E23424



LISER MANLIAL

GT-AXE 16000 ROG Rapture Quad band Gaming Router



E23424 Revised Edition v2 April 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 of 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	Getti	ng to know your wireless router
1.1	Welco	ome!7
1.2	Packa	ge contents7
1.3	Your	wireless router8
1.4	Positi	oning your router 10
1.5	Setup	Requirements 11
2	Getti	ng started
2.1	Route	er Setup 12
	Α.	Wired connection13
	В.	Wireless connection14
2.2	Quick	Internet Setup (QIS) with Auto-detection
2.3	Conn	ecting to your wireless network
3	Confi	guring the General and Advanced Settings
3.1	Loggi	ng into the Web GUI 20
3.2	Admi	nistration 22
	3.2.1	Operation Mode22
	3.2.2	System23
	3.2.3	Firmware Upgrade24
	3.2.4	Restore/Save/Upload Setting24
3.3	AiClo	ud 2.0
	3.3.1	Cloud Disk26
	3.3.2	Smart Access
	3.3.3	AiCloud Sync29
3.4	ASUS	AiMesh
	3.4.1	Before setting
	3.4.2	AiMesh Setup steps30
	3.4.3	Troubleshooting
	3.4.4	Relocation
	3.4.5	FAQ (Frequently Asked Questions)

Table of contents

3.5	AiProtection	
	3.5.1 Configuring AiProtection	
	3.5.2 Blocking Malicious Sites	
	3.5.3 Two-Way IPS	40
	3.5.4 Infected Device Prevention and Blocking	41
	3.5.5 Setting up Parental Control	42
3.6	Dash Board	
3.7	Firewall	
	3.7.1 General	
	3.7.2 URL Filter	
	3.7.3 Keyword filter	
	3.7.4 Network Services Filter	50
	3.7.5 IPv6 Firewall	51
3.8	Game Acceleration	
	3.8.1 QoS	53
	3.8.2 Gear Accelerator	54
3.9	Game Radar	
3.10	Guest Network	
3.11	IPv6	
3.12	LAN	
	3.12.1 LAN IP	60
	3.12.2 DHCP Server	61
	3.12.3 Route	63
	3.12.4 IPTV	64
3.13	Network Map	
	3.13.1 Setting up the wireless security settings	65
	3.13.2 Managing your network clients	67
	3.13.3 Monitoring your USB device	68
3.14	Open NAT & Game Profile	
3.15	Smart Connect	72
	3.15.1 Setting up Smart Connect	72

Table of contents

	3.15.2 Smart Connect Rule	73
3.16	System Log	76
3.17	Traffic Analyzer	77
3.18	USB Application	
	3.18.1 Using AiDisk	79
	3.18.2 Using Servers Center	81
	3.18.3 3G/4G	86
3.19	VPN	
	3.19.1 VPN Fusion	
	3.19.2 Instant Guard	90
3.20	WAN	
	3.20.1 Internet Connection	91
	3.20.2 Dual WAN	94
	3.20.3 Port Trigger	95
	3.20.4 Virtual Server/Port Forwarding	97
	3.20.5 DMZ	
	3.20.6 DDNS	
	3.20.7 NAT Passthrough	
3.21	Wi-Fi Radar	
	3.21.1 Wi-Fi Site Survey	
	3.21.2 Wireless Channel Statistics	
	3.21.3 Advanced Troubleshooting	
3.22	Wireless	
	3.22.1 General	
	3.22.2 WPS	
	3.22.3 Bridge	
	3.22.4 Wireless MAC Filter	
	3.22.5 RADIUS Setting	
	3.22.6 Professional	

4 Utilities

4.1	Device Discovery	118
4.2	Firmware Restoration	119
4.3	Setting up your printer server	120
	4.3.1 ASUS EZ Printer Sharing	120
	4.3.2 Using LPR to Share Printer	124
4.4	Download Master	129
	4.4.1 Configuring Bit Torrent download settings	130
	4.4.2 NZB settings	131

5 Troubleshooting

5.1	Basic Troubleshooting	132
5.2	Frequently Asked Questions (FAQs)	134

Appendices

Safety Notices	152
Service and Support	154

Getting to know your wireless 1 router

Welcome! 1.1

Thank you for purchasing ROG Rapture Wireless Router! The stylish router features 2.4GHz, 5GHz and 6GHz 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 $\mathbf{\nabla}$
- $\mathbf{\nabla}$ Network cable (RJ-45)
- ☑ AC adapter
- ✓ Ouick 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	WPS button This button launches the WPS Wizard.
2	LED button (LED Key) Press this button to turn on /off the LED.
3	Power (DCIN) port Insert the bundled AC adapter into this port and connect your router to a power source.
4	Power switch Press this switch to power on or off the system.
5	USB 2.0 port Insert a USB 2.0 compatible device such as a USB hard disk or USB flash drive into this port.
6	USB 3.2 Gen 1 port Insert a USB 3.2 Gen 1 compatible device such as a USB hard disk or USB flash drive into this port.
7	Reset button This button resets or restores the system to its factory default settings.

8	1GE LAN ports
	Connect network cables into these ports to establish LAN connection.
9	2.5 / 1GE WAN (Internet) port
	Connect a network cable into this port to establish 2.5 / 1GE WAN connection.
10	10GE ports
	Connect network cables into these ports to prioritize the packets.
1	2.5 / 1GE WAN (Internet) LED
	Red: No IP or no physical connection.
	On : Has physical connection to a wide area network (WAN).
12	LAN LED
	Off: No power or no physical connection.
	On : Has physical connection to a local area network (LAN).
13	10GE LED
	Off: No 10GE connection.
	On : Has physical connection to 10GE port.
14	6GHz / 5GHz-2 / 5GHz-1 / 2.4GHz Wi-Fi LED
	Off: No 6GHz / 5GHz-2 / 5GHz-1 / 2.4GHz signal.
	On : Wireless system is ready.
	Flashing: Transmitting or receiving data via wireless connection.
15	Power LED
•	Off: No power.
	On: Device is ready.
	Flashing slow: Rescue mode.

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 +19.5V with max 3.33A 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 <u>http://www.asus.com</u> to get the latest firmware updates.
- To ensure the best wireless signal, orient the four 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 and 6GHz 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: <u>https://www.realtek.com/en/downloads</u>
 - Mediatek: <u>https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi</u>
 - 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 <u>http://www.asusrouter.com</u>
- 3. Set up a password for your router to prevent unauthorized access.



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.

Currently connected ASUS router Internet acce	to: 4	11 ×
Wireless Network Co	onnection ^	
ARIES_RT-N66U	Connected	-
ASUS Ariel 2G	.atl	
ASUS_XX_2G	lin.	
	Connect	
Alen_Private	lte.	
ASUSPM-Public	-atl	
ALIGU_87U_2G	.atl	
ASUS hm66 2G	.at	-
Open Network a	nd Sharing Center	

2.4G Wi-Fi Name (SSID):	ASUS_XX_2G
5G Wi-Fi Name (SSID):	ASUS_XX_5G
6G Wi-Fi Name (SSID):	ASUS_XX_6G

* 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 <u>http://www.asusrouter.com</u>.
- 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 unauthorize	d access to your ASUS wireless router.
Router Login Name	admin
New Password	
Retype Password	Show password

2.2 Quick Internet Setup (QIS) with Autodetection

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:

 Launch a web browser. You will be redirected to the ASUS Setup Wizard (Quick Internet Setup). If not, key in <u>http://www.asusrouter.com</u> 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, 5 GHz and 6GHz wireless connection. Click **Apply** when done.

HIRELESS SETTINGS	Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.	
	2.4 GHz Network Name (SSID)	
	2.4 GHz Wireless Security	8
	5 GHz-1 Network Name (SSID)	
	5 GHz-1 Wireless Security	Q
	5 GHz-2 Network Name (SSID)	
	5 GHz-2 Wireless Security	8
	6 GHz Network Name (SSID)	
and the second	6 GHz Wireless Security	Q
	Separate 2.4 GHz, 5 GHz-1, 5 GHz-2 and 6 GHz	
	PROVIDE PROVIDE	

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

LUCIN Instrume Prosoning Settings	Change the router password to prevent unauthorized access to your ASUS wireless router. Router Login Name		
	New password	•	
	Retype Password		
	PREVIOUS		

NOTE: The wireless router's login username and password is different from the 2.4GHz/5GHz/6GHz 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/6GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz/6GHz 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 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

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: <u>http://www.asusrouter.com</u>.
- 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 / AiMesh Router mode (Default): In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
 - Access Point(AP) / AiMesh Router in AP mode: In this mode, the router creates a new wireless network on an existing network.
 - **Repeater mode**: In Repeater mode, GT-AXE16000 wirelessly connects to an existing wireless network to extend the wireless coverage. In this mode, the firewall, IP sharing, and NAT functions are disabled.
 - **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.

- **AiMesh node**: 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 <u>http://www.asus.com</u>

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 <u>http://www.asusrouter.com</u> 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 <u>https://[yourASUSDDNSname].asuscomm.com</u> for a very secure Cloud Disk and Smart Access usage.

3.3.3 AiCloud Sync

AiCloud 2.0 -	AiCloud Sync				
USB«:(Enables AiClos <u>AQ</u>	ud Sync functionality. For ste	p-by-step istructions	, go to <u>F</u>
Cloud List					
Provider	Username	Rule	Folder Name	Connection Status	Delete
No USB disk detected.					
		Ad	ld new count		

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 ASUS AiMesh

3.4.1 Before setting

Preparing to setup an AiMesh Wi-Fi system

- 1. Two (2) ASUS routers (models supporting AiMesh: <u>https://www.asus.com/AiMesh/</u>).
- 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.



AiMesh node

AiMesh router

3.4.2 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.

/isus	
Network Map	AiMesh
	Find AiMesh node Search
AiMesh node	

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.

Successfully added RT-ABCDE to your AiMesh system, it will take awhile to show up as connected in the AiMesh router list.
OK

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



3.4.3 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 fireware at: <u>https://www.asus.com/AiMesh/</u>
 - 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 <u>http://www.asusrouter.com</u>.
 - 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.



3.4.4 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.



3.4.5 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 (<u>http://www. asusrouter.com</u>), 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.

3.5 AiProtection

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


3.5.1 Configuring AiProtection

AiProtection prevents network exploits and secures your network from unwanted access.



To Configure AiProtection:

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

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

	Router Security Assessment		HOME
	Default router login username and password changed -	No	
	Wireless password strength check -	Very Weak	
	Wireless encryption enabled -	Weak	
	WPS disabled -		
	UPnP service disabled -		
	Web access from WAN disabled -	Yes	
	PING from WAN disabled -	Yes	
	DMZ disabled -	Yes	3
	Port trigger disabled -	Yes	ange
	Port forwarding disabled -	Yes	Junge
	Anonymous login to FTP share disabled -	Yes	
	Disable guest login for Network Place Share -	Yes	
	Malicious Website Blocking enabled -	Yes	U
	Vulnerability Protection enabled -	Yes	otecti
	Infected Device Prevention and Blocking -	Yes	
1			

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

- (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.

3.5.2 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**.
- 2. From the AiProtection main page, click **Network Protection**.
- 3. From the Malicious Sites Blocking pane, click **ON**.



3.5.3 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**.
- 2. From the AiProtection main page, click Network Protection.
- 3. From the Two-Way IPS pane, click **ON**.



3.5.4 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**.
- 2. From the AiProtection 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**.

This feature prever personal information	its infected devices n or attack other de	from being enslaved by both vices.	ets or zombie attacks which might steal you
5	ecurity Event		Threat Activities
Sinc	Protection e 2019/03/26 10:33	Protection 2	1 1 1 1
	Top Client		
		1	
	Detail	s of a Successfully Protect	21 3/22 3/23 3/24 3/25 3/26 cted Event
lime	Threat	Source	Destination

3.5.5 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**.
- 2. From the AiProtection main page, click Parental Controls.



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.
- 2. From the AiProtection 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		/eb & Apps Filters	Time Scheduling
	Time Scheduling allows you	to set up time I	imits for a specific clie	nt's network usage:
	 In the [Clients Name] of control. You may also Address] column. 	column, select key in the clien	the client whose netwo Its MAC address in the	ork usage you want to [Clients MAC
-200	2. In the [Add / Delete] co	olumn, click the	plus(+) icon to add th	e client.
	3. In the [Time Managem	ent] column, c	lick the edit icon to edit	the Active Schedule.
	4. Select your time slot w	ith a click. You	can hold and drag to	extend the duration.
	5. Click [OK] to save the	settings made.		
	Note:			
	 Clients that are added to by default. 	Parental Contr	ols will have their inter	net access restricted
	2. Please disable NAT Acce	leration for mo	re precise scheduling	control.
Enable Time Scheduling	ON			
	Sat May 05	07-53-34 20	18	
System Time	* Reminder: Th	e system time ha	s not been synchronized v	with an NTP server.
	* Reminder: Th	* Reminder: The System time zone is different from your locale setting.		
Client List (Max Limit	: 16)			
•	Client Name (MAC Address)		Time Management	Add / Delete
 ex		-		Ð
	No c	data in table.		
		Apply		
		white a		

To configure Time Scheduling:

- 1. From the navigation panel, go to **General** >**AiProtection** > **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.

3.6 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.

HIRELESS STATE 24 5 6 HEN IP 192.168.1.115		HODE Wireless router CLIENTS 1 ONLINE
NETHORK TREAL 260 RBbs 100 RBbs 0 RBbs 0 RBbs 1241:30 IWI 124 NETHORK PIR 104 104 104 104 104 104 104 104 104 104	FFIC Montham 200 IVW 124230 IVW 124330 IVW 200 IVW 124230 IVW 124330 IVW 124330 IVW 124330 IVW 124330 IVW 124330 IVW 124330 IVW 12430 IVW 12430 IVW 12430 IVW 124430 IVW 124450	Download 5.18 KB Upload 5.73 KB
		As States Broathing Reinboar

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.

AURA RGE	3	AURA RGB
		#FF0000
Enable Aura	ON	
STATIC Ar	BREATHING	FLASH
	COME	т

- **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.

BUUST KEY		Bind one of the followi Key. When the bound f he Boost Key's LED w	ng functions to your Boost unction has been activated ill turn on.	
LED On/Off	DFS Channel	Aura RGB	Game Boost	

3.7 Firewall

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

NOTE: The Firewall feature is enabled by default.

3.7.1 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.

3.7.2 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.

3.7.3 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 🕑 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.

3.7.4 Network Services Filter

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

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.					
East the source in more statistic uppy war has one performences. 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.					
Internet service.	at, in addresses datative the submet will have to access the internet of any				
Network Services Filter					
Enable Network Services Filter	● Yes ● No				
Filter table type	Black List V				
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				
	тср т				
	No data in table.				
	Арріу				

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.
- 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.

3.7.5 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.

Firewall - IPv6 Firewall						
All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.						
You can leave the remote (2001::1111:2222:3333/64	You can leave the remote IP empty to allow traffic from any remote host. A subnet can also be specified. (2001::111.2222-3333/64 for example)					
Basic Config						
Enable IPv6 Firewall		© Yes ● No				
Famous Server List		Please select 🔻				
Inbound Firewall Rules	s (Max Limit : 128)					
Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete	
				тср 🔻	Ð	
	No data in table.					
		Apply				

3.8 Game Acceleration

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.



Game Boost To enable Game Boost:

From Game Boost, move the Enable Game Boost slider to ON.

3.8.1 QoS

This feature ensures bandwidth for prioritized tasks and apps.



To enable the QoS function:

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

4. Click **Automatic Setting** for optimal bandwidth automatically or **Manual Setting** to set the upload and download bandwidth manually.

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

5. Click **Apply**.

3.8.2 Gear Accelerator

Gear Accelerator allows you to prioritize game devices wirelessly via online control panel for the best gaming experience.



To configure Gear Accelerator:

- 1. From the navigation panel, go to **General > Game Acceleration**.
- 2. From the Gear Accelerator tab, click ON.
- 3. After applying setting, click **Add** to choose the client name.
- 4. Click 🕑 to add the client's profile.
- 5. Click **Apply** to save the settings

NOTE: If you want delete the client profile, click Θ .

3.9 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.

3.10 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-AXE16000 supports up to nine SSIDs (three 2.4GHz, three 5GHz and three 6GHz).

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, 5GHz or 6GHz frequency band for the guest network that you want to create.
- 3. Click Enable.

Suest Network				
The Gu your loo	iest Network provides Inti cal network.	ernet connection for guests	but restricts access to	
2.4 GHz				
Network Name (SSID)				
Authentication Method				
Network Key	Enable	Enable	Enable	
Time Remaining			Default setting by Alexa/IFTTT	
Access Intranet				
Network Name (SSID)				
Authentication				
Method				
Network Key	Enable	Enable	Enable	
Time Remaining			Default setting by Alexa/IFTTT	
Access Intranet				
Network Name (SSID)				
Authentication				
Method				
Network Key	Enable	Enable	Enable	
Time Remaining			Default setting by Alexa/IFTTT	
Access Intranet				

- 4. To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
- 5. Assign a wireless name for your temporary network on the Network Name (SSID) field.
- 6. Select an Authentication Method.
- 7. If you select a WPA authentication method, select a WPA Encryption.
- 8. Specify the Access time or choose Limitless.
- 9. Select **Disable** or **Enable** on the Access Intranet item.
- 10.When done, click **Apply**.

3.11 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.

IPv6					
Configure the IPv6 Internet setting of ASUS Router. <u>TPv6 FAQ</u>					
Basic Config					
Connection type	Disable				
	Ар	ply			

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.

3.12 LAN

3.12.1 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.

LAN - LAN IP	
Configure the LAN setting of ASUS Router.	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
	Apply

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**.

3.12.2 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.

LAN - DHCP Server					
DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the of DNS server IP and default gateway IP. GT-AC5300 supports up to 253 IP addresses for your local network.					
Basic Config					
Enable the DHCP Server	● Yes ● No				
GT-AC5300's Domain Name					
IP Pool Starting Address	192.168.1.2				
IP Pool Ending Address	192.168.1.254				
Lease time	86400				
Default Gateway					
DNS and WINS Server Setting					
DNS Server					
WINS Server					
Enable Manual Assignment					
Enable Manual Assignment	• Yes • No				
Manually Assigned IP around the DHCP	list (Max Limit : 64)				
Client Name (MAC Ad	ldress)	IP Address	Add / Delete		
ex: 2C:4D:54:E8:64:E0	-		\oplus		
	No data in table.				
	Apply				

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 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.

3.12.3 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.

LAN - Route					
This function allows y share the same conne	ou to add routing rules into GT- ection to the Internet.	AC5300. It is useful if you (connect several ro	uters behind G	T-AC5300 to
Basic Config					
Enable static routes	• Ye:	s ONO			
Static Route List (Max Limit : 32)				
Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
			-	LAN 🔻	Ð
		No data in table.			
		Apply			

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.

3.12.4 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.

LAN - IPTV				
To watch IPTV, the WAN port must be connected to the Internet. Please go to <u>WAN - Dual WAN</u> to confirm that WAN port is assigned to primary WAN.				
LAN Port				
IPTV/ VoIP Port Settings	CANL/ LANZ 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.			
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)				
	Арріу			

3.13 Network Map

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

		Syst	tem Status			
Inte Cor	rnet status: nnected	Wireless Sta	itus Aura RGB			
WAI	N IP: 192.168.1.115 NS: GO	CPU				
			Core 1 1%			
			Core 2 0%			
			Core 3 0%			
Wireless:	Security level:	100%	Core 4 0%			
	WPA2- Personal	50%				
		RAM Used Free Total				
	Ŷ	100%	450 MB 1024 MB 56%			
Clients: 2	USB 3.0 No Device	50%				
View List		0%				
		Ethernet P	Ethernet Ports			
		Ports	Status			
		WAN	100 Mbps			
	USB 3.0	LAN 1	Unplugged			
AiMesh Node: 0	No Device	LAN 2	Unplugged			
		LAN 3	Unplugged			
		LAN 4	Unplugged			
		LAN 5	Unplugged			

3.13.1 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:

- 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, 5GHz and 6GHz bands.

2.4GHz security settings



6GHz security settings



5GHz security settings



- On the Network 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.



3.13.2 Managing your network clients



To manage your network clients:

- 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.

3.13.3 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.

		External USB disk status			
	Internet status: <u>Connected</u> WAN IP: 192.168.123.122	Information Model Name:	Health Scanner		
	DDNS: GO	Generic USB	Flash Disk		
		Available space:			
		7.028 GB			
		Total space:			
Wireless:	Security level:	7.359 GB			
MPA2- Personal	Media Server:	GO			
5.2	Personal	AiDisk Wizard:	GO		
		Safely Remove	e disk: Remove		
R	*				
Cliente: NoN	USB 3.0				
Clients. Man	No Device				
View List	USB 3.0 Generic USB F1+				

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 Plugn-Share Disk Support List at <u>http://event.asus.com/networks/</u> <u>disksupport</u>
- 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 Using AiCloud 2.0** in this user manual.

To monitor your USB device:

- 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:

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

Operation Mode: <u>Wireles</u> SID: <u>Welcome to</u> We	<u>s router</u> Firmw Picome to W	are Version: <u>3.0.0.4.382</u> lelcome to	2 10397	(4) 🗎 👤 🍙 🍦 🌣
	Internet sta <u>Connecte</u> WAN IP: 19 DDNS: <u>GO</u>	atus: d 12.168.123.122	Exter Elect USB USB Flash Information Health Model Name: Generic USB Flash Disk Available space:	disk Generic Disk
			7.028 GB	
			Total space:	
Wireless:		Security	7.359 GB	
2.4 5.1		WPA2-	Media Server:	GO
5.2		Personal	AiDisk Wizard:	GO

3.14 Open NAT & Game Profile

Open NAT offers a hassle-free way to create port forwarding rules for online games and optimizes the routing packets from your game console to the modem with an optimized gaming experience.

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 configure Open NAT:

- 1. From the navigation panel, go to **General > Open NAT**.
- 2. Slide on Enable Port Forwarding.
- 3. From the **Game List**, select a game and complete basic settings.
- 4. Click **OK**.

3.15 Smart Connect

Smart Connect is designed to automatically steer clients to one of three radios (2.4 GHz, 5 GHz and 6 GHz) 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: <u>http://www.asusrouter.com</u>.
- 2. On the login page, key in the user name 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		
et up the wireless related information	below.	
Enable Smart Connect	ON Snart Connect Rule	
Smart Connect	Tri-band Smart Connect (2.4 GHz, 5 GHz and 6 GHz) 🗸	
Network Name (SSID)	ASU5_GT-AXE11000	
2.4 / 5 GHz		
Authentication Method	MPA2/MPA3-Personal 🗸	
WPA Encryption	AES 🗸	
WPA Pre-Shared Key	asus1234	
Protected Management Frames	Capable 🗸	
Group Key Rotation Interval	3600	
2.4 GHz		
Channel bandwidth	20/40 WHz 🗸	
Control Channel	Auto V Gurrent Control Channel: 4	
Extension Channel	Auto 🗸	
5 GHz		
Channel bandwidth	20/40/80/160 MHz V Enable 180 MHz	
Control Channel	Auto Current Control Channel: 40	
Extension Channel		
6 GHz		
Channel bandwidth	20/40/80/160 MHz 🗸	
	Auto V Current Control Channel: 37	
Control Channel	enable PSC (Preferred Scanning Channel) to ensure the 6GHz devices connectivity. Please check FAQ.	
Extension Channel	Auto V	
Authentication Method	MPA3-Personal	
WPA Encryption	AES V	
WPA Pre-Shared Key	atus 1234	
Protected Management Frames	Required V	
Group Key Rotation Interval	2000	
	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.

et up the Smart Conne	ect related information below.		View List
Steering Trigger Co	ndition		
Band	2.4 GHz	5 GHz	8 GHz
Enable Load Balance	• Yes • No	🛡 Yes 🔍 No	• Yes • No
Bandwidth Utilization	0%	0%	0%.
RSSI	Greater 🗸 -62 dBr	n Less 🗸 -82 dBm	Less 🗸 -82 dBm
PHY Rate Less	Disable	Disable	Disable
PHY Rate Greater	Disable	Disable	Disable
VHT	A11 🗸	A11 🗸	AC only 🗸
STA Selection Polic	Y		
RSSI	Greater 🗸 -62 dBr	n Less 🗸 -82 dBm	Less 🗸 -82 dBm
PHY Rate Less	Disable	Disable	Disable
PHY Rate Greater	Disable	Disable	Disable
VHT	A11 🗸	A11 🗸	AC only 🗸
Interface Select and	I Qualify Procedures		
Target Band 1: 6 0	Hz 🗸 2 5 GHz 🗸 1:	6 GHz 🗸 2: 2.4 GHz 🗸	1: 5 GHz 🗸 2: 2.4 GHz 🗸
Bandwidth Utilization	ox 🛛	0%	0%
VHT A11	~	an 🗸	AC only 🗸
Bounce Detect			
Window Time	60 seconds		
Counts			
Dwell Time	180 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.

Steering Trigger Con	dition		
Band	2.4GHz	5GHz-1	5GHz-2
Enable Load Balance	• Yes • No	• Yes • No	• Yes • No
Bandwidth Utilization	0%	80%	0%
RSSI	Greater V -52 dBm	Less 🔻 -82 dBm	Less T -82 dBm
PHY Rate Less	Disable	Disable	Disable
PHY Rate Greater	> 110 Mbps	Disable	Disable
VHT	A11 V	A11 •	AC only •

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.

STA Selection Policy				
RSSI	Greater 🔻	-52 dBm	Less -82 dBm	Less • -82 dBm
PHY Rate Less		Disable	Disable	Disable
PHY Rate Greater	•	> 110 Mbps	Disable	Disable
VHT	A]]		not-allowed *	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.

Interface Select and	Qualify Procedures		
Target Band	1: 5GHz-2 • 2: 5GHz-1 •	1: 2.4GHz • 2: 5GHz-2 •	1: 2.4GHz • 2: 5GHz-1 •
Bandwidth Utilization	0%	60%	0%
VHT	• [[A	A11 •	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**.

Window Time	180	seconds
Counts		
Dwell Time	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

This page shows the detailed	system's activities.
System Time	Mon, Apr 10 15:24:24 2017
Uptime	3 days 21 hours 22 minute(s) 58 seconds
pr 10 13:45:22 kernel: j	ffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, pad
pr 10 13:45:22 kernel: j	1132: warning: (14162) j1132_sum_write_data: Not enough space for summary, pad
pr 10 13:45:22 kernel: j	1152: Warning: (14102) jiisz sum write data: Not enough space for summary, pad
pr 10 13:45:23 kernel: j	ffe2: warning: (14162) jffe2 sum_write_data. Not enough space for summary, pad
pr 10 13:45:43 kernel: j	ffs2: warning: (14183) iffs2 sum write data: Not enough space for summary, pad
pr 10 13:47:23 kernel: j	ffs: warning: (14273) iffs: sum write data: Not enough space for summary pad
pr 10 06:37:37 dnamasg-d	hcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
or 10 06:37:40 dnsmasg-d	hcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
pr 10 06:37:47 dnsmasq-d	hcp[1663]: Ignoring domain corpnet.asus for DHCP host name X15167-NB
pr 10 14:45:24 rc servic	e: httpd 732:notify rc restart ftpd
pr 10 14:45:24 FTP Serve	r: daemon is stoped
pr 10 14:45:24 FTP serve	r: daemon is started
pr 10 14:45:24 miniupnpd	[14154]: shutting down MiniUPnPd
pr 10 14:45:24 start_nat	_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
pr 10 14:45:24 miniupnpd	[17141]: version 1.9 started
pr 10 14:45:24 miniupnpd	[17141]: HTTP listening on port 43450
pr 10 14:45:24 miniupnpd	[17141]: Listening for NAT-PMP/PCP traffic on port 5351
pr 10 14:53:49 rc_servic	e: httpd 732:notify_rc restart_webdav
pr 10 14:53:49 WEBDAV Se	rver: daemon is stoped
pr 10 14:53:49 miniupnpd	[17141]: shutting down MiniUPnPd
pr 10 14:53:49 start_nat	_rules: apply the nat_rules(/tmp/nat_rules_eth0_eth0)!
pr 10 14:53:49 WEBDAV se	rver: daemon is started
pr 10 14:53:49 miniupnpd	[17578]: version 1.9 started
pr 10 14:53:49 miniupnpd	[17578]: HTTP listening on port 52738
pr 10 14:53:49 miniupnpd	[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 3.0 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 <u>http://event.asus.com/2009/networks/disksupport/</u> for the file system support table.



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.

My FTF	e server is shared.	2 3			
0 admi	n rights				
 limite limitl 	ed access rights ess access rights				
	Account	Password	Read	Write	
	admin				
		Previous Next			

 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.

	2 3
Create your domain name via t	ne ASUS DDNS services.
• I will use the service	
Key in the name	.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.
- 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 UPnP-supported devices to access multimedia files from the USB disk connected to your wireless router.

NOTE: Before using the UPnP 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 Servers**. Refer to the following for the descriptions of the fields:

- Enable iTunes Server?: Select ON/OFF to enable/disable the iTunes Server.
- Enable UPnP Media Server: Select ON/OFF to enable/ disable the UPnP 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.

USB Application - Netwo	ork Place (Samba) Sha	re / Cloud Dis	sk			5
Set the account and permission	of network place(samba) ser	vice.				
Enable Share	ON					
Allow guest login		Usemame and p place(Samba)	bassword is nece	ssary to log in	network	
Device Name	ASUS Router					
Work Group	WORKGROUP					
NTFS Sparse Files Support	Disable 🔻					
		Apply				
⊕ ⊝ ⊘						
<u>a</u> dmin	ASUS Router	sh Disk	R/W	R	No	
		Save P	ermission			

To use Samba share:

1. From the navigation panel, go to Advanced Settings > USB Application > 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 \varTheta.
- 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.

SSID: Melcome to Welcome to.	Welcome.to	
Media Servel Add new folder in s	da) Share / Cloud Disk FIP Share ×	
The default ac	cess rights for a new folder is	
USB Application - Network P	lace (Samba) Share / Cloud Disk	
Set the accor Folder Name:	twork place(samba) service.	
Enable Share	ON Add	
	lisemane unit national l	

- 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 3.13.3 Monitoring your USB device.

USB Application - FTP S	Share 5
Set the account and permission	n of FTP service.
Enable FTP	
Allow anonymous login	OFF Username and password is necessary to log in FTP service.
Maximum number of concurrent	nt connections 5
Character set on FTP Server	UTF-8
	Αρρίγ
⊕ ⊝ ⊘	
admin	ASUS Router R/W W R No
	Save Permission

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** > **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: <u>http://event.asus.com/2009/networks/3gsupport/</u>

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		РРТР	OpenVPN	IPSec VPN
The wireless router currently use set up the port forwarding.	s a private WAN IP address	(192.168.x.x, 10.x.x.x or 172	.16.x.x). Please refer	to the <u>FAQ</u> and
Basic Config				
Enable PPTP VPN Server	ON			
VPN Details	General	~		
Network Place (Samba) Support	🔍 Yes 🔍 No			
The VPN server allows you to ac	cess your home network any	time, anywhere.		
To use the VPN server Please fr	allow these steps			
(1) Enable the PPTP VPN server				
(2) Set the IP pool for client IP. (1	Maximum 10 clients)			
(3) Set up the username and pas	sword for VPN client.			
(4) Open the VPN connection pre-	ogram on your computer or s	martphone.		
(5) Add a new PPTP VPN conne	ction and the VPN server add	tress is192.168.1.115		
(6) If your WAN IP address is dyn	namic, <u>please click her</u>	e to set the DDNS.		
(7) If you cannot use ASUS DDN	IS services, please go to <u>htt</u>	p://iplookup.asus.com	n/nslookup.php to	reach your interne
IP address to use this service.				
• VPN Server FAQ				
Username and Password (M	ax Limit : 16)			
Connection Status	Username	Password	Add / Dele	ete Edit
			Ð	

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.

Client Na	ame (MAC Address) IP Address	Connection Name	Activate	e Delete		
u can add VP	N policies to the ex	coeption list, so that different client devi	ces can connect to differen	nt VPN tunnels.			
xception i	LISE (Max Lin	IL: 64) 🕀					
voontion	iet / May Lim	AL FALLA					
		No data in t	table.				
۲	Connected		Internet				
Default	Status	Connection Name	VPN type	Activate	Editor		
ows you to cr	eate VPN connecti	on prohies. The max number of concurr	rent active VPN connection	ns 15 4.			
erver List	(wax Limit :						
N Eurion E	10						
Activate the	VPN policy in Ex	ception List, and click Apply at the bo	ottom of the page.				
Assign a VP	N connection to t	beption cist and select the online cli be client device, and click OV	ent you want to configur				
Activate the	VPN connection	you created in Server List.					
Click the "+"	button beside Se	rver List to add a new VPN tunnel.					
start, please	follow the steps	below:					
		ouress to the region where the gam	e server is located, to in	prove your ping to g	ame servers.		
		rom disconnecting with game server	s. Building a VPN conne	ection also can simpl	y change your IP		
		For Gamer, VPN connection counter	acts DDoS attacks to pro	event your PC game	or your stream		
1	100	o Internet not VPN.					
<u> </u>		ome network without having to insta	all VPN software, while y	our smartphone rem	ains connected		
/PN	(m *)	ray players do not support VPN software. This feature provides VPN access to such devices in a					
	(levices to connect to different VPN t	unnels. Some devices li	ke set-top boxes, sm	art TVs and Blu-		

To start, please follow the steps below:

- 1. Click Gebeside Server List to add a new VPN tunnel.
- 2. Activate the VPN connection you created in Server List.
- 3. Click 🕑 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.

efault	Status	Connection Name	VPN type	Activate	Editor
0	Connected		Internet		
		No data in	table.		
eption I	List (Max Limit : 6	4) 🕀			
eption I an add VP	List (Max Limit : 6	i 4) ⊕ n list, so that different client de	vices can connect to differer	it VPN tunnels.	
eption I an add VP Client Na	List (Max Limit : 6 PN policies to the exceptio ame (MAC Address)	i4) 🕁 n list, so that different client de IP Address	vices can connect to differer Connection Name	it VPN tunnels. Activate	Delete

3.19.2 Instant Guard

Instant Guard runs your own private VPN server on your own router. When you use a VPN tunnel, all your data passes through the server. With Instant Guard, you're in total control of your own server, making it the safest possible solution.

istant Guard allows you your VPN Server with I	to create a VPN tunne nstant Guard app.	el with just one click via the AS	US Router app. You ca	n monitor who's connected
Basic Config				
Enable Instant Guard		ON		
Server IP Address				
System Log		Check log		
Connection Status				
Domoto ID	Client status	Access time	Device	PSKRAUTHTIME

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	
GT-AC5300 supports several connection type beside WAN Connection Type. The setting file	es to WAN (wide area network). These types are selected from the dropdown menu elds differ depending on the connection type you selected.
Configure the Ethernet WAN settings of GT-#	.C5300.
Basic Config	
WAN Connection Type	Automatic IP V
Enable WAN	O Yes ● No
Enable NAT	● Yes ● No
Enable UPnP UPnP FAQ	● Yes ● No
WAN DNS Setting	
Connect to DNS Server automatically	● Yes ● No
Account Settings	
Authentication	None
Host-Uniq (Hexadecimal)	
Special Requirement from ISP	
Host Name	
MAC Address	MAC Clone
DHCP query frequency	Aggressive Mode 🔻
Extend the TTL value	● Yes ● No
Spoof LAN TTL value	● Yes ● No
	Αρρίγ

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.

WAN - Dual WAN	
GT-AC5300 provides Dual WAN support. Se Load Balance mode to optimize bandwidth, r WAN connections.	lect Failover mode to use a secondary WAN for backup network access. Select maximize throughput, minimize response time, and prevent data overload for both
Basic Config	
Enable Dual WAN	
Primary WAN	WAN
Secondary WAN	U5B •
Dual WAN Mode	Fail over Allow failback
Auto Network Detection	
Detect Interval	5 seconds
Failover Execution Time	Continous 12 times (= 60 seconds) detect network failed.
Enable Ping to Internet	● Yes ● No
	Αρρίγ

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.

WAN - Port Trigger					
Port Trigger allows you to temporarily op two methods for opening incoming data the the time and devices must use static IP access to the trigger port. Unlike port for forwarding allows multiple devices to she port. <u>Port Trigger FAQ</u>	en data ports w ports: port forwa addresses. Por warding, port tri warding, port tri warding pope	hen LAN devices requ arding and port trigger. rt trigger only opens th igger does not require in port and port trigger	vire unrestricted access Port forwarding opens the incoming port when a static IP addresses for only allows one client a	to the Internet. he specified dat LAN device red LAN devices. P t a time to acce	There are ta ports all quests fort loss the open
Basic Config					
Enable Port Trigger	• Yes (No			
Well-Known Applications	Please	select 🔹			
Trigger Port List (Max Limit : 32) 🔶					
Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
		No data in table.			
		Αρρίγ			

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** (G) to enter the port trigger information to the list. Click the **Delete** (G) 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 Forward	ling
Virtual Server / Port forwarding allows remote network (LAN). For a faster connection, some forwarding setting. Please refer to the P2P ap ports in router and redirect data through those If you want to specify a Port Range for clients the LAN IP address, and leave the Local Port	computers to connect to a specific computer or service within a private local area P2P applications (such as BitTorrent), may also require that you set the port plication's user manual for details. You can open the multiple port or a range of ports to a single client on your network. so the same network, enter the Service Name, the Port Range (e.g. 10200:10300), empty
 When your network's firewall is disabled an server/web server would be in conflict with 	d you set 80 as the HTTP server's port range for your WAN setup, then your http th ASUS Router's web user interface.
 When you set 20:21 as your FTP server's AC5300's native FTP server. Virtual Server / Port Forwarding 	port range for your WAN setup, then your FTP server would be in conflict with GT-
Basic Config	
Enable Port Forwarding	● Yes ◎ No
Famous Server List	Please select •
FTP Server Port	2021
Port Forwarding List (Max Limit : 32)	
Service Name Source Target	Add / Port Range Local IP Local Port Protocol 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 **3.12 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:

- 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.

WAN - DDNS		
DDNS (Dynamic Domain Name Sy dynamic public IP address, through and other DDNS services.	stem) is a service that allows network clients to connect to its registered domain name. The wireless router is embedd	the wireless router, even with a ded with the ASUS DDNS service
If you cannot use ASUS DDNS ser	rices, please go to <u>http://iplookup.asus.com/nslo</u>	okup.php to reach your internet IP
address to use this service.		
The wireless router currently uses a	a private WAN IP address.	
This router may be in the multiple-N	IAT environment and DDNS service cannot work in this environment	vironment.
Enable the DDNS Client	O Yes ● No	
Server	WWW.ASUS.COM V	
Host Name	Key in the name	.asuscomm.com
DDNS Status	Inactive	
HTTPS/SSL Certificate	Free Certificate from Let's Encrypt Import Yes	our Own Certificate O None
	Anniv	
	obby	

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**.



3.21 Wi-Fi Radar

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

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



To use Wi-Fi Radar:

1. From the navigation panel, go to **General** > **Wi-Fi Radar**, go to **Settings** and configure all the Wi-Fi Radar parameters.



- 2. Click **Start Data Collection**, and set the schedule for data collection.
- 3. Click Submit after you set all the parameters.



3.21.1 Wi-Fi Site Survey

Wi-Fi Site Survey allows you to search for wireless networks in your environment.



3.21.2 Wireless Channel Statistics

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



3.21.3 Advanced Troubleshooting

This feature shows Wi-Fi glitch statistics in your environment.



3.22 Wireless

3.22.1 General

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

Bridge (or named WDS - Wireless also be considered a repeater mo	Distribution System) function allows you to connect t de.	o an access point wirelessly. WDS may
Note:		
The function only support [Op corresponding authentication Click <u>Here</u> to modify. Please r	en System/NONE, Open System/WEP] security authomethod, please select Legacy as your wireless mode efer to this <u>FAQ</u> for more details.	entication method. To set up the first.
To enable WDS to extend the wire	less signal, please follow these steps :	
Select [WDS Only] or [Hyb Ensure that this wireless or S. Key in the remote AP mac router's MAC address. To get the best performant bandwidth, control channe You are currently using the A You are currently using the A	(d) mode and add MAC address of APs in Remote AP user and the APy want to correct to use the same in the remote AP list and open the remote AP's WDS is, please go to Advanced Settings > Wrieless > Gene and extension channel to every router in the network to channel abundwidth. Click target to modify to channel abundwidth. Click target to modify.	2 List. channel. management interface, key in the this ral and assign the same channel c.
Basic Config	to channel. Click <u>Here</u> to modily.	
2.4 GHz MAC		
5 GHz-1 MAC		
6 GHz MAC		
Band	2.4 GHZ 🗸	
AP Mode	AP only 🗸	
Connect to APs in list	Ves No	
Remote AP List (Max Limit :	1)	
	Remote AP List	Add / Delete
		Ð

To configure the basic wireless settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General**.
- 2. Select 2.4GHz, 5GHz or 6GHz 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, 5GHz or 6GHz 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, 5GHz and 6GHz 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**.

3.22.2 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 5. If you select **Client PIN** code, go to step 6.
- 5. To set up WPS using the router's WPS button, follow these steps:
 - a. Click **Start** or press the WPS button found at the 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.

3.22.3 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.

Bridge (or named WDS - Wireles wirelessly. WDS may also be co	s Distribution System) function allows your ASUS Router to connect to an access point insidered a repeater mode.
Note:	
The function only support [O	pen System/NONE, Open System/WEP] security authentication method. To set up the
corresponding authentication	n method, please select Legacy as your wireless mode first.
Click Here to modify. Please	refer to this <u>FAQ</u> for more details.
To enable WDS to extend the wi	reless signal, please follow these steps :
1. Select [WDS Only] or [Hy	brid) 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 ma	c in the remote AP list and open the remote AP's WDS management interface, key in the t
router's MAC address.	
4. To get the best performan	nce, please go to Advanced Settings > Wireless > General and assign the same channel
bandwidth, control chann	el, and extension channel to every router in the network.
You are currently using the A	Auto channel bandwidth. Click Here to modify.
You are currently using the A	Auto channel. Click Hene to modify.
Basic Config	
2.4 GHz MAC	FC:34:97:27:6A:10
5 GHz-1 MAC	FC:34:97:27:6A:14
8 GHz MAC	FC:34:97:27:6A:18
Read	
Dalio	
	AP Only 🗸
AP Mode	
AP Mode Connect to APs in list	● Yes ● No
AP Mode Connect to APs in list Remote AP List (Max Limit	• Yes • No
AP Mode Connect to APs in list Remote AP List (Max Limit	• Yes • No :4) Remote AP List Add / Delet
AP Mode Connect to APs in list Remote AP List (Max Limit	●Yes ●No *4) Remote AP List Add / Delet ▼ ①
AP Mode Connect to APs in list Remote AP List (Max Limit	•Yes •No *4) Remote AP List Add / Delet ••••••••••••••••••••••••••••••••••••
AP Mode Connect to AP's in list Remote AP List (Max Limit	• Yes ● No = 4) Remote AP List Add / Delet ↓ 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.

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

7. Click **Apply**.

3.22.4 Wireless MAC Filter

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

eless MAC filter allows you to	control packets from devices with specified MAC a	ddress in your Wireless LAN.
asic Config		
nd	2.4 GHz ~	
able MAC Filter	O Yes ● No	
AC Filter Mode	Accept ~	
AC filter list (Max Limit : 6	i4)	
	Client Name (MAC Address)	Add / Delete
	: FC:34:97:27:6A:10	\oplus
	No data in table.	

To set up the Wireless MAC filter:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter**.
- 2. Select the frequency band.
- 3. Tick Yes in the Enable Mac Filter field.
- 4. 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.
- 5. On the MAC filter list, click the **Add** 🕑 button and key in the MAC address of the wireless device.
- 6. Click Apply.

3.22.5 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.

This section allows you to set up you select "Authentication Metho	additional parameters for authorizing wireless clients through RADIUS server d" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".	r. It is required while
Band	2.4 GHZ ~	
Server IP Address		
Server Port	1812	
Connection Secret		

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 **3.22.1 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**.

3.22.6 Professional

The Professional screen provides advanced configuration options.

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

Wireless - Professional		
Wireless Professional Setting allows you	to set up additional parameters for wireless. But default values are recommended.	
Band	2.4 GHZ V	
Enable Radio	O Yes ● No	
Enable wireless scheduler	● Yes ● No	
Set AP Isolated	● Yes ● No	
Roaming assistant	Enable V Disconnect clients with RSSI lower than: -70 dBm	
Hide SSID	Ves O No	
Wireless Mode	Auto 🗸 Isig Protection	
802_11ax / Wi-Fi 6 mode	Enable V If compatibility issue occurs when enabling 802.11ax / Wi-Fi 6	
Wi-Fi Agile Multiband	Disable 🗸	
Target Wake Time	Disable 🗸	
Bluetooth Coexistence	Disable 🗸	
Enable IGMP Snooping	Enable 🗸	
Multicast Rate(Mbps)	Auto	
Preamble Type	Long	
AMPDU RTS	Enable 🗸	
RTS Threshold	2347	
DTIM Interval		
Beacon Interval	100	
Enable TX Bursting	Enable V	
Enable WMM	Enable 🗸	
Enable WMM No-Acknowledgement	Disable 🗸	
Enable WMM APSD	Enable 🗸	
Optimize AMPDU aggregation	Disable 🗸	
Modulation Scheme	Up to MCS 11 (NitroqAM/1024-QAM) V	
Airtime Fairness	Disable 🗸	
Multi-User MIMO	Disable 🗸	
OFDMA/802.11ax MU-MIMO	Disable 🗸	
Explicit Beamforming	Enable 🗸	
Universal Beamforming	Enable 🗸	
Tx power adjustment	Performance	
	Apply	

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.
- **Enable wireless scheduler**: Select **Yes** to enable and configure wireless scheduler. Select **No** to disable wireless scheduler.
 - 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 thefts 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
- **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.

4 Utilities

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
- Device Discovery v1.4.7.1 at <u>http://dlcdnet.asus.com/pub/ASUS/</u> LiveUpdate/Release/Wireless/Discovery.zip
- Firmware Restoration v1.9.0.4 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Rescue.zip</u>
- Windows Printer Utility v1.0.5.5 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Printer.zip</u>
- 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.

Firmware Restora	tion	×
<u>F</u> ilename:	l	<u>B</u> rowse
Status — After locating th	e firmware file, click Upload.	
	<u>U</u> pload <u>Q</u> lose	

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

From your computer's desktop, click
 Start > All Programs > ASUS Utility GT-AXE16000 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** 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.

	ASUS Printer Setup Utility - InstallShield Wizard
Printer.exe	Please wait while the InstallShield Wizard extracts the files needed to install ASUS Printer Setup Utility on your computer. This may take a few moments.
_	Extracting UsbService64.exe
	InstallShield
	< Back Next > Cancel

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 Next.

🕒 🖶 Add Printer	
Choose a printer port	
A printer port is a type of con	nection that allows your computer to exchange information with a printer.
Use an existing port:	LPT1: (Printer Port)
Oreate a new port:	
Type of port:	Standard TCP/IP Port
	Next Cancel

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

🚱 🖶 Add Printer		
Type a printer hostnan	ne or IP address	
Device type:	TCP/IP Device	Ţ
Hostname or IP address:	192.168.1.1	
Port name:	192.168.1.1	
Query the printer and auto	matically select the driver to use	
	(Next Cancel

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



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

on Settings		_
Port Name:	192.168.1.1	
Printer Name or IP Addres	is: 192.168.1.1	
Protocol		
Raw	() LPR	
Raw Settings		
Port Number:	9100	
LPR Settings		
Queue Name:	LPRServer	
LPR Byte Counting E	nabled	
SNMP Status Enabled	d	
Community Name:	public	
	1	
SNMP Device Index:		
SNMP Device Index:		

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

🚱 🌧 Add Printer	
Additional port	information required
The device is not 1. The device is 2. The network i 3. The device is 4. The address o If you think the a address and perfi-	found on the network. Be sure that: urned on. s connected. morpedy configured. no the previous page is correct. ddress is not correct, click Back to return to the previous page. Then correct the manather search on the network. If you are sure the address is correct, select the
Device Type Standard Custom	Generic Network Card • Settings-
	Next Cancel

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.

🕒 🖶 Ade	l Printer	3
Install	the printer driver Choose your printer from the list. Click Windows Update to see more models. To install the driver from an installation CD, click Have Disk.	
Manu Kyoce Lanier Lexma Micro	iacturer Printers Pri]
	Next Cancel	

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

/ISUS	
Task	
<i>-</i> .	Dit Torrent Setting
Task	Port
Settings	Use the default port Use the following port
a	Incoming port
Seneral General	Speed Limits:
	Maximum download speed: KB/S
Bit Torrent	Maximum upload speed: KB/S
	BilTorrent Network setting
📩 мzв	BitTorrent protocol encryption Encryption disabled
	Max peers allowed per torrent 100
	Effable DHT to activate trackless torrent download. DHT network
	Apply

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**.

Task J2E Sotting Settings isday:USENET Server for USENET Server © General USENET Server for 199 W ist Torvert USENET Server for 199 Maximum duvelical speed Kold Start USENet Terver USENet Terver 199 Maximum duvelical speed Kold Start Contem Password Outline Password 100 Number of concectors per fAZE task 2	/islis		
Task IZE Settings Settings Evelop USENET sever is download IZE New Contral USENET Sever is With Torrert USENET Sever is Status Status Status Status Bit Torrert USENET Sever is Distance KDIS Bit Torrert USENET Sever is Distance KDIS Distance Content Pasawed Distance Distance Distance Distance Distance Distance			
Settings USENET server to download NZE Base: Settings USENET Server to download NZE Base: Contract USENET Server to 119 Statument download speed KXPB Statument download speed KXPB Statument download speed KXPB Descent download speed Contem Pasawod Contem Pasawod Contem Pasawod Number of connections per KZB tass Z	Task	NZB Setting	
Settings USENET Server Ceneral USENET Server /ot Mathematical speed NBS State SSUFLIS connection only Password Contem Password Number of connections per fAZE tass Z	🧾 Task	Setup USENET server to download NZB files:	
USENET Sover Pot 19 X General Maamun dowisad speed X Bit Torrent SSUTLS connection only Variance Contem Pasaword Contem Pasaword Number of connections per AGE tasts	Settings	USENET Server	
General Matmum diveribad speed KBS Matmum diveribad speed KBS Stat SSUFLS convection only User name Plasawod Contem Pasawod Number of contexcions per fAZB tass 2	3 .22	USENET Server Port	119
Stuffscondult only User name Pasawod Contem Pasawod Number of contections per fu2b tasts	General	Maximum download speed	KB/S
User name	🔊 Bit Torrent	SSL/TLS connection only	
N28 Passed Contem Passed Number of contextons per NGD tass 2	2.2	User name	
Contirm Password Number of contections per N28 tasks 2	NZB	Password	
Number of connections per NZB tasks 2		Confirm Password	
		Number of connections per NZB tasks	2
Apply			Apply
2011 ASUSTeK Computer Inc. All rights reserved.			2011 ASUSTeK Computer Inc. All rights reserved.

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:

<u>https://www.asus.com/support</u> 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.

- 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 <u>https://rog.asus.com/networking/rog-rapture-gt-axe16000-model/helpdesk_download</u> 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 poweredon 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, follow these steps:
 - 1. Launch Internet Explorer, then click **Tools** > **Internet Options**.
 - In the General tab, under Browsing history, click Delete..., select Temporary Internet files and website files and Cookies and website data then click Delete.

eneral Se	ecurity P	rivacy (Content	Connections	Programs	Advar	nced
Home page							_
	To create	home pa	ge tabs,	type each ad	dress on its (own line	
	https://	'www.ms	n.com/?	PC=UF01		~	
		Use curre	ent	Use default	Use n	ew tab	
Startup –							_
OStar	t with tabs	from the	last ses	sion			
Start	t with hom	e page					
Tabs —							_
Change	how webp	bages are	displaye	d in tabs.	Te	abs	
Browsina	history —						_
Delete t	emporary ormation.	files, hist	ory, cool	des, saved pa	sswords, an	d web	
	te browsir	ig history	on exit				
Dele							
🗌 Dele				Delete	Set	tings	
Dele	ce			Delete	Set	tings	
Dele Appearan Colo	ce	Langui	ages	Delete	Set	tings ssibility	
Dele	ce	Langua	ages	Delete Fonts	Acce	tings ssibility	
Dele	ce	Langua	ages	Pelete	Acce	tings ssibility	

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:
 - Launch the web GUI. Go to Advanced Settings > Network Map> Clients and search for the device that you want to connect to the router.
 - 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.

LAN - DHCP Server			
DHCP (Dynamic Host Configuration Protocol server can assign each client an IP address supports up to 253 IP addresses for your loc) is a protocol for the automatic configue and informs the client of the of DNS set al network.	ration used on IP networks. Th rver IP and default gateway IF	ne DHCP 9. GT-AC5300
Basic Config			
Enable the DHCP Server	O Yes ● No		
GT-AC5300's Domain Name			
IP Pool Starting Address	192.168.1.2		
IP Pool Ending Address	192.168.1.254		
Lease time	86400		
Default Gateway			
DNS and WINS Server Setting			
DNS Server			
WINS Server			
Enable Manual Assignment			
Enable Manual Assignment	• Yes • No		
Manually Assigned IP around the DHCF	list (Max Limit : 64)		
Client Name (MAC A	ddress)	IP Address	Add / Delete
	-		Ð
	No data in table.		
	Apply		

 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.

Wireless - General	
Set up the wireless related information below.	
Enable Smart Connect	
Band	2.4GHZ ¥
Network Name (SSID)	Welcome to test
Hide SSID	● Yes ● No
Wireless Mode	Auto 🔻 🗖 Optimized for Xbox 🗳 b/g Protection
Channel bandwidth	20/40 MHz •
Control Channel	Auto Current Control Channel: 5
Extension Channel	Auto •
Authentication Method	WPA2-Personal
WPA Encryption	AES V
WPA Pre-Shared Key	12345678
Protected Management Frames	Disable 🔻
Group Key Rotation Interval	3600
	Арріу

- 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 > 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_XX_2G
SSID (5GHz):	ASUS_XX_5G
SSID (6GHz):	ASUS_XX_6G

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®

- 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.

utomatic con se of manual	figuration ma settings, dis	ay override man able automatic o	ual setting configurati	s. To ensure the on.
Automatica	lly detect se	ttings		
Use automa	atic configura	ation script		
Address				
Hudi 655				
oxy server				
lise a prov	v server for	vour LAN (These	e settings	will not apply to
ose a prox	PN connection	ons).	L Secongs	minoc apply to
dial-up or V				12
Address:	Ľ	Port:	80	Advanced
Address:		Port:	80	Advanced
Address:	proxy serve	Port: r for local addre	80 sses	Advanced

MAC OS

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

	Location: (Show: (Automatic Built-in Ethernet	•	
	TCP/IP PPPo	DE AppleTalk Pr	roxies Ethernet	
Vert We See Str SO Go Bypass these H	P Proxy b Proxy (HTTP) (ure Web Proxy (HTTPS) eaming Proxy (RTSP) CKS Proxy pher Proxy proxy settings for osts & Domains:		Set Password	sword
√ Use I	Passive FTP Mode (PA)	5V)		(7)

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

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

Windows®

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



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

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

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

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

5. Click OK when done.

General Connection IPv4 Connectivity: Interne IPv5 Connectivity: No network acces Media State: Duration: O3:29:3 Speed: 1.0 Gbp Details Activity Sent Configure Received Bytes: 71,424,646 Diagnose Ethernet Properties Wetworking Authentication Connect using: Internet Properties Wetworking Configure Internet Properties Use to following items: Configure Internet Properties Use to following items: Internet Properties Interne	d H1
Connection IPv4 Connectivity: Interne IPv6 Connectivity: No network access Media State: Connectivity: No network access Media State: Datalis Activity Continue Sent Ethernet Properties Ethernet Ethernet Properties Ethernet Et	et ss sed 311 ss s d d 411
Connectivity: Interne IPv4 Connectivity: No network access Media State: Enable Duration: 03:29:3 Speed: 1.0 Gbp Details Activity	et (1997)
IP-4 Connectivity: Interne IP-6 Connectivity: No network access Media State: Enable Duration: 03:29:3 Speed: 1.0 Gbp Details Operation: Activity	et ss ss dd 31 35 d 41 ×
IP-06 Connectivity: No network acces: Media State: Enable Duration: 03:29:3 Speed: 1.0 Gbp Details Activity Activity	ss ed 311 205 41 *1
Media state: Enable Duration: 03:29:3 Speed: 1.0 Gbp Details Image: Comparison of Co	ed 31 25 d 41 X
Duration: 03:29:3 Speed: 1.0 Gbp Details Activity Activity Sent — Properties Bytes: 71,424,646 70,727,24 Properties Disable Diagnose Ethemet Properties letworking Authentication Connect using: Intel(R) Ethemet Connection (2) 1219-V Configure This connection uses the following items: Internet Properties Intel(R) Ethemet Connection 4 (TCP/IPv4) Configure This connection uses the following items: Internet Properties	81 55 d 41 X
Speed: 1.0 Gbp Details Activity Sent Sent Sent Sent Sent Sent Sent Sent	d
Details Activity Sent Bytes: 71,424,646 70,727,24 Properties Disable Diagnose Itemet Properties Itemet Propertitemet Properties It	d H1 ×
Activity Received Bytes: 71,424,646 J 70,727,24 Properties Diable Diagnose Ethernet Properties Etworking Authentication Connect using: Intel(R) Ethemet Connection (2) 1219-V Configure This connection uses the following items: Configure Configure Config	d H1 ×
Activity Sent Received Bytes: 71,424,646 70,727,24 Properties Disable Diagnose Ethernet Properties letworking Authentication Connect using: Intel(R) Ethernet Connection (2) 1219-V Configure This connection uses the following items: Configure This connection uses the following items: Configure	d H1 ×
Activity	d H1 ×
Sent — Received Bytes: 71,424,646 70,727,24 Properties Disable Diagnose Ethernet Properties letworking Authentication Connect using: Intel(R) Ethemet Connection (2) 1219-V Configure This connection uses the following items: Configure This connection uses the following items: Configure	d H1 X
Bytes: 71,424,646 70,727,24	H1 ×
	×
	×
Ethernet Properties Ethernet Properties Ethernet Properties Ethernet Properties Ethernet Connection (2) 1219-V Configure This connection uses the following items: This connection uses the	×
Ethernet Properties etworking Authentication Connect using: Intel(R) Ethernet Connection (2) 1219-V This connection uses the following items: Configure This connection uses the following items: Thermet Protocol Version 4 (TCP/IPV4) Thermet Protocol Version 4 (TCP/IPV4) Microsoft LDP Protocol Driver	×
Ethernet Properties Letworking Authentication Connect using: Letworking Intel(R) Ethernet Connection (2) 1219-V This connection uses the following items: Configure This connection uses the following items: Letworking items Protocol Venion 4 (TCP/IPv4) Therosoft LLDP Protocol Driver	×
Internet: Protocol Internet: Protocol Driver Internet: Protocol Protoc	
interview Connect using: Intel(R) Ethemet Connection (2) 1213-V This connection uses the following items: Image: Configure (Configure) Interview Interview <td></td>	
Connect using: Intel(R) Ethemet Connection (2) 1219-V This connection uses the following items: Configure This connection uses the following items: Configure	`
Intel(R) Ethemet Connection (2) 1219-V Intel(R) Ethemet Connection (2) 1219-V Configure This connection uses the following items: Intel(R) Ethemet Protocol Venion 4 (TCP/IPv4) Intervent Protocol Driver Intervent LDP Protocol Driver Intervent Protocol Protocol Driver Intervent Protocol Pr	
	•
Configure This connection uses the following items: Image: Construction of the state of the stat	•
This connection uses the following items:	•
COS Packet Scheduler Cos Packet Scheduler Menosoft Version 4 (TCP/IPv4) Merosoft Version 4 (TCP/IPv4) Merosoft LDP Protocol Driver	•
Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 Adapter Multiplexor Protocol Internet Protocol Driver	
Microsoft Network Adapter Multiplexor Protocol	1
Microsoft LLDP Protocol Driver	
Internet Protocol Version 6 (TCP/IPv6)	
Link-Layer Topology Discovery Responder	
Link-Layer Topology Discovery Mapper I/O Driver	1
< >>	
Install Uninstall Properties	
Description	_
Transmission Control Protocol/Internet Protocol. The default	
wide area network protocol that provides communication	
across diverse interconnected networks.	
aternet Protocol Version 4 (TCP/IPv4) Properties	×
Remer Protocol Version 4 (TCP/IPV4) Properties	~
General Alternate Configuration	
You can get ID settings assigned automatically if your petwork support	
this capability. Otherwise, you need to ask your network administrator	te
for the appropriate IP settings.	rts r
Obtain an IP address automatically	rts vr
Olise the following IP address:	rts or
TD addresses	rts or
IP duuress:	rts vr
	rts vr
Subnet mask:	rts vr
Subnet mask:	rts vr
Subnet mask:	rts xr
Subnet mask: Default gateway:	rts xr
Subnet mask: Default gateway: Obtain DNS server address automatically Use the following DNS server addresses:	rts vr
Subnet mask: Default gateway: Obtan DNS server address automatically O Use the following DNS server addresses: Preferred DNS server:	rts xr
Subnet mask: Default gateway: Obtain DNS server address automatically O Use the following DNS server addresses: Preferred DNS server:	rts xr
Subnet mask: Default gateway: O Obtain DNS server address automatically Use the following DNS server addresses: Preferred DNS server: Alternate DNS server:	rts xr
Subnet mask: Default gateway: Control to a submatcally Outse the following DNS server addresses: Preferred DNS server: Alternate DNS server: Control to a se	тts x
Subnet mask: Default gateway: Obtain DNS server address automatically Ouse the following DNS server addresses: Prefered DNS server: Alternate DNS server: Validate settings upon exit Advanced.	rts vr

MAC OS

- Click the Apple icon located on the top left of your screen.
- 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.

	L	ocation: Automatic		\$	
		Show: Built-in Ether	net	;	
	ТСР	/IP PPPoE AppleTa	lk Proxies Et	hernet	
Г	Configure IPv4:	Using DHCP	:		
	IP Address:	192.168.182.103	(Renew DHC	P Lease
	Subnet Mask:	255.255.255.0	DHCP Client ID:		
	Router:	192.168.182.250		(If required)	
	DNS Servers:	192.168.128.10			(Optional)
5	Search Domains:				(Optional)
	IPv6 Address:	fe80:0000:0000:0000:	0211:24ff:fe32:b1	8e	
		Configure IPv6			(?)

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

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

Windows®

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

