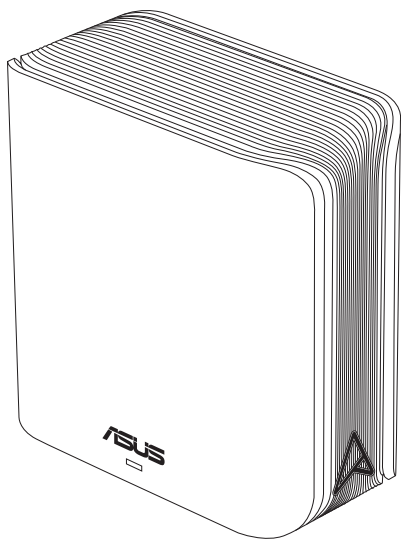


Manual de usuario

ZenWiFi BD4

Enrutador de doble banda BE3600



ASUS
IN SEARCH OF INCREDIBLE

S23951

Primera edición

Agosto de 2024

Copyright © 2024 ASUSTeK Computer Inc. Todos los derechos reservados.

Se prohíbe la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a cualquier idioma de este manual, íntegra o parcialmente, incluidos los productos y el software que en él se describen, de ninguna forma ni a través de ningún medio, a excepción de que tales actividades sean llevadas a cabo por el comprador con fines de conservación, sin autorización expresa por escrito de ASUSTeK Computer Inc. ("ASUS").

La garantía y los servicios de reparación vinculados al producto no serán de aplicación si: (1) el producto ha sido reparado, modificado o alterado, a excepción de que tal reparación, modificación o alteración haya sido autorizada por escrito por ASUS; o (2) no sea posible determinar el número de serie del producto o aquél no se encuentre presente.

ASUS PROPORCIONA ESTE MANUAL "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPRESAS NI IMPLÍCITAS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS O CONDICIONES DE COMERCIABILIDAD O AJUSTE A UNA FINALIDAD EN PARTICULAR. NI ASUS, NI SUS DIRECTORES, RESPONSABLES, EMPLEADOS O AGENTES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, ACCIDENTAL O CONSECUENTE (INCLUIDOS AQUELLOS DERIVADOS DE PÉRDIDAS DE BENEFICIOS, PÉRDIDAS DE OPORTUNIDADES COMERCIALES, IMPOSIBILIDAD DE USAR EL EQUIPO, PÉRDIDAS DE DATOS, INTERRUPCIONES DE LA ACTIVIDAD COMERCIAL Y OTROS PERJUICIOS DE CARÁCTER SIMILAR), AÚN CUANDO ASUS HAYA SIDO ADVERTIDA DE LA POSIBILIDAD DE QUE TALES DAÑOS TENGAN LUGAR COMO RESULTADO DE ALGÚN DEFECTO O ERROR EN ESTE MANUAL O EN EL PRODUCTO.

LAS ESPECIFICACIONES Y LA INFORMACIÓN QUE CONTIENE ESTE MANUAL SE PONEN A DISPOSICIÓN DEL PROPIETARIO CON FINES EXCLUSIVAMENTE INFORMATIVOS; AMBAS SE ENCUENTRAN SUJETAS A CAMBIOS EN CUALQUIER MOMENTO SIN AVISO PREVIO Y NO DEBEN CONSIDERARSE UN COMPROMISO EMPRENDIDO POR ASUS. ASUS NO ASUME RESPONSABILIDAD U OBLIGACIÓN ALGUNA EN RELACIÓN CON AQUELLOS ERRORES O IMPRECISIONES QUE ESTE MANUAL PUDIERA CONTENER, INCLUIDOS LOS PRODUCTOS Y EL SOFTWARE QUE EN ÉL SE DESCRIBEN.

Los nombres de productos y empresas que aparecen en este manual podrían ser o no marcas comerciales registradas o estar vinculados a derechos de autor en posesión de sus respectivas empresas propietarias; su uso se lleva a cabo exclusivamente con fines de identificación y explicación y en beneficio del propietario del producto, sin intención alguna de infringir los derechos indicados.

Contenidos

1 Conociendo su router inalámbrico

1.1	¡Bienvenido!	6
1.2	Contenido del paquete	6
1.3	El router inalámbrico	7
1.4	Ubicar el router inalámbrico	8
1.5	Requisitos de configuración	9

2 Introducción

2.1	Configuración del router	10
A.	Conexión por cable	11
B.	Conexión inalámbrica	12
2.2	Función Configuración rápida de Internet (QIS, Quick Internet Setup) con detección automática	14
2.3	Conectarse a la red inalámbrica	16

3 Definición de la configuración general y avanzada

3.1	Inicio de sesión en la interfaz gráfica del usuario web...	17
3.1.1	Para definir la configuración de seguridad inalámbrica	19
3.1.2	Administración de los clientes de red	20
3.2	CdS adaptativa	21
3.2.1	Administración del ancho de banda de la calidad de servicio (QoS, Quality of Service)	21
3.3	Administración	24
3.3.1	Modo de funcionamiento	24
3.3.2	Sistema	25
3.3.3	Actualización del firmware	26
3.3.4	Restaurar / Guardar / Enviar configuración	26
3.4	AiProtection	27
3.4.1	Protección de red	27
3.4.2	Configurar el control parental	31

Contenidos

3.5	Firewall.....	34
3.5.1	General.....	34
3.5.2	Filtro de direcciones URL.....	35
3.5.3	Filtro de palabras clave	36
3.5.4	Filtro de servicios de red.....	37
3.6	IPv6	38
3.7	LAN.....	39
3.7.1	Dirección IP LAN.....	39
3.7.2	DHCP Server (Servidor DHCP)	40
3.7.3	Ruta	42
3.7.4	IPTV	43
3.8	Red	44
3.8.1	Red principal - Filtro MAC	44
3.8.2	Red para invitados.....	46
3.8.2.1	Red para invitados	46
3.8.2.2	Smart Home Master.....	48
3.9	Registro del sistema.....	52
3.10	Analizador de tráfico	53
3.11	WAN.....	54
3.11.1	Conexión a Internet.....	54
3.11.2	Dual WAN (WAN dual)	57
3.11.3	Activador de puerto.....	58
3.11.4	Servidores virtuales/Reenvío de puertos	60
3.11.5	DMZ	63
3.11.6	DDNS	64
3.11.7	Paso a través NAT	65
3.12	Inalámbrico	66
3.12.1	WPS	66
3.12.2	Puente.....	68

Contenidos

3.12.3	Configuración de RADIUS	70
3.12.4	Profesional	71
4	Uso de las utilidades	
4.1	Detección de dispositivos.....	74
4.2	Restauración de firmware.....	74
5	Resolución de problemas	
5.1	Soluciones básicas de problemas	76
5.2	Preguntas más frecuentes (P+F)	79
	Apéndices	
	Avisos de seguridad	97
	Servicio y Soporte	99

1 Conociendo su router inalámbrico

1.1 ¡Bienvenido!

¡Gracias por adquirir un router inalámbrico ASUS ZenWiFi BD4!

Con un acento metálico en el color del monograma A en el chasis blanco minimalista, ZenWiFi BD4 cuenta con bandas dual de 2.4 GHz y 5 GHz para una transmisión HD inalámbrica simultánea inigualable; servidor SMB, servidor UPnP AV y servidor FTP para compartir archivos 24 horas al día los 7 días de la semana; capacidad para controlar 300,000 sesiones; y la tecnología de red ecológica de ASUS, que proporciona un 70% ahorro de energía.

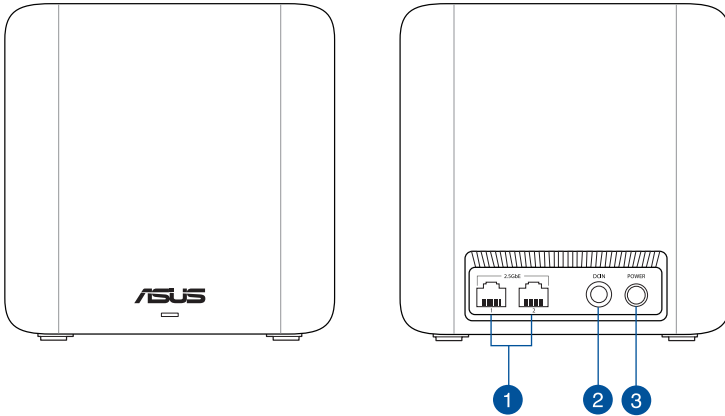
1.2 Contenido del paquete

- | | |
|--|---|
| <input checked="" type="checkbox"/> Router inalámbrico ZenWiFi BD4 | <input checked="" type="checkbox"/> Cable de red (RJ-45) |
| <input checked="" type="checkbox"/> Adaptador de alimentación | <input checked="" type="checkbox"/> Guía de inicio rápido |
| <input checked="" type="checkbox"/> Tarjeta de garantía | |

NOTAS:

- Si cualquiera de los artículos falta o se encuentra dañado, póngase en contacto con ASUS para realizar preguntas técnicas u obtener soporte técnico. Consulte **Service and Support (Servicio y soporte)** que se encuentra en la parte posterior de esta guía.
 - Conserve el material de embalaje original por si necesitara hacer uso de la garantía para realizar reparaciones o sustituciones.
-

1.3 El router inalámbrico



- 1 Puertos 2.5GbE (Detección automática de WAN/LAN)**
Conecte los cables de red en estos puertos para establecer una conexión WAN/LAN de 2.5GbE.
- 2 Puerto de alimentación (entrada de CC) (DCIN)**
Inserte el adaptador de CA integrado en este puerto y conecte el router a una toma de corriente.
- 3 Botón de encendido**
Presione este botón para encender o apagar el sistema.

NOTAS:

- Utilice únicamente el cargador incluido con el paquete. Si usa otros adaptadores, el dispositivo puede resultar dañado.
- **Especificaciones:**

Adaptador de alimentación de CC	Salida de CC: +12 V con una corriente máxima de 1.5 A		
Temperatura de funcionamiento	0~40°C	Almacenamiento	0~70°C
Humedad de funcionamiento	50~90%	Almacenamiento	20~90%

1.4 Ubicar el router inalámbrico

Para conseguir la mejor transmisión de señal inalámbrica entre el router inalámbrico y los dispositivos de red conectados a él, asegúrese de:

- Colocar el router inalámbrico en un área centralizada para conseguir la máxima cobertura inalámbrica para los dispositivos de red.
- Mantenga el dispositivo alejado de obstáculos metálicos y de la luz solar directa.
- Mantenga el producto alejado de dispositivos WiFi de 802.11g o 20 MHz, equipos periféricos de 2.4 GHz, dispositivos Bluetooth, teléfonos inalámbricos, transformadores, motores de alto rendimiento, luces fluorescentes, hornos microondas, frigoríficos y otros equipos industriales para evitar interferencias o pérdidas de señal.
- Actualícese siempre a la versión de firmware más reciente. Visite el sitio Web de ASUS en <http://www.asus.com> para obtener las actualizaciones de firmware más recientes.

1.5 Requisitos de configuración

Para configurar la red, necesita uno o dos equipos con los siguientes requisitos de sistema:

- Puerto Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Funcionalidad inalámbrica IEEE 802.11a/b/g/n/ac/ax
- Un servicio TCP/IP instalado
- Explorador web, como por ejemplo Internet Explorer, Firefox, Safari o Google Chrome

NOTAS:

- Si el equipo no cuenta con funcionalidad inalámbrica integrada, puede instalar un adaptador WLAN IEEE 802.11a/b/g/n/ac/ax en él para conectarse a la red.
- Con su tecnología de doble banda, el router inalámbrico admite señales inalámbricas de 2,4 GHz y 5 GHz simultáneamente. Esta característica permite llevar a cabo actividades relacionadas con Internet (como navegar o leer y redactar mensajes de correo electrónico) utilizando la banda de 2,4 GHz y, al mismo tiempo, transmitir por secuencias archivo de audio y vídeo en alta definición (como por ejemplo películas o música) utilizando la banda de 5 GHz.
- Algunos dispositivos IEEE 802.11n que desea conectar a la red puede que no admitan la banda de 5 GHz. Consulte el manual del dispositivo para conocer las especificaciones.
- Los cables Ethernet RJ-45 que se utilizarán para conectar dispositivos de red no deben tener más de 100 metros.

¡IMPORTANTE!

- Algunos adaptadores inalámbricos podrían tener problemas de conectividad con PA WiFi 802.11ax.
- Si experimenta tal problema, asegúrese de actualizar el controlador a la versión más reciente. Consulte el sitio de soporte técnico oficial del fabricante, donde puede obtener los controladores de software, las actualizaciones y otra información 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 Introducción

2.1 Configuración del router

¡IMPORTANTE!

- Utilice una conexión inalámbrica cuando configure el router inalámbrico para evitar posibles problemas de configuración.
 - Antes de configurar el router inalámbrico de ASUS, lleve a cabo las tareas siguientes:
 - Si va a reemplazar un router existente, desconéctelo de la red.
 - Desconecte los cables de la configuración de módem existente. Si el módem tiene una batería de repuesto, quítela también.
 - Reinicie el equipo (recomendado).
-



¡ADVERTENCIA!

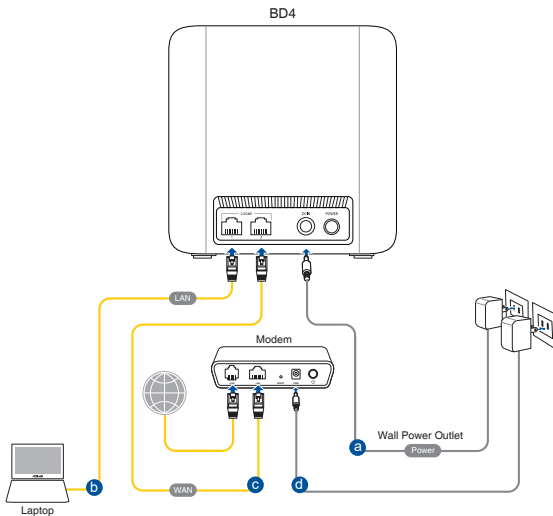
- Los cables de alimentación se deben enchufar a tomas de corriente que estén provistas de una conexión a tierra adecuada. Conecte el equipo solamente a una toma de corriente cercana y de fácil acceso.
 - No intente reparar la fuente de alimentación personalmente si se avería. Póngase en contacto con un técnico de mantenimiento autorizado o con su distribuidor.
 - NO cubra los orificios de ventilación del equipo de sobremesa para evitar que el sistema se caliente en exceso.
 - NO monte este equipo a una altura superior a 2 metros.
 - Use este producto en entornos sometidos a una temperatura ambiente comprendida entre 0 °C (32 °F) y 40 °C (104 °F).
-

A. Conexión por cable

NOTA: Puede utilizar un cable de empalme o un cable cruzado para la conexión cableada.

Para configurar el router inalámbrico a través de una conexión cableada:

1. Enchufe el router a una toma de corriente eléctrica y enciéndalo. Conecte el cable de red desde el equipo a un puerto 2.5GbE del router.

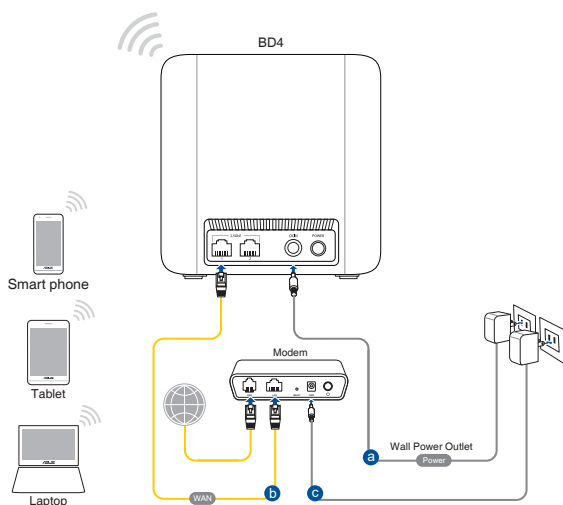


2. La GUI Web se inicia automáticamente cuando abre un explorador Web. Si no se inicia automáticamente, escriba <http://www.asusrouter.com>.
3. Configure una contraseña para el router para evitar el acceso no autorizado.

B. Conexión inalámbrica

Para configurar el router inalámbrico a través de una conexión inalámbrica:

1. Enchufe el router a una toma de corriente eléctrica y enciéndalo.



2. Conéctese al nombre de red (SSID) mostrado en la etiqueta del producto que se encuentra en la parte posterior del router. Para mejorar la seguridad de la red, cambie a un SSID único y asigne una contraseña.

Nombre Wi-Fi (SSID):	ASUS_XX
----------------------	---------

* **XX** y hace referencia a los dos últimos dígitos de la dirección MAC de 2,4 GHz. Puede encontrarlo en la etiqueta situada en la parte posterior del router.

3. La GUI Web se inicia automáticamente cuando abre un explorador Web. Si no se inicia automáticamente, escriba <http://www.asusrouter.com>.
4. Configure una contraseña para el router para evitar el acceso no autorizado.

NOTAS:

- Para obtener detalles sobre la conexión a una red inalámbrica, consulte el manual del usuario del adaptador WLAN.
 - Para definir la configuración de seguridad para la red, consulte la sección **3.1.1 Definición de la configuración de seguridad inalámbrica** de este manual.
-

2.2 Función Configuración rápida de Internet (QIS, Quick Internet Setup) con detección automática

La función QIS le ayuda a configurar rápidamente la conexión a Internet.

NOTA: Cuando establezca la conexión de Internet por y primera vez, presione el botón Reiniciar del router inalámbrico para restablecer su configuración predeterminada de fábrica.

Para utilizar QIS con detección automática:

1. Inicie un explorador Web. Se le redirigirá al Asistente para configuración de ASUS (Configuración rápida de Internet). Si no, introduzca la siguiente dirección de forma manual <http://www.asusrouter.com>.
2. El router inalámbrico detectará automáticamente si el tipo de conexión ISP es **Dynamic IP (Dirección IP dinámica)**, **PPPoE**, **PPTP** o **L2TP**. Especifique la información necesaria para el tipo de conexión ISP.

¡IMPORTANTE! Obtenga la información necesaria sobre el tipo de conexión a Internet de su ISP.

NOTAS:



- La detección automática del tipo de conexión de su ISP se realiza cuando el router inalámbrico se configura por primera vez o cuando se restablece la configuración predeterminada de dicho router.
 - Si QIS no puede detectar el tipo de conexión de Internet, haga clic en **Manual setting (Configuración manual)** y defina manualmente la configuración de la conexión.
-
3. Asigne el nombre de la red inalámbrica (SSID) y la clave de seguridad para su conexión inalámbrica de red WiFi 7. Cuando haya terminado, haga clic en **Apply (Aplicar)**.
 4. En la página **Login Information Setup (Información de inicio de sesión)**, cambie la contraseña de inicio de sesión del router para impedir el acceso no autorizado.

NOTA: El nombre de usuario y la contraseña de inicio de sesión del router inalámbrico son diferentes del nombre de red de WiFi 7 (SSID) y de la clave de seguridad. El nombre de usuario y la contraseña de inicio de sesión del router inalámbrico le permiten iniciar sesión en la interfaz gráfica del usuario Web para definir la configuración de dicho router. El nombre de red de WiFi 7 (SSID) y la clave de seguridad permiten a los dispositivos Wi-Fi iniciar sesión y conectarse a la red de WiFi 7.

2.3 Conectarse a la red inalámbrica

Después de configurar el router inalámbrico a través de QIS, puede conectar el equipo u otros dispositivos inteligentes a la red inalámbrica.

Para conectarse a la red:

1. En el equipo, haga clic en el icono de red  del área de notificación para mostrar las redes inalámbricas disponibles.
2. Seleccione la red inalámbrica a la que desea conectarse y, a continuación, haga clic en **Connect (Conectar)**.
3. Puede que tenga que escribir la clave de seguridad de la red si se trata de una red inalámbrica segura y, a continuación, hacer clic en **OK (Aceptar)**.
4. Espere mientras el equipo establece conexión con la red inalámbrica correctamente. Se mostrará el estado de la conexión y el icono de red indicará el estado de conectado .

NOTAS:

- Consulte los capítulos siguientes para obtener más detalles sobre cómo definir la configuración de la red inalámbrica.
 - Consulte el manual del usuario del dispositivo para obtener más detalles sobre cómo conectarlo a la red inalámbrica.
-

3 Definición de la configuración general y avanzada

3.1 Inicio de sesión en la interfaz gráfica del usuario web

El router inalámbrico de ASUS incluye una intuitiva interfaz gráfica del usuario web (GUI, Graphics User Interface) que permite configurar fácilmente sus distintas funciones mediante un explorador Web, como por ejemplo Internet Explorer, Firefox, Safari o Google Chrome.

NOTA: Las características pueden variar en función de las diferentes versiones de firmware.

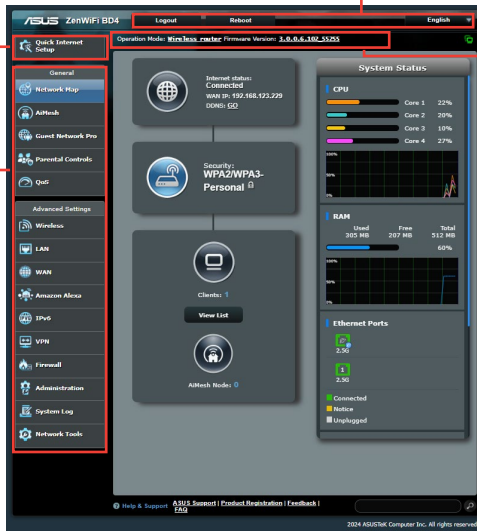
Para iniciar sesión en la interfaz gráfica del usuario web:

1. En su explorador web (Internet Explorer, Firefox, Safari o Google Chrome) inserte manualmente la dirección IP predeterminada del router inalámbrico: <http://www.asusrouter.com>.
2. En la página de inicio de sesión, Introduzca el nombre de usuario y la contraseña que haya establecido **2.2 Quick Internet Setup (QIS) with Auto-dection (2.2 Configuración rápida de Internet (QIS) con Detección automática)**.
3. Ahora puede utilizar la interfaz gráfica del usuario Web (GUI Web) para definir las diferentes configuraciones del router inalámbricos de ASUS.

Botones de los principales comandos

QIS-
Configuración
rápida de
Internet

Panel de
navegación



Título de
información

* La imagen es solo para referencia.

NOTA: Si inicia sesión en la interfaz gráfica del usuario Web por primera vez, se le redirigirá a la página Quick Internet Setup (QIS) (Configuración rápida de Internet) automáticamente.

3.1.1 Para definir la configuración de seguridad inalámbrica

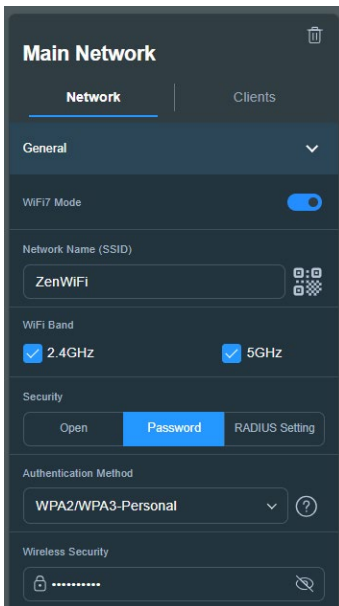
Para proteger la red inalámbrica contra accesos no autorizados, es necesario definir la configuración de seguridad de la misma.

Para definir la configuración de seguridad inalámbrica:

1. En el panel de navegación, vaya a **General > ficha Network Map (Mapa de red)**.
2. Seleccione la red y podrá configurar los ajustes de seguridad inalámbrica, como SSID, nivel de seguridad y ajustes de cifrado.

NOTA: Puede definir diferentes configuraciones de seguridad inalámbricas para las bandas de 2.4 GHz y 5 GHz.

Configuración de 2.4 GHz/5 GHz



3. En el campo **Network Name (SSID) (Nombre de red (SSID))**, escriba un nombre único para la red inalámbrica.

4. En la lista desplegable **Cifrado WEP**, seleccione el método de cifrado para la red inalámbrica.

¡IMPORTANTE! El estándar IEEE 802.11n/ac/ax prohíbe el uso de alto rendimiento con WEP o WPA-TKP como el cifrado unidifusión. Si utiliza estos métodos de cifrado, la tasa de datos caerá a la conexión de 54 Mbps IEEE 802.11g.

5. Escriba su clave de paso de seguridad.
6. Cuando haya terminado, haga clic en **Apply (Aplicar)**.

3.1.2 Administración de los clientes de red



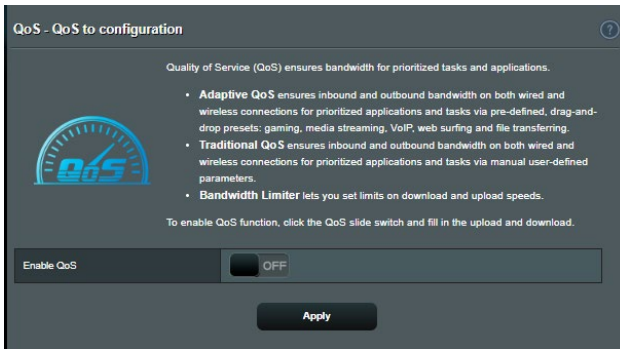
Para administrar los clientes de red:

1. En el panel de navegación, vaya a **General > Network Map (Mapa de red)**.
2. En la pantalla Network Map (Mapa de red), seleccione el icono **Client Status (Estado de los clientes)** para mostrar la información sobre los clientes de la red.
3. Para bloquear el acceso de un cliente a la red, seleccione dicho cliente y haga clic en **block (bloquear)**.

3.2 CdS adaptativa

3.2.1 Administración del ancho de banda de la calidad de servicio (QoS, Quality of Service)

La calidad de servicio (QoS) permite establecer la prioridad del ancho de banda y administrar el tráfico de la red.



Para configurar la prioridad del ancho de banda:

1. En el panel de navegación, vaya a **General > Adaptive QoS (CdS adaptativa) > QoS (CdS)**.
2. Haga clic en **ON (ACTIVAR)** para habilitar la regla predeterminada y rellene los campos de ancho de banda de carga y descarga.

NOTA: Solicite la información del ancho de banda a su ISP.

3. Haga clic en **Apply (Aplicar)**.

NOTA: la opción User Specify Rule List (Lista de reglas específicas del usuario) es para configuración avanzada. Si desea dar prioridad a aplicaciones y servicios de red específicos, seleccione **User-defined QoS rules (Reglas de CdS definidas por el usuario)** o **User-defined Priority (Prioridad definida por el usuario)** en la lista desplegable situada en la esquina superior derecha.

4. En la página **User-defined QoS rules (Reglas de CdS definidas por el usuario)**, existen cuatro tipos de servicio en línea predeterminados: navegación por Internet, HTTPS y transferencias de archivos. Seleccione el servicio que prefiera, rellene los campos **Source IP or MAC (Dirección IP o MAC de origen)**, **Destination Port (Puerto de destino)**, **Protocol (Protocolo)**, **Transferred (Transferidos)** y **Priority (Prioridad)** y, a continuación, haga clic en **Apply (Aplicar)**. La información se configurará en la pantalla QoS rules (Reglas de CdS).
-

NOTAS:

- Para rellenar la dirección IP o MAC de origen, puede:
 - a) Indicar una dirección IP específica, como por ejemplo "192.168.122.1".
 - b) Indicar direcciones IP dentro de una subred o dentro del mismo grupo de direcciones IP, como por ejemplo "192.168.123.*" o "192.168.*.*"
 - c) Indicar todas las direcciones IP como "*.*.*.*" o dejar el campo en blanco.
 - d) El formato de la dirección MAC consiste en seis grupos de dos dígitos hexadecimales separados por dos puntos (:), en orden de transmisión (por ejemplo 12:34:56:aa:bc:ef)
 - Para el intervalo de puertos de origen o destino, puede llevar a cabo una de las acciones siguientes:
 - a) Indicar un puerto específico, como por ejemplo "95".
 - b) Indicar puertos comprendidos dentro de un intervalo, como por ejemplo "103:315"; ">100" o "<65535".
 - La columna **Transferred (Transferidos)** contiene información sobre el tráfico ascendente y descendente (tráfico de red saliente y entrante) para una sección. En esta columna, puede establecer el límite de tráfico de red (en KB) para un servicio específico para generar prioridades determinadas para el servicio asignado a un puerto concreto. Por ejemplo, si dos clientes de red, PC 1 y PC 2, acceden a Internet (establecido en el puerto 80), pero PC 1 supera el límite de tráfico de red debido algunas tareas de descarga, pasará a tener una prioridad más baja. Si no desea establecer el límite de tráfico, déjelo en blanco.
-

5. En la página **User-defined Priority (Prioridad definida por el usuario)**, puede dar prioridad a las aplicaciones o los dispositivos de la red en cinco niveles en la lista desplegable **User-defined QoS rules (Reglas de CdS definidas por el usuario)**. Basándose en el nivel de prioridad, puede utilizar los métodos siguientes para enviar paquetes de datos:
 - Cambie el orden de paquetes de red ascendentes que se envían a Internet.
 - En la tabla **Upload Bandwidth (Ancho de banda de carga)**, establezca **Minimum Reserved Bandwidth (Ancho de banda reservado mínimo)** y **Maximum Bandwidth Limit (Límite de ancho de banda máximo)** para varias aplicaciones de red con diferentes niveles de prioridad. Los porcentajes indican las tasas de ancho de banda de carga que están disponibles para aplicaciones de red especificadas.

NOTAS:

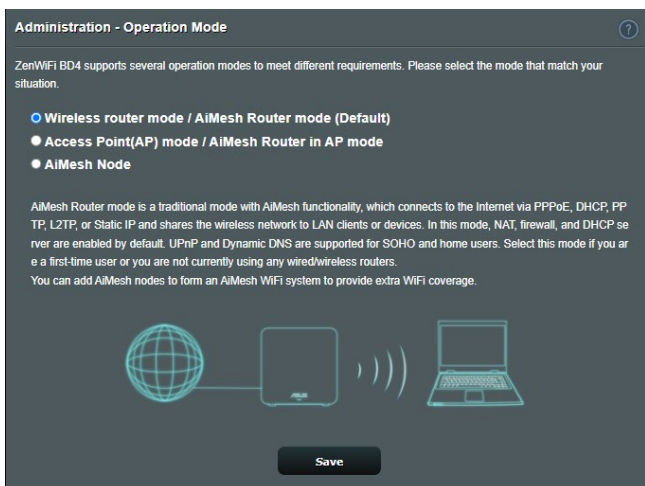
- los paquetes de baja prioridad se ignoran para garantizar la transmisión de los paquetes de alta prioridad.
 - En la tabla **Download Bandwidth (Ancho de banda de descarga)**, establezca **Maximum Bandwidth Limit (Límite de ancho de banda máximo)** para varias aplicaciones de red en el orden correspondiente. El paquete ascendente de prioridad más alta dará lugar al paquete descendente de prioridad más alta.
 - Si las aplicaciones de alta prioridad no tienen paquetes para enviar, la tasa de transmisión total de la conexión de Internet estará disponible para los paquetes de baja prioridad.
-
6. Establezca el paquete de prioridad más alta. Para garantizar una experiencia de juego en línea homogénea, puede establecer ACK, SYN y ICMP como el paquete de más alta prioridad.

NOTA: Asegúrese de habilitar CdS primero y configure los límites de tasa de carga y descarga.

3.3 Administración

3.3.1 Modo de funcionamiento

La página Operation Mode (Modo de funcionamiento) permite seleccionar el modo apropiado para la red.



Para configurar el modo de funcionamiento:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Administration (Administración) > Operation Mode (Modo de funcionamiento)**.
2. Seleccione cualquiera de estos modos de funcionamiento:
 - **Wireless router mode (default) (Modo Router inalámbrico (predeterminado)):** En el modo Router inalámbrico, el router inalámbrico se conecta a Internet y proporciona acceso a Internet a los dispositivos disponibles en su propia red local.
 - **Access Point mode (Modo Punto de acceso):** En este modo, el router crea una nueva conexión inalámbrica en una vez existente.
 - **AiMesh Node (Nodo AiMesh):** Puede establecer ZenWiFi BD4 como un nodo AiMesh para extender la cobertura Wi-Fi de los routers AiMesh existentes.

3. Haga clic en **Save (Guardar)**.

NOTA: El router se reiniciará cuando se cambie de modo.

3.3.2 Sistema

La página **System (Sistema)** permite definir la configuración inalámbrica del router.

Para definir la configuración del sistema:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Administration (Administración) > System (Sistema)**.
2. Puede configurar los ajustes parámetros:
 - **Change router login password (Cambiar contraseña de inicio de sesión del router):** Puede cambiar la contraseña y el nombre de inicio de sesión para el router inalámbrico introduciendo un nombre y contraseña nuevos.
 - **WPS button behavior (Comportamiento del botón WPS):** El botón físico WPS del router inalámbrico se puede utilizar para activar WPS.
 - **Time Zone (Zona horaria):** Seleccione la zona horaria para la red.
 - **NTP Server (Servidor NTP):** El router inalámbrico puede acceder a un servidor NTP (Network time Protocol, es decir, Protocolo de hora de red) para sincronizar la hora.
 - **Enable Telnet (Habilitar Telnet):** Haga clic en **Yes (Sí)** para habilitar los servicios Telnet en la red. Haga clic en **No** para deshabilitar Telnet.
 - **Authentication Method (Método de autenticación):** Puede seleccionar HTTP, HTTPS o ambos protocolos para proteger el acceso del router.
 - **Enable Web Access from WAN (Habilitar acceso Web desde WAN):** Seleccione **Yes (Sí)** para permitir que los dispositivos que se encuentran fuera de la red accedan a la configuración GUI del router inalámbrico. Seleccione **No** para impedir el acceso.
 - **Only allow specific IP (Permitir solo direcciones IP específicas):** Haga clic en **Yes (Sí)** si desea especificar las direcciones IP de dispositivos a los que se permite acceder a la configuración GUI del router inalámbrico desde WAN.
3. Haga clic en **Apply (Aplicar)**.

3.3.3 Actualización del firmware

NOTA: Descargue la versión más reciente del firmware del sitio Web de ASUS, a través de la dirección <http://www.asus.com>.

Para actualizar el firmware:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Administration (Administración) > Firmware Upgrade (Actualizar firmware)**.
 2. En el campo **Firmware Version (Versión de firmware)**, haga clic en **Check (Comprobar)** para buscar el archivo descargado.
 3. Haga clic en **Upload (Enviar)**.
-

NOTAS:

- Cuando el proceso de actualización se complete, espere un poco para que el sistema se reinicie.
 - Si falla el proceso de actualización el router entrará automáticamente en el modo de emergencia o fallo y el LED de alimentación del panel delantero parpadeará lentamente. Para recuperar o restaurar el sistema, consulte la sección **4.2 Restauración del firmware**.
-

3.3.4 Restaurar / Guardar / Enviar configuración

Para restaurar / guardar / enviar la configuración:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Administration (Administración) > Restore/Save/Upload Setting (Restaurar, guardar o cargar configuración)**.
 2. Seleccione las tareas que desee realizar:
 - Para restaurar la configuración predeterminada de fábrica haga clic en **Restore (Restaurar)** y después en **OK (Aceptar)** en el mensaje de confirmación.
 - Para guardar la configuración del sistema actual, haga clic en **Save setting (Guardar configuración)**, desplácese a la carpeta en la que pretende guardar el archivo y, por último, haga clic en **Save (Guardar)**.
 - Para restaurar la configuración anterior del sistema, haga clic en **Upload (Enviar)** para localizar el archivo que desee restaurar y haga clic en **Open (Abrir)**.
-

¡IMPORTANTE! Si se producen problemas, cargue la versión de firmware más reciente y defina la nueva configuración. No restaure la configuración predeterminada del router.

3.4 AiProtection

Proporciona supervisión en tiempo real que detecta malware, spyware y acceso no deseado. También filtra sitios Web y aplicaciones no deseados y permite programar un tiempo durante el que un dispositivo conectado es capaz de acceder a Internet.

3.4.1 Protección de red

La protección de red impide explotaciones de red y protege su red contra acceso no autorizado.

The screenshot displays the AiProtection control panel. At the top, it states "Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access." and includes a "Trend Micro SMART HOME NETWORK" logo. A diagram shows a network flow from a globe (2) through a router (1) to a smartphone (3) and a laptop. Below this is a toggle switch for "Enabled AiProtection" which is currently set to "OFF".

Feature	Description	Status	Protection Level
Router Security Assessment	Scan your router to find vulnerabilities and offer available options to enhance your devices protection.	Scan	1 Danger
Malicious Sites Blocking	Restrict access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking, and ransomware attacks.	ON	0 Protection
Two-Way IPS	The Two-Way Intrusion Prevention System protects any device connected to the network from spam or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability attacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outgoing packets from infected devices and avoids botnet attacks.	ON	0 Protection
Infected Device Prevention and Blocking	This feature prevents infected devices from being enslaved by botnets or zombie attacks which might steal your personal information or attack other devices.	ON	0 Protection

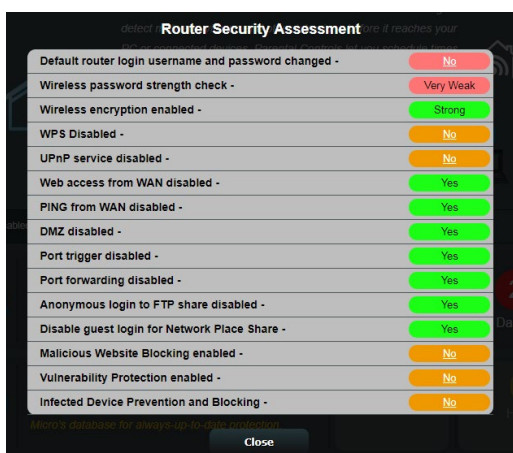
An "Alert Preference" button is located at the bottom right of the interface.

Configurar la protección de red

Para configurar la protección de red:

1. En el panel de navegación, vaya a **General > AiProtection**.
2. En la página principal **AiProtection**, haga clic en **Network Protection (Protección de red)**.
3. En la ficha **Network Protection (Protección de red)**, haga clic en **Scan (Explorar)**.

Cuando la exploración termine, la utilidad mostrará los resultados en la página **Router Security Assessment (Evaluación de la seguridad del router)**.



¡IMPORTANTE! Los elementos marcados como **Yes (Sí)** en la página **Router Security Assessment (Evaluación de la seguridad del router)** se consideran que tienen un estado **seguro**. Es muy recomendable que los elementos marcados como **No, Weak (Débil)** o **Very Weak (Muy débil)** se configuren en consecuencia.

4. (Opcional) En la página **Router Security Assessment (Evaluación de la seguridad del router)**, configure manualmente los elementos marcados como **No, Weak (Débil)** o **Very Weak (Muy débil)**. Para ello:
 - a. Haga clic en un elemento.

NOTA: Cuando haga clic en un elemento, la utilidad le remitirá a la página de configuración de dicho elemento.

- b. En la página de configuración de seguridad del elemento, realice la configuración y los cambios necesarios y haga clic en **Apply (Aplicar)** cuando termine.
 - c. Vuelva a la página **Router Security Assessment (Evaluación de la seguridad del router)** y haga clic en **Close (Cerrar)** para salir de la página.
5. Para definir automáticamente la configuración de seguridad, haga clic en **Secure Your Router (Proteger el router)**.
 6. Cuando aparezca un mensaje, haga clic en **OK (Aceptar)**.

Bloqueo de sitios malintencionados

Esta función restringe el acceso a sitios Web malintencionados conocidos en la base de datos para disponer de una protección continuamente actualizada.

NOTA: Esta función se habilita automáticamente si ejecuta **Router Weakness Scan (Exploración de debilidad del router)**.

Para habilitar el bloqueo de sitios malintencionados:

1. En el panel de navegación, vaya a **General > AiProtection**.
2. En la página principal **AiProtection**, haga clic en **Network Protection (Protección de red)**.
3. En el panel **Malicious Sites Blocking (Bloqueo de sitios malintencionados)**, haga clic en **ON (ACTIVAR)**.

IPS bidireccional

La función IPS (Intrusion Prevention System, es decir, Sistema de prevención de intrusiones) bidireccional protege su router de los ataques de la red tanto bloqueando paquetes entrantes maliciosos como detectando paquetes salientes sospechosos.

NOTA: Esta función se habilita automáticamente si ejecuta **Router Weakness Scan (Exploración de debilidad del router)**.

Para habilitar la protección contra vulnerabilidades:

1. En el panel de navegación, vaya a **General > AiProtection**.
2. En la página principal **AiProtection**, haga clic en **Network Protection (Protección de red)**.
3. En el panel **Two-Way IPS (IPS bidireccional)**, haga clic en **ON (ACTIVAR)**.

Prevención y bloqueo de dispositivos infectados

Esta función impide que los dispositivos infectados comuniquen información personal o el estado infectado a sus homólogos externos.

NOTA: Esta función se habilita automáticamente si ejecuta **Router Weakness Scan (Exploración de debilidad del router)**.

Para habilitar la protección contra vulnerabilidades:

1. En el panel de navegación, vaya a **General > AiProtection**.
2. En la página principal **AiProtection**, haga clic en **Network Protection (Protección de red)**.
3. En el panel **Infected Device Prevention and Blocking (Prevención y bloqueo de dispositivos infectados)**, haga clic en **ON (ACTIVAR)**.

Para configurar la preferencia de alertas:

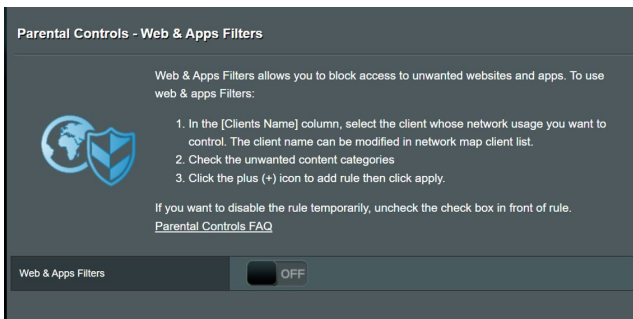
1. En el panel **Infected Device Prevention and Blocking (Prevención y bloqueo de dispositivos infectados)**, haga clic en **Alert Preference (Preferencia de alertas)**.
2. Seleccione o escriba el proveedor de correo electrónico, la cuenta de correo electrónico y la contraseña y, a continuación, haga clic en **Apply (Aplicar)**.

3.4.2 Configurar el control parental

El control parental le permite controlar el tiempo de acceso a Internet o establecer el límite de tiempo para el uso de red de un cliente.

Para ir a la página principal de Parental Controls (Controles parentales):

En el panel de navegación, vaya a **General > Parental Controls (Controles parentales)**.



Filtros Web y de aplicaciones

Filtros Web y de aplicaciones es una función de **Parental Controls (Controles parentales)** que le permite bloquear el acceso a sitios o aplicaciones Web no deseados.

Para configurar los filtros Web y de aplicaciones:

1. En el panel de navegación, vaya a **General > Parental Controls (Controles parentales)**.
2. En el panel **Web & Apps Filters (Filtros Web y de aplicaciones)**, haga clic en **ON (ACTIVAR)**.
3. Cuando aparezca el mensaje del contrato de licencia del usuario final (CLUF), haga clic en **I agree (Acepto)** para continuar.
4. En la columna **Client List (Lista de clientes)**, seleccione o escriba el nombre del cliente del cuadro de lista desplegable.

5. En la columna **Content Category (Categoría de contenido)**, seleccione los filtros de las cuatro categorías principales: **Adult (Adulto)**, **Instant Message and Communication (Mensaje y comunicación instantáneos)**, **P2P and File Transfer (P2P y transferencia de archivos)** y **Streaming and Entertainment (Streaming y entretenimiento)**.
6. Haga clic en  para agregar el perfil del cliente.
7. Haga clic en **Apply (Aplicar)** para guardar la configuración.

Parental Controls - Web & Apps Filters


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

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

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

Web & Apps Filters ON

Client List (Max Limit : 64)

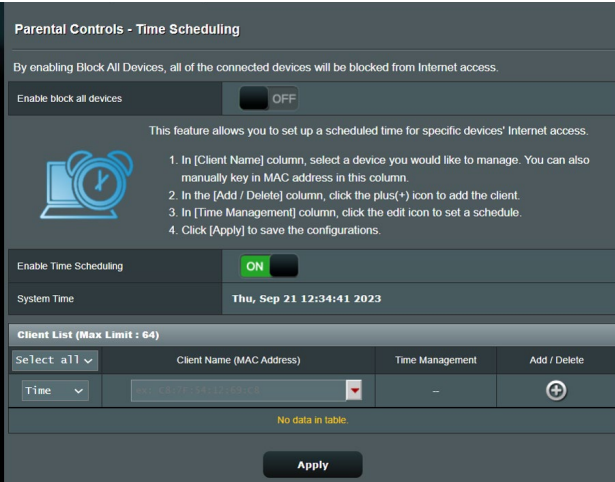
<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	<input type="text" value="192.168.1.100"/>	<input type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.	
		<input type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.	
		<input type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.	
		<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	
No data in table.			

Apply

Programación de tiempo

La programación de tiempo le permite establecer el límite de tiempo para el uso de red de un cliente.

NOTA: Asegúrese de que la hora del sistema está sincronizada con el servidor NTP.



Parental Controls - Time Scheduling

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

Enable block all devices OFF

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

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

Enable Time Scheduling ON

System Time Thu, Sep 21 12:34:41 2023

Client List (Max Limit : 64)

Select	Client Name (MAC Address)	Time Management	Add / Delete
Time		-	+


No data in table.

Apply

Para configurar la programación de tiempo:

1. En el panel de navegación, vaya a **General > Parental Controls (Controles parentales) > Time Scheduling (Programación de tiempo)**.
2. En el panel **Enable Time Scheduling (Habilitar programación de tiempo)**, haga clic en **ON (ACTIVAR)**.
3. En la columna **Clients Name (Nombre del cliente)**, seleccione o escriba el nombre del cliente del cuadro de lista desplegable.

NOTA: También puede escribir la dirección MAC del cliente en la columna **Client's MAC address (Dirección MAC del cliente)**. Asegúrese de que el nombre del cliente no contiene caracteres especiales o espacios, ya que estos podrían hacer que el enrutador funcionara anormalmente.

4. Haga clic en  para agregar el perfil del cliente.
5. Haga clic en **Apply (Aplicar)** para guardar la configuración.

3.5 Firewall

El router inalámbrico puede actuar como un firewall de hardware para la red.

NOTA: La función Firewall está habilitada de forma predeterminada.

3.5.1 General

Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.
[DoS Protection FAQ](#)

Enable Firewall Yes No

Enable DoS protection Yes No

Logged packets type

Respond ICMP Echo (ping) Request from WAN Yes No

Basic Config

Enable IPv4 inbound firewall rules Yes No

Inbound Firewall Rules (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>
No data in table.			

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified.
(2001::1111:2222:3333/64 for example)

Basic Config

Enable IPv6 Firewall Yes No

Famous Server List

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="button" value="⊕"/>
No data in table.					

Para definir configuración básica de Firewall:

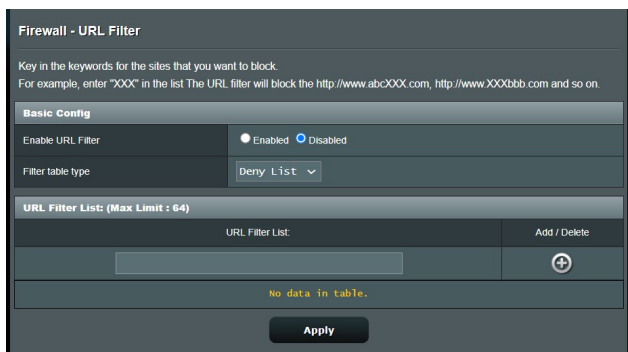
1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Firewall > General**.
2. En el campo **Enable Firewall (Habilitar Firewall)**, seleccione **Yes (Sí)**.

3. En la protección **Enable DoS (Habilitar DdS)**, seleccione **Yes (Sí)** para proteger la red contra ataques DoS (Denial of Service, es decir, denegación de servicio), aunque esto puede afectar al rendimiento del router.
4. También puede supervisar los paquetes intercambiados entre la conexión LAN y WAN. En el campo Logged packets type (Tipo de paquetes registrados), seleccione **Dropped (Caídos)**, **Accepted (Aceptados)** o **Both (Ambos)**.
5. Haga clic en **Apply (Aplicar)**.


3.5.2 Filtro de direcciones URL

Puede especificar palabras claves o direcciones Web para indicar direcciones URL.

NOTA: El filtro de direcciones URL se basa en una consulta DNS. Si el cliente de red ya ha accedido a un sitio Web, como por ejemplo, <http://www.abcxxx.com>, dicho sitio no se bloqueará (una memoria DNS del sistema almacena los sitios Web previamente visitados). Para resolver este problema, borre la memoria DNS antes de configurar el filtro de direcciones URL.

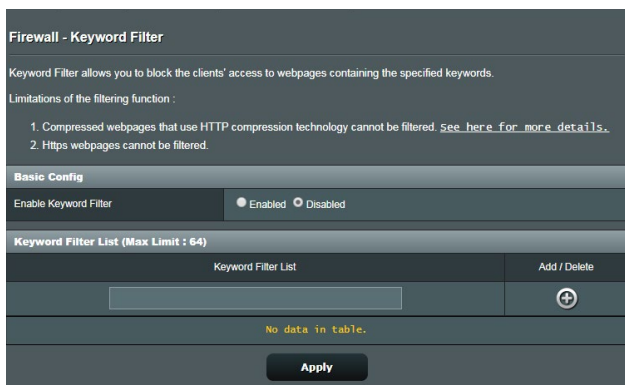


Para configurar un filtro de direcciones URL:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Firewall > URL Filter (Filtro de direcciones URL)**.
2. En el campo Enable URL Filter (Habilitar filtro de direcciones URL), seleccione **Enabled (Habilitado)**.
3. Escriba una dirección URL y haga clic en el botón .
4. Haga clic en **Apply (Aplicar)**.

3.5.3 Filtro de palabras clave

El filtro de palabras clave bloquea el acceso páginas Web que contengan palabras clave específicas.



Para configurar un filtro de palabras clave:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Firewall > Keyword Filter (Filtro de palabras clave)**.
2. En el campo Enable Keyword Filter (Habilitar filtro de palabras clave), seleccione **Enabled (Habilitado)**.
3. Escriba una palabra o frase y haga clic en el botón **Add (Agregar)**.
4. Haga clic en **Apply (Aplicar)**.

NOTAS:

- El filtro de palabras clave se basa en una consulta DNS. Si el cliente de red ya ha accedido a un sitio Web, como por ejemplo, <http://www.abcxxx.com>, dicho sitio no se bloqueará (una memoria DNS del sistema almacena los sitios Web previamente visitados). Para resolver este problema, borre la memoria DNS antes de configurar el filtro de palabras clave.
 - Las páginas Web comprimidas utilizando compresión HTTP no se pueden filtrar. Las páginas HTTPS tampoco se pueden bloquear utilizando un filtro de palabras clave.
-

3.5.4 Filtro de servicios de red

El filtro de servicios de red bloquea los intercambios de paquetes LAN a WAN y restringe a los clientes de red el acceso a servicios Web específicos, como por ejemplo Telnet o FTP.

Firewall - Network Services Filter

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

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

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network

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

Network Services Filter

Enable Network Services Filter Yes No

Filter table type

Well-Known Applications

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


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

Date to Enable LAN to WAN Filter Sat Sun

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

Filtered ICMP packet types


Network Services Filter Table (Max Limit : 32)

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

No data in table.

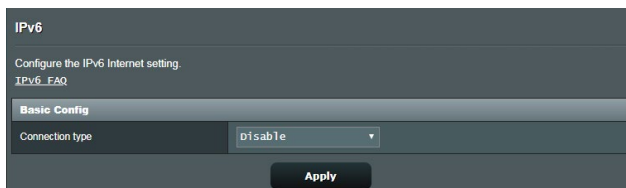
Apply

Para configurar un filtro de servicio de red:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Firewall > Network Service Filter (Filtro de servicios de red)**.
2. En el campo Enable Network Services Filter (Habilitar filtros de servicios de red), seleccione **Yes (Sí)**.
3. Seleccione el tipo de tabla de filtro. **Deny (Rechazar)** bloquea los servicios de red especificados. **Allow (Permitir)** limita el acceso solamente a los servicios de red especificados .
4. Especifique el día y la hora en los que se activarán los filtros.
5. Para especificar un servicio de red para filtrar, especifique la información correspondiente en los siguientes campos: Source IP (Dirección IP de origen), Destination IP (Dirección IP de destino), Port Range (Intervalo de puertos) y Protocol (Protocolo). Haga clic en el botón  .
6. Haga clic en **Apply (Aplicar)**.

3.6 IPv6

Este router inalámbrico es compatible con el direccionamiento IPv6, un sistema que admite más direcciones IP. Este estándar todavía no se utiliza mayoritariamente. Póngase en contacto con su ISP si el servicio de Internet admite IPv6.



Para configurar IPv6:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > IPv6**.
2. Seleccione una opción en **Connection type (Tipo de conexión)**. Las opciones de configuración varían en función del tipo de conexión seleccionado.
3. Especifique la configuración de DNS y LAN IPv6.
4. Haga clic en **Apply (Aplicar)**.

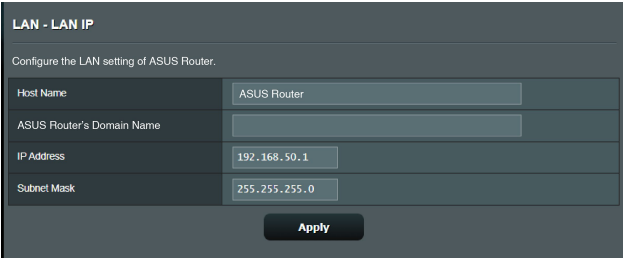
NOTA: Consulte a su ISP para obtener información específica sobre IPv6 para su servicio de Internet.

3.7 LAN

3.7.1 Dirección IP LAN

La pantalla LAN IP (Dirección IP LAN) permite modificar la configuración de dirección IP LAN del router inalámbrico.

NOTA: Todos los cambios en la dirección IP LAN se reflejarán en la configuración DHCP.



The screenshot shows the 'LAN - LAN IP' configuration page. At the top, it says 'Configure the LAN setting of ASUS Router.' Below this, there are four input fields: 'Host Name' with the value 'ASUS Router', 'ASUS Router's Domain Name' (empty), 'IP Address' with the value '192.168.50.1', and 'Subnet Mask' with the value '255.255.255.0'. At the bottom center, there is an 'Apply' button.

Para modificar la configuración de dirección IP LAN:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > LAN > LAN IP (Dirección IP LAN)**.
2. Modifique los campos **IP address (Dirección IP)** y **Subnet Mask (Máscara de subred)**.
3. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

3.7.2 DHCP Server (Servidor DHCP)

El router inalámbrico utiliza DHCP para asignar direcciones IP automáticamente en su red. Puede especificar el intervalo de direcciones IP y el tiempo de arrendamiento para los clientes de la red.

LAN - DHCP Server

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

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

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

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

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

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

Para configurar el servidor DHCP:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > LAN > DHCP Server (Servidor DHCP)**.
2. En el campo **Enable the DHCP Server (Desea habilitar el servidor DHCP)**, active la opción **Yes (Sí)**.
3. En el cuadro de texto **Domain Name (Nombre de dominio)**, especifique un nombre de dominio para el router inalámbrico.

4. En el campo **IP Pool Starting Address (Dirección inicial del conjunto de direcciones IP)**, introduzca la dirección IP inicial.
5. En el campo **IP Pool Ending Address (Dirección final del conjunto de direcciones IP)**, introduzca la dirección IP final.
6. En el campo **Lease Time (Tiempo de arrendamiento)**, escriba cuándo expirarán las direcciones IP y cuándo el router inalámbrico asigna nuevas direcciones IP a los clientes de la red.

NOTAS:

- Le recomendamos utilizar el formato de dirección IP 192.168.50.xxx (donde xxx puede ser cualquier número comprendido entre 2 y 254) cuando se especifique un intervalo de direcciones IP.
 - Una dirección inicial del conjunto de direcciones IP no debe ser mayor que la dirección final del conjunto de direcciones IP.
-
7. En la sección **DNS and WINS Server Settings (Configuración de DNS y WINS de servidor)**, escriba el servidor DNS y la dirección IP del servidor WINS en caso de que sea necesario.
 8. El router inalámbrico también puede asignar direcciones IP manualmente a dispositivos de la red. En el campo **Enable Manual Assignment (Habilitar asignación manual)**, elija **Yes (Sí)** para asignar una dirección IP a direcciones MAC específicas de la red. Se pueden agregar hasta dar 32 direcciones MAC a la lista DHCP para asignación manual.

3.7.3 Ruta

Si la red utiliza más de un router inalámbrico, puede configurar una tabla de enrutamiento para compartir el mismo servicio de internet.

NOTA: Le recomendamos que no cambie la configuración de enrutamiento predeterminada a menos que tenga conocimientos avanzados de tablas de enrutamiento.

LAN - Route

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

Basic Config

Enable static routes Yes No



Static Route List (Max Limit : 32)

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

No data in table.

Apply

Para configurar la tabla de enrutamiento LAN:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > LAN > Route (Ruta)**.
2. En el campo **Enable static routes (Habilitar rutas estáticas)**, elija **Yes (Sí)**.
3. En **Static Route List (Lista de rutas estáticas)**, especifique la información de la red de otros puntos de acceso o nodos. Haga clic en el botón **Add (Agregar)**  o **Delete (Eliminar)**  para agregar un dispositivo a la lista o quitarlo de esta, respectivamente.
4. Haga clic en **Apply (Aplicar)**.

3.7.4 IPTV

El router inalámbrico admite conexión con servicios IPTV a través de un ISP o una LAN. La ficha IPTV proporciona parámetros de configuración necesarios para configurar IPTV, VoIP, multidifusión y UDP para su servicio. Póngase en contacto con su ISP para obtener información específica relacionada con el servicio.

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there is a warning: 'To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.' Below this, the 'LAN Port' section contains two dropdown menus: 'Select ISP Profile' set to 'None' and 'Choose IPTV STB Port' set to 'None'. The 'Special Applications' section contains three settings: 'Use DHCP routes' set to 'Microsoft', 'Enable multicast routing (IGMP Proxy)' set to 'Disable', and 'UDP Proxy (Udpxy)' set to '0'. An 'Apply' button is located at the bottom center of the form.

LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None

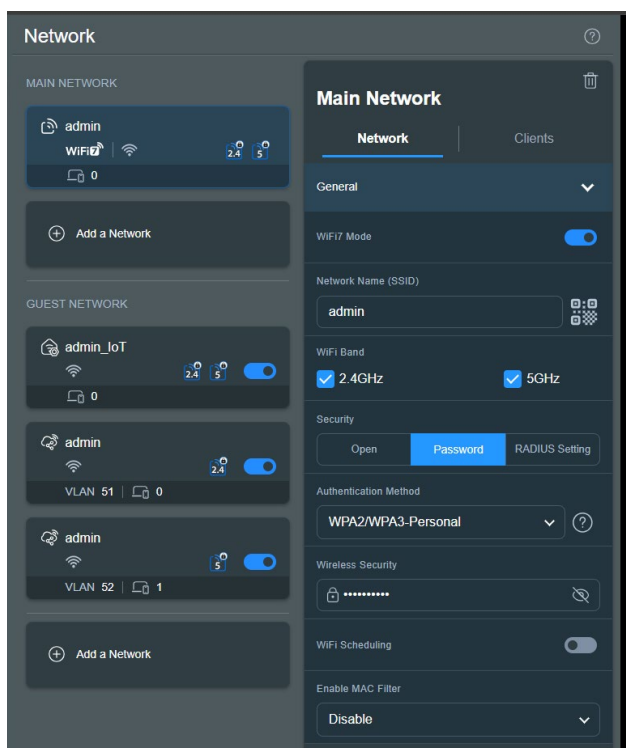
Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
UDP Proxy (Udpxy)	0

Apply

3.8 Red

3.8.1 Red principal - Filtro MAC

El filtro MAC inalámbrico proporciona control sobre los paquetes transmitidos a una dirección MAC (Media Access Control, es decir, Control de acceso al medio) especificada de la red inalámbrica.





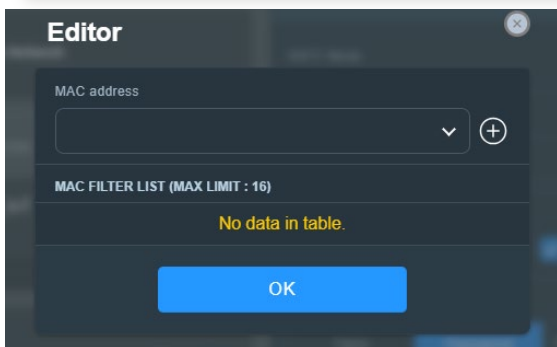
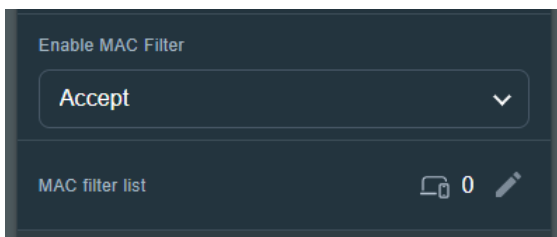
Para configurar el filtro MAC inalámbrico:

1. En el panel de navegación, vaya a **General (General) > Network (Red) > Main Network (Red principal)** y seleccione el nombre de red (SSID) de la red principal.
2. En la lista desplegable **Enable Mac Filter (Habilitar filtro Mac)**, seleccione **Accept (Aceptar)** o **Reject (Rechazar)**.
 - Seleccione **Accept (Aceptar)** para permitir que los dispositivos de la lista de filtros MAC accedan a la red inalámbrica.

- Seleccione **Rejecj (Rechazar)** para impedir que los dispositivos de la lista de filtros MAC accedan a la red inalámbrica.

NOTA: Seleccione **Disable (Deshabilitar)** si desea desactivar **Enable MAC Filter (Habilitar filtro MAC)**.

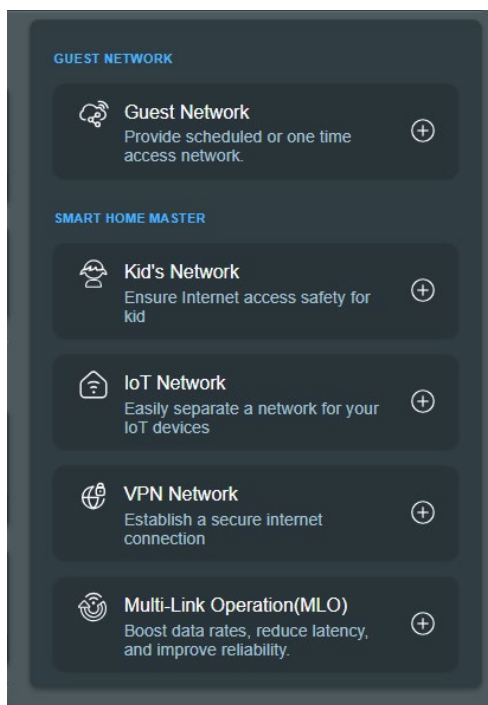
4. En la lista de filtros MAC, haga clic en  para acceder a la página **Editor** y, a continuación, haga clic en  e introduzca la dirección MAC del dispositivo inalámbrico.
5. Haga clic en **OK (Aceptar)**.



3.8.2 Red para invitados

3.8.2.1 Red para invitados

La red para invitados proporciona a los visitantes temporales conectividad a Internet a través de acceso a SSID o redes independientes sin proporcionar acceso a su red privada.



NOTA: ZenWiFi BD4 admite hasta tres SSID en la red de invitados.

Para crear una red para invitados:

1. En el panel de navegación, vaya a **General > Network (Red) > Guest Network (Red para invitados) > Add a Network (Agregar una red)**.
2. Seleccione **Guest Network (Red de invitados)** y asigne un nombre de red para su red temporal en el campo **Network Name (Nombre de red) (SSID)**.
3. Seleccione un método de autenticación en **Security (Seguridad)**.

4. Especifique la hora de acceso o elija **Scheduled (Programado)** para agregar un perfil de programación en línea.
5. Seleccione la **WiFi Band (Banda WiFi)** para la red de invitados que desea crear.
6. Habilite o deshabilite el **Bandwidth Limiter (Limitador de ancho de banda)**.
7. Habilite o deshabilite el **Access Intranet (Acceso a la Intranet)**.
8. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

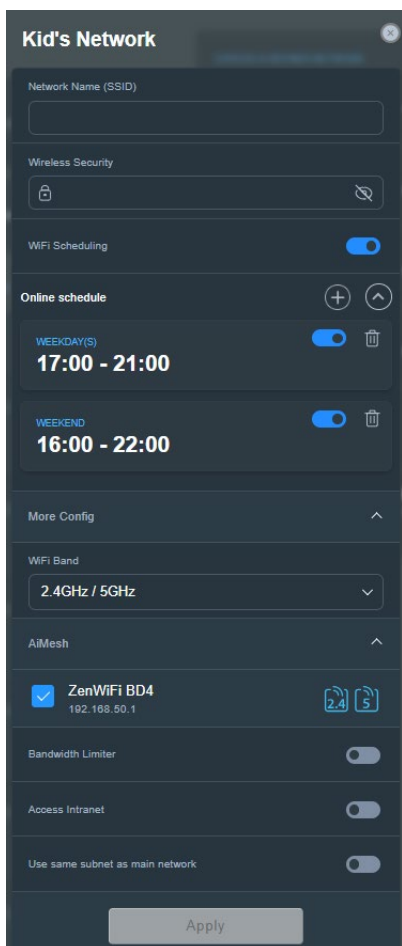
The screenshot shows the 'Guest Network' configuration page. At the top, there is a 'Network Name (SSID)' input field. Below it, the 'Security' section has two options: 'Open' (selected) and 'Password'. The 'WiFi Scheduling' section is enabled with a toggle switch. Underneath, there are two radio buttons: 'Scheduled' and 'One Time Access' (selected). Below these are several buttons for duration: '30 mins', '1 hr(s)', '2 hr(s)' (selected), '4 hr(s)', '6 hr(s)', and 'Custom'. A 'More Config' section is expanded, showing 'WiFi Band' set to '2.4GHz / 5GHz'. The 'AiMesh' section is also expanded, showing 'ZenWiFi BD4' with IP '192.168.50.1' and two mesh icons. At the bottom, there are three toggle switches: 'Bandwidth Limiter' (disabled), 'Access Intranet' (disabled), and 'Use same subnet as main network' (disabled). An 'Apply' button is at the very bottom.

3.8.2.2 Smart Home Master

Smart Home Master es una herramienta poderosa y fácil de usar para la segmentación de redes. Simplifica el proceso de creación y administración de situaciones de subredes avanzadas, como crear un SSID específico para los dispositivos de sus hijos, conectarse a una VPN a través de una subred específica o incluso crear un SSID seguro para todos sus dispositivos IoT.

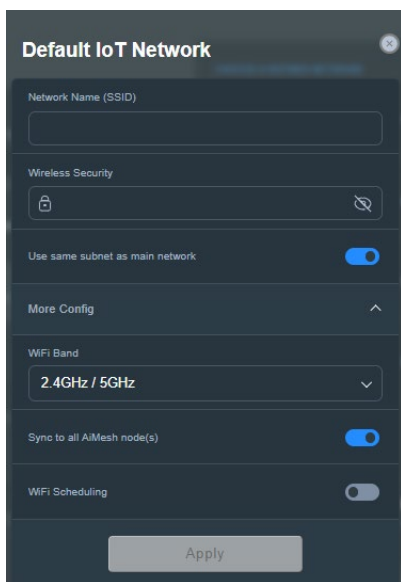
Para crear una red para niños:

1. En el panel de navegación, vaya a **General > Network (Red) > Guest Network (Red para invitados) > Add a Network (Agregar una red)**.
2. Seleccione **Kid's Network (Red para niños)** y asigne un nombre de red y una clave de seguridad en los campos **Network Name (Nombre de red) (SSID)** y **Wireless Security (Seguridad inalámbrica)**.
3. Personalice el tiempo de acceso a Internet en el campo **Online schedule (Horario en línea)**.
4. Seleccione la **WiFi Band (Banda WiFi)** para la red para niños que desea crear.
5. Habilite o deshabilite el **Bandwidth Limiter (Limitador de ancho de banda)**.
6. Habilite o deshabilite el **Access Intranet (Acceso a la Intranet)**.
7. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.



Para crear una red IoT:

1. En el panel de navegación, vaya a **General > Network (Red) > Guest Network (Red para invitados) > Add a Network (Agregar una red)**.
2. Seleccione **IoT Network (Red IoT)** y asigne un nombre de red y una clave de seguridad en los campos **Network Name (Nombre de red) (SSID)** y **Wireless Security (Seguridad inalámbrica)**.
3. Seleccione la **WiFi Band (Banda WiFi)** para la red IoT que desea crear.
4. Personalice el tiempo de acceso a Internet habilitando la **WiFi Scheduling (Programación de WiFi)**.
5. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.



Para crear una red VPN:

1. En el panel de navegación, vaya a **General > Network (Red) > Guest Network (Red para invitados) > Add a Network (Agregar una red)**.
2. Seleccione **VPN Network (Red VPN)** y asigne un nombre de red y una clave de seguridad en los campos **Network Name (Nombre de red) (SSID)** y **Wireless Security (Seguridad inalámbrica)**.
3. Si no ha configurado un perfil VPN para el servidor VPN o el cliente VPN, haga clic en **Go Setting (Ir a configuración)** para crear un perfil VPN.
4. Seleccione la **WiFi Band (Banda WiFi)** para la red VPN que desea crear.
5. Personalice el tiempo de acceso a Internet habilitando la **WiFi Scheduling (Programación de WiFi)**.
6. Habilite o deshabilite el **Bandwidth Limiter (Limitador de ancho de banda)**.
7. Habilite o deshabilite el **Access Intranet (Acceso a la Intranet)**.
8. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.



3.9 Registro del sistema

El registro del sistema contiene las actividades de red grabadas.

NOTA: El registro el sistema se restablece cuando el router se reinicia o apaga.

Para ver el registro del sistema:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > System Log (Registro del sistema)**.
2. Puede ver las actividades de red en cualquiera de estas fichas:
 - Registro general
 - Registro inalámbrico
 - Arrendamientos DHCP
 - IPv6
 - Tabla de enrutamiento
 - Reenvío de puertos
 - Conexiones

System Log - General Log

This page shows the detailed system's activities.

System Time Thu, Aug 23 07:15:34 2018

Uptime 0 days 1 hours 18 minute(s) 11 seconds

Remote Log Server **Apply**

```
Aug 23 06:51:04 miniupnpd[7139]: version 1.9 started
Aug 23 06:51:04 miniupnpd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 miniupnpd[7139]: Listening for NAT-FMP/RCP traffic on port 5351
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_EX_INVALID
Aug 23 07:07:14 rc_service: httpd 1079:notify rc_start_multipath
Aug 23 07:07:14 miniupnpd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 nft: apply nat rules (/tmp/nft_rules_etc0_etc0)
Aug 23 07:07:14 miniupnpd[7688]: version 1.9 started
Aug 23 07:07:14 miniupnpd[7688]: HTTP listening on port 60955
Aug 23 07:07:14 miniupnpd[7688]: Listening for NAT-FMP/RCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 ntp: start NTP update
Aug 23 07:07:15 miniupnpd[7688]: shutting down MiniUPnPd
Aug 23 07:07:15 miniupnpd[7729]: version 1.9 started
Aug 23 07:07:15 miniupnpd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 miniupnpd[7729]: Listening for NAT-FMP/RCP traffic on port 5351
```

Clear **Save**

3.10 Analizador de tráfico

La función de supervisión del tráfico permite acceder al uso del ancho de banda y a la velocidad de Internet o de las redes cableadas e inalámbricas. También permite supervisar el tráfico de red en tiempo real o, incluso, diariamente. También ofrece una opción para mostrar el tráfico de red en las últimas 24 horas.



NOTA: Los paquetes de Internet se transmiten uniformemente a los dispositivos cableados e inalámbricos.

3.11 WAN

3.11.1 Conexión a Internet

La pantalla Internet Connection (Conexión a Internet) permite definir la configuración de varios tipos de conexión WAN.

WAN - Internet Connection

ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of ASUS Router.

Basic Config

WAN Connection Type	Automatic IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). WAN Aggregation FAQ</small>

WAN DNS Setting

DNS Server	Default status: Get the DNS IP from your ISP automatically <small>Assign a DNS service to improve security, block advertisement and gain faster performance.</small>	Assign
Forward local domain queries to upstream DNS	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Enable DNS Rebind protection	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Enable DNSSEC support	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Prevent client auto DoH	Auto	
DNS Privacy Protocol	None	

DHCP Option

Class-Identifier (Option 60)	<input type="text"/>
Client-Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>
Class-Identifier (Option 60)	<input type="text"/>
Client-Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>

Account Settings

Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

Special Requirement from ISP

Host Name	<input type="text"/>
MAC Address	<input type="text"/> MAC Clone
DHCP query frequency	Aggressive Mode
Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

Para definir la configuración de conexión WAN:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN > Internet Connection (Conexión a Internet)**.
2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.
 - **WAN Connection Type (Tipo de conexión WAN):** Elija el tipo de proveedor de servicio de Internet. Las opciones disponibles son las siguientes: **Automatic IP (Dirección IP automática)**, **PPPoE**, **PPTP**, **L2TP** o **fixed IP (Dirección IP fija)**. Si el router no es capaz de obtener una dirección IP válida o si usted no está seguro del tipo de conexión WAN, consulte a su ISP.
 - **Enable WAN (Habilitar WAN):** Seleccione **Yes (Sí)** para permitir el acceso a Internet del router. Seleccione **No** para deshabilitar el acceso a Internet.
 - **Enable NAT (Habilitar NAT):** NAT (Network Address Translation, es decir, Conversión de direcciones de red) es un sistema en el que una dirección IP pública (IP WAN) se utiliza para proporcionar acceso a Internet a clientes de red con una dirección IP privada en una LAN. La dirección IP privada de cada cliente de red se guarda en una tabla NAT y se utiliza para enrutar paquetes de datos entrantes.
 - **Enable UPnP (Habilitar UPnP):** UPnP (Universal Plug and Play, es decir, Conectar y listo universal) permite que varios dispositivos (como por ejemplo enrutadores, televisores, sistemas estéreo, consolas de juego y teléfonos móviles), se controlen a través de una red basada en IP con o sin un centro de control a través de una puerta de enlace. UPnP conecta PC de cualquier tipo de factor de forma, lo cual proporciona una red homogénea para configuración y transferencia de datos remotas. Mediante UPnP, un dispositivo de red se detecta automáticamente. Una vez conectados a la red, los dispositivos se pueden configurar de forma remota para que admitan

aplicaciones P2P, juegos interactivos, videoconferencias y servidores Web o proxy. A diferencia del reenvío de puertos, que implica la configuración manual de los puertos, UPnP configura automáticamente el router para aceptar conexiones entrantes y dirigir solicitudes a un PC específico de la red local.

- **Enable WAN Aggregation (Habilitar la agregación WAN):** La agregación WAN combina dos conexiones de red para aumentar la velocidad WAN hasta 2 Gbps. Conecte el puerto WAN del router y el puerto LAN 4 a los puertos LAN del módem.
- **Connect to DNS Server (Conectar con servidor DNS):** Permite a este router obtener la dirección IP DNS de su ISP automáticamente. Un DNS es un sistema central de Internet que convierte los nombres de Internet en direcciones IP numéricas.
- **Authentication (Autenticación):** Este elemento puede ser especificado por algunos ISP. Consulte a su ISP y rellene esta información si es necesario.
- **Host Name (Nombre de sistema central):** Este campo permite proporcionar un nombre de sistema central para el router. Normalmente es un requisito especial de su ISP. Si su ISP asignó un nombre de equipo central a su PC, especifíquelo aquí.
- **MAC Address (Dirección MAC):** La dirección (Media Access Control, es decir, control de acceso al medio) es un identificador único para el dispositivo de red. Algunos ISP supervisan la dirección MAC de los dispositivos de red que se conectan a su servicio y rechazan cualquier dispositivo no reconocido que intente conectarse. Para evitar problemas de conexión debido a una dirección MAC no registrada, puede:
 - Ponerse en contacto con su ISP y actualizar la dirección MAC asociada con su servicios de ISP.
 - Clonar o cambiar la dirección MAC del router inalámbrico de ASUS para que coincida con la dirección MAC del dispositivo de red anterior reconocido por el ISP.

3.11.2 Dual WAN (WAN dual)

Dual WAN (WAN dual) le permite seleccionar dos conexiones ISP con el router, una WAN principal y una WAN secundaria.

Para configurar Dual WAN (WAN dual):

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN**.
2. Vaya al campo **Dual WAN (WAN dual)** y seleccione **ON (ACTIVAR)**.
3. Elija un valor en **Primary WAN (WAN principal)** y **Secondary WAN (WAN secundario)**. Hay dos opciones de WAN/LAN de 2.5GbE para su elección.
4. Elija **Fail Over (Conmutación por error)** o **Load Balance (Equilibrio de carga)**.
5. Haga clic en **Apply (Aplicar)**.

NOTA: Las explicaciones detalladas están disponibles en las preguntas más frecuentes del sitio de soporte de ASUS:
<https://www.asus.com/support/FAQ/1011719>.

The screenshot shows the 'WAN - Dual WAN' configuration page. At the top, there is a title 'WAN - Dual WAN' and a descriptive paragraph: 'ZenWiFi BD4 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)'. Below this is a 'Basic Config' section with two rows: 'Enable Dual WAN' with a toggle switch set to 'OFF', and 'Primary WAN' with a dropdown menu showing 'WAN'. The next section is 'Auto Network Detection', which includes a note: 'Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.' This section contains three rows: 'Detect Interval' with a value of '3' seconds, 'Internet Connection Diagnosis' with a value of '2' continuous times, and 'Network Monitoring' with radio buttons for 'DNS Query' and 'Ping'. At the bottom of the form is an 'Apply' button.

3.11.3 Activador de puerto

La activación de intervalos de puertos abre un puerto entrante predeterminado durante un período limitado de tiempo siempre que un cliente de la red de área local cree una conexión saliente a un puerto especificado. La activación de puertos se utiliza los siguientes escenarios:

- Varios clientes locales necesitan reenvío de puertos para la misma aplicación en un momento diferente.
- Una aplicación requiere que puertos entrantes específicos sean en diferentes de los puertos salientes.

WAN - Port Trigger

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

Basic Config

Enable Port Trigger Yes No

Well-Known Applications

Trigger Port List (Max Limit : 32)

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

Apply

Para configurar el activación de puerto:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN > Port Trigger (Activador de puerto)**.
2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.
 - **Enable Port Trigger (Habilitar la activador de puerto):** Elija **Yes (SÍ)** para habilitar el activador de puerto.
 - **Well-Known Applications (Aplicaciones conocidas):** Seleccione los juegos y servicios Web más utilizados para agregar a la lista de activación de puertos.
 - **Description (Descripción):** Especifique un nombre corto o una descripción para el servicio.

- **Trigger Port (Puerto disparador):** Especifique un puerto de activador para abrir el puerto entrante.
- **Protocol (Protocolo):** Seleccione el protocolo TCP o UDP.
- **Incoming Port (Puerto entrante):** Especifique un puerto de entrada para recibir datos entrantes de Internet.

NOTAS:

- Cuando se establece conexión con un servidor IRC, un equipo cliente crea una conexión saliente mediante el intervalo de puertos de activación 66660-7000. El servidor IRC responde comprobando el nombre de usuario y creando una nueva conexión con el equipo cliente mediante un puerto entrante.
 - Si la opción Port Trigger (Activador de puerto) se deshabilita, el router no lleva a cabo la conexión porque no es capaz de determinar qué equipo está solicitando acceso IRC. Cuando la opción Port Trigger (Activador de puerto) se habilita, el router asigna un puerto de entrada para recibir los datos entrantes. Este puerto de entrada se cierra cuando ha transcurrido un período de tiempo específico porque el router no está seguro de cuándo ha terminado la aplicación.
 - La activación de puertos solamente permite a un cliente de la red utilizar un servicio determinado y un puerto entrante específico simultáneamente.
 - No puede utilizar la misma aplicación para activar un puerto en varios equipos simultáneamente. El router solamente volverá a reenviar al último equipo para enviar una solicitud o activación al router.
-

3.11.4 Servidores virtuales/Reenvío de puertos

El reenvío de puertos es un método para dirigir el tráfico de red desde Internet a un puerto específico o desde un intervalo de puertos específico a un dispositivo o número de dispositivos de una red local. La configuración del reenvío de puertos en el router permite a los equipos que se encuentran fuera de la red acceder a servicios específicos proporcionados por un equipo que se encuentra dentro de dicha red.

NOTA: Cuando el reenvío de puertos está habilitado, el router de ASUS bloquea el tráfico entrante no solicitado de Internet y solamente permite respuestas desde solicitudes salientes de la LAN. El cliente de red no tiene acceso a Internet directamente y viceversa.

WAN - Virtual Server / Port Forwarding

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

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

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with ASUS Server's web user interface.
- When you set 20.21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with ASUS Server's native FTP server.

Virtual_Server / Port_Forwarding_E60

Basic Config

Enable Port Forwarding OFF

Port Forwarding List (Max Limit : 64)

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

Add profile

Para configurar el reenvío de puertos:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN > Virtual Server / Port Forwarding (Servidor virtual/Reenvío de puertos).**

2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **ON (ACTIVAR)**.
 - **Enable Port Forwarding (Habilitar reenvío de puertos):** Elija **ON (ACTIVAR)** para habilitar el enrutamiento de puertos.
 - **Famous Server List (Lista de servidores famosos):** Determine a qué tipo de servicio desea acceder.
 - **Famous Game List (Lista de juegos famosos):** Este elemento muestra los puertos necesarios para que los juegos en línea más utilizados funcionen correctamente.
 - **FTP Server Port (Puerto del servidor FTP):** Evite asignar el intervalo de puertos 20:21 para el servidor FTP ya que se entraría en conflicto con la asignación del servidor FTP nativo del router.
 - **Service Name (Nombre de servicio):** Especifique un nombre de servicio.
 - **Port Range (Intervalo de puertos):** Si desea especificar el intervalo de puertos para los clientes de la misma red, especifique la información correspondiente en los campos Service Name (Nombre de servicio), Port Range (Intervalo de puertos) (por ejemplo 10200:10300), LAN IP address (Dirección IP LAN) y deje el campo Local Port (Puerto local) vacío. El intervalo de puertos admite diversos formatos, como por ejemplo intervalos propiamente dichos (300:350), puertos individuales (566,789) o una mezcla de ambos (1015:1024,3021).

NOTAS:

- Cuando el firewall de la red está deshabilitado y establece 80 como el intervalo de puertos del servidor HTTP para la configuración de la red WAN, el servidor http/web entra en conflicto con la interfaz Web del usuario del router.
- Una red utiliza los puertos para intercambiar datos, de forma que a cada puerto se le asigna un número de puerto y una tarea específica. Por ejemplo, el puerto 80 se utiliza para HTTP. Un puerto específico solamente se puede utilizar por una aplicación o servicio al mismo tiempo. Por tanto, cuando dos equipos intentan acceder a datos a través del mismo puerto y al mismo tiempo, se produce un error. Por ejemplo, no puede configurar el reenvío de puertos para el puerto 100 para dos equipos simultáneamente.

- **Local IP (Dirección IP local):** Escriba la dirección IP LAN del cliente.
-

NOTA: Utilice una dirección IP estática para el cliente local para que el reenvío de puertos funciona correctamente. Consulte la sección **3.8 LAN** para obtener información.

- **Local Port (Puerto local):** Escriba un puerto específico para recibir los paquetes de reenviados. Deje este campo en blanco si desea que los paquetes entrantes se redirijan al intervalo de puertos especificado.
- **Protocol (Protocolo):** Seleccione el protocolo. Si no está seguro, elija **BOTH (AMBOS)**.

Para comprobar si el reenvío de puertos se ha configurado correctamente:

- Asegúrese de que el servidor o la aplicación está configurada y funcionando.
- Necesitará un cliente fuera de la red LAN pero con acceso a Internet (en lo sucesivo lo denominaremos "Cliente con Internet"). El cliente no debe estar conectado al router ASUS.
- En el cliente con Internet, utilice la dirección IP WAN del router para acceder al servicio. Si el reenvío de puertos se ha realizado correctamente, debe poder acceder a los archivos o a las aplicaciones.

Diferencias entre la activación de puertos y el reenvío de puertos:

- La activación de puertos funcionará aunque no se haya configurado una dirección IP LAN específica. A diferencia del reenvío de puertos, que requiere una dirección IP LAN estática, la activación de puertos permite el reenvío dinámico de puertos mediante el router. Los intervalos de puertos predeterminados se configuran para aceptar conexiones entrantes durante un período limitado de tiempo. La activación de puertos permite que varios equipos ejecuten aplicaciones que normalmente requerirían el reenvío manual de los mismos puertos a cada equipo de la red.
- La activación de puertos es más segura que el reenvío de puertos porque los puertos entrantes no permanecen abiertos durante todo el tiempo. Solamente se abren cuando una aplicación está estableciendo una conexión saliente a través del puerto de activación.

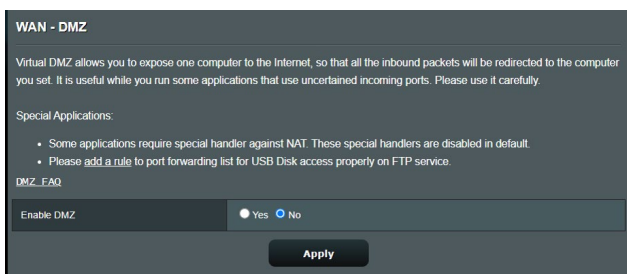
3.11.5 DMZ

DMZ virtual expone un cliente a Internet, permitiendo a dicho cliente recibir todos los paquetes entrantes dirigidos a la red de área local.

El tráfico entrante procedente de Internet se suele descartar y enrutar a un cliente específico solamente si el reenvío de puertos o un activador de puertos se ha configurado en la red. En una configuración DMZ, un cliente recibe todos los paquetes entrantes.

La configuración de DMZ en una red resulta de gran utilidad cuando necesita abrir puertos entrantes o desea hospedar un servidor de dominio, Web o de correo electrónico.

PRECAUCIÓN: La apertura de todos los puertos de un cliente a Internet hace que la red sea vulnerable a ataques externos. Sea consciente de los riesgos de seguridad que implica utilizar DMZ.



Para configurar DMZ:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN > DMZ**.
2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.
 - **IP address of Exposed Station (Dirección IP de la estación expuesta):** Escriba la dirección IP LAN del cliente que proporcionará el servicio DMZ y que se expondrá en Internet. Asegúrese de que el servidor tiene una dirección IP estática.

Para quitar DMZ:

1. Elimine la dirección IP LAN del cliente del cuadro de texto **IP Address of Exposed Station (Dirección IP de la estación expuesta)**.
2. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

3.11.6 DDNS

La configuración de DDNS (Dynamic DNS, es decir, DNS dinámico) permite acceder al router desde fuera de la red a través del servicio DDNS de ASUS o de otro servicio DDNS.

The screenshot shows the 'WAN - DDNS' configuration page. It includes a title bar, a descriptive paragraph about DDNS, a warning about private WAN IP addresses, and a table for configuration options. The 'Enable the DDNS Client' option is selected as 'Yes'. The 'Server' is set to 'www.asus.com' with a 'Deregister' button. The 'Host Name' is 'A8B78A175D4A6FD54D2E6BD6195D85EF7.asuscomm.com'. The 'DDNS Status' is 'Active' and the 'Registration Result' is 'Registration is successful'. The 'HTTPS/SSL Certificate' section has three radio buttons: 'Free Certificate from Let's Encrypt', 'Import Your Own Certificate', and 'None', with 'None' selected. An 'Apply' button is at the bottom.

WAN - DDNS	
<p>DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.</p> <p>If you cannot use ASUS DDNS services, please go to https://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.</p> <p>The wireless router currently uses a private WAN IP address. This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.</p> <p>The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network. Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network. If you want to remotely configure the wireless router, go to here.</p>	
Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.asus.com <input type="button" value="Deregister"/>
Host Name	A8B78A175D4A6FD54D2E6BD6195D85EF7.asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None
<input type="button" value="Apply"/>	

Para configurar DDNS:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > WAN > DDNS**.
2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.
 - **Enable the DDNS Client (Habilitar el cliente DDNS):** Habilite DDNS para acceder al router de ASUS a través del nombre DNS en lugar de la dirección IP WAN.
 - **Server and Host Name (Nombre de servidor y de sistema central):** Elija DDNS de ASUS u otro DDNS. Si desea utilizar DDNS de ASUS, rellene el campo Host Name (Nombre de sistema central) con el formato xxx.asuscomm.com (donde xxx es el nombre del sistema central).

- Si desea utilizar un servicio DDNS diferente, haga clic en FREE TRIAL (PRUEBA GRATUITA) y regístrese en línea primero. Rellene los siguientes campos: User Name or E-mail Address (Nombre de usuario o dirección de correo electrónico) y Password or DDNS key (Contraseña o clave DDNS).
- **Enable wildcard (Habilitar comodín):** Habilite el comodín si el servicio DDNS lo requiere.

NOTAS:

En el servicio DDNS no funcionará en estas condiciones:

- Cuando el router inalámbrico esté utilizando una dirección IP WAN privada (192.168.x.x, 10.x.x.x o 172.16.x.x) tal y como se indica mediante un texto amarillo.
 - El router puede estar en una red que utiliza varias tablas NAT.
-

3.11.7 Paso a través NAT

Paso a través NAT permite a una conexión de redes privadas virtuales (VPN) atravesar el router hasta los clientes de la red. Las opciones PPTP Passthrough (Paso a través PPTP), L2TP Passthrough (Paso a través L2TP), IPsec Passthrough (Paso a través IPsec) RTSP Passthrough (Paso a través RTSP) están habilitadas de forma predeterminada.

Para habilitar o deshabilitar la configuración de paso a través NAT, vaya a **Advanced Settings (Configuración avanzada) > WAN > NAT Passthrough (Paso a través NAT)**. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

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

Apply

3.12 Inalámbrico

3.12.1 WPS

WPS (Wi-Fi Protected Setup, es decir, Configuración protegida Wi-Fi) es un estándar de seguridad inalámbrica que permite conectar fácilmente dispositivos a una red inalámbrica. Puede configurar la función WPS mediante el código PIN o el botón WPS.

NOTA: Asegúrese de que los dispositivos admiten WPS.

Wireless - WPS

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

Enable WPS	<input checked="" type="checkbox"/>
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled <input type="button" value="Reset"/> Pressing the reset button resets the network name (SSID) and WPA encryption key
AP PIN Code	<input type="text" value="51246044"/>

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

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

WPS Method: Push button Client PIN Code

Para habilitar WPS en la red inalámbrica:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Wireless (Inalámbrico) > WPS**.
2. En el campo **Enable WPS (Habilitar WPS)**, mueva el control deslizante a **ON (ACTIVAR)**.
3. De forma predeterminada, WPS utiliza 2.4 GHz. Si desea cambiar la frecuencia a 5 GHz, seleccione **OFF (DESACTIVAR)** para la función WPS, haga clic en **Switch Frequency (Cambiar frecuencia)** en el campo **Current Frequency (Frecuencia actual)** y vuelva a seleccionar **ON (ACTIVAR)** para WPS.

NOTA: WPS admite la autenticación con las opciones Open System (Sistema abierto), WPA-Personal y WPA2-Personal. WPS no admite redes inalámbricas que utilicen los métodos de cifrado Shared Key (Clave compartida), WPA-Enterprise (WPA-Empresarial), WPA2-Enterprise (WPA2-Empresarial) y RADIUS.

4. En el campo WPS Method (Método WPS), seleccione **Push Button (Pulsador)** o **Client PIN Code (Código PIN de cliente)**. Si selecciona **Push Button (Pulsador)**, vaya al paso 5. Si selecciona el **Client PIN Code (Código PIN de cliente)**, vaya al paso 6.
5. Para configurar WPS utilizando el botón WPS del router, siga estos pasos:
 - a. Haga clic en **Start (Inicio)** o presione el botón WPS que se encuentra en la parte posterior de router inalámbrico.
 - b. Presione el botón WPS del dispositivo inalámbrico. Se suele identificar por el logotipo WPS.

NOTA: Compruebe el dispositivo inalámbrico o su manual de usuario para conocer la ubicación del botón WPS.

- c. El router inalámbrico buscará todos los dispositivos WPS disponibles. Si el router inalámbrico no encuentra ningún dispositivo WPS, cambiará al modo de espera.
6. Para configurar WPS utilizando el código PIN del cliente, siga estos pasos:
 - a. Busque el código PIN WPS en el manual de usuario del dispositivo inalámbrico o en el propio dispositivo.
 - b. Escriba el código PIN del cliente en el cuadro de texto.
 - c. Haga clic en **Start (Inicio)** para activar el modo de inspección WPS en el router inalámbrico. Los indicadores LED del router parpadearán rápidamente tres veces hasta que la configuración WPS se complete.

3.12.2 Puente

La función Bridge (Puente) o WDS (Wireless Distribution System, es decir, Sistema de distribución inalámbrico) permite al router inalámbrico de ASUS conectarse a otro punto de acceso inalámbrico exclusivamente, lo que impide que otros dispositivos o estaciones inalámbricas accedan a dicho router. También se puede considerar como un repetidor inalámbrico en el que el router inalámbrico de ASUS se comunica con otro punto de acceso y otros dispositivos inalámbricos.

Wireless - Bridge

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

Note:

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

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

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

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

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

Basic Config

2.4 GHz MAC	<input type="text" value="c8:7f:54:12:69:c8"/>
5 GHz MAC	<input type="text" value="c8:7f:54:12:69:cc"/>
Band	2.4 GHz ▾
AP Mode	AP Only ▾
Connect to APs in list	<input type="radio"/> Yes <input checked="" type="radio"/> No

Remote AP List (Max Limit : 4)

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

Para configurar el puente inalámbrico:


1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Wireless (Inalámbrico) > WDS**.
2. Seleccione la banda de frecuencia para el puente inalámbrico.
3. En el campo **AP Mode (Modo PA)**, seleccione cualquiera de estas opciones.
 - **AP Only (Solo PA):** Deshabilita la función de puente inalámbrico.

- **WDS Only (Solo WDS):** Habilita la función de puente inalámbrico pero impide que otros dispositivos o estaciones inalámbricas se conecten al router.
- **HYBRID (HÍBRIDO):** Habilita la función de puente inalámbrico y permite que otros dispositivos o estaciones inalámbricas se conecten al router.

NOTA: En el modo Hybrid (Híbrido), los dispositivos inalámbricos conectados al router inalámbrico de ASUS solo recibirán la mitad de la velocidad de conexión del punto de acceso.

4. En el campo **Connect to APs in list (Conectarse a PA de la lista)**, haga clic en **Yes (Sí)** si desea conectarse a un punto de acceso que se encuentra en Remote AP List (Lista de PA remotos).
5. En el campo **Control Channel (Canal de control)**, seleccione el canal operativo para el puente inalámbrico. Seleccione **Auto (Automático)** para permitir que el router seleccione automáticamente el canal que tenga la menor cantidad de interferencias.

NOTA: La disponibilidad de los canales varía en función del país o región.

6. En **Remote AP List (Lista de PA remotos)**, escriba una dirección MAC y haga clic en el botón **Add (Agregar)**  para entrar en la dirección MAC de otros puntos de acceso disponibles.

NOTA: Cualquier punto de acceso agregado a la lista debe estar en el mismo canal de control que el router inalámbricos de ASUS.

7. Haga clic en **Apply (Aplicar)**.

3.12.3 Configuración de RADIUS

La configuración RADIUS (Remote Authentication Dial In User Service) proporciona un nivel adicional de seguridad cuando se eligen los modos de autenticación WPA-Enterprise (WPA-Empresarial), WPA2-Enterprise (WPA2-Empresarial) o Radius with 802.1x (Radius con 802.1x).

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

Para definir la configuración de RADIUS inalámbrica:

1. Asegúrese de que el modo autenticación del router inalámbrico se establece en WPA-Enterprise (WPA-Empresarial), WPA2-Enterprise (WPA2-Empresarial) o Radius with 802.1x (Radius con 802.1x).
2. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada) > Wireless (Inalámbrico) > ficha RADIUS Setting (Configuración de RADIUS)**.
3. Seleccione la banda de frecuencia.
4. En el campo **Server IP Address (Dirección IP del servidor)**, escriba la dirección IP del servidor RADIUS.
5. En el campo **Connection Secret (Secreto de conexión)**, asigne la contraseña para acceder al servidor RADIUS.
6. Haga clic en **Apply (Aplicar)**.

3.12.4 Professional

La pantalla Professional (Profesional) proporciona opciones de configuración avanzada.

NOTA: Le recomendamos utilizar los valores predeterminados de esta página.

Wireless - Professional	
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.	
Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
Set AP Isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No
Roaming assistant	Enable Disconnect clients with RSSI lower than: -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="range"/> Performance
Apply	

En la pantalla **Professional Settings (Configuración personal)**, puede definir lo siguiente:

- **Band (Banda):** Seleccione la banda de frecuencia que se aplicará a la configuración profesional.
- **Enable Radio (Habilitar radio):** Seleccione **Yes (Sí)** para habilitar la conexión de red inalámbrica. Seleccione **No** para deshabilitar la conexión de red inalámbrica.

- **Enable wireless scheduler (Habilitar programador inalámbrico):** Puede elegir un formato de reloj de 24 o 12 horas. El color de la tabla indica Permitir o Rechazar. Haga clic en el marco para cambiar la configuración de la hora de los días laborables y, a continuación, haga clic en **OK (Aceptar)** cuando finalice.

Wireless - Professional

* Reminder: The System time zone is different from your locale setting.

Clock Format: 24-hour ▾ Allow Deny

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **Set AP isolated (Establecer PA aislado):** El elemento Set AP Isolated (Establecer PA aislado) impide que los dispositivos inalámbricos de la red se comuniquen entre sí. Esta función es útil si hay muchos invitados que se unan a la red y la abandonen con frecuencia. Seleccione **Yes (Sí)** para habilitar esta función o **No** para deshabilitarla.
- **Multicast rate (Mbps) (Tasa de multidifusión (Mbps)):** Seleccione la tasa de transmisión de multidifusión o haga clic en **Disable (Deshabilitar)** para desactivar la transmisión única simultánea.

- **Preamble Type (Tipo de preámbulo):** Esta opción define la longitud de tiempo que el router emplea para la comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check). CRC es un método que detecta errores durante la transmisión de datos. Seleccione **Short (Corto)** para una red inalámbrica ocupada con mucho tráfico de red. Seleccione **Long (Largo)** si la red inalámbrica está compuesta de dispositivos inalámbricos más antiguos.
- **RTS Threshold (Umbral RTS):** Seleccione un valor más pequeño para el umbral RTS (Request to Send, es decir, Solicitud para enviar) para mejorar la comunicación inalámbrica en una red inalámbrica ocupada o con mucho ruido que tenga mucho tráfico de red y numerosos dispositivos inalámbricos.
- **DTIM Interval (Intervalo DTIM):** El intervalo DTIM (Delivery Traffic Indication Message) o tasa de señalización de datos, es el período de tiempo antes del cual una señal se envía a un dispositivo inalámbrico que se encuentra en modo de suspensión para indicar que un paquete de datos está esperando a ser entregado. El valor predeterminado es tres milisegundos.
- **Beacon Interval (Intervalo de señalización):** El intervalo de señalización es el tiempo entre un DTIM y el siguiente. El valor predeterminado es 100 milisegundos. Reduzca el valor del intervalo de señalización para una conexión inalámbrica inestable o para dispositivos en itinerancia.
- **Enable TX Bursting (Habilitar ráfaga de transmisión):** Esta opción mejora la velocidad de transmisión entre el router inalámbrico y los dispositivos 802.11g.
- **Enable WMM APSD (Habilitar WMM APSD):** Habilite esta opción (WMM APSD, Wi-Fi Multimedia Automatic Power Save Delivery) para mejorar la administración de energía entre dispositivos inalámbricos. Seleccione **Disable (Deshabilitar)** Para desactivar WMM APSD.

4 Uso de las utilidades

4.1 Detección de dispositivos

Device Discovery (Detección de dispositivos) es una utilidad ASUS WLAN que detecta routers inalámbricos ASUS y permite definir la configuración de red inalámbrica.

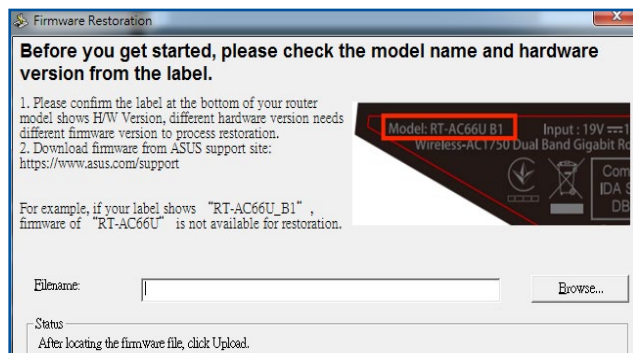
Para abrir la utilidad Device Discovery (Detección de dispositivos):

- Desde el escritorio de su equipo, haga clic en **Start (Inicio) > All Programs (Todos los programas) > ASUS Utility (Utilidad ASUS) > Router inalámbrico ASUS > Device Discovery (Detección de dispositivos)**.

NOTA: Cuando establezca el router en el modo de punto de acceso, necesitará utilizar la detección de dispositivos para obtener la dirección IP de la router.

4.2 Restauración de firmware

La restauración de firmware se utiliza en un router inalámbrico de ASUS que falló durante su proceso de actualización de firmware. El dispositivo carga el firmware que usted especifique.



¡IMPORTANTE! Inicie el modo de rescate antes de usar la utilidad de restauración de firmware.

NOTA: Esta función no se admite en MAC OS.

Para iniciar el modo de rescate y usar la utilidad de restauración de firmware:

1. Desenchufe el router inalámbrico de la fuente de alimentación.
2. Mantenga presionado el botón Restablecer situado en el panel posterior mientras vuelve a enchufar el router inalámbrico en la fuente de alimentación. Suelte el botón Restablecer cuando el LED de alimentación situado en el panel frontal parpadee lentamente, lo que indica que el router inalámbrico se encuentra en el modo de rescate.
3. Establezca una dirección IP estática en el equipo y utilice lo siguiente para definir la configuración TCP/IP:

IP address (Dirección IP): 192.168.1.x

Subnet mask (Máscara de subred): 255.255.255.0

4. En el escritorio del equipo, haga clic en **Start (Inicio) > All Programs (Todos los programas) > ASUS Utility (ASUS Utility) > Wireless Router (Router inalámbrico) > Firmware Restoration (Restauración del firmware)**.
5. Especifique un archivo de firmware y haga clic en **Upload (Cargar)**.

NOTA: Esta no es una utilidad de actualización de firmware y no se puede utilizar en un router inalámbrico de ASUS de trabajo. Las actualizaciones normales de firmware se deben realizar a través de la interfaz Web. Consulte el **Capítulo 3: Definición de la configuración general y avanzada** para obtener más detalles.

5 Resolución de problemas

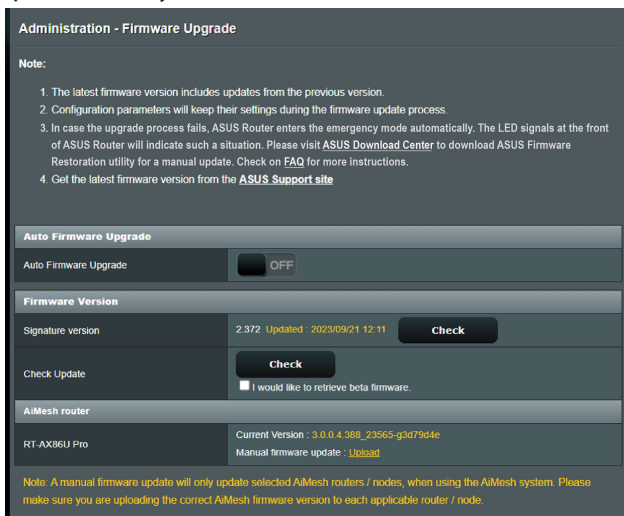
En este capítulo se proporcionan soluciones para problemas que puede tener con el router. Si tiene problemas que no se mencionan en este capítulo, visite el sitio de soporte técnico de ASUS en: <https://www.asus.com/support> para obtener más información del producto y detalles de contacto del Servicio de soporte técnico de ASUS.

5.1 Soluciones básicas de problemas

Si tiene problemas con el router, intente llevar a cabo los pasos básicos de esta sección antes de buscar otras soluciones.

Actualizar el firmware a la versión más reciente.

1. Inicie la GUI Web. Vaya a **Advanced Settings (Configuración avanzada) > Administration (Administración) > Firmware Upgrade (Actualizar firmware)**. Haga clic en **Check (Comprobar)** para ver si hay una versión de firmware más reciente disponible.



2. Si hay una versión de firmware más reciente disponible, visite el sitio Web global de ASUS en <https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/> para descargarla.
3. En la página **Firmware Version (Versión de firmware)**, haga clic en **Check (Comprobar)** para buscar el archivo de firmware.
4. Haga clic en **Upload (Cargar)** para actualizar el firmware.

Reinicie la red siguiendo la siguiente secuencia:

1. Apague el módem.
2. Desenchufe el módem.
3. Apague el router y los equipos.
4. Enchufe el módem.
5. Encienda el módem y, a continuación, espere 2 minutos.
6. Encienda el router y, a continuación, espere 2 minutos.
7. Encienda los equipos.

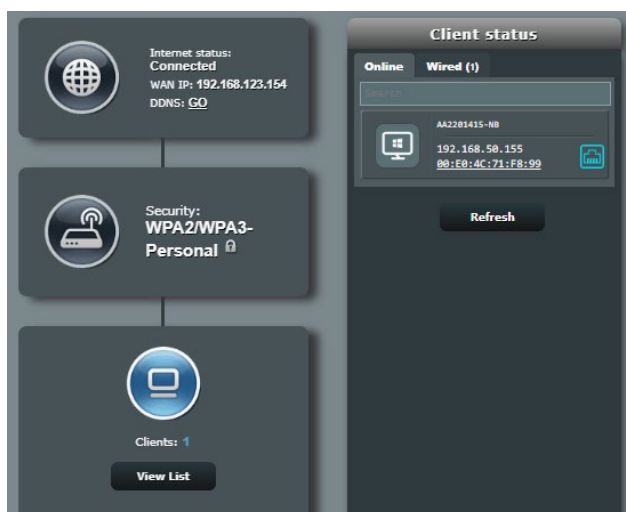
Compruebe si la configuración inalámbrica del equipo coincide con la de su router.

- Cuando conecte el equipo al router de forma inalámbrica, asegúrese de que el SSID (nombre de red inalámbrica), el método de cifrado y la contraseña son correctos.

Compruebe si la configuración de red es correcta.

- Cada cliente de la red debe tener una dirección IP válida. ASUS recomienda utilizar el servidor DHCP del router inalámbrico para asignar direcciones IP a los equipos de la red.

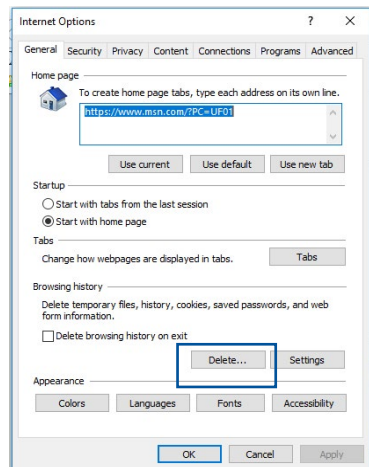
- Algunos proveedores de servicio de módem de cable exigen el uso de la dirección MAC del equipo inicialmente registrado en la cuenta. Puede ver la dirección MAC en la GUI Web, **Network Map (Mapa de red)** > página **Clients (Clientes)** y mantener el cursor del ratón sobre el dispositivo en **Client status (Estado del cliente)**.



5.2 Preguntas más frecuentes (P+F)

No puedo acceder a la GUI del router mediante un explorador Web

- El equipo está conectado mediante un cable. Compruebe la conexión del cable Ethernet y el estado del LED tal y como se describió en la sección anterior.
- Asegúrese de que utiliza la información de inicio de sesión correcta. Asegúrese de que la tecla Bloq Mayús está deshabilitada al introducir la información de inicio de sesión.
- Elimine las cookies y los archivos del explorador Web. Para Internet Explorer, siga estos pasos:
 1. Inicie Internet Explorer y, a continuación, haga clic en **Tools (Herramientas) > Internet Options (Opciones de internet)**.
 2. En la ficha **General**, bajo **Browsing history (Historial de exploración)**, haga clic en **Delete... (Eliminar...)**, seleccione **Temporary Internet Files and website files (Archivos temporales de Internet y archivos de sitio web)** y **Cookies and website data (Cookies y datos del sitio web)**, a continuación, haga clic en **Delete (Eliminar)**.



NOTAS:

- Los comandos para eliminar cookies y archivos varían en función de los exploradores Web.
- Deshabilite la configuración del servidor proxy, cancele la conexión de acceso telefónico a redes y establezca la configuración TCP/IP para obtener la dirección IP automáticamente. Para obtener más detalles, consulte el capítulo 1 de este manual del usuario.
- Asegúrese de que utiliza cables Ethernet CAT5e o CAT6.

El cliente no puede establecer una conexión inalámbrica con el router.

NOTA: Si tiene problemas al conectarse a una red de 5 GHz, asegúrese de que el dispositivo inalámbrico admite 5 GHz o tiene funcionalidades de banda dual.

- **Se encuentra fuera del alcance de la red:**
 - Coloque el router más cerca del cliente inalámbrico.
- **El servidor DHCP se ha deshabilitado:**
 1. Inicie la GUI Web. Vaya a **General > Network Map (Mapa de red) > Clients (Clientes)** y busque el dispositivo que desee conectar al router.
 2. Si no puede encontrar el dispositivo en **Network Map (Mapa de red)**, vaya a **Advanced Settings (Configuración avanzada) > LAN > DHCP Server (Servidor DHCP)**, lista **Basic Config (Configuración básica)**, seleccione **Yes (Sí)** en **Enable the DHCP Server (Habilitar el servidor DHCP)**.

LAN - DHCP Server

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

Basic Config

Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
ASUS Router's Domain Name	<input type="text"/>
IP Pool Starting Address	<input type="text" value="192.168.50.2"/>
IP Pool Ending Address	<input type="text" value="192.168.50.254"/>
Lease time	<input type="text" value="86400"/>
Default Gateway	<input type="text"/>

DNS and WINS Server Setting

DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>
Advertise router's IP in addition to user-specified DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WINS Server	<input type="text"/>

Manual Assignment

Enable Manual Assignment	<input type="radio"/> Yes <input checked="" type="radio"/> No
--------------------------	---

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

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

No data in table.

- El SSID se ha ocultado. Si el dispositivo no puede encontrar SSID de otros enrutadores ni tampoco el SSID de su router, vaya a **Advanced Settings (Configuración avanzada) > Wireless (Inalámbrico) > General**, seleccione **No** en **Hide SSID (Ocultar)** y seleccione **Auto (Automático)** en **Control Channel (Canal de control)**.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4 GHz
Network Name (SSID)	LIÃO
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input type="checkbox"/> big Protection <input type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ</small>
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto <small>Current Control Channel: 5</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** Weak
Group Key Rotation Interval	3600

Apply

- Si está utilizando un adaptador LAN inalámbrico, compruebe si el canal inalámbrico en uso es conforme a los canales disponibles en su país o área. Si no lo es, ajuste el canal, el ancho de banda y el modo inalámbrico.
- Si sigue sin poder conectarse al router de forma inalámbrica, puede restablecer la configuración predeterminada de fábrica de dicho router. En la GUI del router, haga clic en **Administration (Administración) > Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**.

Administration - Restore/Save/Upload Setting

This function allows you to save current settings of ASUS Router to a file, or load settings from a file.

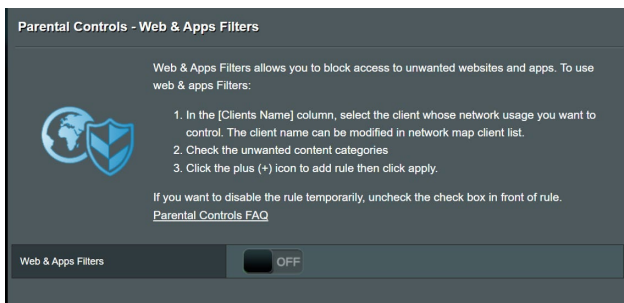
Factory default	Restore <input type="checkbox"/> Initialize all the settings, and clear all the data log for AIProtection, Traffic Analyzer, and Web History.
Save setting	Save setting <input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router. <input type="checkbox"/> Transfer ASUS DDNS name
Restore setting	Upload

No es posible acceder a Internet.

- Compruebe si el router se puede conectar a la dirección IP WAN de su ISP. Para ello, inicie la GUI Web y vaya a **General > Network Map (Mapa de red)** y compruebe **Internet Status (Estado de Internet)**.
- Si el router no se puede conectar a la dirección IP WAN de su ISP, intente reiniciar la red tal y como se describe en el apartado **Restart your network in following sequence (Reinicie la red siguiendo la siguiente secuencia)** de la sección **Basic Troubleshooting (Soluciones básicas de problemas)**.



- El dispositivo se ha bloqueado a través de la función Parental Control (Control parental). Vaya a **General > Parental Controls (Control parental)** y vea si el dispositivo se encuentra en la lista. El dispositivo se encuentra en **Client Name (Nombre del cliente)**, quítelo mediante el botón **Delete (Eliminar)** o ajuste la configuración de administración de tiempo.



- Si todavía no tiene acceso a Internet, intente reiniciar el equipo y compruebe la dirección IP y la dirección de la puerta de enlace de la red.

Olvidó el SSID (nombre de red) o la contraseña de red

- Configure un nuevo SSID y una nueva clave de cifrado mediante la conexión cableada (cable Ethernet). Inicie la GUI Web, vaya a **Network Map (Mapa de red)**, haga clic en el icono de router, especifique un nuevo SSID y una nueva clave de cifrado y, a continuación, haga clic en **Apply (Aplicar)**.
- Restablezca la configuración predeterminada del router. Inicie la GUI Web, haga clic en **Administration (Administración) > Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**.

¿Cómo restaurar el sistema a su configuración predeterminada?

- Vaya a **Administration (Administración) > Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**.

Error al actualizar el firmware.

Inicie el modo de rescate y ejecute la utilidad de restauración del firmware. Consulte la sección **4.2 Restauración del firmware** para obtener información sobre cómo emplear la utilidad de restauración del firmware.

No se puede acceder a la interfaz gráfica de usuario Web

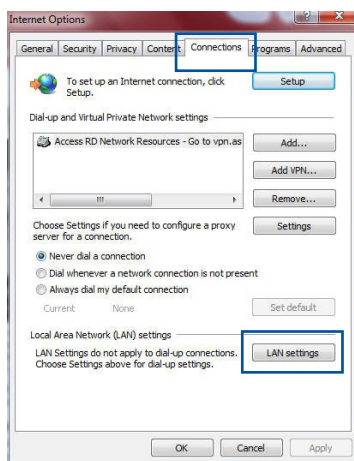
Antes de configurar el router inalámbrico, lleve a cabo los pasos descritos en esta sección para el equipo principal y los clientes de red.

A. Deshabilite el servidor proxy si se encuentra habilitado.

Windows®

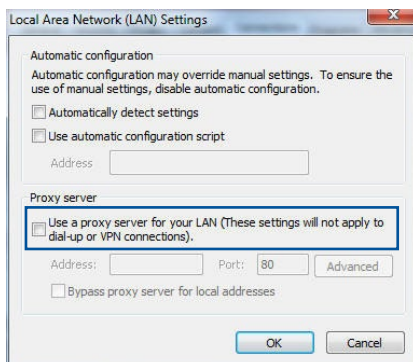
1. Haga clic en **Start (Inicio)** > **Internet Explorer** para iniciar el explorador web.

2. Haga clic en **Tools (Herramientas)** > **Internet options (Opciones de Internet)** > **Connections (Conexiones)** > **LAN settings (Configuración de LAN)**.



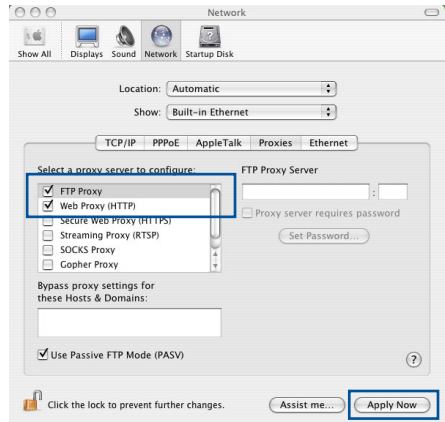
3. En la pantalla Local Area Network (LAN) Settings (Configuración de la red de área local (LAN)), desactive la opción **Use a proxy server for your LAN (Usar un servidor proxy para la LAN)**.

4. Haga clic en **OK (Aceptar)** cuando haya terminado.



MAC OS

1. En el explorador Safari, haga clic en **Safari** > **Preferences...** (**Preferencias...**) > **Advanced (Avanzado)** > **Change Settings...** (**Cambiar ajustes...**).
2. En la pantalla Network (Red), anule la selección de los elementos **FTP Proxy (Proxy de FTP)** y **Web Proxy (HTTP) (Proxy de web (HTTP))**.
3. Haga clic en **Apply Now (Aplicar ahora)** cuando termine.

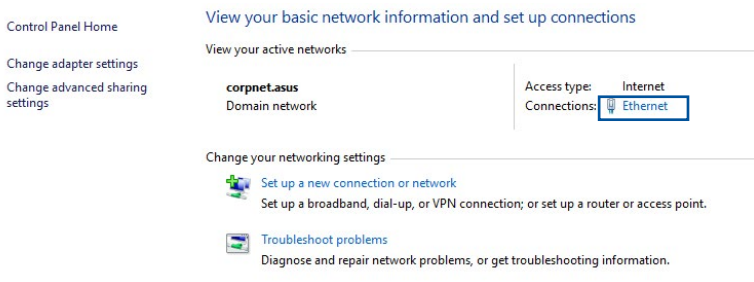


NOTA: Consulte la función de ayuda del explorador para obtener detalles sobre cómo deshabilitar el servidor proxy.

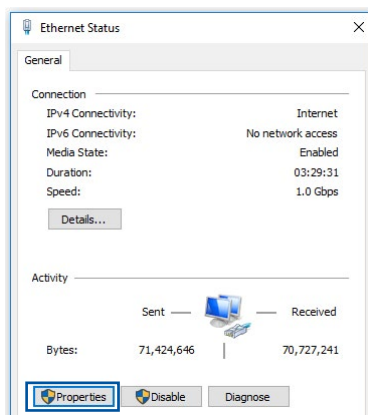
B. Establezca la configuración TCP/IP del equipo para que reciba una dirección IP automáticamente.

Windows®

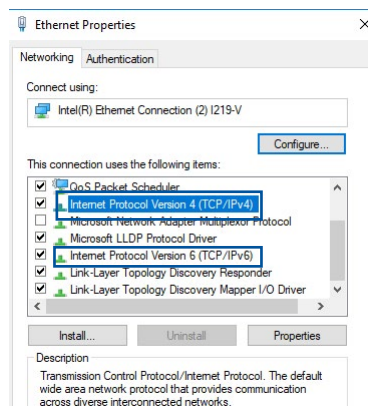
1. Haga clic en **Start (Inicio)** > **Control Panel (Panel de control)** > **Network and Sharing Center (Centro de redes y de recursos compartidos)**, luego haga clic en la conexión de red para mostrar su ventana de estado.



- Haga clic en **Properties (Propiedades)** para mostrar la ventana Ethernet Properties (Propiedades de Ethernet).



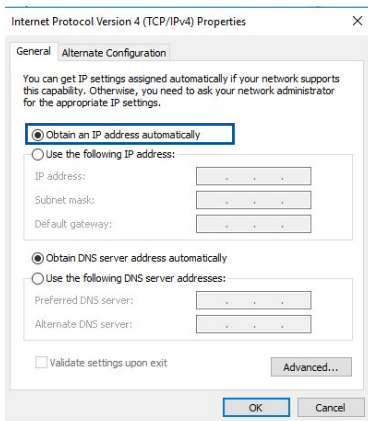
- Seleccione **Internet Protocol Version 4 (TCP/IPv4) (Protocolo de Internet versión 4 (TCP/IPv4) (Propiedades))** o **Internet Protocol Version 6 (Protocolo de Internet versión 6 (TCP/IPv6))**, y haga clic en **Properties**.




- Active la opción **Obtain an IP address automatically (Obtener una dirección IP automáticamente)**.

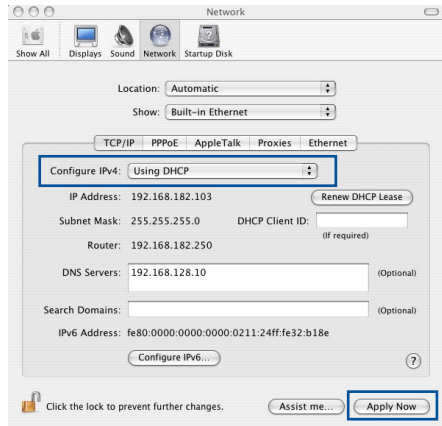
Para tener la configuración IPv6 IP automáticamente el, active la opción **Obtain an IPv6 address automatically (Obtener una dirección IPv6 automáticamente)**.

- Haga clic en **OK (Aceptar)** cuando haya terminado.



MAC OS

1. Haga clic en el icono de Apple  situado en la esquina superior izquierda de la pantalla.
2. Haga clic en **System Preferences (Preferencias del Sistema) > Network (Red) > Configure... (Configurar...)**.
3. En la ficha **TCP/IP**, seleccione **Using DHCP (Usar DHCP)** en la lista desplegable **Configure IPv4 (Configurar IPv4)**.
4. Haga clic en **Apply Now (Aplicar ahora)** cuando termine.

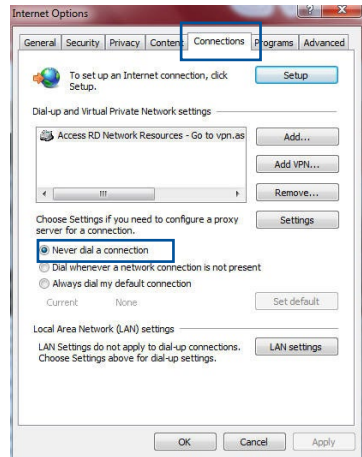


NOTA: Consulte el material de ayuda y soporte técnico de su sistema operativo si desea obtener más información acerca de la configuración de los protocolos TCP/IP.

C. Deshabilite todas las conexiones de acceso telefónico, si hay alguna habilitada.

Windows®

1. Haga clic en **Start (Inicio) > Internet Explorer** para iniciar el explorador web.
2. Haga clic en **Tools (Herramientas) > Internet options (Opciones de Internet) > Connections (Conexiones)**.
3. Active la opción **Never dial a connection (No marcar nunca una conexión)**.
4. Haga clic en **OK (Aceptar)** cuando haya terminado.



NOTA: Consulte la ayuda del explorador si desea obtener información acerca de cómo deshabilitar las conexiones de acceso telefónico.

Apéndices

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 seguridad

Cuando utilice este producto, siga siempre las precauciones de seguridad fundamentales, incluidas, entre otras, las siguientes:



¡ADVERTENCIA!

- Los cables de alimentación se deben enchufar a tomas de corriente que estén provistas de una conexión a tierra adecuada. Conecte el equipo solamente a una toma de corriente cercana y de fácil acceso.
 - No intente reparar la fuente de alimentación personalmente si se avería. Póngase en contacto con un técnico de mantenimiento autorizado o con su distribuidor.
 - NO cubra los orificios de ventilación del equipo de sobremesa para evitar que el sistema se caliente en exceso.
 - NO monte este equipo a una altura superior a 2 metros.
 - Use este producto en entornos sometidos a una temperatura ambiente comprendida entre 0 °C (32 °F) y 40 °C (104 °F).
 - Lea las pautas de funcionamiento y el intervalo de temperatura proporcionado antes de utilizar el producto.
 - Preste especial atención a la seguridad personal cuando utilice este dispositivo en aeropuertos, hospitales, estaciones de servicio y garajes profesionales.
 - Interferencias de productos sanitarios: Para reducir el riesgo de interferencias, mantenga una distancia mínima de al menos 15 cm (6 pulgadas) entre los productos sanitarios implantados y los productos ASUS.
 - Para minimizar el nivel de radiación, utilice los productos ASUS de manera que las condiciones de recepción sean buenas .
 - Mantenga el dispositivo alejado de mujeres embarazadas y de la parte inferior del abdomen de los adolescentes.
 - NO utilice este producto si se observan defectos visibles o si se ha mojado, dañado o modificado. Solicite asistencia al servicio técnico.
-



¡ADVERTENCIA!

- NO coloque el equipo sobre una superficie irregular o inestable.
 - NO coloque objetos sobre la tableta ni los deje caer sobre ella. Evite exponer el producto a impactos mecánicos, como aplastamiento, flexión, perforación o trituración.
 - NO desmonte, abra, caliente en microondas, incinere ni pinte este producto; tampoco ni introduzca objetos extraños en él.
 - Consulte la etiqueta de valores nominales situada en la parte inferior del producto y asegúrese de que su adaptador de alimentación cumple con dichos valores.
 - Mantenga el producto alejado de fuentes de incendio y calor.
 - NO exponga el equipo a líquidos, lluvia o humedad, ni lo use cerca de ninguno de tales elementos. NO use el producto durante tormentas eléctricas.
 - Conecte los circuitos de salida PoE de este producto exclusivamente a redes PoE, sin enrutarlos a instalaciones externas.
 - A fin de evitar posibles descargas eléctricas, desconecte el cable de alimentación de la toma de suministro eléctrico antes de cambiar la posición del sistema.
 - Utilice únicamente accesorios que hayan sido aprobados por el fabricante del dispositivo para funcionar con este modelo. El uso de otros tipos de accesorios puede anular la garantía o infringir normas y leyes locales, así como presentar riesgos de seguridad. Póngase en contacto con su distribuidor local para conocer la disponibilidad de accesorios autorizados.
 - El uso de este producto de una manera no recomendada en las instrucciones proporcionadas puede generar riesgo de incendio o lesiones personales.
-

Servicio y Soporte

Visite nuestro sitio web en varios idiomas en <https://www.asus.com/support/>.

