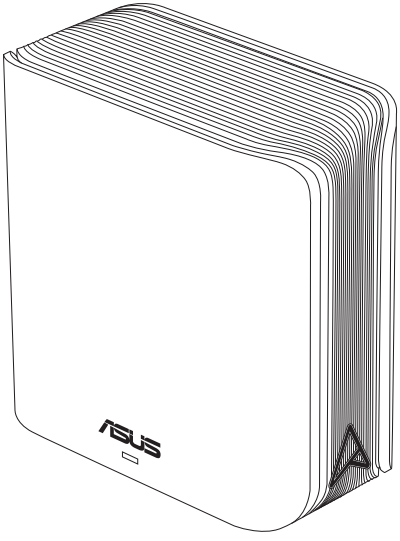
Guia de l'usuari

ZenWiFi BD4

Rúter de doble Bandes BE3600



IN SEARCH OF INCREDIBLE

CL23951

Primera edició

Agost de 2024

Índex

Índex

Índex

1 Informació sobre el wireless router

1.1 Benvingut/da!

Gràcies per comprar un wireless router ASUS ZenWiFi BD4.

El ZenWiFi BD4, amb un detall metàl·lic en color de la lletra A sobre una carcassa blanca minimalista, compta amb banda dual de 2,4 GHz i 5 GHz i ofereix un streaming simultani sense fil en HD 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.

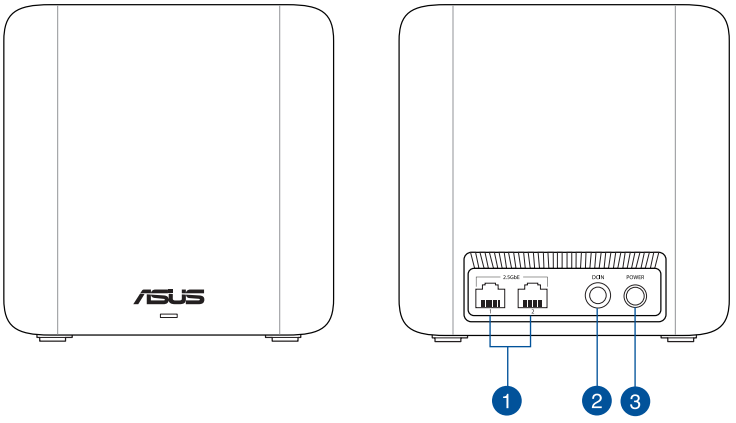
1.2 Contingut del paquet

- ☑ Wireless router ZenWiFi BD4
- ☑ Adaptador d'alimentació
- ☑ Targeta de garantia
- ☑ Cable de xarxa (RJ-45)
- ☑ 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 **Servei i assistència tècnica** que trobareu al darrere d'aquest manual.
- Conserveu el material d'embalatge original per si us cal cap reparació o substitució en garantia en el futur.

1.3 El wireless router



1	**Ports 2.5GbE (Detecció automàtica de WAN/LAN)** Connecteu els cables de xarxa en aquests ports per establir una connexió 2.5GbE WAN/LAN.
2	**Port Power (DCIN)** Inseriu l'adaptador de CA inclòs en aquest port i connecteu el router a la xarxa elèctrica.
3	**Botó d'alimentació** Premeu aquest botó per encendre o apagar el dispositiu.

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: +12V amb corrent de 1,5A		
Temperatura de funcionament	0-40ºC	Emmagatzematge	0-70ºC
Humitat de funcionament	50–90%	Emmagatzematge	20–90%

1.4 Ubicació del wireless router

Per garantir 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 wireless router allunyat d'obstacles metàl·lics i de la llum del sol directa.
- Manteniu el wireless router 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.

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 802.11a/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 802.11a/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).

ADVERTÈNCIA!

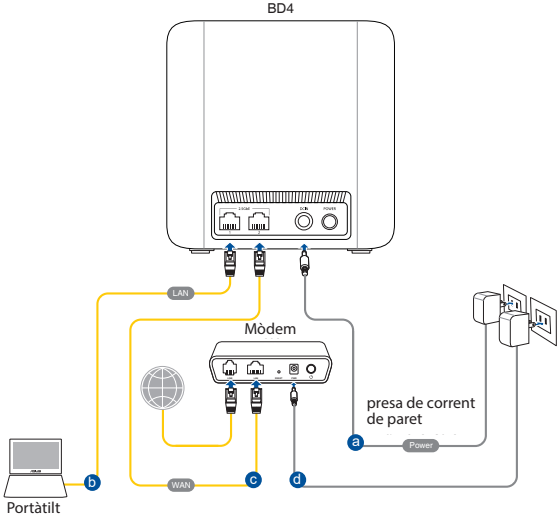
- Els cables d'alimentació han de tenir connexió a terra. Connecteu l'equip únicament a un endoll de paret de fàcil accés.
- Si l'adaptador s'espatlla, no proveu de reparar-lo. Poseu-vos en contacte amb un tècnic qualificat o amb el vostre distribuïdor.
- NO feu servir cables, accessoris o perifèrics fets malbé.
- NO instal·leu aquest equip a més de 2 metres d'alçada.
- Utilitzeu aquest producte en entorns amb temperatures ambientals entre els 0 i els 40º C.

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. Endolleu el router a una presa de corrent i enceneu-lo. Connecteu el cable de xarxa de l'ordinador a un port 2.5GbE del router.

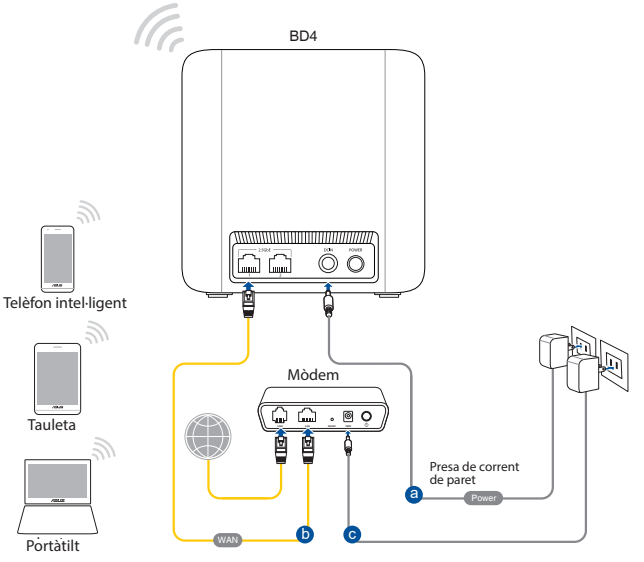


2. La interfície gràfica (GUI) en línia s'inicia automàticament en obrir un navegació web. Si no s'inicia automàticament, introduïu http://www.asusrouter.com.
3. Configureu una contrasenya per evitar accessos no autoritzats al router.

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 la Wi-Fi (SSID):	ASUS_XX

* **XX** es refereix als dos últims dígits de l'adreça MAC de 2,4 GHz. La trobareu a l'etiqueta del darrere del 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 **3.1.1 Configuració dels paràmetres de seguretat wireless** d'aquest manual d'usuari.

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 **Configuració manual** i configureu manualment els paràmetres de la connexió.

3. Assigneu el nom de la xarxa sense fil (SSID) i la clau de seguretat per a la vostra connexió sense fil de la xarxa WiFi 7. 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.

NOTA: El nom d'usuari i la contrasenya del wireless router és diferent del nom de la xarxa (SSID) de WiFi 7 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 WiFi 7 (SSID) i la clau de seguretat, els dispositius Wi-Fi poden iniciar la sessió i connectar-se a la xarxa de WiFi 7.

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 notificacions 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

El wireless router 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 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.

* Aquesta imatge es mostra únicament com a referència.

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

3.1.1 Configuració dels paràmetres de seguretat wireless

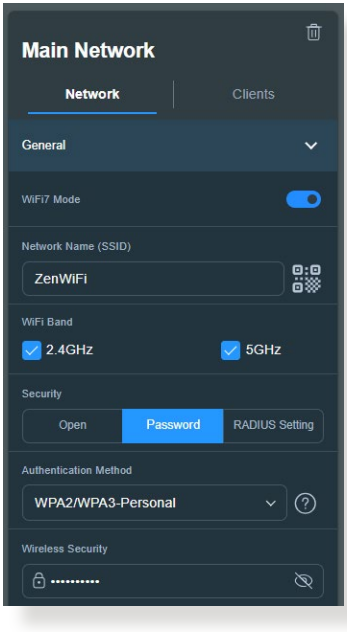
Per protegir la xarxa wireless contra accessos no autoritzats, haureu de configurar els paràmetres de seguretat.

Per configurar els paràmetres de seguretat wireless:

1. Des del tauler de navegació, aneu a **General** > **Mapa de la xarxa**.
2. Seleccioneu la xarxa i 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 / 5 GHz



3. Al camp **Nom de la xarxa (SSID)**, introduïu un nom únic per a la xarxa wireless.

4. A la llista desplegable **Xifratge WEP**, seleccioneu el mètode de xifratge de la xarxa wireless.

IMPORTANT! L'estàndard IEEE 802.11n/ac/ax prohibeix l'ús d'altes 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. Introduïu la clau de pas de seguretat.
6. Quan acabeu, premeu **Aplicar**.

3.1.2 Gestió dels clients de la xarxa

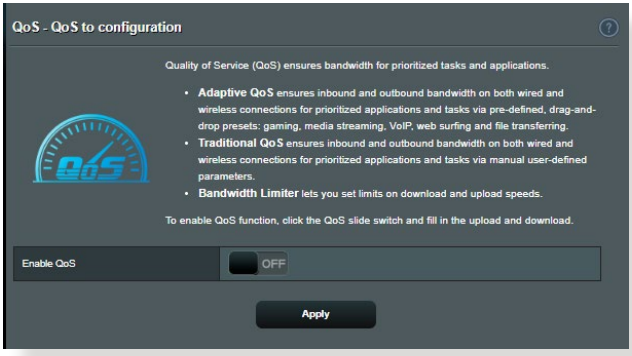
Per gestionar els clients de la xarxa:

1. Des del tauler de navegació, aneu a **General** > **Mapa de la xarxa**.
2. A la pantalla Mapa de la xarxa, seleccioneu la icona **estat del client** per mostrar la informació del client de la xarxa.
3. Per blocar l'accés d'un client a la vostra xarxa, seleccioneu el client i premeu **blocar**.

3.2 QoS adaptativa

3.2.1 Gestió de l'ample de banda de la qualitat de servei (QoS)

La qualitat de servei (QoS) us permet establir la prioritat de l'ample de banda i gestionar el tràfic de la xarxa.



Per establir la prioritat de l'ample de banda:

1. Des del tauler de navegació, aneu a **General** > **QoS adaptativa** > **QoS**.
2. Premeu **Activar** per activar la QoS. Ompliu els camps d'ample de banda de pujada i de baixada.

   NOTA: Demaneu la informació de l'ample de banda al vostre proveïdor de serveis d'Internet (ISP).

3. Premeu **Aplicar**.

   NOTA: La llista de normes d'especificació d'usuari permet la configuració avançada. Si voleu prioritzar serveis de la xarxa i aplicacions específiques de la xarxa, seleccioneu **Normes QoS definides per l'usuari** o **Prioritat definida per l'usuari** de la llista desplegable que trobareu a la cantonada superior dreta.

4. A la pàgina **Normes de QoS definides per l'usuari**, hi ha quatre tipus de servei en línia per defecte: navegació per Internet, HTTPS transferències de fitxers. Seleccioneu el servei preferent, ompliu els camps **IP o MAC d'origen**, **Port de destinació**, **Protocol**, **Transferit** i **Prioritat**; seguidament, premeu **Aplicar**. La informació es configurarà a la pantalla de normes de QoS.

NOTES:

- Per omplir l'adreça IP o MAC d'origen, podeu:
  a) Introduir una adreça IP específica, com ara "192.168.122.1".
  b) Introduir adreces IP en una subxarxa o al mateix grup IP, com ara "192.168.123.*" o "192.168.*.*"
  c) Introduir totes les adreces IP com a "*.*.*.*" o deixar el camp en blanc.
  d) El format de l'adreça MAC és sis grups de dos dígits hexadecimals, separats per dos punts (:), en ordre de transmissió (p. ex. 12:34:56:aa:bc:ef)
- Per al port d'orígen o de destinació, podeu:
  a) Introduir un port específic, com ara "95".
  b) Introduir ports en un rang, com ara "103:315", ">100" o "<65535".
- La columna **Transferit** conté informació sobre el tràfic de pujada i de baixada (tràfic de la xarxa de sortida i d'entrada) per a una secció. En aquesta columna podeu establir el límit del tràfic de la xarxa per a un servei específic amb l'objectiu de generar prioritats específiques per al servei assignat a un port específic. Per exemple, si dos clients de la xarxa (PC 1 i PC 2) accedeixen a Internet (establerta al port 80), però el PC 1 supera el límit del tràfic de la xarxa perquè està descarregant dades, el PC 1 tindrà una prioritat més baixa. Si no voleu establir cap límit, deixeu-lo en blanc.

5. A la pàgina **Prioritat definida per l'usuari**, podeu prioritzar els dispositius o les aplicacions de la xarxa en cinc nivells des de la llista desplegable de **Normes de QoS definides per l'usuari**.

   El funció del nivell de prioritat, podeu utilitzar els mètodes següents per enviar paquets de dades:

   - Canvieu l'ordre els paquets de la xarxa de pujada que s'envien a Internet.
   - A la taula **Ample de banda de pujada**, estabiu l'**Ample de banda reservat mínim** i l'**Ample de banda reservat màxim** per a múltiples aplicacions de la xarxa amb nivells de prioritat diferents. El percentatge indica les velocitats d'ample de banda de pujada disponibles per a les aplicacions de xarxa especificades.

NOTES:

- Els paquets amb baixa prioritat s'ometen per garantir la transmissió dels paquets d'alta prioritat.
- A la taula **Ample de banda de baixada**, estabiu el **Límit d'ample de banda màxim** per a múltiples aplicacions de xarxa en l'ordre corresponent. El paquet de pujada amb la prioritat més alta causarà el paquet de baixa amb la prioritat més alta.
- Si no s'envien paquets des d'aplicacions d'alta prioritat, no es reduirà la velocitat de transmissió per Internet per als paquets de baixa prioritat.

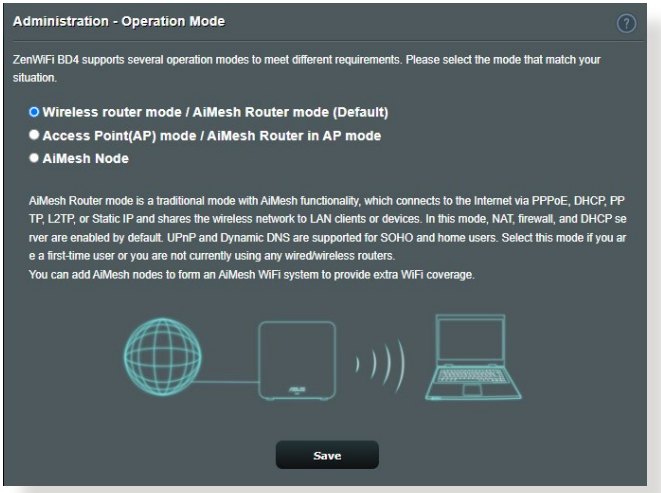
6. Estabiu el paquet amb la prioritat més alta. Per garantir una bona experiència en el joc en línia, podeu establir ACK, SYN i ICMP com al paquet amb la prioritat més alta.

NOTA: Assegureu-vos d'activar la QoS en primer lloc i de configurar els límits de velocitat de pujada i de baixada.

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 (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**: En aquest mode, el router crea una nova xarxa wireless en una xarxa existent.
   - **Node AiMesh**: Podeu configurar l'ZenWiFi BD4 com a node AiMesh per ampliar la cobertura WiFi d'un router AiMesh existent.
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'inici de sessió del router**: Podeu canviar la contrasenya i el nom d'inici de sessió del wireless router i introduir-ne de nous.
   - **Comportament de botó WPS**: El botó WPS físic del wireless router es pot utilitzar per activar la funció WPS.
   - **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.
   - **Permet només IP específiques**: Premeu **Sí** si voleu especificar les adreces IP dels serveis que poden accedir als paràmetres de la GUI del wireless router des de la WAN.
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 **Firmware Version (Versió de microprogramari)**, premeu **Comprovar** i trieu el fitxer que heu baixat.
3. Premeu **Pujar**.

NOTES:

- Quan el procés d'actualització finalitzi, espereu que el sistema es reinicïi.
- 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 la configuració**, aneu a la carpeta de destí del fitxer i premeu **Desar**.
   - Per restablir els paràmetres d'un fitxer de configuració del sistema, premeu **Pujar** per localitzar el fitxer i feu clic a **Obrir**.

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 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 podrà accedir a Internet un dispositiu connectat.

3.4.1 Protecció per contrasenya

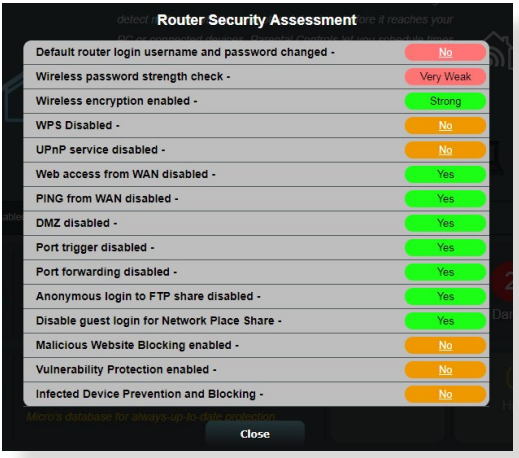
La protecció per contrasenya evita el mal ús de la xarxa i la protegeix d'accessos no autoritzats.

Configuració de la protecció de la xarxa

Per configurar la protecció 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**.

   Quan acaba d'escanejar, la utilitat en mostra els resultats a la pàgina **Avaluació de la seguretat del router**.



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**. Els elements que es marquen amb el text **No**, **Dèbil** o **Molt dèbil** haurien de configurar-se degudament.

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. Premeu un element.

NOTA: Quan premeu un element, la utilitat obre la pàgina de configuració corresponent.

   b. Des de la pàgina de paràmetres de seguretat de l'element en qüestió, apliqueu els paràmetres i els canvis necessaris i premeu **Aplicar** quan acabeu.

c. Torneu a la pàgina d'**Avaluació de la seguretat del router** i premeu **Tancar** per tancar-la.

5. Per configurar automàticament els paràmetres de seguretat, premeu **Protegir el router**.
6. Quan aparegui un missatge, premeu **D'acord**.

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 **Protecció de la xarxa**.
3. A la subfinestra de **Bloqueig de llocs maliciosos**, premeu **Activar**.

IPS bidireccional

El sistema de prevenció de les intrusions (IPS) bidireccional protegeix el router d'atacs de la xarxa bloquejant els paquets d'entrada maliciosos i detectant paquets de sortida sospitosos.

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 **Protecció de la xarxa**.
3. Des de la subfinestra d'**IPS bidireccional**, premeu **Activar**.

Prevenció 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 prevenció i bloqueig de dispositius infectats:

1. Des del tauler de navegació, aneu a **General** > **AiProtection**.
2. A la pàgina principal d'**AiProtection**, premeu **Protecció de la xarxa**.
3. Des de la subfinestra de **Prevenció i bloqueig de dispositius infectats**, premeu **Activar**.

Per configurar les preferències de les alertes:

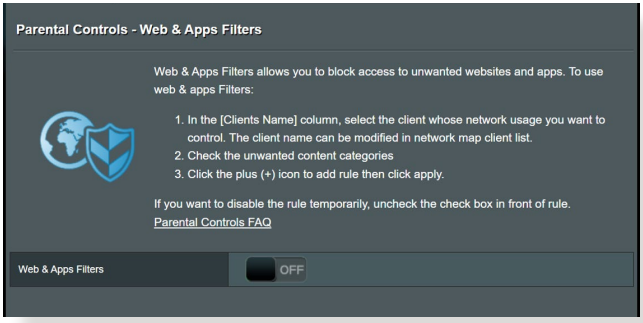
1. Des de la subfinestra de **Prevenció i bloqueig de dispositius infectats**, premeu **Preferències de les alertes**.
2. Seleccioneu o introduïu el proveïdor de correu, el compte de correu electrònic i la contrasenya i, seguidament, premeu **Aplicar**.

3.4.2 Configuració dels controls parentals

El control 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 anar a la pàgina principal dels controls parentals:

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



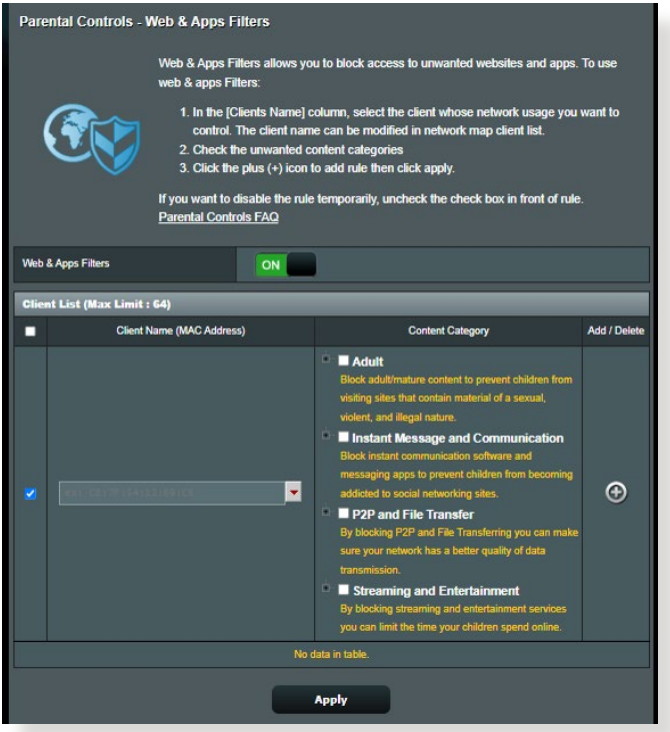
Filtres d'apps i webs

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**.
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**.

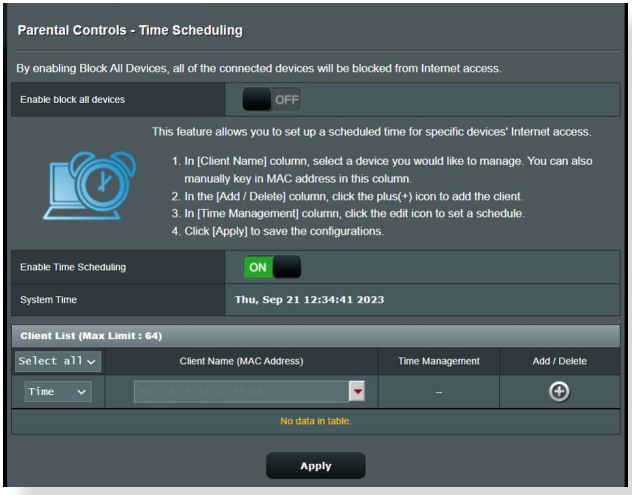
6. Premeu ⊕ per afegir el perfil del client.
7. Premeu **Aplicar** per desar els paràmetres.



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.



Per configurar la planificació temporal:

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

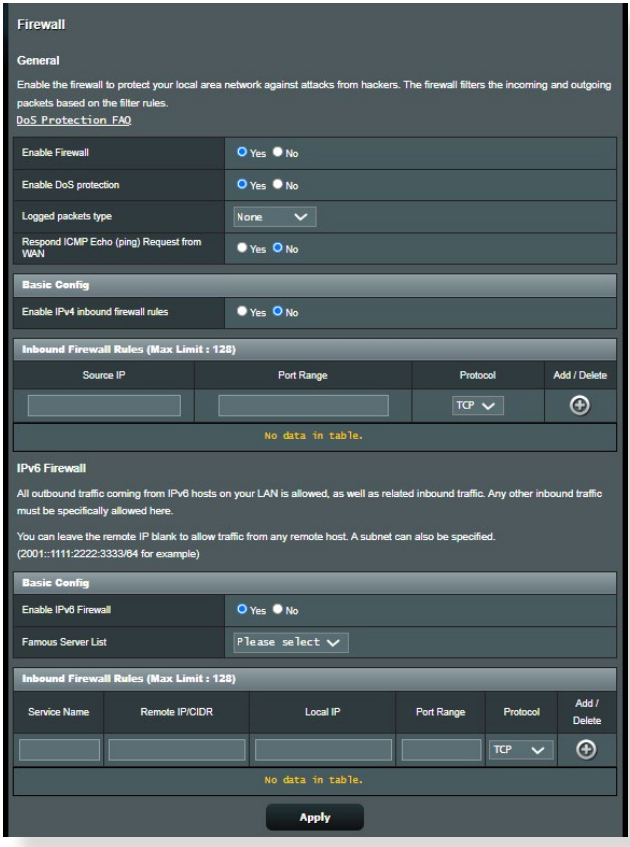
4. Premeu per afegir el perfil del client.
5. Premeu **Aplicar** per desar els paràmetres.

3.5 Firewall

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

NOTA: La funció de firewall està habilitada per defecte.

3.5.1 General



Per configurar els paràmetres bàsics del firewall:

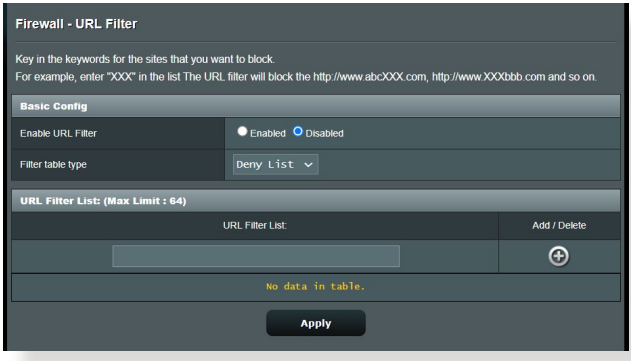
1. Des del tauler de navegació, aneu a **Configuració avançada** > **Firewall** > **General**.

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**.

3.5.2 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.

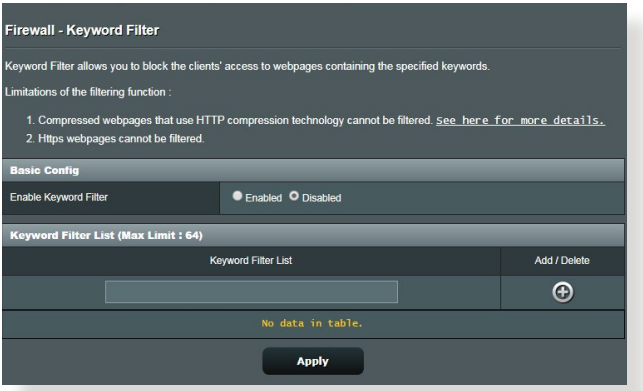


Per configurar un filtre d'URL:

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**.

3.5.3 Filtre de paraules clau

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



Per configurar un filtre de paraules clau:

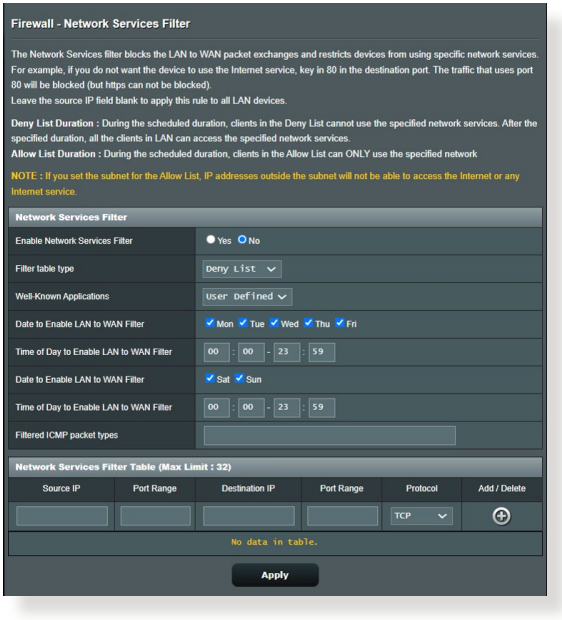
1. Des del tauler de navegació, aneu a **Configuració avançada** > **Firewall** > **Filtre de paraules clau**.
2. Al camp Habilitar filtre de paraules clau, seleccioneu **Habilitat**.
3. Introduïu una paraula o frase i premeu el botó **Afegir**.
4. Premeu **Aplicar**.

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.

3.5.4 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.



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 **Sí**.
3. Seleccioneu el tipus de taula de filtres. **Rebutjar** bloqueja els serveis de la xarxa especificats. **Permetre** 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**.

3.6 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. Introduïu els paràmetres de DNS i LAN d'IPv6.
4. Premeu **Aplicar**.

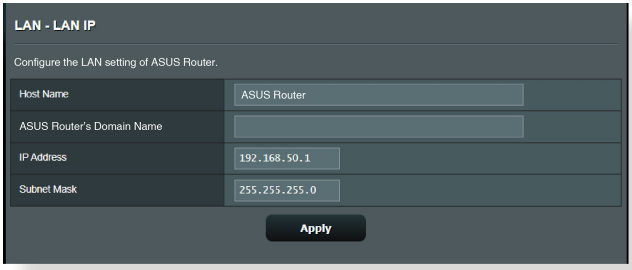
NOTA: Demaneu al vostre proveïdor de serveis d'Internet (ISP) informació específica d'IPv6 per al vostre servei d'Internet.

3.7 LAN

3.7.1 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.

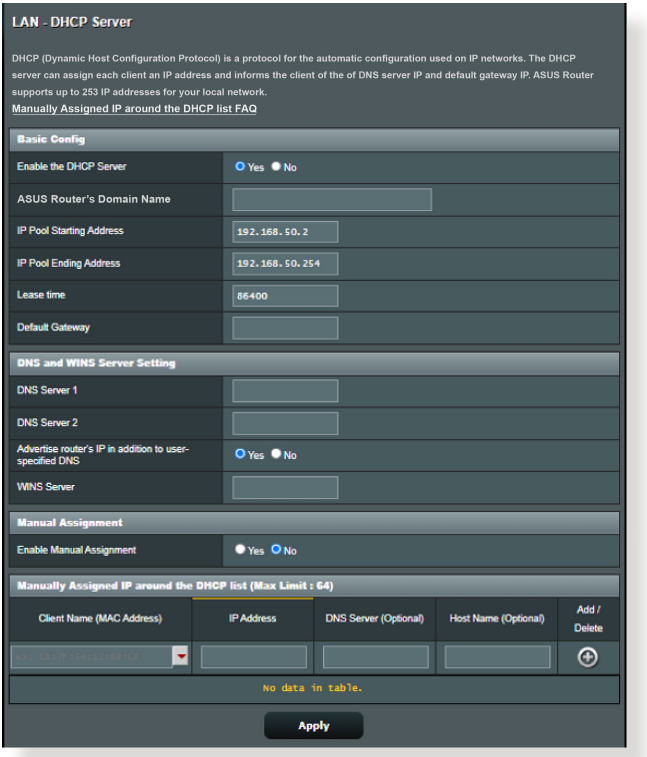


Per modificar la configuració de la IP de la xarxa LAN:

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**.

3.7.2 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.



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 **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**, especifiqueu en segons quan caduca una adreça IP assignada. Quan s'esgota el límit temporal, el servidor DHCP assigna una nova adreça IP.

NOTES:

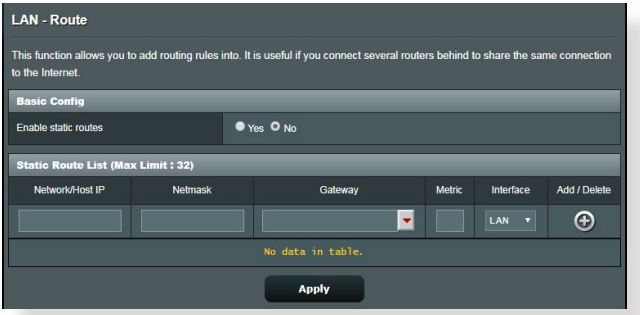
- Us recomanem que, quan especifiqueu un interval d'adreces IP, utilitzeu el format d'adreça IP 192.168.50.xxx (en què xxx pot ser qualsevol número entre 2 i 254).
- L'adreça inicial del pool d'IP no pot ser més gran que la final.

7. A la secció **Configuració de DNS i de WINS 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.

3.7.3 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.

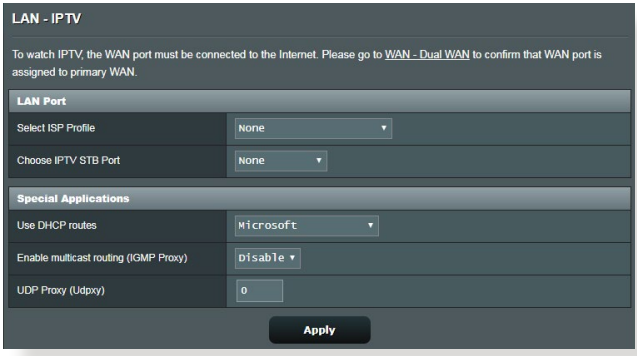


Per configurar la taula d'encaminament LAN:

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**.

3.7.4 IPTV

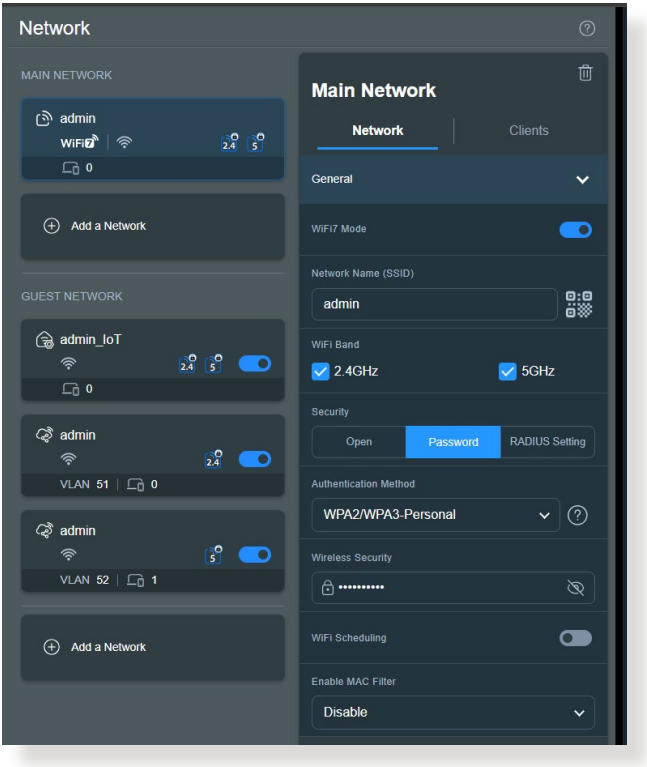
El wireless router admet la connexió als serveis IPTV mitjançant un proveïdor de serveis d'Internet (ISP) o una xarxa LAN. La IPTV ofereix els paràmetres de configuració necessaris per configurar IPTV, VoIP, multidifusió i UDP per al vostre servei. Poseu-vos en contacte amb el vostre proveïdor de serveis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



3.8 Xarxa

3.8.1 Xarxa principal - Filtre 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.



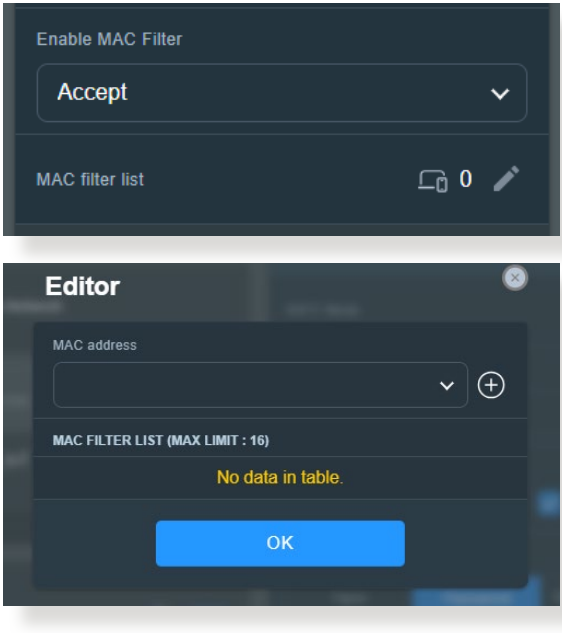
Per configurar el filtre wireless MAC:

1. Des del tauler de navegació, ves a **General (General)** > **Network (Xarxa)** > **Main Network (Xarxa principal)** i selecciona el nom (SSID) de la xarxa principal.
2. A la llista desplegable **Activar 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.

NOTA: Selecciona **Desactivar** si vols desactivar **Activar filtre MAC**.

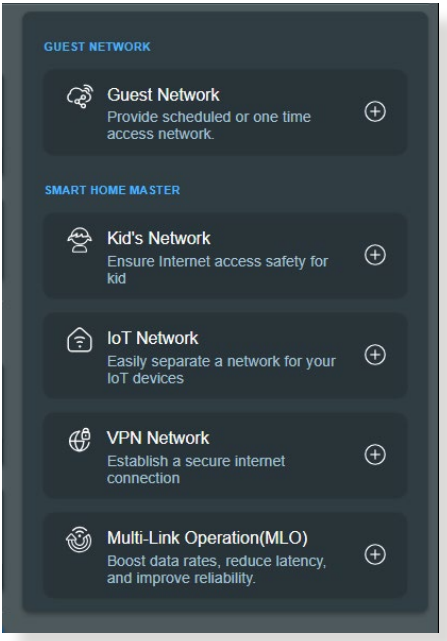
3. A la llista de filtres MAC, Fes clic a per accedir a la pàgina Editor i, seguidament, fes clic a i introdueix l'adreça MAC del dispositiu sense fil.
4. Premeu **D'acord**.



3.8.2 Xarxa per a convidats

3.8.2.1 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.

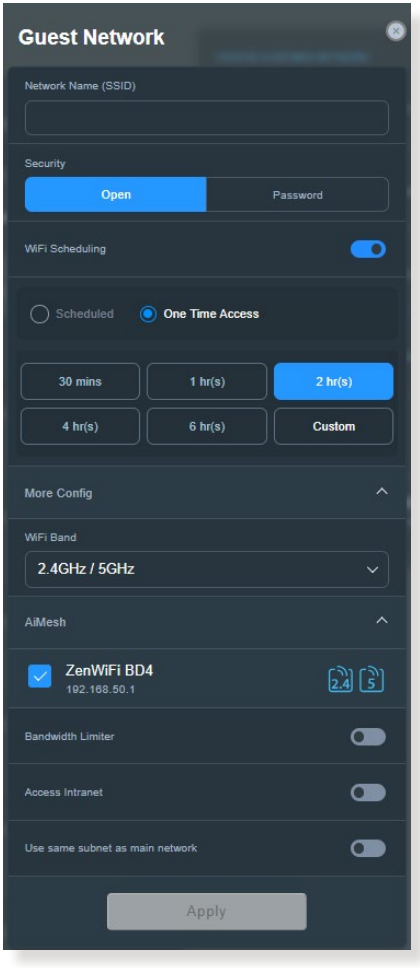


NOTA: ZenWiFi BD4 admet fins a tres SSID a la Xarxa de Convidats.

Per crear una xarxa de convidats:

1. Des del tauler de navegació, aneu a **General** > **Xarxa** > **Xarxa de convidats** > **Afegeix una xarxa**.
2. Seleccioneu **Xarxa de Convidats** i assigneu un nom a la vostra xarxa temporal al camp **Nom de la Xarxa (SSID)**.
3. Seleccioneu un mètode d'autenticació a **Seguretat**.
4. Especifiqueu el temps d'accés o trieu **Programat** per afegir un perfil de programació en línia.

5. Seleccioneu la **Banda WiFi** per a la xarxa de convidats que voleu crear.
6. Activeu o desactiveu el **Limitador d'Ample de Banda**.
7. Activeu o desactiveu **l'Accés a l'Intranet**.
8. Quan acabeu, premeu **Aplicar**.

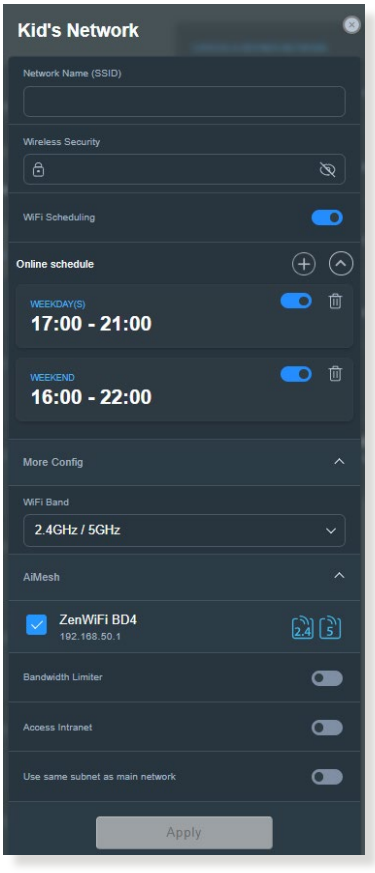


3.8.2.2 Smart Home Master

L'Smart Home Master és una eina potent i fàcil de fer servir per a la segmentació de xarxes. Simplifica el procés de creació i administració d'entorns de subxarxes avançats; per exemple, per crear un SSID dedicat per als dispositius dels teus fills, connectar-te a una VPN a través d'una subxarxa dedicada o fins i tot crear un SSID segur per a tots els teus dispositius IoT.

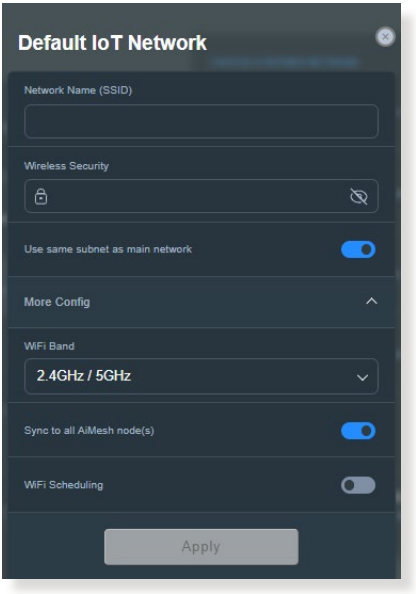
Per crear una Xarxa per a Nens:

1. Des del tauler de navegació, aneu a **General** > **Xarxa** > **Xarxa de convidats** > **Afegeix una xarxa**.
2. Seleccioneu **Xarxa per a Nens** i assigneu un nom de xarxa i una clau de seguretat als camps **Nom de la Xarxa (SSID)** i **Seguretat Sense Fil**.
3. Personalitzeu el temps d'accés a Internet al camp de **Programació en Línia**.
4. Seleccioneu la **Banda WiFi** per a la xarxa per a nens que voleu crear.
5. Activeu o desactiveu el **Limitador d'Ample de Banda**.
6. Activeu o desactiveu **l'Accés a l'Intranet**.
7. Quan acabeu, premeu **Aplicar**.



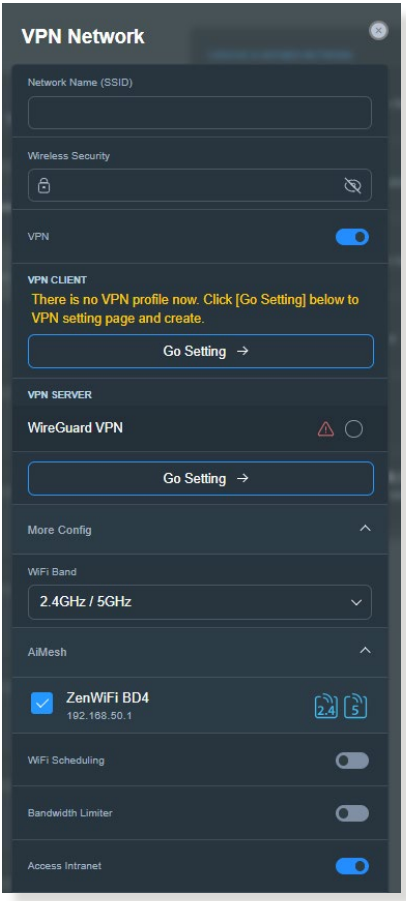
Per crear una Xarxa per a IoT:

1. Des del tauler de navegació, aneu a **General** > **Xarxa** > **Xarxa de convidats** > **Afegeix una xarxa**.
2. Seleccioneu **Xarxa per a IoT** i assigneu un nom de xarxa i una clau de seguretat als camps **Nom de la Xarxa (SSID)** i **Seguretat Sense Fil**.
3. Seleccioneu la **Banda WiFi** per a la xarxa per a IoT que voleu crear.
4. Personalitza el temps d'accés a Internet activant la **Programació WiFi**.
5. Quan acabeu, premeu **Aplicar**.



Per crear una xarxa VPN:

1. Des del tauler de navegació, aneu a **General** > **Xarxa** > **Xarxa de convidats** > **Afegeix una xarxa**.
2. Seleccioneu **Xarxa VPN** i assigneu un nom de xarxa i una clau de seguretat als camps **Nom de la Xarxa (SSID)** i **Seguretat Sense Fil**.
3. Si no heu configurat un perfil de VPN per al servidor VPN o el client VPN, feu clic a **Anar a la configuració** per crear un perfil de VPN.
4. Seleccioneu la **Banda WiFi** per a la xarxa VPN que voleu crear.
5. Personalitza el temps d'accés a Internet activant la **Programació WiFi**.
6. Activeu o desactiveu el **Limitador d'Ample de Banda**.
7. Activeu o desactiveu **l'Accés a l'Intranet**.
8. Quan acabeu, premeu **Aplicar**.


VPN Network
Network Name (SSID)
Wireless Security
VPN
VPN CLIENT
There is no VPN profile now. Click [Go Setting] below to VPN setting page and create.
Go Setting →
VPN SERVER
WireGuard VPN
Go Setting →
More Config
WiFi Band
2.4GHz / 5GHz
AiMesh
ZenWiFi BD4
192.168.50.1
WiFi Scheduling
Bandwidth Limiter
Access Intranet

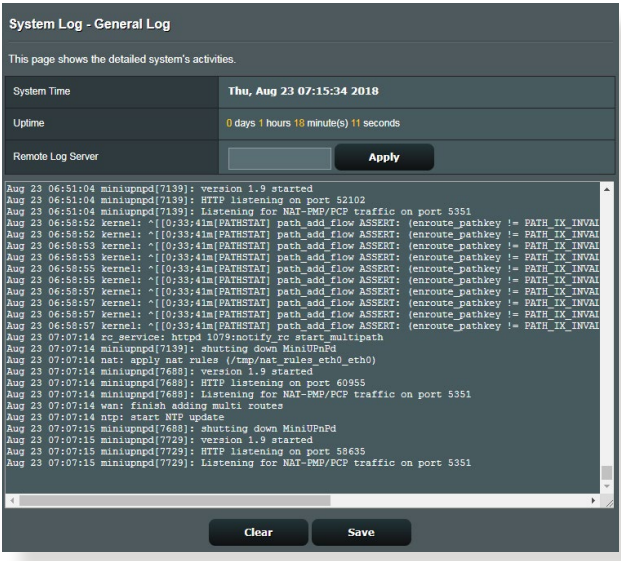
3.9 Registre del sistema

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



3.10 Analitzador de trànsit

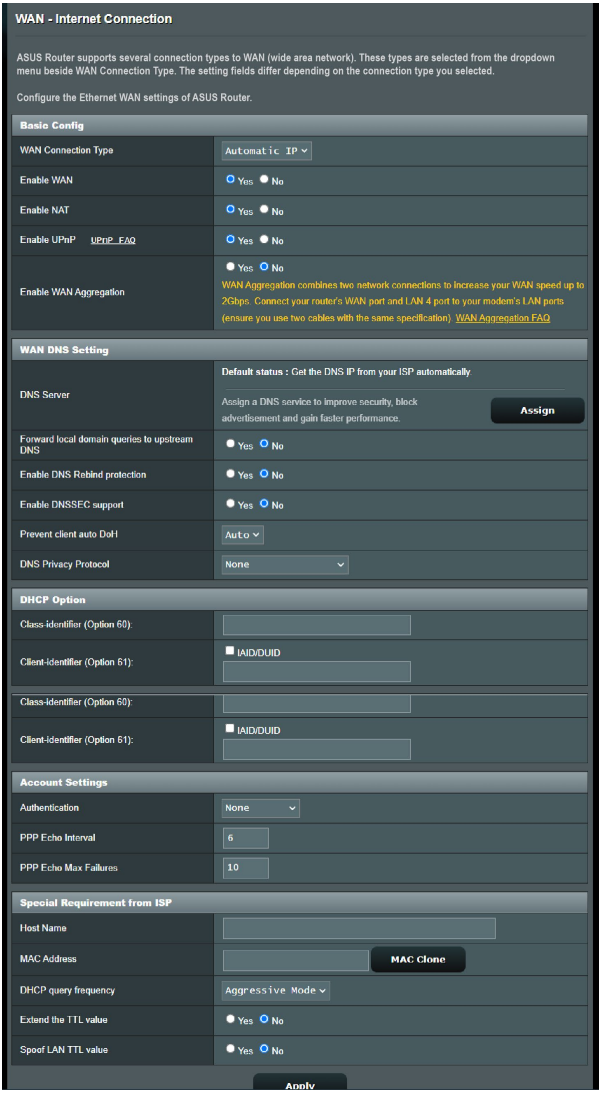
La funció de supervisió del trànsit permet accedir a les dades d'ús i de velocitat de l'ample de banda d'Internet i de les xarxes amb fil i wirelesss. Permet supervisar el trànsit de la xarxa en temps real o a diari. També ofereix l'opció de mostrar el trànsit de la xarxa de les 24 hores anteriors.

NOTA: Els paquets d'Internet es transmeten de manera uniforme als dispositius amb fil i wirelesss.

3.11 WAN

3.11.1 Connexió a Internet

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



Per configurar els paràmetres de la connexió WLAN:

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.
   - **Habilitar agrupació WAN**: L'agrupació WAN combina dues connexions de xarxa per augmentar la velocitat de la WAN fins a 2 Gbps. Connecteu el port WAN del router i el port LAN

4 als ports LAN del mòdem.

- **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.

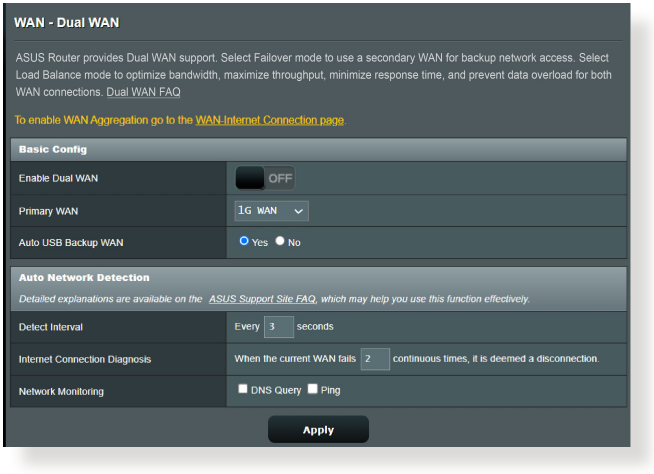
3.11.2 WAN dual

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

Per configurar la WAN dual:

1. Des del tauler de navegació, aneu a **Configuració avançada** > **WAN**.
2. Aneu al camp **WAN dual** i trieu **Activar**.
3. Seleccioneu **WAN primària** i **WAN secundària**. Hi ha dues opcions WAN/LAN de 2.5GbE per a tu
4. Seleccioneu **Commutació** o **Equilibri de càrregues**.
5. Premeu **Aplicar**.

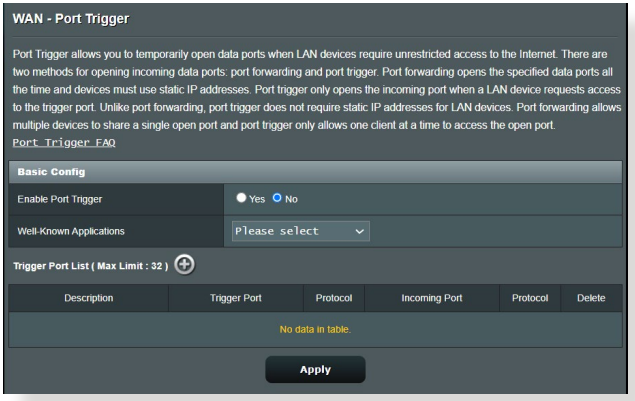
NOTA: Trobareu informació detallada a les PMF del lloc de suport d'ASUS **https://www.asus.com/support/FAQ/1011719**



3.11.3 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.



Per configurar l'activació de ports:

1. Des del tauler de navegació, aneu a **Configuració avançada** > **WAN** > **activació de ports**.
2. Configureu els següents paràmetres. Quan acabeu, premeu **Aplicar**.
   - **Habilitar activació de ports**: Seleccioneu **Sí** per habilitar l'activació de ports.
   - **Aplicacions conegudes**: Seleccioneu jocs i serveis web populars per afegir-los a la llista d'activació de ports.
   - **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.

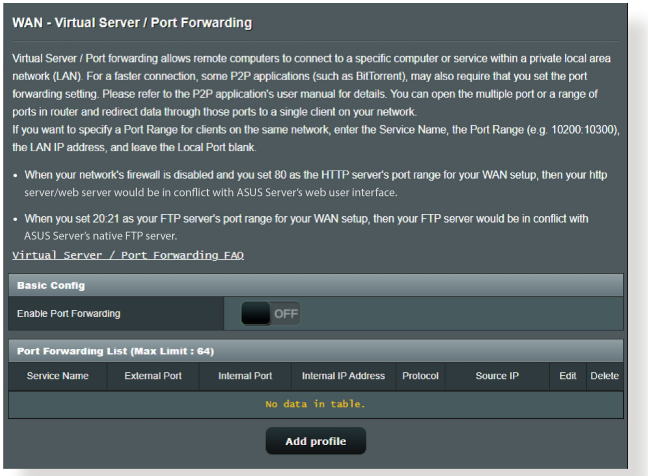
NOTES:

- 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.

3.11.4 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.

NOTA: Si s'habilita el reenviament de port, el router ASUS bloqueja el trànsit d'entrada no sol·licitat procedent d'Internet i només permet respostes procedents de peticions de sortida de la LAN. El client de la xarxa no té accés directe a Internet i viceversa.



Per configurar el reenviament de port:

1. Des del tauler de navegació, aneu a **Configuració avançada** > **WAN** > **Servidor virtual / reenviament de port**.
2. Configureu els següents paràmetres. Quan acabeu, premeu **Activar**.
   - **Habilita el redireccionament de port**: Trieu **Activar** per habilitar el reenviament de port.
   - **Llista de servidors populars**: Determineu el tipus de servei al qual voleu accedir.

- **Llista de jocs populars**: Inclou els ports que necessiten els jocs en línia populars per funcionar correctament.
- **Port de servidor FTP**: No assigneu l'interval de ports 20:21 al servidor d'FTP perquè entraria en conflicte amb l'assignació del servidor d'FTP nadiu del router.
- **Nom del servei**: Introduïu el nom del servei.
- **Interval de ports**: Si voleu especificar un interval de ports per als clients de la mateixa xarxa, introduïu el Nom del servei, l'Interval de ports (p. ex. 10200:10300), l'Adreça IP de la LAN i deixeu el Port local buit. L'interval de ports accepta diferents formats, com ara un interval de ports (300:350), ports individuals (566,789) o una combinació (1015:1024,3021).

NOTES:

- Si el firewall està deshabilitat i establiu 80 com a interval de ports del vostre servidor d'HTTP per a la configuració de la WAN, el servidor http/servidor web entrarà en conflicte amb la interfície de l'usuari web del router.
- Una xarxa utilitza els ports per intercanviar dades i a cada port s'assigna un número de port i una tasca específica. Per exemple, el port 80 s'utilitza per a l'HTTP. Un port específic només pot utilitzar-se per a una aplicació o un servei. Per tant, si tenim dos equips que intenten accedir a les dades a través del mateix port simultàniament, la connexió no serà possible. Per exemple, no podeu configurar el reenviament de port per al port 100 per a dos equips alhora.

- **IP local**: 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 **3.8 LAN** per obtenir més informació.

- **Port local**: 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.

- **Protocol**: Seleccioneu el protocol. No no n'esteu segur, seleccioneu **TOTS DOS**.

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.

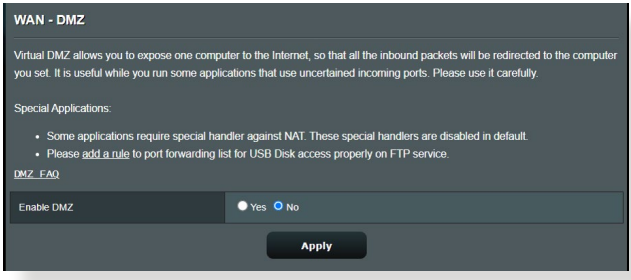
3.11.5 DMZ

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 riscs 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**.

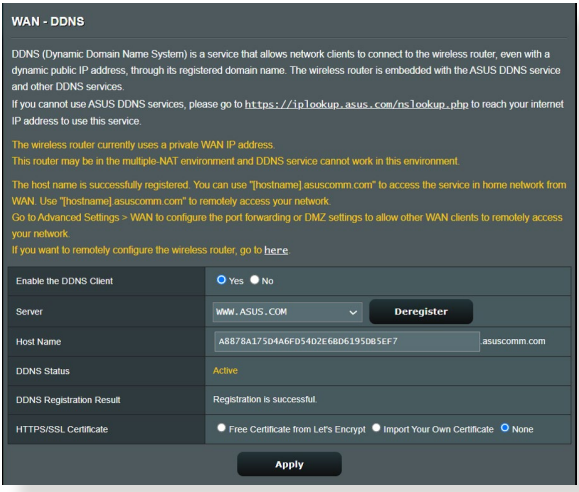
- **Adreça IP de l'estació exposada:** Introduïu l'adreça IP de la LAN del client que oferirà el servei de DMZ i estarà exposat a Internet. Comproveu que el client del servidor té una adreça IP estàtica.

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**.

3.11.6 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.



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:

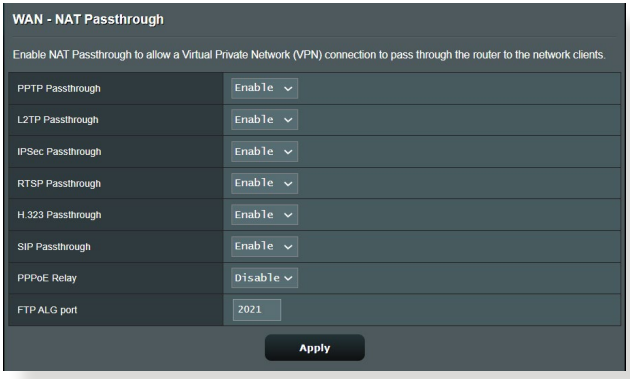
El servei de DDNS no funciona en aquests casos:

- 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.

3.11.7 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**.

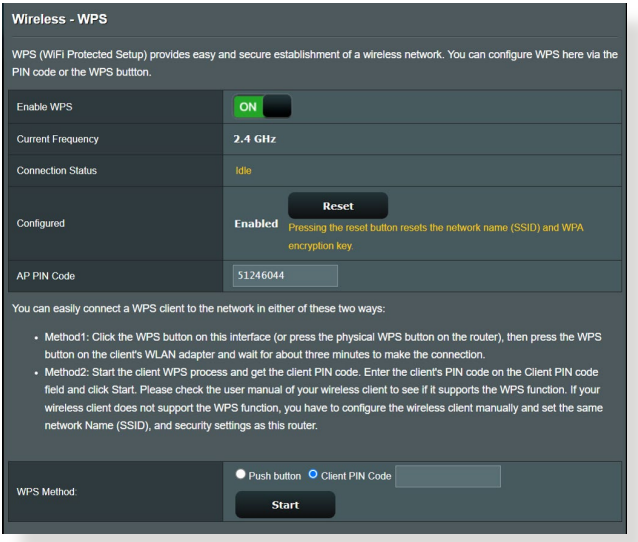


3.12 Wireless

3.12.1 WPS

WPS (configuració protegida per Wi-Fi, de l'anglès Wi-Fi 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.



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-Personal i WPA2-Personal. WPS no admet xarxes wireless que facin servir un mètode de xifratge de clau compartida, WPA-Enterprise, WPA2-Enterprise i RADIUS.

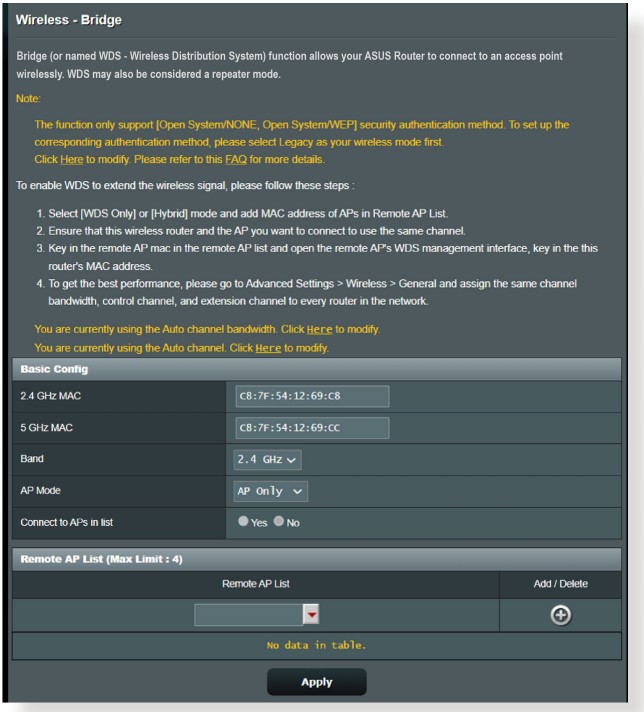
4. Al camp del mètode WPS, seleccioneu **Botó polsador** o **Codi PIN de client**. Si trieu **Botó polsador**, aneu al pas 5. Si trieu **Codi PIN de client**, aneu al pas 6.
5. Per configurar la WPS mitjançant el botó de WPS del router, seguiu aquests passos:
   a. Premeu **Inici** o premeu el botó de 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.

3.12.2 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.



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. Al camp **Canal de control**, seleccioneu el canal operatiu per al wireless bridge. Seleccioneu **Auto** perquè el router pugui seleccionar automàticament el canal amb menys interferències.

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

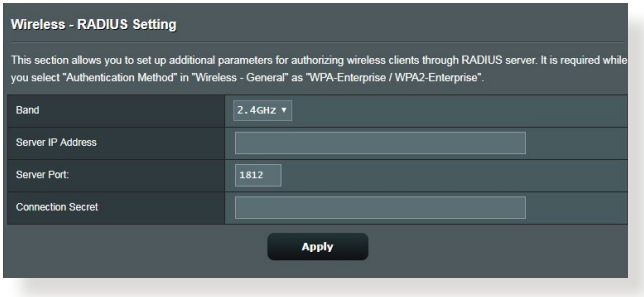
6. A la **Remote AP List (llista d'AP remots)**, introduïu una adreça MAC i premeu el botó **Afegir**  per introduir l'adreça MAC d'altres punts d'accés disponibles.

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**.

3.12.3 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.



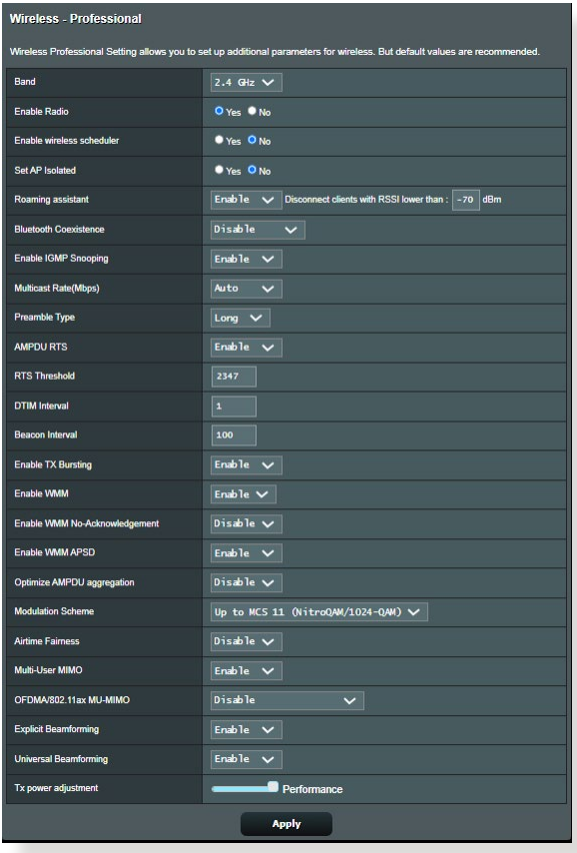
Per configurar la funció RADIUS wireless:

1. Confirmeu que el mode d'autenticació del wireless router és WPA-Enterprise, WPA2-Enterprise o Radius amb 802.1x.
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 **Secret de connexió**, introduïu la contrasenya que s'utilitzarà per accedir al servidor RADIUS.
6. Premeu **Aplicar**.

3.12.4 Professional

La pantalla Professional ofereix opcions de configuració avançades.

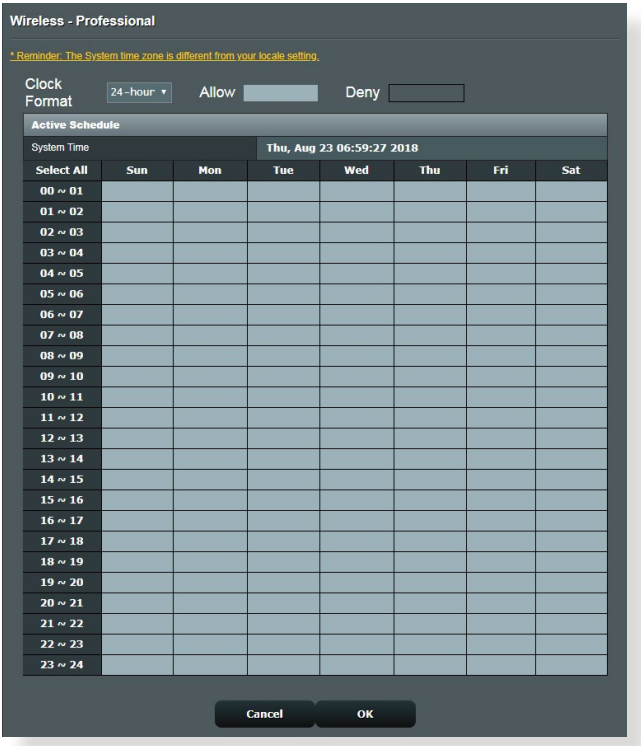
NOTA: Us recomanem que empreu els valors predeterminats d'aquesta pàgina.



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**: Podeu seleccionar un format horari de 24 o de 12 hores. El color de la taula indica Permetre o Rebutjar. Feu clic a les caselles corresponents per canviar la configuració de l'hora dels dies de la setmana i premeu **D'acord** quan acabeu.



- **Establir AP aïllat**: L'element Establir AP aïllat evita que els dispositius wirelesss 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 **Sí** per activar aquesta funció o seleccioneu **No** per desactivar-la.
- **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 el router 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 **Breu** per a una xarxa wireless ocupada amb molt tràfic. Seleccioneu **Llarg** si la vostra xarxa wireless consta de dispositius wireless més antics o heretats.
- **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.

4 Utilitats

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.

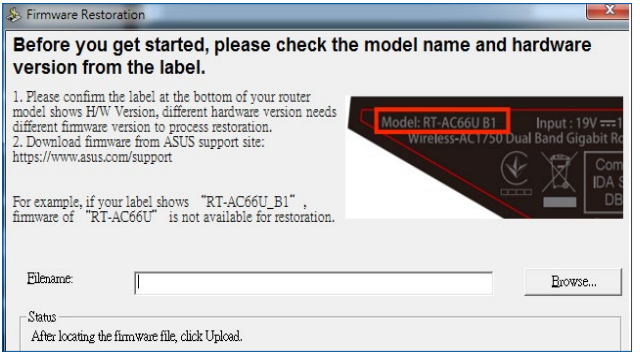
Per executar la utilitat Device Discovery:

- Des de l'escriptori de l'ordinador, premeu **Inicia** > **Tots els programes** > **Utilitat ASUS** > **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. Desendolleu 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** > **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.

5 Solució de problemes

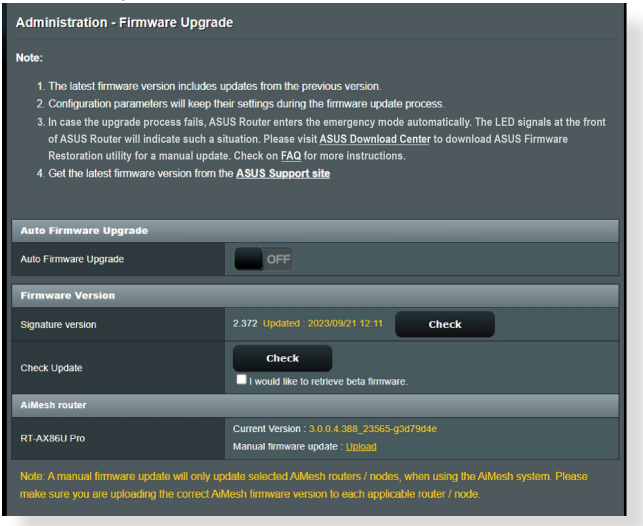
Aquest capítol ofereix solucions per als possibles problemes que poden aparèixer amb el router. Si us trobeu amb algun problema que no apareix en aquest capítol, visiteu el lloc web de suport tècnic d'ASUS a: https://www.asus.com/support/ per obtenir més informació sobre el producte i les dades de contacte 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://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/ per baixar el firmware més recent.
3. Des de la pàgina **Firmware Version (Versió de microprogramari)**, premeu **Comprovar** 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 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'encriptació i la contrasenya són correctes.

Comproveu si la configuració de xarxa és correcta.

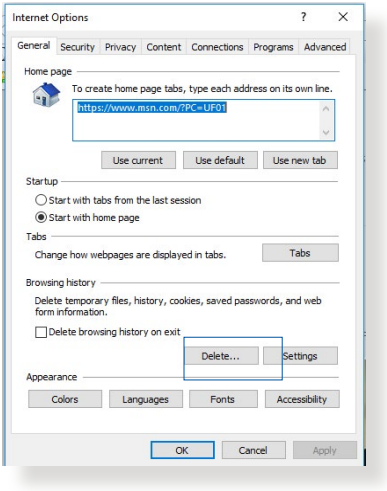
- Tots els clients de la xarxa han de tenir una adreça IP vàlida. ASUS recomana utilitzar el servidor de DHCP del wireless router per assignar adreces IP als ordinadors de la xarxa.
- Alguns proveïdors de servei de mòdem per cable exigeixen l'ús de l'adreça MAC de l'ordinador inicialment registrat en 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**.


Internet status:
Connected
WAN IP: 192.168.123.154
DDNS: GO
Security:
WPA2/WPA3-Personal
Clients: 1
View List
Client status
Online
Wired (1)
AA2281415-NB
192.168.50.155
00:E0:4C:71:F8:99
Refresh

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. 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**.



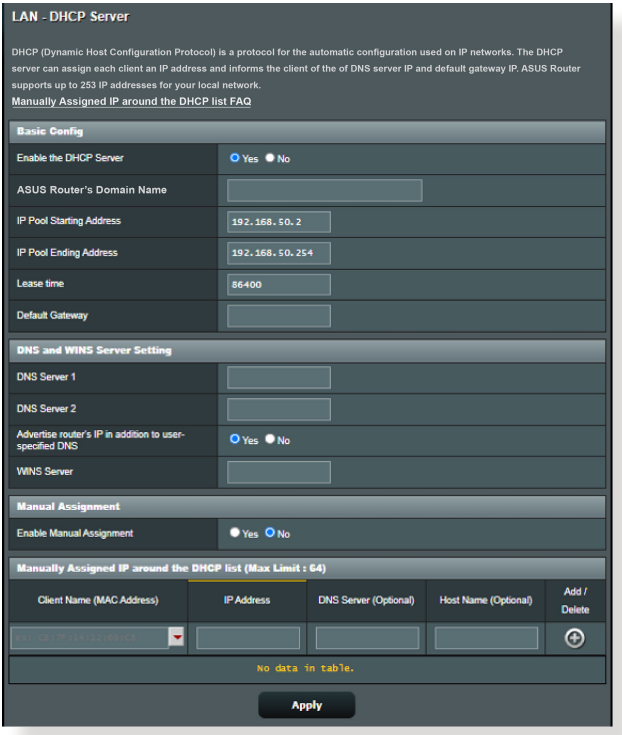
NOTES:

- 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.

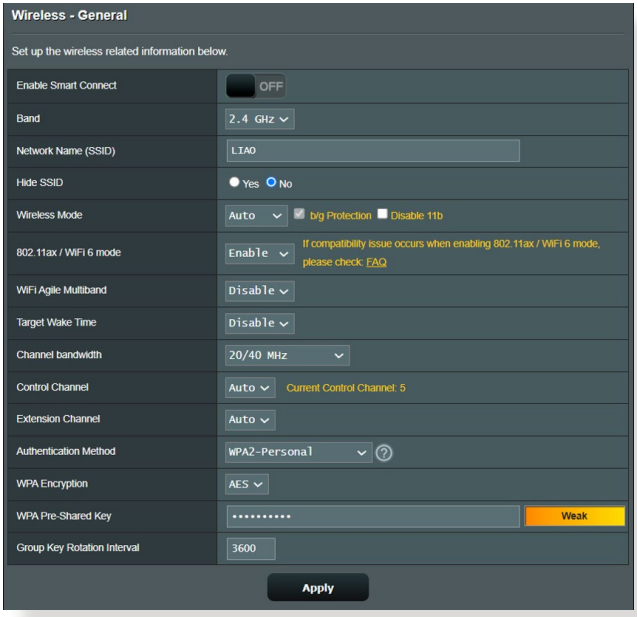
El client no pot establir una connexió per xarxa wireless amb el router.

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.

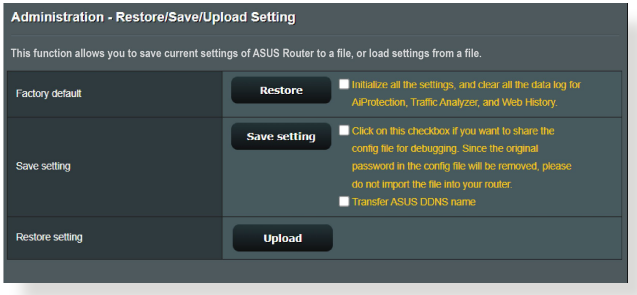
- **Fora d'abast:**
  - Apropeu el router al client wireless.
- **El servidor de DHCP s'ha deshabilitat:**
  1. Executeu la interfície gràfica (GUI) en línia. Aneu a **General** > **Mapa de la xarxa** > **Clients** i cerqueu el dispositiu que voleu connectar al router.
  2. Si no trobeu el dispositiu al **Mapa de la xarxa**, aneu a **Configuració avançada** > **LAN** > **Servidor DHCP**, llista de **Configuració bàsica**, seleccioneu **Sí** a **Habilitar el servidor DHCP**.



- 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**.



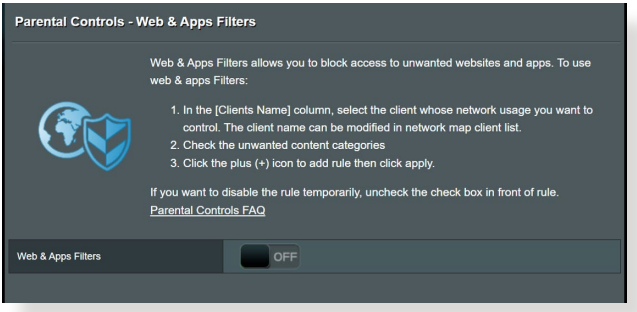
- Si utilitzeu un adaptador LAN wireless, comproveu si el canal wireless que utilitzeu és correcte per als canals disponibles a la vostra regió/país. Si no ho és, ajusteu el canal, l'ample de banda del canal i el mode wireless.
- Si encara no us podeu connectar al wireless router, restabliu la configuració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



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.

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.

Com restablir la configuració predeterminada de l'sistema?

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

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.

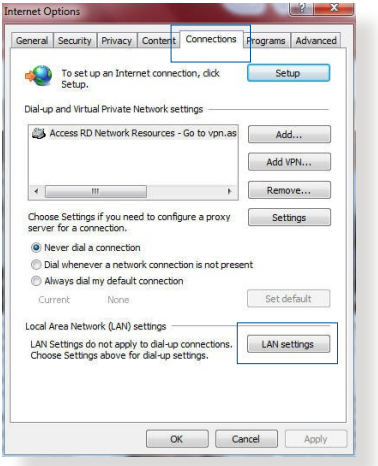
No es pot accedir a la interfície gràfica (GUI) en línia.

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

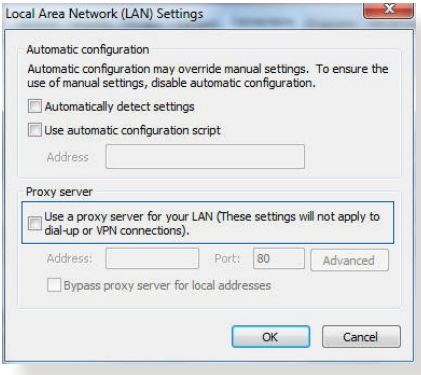
A. Deshabiliteu el servidor intermediari, si està habilitat.

Windows®

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

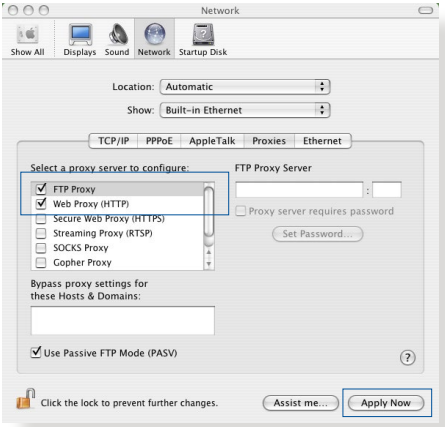


3. A la pantalla de configuració de la LAN, desmarqueu **Utilitza un servidor intermediari per a la LAN**.
4. Premeu **D'acord** quan acabeu.



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**.

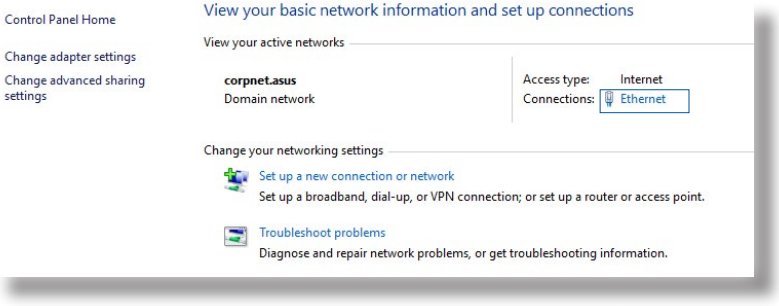


NOTA: Consulteu la funció d'ajuda del vostre navegador per saber com desactivar el servidor intermediari.

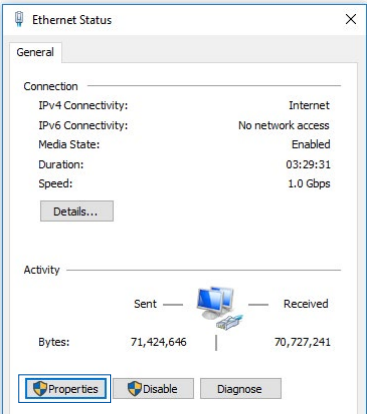
B. Configureu els paràmetres de TCP/IP per obtenir automàticament una adreça IP.

Windows®

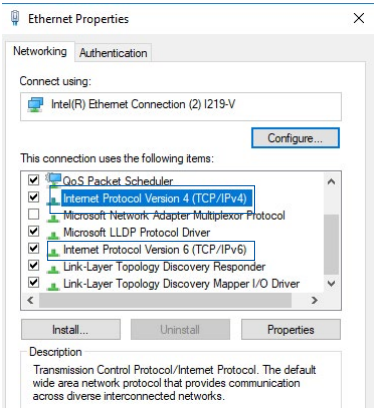
1. Premeu **Inicia** > **Tauler de control** > **Centre de xarxes i de recursos compartits**, premeu la connexió de xarxa per veure'n la finestra d'estat.



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



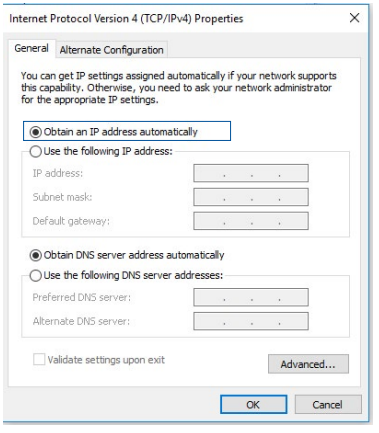
3. Seleccioneu **Versió 4 de protocol d'Internet (TCP/IPv4)** o **Versió 6 de protocol d'Internet (TCP/IPv6)** i premeu **Propietats**.



4. Per obtenir la configuració IP IPv4 automàticament, marqueu **Obtén l'adreça IP automàticament**.

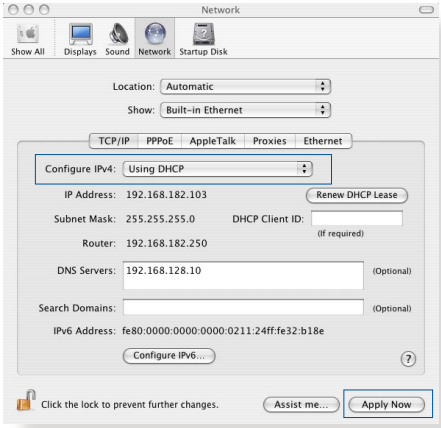
   Per obtenir la configuració IP IPv6 automàticament, marqueu **Obtén l'adreça IPv6 automàticament**.

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**.

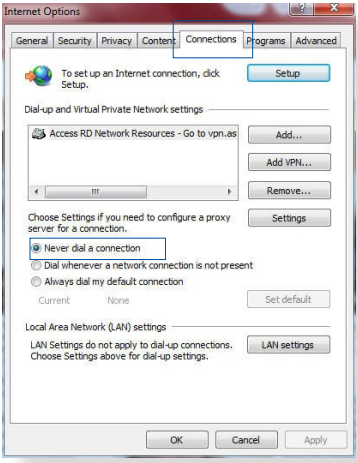


NOTA: Consulteu la funció d'ajuda i assistència tècnica del vostre sistema operatiu per obtenir informació sobre la configuració TCP/IP de l'equip.

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.

Apèndix

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

Avisos de seguretat

Durant l'ús d'aquest producte, seguiu sempre les precaucions bàsiques de seguretat, entre altres:

ADVERTÈNCIA!

- Els cables d'alimentació han de tenir connexió a terra. Connecteu l'equip únicament a un endoll de paret de fàcil accés.
- Si l'adaptador s'espatlla, no proveu de reparar-lo. Poseu-vos en contacte amb un tècnic qualificat o amb el vostre distribuïdor.
- NO feu servir cables, accessoris o perifèrics fets malbé.
- NO instal·leu aquest equip a més de 2 metres d'alçada.
- Utilitzeu aquest producte en entorns amb temperatures ambientals entre els 0 i els 40º C.
- Abans de fer servir el producte, llegiu les instruccions d'ús i respecteu l'interval de temperatures que s'hi especifica.
- Si feu servir aquest dispositiu en aeroports, hospitals, benzineres i tallers professionals, vetlleu per la vostra seguretat personal.
- Interferències amb dispositius mèdics: Manteniu una distància mínima de com a mínim 15 cm entre els dispositius mèdics implantats i els productes d'ASUS per reduir el risc d'interferències.
- Feu servir els productes d'ASUS amb bones condicions de recepció per minimitzar-ne els nivells de radiació.
- Allunyeu el producte de les dones embarassades i no l'apropeu a la part inferior de l'abdomen dels adolescents.
- NO utilitzeu aquest producte si s'hi observen defectes visibles, s'ha mullat, modificat o espatllat. Porteu-lo a reparar a un centre especialitzat.

ADVERTÈNCIA!

- NO el col·loqueu sobre superfícies de treball irregulars o inestables.
- NO col·loqueu ni deixeu caure cap objecte sobre el producte. No exposeu el producte a cap tipus d'alteració mecànica (no l'aixafeu, el doblegueu, el punxeu ni el tritureu).
- NO desmunteu el producte, no l'obriu, no el poseu al microones, no el cremeu, no el pinteu ni hi llenceu cap objecte a l'interior.
- Consulteu l'etiqueta que hi ha a la part inferior del producte i comproveu que el vostre adaptador de corrent s'ajusta a les especificacions que hi trobareu.
- Manteniu el producte allunyat del foc i les fonts de calor.
- NO l'exposeu a líquids, pluja o la humitat, ni l'utilitzeu en aquestes condicions. NO feu servir el producte durant una tempesta elèctrica.
- Connecteu els circuits de sortida PoE d'aquest producte exclusivament a xarxes de PoE, sense encaminar-los cap a instal·lacions externes.
- Per evitar descàrregues elèctriques, desconnecteu el cable de l'endoll abans de reubicar el sistema.
- Feu servir només els accessoris aprovats per a aquest model pel fabricant del dispositiu. L'ús d'altres tipus d'accessoris pot invalidar la garantia o pot infringir la normativa local i generar riscs per a la seguretat. Per saber quins accessoris autoritzats teniu al vostre abast, poseu-vos en contacte amb el vostre distribuïdor local.
- Si no respecteu les instruccions d'ús d'aquest producte, podeu provocar un incendi o causar lesions personals.

Servei i assistència tècnica

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