

E23420



REPUBLIC OF
GAMERS

USER MANUAL

GT-AX11000

ROG Rapture Tri-band Gaming Router

ASUS

E23420

Revised Edition v3

March 2024

Copyright © 2024 ASUSTeK Computer Inc. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Table of contents

1	Getting to know your wireless router	
1.1	Welcome!	7
1.2	Package contents	7
1.3	Your wireless router	8
1.4	Positioning your router	10
1.5	Setup Requirements	11
2	Getting started	
2.1	Router Setup	12
	A. Wired connection	13
	B. Wireless connection	14
2.2	Quick Internet Setup (QIS) with Auto-detection	16
2.3	Connecting to your wireless network	19
3	Configuring the General and Advanced Settings of ROG Gaming Center	
3.1	Logging into the Web GUI	20
3.2	Administration	22
	3.2.1 Operation Mode	22
	3.2.2 System	23
	3.2.3 Firmware Upgrade	24
	3.2.4 Restore/Save/Upload Setting	24
3.3	AiCloud 2.0	25
	3.3.1 Cloud Disk	26
	3.3.2 Smart Access	28
	3.3.3 AiCloud Sync	29

Table of contents

3.4	Aiprotection Pro	30
3.4.1	Configuring Aiprotection Pro	31
3.4.2	Blocking Malicious Sites	33
3.4.3	Two-Way IPS.....	34
3.4.4	Infected Device Prevention and Blocking.....	35
3.4.5	Setting up Parental Control.....	36
3.5	Dash Board	39
3.6	Firewall.....	42
3.6.1	General.....	42
3.6.2	URL Filter	43
3.6.3	Keyword filter	44
3.6.4	Network Services Filter	45
3.6.5	IPv6 Firewall	46
3.7	Game Boost.....	47
3.7.1	QoS.....	48
3.7.2	Web History.....	49
3.8	Game Private Network.....	50
3.9	Game Profile.....	52
3.10	Game Radar.....	54
3.11	Guest Network	56
3.12	IPv6.....	58
3.13	LAN.....	59
3.13.1	LAN IP	59
3.13.2	DHCP Server.....	60
3.13.3	Route	62
3.13.4	IPTV	63

Table of contents

3.14	Network Map	64
	3.14.1 Setting up the wireless security settings.....	65
	3.14.2 Managing your network clients.....	66
	3.14.3 Monitoring your USB device	68
	3.14.4 ASUS AiMesh	70
3.15	Smart Connect	76
	3.15.1 Setting up Smart Connect	76
	3.15.2 Smart Connect Rule	77
3.16	System Log	80
3.17	Traffic Analyzer	81
3.18	USB Application	82
	3.18.1 Using AiDisk.....	83
	3.18.2 Using Servers Center.....	85
	3.18.3 3G/4G	90
3.19	VPN	91
	3.19.1 VPN Fusion.....	92
3.20	WAN	94
	3.20.1 Internet Connection.....	94
	3.20.2 Dual WAN	97
	3.20.3 Port Trigger.....	98
	3.20.4 Virtual Server/Port Forwarding	100
	3.20.5 DMZ.....	103
	3.20.6 DDNS	104
	3.20.7 NAT Passthrough.....	105
3.21	Wireless	106
	3.21.1 General.....	106
	3.21.2 WPS	108
	3.21.3 Bridge.....	110
	3.21.4 Wireless MAC Filter	112
	3.21.5 RADIUS Setting	113
	3.21.6 Professional	114

3.22	WiFi Radar	118
	3.22.1 WiFi Site Survey.....	119
	3.22.2 Wireless Channel Statistics	120
	3.8.3 Advanced Troubleshooting.....	120

4 Utilities

4.1	Device Discovery	121
4.2	Firmware Restoration	122
4.3	Setting up your printer server	123
	4.3.1 ASUS EZ Printer Sharing	123
	4.3.2 Using LPR to Share Printer	127
4.4	Download Master.....	132
	4.4.1 Configuring Bit Torrent download settings	133
	4.4.2 NZB settings.....	134

5 Troubleshooting

5.1	Basic Troubleshooting	135
5.2	Frequently Asked Questions (FAQs)	137

Appendices

	Safety Notices.....	155
	Service and Support.....	157

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing ROG Rapture Wireless Router!

The stylish router features 2.4GHz, 5GHz-1 and 5GHz-2 triple bands for an unmatched concurrent wireless HD streaming; SMB server, UPnP AV server, and FTP server for 24/7 file sharing; a capability to handle 300,000 sessions; and the ASUS Green Network Technology, which provides up to 70% power-saving solution.

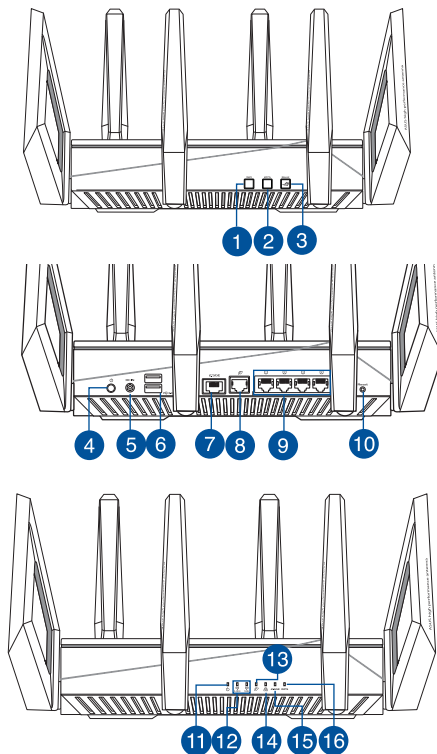
1.2 Package contents

- ROG Rapture gaming router
- AC adapter
- Network cable (RJ-45)
- Quick Start Guide

NOTES:

- If any of the items is damaged or missing, contact ASUS for technical inquiries and support. Refer to **Service and Support** 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



-
- 1 Wi-Fi On/Off button**
Press this button to turn on /off the Wi-Fi connection.

 - 2 WPS button**
This button launches the WPS Wizard.

 - 3 Boost Key**
Press this button to turn on/off LED, DFS channel, Aura RGB and Game Boost.

 - 4 Power button**
Press this button to power on or off the system.

 - 5 Power (DCIN) port**
Insert the bundled AC adapter into this port and connect your router to a power source.

 - 6 USB 3.0 port**
Insert USB 3.0 devices such as USB hard disks or USB flash drives into this port.

 - 7 2.5G Gaming port**
Connect network cables into these ports to prioritize the packets.
-

8	WAN (Internet) port Connect a network cable into this port to establish WAN connection.
9	LAN ports Connect network cables into these ports to establish LAN connection.
10	Reset button This button resets or restores the system to its factory default settings.
11	Power LED Off: No power. On: Device is ready. Flashing slow: Rescue mode.
12	2.4GHz / 5GHz Wi-Fi LED Off: No 2.4GHz / 5GHz signal. On: Wireless system is ready. Flashing: Transmitting or receiving data via wireless connection.
13	WAN (Internet) LED Red: No IP or no physical connection. On: Has physical connection to a wide area network (WAN).
14	LAN LED Off: No power or no physical connection. On: Has physical connection to a local area network (LAN).
15	2.5G Gaming port LED Off: No 2.5G gaming port connection. On: Has physical connection to 2.5G gaming port.
16	WPS LED Off: WPS verification process is off or completed. Flashing: WPS verification process is activated.

NOTES:

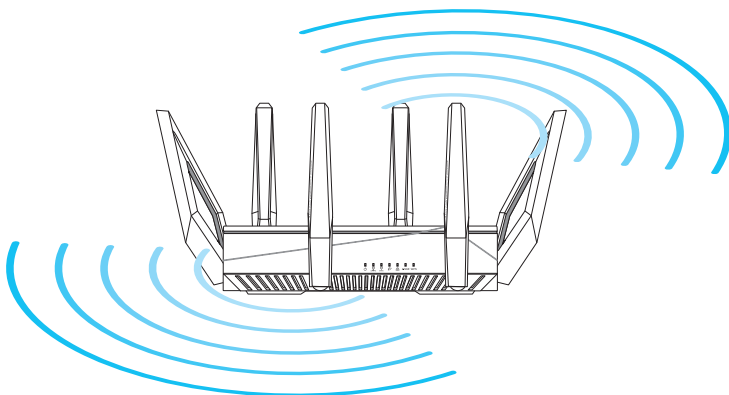
- Use only the adapter that came with your package. Using other adapters may damage the device.
- **Specifications:**

DC Power adapter	DC Output: +19V with max 3.42A current		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

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.
- To ensure the best wireless signal, orient the six detachable antennas as shown in the drawing below.



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 triple band technology, your wireless router supports 2.4GHz, 5GHz-1 and 5GHz-2 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.

IMPORTANT!

- Some wireless adapters might have connectivity issues to 802.11ax WiFi APs.
- If you're experiencing such issue, please ensure you update the driver to the latest version. Check your manufacturer's official support site where software drivers, updates, and other related information can be obtained.
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/>

2 Getting started

2.1 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).
-



WARNING!

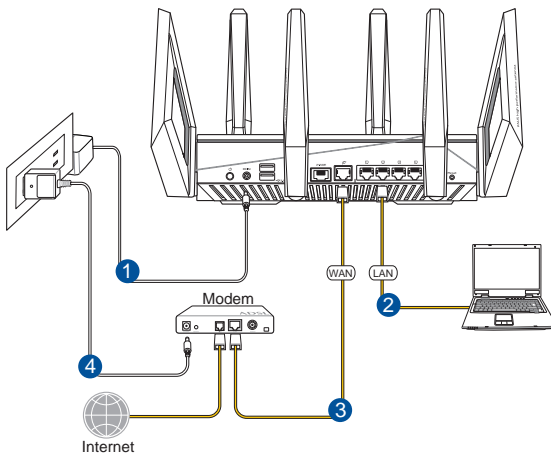
- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
 - If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
 - DO NOT use damaged power cords, accessories, or other peripherals.
 - DO NOT mount this equipment higher than 2 meters.
 - Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
-

A. Wired connection

NOTE: You can use either a straight-through cable or a crossover cable for wired connection.

To set up your wireless router via wired connection:

1. Plug your router into a power outlet and power it on. Connect the network cable from your computer to a LAN port on your router.



2. The web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <http://www.asusrouter.com>
3. Set up a password for your router to prevent unauthorized access.

Login Information Setup

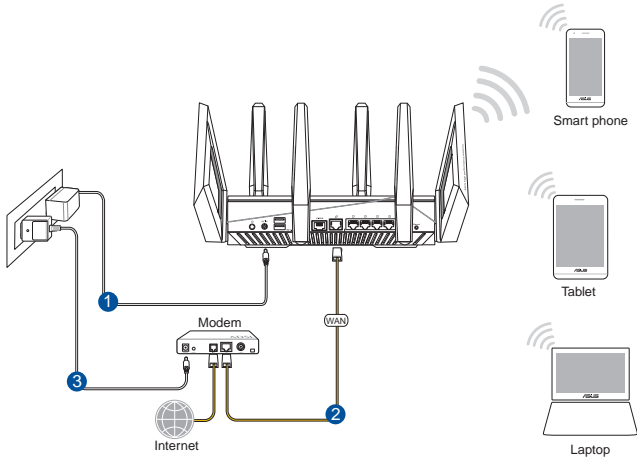
Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name	<input type="text" value="admin"/>
New Password	<input type="password"/>
Retype Password	<input type="password"/> <input type="checkbox"/> Show password

B. Wireless connection

To set up your wireless router via wireless connection:

1. Plug your router into a power outlet and power it on.



2. Connect to the network name(SSID) shown on the product label on the back side of the router. For better network security, change to a unique SSID and assign a password.



2.4G Wi-Fi Name (SSID):	ASUS_XX_2G
5G-1 Wi-Fi Name (SSID):	ASUS_XX_5G
5G-2 Wi-Fi Name (SSID):	ASUS_XX_5G_Gaming

* **XX** refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back of your ROG router.

3. Once connected, the web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <http://www.asusrouter.com>.
4. Set up a password for your router to prevent unauthorized access.

NOTES:

- For details on connecting to a wireless network, refer to the WLAN adapter's user manual.
 - To set up the security settings for your network, refer to the section **Setting up the wireless security settings** in Chapter 3 of this user manual.
-

Login Information Setup

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

Router Login Name

New Password

Retype Password Show password

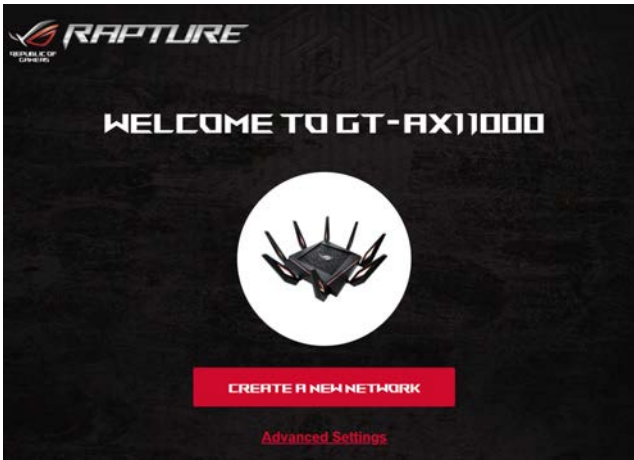
2.2 Quick Internet Setup (QIS) with Auto-detection

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. Launch a web browser. You will be redirected to the ASUS Setup Wizard (Quick Internet Setup). If not, key in <http://www.asusrouter.com> manually.

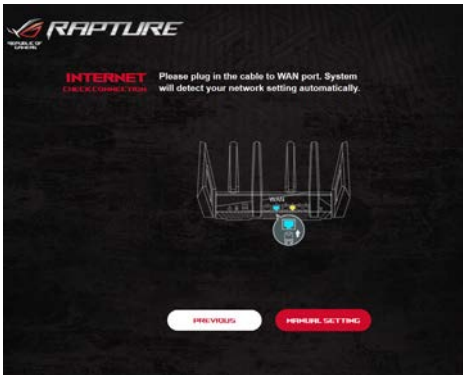


2. The wireless router automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP** and **L2TP**. Key in the necessary information for your ISP connection type.

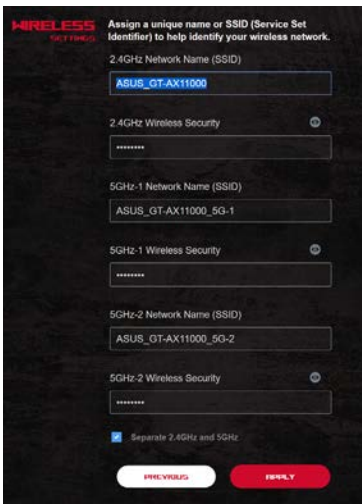
IMPORTANT! Obtain the necessary information from your ISP about the Internet connection type.

NOTES:

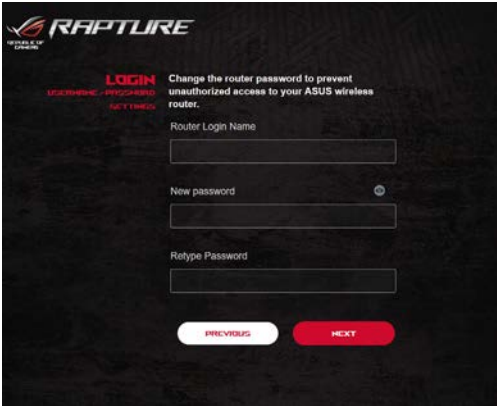
- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
 - If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your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



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



4. On the **Login Information Setup** page, change the router's login password to prevent unauthorized access to your wireless router.





NOTE: 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.

2.3 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 and Advanced Settings of ROG Gaming Center

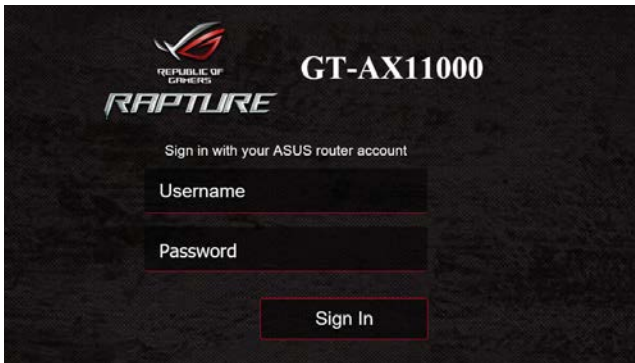
3.1 Logging into the Web GUI

Your ROG Rapture gaming router comes with an intuitive web graphical user interface (GUI) - ROG Gaming Center, which gives you total network control, with need-to-know information such as connected device status and worldwide game-server ping values, and instant access to all the amazing gaming features.

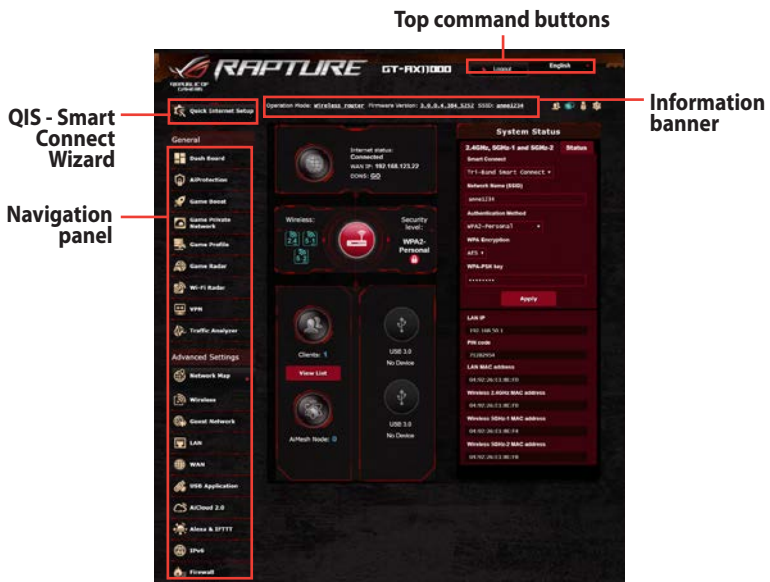
NOTE: The features may vary with different firmware versions.

To log into the web GUI:

1. On your web browser, manually key in the wireless router's default IP address: <http://www.asusrouter.com>.
2. On the login page, key in the user name and password that you have set in **2.2 Quick Internet Setup (QIS) with Auto-dection**.



3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



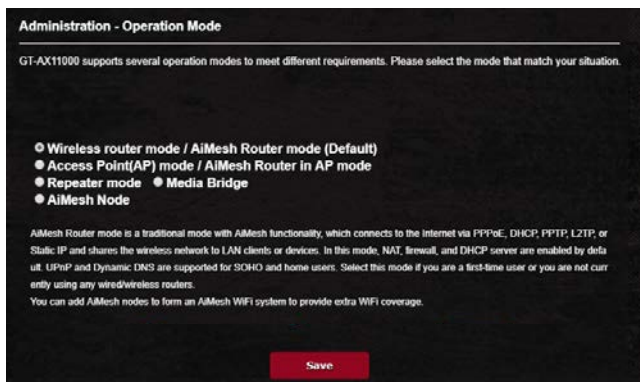
* The image is for reference only.

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.

3.2 Administration

3.2.1 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**.
2. Select any of these operation modes:
 - **Wireless 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.
 - **Media Bridge:** This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via ethernet.
 - **Repeater mode:** In Repeater mode, GT-AX11000 wirelessly connects to an existing wireless network to extend the wireless coverage. In this mode, the firewall, IP sharing, and NAT functions are disabled.
 - **AiMesh mode:** This setup requires at least two ASUS routers which support AiMesh. Enable AiMesh node, and log in AiMesh router web UI to search for available AiMesh nodes

nearby to join your AiMesh system. AiMesh system provides whole-home coverage and centralized management.

3. Click **Apply**.

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

3.2.2 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**.
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.
 - **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.
 - **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 Web Access from WAN:** Select **Yes** to allow devices outside the network to access the wireless router GUI settings. Select **No** to prevent access.
 - **Allow only specified IP address:** Click **Yes** if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
 - **Client List:** Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked **Yes** in the **Only allow specific IP** item.
3. Click **Apply**.

3.2.3 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**.
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 **4.2 Firmware Restoration**.
-

3.2.4 Restore/Save/Upload Setting

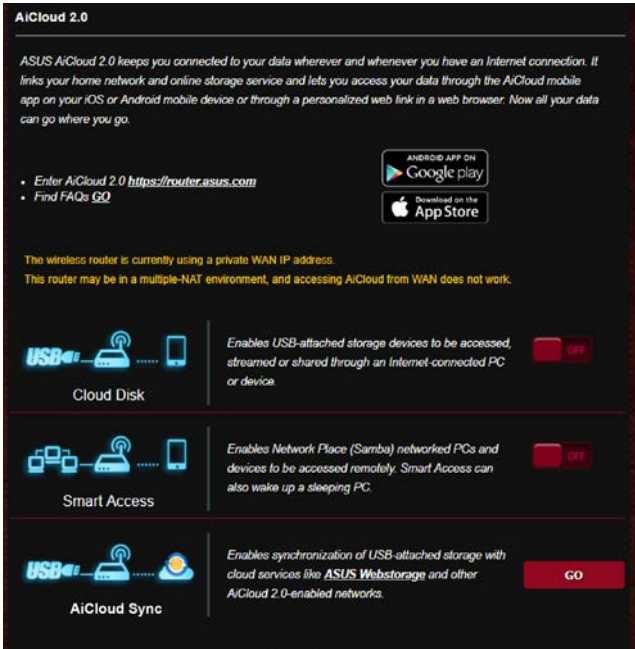
To restore/save/upload wireless router settings:

1. From the navigation panel, go to **Advanced Settings > Administration > Restore/Save/Upload Setting**.
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.

3.3 AiCloud 2.0

AiCloud 2.0 is a cloud service application that allows you to save, sync, share, and access your files.



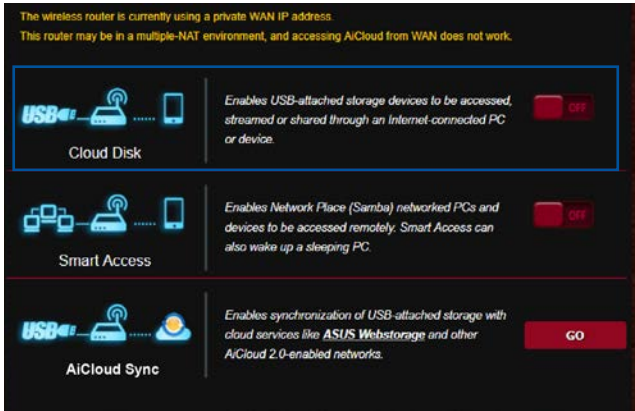
To use AiCloud:

1. From Google Play Store or Apple Store, download and install the ASUS AiCloud app to your smart device.
2. Connect your smart device to your network. Follow the instructions to complete the AiCloud setup process.

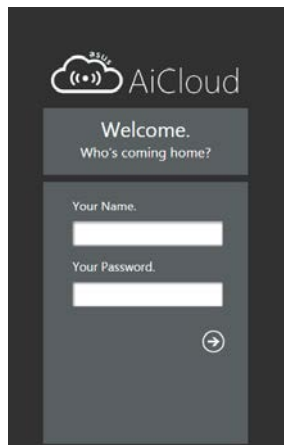
3.3.1 Cloud Disk

To create a cloud disk:

1. Insert a USB storage device into the wireless router.
2. Turn on **Cloud Disk**.



3. Go to <http://www.asusrouter.com> and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.



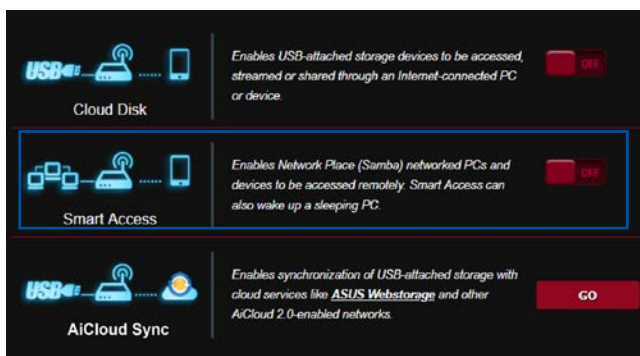
4. You can now start accessing Cloud Disk files on devices connected to the network.

NOTE: When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud for security reason.



3.3.2 Smart Access

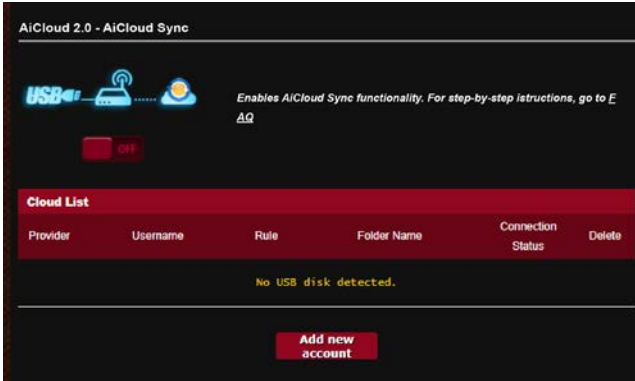
The Smart Access function allows you to easily access your home network via your router's domain name.



NOTES:

- You can create a domain name for your router with ASUS DDNS. For more details, refer to section **3.20.6 DDNS**.
 - By default, AiCloud provides a secure HTTPS connection. Key in [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) for a very secure Cloud Disk and Smart Access usage.
-

3.3.3 AiCloud Sync



To use AiCloud Sync:


1. Launch AiCloud, click **AiCloud Sync** > **Go**.
2. Select **ON** to enable AiCloud Sync.
3. Click **Add new account**.
4. Enter your ASUS WebStorage account password and select the directory that you want to sync with WebStorage.
5. Click **Apply**.

3.4 Aiprotection Pro


Aiprotection Pro provides real-time monitoring that detects malware, spyware, and unwanted access. It also filters unwanted websites and apps and allows you to schedule Internet access time for a connected device.

AiProtection

AiProtection with Trend Micro provides real-time network monitoring to detect malware, viruses, and intrusions before they can reach your PC or device. Parental Controls let you schedule times that a connected device is able to access the Internet. You can also restrict unwanted websites and apps.

 **Network Protection**

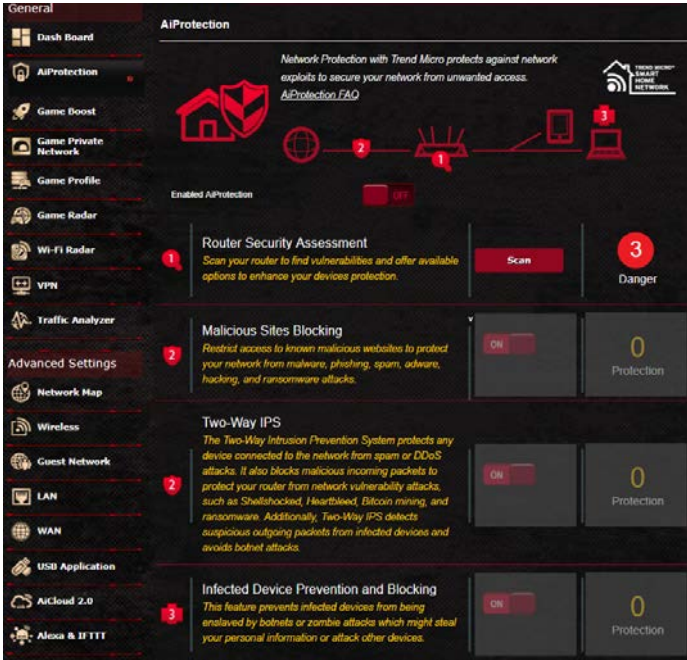
- Router Security Assessment
- Malicious Sites Blocking
- Vulnerability Protection
- Infected Device Prevention and Blocking

 **Parental Controls**

- Time Scheduling
- Web & Apps Filters

3.4.1 Configuring Aiprotection Pro

Aiprotection Pro prevents network exploits and secures your network from unwanted access.



To Configure Aiprotection Pro:

1. From the navigation panel, go to **General > Aiprotection Pro**.
2. From the Aiprotection Pro main page, click **Network Protection**.
3. From the Network Protection tab, click **Scan**.

The search results are displayed on the **Router Security Assessment** page.



IMPORTANT! Items marked with **Yes** on the **Router Security Assessment** page are considered to be safe.

4. (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 to go 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.
5. Click **OK** on the confirmation message.

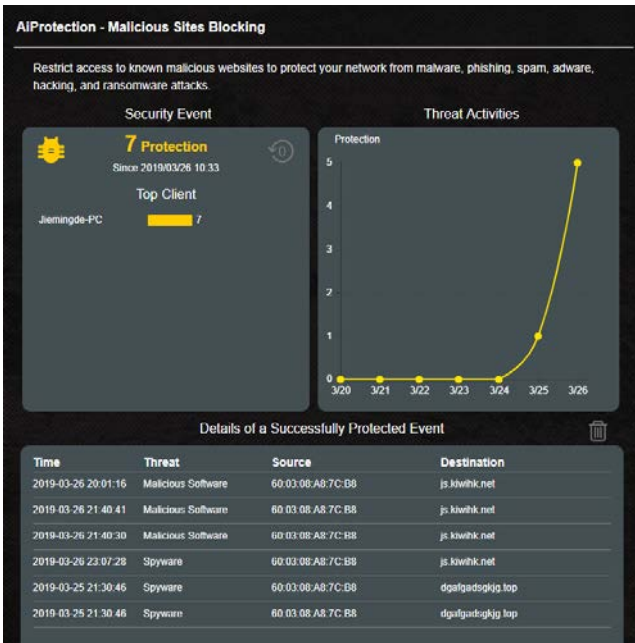
3.4.2 Blocking Malicious Sites

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 Pro**.
2. From the Aiprotection Pro main page, click **Network Protection**.
3. From the Malicious Sites Blocking pane, click **ON**.



3.4.3 Two-Way IPS

This feature resolves common exploits within the router configuration.

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

To enable Two-Way IPS:

1. From the navigation panel, go to **General > Aiprotection Pro**.
2. From the Aiprotection Pro main page, click **Network Protection**.
3. From the Two-Way IPS pane, click **ON**.

AiProtection - 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.

Security Event

7 Protection
Since 2019/03/26 10:33

Top Client

- 00:00:EA:11:9F:63 4
- 00:00:EA:11:A0:DB 2
- 00:00:F1:11:6C:7C 1

Severity Level

Protection High Medium Low

Graph showing severity level over time (3/20 to 3/26). The severity level is low (green) until 3/25, then rises sharply to high (red) on 3/26.

Details of a Successfully Protected Event

Time	Level	Type	Source	Destination	Security Alert
2019-03-26 14:52:20	High	External Attacks	134.209.122.105	36.226.184.39	EXPLOIT Netcore Router Back door Access
2019-03-26 14:25:03	High	External Attacks	185.244.25.231	36.226.184.39	EXPLOIT Remote Command Execution via Shell Script -2
2019-03-26 14:23:41	High	External Attacks	185.244.25.231	36.226.184.39	EXPLOIT Netcore Router Back door Access
2019-03-26 14:20:12	High	External Attacks	159.89.134.126	36.226.184.39	EXPLOIT Remote Command Execution via Shell Script -2
2019-03-26 14:18:25	High	External Attacks	159.89.134.126	36.226.184.39	EXPLOIT Netcore Router Back door Access
2019-03-26 12:44:15	High	External Attacks	185.244.25.231	36.226.184.39	EXPLOIT Remote Command Execution via Shell Script -2
2019-03-26 12:42:52	High	External Attacks	185.244.25.231	36.226.184.39	EXPLOIT Netcore Router Back door Access

3.4.4 Infected Device Prevention and Blocking

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

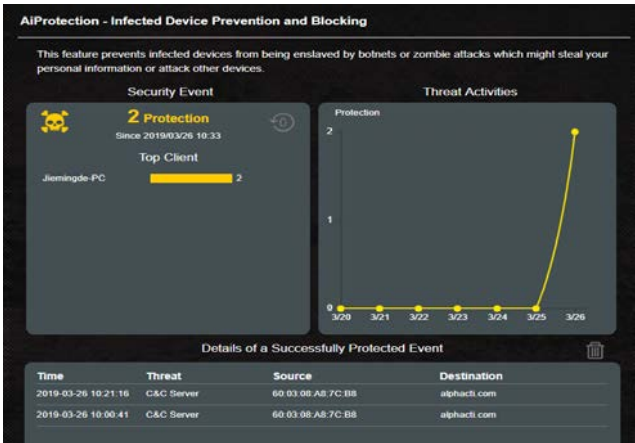
NOTE: This function is automatically enabled if you run the Router Weakness Scan.

To enable infected device prevention and blocking:

1. From the navigation panel, go to **General > Aiprotection Pro**.
2. From the Aiprotection Pro main page, click **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**.



3.4.5 Setting up Parental Control

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

To enable Two-Way IPS:

1. From the navigation panel, go to **General > Aiprotection Pro**.
2. From the Aiprotection Pro main page, click **Parental Controls** tab.

AIProtection - Web & Apps Filters Web & Apps Filters Time Scheduling

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 : 16)

<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input type="checkbox"/>		<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"/>		<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 checked="" type="checkbox"/>	ex: 10:31:0F:89:26:1D	<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"/>		<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	

Web & Apps Filters

Web & Apps Filters is a feature of Parental Controls that allows you to block access to unwanted web sites or applications.

To configure Web & Apps Filters:

1. From the navigation panel, go to **General > Aiprotection Pro**.
2. From the Aiprotection Pro main page, click **Parental Controls** icon to go to the Parental Controls tab.
3. From the **Enable Web & Apps Filters** pane, click **ON**.
4. When the End Users License Agreement (EULA) message prompt appears, click **I agree** to continue.
5. From the **Client List** column, select or key in the client's name from the dropdown list box.
6. From the **Content Category** column, select the filters from the four main categories: **Adult, Instant Message and Communication, P2P and File Transfer**, and **Streaming and Entertainment**.
7. Click  to add the client's profile.
8. Click **Apply** to save the settings.

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.

AiProtection - Time Scheduling Web & Apps Filters Time Scheduling

Time Scheduling allows you to set up time limits for a specific client's network usage:

1. In the [Clients Name] column, select the client whose network usage you want to control. You may also key in the clients MAC address in the [Clients MAC Address] column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In the [Time Management] column, click the edit icon to edit the Active Schedule.
4. Select your time slot with a click. You can hold and drag to extend the duration.
5. Click [OK] to save the settings made.

Note:

1. Clients that are added to Parental Controls will have their internet access restricted by default.
2. Please disable NAT Acceleration for more precise scheduling control.

Enable Time Scheduling **ON**

System Time **Sat, May 05 07:53:34 2018**
*Reminder: The system time has not been synchronized with an NTP server.
*Reminder: The System time zone is different from your locale setting.

Client List (Max Limit : 16)

Client Name (MAC Address)	Time Management	Add / Delete
<input checked="" type="checkbox"/> 08:00:18:31:8F:89:26:E0	-	<input type="button" value="⊕"/>

No data in table.

Apply

To configure Time Scheduling:

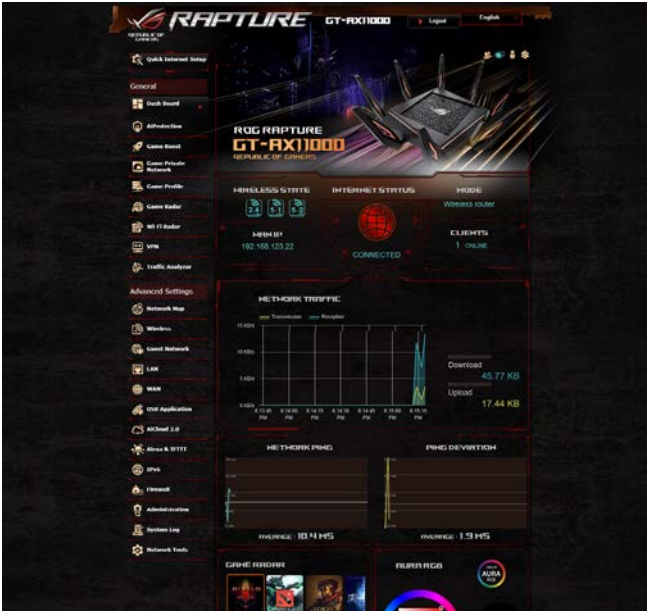
1. From the navigation panel, go to **General > AiProtection Pro > Parental Controls > Time Scheduling**.
2. From the **Enable Time Scheduling** pane, click **ON**.
3. From the **Clients Name** column, select or key in the client's name from the dropdown list box.

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.

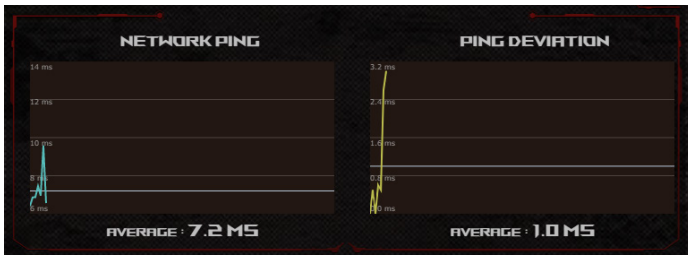
3.5 Dash Board

Dash Board allows you to monitor the real-time traffic for your networking environment and analyze the real-time network ping and ping deviation.

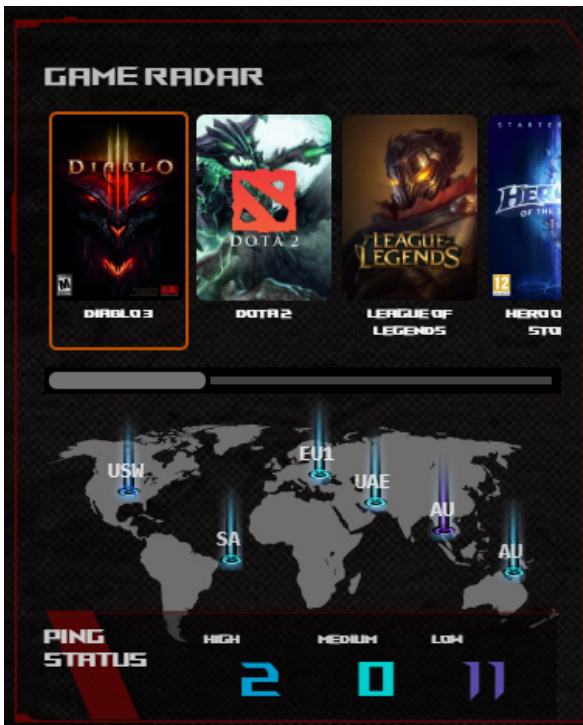


Network ping refers to online game experiences. Higher ping means higher latency for real-time games. For most online games, network ping that is less than 99 ms is considered good quality. If network ping is less than 150 ms, the quality is acceptable. Generally, if network ping is more than 150 ms, it is hard to play game smoothly.

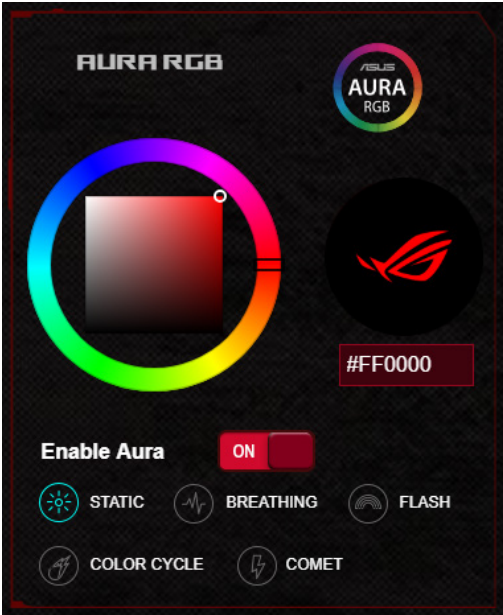
Ping deviation is also highly related with online game experiences. With higher ping deviation, it is much easier causing possible toggle when playing online game. There is no baseline for ping deviation. However, lower ping deviation is better.



- **Game Radar:** Game Radar from Dashboard could give you a quick look about ping time for specific game server.



- **Aura RGB:** Allows users to define or turn on/off the Aura RGB from Dashboard. You can setup any color and choose either of the five lighting patterns.



- **Boost Key:** ROG Rapture gaming router supports Boost Key and allows users to define the functions of Boost Key from Dashboard.
 - LED on/off
 - DFS channel on/off
 - Aura RGB on/off
 - Game Boost: enable/disable prioritizing the gaming packet.



3.6 Firewall

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

NOTE: The Firewall feature is enabled by default.

3.6.1 General

To set up basic Firewall settings:

1. From the navigation panel, go to **Advanced Settings > Firewall > General**.
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**.

3.6.2 URL Filter

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

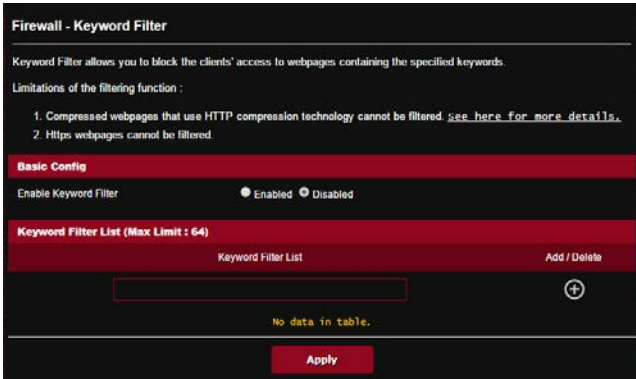
NOTE: The URL Filter is based on a DNS query. If a network client has already accessed a website such as `http://www.abcxxx.com`, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

To set up a URL filter:

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

3.6.3 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**.
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.
-

3.6.4 Network Services Filter

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

Leave the source IP field blank to apply this rule to all LAN devices.

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

White List Duration : During the scheduled duration, clients in the White List can ONLY use the specified network services. After the specified duration, clients in the White List and other network clients will not be able to access the Internet or any Internet service.

NOTE : If you set the subnet for the White 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 **Black List**

Well-Known Applications **User Defined**

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

Time of Day to Enable LAN to WAN Filter 00 : 00 - 23 : 59

Date to Enable LAN to WAN Filter Sat Sun

Time of Day to Enable LAN to WAN Filter 00 : 00 - 23 : 59

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.

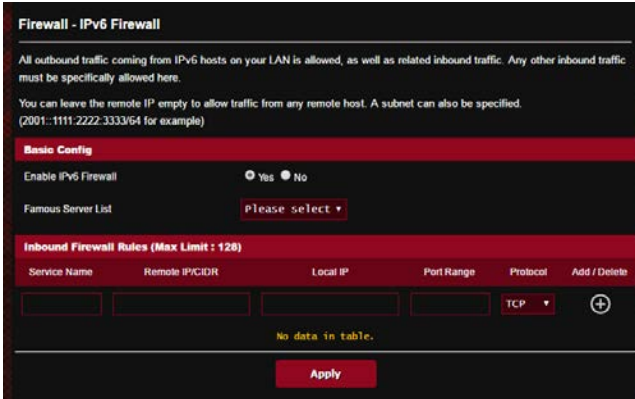
Apply

To set up a Network Service filter:

1. From the navigation panel, go to **Advanced Settings > Firewall > Network Service Filter**.
2. On the **Enable Network Services Filter** field, select **Yes**.
3. Select the Filter table type. **Black List** blocks the specified network services. **White 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**.

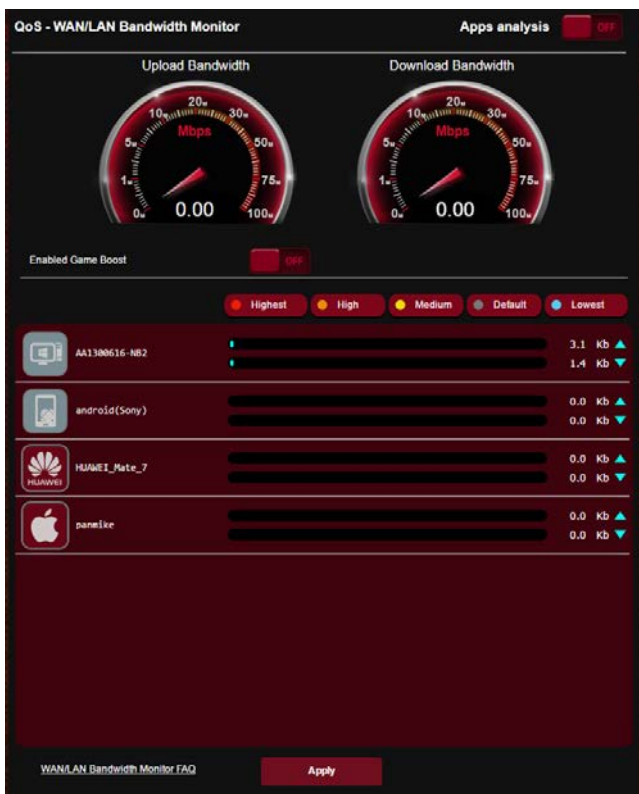
3.6.5 IPv6 Firewall

By default, your ASUS wireless router blocks all unsolicited incoming traffic. The IPv6 Firewall function allows incoming traffic coming from specified services to go through your network.



3.7 Game Boost

This feature allows you to enable Game Boost with one click. When Game Boost is enabled, ROG Rapture gaming router puts the gaming packet as the top priority to provide you with the best gaming experience.



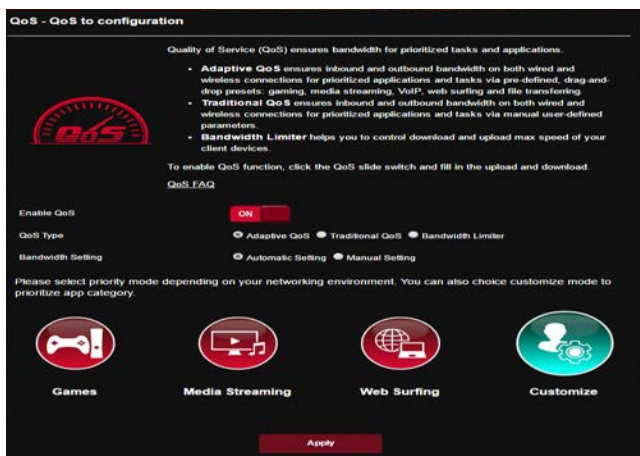
Apps analysis

To enable Apps analysis:

From the **Game Boost** tab, go to the **Apps Analysis** pane, and click **ON**.

3.7.1 QoS

This feature ensures bandwidth for prioritized tasks and apps.



To enable the QoS function:

1. From the navigation panel, go to **General > Game Boost> QoS**.
2. From the **Enable QoS** pane, click **ON**.
3. 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.

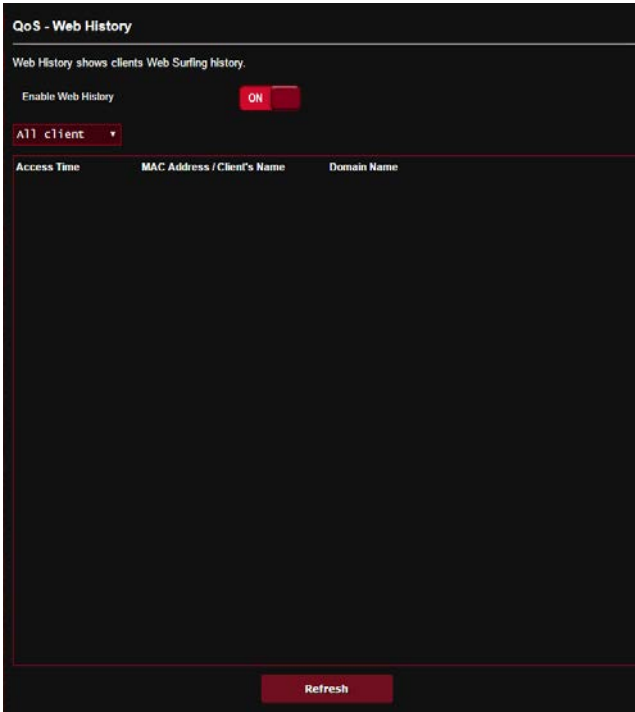
4. Select the QoS Type (Adaptive, Traditional or Bandwidth limiter) for your configuration.

NOTE: Refer to the QoS tab for the definition of the QoS Type.

5. Click **Apply**.

3.7.2 Web History

This feature displays the history and details of the sites or URLs that the client visited.



To view the Web History:

1. From the navigation panel, go to **General > Game Boost> Web History**.
2. (Optional) Click **Refresh** to clear the list.

3.8 Game Private Network

The WtFast-powered Gamers Private Network (GPNTM) reduces your average game latency and helps reduce flux spikes and packet losses with your connection. You can enjoy a faster, smoother, and more responsive connection with virtually all MMO games.



To update the firmware:

1. Launch the web browser and key in <http://www.asusrouter.com>, enter the router’s login name and password to enter ASUSWRT GUI.
2. Go to **Administration > Firmware Upgrade** and click **Check** and follow the onscreen instructions to upgrade the firmware.

You can also download the latest firmware from <http://support.asus.com/ServiceHome.aspx> to upgrade the firmware manually.

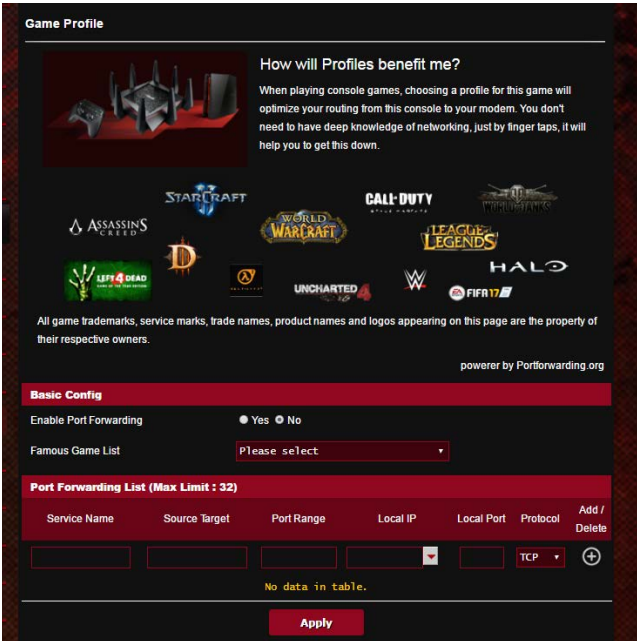
To use WTFast:

1. From the navigation panel, go to **General > Game Boost**.
2. Create a free WTFast account via <https://www.wtfast.com/>.
3. Log into the WTFast account.
4. From the **WTFast Rules** list, create the profile for the device that you want to use WTFast GPN on.
5. Select a GPN server according to your location or select "Auto" and "Apply" settings.
6. Enable GPN profile BEFORE you launch the game.

NOTE: Free account supports one device, if you would like to upgrade to multiple devices, click **Upgrade** to make subscription.

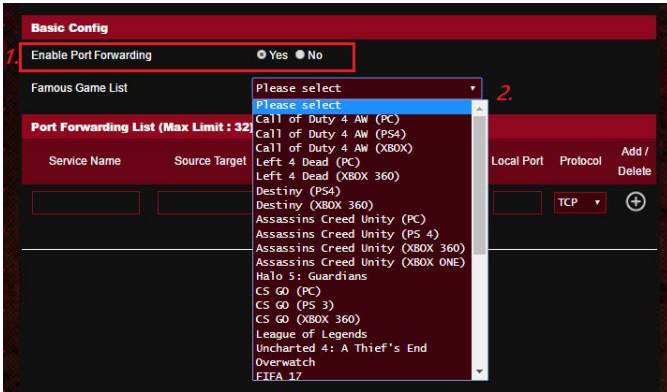
3.9 Game Profile


When playing PC or console games, there may be some connection issues due to the ISP or router settings in your environment such as NAT and port blocks. Game Profile helps ensure that ROG Rapture gaming router is not blocking the game connection.

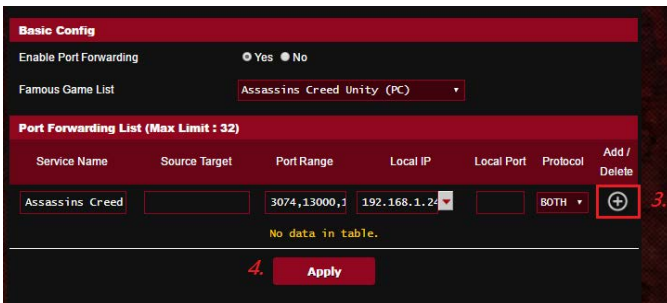


To use Game Profile:

1. From the navigation panel, go to **General > Game Profile** and tick **Yes** to enable port forwarding.
2. Choose a game from **Famous Game List**, which will be updated from time to time.



3. Click  to add the game.
4. Click **Apply** to apply all the profiles.



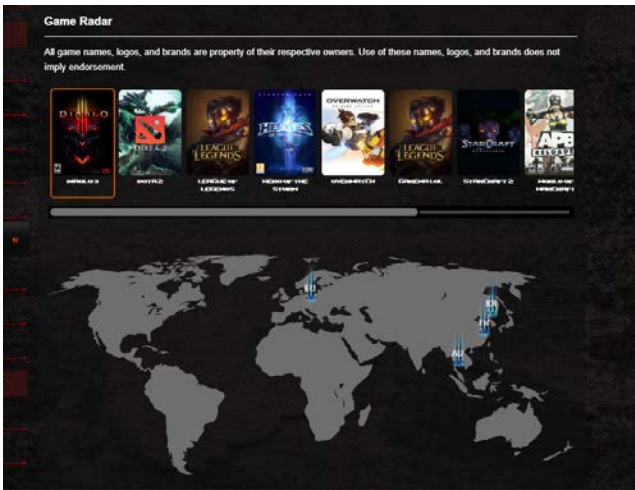
3.10 Game Radar

Game Radar is a diagnostic tool that helps you identify the connection quality of servers for specific games.



To use Game Radar:

1. From the navigation panel, go to **General > Game Radar** and select a game from the game list.



2. Check the **Ping Status** of each server.
3. For a smooth online gaming experience, select a game server with low ping status.

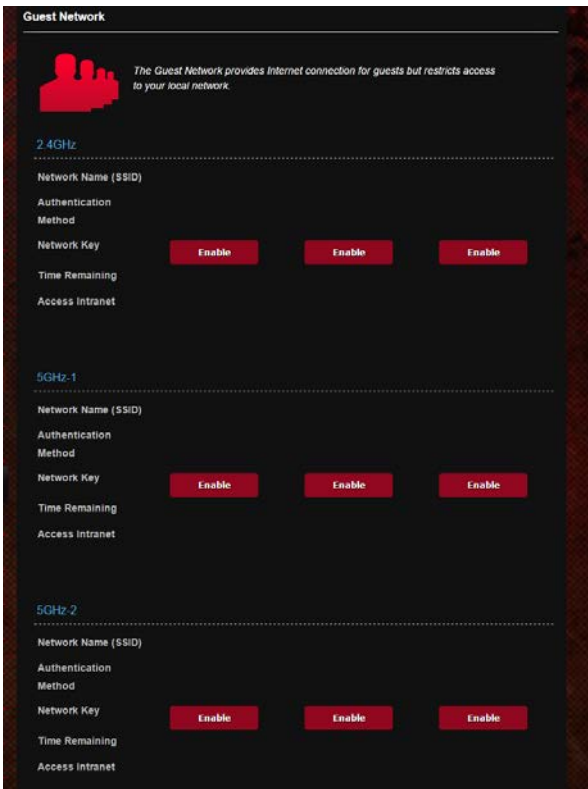
3.11 Guest Network

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

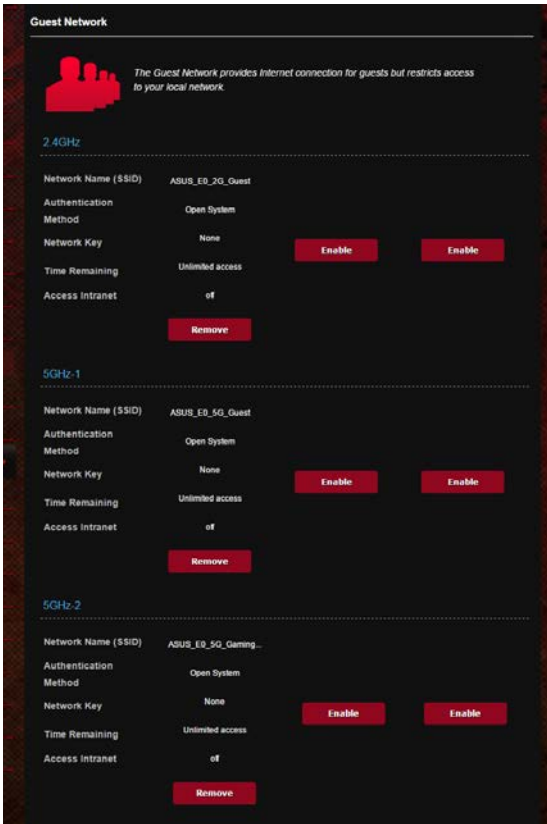
NOTE: GT-AX11000 supports up to nine SSIDs (three 2.4GHz, three 5GHz-1 and three 5GHz-2).

To create a guest network:

1. From the navigation panel, go to **Advanced Settings > 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**.



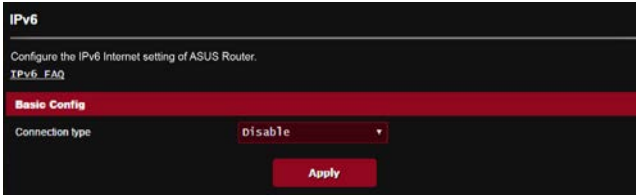
- To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
- Assign a wireless name for your temporary network on the Network Name (SSID) field.



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

3.12 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**.

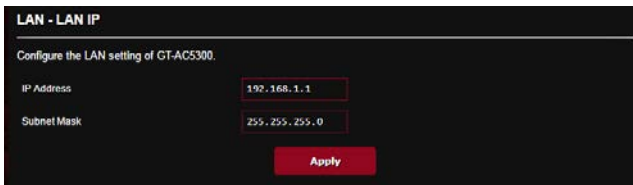
NOTE: Please refer to your ISP regarding specific IPv6 information for your Internet service.

3.13 LAN

3.13.1 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.



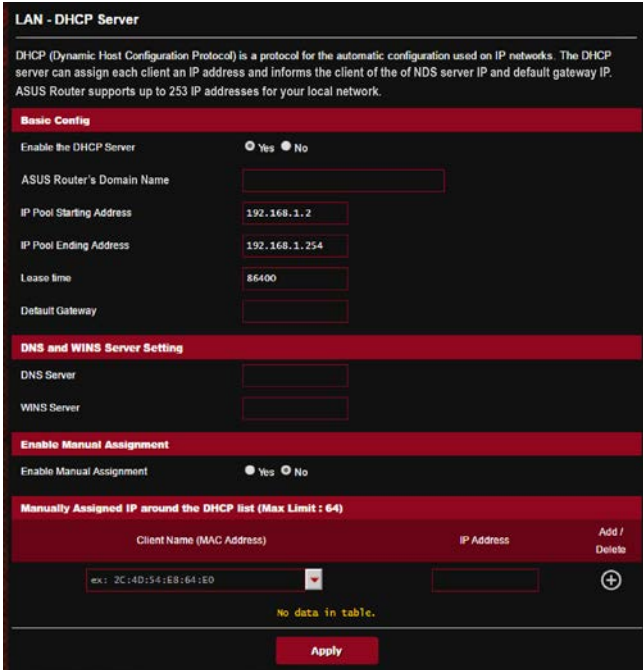
The screenshot shows a configuration page titled "LAN - LAN IP" for a "GT-AC5300" device. The page instructs the user to "Configure the LAN setting of GT-AC5300." There are two input fields: "IP Address" with the value "192.168.1.1" and "Subnet Mask" with the value "255.255.255.0". A red "Apply" button is located at the bottom right of the form.

To modify the LAN IP settings:

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

3.13.2 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**.
2. In the **Enable the DHCP Server** field, tick **Yes**.
3. In the **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:

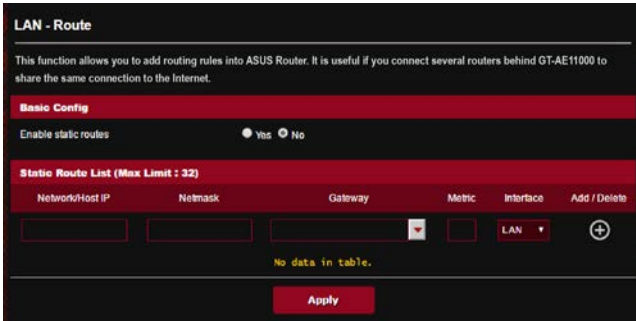
- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.

-
7. In the **DNS and WINS Server Settings** section, 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.



3.13.3 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**.
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**.

3.13.4 IPTV

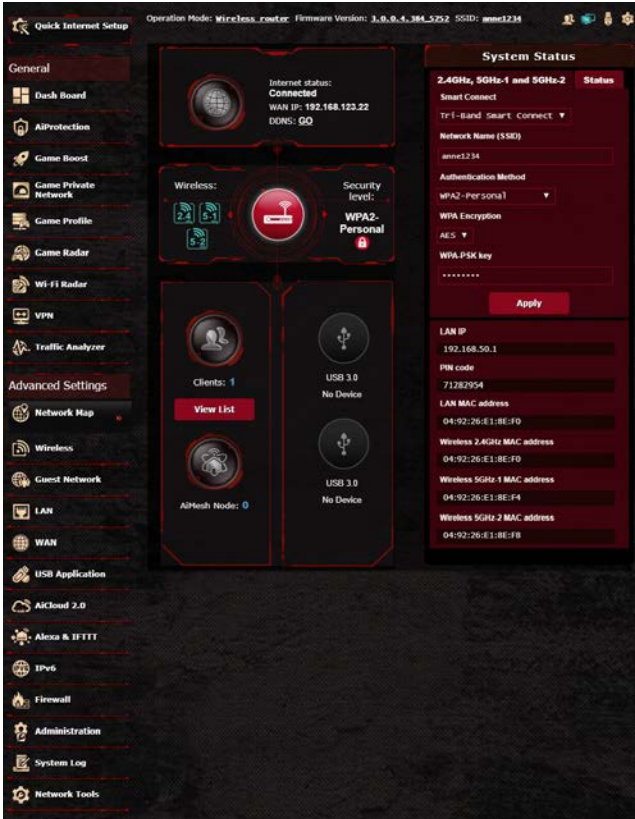
The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.

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 is a red header 'LAN Port'. The main configuration area is divided into two sections: 'IPTV/VoIP Port Settings' and 'Special Applications'. In the 'IPTV/VoIP Port Settings' section, there are three rows: 'LAN1/ LAN2' with a dropdown menu, 'Select ISP Profile' with a dropdown menu set to 'None', and 'Choose IPTV STB Port' with a dropdown menu set to 'None'. A yellow note states: 'Gaming Ports are set up in LAN1 and LAN2. If you would like to use Gaming Ports, please choose LAN 5/LAN 6 for your IPTV or VoIP port.' The 'Special Applications' section contains four rows: 'Use DHCP routes' with a dropdown menu set to 'Microsoft', 'Enable multicast routing (IGMP Proxy)' with a dropdown menu set to 'Disable', 'Enable efficient multicast forwarding (IGMP Snooping)' with a dropdown menu set to 'Disable', and 'UDP Proxy (Udpxy)' with a text input field containing '0'. At the bottom right of the form is a red 'Apply' button.

LAN - IPTV	
To watch IPTV, the WAN port must be connected to the Internet. Please go to WAN - Dual WAN to confirm that WAN port is assigned to primary WAN.	
LAN Port	
IPTV/VoIP Port Settings	LAN1/ LAN2 ▾ <small>Gaming Ports are set up in LAN1 and LAN2. If you would like to use Gaming Ports, please choose LAN 5/LAN 6 for your IPTV or VoIP port.</small>
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾
Special Applications	
Use DHCP routes	Microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
Enable efficient multicast forwarding (IGMP Snooping)	Disable ▾
UDP Proxy (Udpxy)	0
Apply	

3.14 Network Map

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



3.14.1 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 **Advanced Settings** > **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

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Network Name (SSID)
Welcome to test

Authentication Method
WPA2-Personal

WPA Encryption
AES

WPA-PSK key

Apply

5GHz-1 security settings

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Network Name (SSID)
Welcome to test_5G

Authentication Method
WPA2-Personal

WPA Encryption
AES

WPA-PSK key

Apply

5GHz-2 security settings

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Network Name (SSID)
Welcome to test_5G-2

Authentication Method
WPA2-Personal

WPA Encryption
AES

WPA-PSK key

Apply

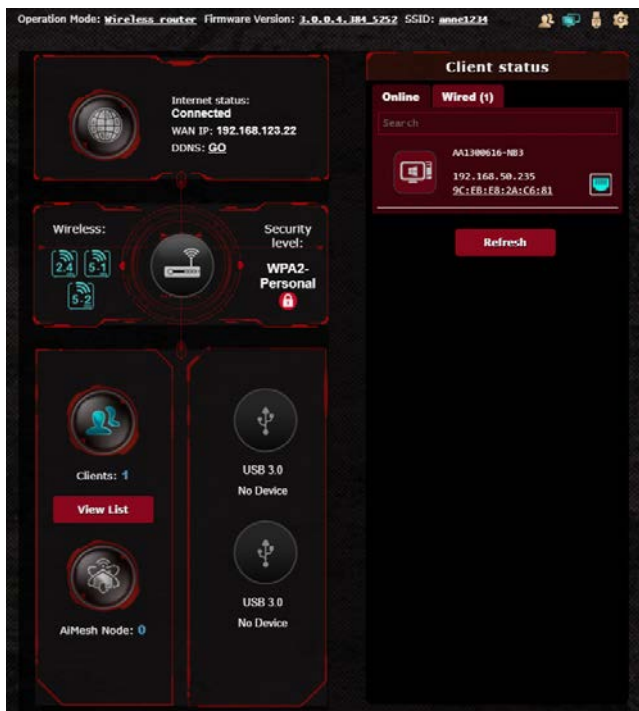
3. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.
4. From the **Authentication Method** dropdown list, select the authentication method for your wireless network.

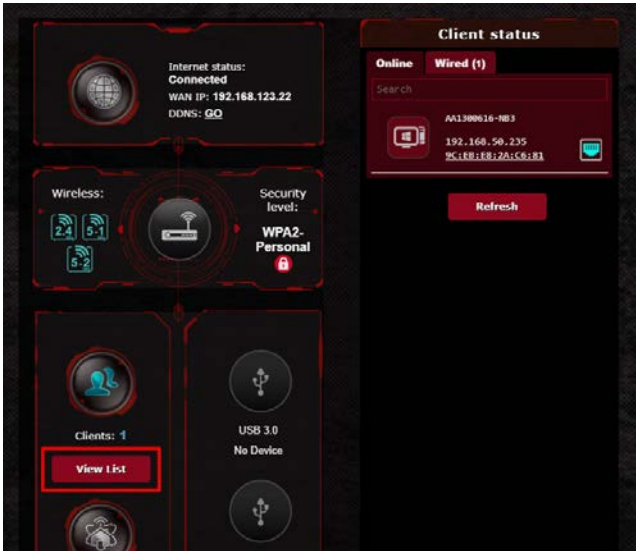
If you select WPA-Personal or WPA-2 Personal as the authentication method, key in the WPA-PSK key or security passkey.

IMPORTANT! The IEEE 802.11n/ac 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 Click **Apply** when done.

3.14.2 Managing your network clients





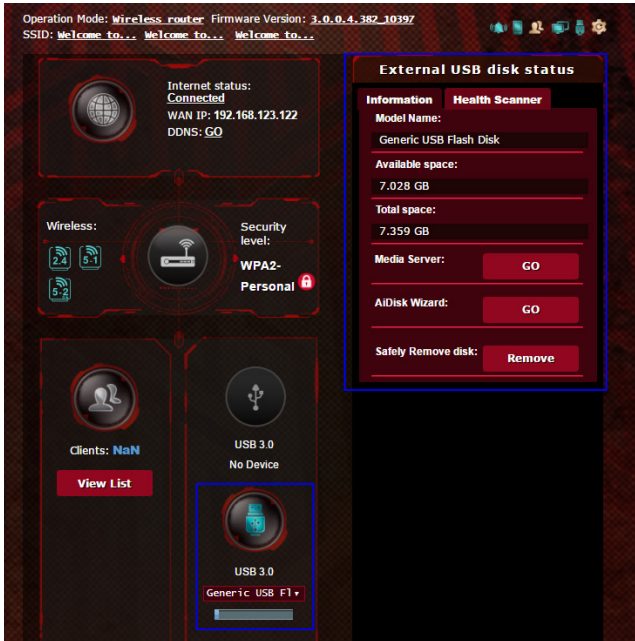
Internet	Icon	Clients Name	Clients IP Address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
🌐	📱	android(Sony)	192.168.1.116	DHCP	A0:E4:53:FC:42:CA	433.3	40.5	02:50:55
🌐	📱	HUAWEI_Mate_7	192.168.1.201	DHCP	E0:19:1D:EC:62:0D	150	13.5	02:31:02
🌐	📱	AA1300616-NB2	192.168.1.240	DHCP	50:46:50:E4:55:B4	-	-	-

To manage your network clients:

1. From the navigation panel, go to **Advanced Settings > Network Map**.
2. On the **Network Map** screen, select the **Clients** icon to display your network client's information.
3. Click View List below the **Clients** icon to display all the clients.
4. To block a client's access to your network, select the client and click the open lock icon.

3.14.3 Monitoring your USB device

The ASUS wireless router provides two USB ports for connecting USB devices or USB printer to allow you to share files and printer with clients in your network.



NOTES:

- To use this feature, you need to plug a USB storage device, such as a USB hard disk or USB flash drive, to the USB 3.0/2.0 ports on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the Plug-n-Share Disk Support List at <http://event.asus.com/networks/disksupport>
- The USB ports support two USB drives or one printer and one USB drive at the same time.

IMPORTANT! You first need to create a share account and its permission /access rights to allow other network clients to access the USB device via an FTP site/third-party FTP client utility, Servers Center, Samba, or AiCloud. For more details, refer to the section **3.18 USB Application** and **3.3 AiCloud 2.0** in this user manual.

To monitor your USB device:

1. From the navigation panel, go to **Advanced Settings > Network Map**.
2. On the Network Map screen, select the **USB Disk Status** icon to display your USB device's information.
3. On the AiDisk Wizard field, click **GO** to set up an FTP server for Internet file sharing.


NOTES:

- For more details, refer to the section **3.18.2 Using Servers Center** in this user manual.
 - The wireless router works with most USB HDDs/Flash disks (up to 4TB size) and supports read-write access for FAT16, FAT32, NTFS, and HFS+.
-

Safely removing the USB disk

IMPORTANT: Incorrect removal of the USB disk may cause data corruption.

To safely remove the USB disk:

1. From the navigation panel, go to **Advanced Settings > Network Map**.
2. In the upper right corner, click  > **Eject USB disk**. When the USB disk is ejected successfully, the USB status shows **Unmounted**.



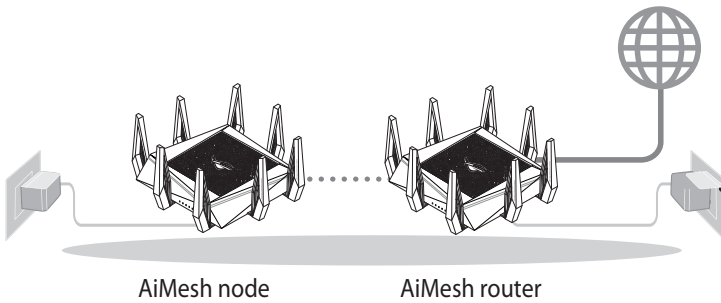
3.14.4 ASUS AiMesh

3.14.4.1 Before setting

Preparing to setup an AiMesh Wi-Fi system

1. Two (2) ASUS routers (models supporting AiMesh: <https://www.asus.com/AiMesh/>).
2. Assign one as AiMesh router, and another one as AiMesh node.

NOTE: If you have multiple AiMesh routers, we recommend using the router with the highest specifications as your AiMesh router and the others as AiMesh nodes.



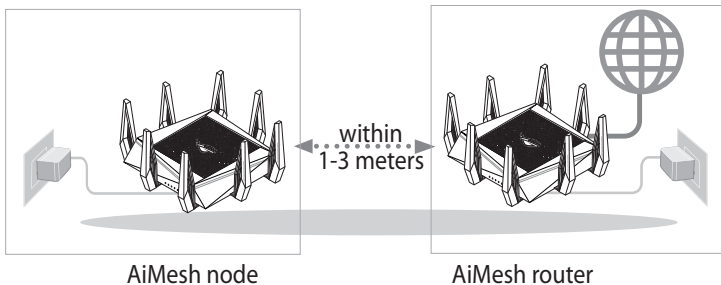
3.14.4.2 AiMesh Setup steps

Prepare

Place your AiMesh router and node within 1-3 meters of each other during the setup process.

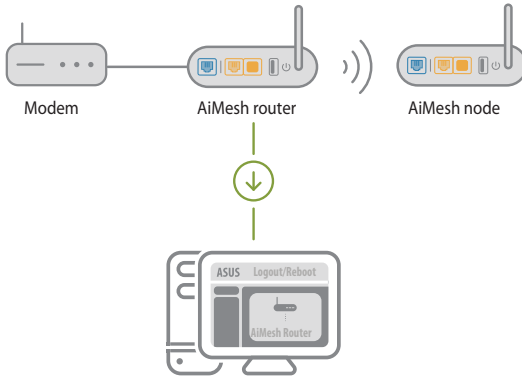
AiMesh node

Factory default status. Keep power on and standby for AiMesh system settings.



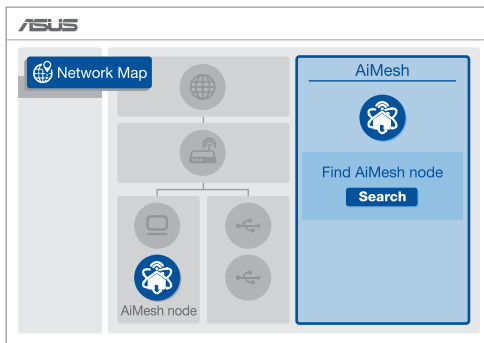
AiMesh router

- 1) Refer to the other router **Quick Start Guide** to connect your AiMesh router to your PC and modem, and then log in into the web GUI.



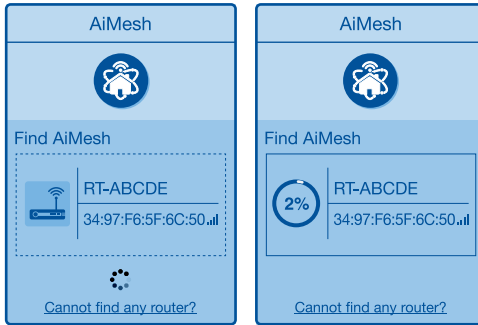
- 2) Go to Network Map page, click AiMesh icon and then Search for your extending AiMesh node.

NOTE: If you cannot find the AiMesh icon here, click on firmware version and update the firmware.

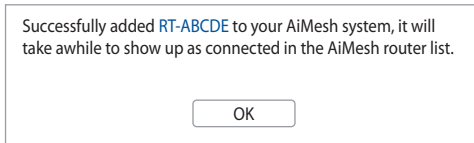


- 3) Click **Search**, it will automatically search for your AiMesh node. When the AiMesh node shows on this page, click it to add it into the AiMesh system.

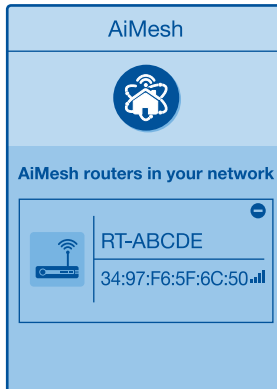
NOTE: If you cannot find any AiMesh node, please go to **TROUBLE SHOOTING**.



- 4) A message is displayed when synchronization is completed.



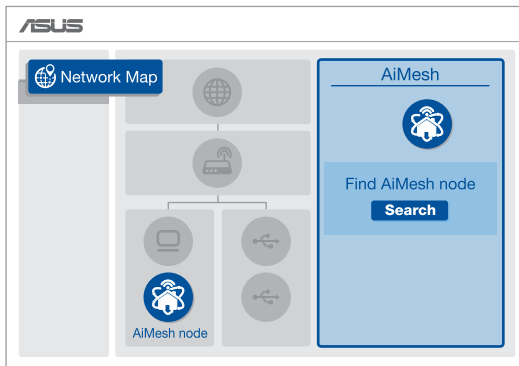
- 5) Congratulations! You will find the pages below show up when an AiMesh node has been successfully added to the AiMesh network.



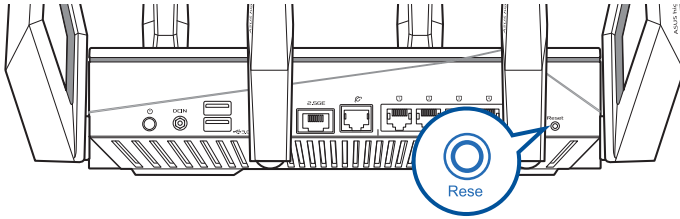
3.14.4.3 Troubleshooting

If your AiMesh router cannot find any AiMesh node nearby or synchronization fails, please check followings and try again.

- 1) Move your AiMesh node closer to the AiMesh router ideally. Ensure it is within 1-3 meters.
- 2) Your AiMesh node is powered on.
- 3) Your AiMesh node is upgraded to AiMesh supported firmware.
 - i. Download AiMesh - supported firmware at:
<https://www.asus.com/AiMesh/>
 - ii. Power on your AiMesh node and connect it to your PC via a network cable.
 - iii. Launch a web GUI. You will be redirected to the ASUS Setup Wizard. If not, navigate to <http://www.asusrouter.com>
 - iv. Go to **Administration > Firmware Upgrade**. Click on **Choose File**, and upload the AiMesh-supported firmware.
 - v. After firmware uploaded, please go to Network Map page to confirm whether AiMesh icon showed up.



- vi. Press the reset button on your AiMesh node for at least 5 seconds. Release the reset button when the power LED is flashing slowly.



3.14.4.4 Relocation

The best performance:

Locate your AiMesh node and router at the best place.

NOTES:

- To minimize interference, keep the routers away from devices like cordless phones, Bluetooth devices and microwave ovens.
- We recommend that you place the routers in an open or spacious location.



3.14.4.5 FAQ (Frequently Asked Questions)

Q1: Does the AiMesh router support Access Point mode?

A: Yes. You can choose to set the AiMesh router as router mode or access point mode. Please go to web GUI (<http://www.asusrouter.com>), and go to the page **Administration > Operation Mode**.

Q2: Could I setup wired connection between AiMesh routers (Ethernet backhaul)?

A: Yes. AiMesh system supports both wireless and wired connection between AiMesh router and node to maximize throughput and stability. AiMesh analyzes the wireless signal strength for each frequency band available, and then determines automatically whether a wireless or wired connection is best to serve as the inter-router connection backbone.

- 1) Follow the setup steps to establish a connection between the AiMesh router and node via Wi-Fi first.
- 2) Place the node in the ideal locations for best coverage. Run an Ethernet cable from the LAN port of the AiMesh router to the WAN port of AiMesh node.



- 3) AiMesh system will auto-select the best path for data transmission, whether wired or wireless.

3.15 Smart Connect

Smart Connect is designed to automatically steer clients to one of three radios (one 2.4 GHz, one lowband 5GHz, one high-band 5GHz) to maximize total wireless throughput use.

3.15.1 Setting up Smart Connect

You can enable Smart Connect from the Web GUI through the following two ways:

- **Via the Wireless screen**

1. On your web browser, manually key in the wireless router's default IP address: <http://www.asusrouter.com>.
2. On the login page, key in the username and password and click **OK**. The QIS page launches automatically.
3. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General**.
4. Move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band for optimal speed.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4GHz
Network Name (SSID)	Welcome to test
Hide SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No
Wireless Mode	AUTO <input type="checkbox"/> Optimized for Xbox <input checked="" type="checkbox"/> Big Protection
Channel bandwidth	20/40 MHz
Control Channel	AUTO Current Control Channel: 5
Extension Channel	AUTO
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	12345678
Protected Management Frames	Disable
Group Key Rotation Interval	3600

Apply

3.15.2 Smart Connect Rule

ASUSWRT provides default condition settings to trigger switching mechanism. You can also change the trigger conditions according to your networking surroundings. To change the settings, go to the **Smart Connect Rule** tab on the Network Tools screen.

Wireless - Smart Connect Rule

Set up the Smart Connect related information below [View List](#)

Steering Trigger Condition

	2.4GHz	5GHz-1	5GHz-2
Enable Load Balance	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
Bandwidth Utilization	<input type="range"/> 0%	<input type="range"/> 80%	<input type="range"/> 0%
RSSI	Greater <input type="text" value="-52"/> dBm	Less <input type="text" value="-82"/> dBm	Less <input type="text" value="-82"/> dBm
PHY Rate Less	<input type="range"/> Disable	<input type="range"/> Disable	<input type="range"/> Disable
PHY Rate Greater	<input type="range"/> > 110 Mbps	<input type="range"/> Disable	<input type="range"/> Disable
VHT	All	All	AC only

STA Selection Policy

RSSI	Greater <input type="text" value="-52"/> dBm	Less <input type="text" value="-82"/> dBm	Less <input type="text" value="-82"/> dBm
PHY Rate Less	<input type="range"/> Disable	<input type="range"/> Disable	<input type="range"/> Disable
PHY Rate Greater	<input type="range"/> > 110 Mbps	<input type="range"/> Disable	<input type="range"/> Disable
VHT	All	not-allowed	AC only

Interface Select and Qualify Procedures

Target Band	1: 5GHz-2 <input type="text"/> 2: 5GHz-1 <input type="text"/>	1: 2.4GHz <input type="text"/> 2: 5GHz-2 <input type="text"/>	1: 2.4GHz <input type="text"/> 2: 5GHz-1 <input type="text"/>
Bandwidth Utilization	<input type="range"/> 0%	<input type="range"/> 60%	<input type="range"/> 0%
VHT	All	All	AC only

Bounce Detect

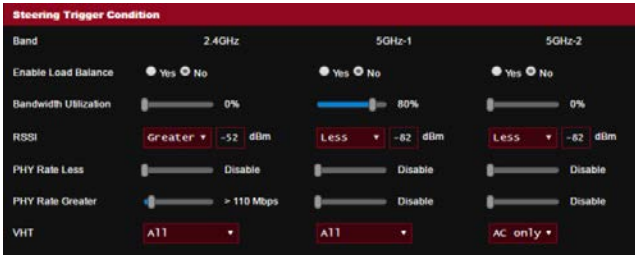
Window Time	<input type="text" value="160"/> seconds
Counts	<input type="text" value="2"/>
Dwell Time	<input type="text" value="3600"/> seconds

Smart Connect Rule controls are divided into four sections:

- Steering Trigger Condition
- STA Selection Policy
- Interface Select and Qualify Procedures
- Bounce Detect

Steering Trigger Condition

This set of controls sets the criteria to initiate band steering.



- **Bandwidth Utilization**

When bandwidth use exceeds this percentage, steering will be initiated.

- **Enable Load Balance**

This controls load balancing.

- **RSSI**

If the received signal level of any associated client meets this criteria, steering will be triggered.

- **PHY Rate Less / PHY Rate Greater**

These controls determine STA link rates that trigger band steering.

- **VHT**

This controls determines how 802.11ac and non-ac clients are handled.

- **ALL** (default) means any type of client can trigger steering.
- **AC only** means a client must support 802.11ac to trigger steering.
- **Not-allowed** means only non-802.11ac clients will trigger steering, i.e. 802.11a/b/g/n.

STA Selection Policy

Once steering has been triggered, ASUSWRT will follow the STA Selection Policy to select a client(STA) that is going to be steered to the most appropriate band.

The screenshot shows the 'STA Selection Policy' configuration panel. It includes three RSSI settings, each with a dropdown menu and a value field: 'Greater' with '-52 dBm', 'Less' with '-82 dBm', and 'Less' with '-82 dBm'. Below these are three 'PHY Rate' settings, each with a slider and a text field: 'Less' with 'Disable', 'Greater' with '> 110 Mbps', and 'Greater' with 'Disable'. At the bottom are three 'VHT' settings with dropdown menus: 'All', 'not-allowed', and 'AC only'.

Interface Select and Qualify Procedures

These controls determine where the steered client will end up. The **Target Band** controls specify first and second choice of steering targets. Clients meeting the STA selection policy criteria for the radio will be steered to the first target if that radio's **Bandwidth Utilization** is less than the set value. Otherwise, the client will be sent to the second **Target Band** radio.

The screenshot shows the 'Interface Select and Qualify Procedures' configuration panel. It features three 'Target Band' settings, each with two dropdown menus: '1: 5GHz-2' and '2: 5GHz-1', '1: 2.4GHz' and '2: 5GHz-2', and '1: 2.4GHz' and '2: 5GHz-1'. Below these are three 'Bandwidth Utilization' sliders, each with a percentage value: '0%', '60%', and '0%'. At the bottom are three 'VHT' settings with dropdown menus: 'All', 'All', and 'AC only'.

Bounce Detect

This set of controls determines how often a client can be steered. This is intended to prevent clients from constantly moving around. It does not, however, prevent clients from disconnecting on their own, or counting them as bounces if they do. Each client can be steered N **Counts** within the **Window Time**. When the Count limit is hit, the client will not be steered again for **Dwell Time**.

The screenshot shows the 'Bounce Detect' configuration panel. It includes three settings: 'Window Time' set to '1.80 seconds', 'Counts' set to '2', and 'Dwell Time' set to '3600 seconds'.

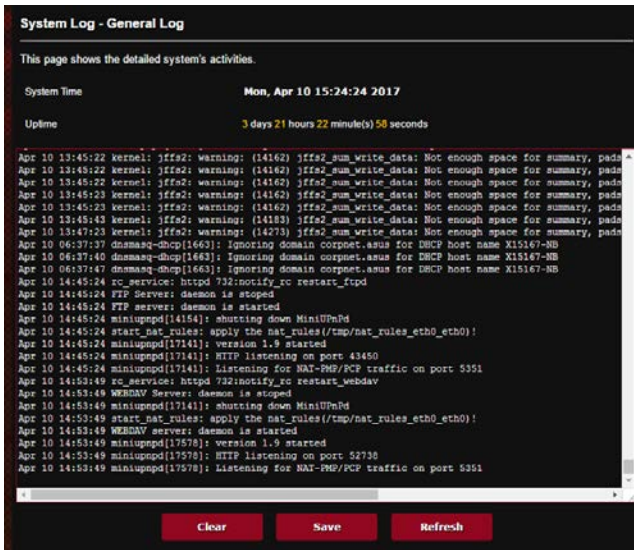
3.16 System Log

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

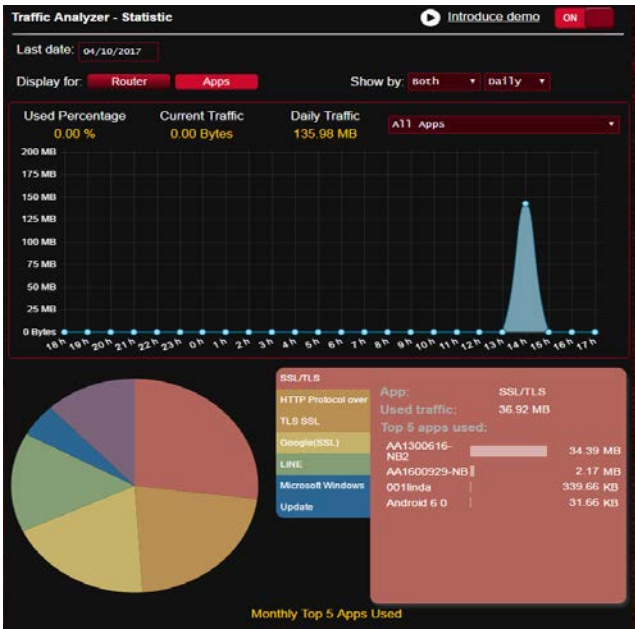


The screenshot displays the 'System Log - General Log' interface. At the top, it states 'This page shows the detailed system's activities.' Below this, the 'System Time' is 'Mon, Apr 10 15:24:24 2017' and the 'Uptime' is '3 days 21 hours 22 minute(s) 50 seconds'. The main area contains a scrollable list of system events with timestamps and descriptions. At the bottom, there are three buttons: 'Clear', 'Save', and 'Refresh'.

```
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:45:43 kernel: jffs2: warning: (14183) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 13:47:23 kernel: jffs2: warning: (14273) jffs2_sum_write_data: Not enough space for summary, padding
Apr 10 06:37:37 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
Apr 10 06:37:40 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
Apr 10 06:37:47 dnsmasq-dhcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
Apr 10 14:45:24 rc_service: httpd 732:notify_rc restart ftpd
Apr 10 14:45:24 FTP Server: daemon is stopped
Apr 10 14:45:24 FTP Server: daemon is started
Apr 10 14:45:24 minisuppd[14154]: shutting down MiniUPnPd
Apr 10 14:45:24 start_nat_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
Apr 10 14:45:24 minisuppd[17141]: version 1.9 started
Apr 10 14:45:24 minisuppd[17141]: HTTP listening on port 13160
Apr 10 14:45:24 minisuppd[17141]: Listening for NAT-PMP/PCP traffic on port 5351
Apr 10 14:53:49 rc_service: httpd 732:notify_rc restart webdav
Apr 10 14:53:49 WEBDAV Server: daemon is stopped
Apr 10 14:53:49 minisuppd[17141]: shutting down MiniUPnPd
Apr 10 14:53:49 start_nat_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
Apr 10 14:53:49 WEBDAV server: daemon is started
Apr 10 14:53:49 minisuppd[17578]: version 1.9 started
Apr 10 14:53:49 minisuppd[17578]: HTTP listening on port 52730
Apr 10 14:53:49 minisuppd[17578]: Listening for NAT-PMP/PCP traffic on port 5351
```


3.17 Traffic Analyzer

Traffic Analyzer gives you an at-a-glance view of what's happening on your network on a daily, weekly, or monthly basis. It lets you to quickly see each user's bandwidth usage or the device or app used, helping you reduce the bottlenecks in your Internet connection. It's also a great way to monitor the users' Internet usage or activities.



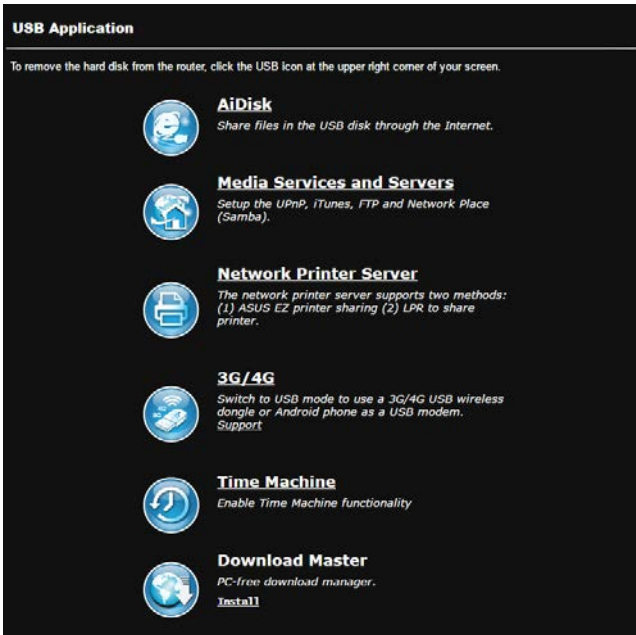
To configure the Traffic analyzer:

1. From the navigation panel, go to **General > Traffic Analyzer**.
2. From the **Traffic Analyzer** main page, turn on traffic analyzer statistic.
3. Select the date whose chart you want to display.
4. On the **Display for** field, select Router or Apps to display the traffic information.
5. On the **Show by** field, select how you want to display the traffic information.

3.18 USB Application







The USB Applications function provides AiDisk, Servers Center, Network Printer Server and Download Master submenus.

IMPORTANT! To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <http://event.asus.com/2009/networks/disksupport/> for the file system support table.



USB Application

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

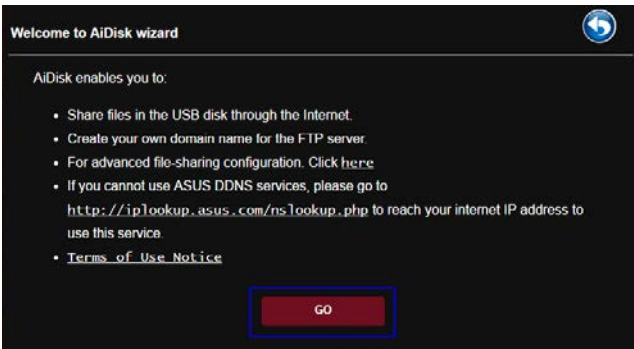
-  **AiDisk**
Share files in the USB disk through the Internet.
-  **Media Services and Servers**
Setup the UPnP, iTunes, FTP and Network Place (Samba).
-  **Network Printer Server**
The network printer server supports two methods: (1) ASUS EZ printer sharing (2) LPR to share printer.
-  **3G/4G**
Switch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

3.18.1 Using AiDisk

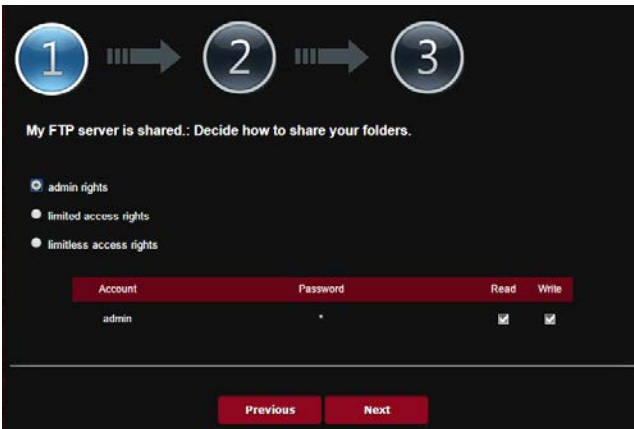
AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

1. From the navigation panel, go to **Advanced Settings > USB application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.



3. Select the access rights that you want to assign to the clients accessing your shared data.



4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select **I will use the service and accept the Terms of service** and key in your domain name. When done, click **Next**.

1 → 2 → 3

Create your domain name via the ASUS DDNS services.

I will use the service

.asuscomm.com

Disable DDNS.

Previous Next

You can also select **Skip ASUS DDNS settings** then click **Next** to skip the DDNS setting.

5. Click **Finish** to complete the setting.
6. To access the FTP site that you created, launch a web browser or a third-party FTP client utility and key in the ftp link (**ftp://<domain name>.asuscomm.com**) you have previously created.

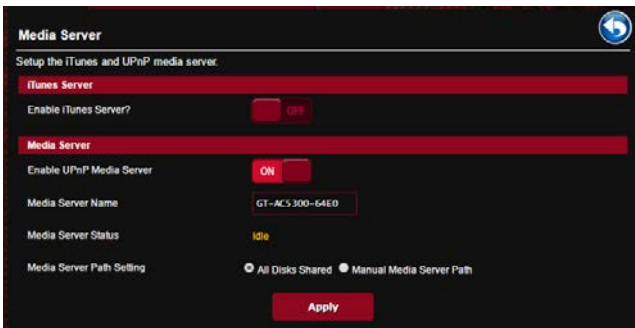
3.18.2 Using Servers Center

Servers Center allows you to share the media files from the USB disk via a Media Server directory, Samba share service, or FTP share service. You can also configure other settings for the USB disk in the Servers Center.

Using Media Server

Your wireless router allows DLNA-supported devices to access multimedia files from the USB disk connected to your wireless router.

NOTE: Before using the DLNA Media Server function, connect your device to the router's network.

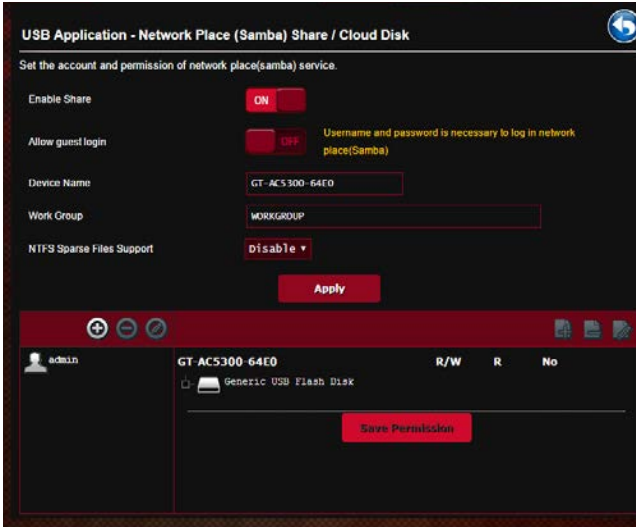


To launch the Media Server setting page, go to **Advanced Settings > USB application > Media Services and Servers > Media Servers**. Refer to the following for the descriptions of the fields:

- **Enable iTunes Server?:** Select ON/OFF to enable/disable the iTunes Server.
- **Enable DLNA Media Server:** Select ON/OFF to enable/disable the DLNA Media Server.
- **Media Server Status:** Displays the status of the media server.
- **Media Server Path Setting:** Select **All Disks Shared** or **Manual Media Server Path**.

Using Network Place (Samba) Share service

Network Place (Samba) Share allows you to set up the accounts and permissions for the Samba service.



To use Samba share:

1. From the navigation panel, go to **Advanced Settings > USB application > Media Services and Servers > Network Place (Samba) Share / Cloud Disk.**

NOTE: Network Place (Samba) Share is enabled by default.


2. Follow the steps below to add, delete, or modify an account.

To create a new account:


- a) Click **+** to add new account.
- b) In the **Account** and **Password** fields, key in the name and password of your network client. Retype the password to confirm. Click **Add** to add the account to the list.

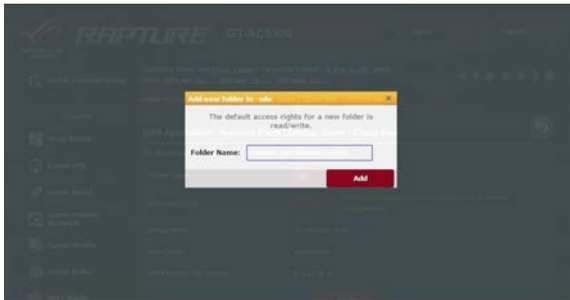


To delete an existing account:

- a) Select the account that you want to delete.
- b) Click .
- c) When prompted, click **Delete** to confirm the account deletion.

To add a folder:

- a) Click .
- b) Enter the folder name, and click **Add**. The folder that you created will be added to the folder list.



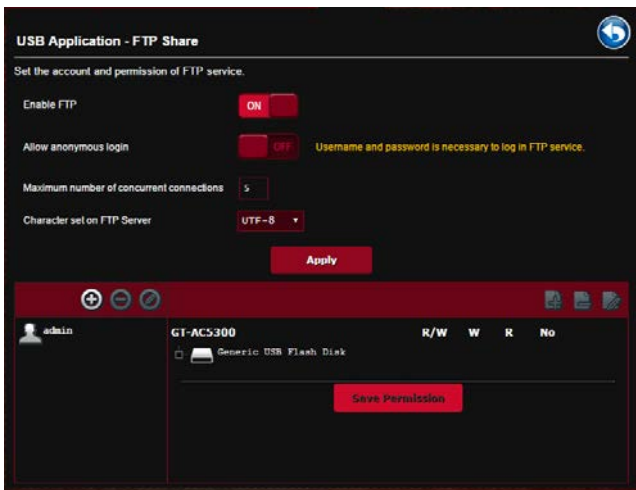
3. From the list of folders, select the type of access permission that you want to assign for specific folders:
 - **R/W**: Select this option to assign read/write access.
 - **R**: Select this option to assign read-only access.
 - **No**: Select this option if you do not want to share a specific file folder.
4. Click **Apply** to apply the changes.

Using the FTP Share service

FTP share enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

IMPORTANT:

- Ensure that you safely remove the USB disk. Incorrect removal of the USB disk may cause data corruption.
 - To safely remove the USB disk, refer to the section **Safely removing the USB disk** under **3.14.3 Monitoring your USB device**.
-



To use FTP Share service:

NOTE: Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.18.1 Using AiDisk**.

1. From the navigation panel, click **Advanced Settings > USB application > Media Services and Servers > FTP Share**.
2. From the list of folders, select the type of access rights that you want to assign for specific folders:
 - **R/W:** Select to assign read/write access for a specific folder.
 - **W:** Select to assign write only access for a specific folder.

- **R:** Select to assign read only access for a specific folder.
 - **No:** Select this option if you do not want to share a specific folder.
3. If you prefer, you can set the **Allow anonymous login** field to **ON**.
 4. In the **Maximum number of concurrent connections** field, key in the number of devices that can simultaneously connect to the FTP share server.
 5. Click **Apply** to confirm the changes.
 6. To access the FTP server, key in the ftp link **ftp://<hostname>.asuscomm.com** and your user name and password on a web browser or a third-party FTP utility.

3.18.3 3G/4G

3G/4G USB modems can be connected to the router to allow Internet access.

NOTE: For a list of verified USB modems, please visit:
<http://event.asus.com/2009/networks/3gsupport/>

To set up 3G/4G internet access:

1. From the navigation panel, click **Advanced Settings > USB application > 3G/4G**.
 2. In the **Enable USB Modem** field, select **Yes**.
 3. Set up the following:
 - **Location:** Select your 3G/4G service provider's location from the dropdown list.
 - **ISP:** Select your Internet Service Provider (ISP) from the dropdown list.
 - **APN (Access Point Name) service (optional):** Contact your 3G/4G service provider for detailed information.
 - **Dial Number and PIN code:** The 3G/4G provider's access number and PIN code for connection.
-

NOTE: PIN code may vary from different providers.

- **Username / Password:** The username and password will be provided by the 3G/4G network carrier.
 - **USB Adapter:** Choose your USB 3G / 4G adapter from the dropdown list. If you are not sure of your USB adapter's model or the model is not listed in the options, select **Auto**.
4. Click **Apply**.
-

NOTE: The router will reboot for the settings to take effect.

3.19 VPN

A virtual private network (VPN) provides a secure communication with a remote computer or network over a public network such as the Internet.

NOTE: Before setting up a VPN connection, you would need the IP address or domain name of the VPN server.

VPN Server - PPTP PPTP OpenVPN IPSec VPN

The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x or 172.16.x.x). Please refer to the [FAQ](#) and set up the port forwarding.

Basic Config

Enable PPTP VPN Server ON

VPN Details: General

Network Place (Samba) Support Yes No

The VPN server allows you to access your home network anytime, anywhere.

To use the VPN server. Please follow these steps.

- (1) Enable the PPTP VPN server
- (2) Set the IP pool for client IP. (Maximum 10 clients)
- (3) Set up the username and password for VPN client.
- (4) Open the VPN connection program on your computer or smartphone.
- (5) Add a new PPTP VPN connection and the VPN server address is 192.168.123.22
- (6) If your WAN IP address is dynamic, please [click here](#) to set the DNS.
- (7) If you cannot use ASUS DNS services, please go to <http://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

• [VPN_SERVER_FAQ](#)


Username and Password (Max Limit : 16)

Connection Status	Username	Password	Add / Delete	Edit
-			+	-

No data in table.

Apply

To set up access to a VPN server:

1. From the navigation panel, go to **General > VPN**.
2. On the **Enable PPTP VPN Server** field, select **ON**.
3. On the **VPN Details** dropdown list, select **Advanced Settings** to configure the advanced VPN settings such as broadcast support, authentication, MPPE Encryption, and Client IP address range.
4. On the **Network Place (Samba) Support** field, select **Yes**.
5. Enter the user name and password for accessing the VPN server. Click .
6. Click **Apply**.


3.19.1 VPN Fusion

VPN Fusion allows you to connect to multiple VPN servers simultaneously and assign your client devices to connect to different VPN tunnels. Some devices like set-top boxes, smart TVs and Blu-ray players do not support VPN software. This feature provides VPN access to such devices in a home network without having to install VPN software, while your smartphone remains connected to Internet not VPN. For Gamer, VPN connection counteracts DDoS attacks to prevent your PC game or your stream from disconnecting with game servers. Building a VPN connection also can simply change your IP address to the region where the game server is located, to improve your ping time to game servers.



To start, please follow the steps below:


1. Click the "+" button beside **Server List** to add a new VPN tunnel.
2. Activate the VPN connection you created in Server List.
3. Click the "+" button beside **Exception List** and select the online client you want to configure.
4. Assign a VPN connection to the client device, and click **OK**.
5. Activate the VPN policy in **Exception List**, and click **Apply** at the bottom of the page.

Server List (Max Limit : 16) 

Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.

Default	Status	Connection Name	VPN type	Activate	Editor
<input checked="" type="radio"/>	Connected		Internet		

No data in table.

Exception List (Max Limit : 64) 

You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.

Client Name (MAC Address)	IP Address	Connection Name	Activate	Delete
---------------------------	------------	-----------------	----------	--------

No data in table.

Apply

3.20 WAN

3.20.1 Internet Connection

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

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: Yes No

Enable NAT: Yes No

Enable UPnP: Yes No (UPnP_FAQ)

WAN DNS Setting

Connect to DNS Server automatically: Yes No

Account Settings

Authentication: None ▾

Host-Unix (Hexadecimal):

Special Requirement from ISP

Host Name:

MAC Address: **MAC Clone**

DHCP query frequency: Aggressive Mode ▾

Extend the TTL value: Yes No

Spool LAN TTL value: Yes No

Apply

To configure the WAN connection settings:

1. From the navigation panel, go to **Advanced Settings > WAN > Internet Connection**.
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 **static 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.
- **DHCP query frequency:** Changes the DHCP Discovery interval settings to avoid overloading the DHCP server.

3.20.2 Dual WAN

Your ASUS wireless router provides dual WAN support. You can set the dual WAN feature to any of these two modes:

- **Failover Mode:** Select this mode to use the secondary WAN as the backup network access.
- **Load Balance Mode:** Select this mode to optimize bandwidth, minimize response time and prevent data overload for both primary and secondary WAN connections.

The screenshot shows the 'WAN - Dual WAN' configuration page. At the top, there is a header 'WAN - Dual WAN' and a descriptive paragraph: 'ASUS Router 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 connection.'

The page is divided into two main sections: 'Basic Config' and 'Auto Network Detection'.

Basic Config

- Enable Dual WAN:** A red toggle switch is set to 'ON'.
- Primary WAN:** A dropdown menu is set to 'WAN'.
- Secondary WAN:** A dropdown menu is set to 'USB'.
- Dual WAN Mode:** A dropdown menu is set to 'Fail Over'. To its right, there is a checkbox labeled 'Allow fallback' which is checked.

Auto Network Detection

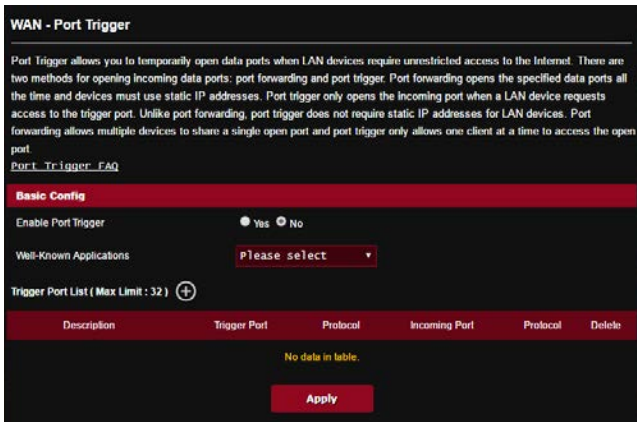
- Detect Interval:** A text input field contains the number '5', followed by the text 'seconds'.
- Failover Execution Time:** The text 'Continuous 12 times (= 60 seconds) detect network failed.' is displayed.
- Enable Ping to Internet:** Two radio buttons are present: 'Yes' (which is selected) and 'No'.

At the bottom of the page, there is a red 'Apply' button.

3.20.3 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**.
2. On the **Enable Port Trigger** field, tick **Yes**.
3. On the **Well-Known Applications** field, select the popular games and web services to add to the Port Trigger List.

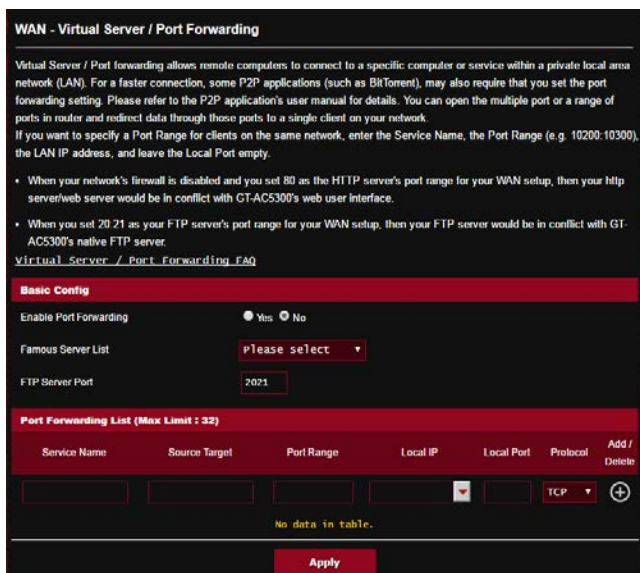
4. On the **Trigger Port List** table, key in the following information:
 - **Description:** Enter a short name or description for the service.
 - **Trigger Port:** Specify a trigger port to open the incoming port.
 - **Protocol:** Select the protocol, TCP, or UDP.
 - **Incoming Port:** Specify an incoming port to receive inbound data from the Internet.
 - **Protocol:** Select the protocol, TCP, or UDP.
5. Click the **Add**  to enter the port trigger information to the list. Click the **Delete**  button to remove a port trigger entry from the list.
6. When done, click **Apply**.

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.
-

3.20.4 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.



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 empty.

- 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 GT-ACS300's web user interface.
- When you set 2021 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with GT-ACS300's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

Basic Config

Enable Port Forwarding Yes No

Famous Server List

FTP Server Port

Port Forwarding List (Max Limit : 32)

Service Name	Source Target	Port Range	Local IP	Local Port	Protocol	Add / Delete
					TCP	+

No data in table.

Apply

To set up Port Forwarding:

1. From the navigation panel, go to **Advanced Settings > WAN > Virtual Server / Port Forwarding**.
2. On the **Enable Port Forwarding** field, tick **Yes**.
3. On the **Famous Server List** field, select the type of service you want to access.
4. On the **Famous Game List** field, select the popular game that you want to access. This item lists the port required for your selected popular online game to work properly.

5. On the **Port Forwarding List** table, key in the following information:



- **Service Name:** Enter a service name.
- **Port Range:** 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 empty. Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,3021).

NOTES:

- 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 the router's web user interface.
- A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.

-
- **Local IP:** Key in the client's LAN IP address.

NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **3.13 LAN** for information.

-
- **Local 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.
 - **Protocol:** Select the protocol. If you are unsure, select **BOTH**.
6. Click the **Add**  to enter the port trigger information to the list. Click the **Delete**  button to remove a port trigger entry from the list.
7. When done, click Apply.

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.

3.20.5 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:

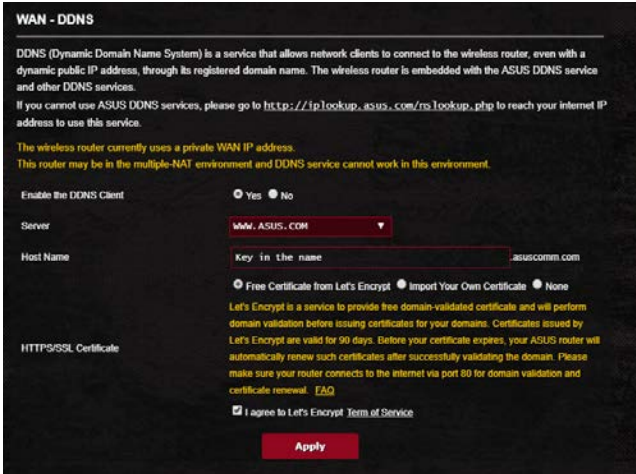
1. From the navigation panel, go to **Advanced Settings > WAN > DMZ**.
2. Configure the setting below. When done, click **Apply**.
 - **IP address of Exposed Station:** Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has 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**.

3.20.6 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**.
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.
-

3.20.7 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**. When done, click **Apply**.

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	

3.21 Wireless

3.21.1 General

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

Wireless - General

Set up the wireless related information below

Enable Smart Connect **ON** [Smart_Connect_Bu1c](#)

Smart Connect **Tri-Band Smart Connect (2.4GHz, 5GHz-1 and 5GHz-2)** ▼

Network Name (SSID)

Hide SSID Yes No

Wireless Mode **Auto** ▼

802.11ax HE frame support **Enable** ▼ If compatibility issue occurs when enabling 802.11ax HE frame support, please check: [FAQ](#)

Channel bandwidth **Auto** ▼

Control Channel **Auto** ▼ Current Control Channel: 11, 36, 144

Extension Channel **Auto** ▼

Authentication Method **WPA2-Personal** ▼

WPA Encryption **AES** ▼

WPA Pre-Shared Key

Protected Management Frames **Disable** ▼

Group Key Rotation Interval

Apply

To configure the basic wireless settings:

1. From the navigation panel, go to **Advanced Settings > Wireless > General**.
2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
3. If you want to use the Smart Connect function, move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band 2.4GHz or 5GHz for optimal speed.

4. 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.

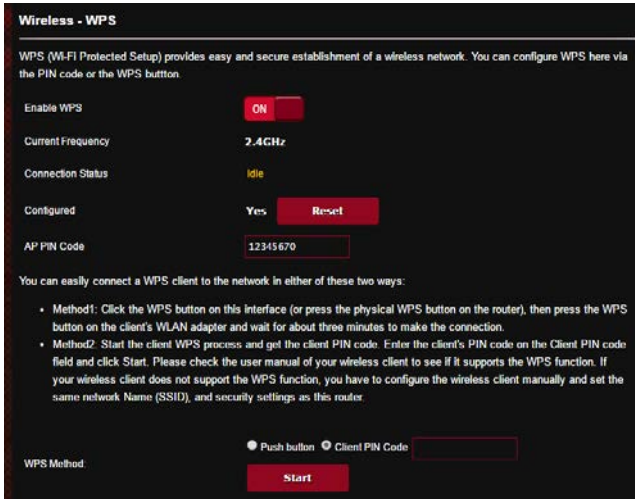
NOTE: You can assign unique SSIDs for the 2.4 GHz and 5GHz frequency bands.

5. 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.
6. 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.
 - **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.
 - **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.
7. Select the operating/control 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 the channel bandwidth to accommodate higher transmission speeds.
9. Select the authentication method.
10. When done, click **Apply**.

3.21.2 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**.
2. In the **Enable WPS** field, move the slider to **ON**.
3. WPS uses 2.4GHz by default. If you want to change the frequency to 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, and WPA2-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 4. If you select **Client PIN** code, go to step 5.
 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 rear 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.

3.21.3 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.

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your GT-AC5300 to connect to an access point wirelessly. WDS may also be considered a repeater mode. But with this method, the devices connected to the access point will only be able to use half of the access point's original wireless speed.

Note: The function does not support [WPA2-Enterprise, WPA-Auto-Enterprise] security authentication method.

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

2.4GHz MAC:

5GHz-1 MAC:

5GHz-2 MAC:

Band:

AP Mode:

Connect to APs in list: Yes No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text" value=""/>	<input type="button" value="+"/>

No data in table.

To set up the wireless bridge:

1. From the navigation panel, go to **Advanced Settings > Wireless > WDS**.
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. By default, the operating/control channel for the wireless bridge is set to **Auto** to allow the router to automatically select the channel with the least amount of interference.

You can modify the **Control Channel** from **Advanced Settings > Wireless > General**.

NOTE: Channel availability varies per country or region.

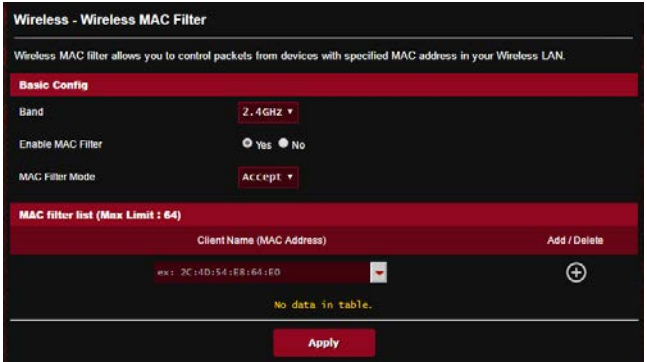
6. On the Remote AP List, key in a MAC address and click the **Add** button  to enter the MAC address of other available Access Points.
-

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


7. Click **Apply**.

3.21.4 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**.
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**.

3.21.5 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.

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:

Server Port: 1812

Connection Secret:

Apply

To set up wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to WPA-Enterprise or WPA2-Enterprise.

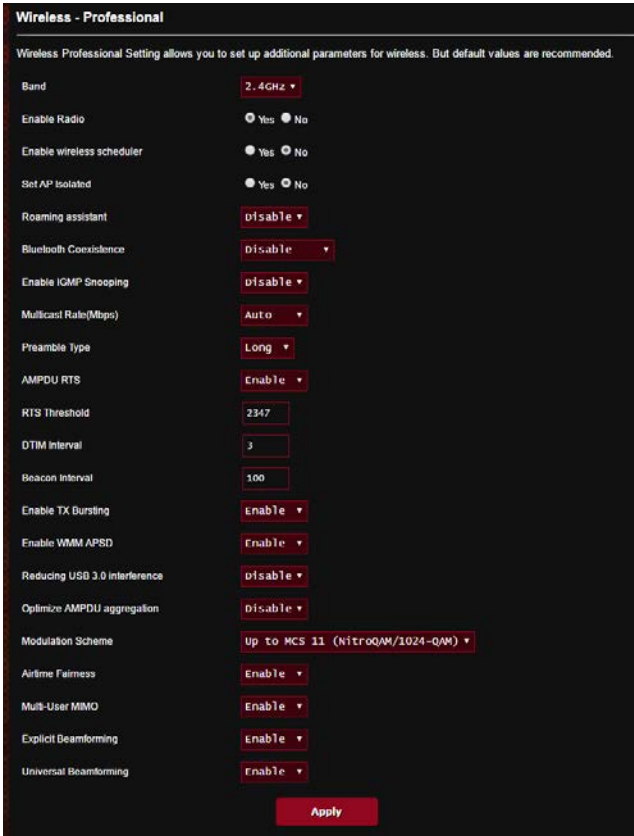
NOTE: Please refer to section **3.21.1 General** for configuring your wireless router's Authentication Mode.

2. From the navigation panel, go to **Advanced Settings > Wireless > RADIUS Setting**.
3. Select the frequency band.
4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
5. In the **Server Port** field, key in the server port.
6. In the **Connection Secret** field, assign the password to access your RADIUS server.
7. Click **Apply**.

3.21.6 Professional

The Professional screen provides advanced configuration options.

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



In the **Professional** settings 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.

- **Date to Enable Radio (weekdays):** You can specify which days of the week wireless networking is enabled.
- **Time of Day to Enable Radio:** You can specify a time range when wireless networking is enabled during the week.
- **Date to Enable Radio (weekend):** You can specify which days of the weekend wireless networking is enabled.
- **Time of Day to Enable Radio:** You can specify a time range when wireless networking is enabled during the weekend.
- **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.
- **Roaming Assistant:** In network configurations that involve multiple Access, Points or wireless repeater, wireless clients sometimes cannot connect automatically to the best available AP because they are still connected to the main wireless router. Enable this setting so that the client will disconnect from the main wireless router if the signal strength is under a specific threshold and connect to a stronger signal.
- **Enable IGMP Snooping:** Enable this function allows the IGMP (Internet Group Management Protocol) to be monitored among devices and optimizes wireless multicast traffic.
- **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.
- **AMPDU RTS:** Enable this function allows to build a group of frames before they are transmitted and use RTS for every AMPDU for communication among 802.11g and 802.11b devices.

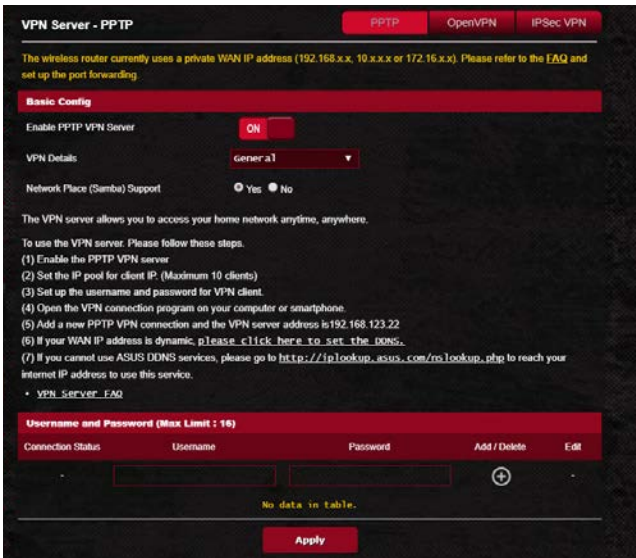
- **RTS Threshold:** Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval:** DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is 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.
- **Reducing USB 3.0 interference:** Enable this function ensures the best wireless performance on the 2.4 GHz band. Disabling this feature increase USB 3.0 port's transmission speed and may affect the 2.4 GHz wireless range.
- **Optimize AMPDU aggregation:** Optimize the max number of MPDUs in an AMPDU and avoid packets get lost or corrupted during transmission in error-prone wireless channels
- **Optimize ack suppression:** Optimize the max number of ack to suppress in a raw.
- **Turbo QAM:** Enable this function allows to support 256-QAM (MCS 8/9) on the 2.4GHz band to achieve better range and throughput on that frequency.

- **Airtime Fairness:** With airtime fairness, the speed of the network is not determined by the slowest traffic. By allocating time equally among clients, Airtime Fairness allows every transmission to move at its highest potential speed.
- **Explicit Beamforming:** The client's WLAN adapter and router both support beam forming technology. This technology allows these device to communicate the channel estimation and steering direction to each other to improve download and uplink speed.
- **Universal Beamforming:** For legacy wireless network adapter that do not support beam forming, the router estimates the channel and determines the steering direction to improve the downlink speed.

3.22 WiFi Radar

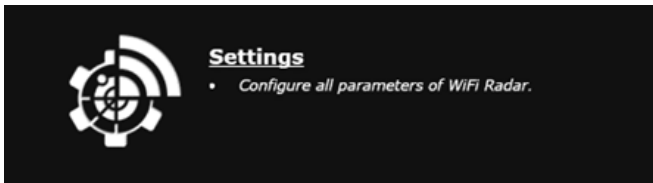
WiFi Radar, an advanced analysis tool for your wireless network, delves deep into the channels and packet data for troubleshooting.

NOTE: Enabling WiFi Radar may result to a drop wireless performance. Only enable WiFi Radar when needed.



To use WiFi Radar:

1. Go to Settings and configure all the WiFi Radar parameters,
1. From the navigation panel, go to **General > WiFi Radar** and set the schedule for data recording.



- Click **Start Data Collection**.
- Click **Submit** after you set all the parameters.

Settings
Configure parameters of WiFi Probe

Sample Interval:
 5 Second 10 Second 15 Second 20 Second

Start/Stop Data Collection

Start collecting data every:
 Sunday Monday Tuesday Wednesday Thursday Friday Saturday

From 00:00:00 To 23:59:59

Database Size

Database Size: 0 MB
(Please note that, for example, 2 GB's collected using a 5 seconds sample interval for 1 hour will occupy approximately 1.50 MB of database)

Once Database size reaches maximum limit: Overwrite Older Data Stop Data Collection

Counters

Channel Statistics
 Channel Statistics
 Rx-CRC Failures
 Bad PLCP
 Bad FCS
 Packet Rejected
 Packet Stored
 Packet Dropped
 Packet Retried
 Channel Utilization
 Channel Length Per Precedence
 Data Throughput
 Physical Rate
 RTS Fail
 Retry Drop
 Pll Lock
 Acked

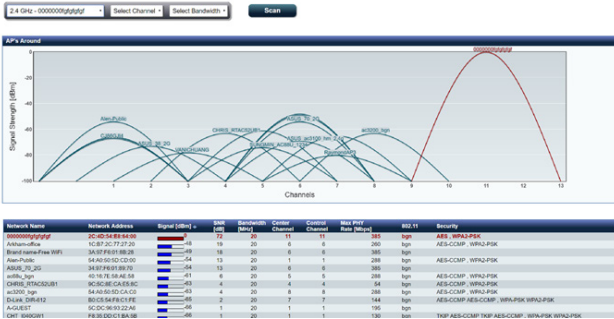
Export Database

Download Database File

<http://mtools.sourceforge.jp/WiFi-Probe-2.2.017-11-02-14-047-080/> (in **English**)

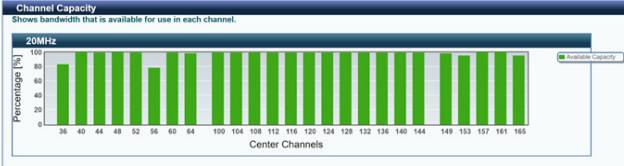
3.22.1 WiFi Site Survey

WiFi Site Survey allows you to search for wireless networks in your environment.



3.22.2 Wireless Channel Statistics

This feature shows channel usage of all bands and channel distribution statistics in your environment.



3.8.3 Advanced Troubleshooting

This feature shows WiFi glitch statistics in your environment.



4 Utilities

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
 - Device Discovery v1.4.7.1 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
 - Firmware Restoration v1.9.0.4 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Windows Printer Utility v1.0.5.5 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
 - The utilities are not supported on MAC OS.
-

4.1 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.

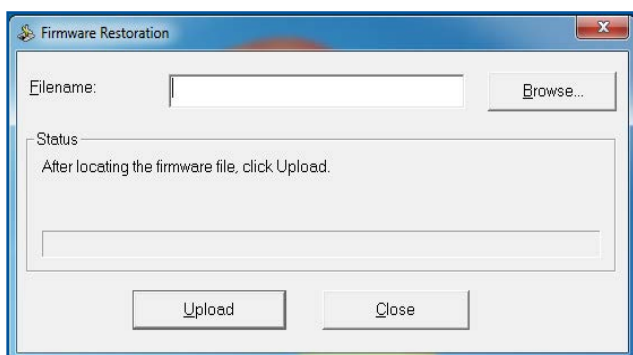
To launch the Device Discovery utility:

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

4.2 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.

NOTE: This feature is not supported on MAC OS.

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

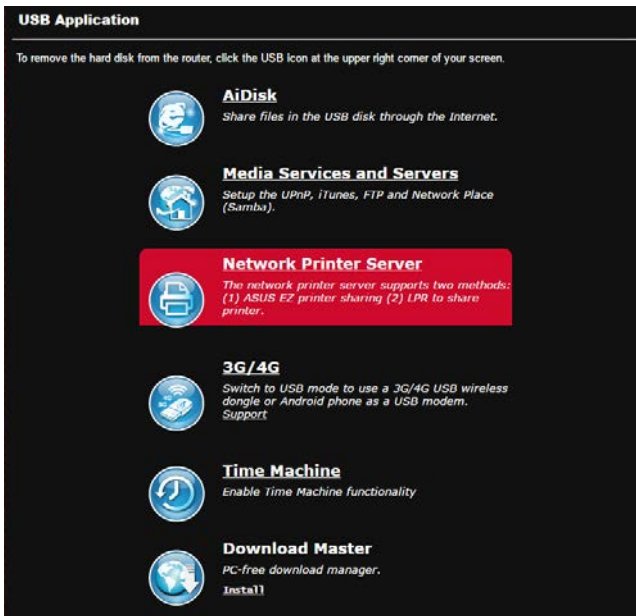
4. From your computer's desktop, click **Start > All Programs > ASUS Utility GT-AX11000 Wireless Router > Firmware Restoration.**
5. Specify a firmware file, then click **Upload.**

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 3: Configuring the General and Advanced Settings of ROG Gaming Router** for more details.

4.3 Setting up your printer server

4.3.1 ASUS EZ Printer Sharing

ASUS EZ Printing Sharing utility allows you to connect a USB printer to your wireless router's USB port and set up the print server. This allows your network clients to print and scan files wirelessly.



NOTE: The print server function is supported on Windows® 7/8/8.1/10.

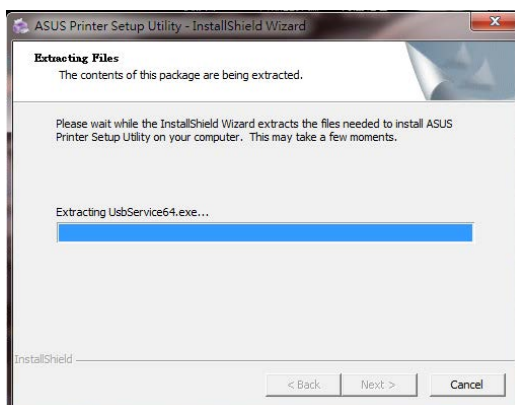
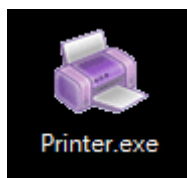
To set up the EZ Printer sharing mode:

1. From the navigation panel, go to **Advanced Settings > USB Application > Network Printer Server**.
2. Click **Download Now!** to download the network printer utility.

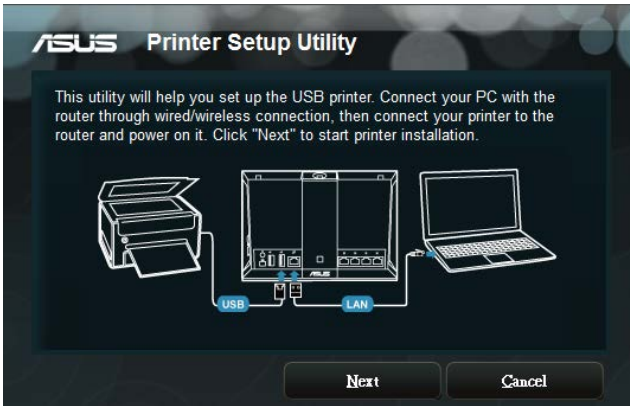


NOTE: Network printer utility is supported on Windows® 7/8/8.1/10. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

3. Unzip the downloaded file and click the Printer icon to run the network printer setup program.



4. Follow the onscreen instructions to set up your hardware, then click **Next**.

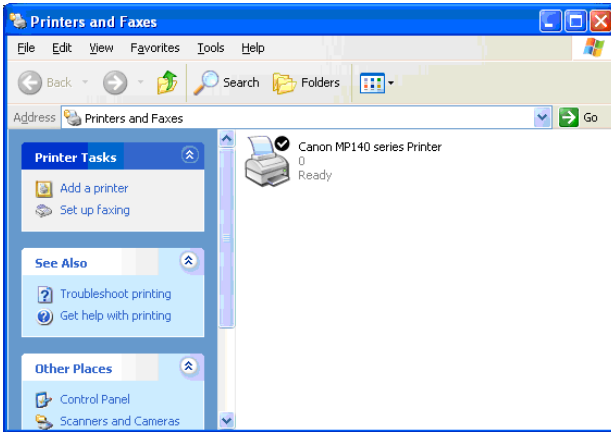


5. Wait a few minutes for the initial setup to finish. Click **Next**.
6. Click **Finish** to complete the installation.

7. Follow the Windows® OS instructions to install the printer driver.



8. After the printer's driver installation is complete, network clients can now use the printer.



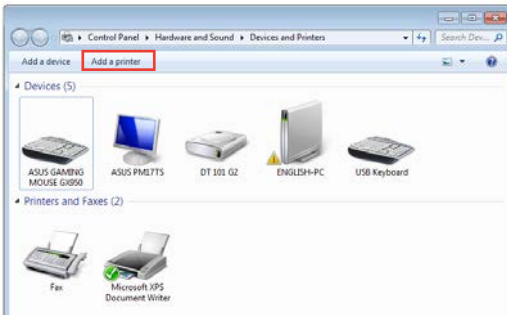
4.3.2 Using LPR to Share Printer

You can share your printer with computers running on Windows® and MAC operating system using LPR/LPD (Line Printer Remote/Line Printer Daemon).

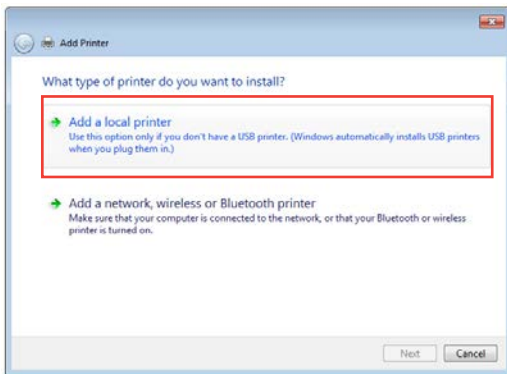
Sharing your LPR printer

To share your LPR printer:

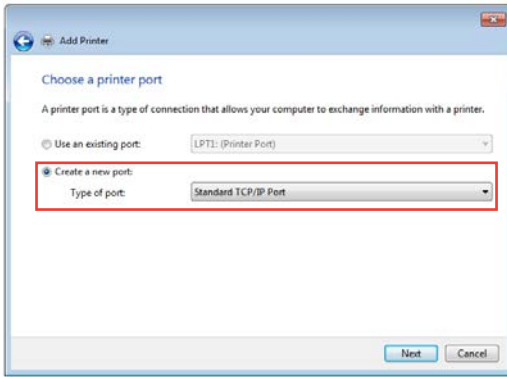
1. From the Windows® desktop, click **Start > Devices and Printers > Add a printer** to run the **Add Printer Wizard**.



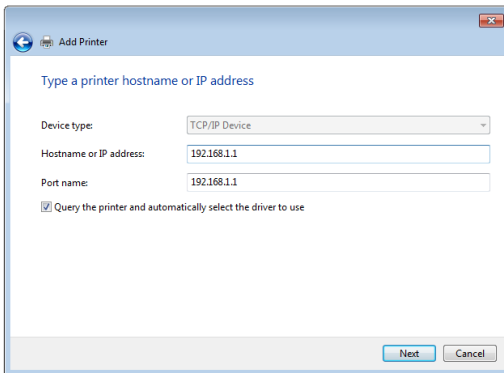
2. Select **Add a local printer** and then click **Next**.



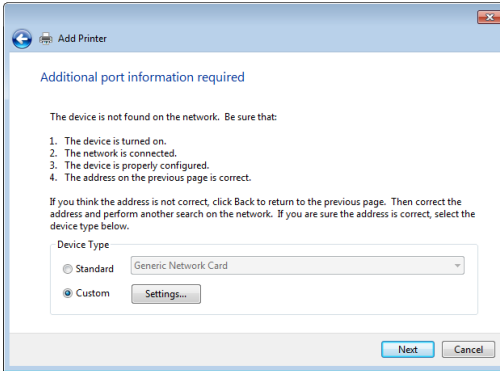
3. Select **Create a new port** then set **Type of Port** to **Standard TCP/IP Port**. Click **New Port**.



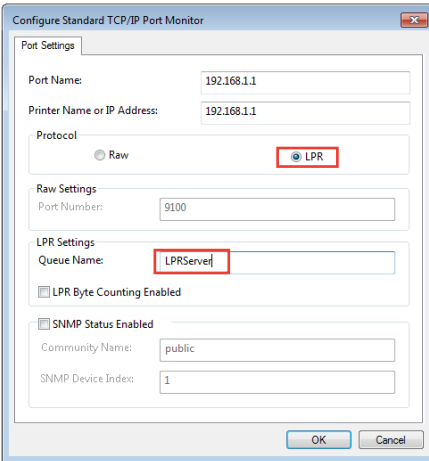
4. In the **Hostname or IP address** field, key in the IP address of the wireless router then click **Next**.



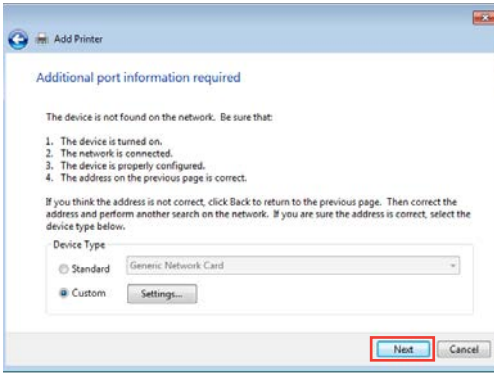
5. Select **Custom** then click **Settings**.



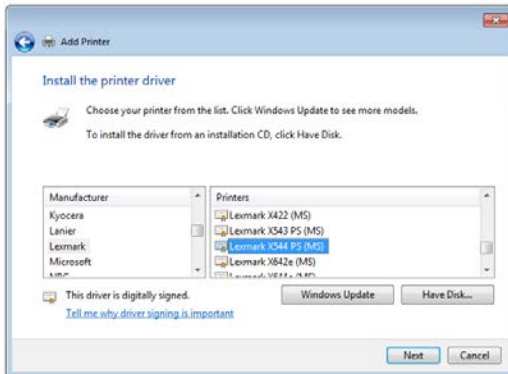
6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.



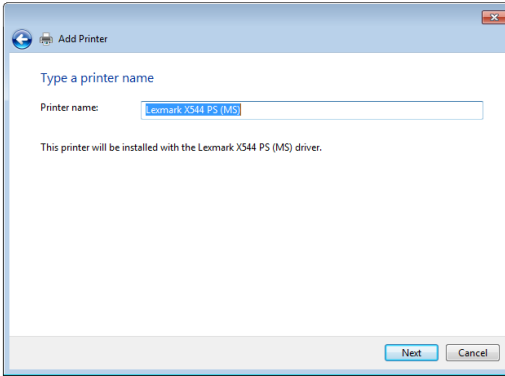
7. Click **Next** to finish setting up the standard TCP/IP port.



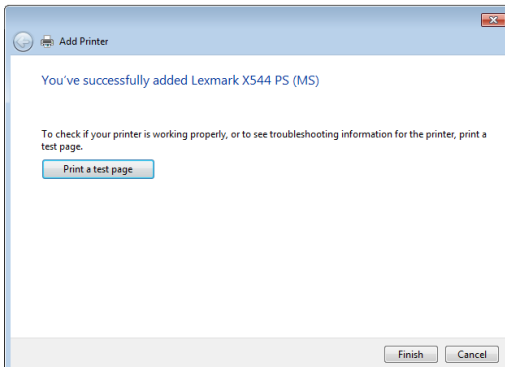
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.



9. Click **Next** to accept the default name for the printer.



10. Click **Finish** to complete the installation.



4.4 Download Master

Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

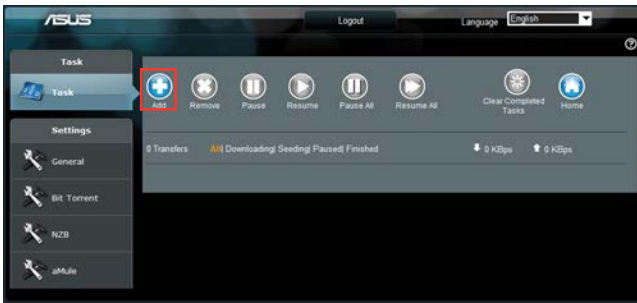
NOTE: You need a USB device connected to the wireless router to use Download Master.

To use Download Master:

1. Click **Advanced Settings > USB application > Download Master** to download and install the utility automatically.

NOTE: If you have more than one USB drive, select the USB device you want to download the files to.

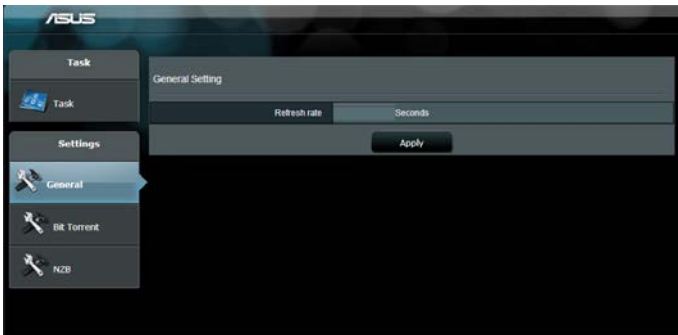
2. After the download process is finished, click the Download Master icon to start using the utility.
3. Click **Add** to add a download task.



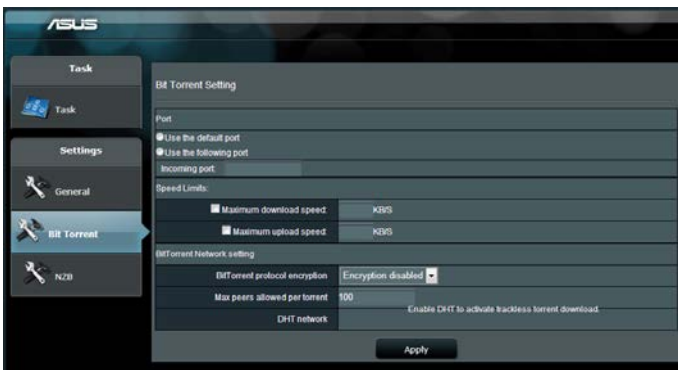
4. Select a download type such as BitTorrent, HTTP, or FTP. Provide a torrent file or a URL to begin downloading.

NOTE: For details on Bit Torrent, refer to section **4.4.1 Configuring the Bit Torrent download settings**.

5. Use the navigation panel to configure the advanced settings.



4.4.1 Configuring Bit Torrent download settings

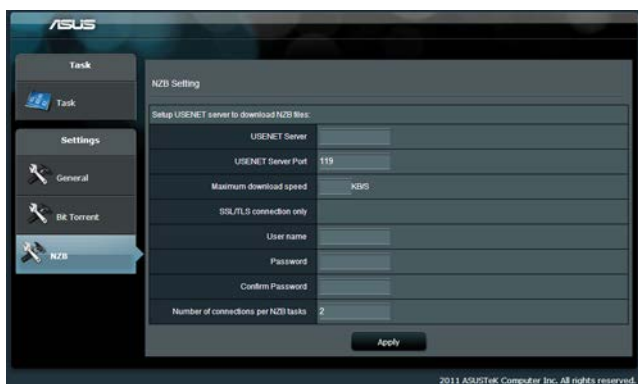


To configure BitTorrent download settings:

1. From Download Master's navigation panel, click **Bit Torrent** to launch the **Bit Torrent Setting** page.
2. Select a specific port for your download task.
3. To prevent network congestion, you can limit the maximum upload and download speeds under **Speed Limits**.
4. You can limit the maximum number of allowed peers and enable or disable file encryption during downloads.

4.4.2 NZB settings

You can set up a USENET server to download NZB files. After entering USENET settings, **Apply**.



5 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.

5.1 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**. Click **Check** to verify if the latest firmware is available.
2. If the latest firmware is available, visit the ASUS global website at https://www.asus.com/Networking/ROG-Rapture-GT-AX11000/HelpDesk_BIOS/ to download the latest firmware.
3. From the **Firmware Upgrade** page, click **Browse** to locate the firmware file.
4. Click **Upload** to upgrade the firmware.

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 computer.

- 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.

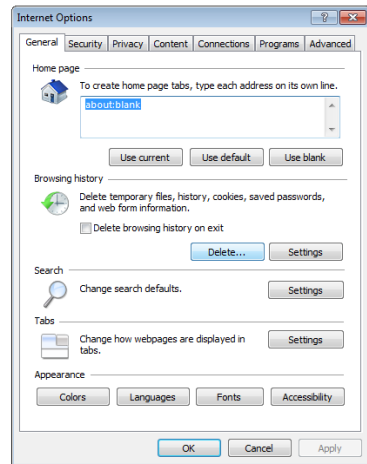
- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. 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**.



5.2 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. 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 8, follow these steps:
 1. Launch Internet Explorer 8, then click **Tools > Internet Options**.
 2. In the **General** tab, under **Browsing history**, click **Delete...**, select **Temporary Internet Files** and **Cookies** then click **Delete**.



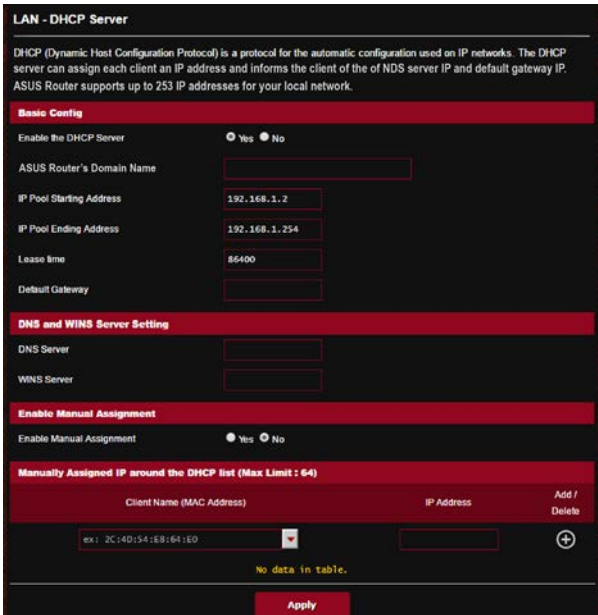
NOTES:

- 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.

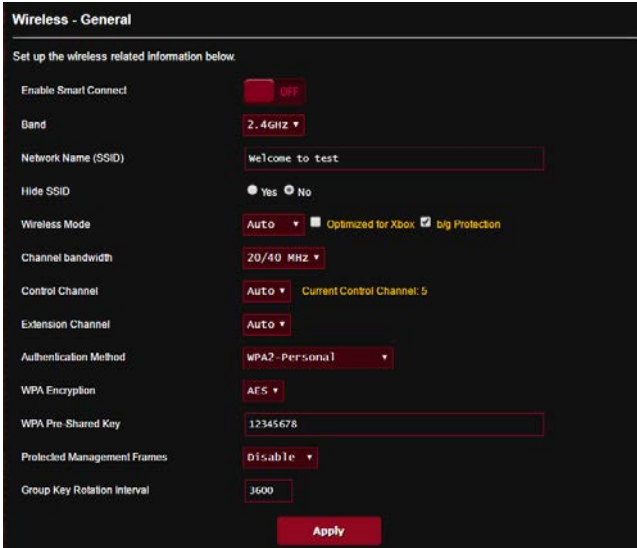
The client cannot establish a wireless connection with the router.

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 **Advanced Settings > 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 **Advanced Settings > 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 > Aiprotection Pro > 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**.

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: http://www.asusrouter.com
(or 192.168.50.1)

Domain Name: (Blank)

Subnet Mask: 255.255.255.0

DNS Server 1: 192.168.50.1

DNS Server 2: (Blank)

SSID (2.4GHz): ASUS

SSID (5GHz): ASUS_5G

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **4.2 Firmware Restoration** on how to use the Firmware Restoration utility.

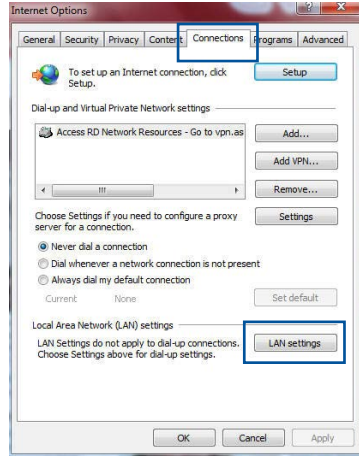
Cannot access Web GUI

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® 7

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

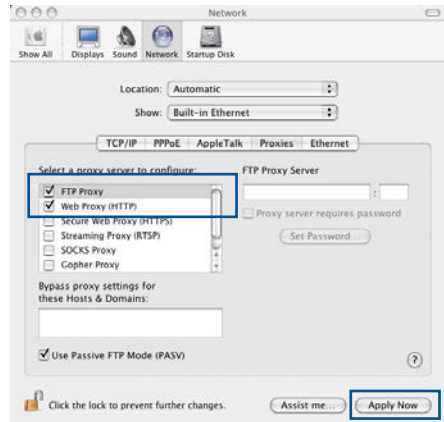


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



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.

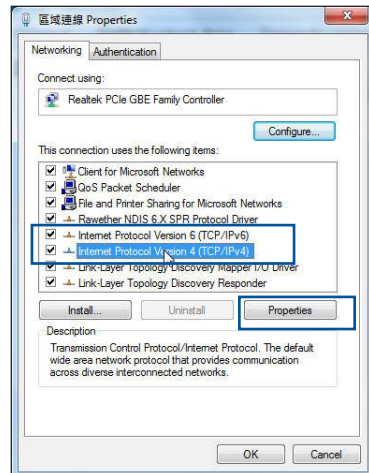


NOTE: Refer to your browser's help feature for details on disabling the proxy server.

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

Windows® 7

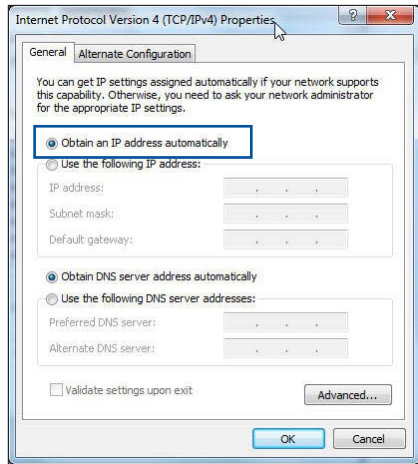
1. Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage network connections**.
2. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.




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

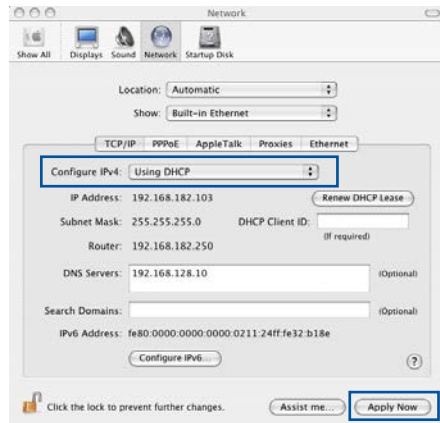
To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

4. 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.

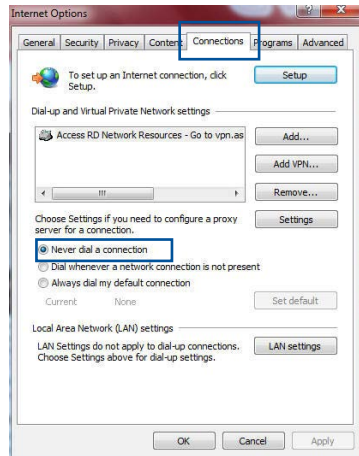


NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

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

Windows® 7

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

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

Safety Notices

When using this product, always follow the fundamental safety precautions, including, but not limited to the following:



WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
 - If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
 - DO NOT use damaged power cords, accessories, or other peripherals.
 - DO NOT mount this equipment higher than 2 meters.
 - Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
 - Read the operational guidelines and the temperature range provided before using the product.
 - Pay particular attention to the personal safety when using this device in airports, hospitals, gas stations and professional garages.
 - Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products to reduce the risk of interference.
 - Kindly use ASUS products in good reception conditions to minimize the radiation's level.
 - Keep the device away from pregnant women and the lower abdomen of the teenager.
 - DO NOT use this product if visible defects can be observed or it has been wet or damaged or modified. Seek servicing for assistance.
-

**WARNING!**

- DO NOT place on uneven or unstable work surfaces.
 - DO NOT place or drop objects on the top of the product. Avoid exposing the product to mechanical shock such as crushing, bending, puncturing or shredding.
 - DO NOT disassemble, open, microwave, incinerate, paint, or shove any foreign objects into this product.
 - Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
 - Keep the product away from fire and heat sources.
 - DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the product during electrical storms.
 - Connect the PoE output circuits of this product exclusively to PoE networks, without routing to external facilities.
 - To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
 - Only use accessories that have been approved by the device manufacturer to work with this model. The use of other types of accessories may invalidate the warranty or violate local regulations and laws, and may pose safety risks. Contact your local retailer for the availability of authorized accessories.
 - Use of this product in a way not recommended in the provided instructions may result in a risk of fire or personal injury.
-

Service and Support

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

