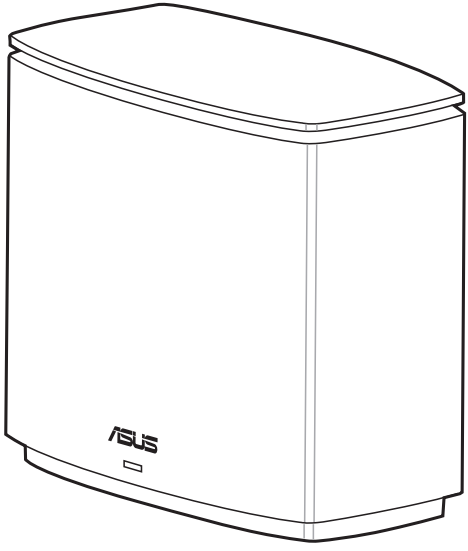
User Guide

ZenWiFi Hybrid

MoCA Mesh Router

Model: XC5



IN SEARCH OF INCREDIBLE

E22780
First Edition
October 2023

Table of contents

Table of contents

Table of contents

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS ZenWiFi XC5 Hybrid Wireless Router!

1.2 Package contents

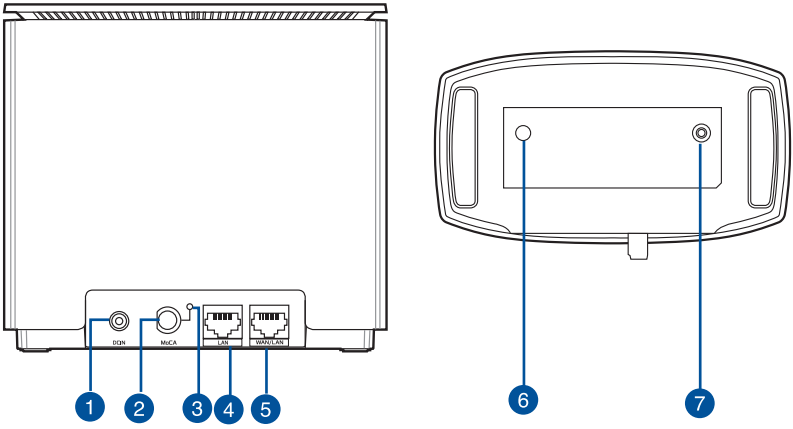
☑ ZenWiFi XC5 Hybrid Wireless Router
☑ Network cable (RJ-45)
☑ Power cable
☑ Quick Start Guide
☑ Warranty card

NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support. Refer to the ASUS Support Hotline list at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your wireless router

ASUS ZenWiFi Hybrid Overview



1	**Power (DC-IN) port** Insert the bundled AC adapter into this port and connect your router to a power source.
2	**MoCA port** Connect a coaxial cable into this port to establish MoCA connection.
3	**MoCA link LED** **Solid white**: MoCA network is connected. **Blinking white**: Transmitting or receiving data via MoCA connection
4	**LAN port** Connect a network cable into this port to establish LAN connection.
5	**WAN / LAN port** Connect your modem to this port with a network cable.
6	**MPS/WPS combo button** Press this button to start WPS or MPS MoCA pairing. **WPS pairing**: Press the button on XC5 and a new wireless client to establish Wi-Fi connection. **MPS pairing (add a new XC5)**: Press the button on XC5 in the existing Mesh System first and then press the MPS button on the new XC5 mesh router. After a short time, the new XC5 will be integrated into your existing Mesh System. **MPS pairing (add a new MoCA device)**: Press the button on XC5 in the existing Mesh System first and then press the MPS button on the new MoCA device. After a short time, the new MoCA device will be integrated into your existing MoCA network.
7	**Reset button**: Press this button to reset or restore the system to its factory settings.

Specifications

DC Power adapter	DC Output: +12V with max 1.5A current		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

ZenWiFi Hybrid LED indications

Solid blue
Your ZenWiFi XC5 is ready for setup.

Solid white
Your ZenWiFi XC5 is online and works well.

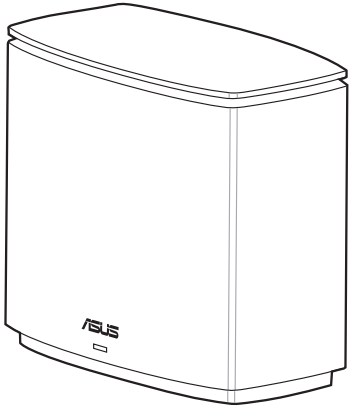
Solid yellow
The signal between your ZenWiFi XC5 router and the node is weak.

Solid red
Your ZenWiFi XC5 router has no Internet connection.
Your ZenWiFi XC5 node is disconnected from the router.

1.4 Positioning your router

For the best wireless signal transmission between the wireless router and the network devices connected to it, ensure that you:

- Place the wireless router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- Keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at **http://www.asus.com** to get the latest firmware updates.



1.5 Setup Requirements

To set up your wireless network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/ 1000BaseTX)
- IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

NOTES:

- If your computer does not have built-in wireless capabilities, you may install an IEEE 802.11a/b/g/n/ac/ax WLAN adapter to your computer to connect to the network.
- With its dual band technology, your wireless router supports 2.4GHz and 5GHz wireless signals simultaneously. This allows you to do Internet-related activities such as Internet surfing or reading/writing e-mail messages using the 2.4GHz band while simultaneously streaming high-definition audio/video files such as movies or music using the 5GHz band.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

1.6 Router Setup

IMPORTANT!

- Use a wired connection when setting up your wireless router to avoid possible setup problems.
- Before setting up your ASUS wireless router, do the following:
  - If you are replacing an existing router, disconnect it from your network.
  - Disconnect the cables/wires from your existing modem setup. If your modem has a backup battery, remove it as well.
  - Reboot your cable modem and computer (recommended).

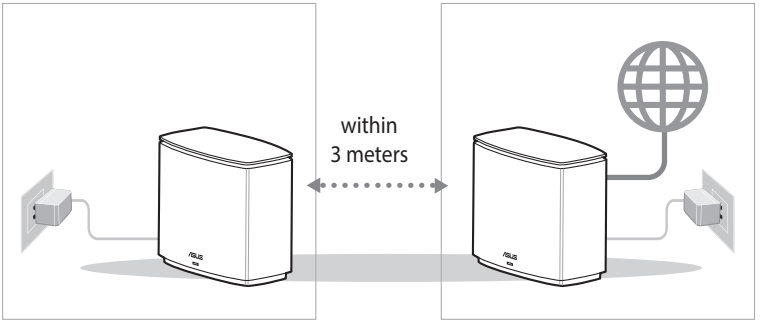
AiMesh Router Setup Steps

01 Prepare

Place your ZenWiFi XC5 router and node within 3 meters of each other during the setup process.

02 AiMesh node

Keep your AiMesh node powered on and standby for AiMesh system settings.

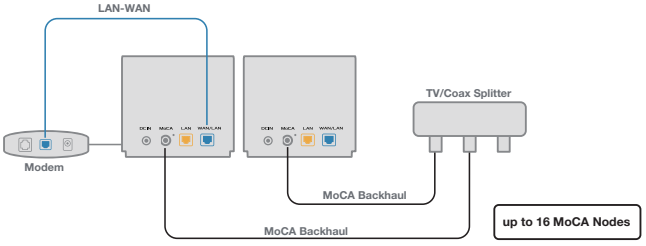


03 Launching ASUS Router APP

Launch ASUS Router APP, and then follow the on-screen instructions to finish the AiMesh setup.

Relocation

Locate the AiMesh router and node close to your existing coaxial port.



NOTES:

- For better transmission quality, ensure that you use RG6 coaxial cables in the network environment.
- The operating frequency range of MoCA 2.5 is 1,125MHz ~ 1,675MHz. Since some splitters may not be able to work properly (e.g., abnormal transmission) within the range, please make sure that the operating frequency of the splitter you use in the network matches that of MOCA 2.5.
- To minimize Wi-Fi interference, keep the routers away from devices like cordless phones, Bluetooth devices and microwave ovens.

2 Getting started

2.1 Installing ASUS Router App

Download free ASUS Router app to set up and manage your router(s).

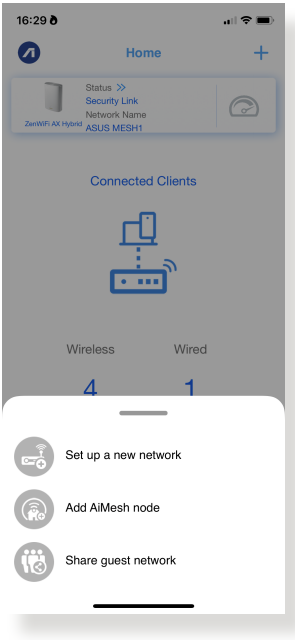
ASUS Router

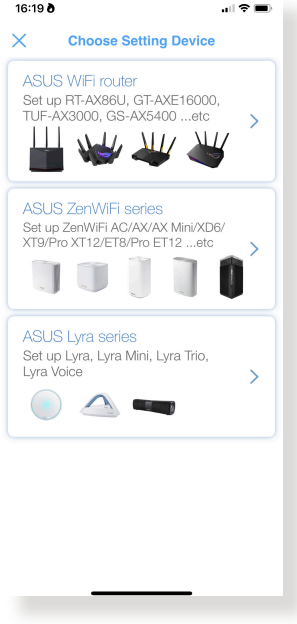
GET IT ON Google Play

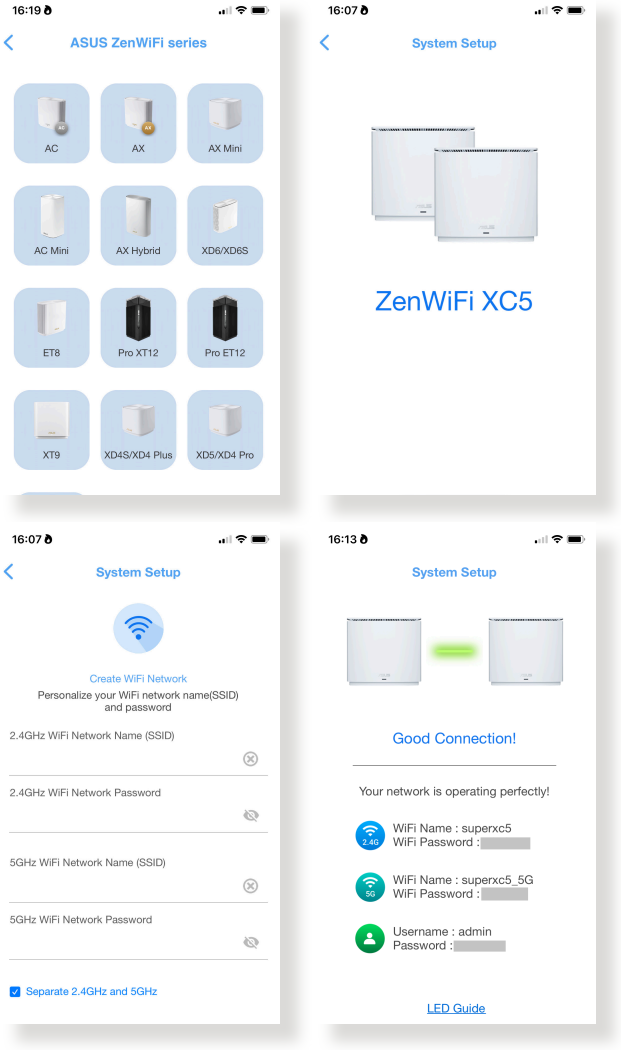
Download on the App Store

2.1.1 Quick Internet Setup (QIS) with ASUS Router App

Open the ASUS Router app and follow the on-screen instructions to set up your network.





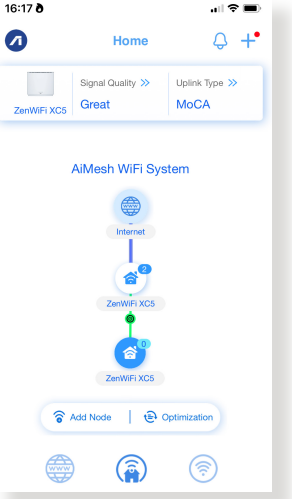


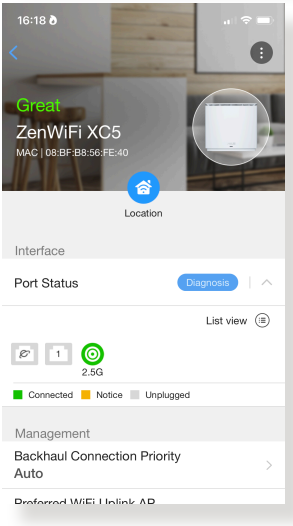
NOTES:

- If you have trouble finding your routers, ensure that the router and node are far enough away from each other.
- When setting up the SSID, you can select **Separate 2.4GHz and 5GHz** to assign different SSIDs for your wireless bands.

To ensure that your router and node have been set up properly, in the ASUS Router app, go to **Home** and check the network connection between the router and the node.

- A green bar between the two nodes indicates strong signal strength;
- Tap the node to check the signal strength or connection quality.





After the node has connected, the router LED indicator may turn green, indicating that the router is performing backend optimizations. At this time, devices can connect to the network, but performance may be limited. We recommend waiting to perform tests until the router LED indicator turns white.

You can go to the router's web GUI for additional configurations if necessary. Refer to the following pages for details.

2.2 Logging into the Web GUI

Your ASUS Wireless Router comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Internet Explorer, Firefox, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

1. On your web browser, enter http://www.asusrouter.com.
2. On the login page, key in the default user name (**admin**) and password (**admin**).
3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.

NOTE: If you are logging into the Web GUI for the first time, you will be directed to the Quick Internet Setup (QIS) page automatically.

2.2.1 Quick Internet Setup (QIS) with Web GUI

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

NOTE: When setting the Internet connection for the first time, press the Reset button on your wireless router to reset it to its factory default settings.

To use QIS with auto-detection:

1. Log into the Web GUI. The QIS page launches automatically.

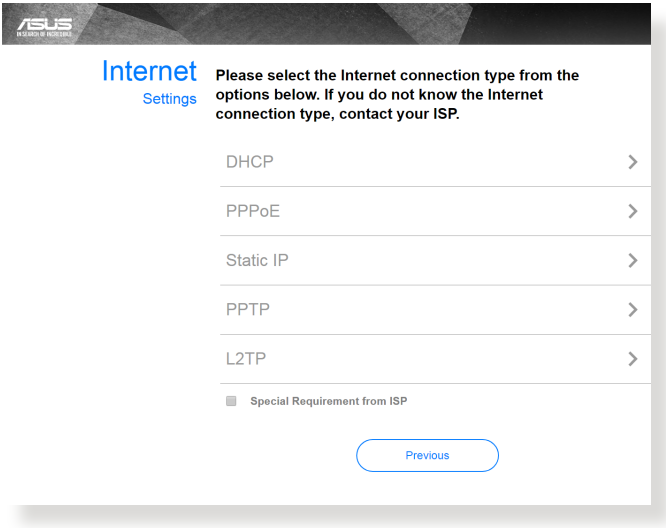
NOTES:

- For details on changing your wireless router's login username and password, refer to section **4.6.2 System**.
- The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

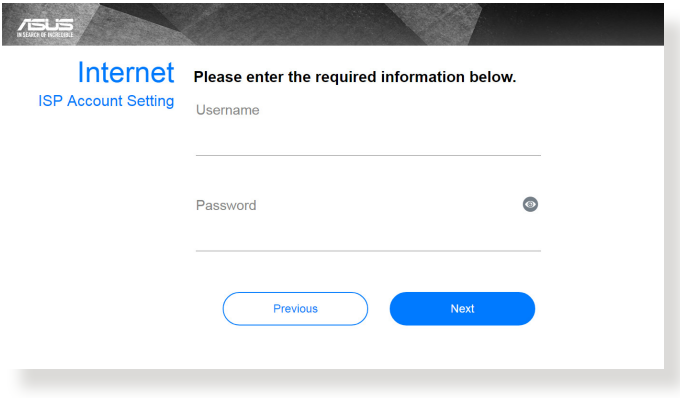
2. The wireless router automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP**, **L2TP**, and **Static IP**. Key in the necessary information for your ISP connection type.

IMPORTANT! Obtain the necessary information from your ISP about the Internet connection type.

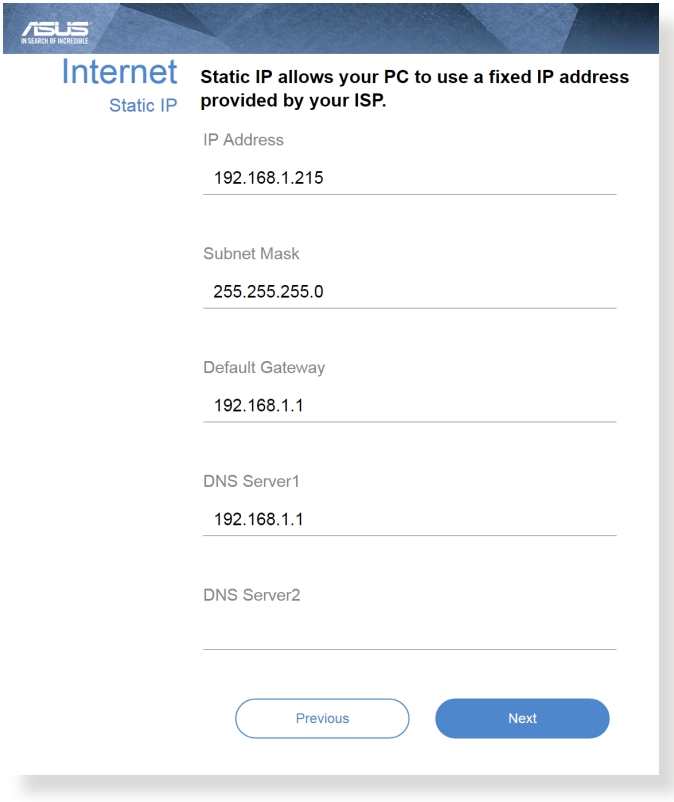
for Automatic IP (DHCP)



for PPPoE, PPTP, and L2TP



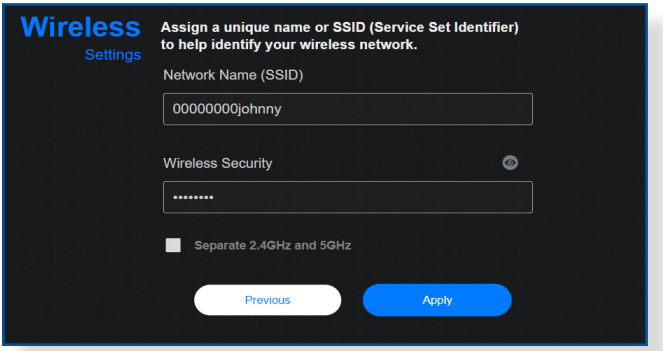
for Static IP



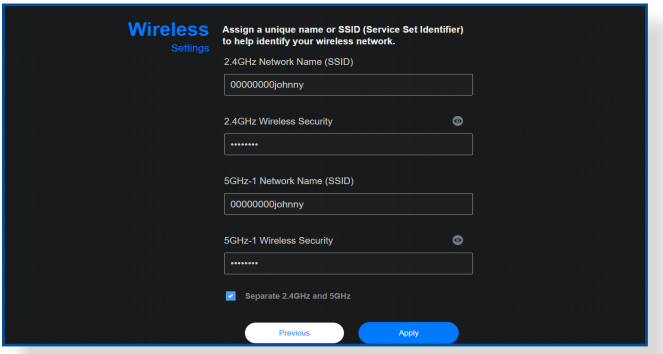
NOTES:

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.

3. Assign the wireless network name (SSID) and security key for your 2.4 GHz and 5 GHz wireless connection. Click **Apply** when done.



NOTE: If you want to assign different SSIDs for your 2.4 GHz and 5 GHz wireless connection, tick **Separate 2.4GHz and 5 GHz**.



2.3 Connecting to your wireless network

After setting up your wireless router via QIS, you can connect your computer or other smart devices to your wireless network.

To connect to your network:

1. On your computer, click the network icon  in the notification area to display the available wireless networks.
2. Select the wireless network that you want to connect to, then click **Connect**.
3. You may need to key in the network security key for a secured wireless network, then click **OK**.
4. Wait while your computer establishes connection to the wireless network successfully. The connection status is displayed and the network icon displays the connected  status.

NOTES:

- Refer to the next chapters for more details on configuring your wireless network's settings.
- Refer to your device's user manual for more details on connecting it to your wireless network.

3 Configuring the General settings

3.1 Using the Network Map

Network Map allows you to configure your network's security settings and manage your network clients.

3.1.1 Setting up the wireless security settings

To protect your wireless network from unauthorized access, you need to configure its security settings.

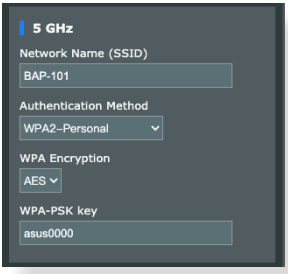
To set up the wireless security settings:

1. From the navigation panel, go to **General** > **Network Map**.
2. On the Network Map screen and under **System status**, you can configure the wireless security settings such as SSID, security level, and encryption settings.

NOTE: You can set up different wireless security settings for 2.4GHz and 5GHz bands.

2.4GHz security settings

5GHz security settings

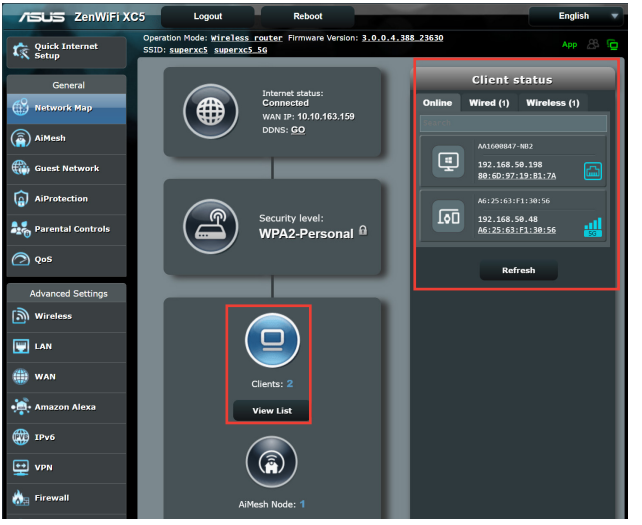


3. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.
4. From the **WEP Encryption** dropdown list, select the encryption method for your wireless network.

IMPORTANT! The IEEE 802.11n/ac/ax standard prohibits using High Throughput with WEP or WPA-TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11g 54Mbps connection.

5. Key in your security passkey.
6. Click **Apply** when done.

3.1.2 Managing your network clients



To manage your network clients:

1. From the navigation panel, go to **General** > **Network Map** tab.
2. On the Network Map screen, select the **Client Status** icon to display your network client's information.
3. To block a client's access to your network, select the client and click **block**.

3.1.3 Setting up AiMesh System

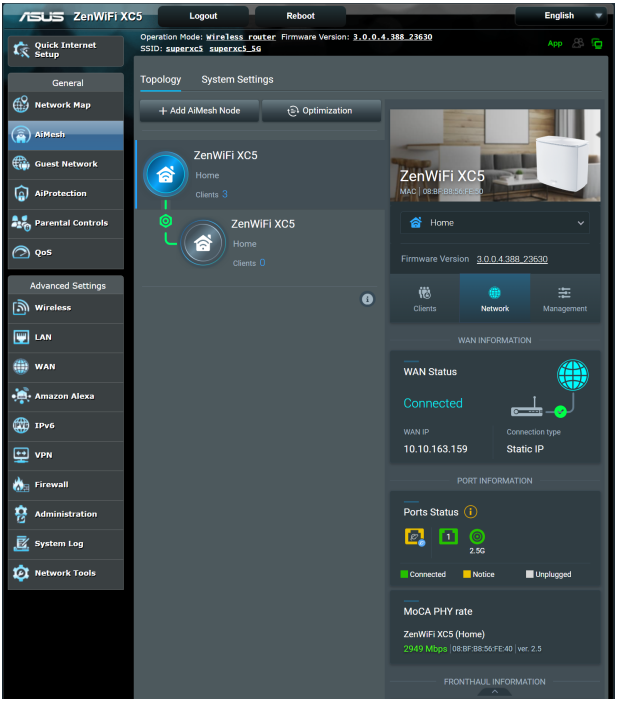
To setup ASUS AiMesh, make sure that the AiMesh node stays in factory defaults. Meanwhile, place the router and node around 3 meters away from each other during setup process.

To set up AiMesh system:

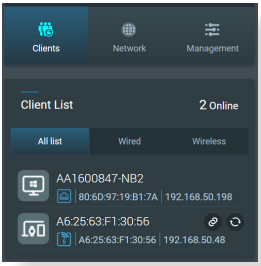
1. Login to your AiMesh router.
2. Go to **Network Map** page, click the **AiMesh Node** icon and then **Search** for your extending AiMesh node.

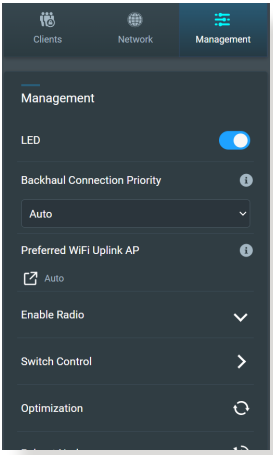
3. When the AiMesh node displays on this page, click it to join the AiMesh system. This will take some time, please wait until the process of adding the AiMesh node finishes.

4. When done, go to **AiMesh** to check the backhaul connection quality for your AiMesh nodes.



5. You can also find the information of the connected clients and tweak backhaul configurations on this page.





Clients

a. Clicking allows you to bind a WiFi client to a specified AiMesh node.

b. When a client has connected to the nearby AiMesh node, clicking allows you to reconnect it to the wireless network again. However, the connection decision rule still relies on the client driver.

Management

a. **Backhaul Connection Priority**: If you have preferred backhaul connection for your AiMesh system, select **a first specified priority** from the dropdown menu on **Backhaul Connection Priority**.

b. **Preferable Uplink AP**: When the node connects to the parent router or other node via WiFi backhaul, you can manually select an specified uplink AP from the dropdown menu.

c. **Enable Radio**: Enable or disable the node's radio manually.

d. **Reconnect Node**: If the backhaul of the node is connected through WiFi and the operating band is not what you expect, click to reconnect to an uplink AP.

e. **Reboot Node**: Click to reboot the node.

f. **Remove Node**: Click to remove one of the nodes from your AiMesh system.

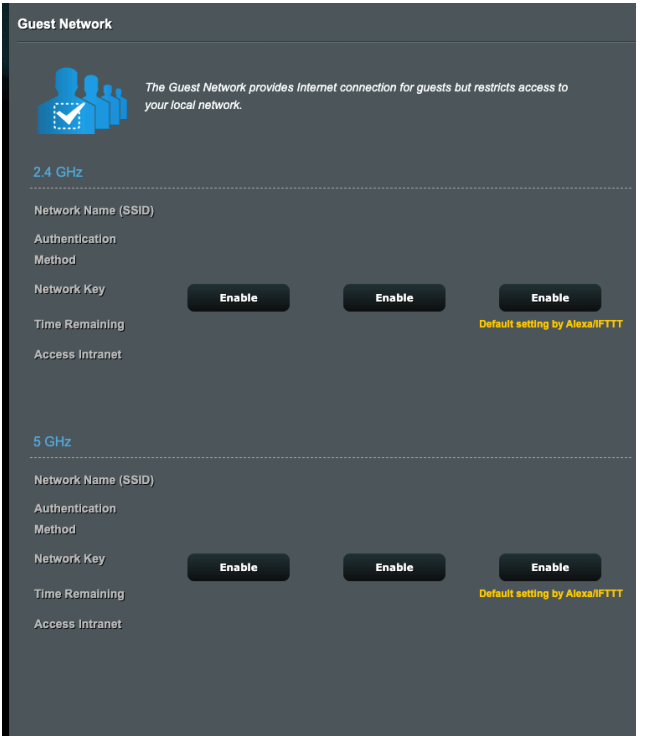
3.2 Creating a Guest Network

The Guest Network provides temporary visitors with Internet connectivity via access to separate SSIDs or networks without providing access to your private network.

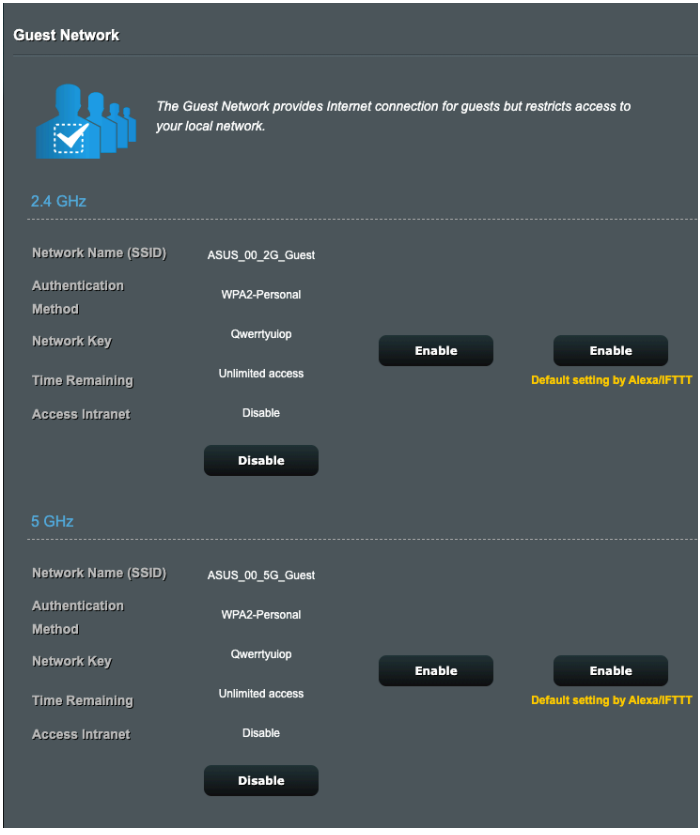
NOTE: ZenWiFi XC5 supports up to six SSIDs.

To create a guest network:

1. From the navigation panel, go to **General** > **Guest Network**.
2. On the Guest Network screen, select 2.4GHz or 5GHz frequency band for the guest network that you want to create.
3. Click **Enable**.



4. To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
5. Assign a wireless name for your temporary network on the Network Name (SSID) field.



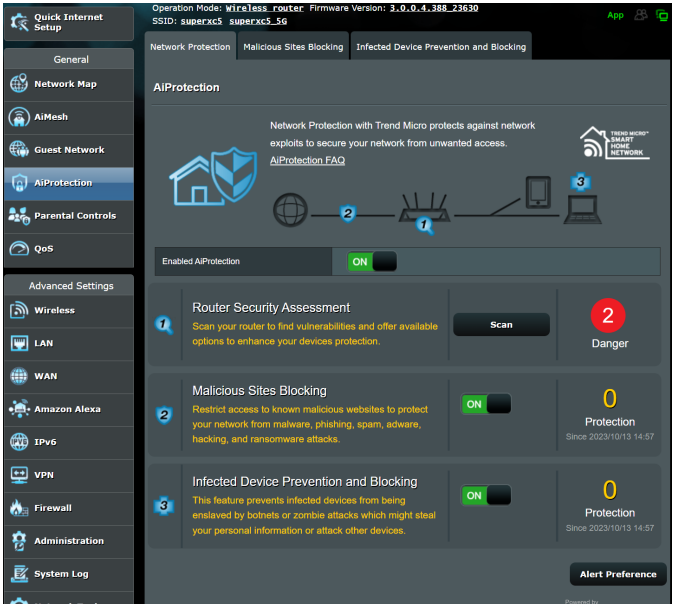
6. Select an Authentication Method.
7. If you select a WPA authentication method, select a WPA Encryption.
8. Specify the Access time or choose **Limitless**.
9. Select **Disable** or **Enable** on the Access Intranet item.
10. When done, click **Apply**.

3.3 AiProtection

AiProtection provides real-time monitoring that detects malware, spyware, and unwanted access. It also filters unwanted websites and apps and allows you to schedule a time that a connected device is able to access the Internet.

3.3.1 Network Protection

Network Protection prevents network exploits and secures your network from unwanted access.

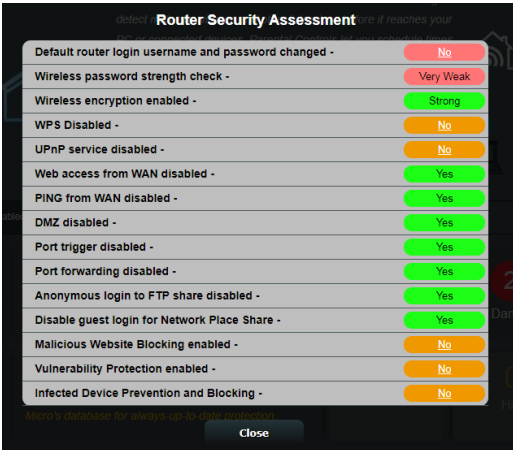


Configuring Network Protection

To configure Network Protection:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the **Network Protection** tab, click **Scan**.

   When done scanning, the utility displays the results on the **Router Security Assessment** page.



IMPORTANT! Items marked as **Yes** on the **Router Security Assessment** page is considered to be at a **safe** status. Items marked as **No**, **Weak**, or **Very Weak** is highly recommended to be configured accordingly.

3. (Optional) From the **Router Security Assessment** page, manually configure the items marked as **No**, **Weak**, or **Very Weak**. To do this:
   a. Click an item.

NOTE: When you click an item, the utility forwards you to the item's setting page.

   b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.
   c. Go back to the **Router Security Assessment** page and click **Close** to exit the page.
4. To automatically configure the security settings, click **Secure Your Router.**
5. When a message prompt appears, click **OK**.

Malicious Sites Blocking

This feature restricts access to known malicious websites in the cloud database for an always-up-to-date protection.

NOTE: This function is automatically enabled if you run the **Router Weakness Scan**.

To enable Malicious Sites Blocking:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the **AiProtection** main page, click on **Network Protection**.
3. From the **Malicious Sites Blocking** pane, click **ON**.

Infected Device Prevention and Blocking

This feature prevents infected devices from communicating personal information or infected status to external parties.

NOTE: This function is automatically enabled if you run the **Router Weakness Scan**.

To enable Infected Device Prevention and Blocking:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the **AiProtection** main page, click on **Network Protection**.
3. From the **Infected Device Prevention and Blocking** pane, click **ON**.

To configure Alert Preference:

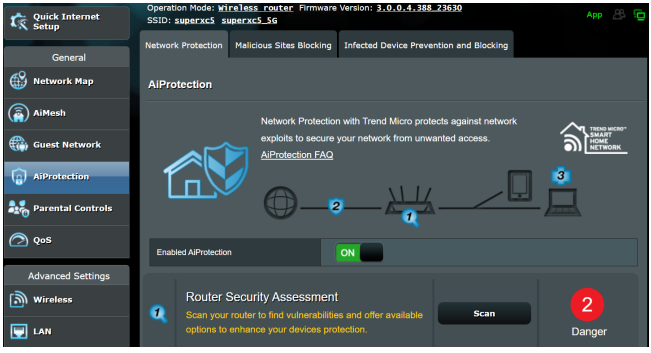
1. From the **Infected Device Prevention and Blocking** pane, click **Alert Preference**.
2. Select or key in the e-mail provider, e-mail account, and password then click **Apply**.

3.3.2 Setting up Parental Controls

Parental Control allows you to control the Internet access time or set the time limit for a client's network usage.

To go to the Parental Controls main page:

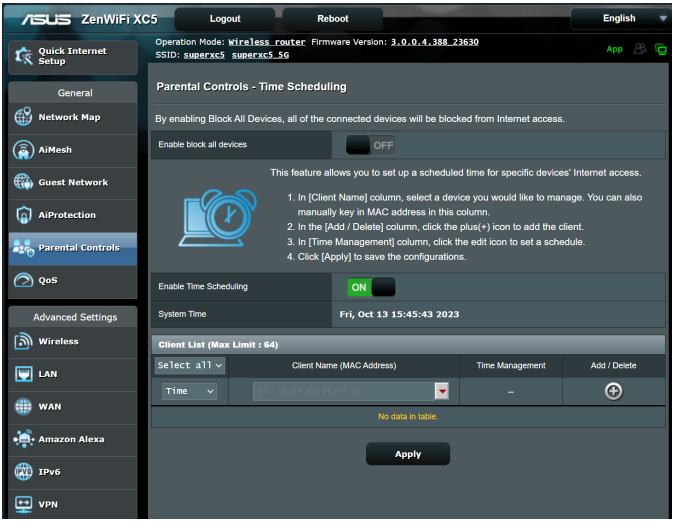
1. From the navigation panel, go to **General** > **Parental Controls**.



Time Scheduling

Time Scheduling allows you to set the time limit for a client's network usage.

NOTE: Ensure that your system time is synchronized with the NTP server.



To configure Time Scheduling:

1. From the navigation panel, go to **General** > **Parental Controls** > **Time Scheduling**.
2. From the **Enable Time Scheduling** pane, click **ON**.
3. From the **Clients Name** column, select or key in the client's name from the drop down list box.

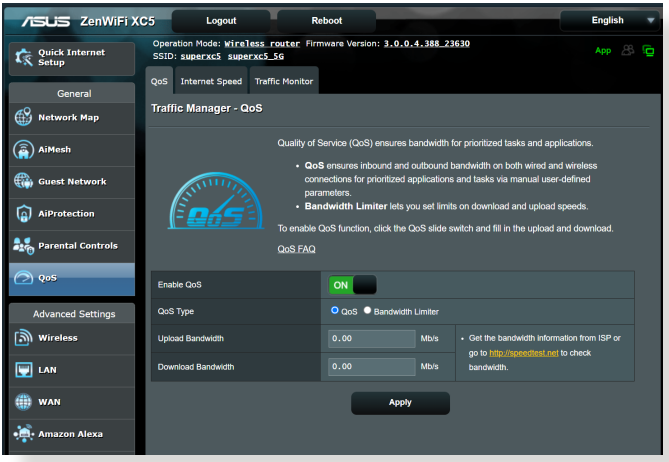
NOTE: You may also key in the client's MAC address in the **Client MAC Address** column. Ensure that the client name does not contain special characters or spaces as these may cause the router to function abnormally.

4. Click ⊕ to add the client's profile.
5. Click **Apply** to save the settings.

3.4 Using the Traffic Manager

3.4.1 Managing QoS (Quality of Service) Bandwidth

Quality of Service (QoS) allows you to set the bandwidth priority and manage network traffic.



To enable the QoS function:

1. From the navigation panel, go to **General** > **QoS** tab.
2. Click **ON** to enable QoS. Fill in the upload and download bandwidth fields.

NOTE: Get the bandwidth information from your ISP. You can also go to http://speedtest.net to check and get your bandwidth.

NOTE: The definition of the QoS Type is displayed on the QoS tab for your reference.

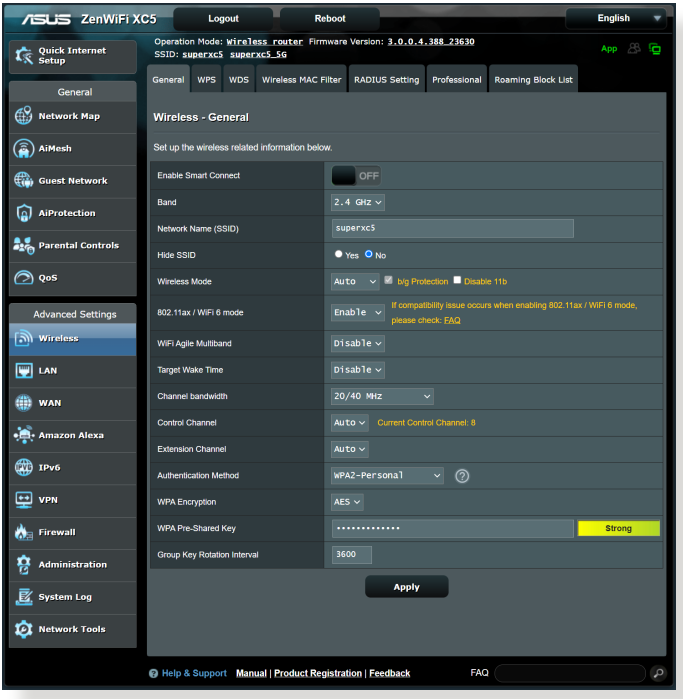
3. Click **Apply**.

4 Configuring the Advanced Settings

4.1 Wireless

4.1.1 General

The General tab allows you to configure the basic wireless settings.



To configure the basic wireless settings:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
2. At ZenWiFi router, the Smart Connect is enabled by default, which means 2.4GHz and 5GHz settings will be synchronized. If you disable Smart Connect, you can select 2.4GHz or 5GHz as the frequency band for your wireless network.
3. Assign a unique name containing up to 32 characters for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

NOTE: You can assign unique SSIDs for the 2.4 GHz and 5GHz frequency bands.

---

4. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
5. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
   - **Auto**: Select **Auto** to allow 802.11AC, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
   - **Legacy**: Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
   - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.

6. Select any of these channel bandwidth to accommodate higher transmission speeds:

   20/40/80/160MHz(default): Select this bandwidth to maximize the wireless throughput.

   20MHz: Select this bandwidth if you encounter some issues with your wireless connection.

7. Select the operating channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.

8. Select any of these authentication methods:
   - **Open System**: This option provides no security.
   - **WPA/WPA2/WPA3 Personal/WPA Auto-Personal**: This option provides strong security. You can use either WPA (with TKIP) or WPA2 (with AES). If you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).

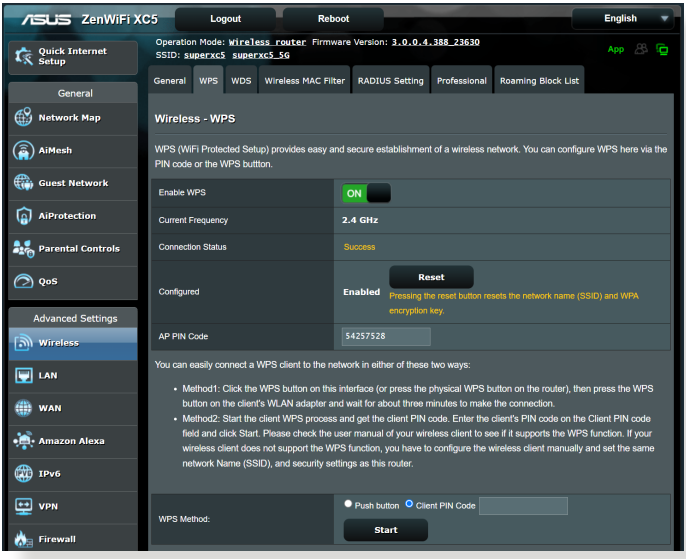
NOTE: Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto** and **encryption method** is **WEP** or **TKIP**.

9.When done, click **Apply**.

4.1.2 WPS

WPS (Wi-Fi Protected Setup) is a wireless security standard that allows you to easily connect devices to a wireless network. You can configure the WPS function via the PIN code or WPS button.

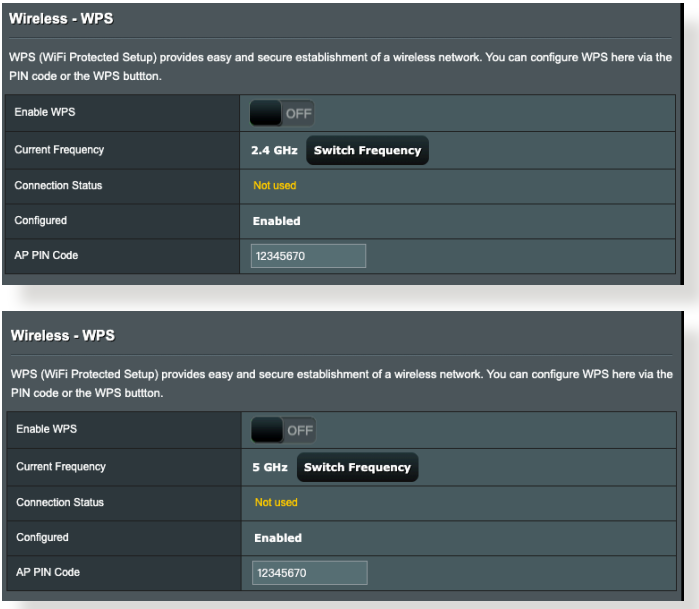
NOTE: Ensure that the devices support WPS.



To enable WPS on your wireless network:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WPS** tab.
2. In the **Enable WPS** field, move the slider to **ON**.
3. If you want to change the frequency to 2.4GHz or 5GHz, turn **OFF** the WPS function, click **Switch Frequency** in the **Current Frequency** field, and turn WPS **ON** again.

NOTE: WPS supports authentication using Open System, WPA-Personal, WPA2-Personal and WPA3-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.



4. In the WPS Method field, select **Push Button** or **Client PIN** code. If you select **Push button**, go to step 5. If you select **Client PIN Code**, go to step 6.
5. To set up WPS using the router's WPS button, follow these steps:
   a. Click **Start** or press the WPS button found at the front of the wireless router.
   b. Press the WPS button on your wireless device. This is normally identified by the WPS logo.

NOTE: Check your wireless device or its user manual for the location of the WPS button.

c. The wireless router will scan for any available WPS devices. If the wireless router does not find any WPS devices, it will switch to standby mode.

6. To set up WPS using the Client's PIN code, follow these steps:

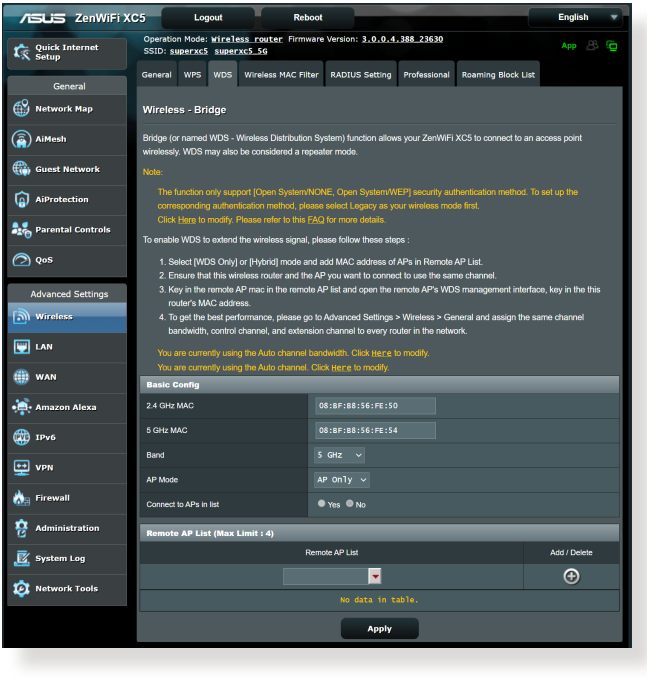
   a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.

   b. Key in the Client PIN code on the text box.

   c. Click **Start** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

4.1.3 Bridge

Bridge or WDS (Wireless Distribution System) allows your ASUS wireless router to connect to another wireless access point exclusively, preventing other wireless devices or stations to access your ASUS wireless router. It can also be considered as a wireless repeater where your ASUS wireless router communicates with another access point and other wireless devices.



To set up the wireless bridge:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WDS** tab.
2. Select the frequency band for the wireless bridge.
3. In the **AP Mode** field, select any of these options:
   - **AP Only**: Disables the Wireless Bridge function.

- **WDS Only**: Enables the Wireless Bridge feature but prevents other wireless devices/stations from connecting to the router.
- **HYBRID**: Enables the Wireless Bridge feature and allows other wireless devices/stations to connect to the router.

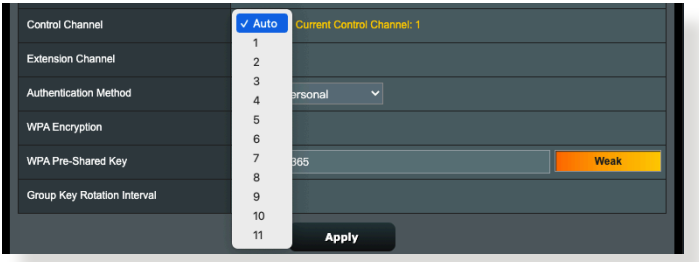
NOTE: In Hybrid mode, wireless devices connected to the ASUS wireless router will only receive half the connection speed of the Access Point.

4. In the **Connect to APs in list** field, click **Yes** if you want to connect to an Access Point listed in the Remote AP List.
5. In the **Control Channel** field, select the operating channel for the wireless bridge. Select **Auto** to allow the router to automatically select the channel with the least amount of interference.

NOTE: Channel availability varies per country or region.

6. On the Remote AP List, key in a MAC address and click the **Add** button to enter the MAC address of other available Access Points.

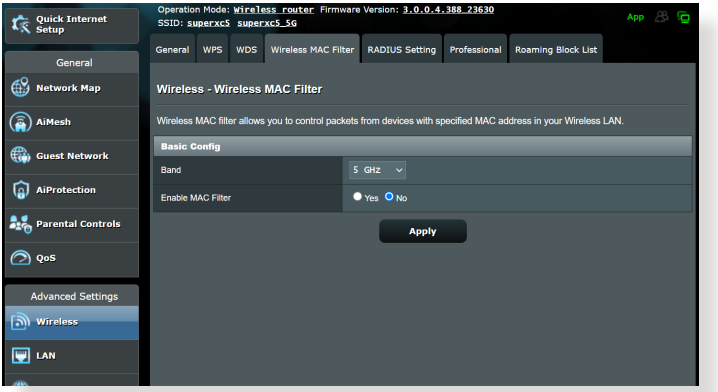
NOTE: Any Access Point added to the list should be on the same Control Channel as the ASUS wireless router.



7. Click **Apply**.

4.1.4 Wireless MAC Filter

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.

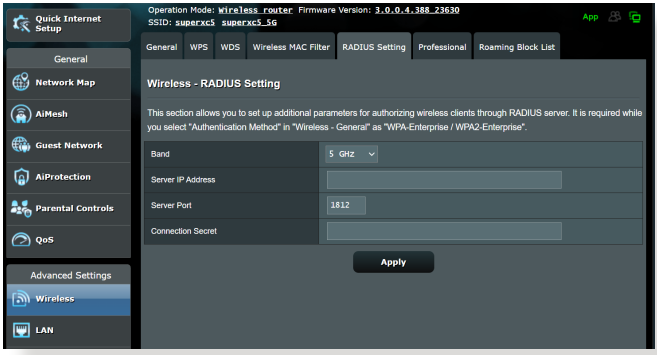


To set up the Wireless MAC filter:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
2. Tick **Yes** in the **Enable Mac Filter** field.
3. In the **MAC Filter Mode** dropdown list, select either **Accept** or **Reject**.
   - Select **Accept** to allow devices in the MAC filter list to access to the wireless network.
   - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
4. On the MAC filter list, click the **Add** button and key in the MAC address of the wireless device.
5. Click **Apply**.

4.1.5 RADIUS Setting

RADIUS (Remote Authentication Dial In User Service) Setting provides an extra layer of security when you choose WPA-Enterprise, WPA2-Enterprise, or Radius with 802.1x as your Authentication Mode.

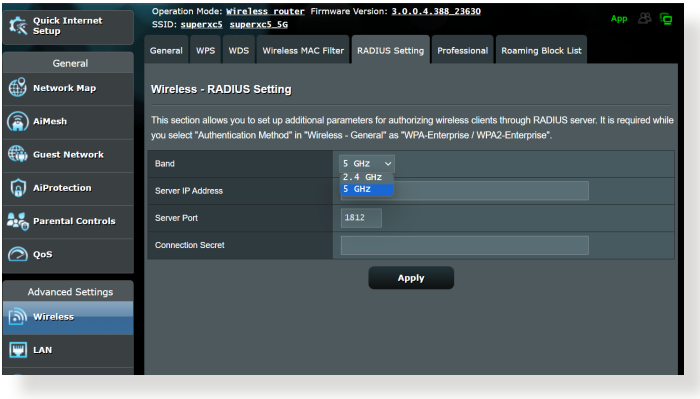


To set up wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to WPA-Enterprise, WPA2-Enterprise, or Radius with 802.1x.

NOTE: Please refer to section **4.1.1 General** section for configuring your wireless router's Authentication Mode.

2. From the navigation panel, go to **Advanced Settings** > **Wireless** > **RADIUS Setting**.
3. Select a frequency band if Smart Connect is disabled.

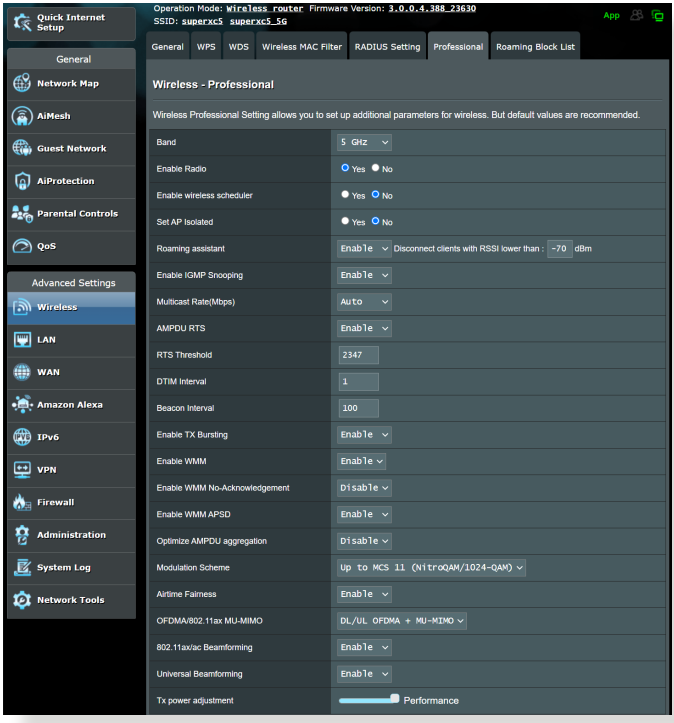


4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
5. In the **Connection Secret** field, assign the password to access your RADIUS server.
6. Click **Apply**.

4.1.6 Professional

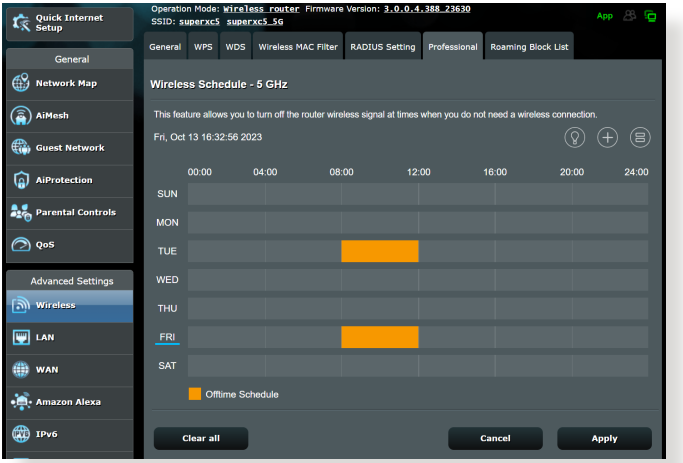
The Professional screen provides advanced configuration options.

NOTE: We recommend that you use the default values on this page.



In the **Professional** screen, you can configure the following:

- **Band**: Select the frequency band that the professional settings will be applied to.
- **Enable Radio**: Select **Yes** to enable wireless networking. Select **No** to disable wireless networking.
- **Enable wireless scheduler**: You can choose clock format as 24-hour or 12-hour. The color in the table indicates Allow or Deny. Click each frame to change the settings of the hour of the weekdays and click **OK** when done.



- **Set AP isolated**: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.

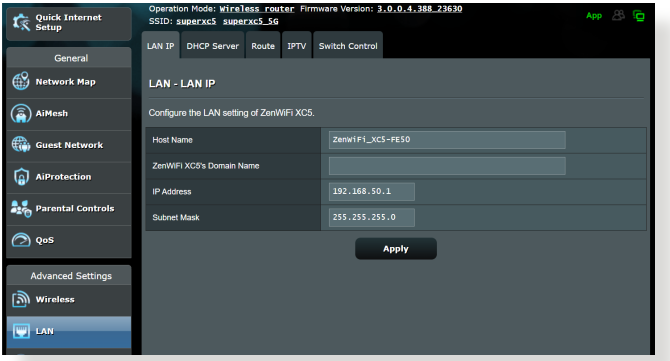
- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.
- **Enable WMM APSD**: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.

4.2 LAN

4.2.1 LAN IP

The LAN IP screen allows you to modify the LAN IP settings of your wireless router.

NOTE: Any changes to the LAN IP address will be reflected on your DHCP settings.

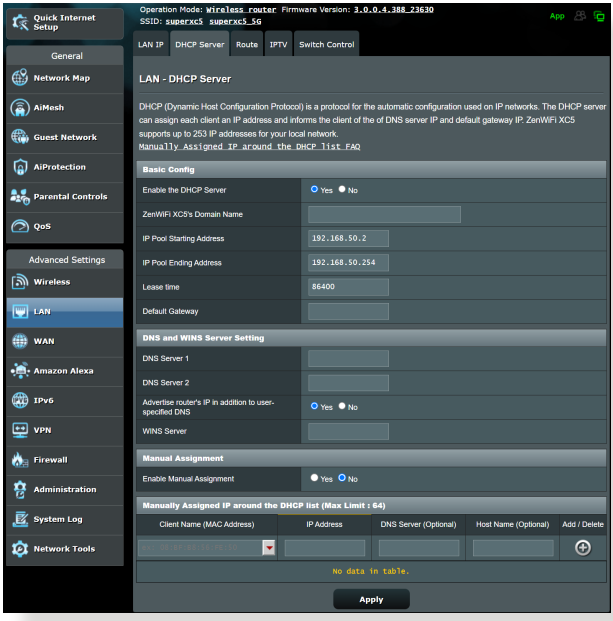


To modify the LAN IP settings:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **LAN IP** tab.
2. Modify the **IP address** and **Subnet Mask**.
3. When done, click **Apply**.

4.2.2 DHCP Server

Your wireless router uses DHCP to assign IP addresses automatically on your network. You can specify the IP address range and lease time for the clients on your network.



To configure the DHCP server:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **DHCP Server** tab.
2. In the **Enable the DHCP Server** field, tick **Yes**.
3. In the **ZenWiFi AX Hybrid's Domain Name** text box, enter a domain name for the wireless router.
4. In the **IP Pool Starting Address** field, key in the starting IP address.
5. In the **IP Pool Ending Address** field, key in the ending IP address.

6. In the **Lease time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

NOTES:

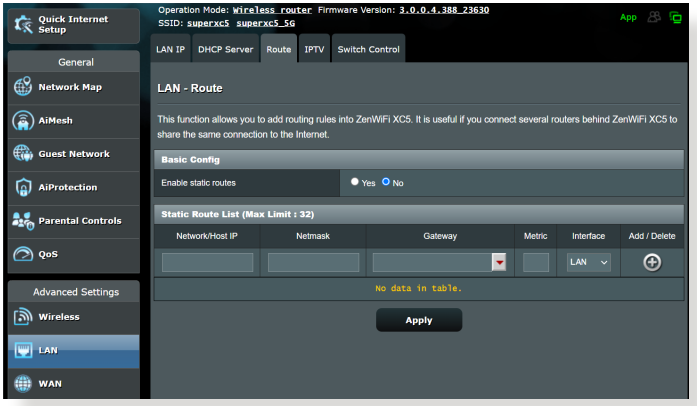
- We recommend that you use an IP address format of 192.168.50.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.

7. In the **DNS Server** and **WINS Server** field, key in your DNS Server and WINS Server IP address if needed.
8. Your wireless router can also manually assign IP addresses to devices on the network. On the **Enable Manual Assignment** field, choose **Yes** to assign an IP address to specific MAC addresses on the network. Up to 32 MAC Addresses can be added to the DHCP list for manual assignment.

4.2.3 Route

If your network makes use of more than one wireless router, you can configure a routing table to share the same Internet service.

NOTE: We recommend that you do not change the default route settings unless you have advanced knowledge of routing tables.

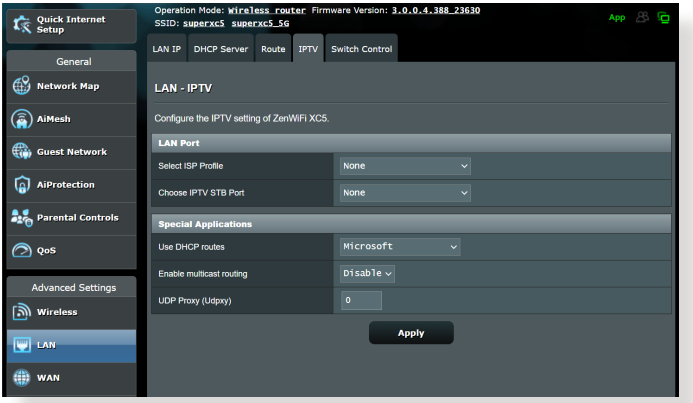


To configure the LAN Routing table:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **Route** tab.
2. On the **Enable static routes** field, choose **Yes**.
3. On the **Static Route List**, enter the network information of other access points or nodes. Click the **Add** or **Delete** button to add or remove a device on the list.
4. Click **Apply**.

4.2.4 IPTV

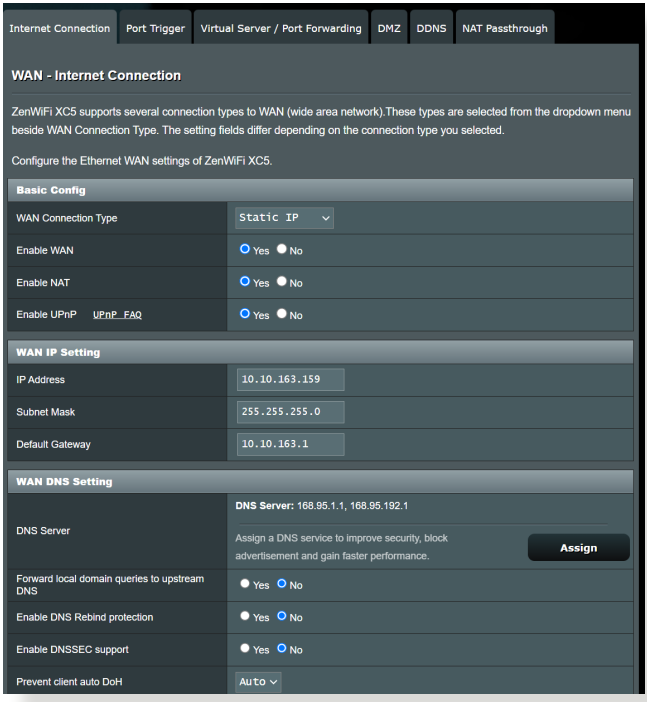
The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.



4.3 WAN

4.3.1 Internet Connection

The Internet Connection screen allows you to configure the settings of various WAN connection types.



To configure the WAN connection settings:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.
2. Configure the following settings below. When done, click **Apply**.
   - **WAN Connection Type**: Choose your Internet Service Provider type. The choices are **Automatic IP**, **PPPoE**, **PPTP**, **L2TP** or **fixed IP**. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.

- **Enable WAN**: Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.
- **Enable NAT**: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Enable UPnP**: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- **Connect to DNS Server automatically**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- **Host Name**: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.
- **MAC Address**: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs

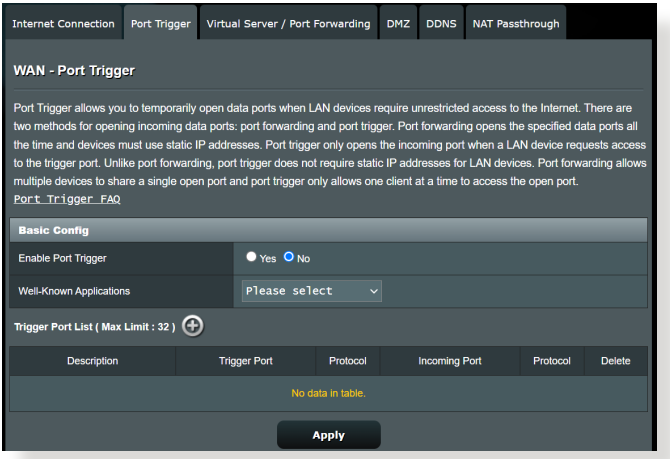
monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:

- Contact your ISP and update the MAC address associated with your ISP service.
- Clone or change the MAC address of the ASUS wireless router to match the MAC address of the previous networking device recognized by the ISP.

4.3.2 Port Trigger

Port range triggering opens a predetermined incoming port for a limited period of time whenever a client on the local area network makes an outgoing connection to a specified port. Port triggering is used in the following scenarios:

- More than one local client needs port forwarding for the same application at a different time.
- An application requires specific incoming ports that are different from the outgoing ports.



To set up Port Trigger:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Port Trigger** tab.
2. Configure the following settings below. When done, click **Apply**.
   - **Enable Port Trigger**: Choose **Yes** to enable Port Trigger.
   - **Well-Known Applications**: Select popular games and web services to add to the Port Trigger List.
   - **Description**: Enter a short name or description for the service.

- **Trigger Port**: Specify a trigger port to open the incoming port.
- **Protocol**: Select the protocol, TCP, or UDP.
- **Incoming Port**: Specify an incoming port to receive inbound data from the Internet.

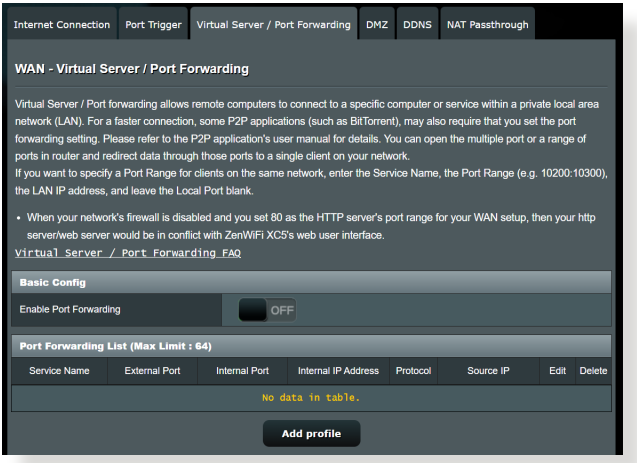
NOTES:

- When connecting to an IRC server, a client PC makes an outgoing connection using the trigger port range 66660-7000. The IRC server responds by verifying the username and creating a new connection to the client PC using an incoming port.
- If Port Trigger is disabled, the router drops the connection because it is unable to determine which PC is requesting for IRC access. When Port Trigger is enabled, the router assigns an incoming port to receive the inbound data. This incoming port closes once a specific time period has elapsed because the router is unsure when the application has been terminated.
- Port triggering only allows one client in the network to use a particular service and a specific incoming port at the same time.
- You cannot use the same application to trigger a port in more than one PC at the same time. The router will only forward the port back to the last computer to send the router a request/trigger.

4.3.3 Virtual Server / Port Forwarding

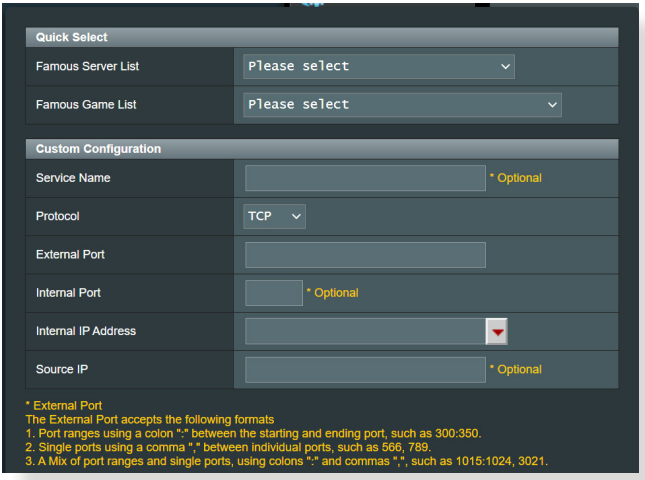
Port forwarding is a method to direct network traffic from the Internet to a specific port or a specific range of ports to a device or number of devices on your local network. Setting up Port Forwarding on your router allows PCs outside the network to access specific services provided by a PC in your network.

NOTE: When port forwarding is enabled, the ASUS router blocks unsolicited inbound traffic from the Internet and only allows replies from outbound requests from the LAN. The network client does not have access to the Internet directly, and vice versa.



To set up Port Forwarding:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Virtual Server / Port Forwarding** tab.
2. Slide the bar to **ON** to enable Port Forwarding, then click **Add Profile**. After configuring the following settings, click **OK**.



- **Famous Server List**: Determine which type of service you want to access.
- **Famous Game List**: This item lists ports required for popular online games to work correctly.
- **Service Name**: Enter a service name.
- **Protocol**: Select the protocol. If you are unsure, select **BOTH**.
- **External Port**: Accept the following formats:
  1) A port range using a colon ":" in the middle to specify the upper and lower limits of the range, such as 300:350;
  2) Individual port numbers using a comma "," to separate them, such as 566, 789;
  3) A Mix of port ranges and individual ports, using colons ":" and commas ",", such as 1015:1024, 3021.
- **Internal Port**: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.

- **Internal IP Address**: Key in the client's LAN IP address.
- **Source IP**: If you want to open your port to a specific IP address from the Internet, input the IP address you want to give access to in this field.

NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **4.2 LAN** for information.

To check if Port Forwarding has been configured successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

4.3.4 DMZ

Virtual DMZ exposes one client to the Internet, allowing this client to receive all inbound packets directed to your Local Area Network.

Inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. In a DMZ configuration, one network client receives all inbound packets.

Setting up DMZ on a network is useful when you need incoming ports open or you want to host a domain, web, or e-mail server.

CAUTION: Opening all the ports on a client to the Internet makes the network vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.

To set up DMZ:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DMZ** tab.
2. Configure the setting below. When done, click **Apply**.

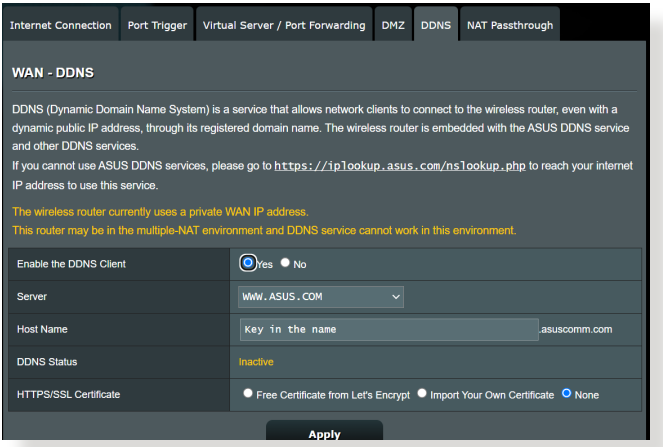
- **IP address of Exposed Station:** Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.

To remove DMZ:

1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
2. When done, click **Apply**.

4.3.5 DDNS

Setting up DDNS (Dynamic DNS) allows you to access the router from outside your network through the provided ASUS DDNS Service or another DDNS service.



To set up DDNS:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DDNS** tab.
2. Configure the following settings below. When done, click **Apply**.
   - **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
   - **Server** and **Host Name**: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).
   - If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.
   - **Enable wildcard**: Enable wildcard if your DDNS service requires one.

NOTES:

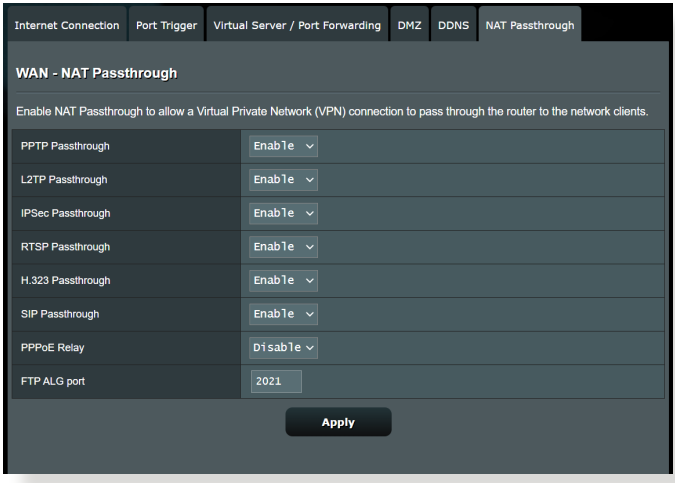
DDNS service will not work under these conditions:

- When the wireless router is using a private WAN IP address (192.168. x.x, 10.x.x.x, or 172.16.x.x), as indicated by a yellow text.
- The router may be on a network that uses multiple NAT tables.

4.3.6 NAT Passthrough

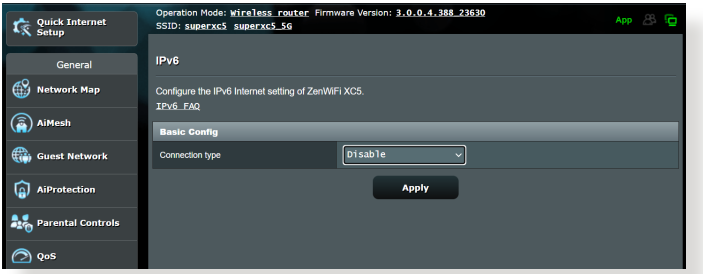
NAT Passthrough allows a Virtual Private Network (VPN) connection to pass through the router to the network clients. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough and RTSP Passthrough are enabled by default.

To enable / disable the NAT Passthrough settings, go to the **Advanced Settings** > **WAN** > **NAT Passthrough** tab. When done, click **Apply**.



4.4 IPv6

This wireless router supports IPv6 addressing, a system that supports more IP addresses. This standard is not yet widely available. Contact your ISP if your Internet service supports IPv6.



To set up IPv6:

1. From the navigation panel, go to **Advanced Settings** > **IPv6**.
2. Select your **Connection type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

NOTE: Please refer to your ISP regarding specific IPv6 information for your Internet service.

4.5 Firewall

The wireless router can serve as a hardware firewall for your network.

NOTE: The Firewall feature is enabled by default.

4.5.1 General

To set up basic Firewall settings:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **General** tab.
2. On the **Enable Firewall** field, select **Yes.**
3. On the **Enable DoS** protection, select **Yes** to protect your network from DoS (Denial of Service) attacks though this may affect your router's performance.
4. You can also monitor packets exchanged between the LAN and WAN connection. On the Logged packets type, select **Dropped**, **Accepted**, or **Both**.
5. Click **Apply**.

4.5.2 URL Filter

You can specify keywords or web addresses to prevent access to specific URLs.

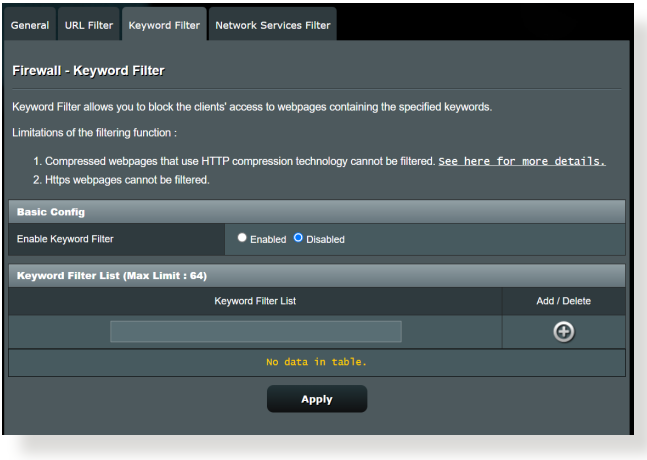
NOTE: The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

To set up a URL filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **URL Filter** tab.
2. On the Enable URL Filter field, select **Enabled**.
3. Enter a URL and click the button.
4. Click **Apply**.

4.5.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.



To set up a keyword filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Keyword Filter** tab.
2. On the Enable Keyword Filter field, select **Enabled**.

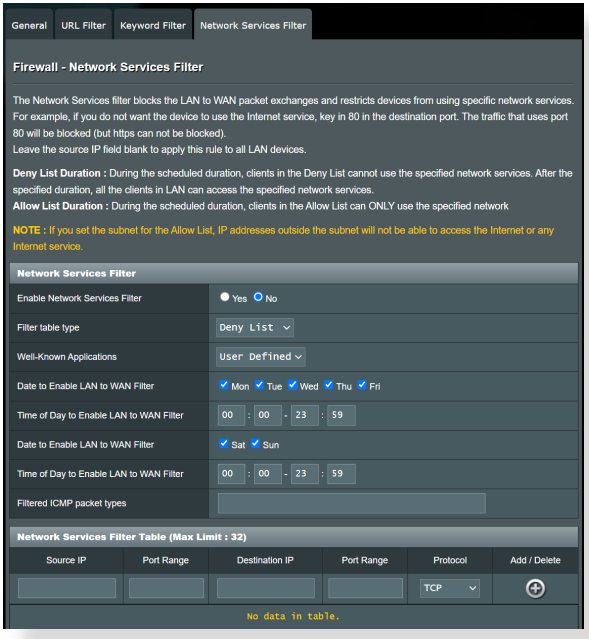
3. Enter a word or phrase and click the **Add** button.
4. Click **Apply**.

NOTES:

- The Keyword Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the Keyword Filter.
- Web pages compressed using HTTP compression cannot be filtered. HTTPS pages also cannot be blocked using a keyword filter.

4.5.4 Network Services Filter

The Network Services Filter blocks LAN to WAN packet exchanges and restricts network clients from accessing specific web services such as Telnet or FTP.



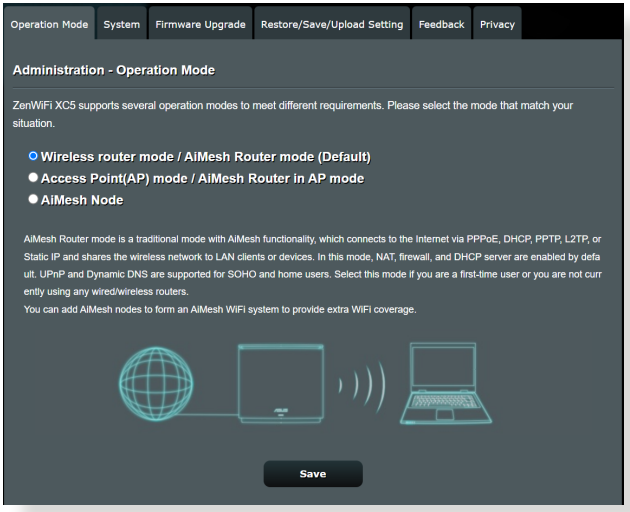
To set up a Network Service filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Network Services Filter** tab.
2. On the **Enable Network Services Filter** field, select **Yes**.
3. Select the Filter table type. **Deny List** blocks the specified network services. **Allow List** limits access to only the specified network services.
4. Specify the day and time when the filters will be active.
5. To specify a Network Service to filter, enter the Source IP, Destination IP, Port Range, and Protocol. Click the  button.
6. Click **Apply**.

4.6 Administration

4.6.1 Operation Mode

The Operation Mode page allows you to select the appropriate mode for your network.



To set up the operating mode:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Operation Mode** tab.
2. Select any of these operation modes:
   - **Wireless router mode / AiMesh Router mode (Default)**: In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
   - **Access Point mode**: In this mode, the router creates a new wireless network on an existing network.
3. Click **Save**.

NOTE: The router will reboot when you change the modes.

4.6.2 System

The **System** page allows you to configure your wireless router settings.

To set up the System settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
2. You can configure the following settings:
   - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
   - **WPS button behavior**: The physical WPS button on the wireless router can be used to activate WPS.
   - **Time Zone**: Select the time zone for your network.
   - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **Network Monitoring**: You can enable DNS Query to check Resolve Hostname and Resolved IP Addresses, or enable Ping, then check your Ping Target.
   - **Auto Logout**: You can set the time of auto-logout.
   - **Enable WAN down browser redirect notice:** This feature allows the browser to display a warning page when the router is disconnected from Internet. When disabled, the warning page will not appear.
   - **Enable Telnet**: Click **Yes** to enable Telnet services on the network. Click **No** to disable Telnet.
   - **Authentication Method**: You can select HTTP, HTTPS, or both protocols to secure router access.
   - **Enable Reboot Scheduler:** When enabled, you can set the Date to Reboot and Time of Day to Reboot.
   - **Enable Web Access from WAN**: Select **Yes** to allow devices outside the network to access the wireless router GUI settings. Select **No** to prevent access.
   - **Enable Access Restrictions**: Click **Yes** if you want to specify the IP addresses of devices that are allowed to access to the

wireless router GUI settings from WAN/LAN.

- **Service**: This feature allows you to configure Enable Telnet/ Enable SSH/SSH Port/Allow Password Login/Authorized Keys/Idle Timeout.

3. Click **Apply**.

4.6.3 Firmware Upgrade

NOTE: Download the latest firmware from the ASUS website at **http://www.asus.com**.

To upgrade the firmware:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Firmware Upgrade** tab.
2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
3. Click **Upload**.

NOTES:

- When the upgrade process is complete, wait for some time for the system to reboot.
- If the upgrade process fails, the wireless router automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly. To recover or restore the system, refer to section **5.2 Firmware Restoration**.

4.6.4 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Restore/Save/Upload Setting** tab.
2. Select the tasks that you want to do:
   - To restore to the default factory settings, click **Restore**, and click **OK** in the confirmation message.
   - To save the current system settings, click **Save**, navigate to the folder where you intend to save the file and click **Save**.
   - To restore from a saved system settings file, click **Browse** to locate your file, then click **Upload**.

IMPORTANT! If issues occur, upload the latest firmware version and configure new settings. Do not restore the router to its default settings.

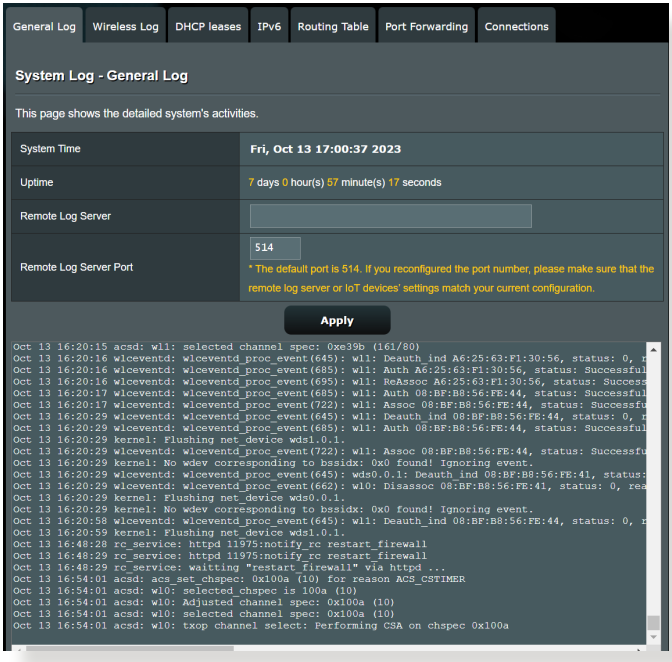
4.7 System Log

System Log contains your recorded network activities.

NOTE: System log resets when the router is rebooted or powered off.

To view your system log:

1. From the navigation panel, go to **Advanced Settings** > **System Log**.
2. You can view your network activities in any of these tabs:
   - General Log
   - Wireless Log
   - DHCP leases
   - IPv6
   - Routing Table
   - Port Forwarding
   - Connections



5 Utilities

NOTE: Download and install the wireless router's utilities from the ASUS website: https://www.asus.com/support/Download-Center/

5.1 Device Discovery

Device Discovery is an ASUS WLAN utility that detects an ASUS wireless router device, and allows you to configure the wireless networking settings.

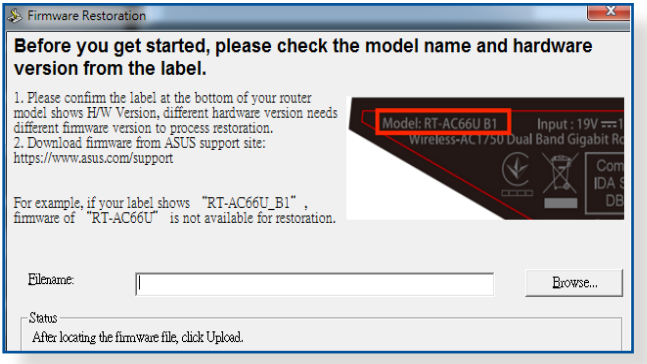
To launch the Device Discovery utility:

- From your computer's desktop, click **Start** > **All Programs** > **ASUS Utility** > **Wireless Router** > **Device Discovery**.

NOTE: When you set the router to Access Point mode, you need to use Device Discovery to get the router's IP address.

5.2 Firmware Restoration

Firmware Restoration is used on an ASUS Wireless Router that failed during its firmware upgrading process. It uploads the firmware that you specify. The process takes about three to four minutes.



IMPORTANT! Launch the rescue mode on the router before using the Firmware Restoration utility.

To launch the rescue mode and use the Firmware Restoration utility:

1. Unplug the wireless router from the power source.
2. Hold the Reset button at the rear panel and simultaneously replug the wireless router into the power source. Release the Reset button when the Power LED at the front panel flashes slowly, which indicates that the wireless router is in the rescue mode.
3. Set a static IP on your computer and use the following to set up your TCP/IP settings:

   IP address: 192.168.1.x

   Subnet mask: 255.255.255.0
4. From your computer's desktop, click **Start** > **All Programs** > **ASUS Utility** > **Wireless Router** > **Firmware Restoration**.
5. Specify a firmware file, then click **Upload**.

NOTE: This is not a firmware upgrade utility and cannot be used on a working ASUS Wireless Router. Normal firmware upgrades must be done through the web interface. Refer to **Chapter 4: Configuring the Advanced Settings** for more details.

6 Troubleshooting

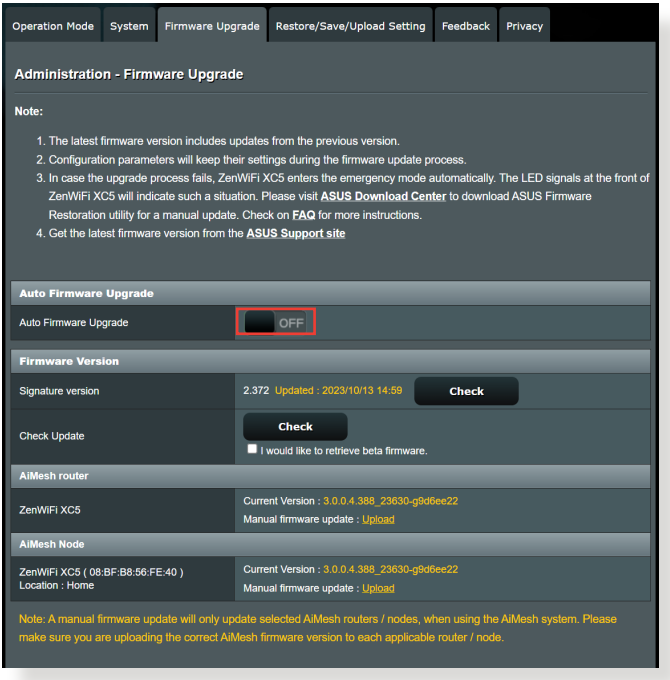
This chapter provides solutions for issues you may encounter with your router. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at: https://www.asus.com/support/ for more product information and contact details of ASUS Technical Support.

6.1 Basic Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

Upgrade Firmware to the latest version.

1. Launch the Web GUI. Go to **Advanced Settings** > **Administration** > **Firmware Upgrade** tab.
2. Slide **Auto Firmware Upgrade** to **ON** to enable automatic firmware upgrade.



3. If you want to upgrade the firmware manually, you can disable **Auto Firmware Upgrade**, click **Check** to verify if the latest firmware is available.
4. If the latest firmware is available, visit the ASUS global website at https://www.asus.com/support to download the latest firmware.
5. Click **Upload** to upgrade the firmware for AiMesh router or AiMesh Node.

Restart your network in the following sequence:

1. Turn off the modem.
2. Unplug the modem.
3. Turn off the router and computers.
4. Plug in the modem.
5. Turn on the modem and then wait for 2 minutes.
6. Turn on the router and then wait for 2 minutes.
7. Turn on computers.

Check if your Ethernet cables are plugged properly.

- When the Ethernet cable connecting the router with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your powered-on computer with the router is plugged in properly, the corresponding LAN LED will be on.

Check if the wireless setting on your computer matches that of your router.

- When you connect your computer to the router wirelessly, ensure that the SSID (wireless network name), encryption method, and password are correct.

Check if your network settings are correct.

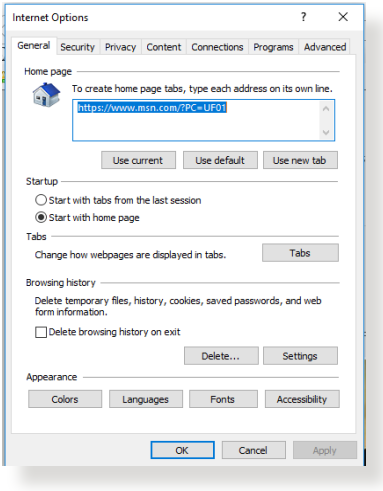
- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.

- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the web GUI, **Network Map** > **Clients** page, and hover the mouse pointer over your device in **Client Status**.

6.2 Frequently Asked Questions (FAQs)

I cannot access the router GUI using a web browser

- If your computer is wired, check the Ethernet cable connection and LED status as described in the previous section.
- Ensure that you are using the correct login information. The default factory login name and password is “admin/admin”. Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer, follow these steps:
  1. Launch Internet Explorer, then click **Tools** > **Internet Options**.
  2. In the **General** tab, under **Browsing history**, click **Delete…**, select **Temporary Internet files and website files** and **Cookies and website data** then click **Delete**.



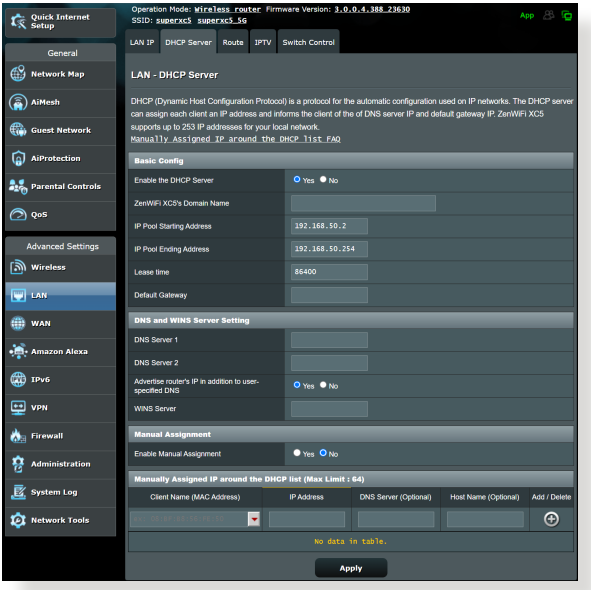
NOTES:

- The commands for deleting cookies and files vary with web browsers.
- Disable proxy server settings, cancel the dial-up connection, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to Chapter 1 of this user manual.
- Ensure that you use CAT5e or CAT6 ethernet cables.

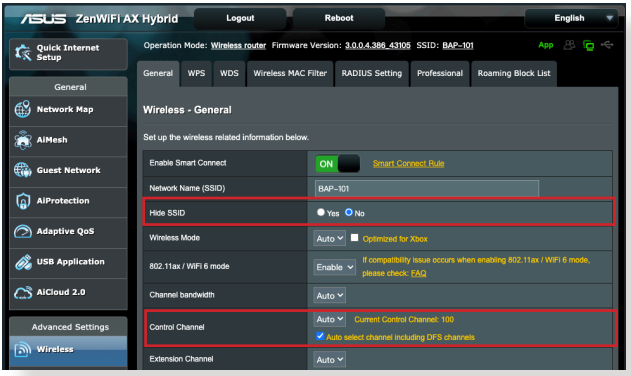
The client cannot establish a wireless connection with the router.

NOTE: If you are having issues connecting to 5GHz network, make sure that your wireless device supports 5GHz or features dual band capabilities.

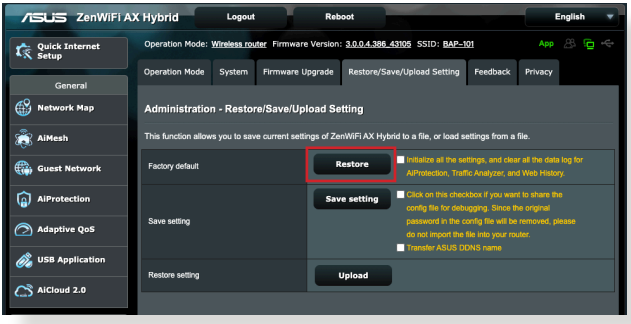
- **Out of Range:**
  - Move the router closer to the wireless client.
  - Try to adjust antennas of the router to the best direction as described in section **1.4 Positioning your router**.
- **DHCP server has been disabled:**
  1. Launch the web GUI. Go to **General** > **Network Map**> **Clients** and search for the device that you want to connect to the router.
  2. If you cannot find the device in the **Network Map**, go to **Advanced Settings** > **LAN** > **DHCP Server**, **Basic Config** list, select **Yes** on the **Enable the DHCP Server**.



- SSID has been hidden. If your device can find SSIDs from other routers but cannot find your router's SSID, go to **Advanced Settings** > **Wireless** > **General**, select **No** on **Hide SSID**, and select **Auto** on **Control Channel**.



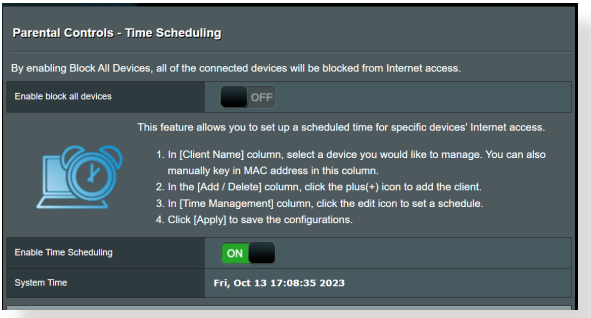
- If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. If not, adjust the channel, channel bandwidth, and wireless mode.
- If you still cannot connect to the router wirelessly, you can reset your router to factory default settings. In the router GUI, click **Administration** > **Restore/Save/Upload Setting** and click **Restore**.



Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to **General**> **Network Map**, and check the **Internet Status**.
- If your router cannot connect to your ISP's WAN IP address, try restarting your network as described in the section **Restart your network in following sequence** under **Basic Troubleshooting**.

- The device has been blocked via the Parental Control function. Go to **General** > **Parental Controls** and see if the device is in the list. If the device is listed under **Client Name**, remove the device using the **Delete** button or adjust the Time Management Settings.



- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.
- Check the status indicators on the ADSL modem and the wireless router. If the WAN LED on the wireless router is not ON, check if all cables are plugged properly.

You forgot the SSID (network name) or network password

- Setup a new SSID and encryption key via a wired connection (Ethernet cable). Launch the web GUI, go to **Network Map**, click the router icon, enter a new SSID and encryption key, and then click **Apply**.
- Reset your router to the default settings. Launch the web GUI, go to **Administration** > **Restore/Save/Upload Setting**, and click **Restore**. The default login account and password are both "admin".

How to restore the system to its default settings?

- Go to **Administration** > **Restore/Save/Upload Setting**, and click **Restore**.

  The following are the factory default settings:

Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	192.168.50.1
Domain Name:	(Blank)
Subnet Mask:	255.255.255.0
DNS Server 1:	www.asusrouter.com
DNS Server 2:	(Blank)
SSID:	ASUS_XX

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **5.2 Firmware Restoration** on how to use the Firmware Restoration utility.

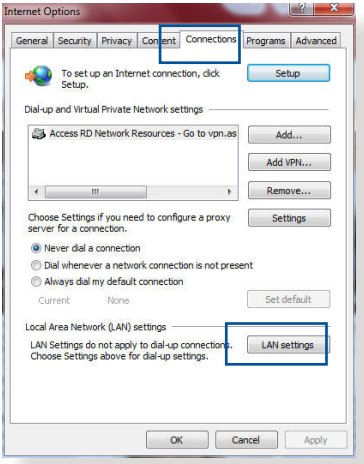
Cannot access Web GUI

Before configuring your wireless router, do the steps described in this section for your host computer and network clients.

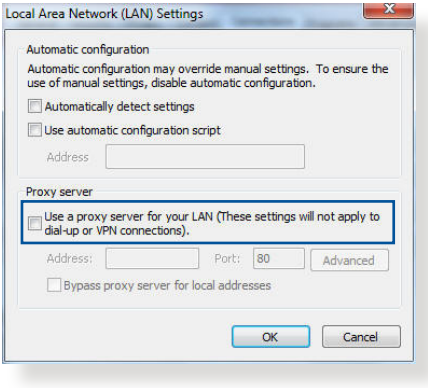
A. Disable the proxy server, if enabled.

Windows®

1. Click **Start > Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections** tab > **LAN settings**.

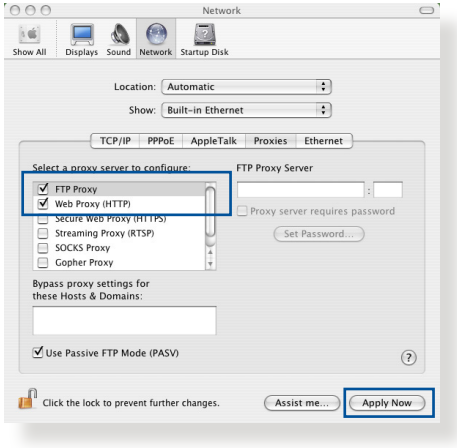


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



MAC OS

1. From your Safari browser, click **Safari** > **Preferences** > **Advanced** > **Change Settings...**
2. From the Network screen, deselect **FTP Proxy** and **Web Proxy (HTTP)**.
3. Click **Apply Now** when done.

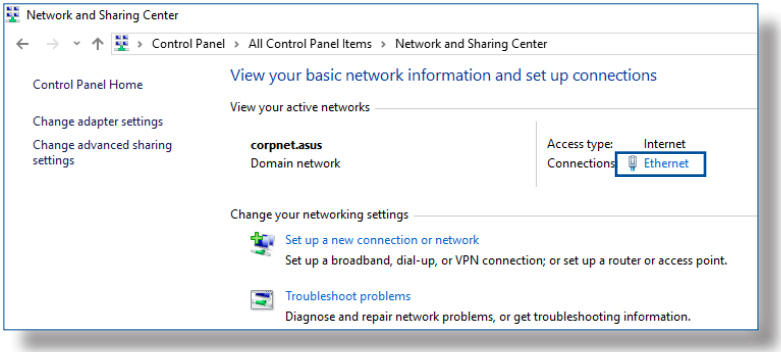


NOTE: Refer to your browser's help feature for details on disabling the proxy server.

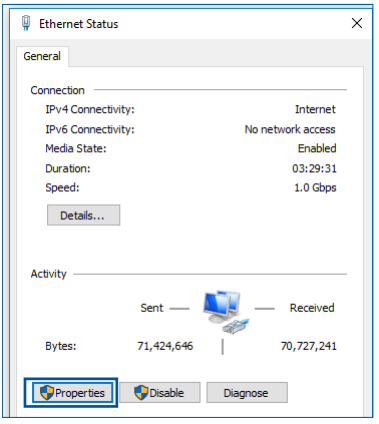
B. Set the TCP/IP settings to automatically obtain an IP address.

Windows®

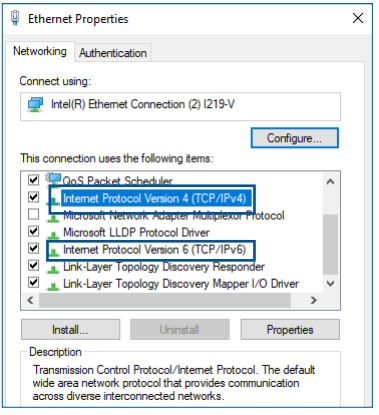
1. Click **Start** > **Control Panel** > **Network and Sharing Center,** then click the network connection to display its status window.



2. Click **Properties** to display the Ethernet Properties window.



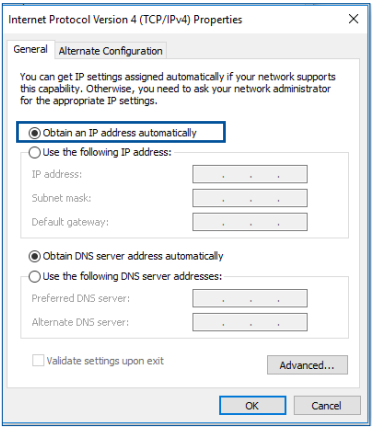
3. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



4. To obtain the IPv4 IP settings automatically, tick **Obtain an IP address automatically**.

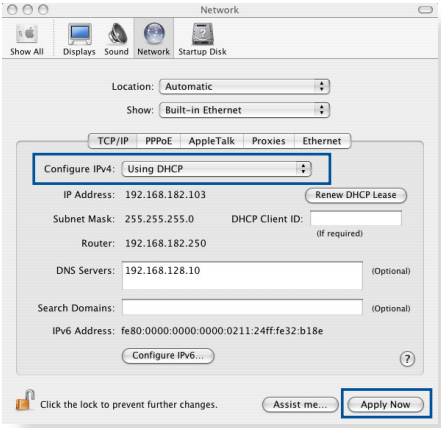
   To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

5. Click **OK** when done.



MAC OS

1. Click the Apple icon located on the top left of your screen.
2. Click **System Preferences** > **Network** > **Configure...**
3. From the **TCP/IP** tab, select **Using DHCP** in the **Configure IPv4** dropdown list.
4. Click **Apply Now** when done.

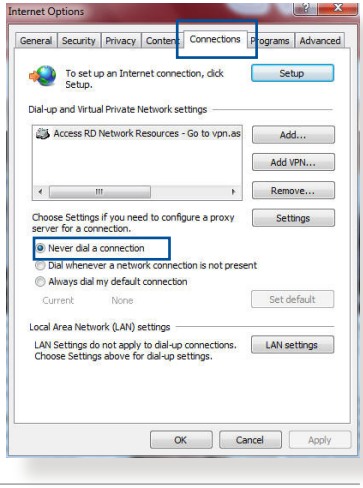


NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

C. Disable the dial-up connection, if enabled.

Windows®

1. Click **Start** > **Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections** tab.
3. Tick **Never dial a connection**.
4. Click **OK** when done.



NOTE: Refer to your browser's help feature for details on disabling the dial-up connection.

Appendices

Service and Support

Visit our multi-language website at https://www.asus.com/support.