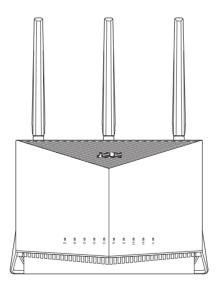
# **User Guide**

# **RT-AX86S**

## Wireless-AX5700 Dual-band Gigabit Router





E19942 First Edition March 2022

#### Copyright © 2022 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		ing to know your wireless router	
1.1		ome!	
1.2		ge contents	
1.3	Your v	wireless router	7
1.4	Positio	oning your wireless router	9
1.5	Setup	Requirements	10
2	Getti	ing started	
2.1	Route	r Setup	11
	A.	Wired connection	11
	В.	Wireless connection	12
2.2	Quick	Internet Setup (QIS) with Auto-detection	14
2.3	Conne	ecting to your wireless network	16
3	Conf	iguring the General settings	
3.1	Loggi	ng into the Web GUI	17
	3.1.1	Setting up the wireless security settings	19
	3.1.2	Managing your network clients	20
	3.1.3	Monitoring your USB device	21
3.2	Creati	ng a Guest Network	24
3.3	AiProt	tection	
	3.3.1	Network Protection	27
	3.3.2	Setting up Parental Controls	31
3.4	Using	the Traffic Manager	
	3.4.1	Managing QoS (Quality of Service) Bandwidth	າ34
3.5	Traffic	Analyzer	
3.6	Game		
	3.6.1	Gear Accelerator	
	3.6.2	Mobile Game Mode	
	3.6.3	Open NAT	40

## Table of contents

2 7			4.1
3.7	Using	the USB Application	
	3.7.1	Using AiDisk	41
	3.7.2	Using Servers Center	43
	3.7.3	3G/4G	48
3.8	Using	AiCloud 2.0	50
	3.8.1	Cloud Disk	51
	3.8.2	Smart Access	52
	3.8.3	AiCloud Sync	53
4	Conf	iguring the Advanced Settings	
4.1	Wirele	255	
	4.1.1	General	54
	4.1.2	WPS	57
	4.1.3	Bridge	59
	4.1.4	Wireless MAC Filter	61
	4.1.5	RADIUS Setting	62
	4.1.6	Professional	63
4.2	LAN		66
	4.2.1	LAN IP	66
	4.2.2	DHCP Server	67
	4.2.3	Route	69
	4.2.4	IPTV	70
4.3	WAN		71
	4.3.1	Internet Connection	71
	4.3.2	Dual WAN	73
	4.3.3	Port Trigger	74
	4.3.4	Virtual Server/Port Forwarding	76
	4.3.5	DMZ	79
	4.3.6	DDNS	80
	4.3.7	NAT Passthrough	81

## Table of contents

4.4	IPv6		
4.5	Firewa	all	
	4.5.1	General	83
	4.5.2	URL Filter	83
	4.5.3	Keyword filter	84
	4.5.4	Network Services Filter	85
4.6	Admiı	nistration	
	4.6.1	Operation Mode	
	4.6.2	System	
	4.6.3	Firmware Upgrade	89
	4.6.4	Restore/Save/Upload Setting	89
4.7	Syster	n Log	
5	Utilit	ies	
5.1	Devic	e Discovery	91
5.2	Firmw	vare Restoration	92
5.3	Settin	g up your printer server	
	5.3.1	ASUS EZ Printer Sharing	
	5.3.2	Using LPR to Share Printer	97
5.4	Down	load Master	102
	5.4.1	Configuring Bit Torrent download settings	
	5.4.2	NZB settings	104
6	Trou	bleshooting	
6.1	Basic	Troubleshooting	105
6.2	Frequ	ently Asked Questions (FAQs)	108
Apr	pendic	es	
		Support	

# 1 Getting to know your wireless router

## 1.1 Welcome!

Thank you for purchasing an ASUS RT-AX86S Wireless Router! The strikingly designed black chassis with gaming-inspired red accents, RT-AX86S features a 2.4GHz and 5GHz dual 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

☑ RT-AX86S Wireless Router

✓ Network cable (RJ-45)

☑ Power adapter

☑ Quick Start Guide

☑ Warranty card

#### NOTES:

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

## **1.3 Your wireless router**

1 WPS LED Off: WPS is not processing. On: WPS is processing.
<ul> <li>LAN 1~4 LEDs</li> <li>Off: No power or no physical connection.</li> <li>On: Has physical connection to a local area network (LAN).</li> </ul>
<ul> <li>WAN (Internet) LED</li> <li>Red: No IP or no physical connection.</li> <li>On: Has physical connection to a wide area network (WAN).</li> </ul>
<ul> <li>USB LED</li> <li>Off: No power or no physical connection.</li> <li>On: Has physical connection to USB devices.</li> </ul>
<ul> <li>2.4GHz LED</li> <li>Off: No 2.4GHz signal.</li> <li>On: Wireless system is ready.</li> <li>Flashing: Transmitting or receiving data via wireless connection.</li> </ul>
<ul> <li>6 5GHz LED</li> <li>Off: No 5GHz signal.</li> <li>On: Wireless system is ready.</li> <li>Flashing: Transmitting or receiving data via wireless connection.</li> </ul>

7	Power LED
	Off: No power.
	<b>On</b> : Device is ready.
	Flashing slow: Rescue mode.
8	LED On/Off button
	This button turns on/off the LED indicators.
9	Power (DCIN) port
	Insert the bundled AC adapter into this port and connect your router to a power source.
10	Power switch
	Press this button to power on or off the system.
A	Reset button
	This button resets or restores the system to its factory default settings.
12	USB 2.0 port
U	Insert a USB 2.0 device such as a USB hard disk or a USB flash drive into this port.
	Insert your iPad's USB cable into this port to charge your iPad.
13	USB 3.0 port
	Insert a USB 3.0 device such as a USB hard disk or a USB flash drive into this port.
	Insert your iPad's USB cable into this port to charge your iPad.
14	WAN (Internet) port
	Connect a network cable into this port to establish WAN connection.
15	LAN 1~4 ports
	Connect network cables into these ports to establish LAN connection.
16	WPS button
-	This button launches the WPS Wizard.

#### NOTES:

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

DC Power adapter		DC Output: +12V with 3A current +19.5V with 2.31A current			
Operating Temperature	0~40°C	Storage	0~70°C		
Operating Humidity	50~90%	Storage	20~90%		

## **1.4 Positioning your wireless router**

For optimal wireless transmission between the wireless router and connected wireless devices, ensure that you:

- Place the wireless router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the wireless router away from metal obstructions and away from direct sunlight.
- Keep the wireless router 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.
- Orient the 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 dual band technology, your wireless router supports 2.4GHz and 5GHz wireless signals simultaneously. This allows you to do Internet-related activities such as Internet surfing or reading/writing e-mail messages using the 2.4GHz band while simultaneously streaming high-definition audio/video files such as movies or music using the 5GHz band.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

#### **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: <u>https://downloadcenter.intel.com/</u>

# 2 Getting started

## 2.1 Router Setup

#### **IMPORTANT!**

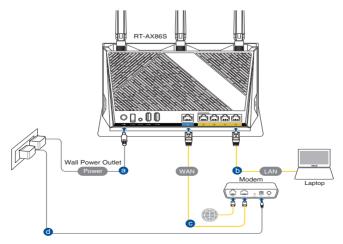
- Use a wired connection when setting up your wireless router to avoid possible setup problems.
- Before setting up your ASUS wireless router, do the following:
  - If you are replacing an existing router, disconnect it from your network.
  - Disconnect the cables/wires from your existing modem setup.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

#### 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.



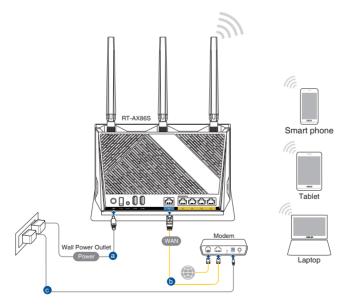
- 2. The web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <u>http://router.asus.com</u>
- 3. Set up a password for your router to prevent unauthorized access.

Login Information Setup					
Change the router password to prevent unauthorized access to your ASUS wireless router.					
Router Login Name	admin				
New Password					
Retype Password	Show password				

#### **B.** Wireless connection

#### To set up your wireless router via wireless connection:

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



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

Wi-Fi Name (SSID): ASUS\_XX

- \* XX refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back of your router.
- 3. Once connected, the web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <u>http://router.asus.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 3.1.1
   Setting up the wireless security settings of this user manual.



### 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:

1. Launch a web browser. You will be redirected to the ASUS Setup Wizard (Quick Internet Setup). If not, key in <u>http://router.asus.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 **Manual Setting** and manually configure your connection settings.

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

Wireless Settings	Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network. 2.4GHz Network Name (SSID)		
	2.4GHz Wireless Security	0	
	5GHz Network Name (SSID)		
	5GHz Wireless Security	•	
	Separate 2.4GHz and 5GHz		
	Previous Apply		

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

NEARING WARDER		
Login Username / Password	Change the router password to prevent unauthorized access to your ASUS wireless router.	
	Router Login Name	
	New password	
	Retype Password	
	Previous Next	

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

## 2.3 Connecting to your wireless network

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

#### To connect to your network:

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

#### NOTES:

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

## **3 Configuring the General settings**

## 3.1 Logging into the Web GUI

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

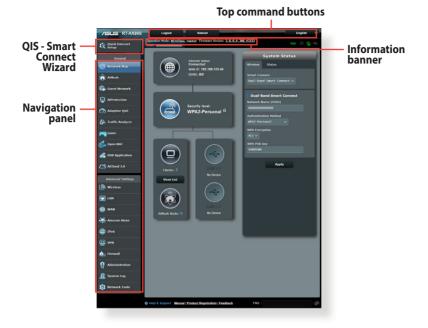
NOTE: The features may vary with different firmware versions.

#### To log into the web GUI:

- 1. On your web browser, manually key in the wireless router's default IP address: <u>http://router.asus.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-detection**.

<b>Q</b> 4	Sign In rt-ax86s
	Sign in with your ASUS router account
	Username
	Password
	Sign In

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



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

#### 3.1.1 Setting up the wireless security settings

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

#### To set up the wireless security settings:

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

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

#### 2.4GHz security settings



#### **5GHz security settings**



3. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.

4. From the **WEP Encryption** dropdown list, select the encryption method for your wireless network.

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

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

#### 3.1.2 Managing your network clients



#### To manage your network clients:

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

#### 3.1.3 Monitoring your USB device

The ASUS Wireless Router provides a USB port for connecting a USB device or a USB printer to allow you to share files and printer with clients in your network.



**NOTE:** To use this feature, you need to plug a USB storage device, such as a USB hard disk or a USB flash drive, to 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 Plug-n-Share Disk Support List at <u>http://event.asus.com/networks/disksupport</u>.

**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 2.0. For more details, refer to the section **3.7 Using the USB Application** and **3.8 Using AiCloud 2.0** in this user manual.

#### To monitor your USB device:

- 1. From the navigation panel, go to **General** > **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 **3.7.2 Using Servers Center** in this user manual.
- The wireless router works with most USB HDDs/Flash disks (up to 2TB size) and supports read-write access for FAT16, FAT32, EXT2, EXT3, and NTFS.

#### Safely removing the USB disk

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

#### To safely remove the USB disk:

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



## 3.2 Creating a Guest Network

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

**NOTE:** RT-AX86S supports up to six SSIDs (three 2.4GHz and three 5GHz SSIDs).

#### To create a guest network:

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

Guest Network			
	The Guest Network provides Interne your local network.	et connection for guests but	restricts access to
Network Name (SS	ID)		
Authentication Method			
Network Key	Enable	Enable	Enable
Time Remaining			Default setting by Alexa/IFTTT
Access Intranet			
Network Name (SS			
Authentication			
Method			
Network Key	Enable	Enable	Enable
Time Remaining			Default setting by Alexa/IFTTT
Access Intranet			

4. To configure additional options, click **Modify**.

Guest Network					
your loc	est Network provides Inte al network.	rnet connection for guests but	restricts access to		
Network Name (SSID)	ASUS_2G_Guest				
Authentication Method	Open System				
Network Key	None	Enable	Enable		
Time Remaining	Unlimited access		Default setting by Alexa/IFTTT		
Access Intranet	off				
	Remove				
Network Name (SSID)	ASUS 5G Guest				
Authentication Method	Open System				
Network Key	None	Enable	Enable		
Time Remaining	Unlimited access		Default setting by Alexa/IFTTT		
Access Intranet	off				
	Remove				

- 5. Click Yes on the Enable Guest Network screen.
- 6. Assign a wireless name for your temporary network on the **Network Name (SSID)** field.
- 7. Select an Authentication Method.
- 8. Select an **Encryption** method.
- 9. Specify the Access time or choose Limitless.
- 10.Select Disable or Enable on the Access Intranet item.
- 11. When done, click **Apply**.

## 3.3 AiProtection

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



#### **3.3.1 Network Protection**

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



#### **Configuring Network Protection** To configure Network Protection:

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

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

Default router login username and password changed -		5
Wireless password strength check -	Very Weak	
Wireless encryption enabled -	Strong	
WPS Disabled -		
UPnP service disabled -		
Web access from WAN disabled -	Yes	
PING from WAN disabled -	Yes	
DMZ disabled -	Yes	
Port trigger disabled -	Yes	
Port forwarding disabled -	Yes	
Anonymous login to FTP share disabled -	Yes	
Disable guest login for Network Place Share -	Yes	D
Malicious Website Blocking enabled -		
Vulnerability Protection enabled -		
Infected Device Prevention and Blocking -		
Micro's database for always-up-to-date protection.		

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

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

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

b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.

c. Go back to the **Router Security Assessment** page and click **Close** to exit the page.

- 5. To automatically configure the security settings, click **Secure Your Router.**
- 6. When a message prompt appears, click **OK**.

#### **Malicious Sites Blocking**

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

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

#### **To enable Malicious Sites Blocking:**

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

#### **Two-Way IPS**

Two-Way IPS (Intrusion Prevention System) protects your router from network attacks by both blocking malicious incoming packets and detecting suspicious outgoing packets.

**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 on **Network Protection**.
- 3. From the Two-Way IPS pane, click ON.

#### **Infected Device Prevention and Blocking**

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

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

#### To enable Infected Device Prevention and Blocking:

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

#### **To configure Alert Preference:**

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

#### 3.3.2 Setting up Parental Controls

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

To go to the Parental Controls main page:

- 1. From the navigation panel, go to **General** > **AiProtection**.
- 2. From the **AiProtection** main page, click on the **Parental Controls** tab.



#### 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 on the **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 drop down 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.



#### 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 drop down list box.

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

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

## 3.4 Using the Traffic Manager

#### 3.4.1 Managing QoS (Quality of Service) Bandwidth

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

	Logout	Reboot				. I	English 🔻			
Cuick Internet	Operation Mode: Wi SSID: ASUS_26 ASI	reless router Firmwa 15_56	re Version: 3.0.	D.4.384_43	60		8 🖻 🔶			
General	Network Protection	Malicious Sites Blocking	Two-Way IPS	Infecte	d Device Prevention a Blocking	nd	Parental Controls			
Network Map	AiProtection - Time Scheduling Web & Apps Filters					Time Scheduling				
Guest Network		Time Scheduling Time Scheduling		t the time lii	nit for a client's netwo	rk usage. To	ouse			
AiProtection					e client whose networ					
Adaptive QoS	control: You may also key in the clients MAC address in the [Clients MAC Address] column 2. In the [Add / Delete] column, click the plus(+) icon to add the client. 3. In the [The Management] column, click the edit con to edit the Adiro Schedule. 4. Select the destred time slots for allowed access times. Forgand hold to create									
🕼. Traffic Analyzer										
Game		Ionger tim 5. Click [OK]	e slots. to save the settir	ngs made.						
👸 USB Application							estricted			
AiCloud 2.0	by default. 2. Please disable <u>NAT Acceleration</u> for more precise scheduling control.									
Advanced Settings	Enable Time Scheduling ON									
Wireless	System Time Thu, Aug 23 06:36:52 2018 System Time General Terminder: This System Time zone is different from your locale setting,									
🕎 LAN	Client List (Max Limit : 16)									
🛞 WAN	•	Client Name (MAC Address)			Time Management	Add	/ Delete			
🍟 Alexa & IFTTT	2	ex: 18:31:6F:31:31:	30	•	-		Ð			
Alexa & II III		No data in table.								

#### To set up bandwidth priority:

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

NOTE: Get the bandwidth information from your ISP.

#### 3. Click Save.

**NOTE:** The User Specify Rule List is for advanced settings. If you want to prioritize specific network applications and network services, select **User-defined QoS rules** or **User-defined Priority** from the drop-down list on the upper-right corner.

4. On the user-defined QoS rules page, there are four default online service types – web surf, HTTPS and file transfers. Select your preferred service, fill in the Source IP or MAC, Destination Port, Protocol, Transferred and Priority, then click Apply. The information will be configured in the QoS rules screen.

#### NOTES:

- To fill in the source IP or MAC, you can:
  - a) Enter a specific IP address, such as "192.168.122.1".
  - b) Enter IP addresses within one subnet or within the same IP pool, such as "192.168.123.\*", or "192.168.\*.\*"
  - c) Enter all IP addresses as "\*.\*.\*" or leave the field blank.
  - d) The format for the MAC address is six groups of two hexadecimal digits, separated by colons (:), in transmission order (e.g. 12:34:56:aa:bc:ef)
- For source or destination port range, you can either:
  - a) Enter a specific port, such as "95".
  - b) Enter ports within a range, such as "103:315", ">100", or "<65535".
- The Transferred column contains information about the upstream and downstream traffic (outgoing and incoming network traffic) for one section. In this column, you can set the network traffic limit (in KB) for a specific service to generate specific priorities for the service assigned to a specific port. For example, if two network clients, PC 1 and PC 2, are both accessing the Internet (set at port 80), but PC 1 exceeds the network traffic limit due to some downloading tasks, PC 1 will have a lower priority. If you do not want to set the traffic limit, leave it blank.

- 5. On the User-defined Priority page, you can prioritize the network applications or devices into five levels from the user-defined QoS rules' dropdown list. Based on priority level, you can use the following methods to send data packets:
  - Change the order of upstream network packets that are sent to the Internet.
  - Under **Upload Bandwidth** table, set **Minimum Reserved Bandwidth** and **Maximum Bandwidth Limit** for multiple network applications with different priority levels. The percentages indicate the upload bandwidth rates that are available for specified network applications.

#### NOTES:

- Low-priority packets are disregarded to ensure the transmission of high-priority packets.
- Under Download Bandwidth table, set Maximum Bandwidth Limit for multiple network applications in corresponding order. The higher priority upstream packet will cause the higher priority downstream packet.
- If there are no packets being sent from high-priority applications, the full transmission rate of the Internet connection is available for lowpriority packets.
- 6. Set the highest priority packet. To ensure a smooth online gaming experience, you can set ACK, SYN, and ICMP as the highest priority packet.

**NOTE:** Ensure to enable QoS first and set up the upload and download rate limits.

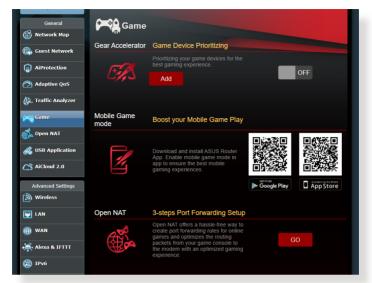
# 3.5 Traffic Analyzer

The traffic monitor feature allows you to access the bandwidth usage and speed of your Internet, wired, or wireless networks. It allows you to monitor network traffic in real-time or on a daily basis. It also offers an option to display the network traffic within the last 24 hours.

/ISUS	Logout		Reboot			-	English	Ŧ
Quick Internet	Operation Mode: M SSID: ASUS_26 A		er Firmware V	ersion: 3.0	.0.4.384_436	D	App 🔏 🤅	è 4
General	Statistic Traffic	Monitor						
Network Map	Traffic Monito							
Guest Network	Traffic Monitor allows			tgoing packe	ts of the following			
AiProtection		Internet		Wired		Wirele		
Adaptive QoS	Reception							
🕼. Traffic Analyzer	Transmission							
Game	NOTE: Packets from Traffic Monitor FAC		evenly transmitter	I to the wired				
🖓 USB Application	Internet Conne	_	Wired W	ireless				
AiCloud 2.0	1025.39 K8/s			WAN			Thu 02:29 pm / 454.10	KB/s
Advanced Settings	717.77 KB/s							-1
Wireless								
LAN LAN	512.70 K8/s							
🛞 WAN								
Alexa & IFTTT	256.35 KB/s							
IPv6								W
VPN	Current		Average		Max	mum	Total	
🚵 Firewall	0.08 KB		17.66 KB	5	1013.2	2 KB/s	10.35 MB	
Administration	0.04 KB	8	0.44 KB/	3	18.24	KB/s	263.85 KB	
👿 System Log								
🔯 Network Tools								

**NOTE:** Packets from the Internet are evenly transmitted to the wired and wireless devices.

# 3.6 Game



# 3.6.1 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**.
- 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 🔘 .

# 3.6.2 Mobile Game Mode

Download the ASUS router app on your mobile phone, enable the Mobile Game Mode with one click to prioritize your mobile phone for a better online gaming experience.

#### To configure Mobile Game Mode:

- 1. Download the ASUS router app, follow the steps to complete the network settings.
- 2. From the main page, click
- 3. Click **GO** to configure Mobile Game Mode on your mobile phone.





# 3.6.3 Open NAT

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.

#### To configure Open NAT:

- 1. From the navigation panel, go to **General > Game**.
- 2. From the **Open NAT** tab, click **GO**.
- 3. Enable Port Forwarding.
- 4. From the **Game Profile** field, click **Add**.
- 5. Select your game and complete basic settings.
- 6. Click **OK**.

# 3.7 Using the 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 a 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.

# 3.7.1 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 **General** > **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.

/1545	Logout	Reboot		English	•
Quick Internet	Operation Mode: <u>WireTess</u> SSID: <u>ASUS_2G</u> <u>ASUS_5G</u>	router Firmware Version: 3.0.0.4.384_4360		App 🖧 🖗	*
General		2 3			
AiProtection	My FTP server is sha	red.: Decide how to share your folders.			
Adaptive QoS	• admin rights				
Game	<ul> <li>limited access rights</li> <li>limitless access rights</li> </ul>				
🔊 USB Application	Account	Password	Read	Write	
AiCloud 2.0					
Advanced Settings					
(in) Wireless		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.

General	
AiProtection	Create your domain name via the ASUS DDNS services. O I will use the service
🔅 Traffic Analyzer	Acystem Live mace assistant com
Advanced Settings	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.

## 3.7.2 Using Servers Center

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

#### **Using Media Server**

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

**NOTE**: Before using the DLNA Media Server function, connect your device to RT-AX86S's network.

/ISUS	Logout Reboot	English 🔻
Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.384_4360</u> SSID: <u>ASUS_26</u> <u>ASUS_56</u>	Арр 💩 🔂 🔶
General	Media Server Network Place (Samba) Share / Cloud Disk FTP Share	
General	Media Server	5
Guest Network	Setup the iTunes and UPnP media server. Thunes Server	_
AiProtection	Enable iTunes Server? OFF	
Adaptive QoS	Media Server	
A>	Enable UPnP Media Server ON	
A. Traffic Analyzer	Media Server Name RT-AX62U-3130	
Game	Media Server Status Idle	
🚲 USB Application	Media Server Path Setting O All Disks Shared   Manual Media Server Path	
AiCloud 2.0	Apply	

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

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

/isus	Logout Reboot	English 🔻
Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.384_4360</u> SSID: <u>ASIS 26</u> Media Server Network Place (Samba) Share / Cloud Disk FTP Share	Арр 🖧 🔁 🗲
Network Map	USB Application - Network Place (Samba) Share / Cloud Disk	<b></b>
Guest Network	Set the account and permission of network place(samba) service. Enable Share ON	
Adaptive QoS	Allow guest logn OFF Usemame and password is necessary to log	j in network
🙀. Traffic Analyzer	Device Name         RT-AX82U-31.30           Work Group         WBRCRDUP	
Game	Apply	
AiCloud 2.0		a e 🔊
Advanced Settings	Admin RT-AX82U-3130 R/W R	No
Wireless	Save	
()) WAN		

#### To use Samba share:

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

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.

Add new account	×
i New account has no r	ead/write access rights.
Account:	ce(samba) service.
Password:	ON
Retype password:	
	Add (Samba

#### 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.

Add new folder in sda1	×
The default access rights	for a new folder is read/write.
Folder Name:	place(samba) service.
	Add

- 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 3.1.3 Monitoring your USB device.

/isus	Logout Reboot English V
Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.384_4360</u> App 🛞 🕞 🚓
General	Media Server Network Place (Samba) Share / Cloud Disk FTP Share
Network Map	USB Application - FTP Share
Guest Network	Set the account and permission of FTP service.
AiProtection	Enable FTP OFF
Adaptive QoS	Allow anonymous login OFF Username and paseword is necessary to log in FTP service.
Traffic Analyzer	Maximum number of concurrent connections 5
🙈 Game	Character set on FTP Server UTF-8 •
USB Application	Apply
AiCloud 2.0	
Advanced Settings	Admin RT-AXS2U R/W W R No
Mireless	
	Saye
🌐 WAN	

#### To use FTP Share service:

**NOTE:** Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.6.1 Using AiDisk**.

- 1. From the navigation panel, click **General** > **USB application** > **Media Services and Servers** > **FTP Share** tab.
- 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. Click Apply to confirm the changes.
- 4. 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.

# 3.7.3 3G/4G

3G/4G USB modems can be connected to RT-AX86S to allow Internet access.

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

K Setup							-	
General	Internet Connection	Dual WAN	Port Trigger	Virtual Ser Forwa	ver / Port rding	DMZ	DDNS	NAT Passthrough
Network Map	USB Modem / USB Tethering							
🛞 Guest Network	Switch to USB mode t		USB wireless o	longle or Android pl				
AiProtection	WAN Index							
•	WAN Type		USB					
Adaptive QoS	Basic Config	_		_				
🕼. Traffic Analyzer	Enable USB Mode		ON					
Game	Select USB Device		USB	Noden 🔹				
🔊 USB Application	APN Configuration							
	Telecommunications S	tandards						
AiCloud 2.0	APN Service(optional)							
Advanced Settings	Dial Number							
Wireless	User Name							
	Password							
	Authentication							
()) WAN	PIN code							
Alexa & IFTTT	USB Adapter							
1Pv6	USB MTU							
++ VPN	Special Requireme	ent from ISP						
	Extend the TTL value		• Ye					
Firewall	Spoof LAN TTL value		• Ye	s <sup>O</sup> No				
Provident Administration				Apply				
🧱 System Log								
🔯 Network Tools								
	Help & Support	Manual   <u>Utility</u>	Feedback   P	roduct Registratio	n FAQ			P
					2010 40	ICT-N Com		. All rights reserved.

#### To set up 3G/4G internet access:

- 1. From the navigation panel, click **General** > **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.

# 3.8 Using 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 2.0:

- 1. From Google Play Store or Apple Store, download and install the ASUS AiCloud 2.0 app to your smart device.
- 2. Connect your smart device to your network. Follow the instructions to complete the AiCloud 2.0 setup process.

# 3.8.1 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>https://router.asus.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 2.0 for security reason.

#### 3.8.2 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 4.3.6 DDNS.
- By default, AiCloud 2.0 provides a secure HTTPS connection. Key in <u>https://[yourASUSDDNSname].asuscomm.com</u> for a very secure Cloud Disk and Smart Access usage.

# 3.8.3 AiCloud Sync

	Logout Reboot	Eng	jlish 🔻
Quick Internet Setup General	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>ASUS ASUS_SG</u> AlCloud 2.0 AlCloud Sync Settings Log	Арр 🤰	š <u>6</u> 4
🛞 Network Map	AiCloud 2.0 - AiCloud Sync		
Guest Network			
🔿 Traffic Manager	USB Enables AlCloud Sync functionality. For step-by-step EAG	p instructions,	go to
Parental Controls	OFF		
👸 USB Application	Cloud List		_
AiCloud 2.0		nection Status	Delete
Advanced Settings	No data in table.		
Wireless			

#### To use AiCloud Sync:

- 1. Launch AiCloud 2.0, click AiCloud Sync.
- 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**.

# 4 Configuring the Advanced Settings

# 4.1 Wireless

# 4.1.1 General

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

Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS_26</u> <u>ASUS_56</u>	ware Version: <u>3.0.0.4.384.4360</u> App <u>8</u> <u>C</u> <del>C</del>		
General	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roaming Block List		
Network Map	Wireless - General			
Guest Network	Set up the wireless related information below	٨		
AiProtection	Enable Smart Connect	OFF		
Adaptive QoS	Band	2.4GHZ *		
	Network Name (SSID)	ASUS_2G		
K. Traffic Analyzer	Hide SSID	● Yes O No		
Game Game	Wireless Mode	Auto 🔹 🗖 Optimized for Xbox 🖾 big Protection		
🔊 USB Application	Channel bandwidth	20/40 MHz •		
AiCloud 2.0	Control Channel	Auto  Current Control Channel: 4		
C MICIONU 210	Extension Channel	AUTO V		
Advanced Settings	Authentication Method	WPA2-Personal •		
Wireless	WPA Encryption	AES V		
	WPA Pre-Shared Key	12345678		
() WAN	Protected Management Frames	Disable •		
Alexa & IFTTT	Group Key Rotation Interval	3600		
т () 1Рv6		Apply		

#### To configure the basic wireless settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
- 2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
- 3. Assign a unique name containing up to 32 characters for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

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

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

**40MHz:** Select this bandwidth to maximize the wireless throughput.

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

- 7. Select the operating channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
- 8. Select any of these authentication methods:
  - Open System: This option provides no security.
  - **Shared Key**: You must use WEP encryption and enter at least one shared key.

- WPA/WPA2 Personal/WPA Auto-Personal: This option provides strong security. You can use either WPA (with TKIP) or WPA2 (with AES). If you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).
- WPA/WPA2 Enterprise/WPA Auto-Enterprise: This option provides very strong security. It is with integrated EAP server or an external RADIUS back-end authentication server.
- Radius with 802.1x

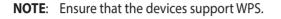
**NOTE:** Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto** and **encryption method** is **WEP** or **TKIP**.

- 9. Select any of these WEP (Wired Equivalent Privacy) Encryption options for the data transmitted over your wireless network:
  - **Off**: Disables WEP encryption
  - 64-bit: Enables weak WEP encryption
  - 128-bit: Enables improved WEP encryption

10.When done, click **Apply**.

## 4.1.2 WPS

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



Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS 26</u> <u>ASUS 56</u>	ware Version: <u>3.0.0.4.384.4360</u> App <u>&amp; C</u> +
General	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roaming Block List
Metwork Map	Wireless - WPS	
Guest Network	WPS (Wi-Fi Protected Setup) provides easy the PIN code or the WPS buttton.	and secure establishment of a wireless network. You can configure WPS here via
AiProtection	Enable WPS	
Adaptive QoS	Current Frequency	2.4GHz
🕼. Traffic Analyzer	Connection Status	Idle
Game	Configured	Yes Reset
👸 USB Application	AP PIN Code	12345670
AiCloud 2.0 Advanced Settings Wireless	button on the client's WLAN adapter a Method2: Start the client WPS proces field and click Start. Please check the	is interface (or press the physical WPS bullon on the router), then press the WPS nd wait for about three minutes to make the connection. Is and get the client PIN code. Enter the client's PIN code on the Client PIN code user manual of your wreless client to see if it supports the WPS function. If your PS function, you have to configure the wireless client manually and set the same
🜐 WAN	WPS Method:	Push button     Client PIN Code  Start

#### To enable WPS on your wireless network:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WPS** tab.
- 2. In the Enable WPS field, move the slider to ON.
- 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.

- 3. In the WPS Method field, select **Push Button** or **Client PIN** code. If you select **Push Button**, go to step 4. If you select **Client PIN** code, go to step 5.
- 4. 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.
- 5. To set up WPS using the Client's PIN code, follow these steps:
  - a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.
  - b.Key in the Client PIN code on the text box.
  - c. Click **Start** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

# 4.1.3 Bridge

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

Quick Internet Setup	Operation Mode: <u>Mincless router</u> Firmware Version: <u>3.0.0.4.384_4360</u> App <u>App</u> App <u>App</u> <u>App</u> App			App 🔱 🔁 🔶
General	General WPS WDS Wirele	ss MAC Filter RADIUS Setting	Professional Roaming E	Block List
Metwork Map	Wireless - Bridge			
Guest Network	Bridge (or named WDS - Wireless Di WDS may also be considered a repe			
AiProtection	to use half of the access point's origin Note:The function only support [Oper		P) security authentication meth	iod.
Adaptive QoS	To enable WDS to extend the wireles			
Traffic Analyzer	2. Ensure that this wireless route	mode and add MAC address of AP er and the AP you want to connect to	o use the same channel.	
Game	router's MAC address.	the remote AP list and open the rem		
\delta USB Application	<ol> <li>To get the best performance, please go to Advanced Settings &gt; Wireless &gt; Coneral and assign the same channel bandwidth, control channel, and extension channel to every router in the network.</li> </ol>			
AiCloud 2.0	You are currently using the Auto	channel bandwidth. Click <u>Here</u> to m channel. Click <u>Here</u> to modify.	rodify.	
	Basic Config			and the second se
Advanced Settings	2.4GHz MAC	00:00:00:00:00:00		
En marss	5GHz MAC	00:00:00:00:00:00		
🕎 LAN	Band			
() WAN	AP Mode			
👬 Alexa & IFTTT	Connect to APs in list  Ves  No			
1Pv6	Remote AP List (Max Limit : 4)			
		Remote AP List		Add / Delete
YPN		•		Ð
🚵 Firewall	No data in table.			
Reference Administration	Αρρίγ			

To set up the wireless bridge:

- From the navigation panel, go to Advanced Settings > Wireless > WDS tab.
- 2. Select the frequency band for the wireless bridge.
- 3. In the **AP Mode** field, select any of these options:
  - AP Only: Disables the Wireless Bridge function.
  - **WDS Only**: Enables the Wireless Bridge feature but prevents other wireless devices/stations from connecting to the router.

• **HYBRID**: Enables the Wireless Bridge feature and allows other wireless devices/stations to connect to the router.

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

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

NOTE: Channel availability varies per country or region.

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

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

7. Click Apply.

# 4.1.4 Wireless MAC Filter

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

/ISUS	Logout Rebo	pt	English 🔻		
Quick Internet	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS_26</u> <u>ASUS_56</u>	ware Version: <u>3.0.0.4.384_4360</u>	Арр 🔏 🔁 🔶		
General	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roamin	ng Block List		
Network Map	Wireless - Wireless MAC Filter				
Guest Network	Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.				
AiProtection	Basic Config Band	2.4GHz *			
Adaptive QoS	Enable MAC Filter	O Yes ● No			
🗼. Traffic Analyzer	MAC Filter Mode	Accept •			
🙈 Game	MAC filter list (Max Limit : 64)				
	Client	Name (MAC Address)	Add / Delete		
👸 USB Application	ex: 18:31:8F	af a 11 a 11 a 20			
AiCloud 2.0	No data in table.				
Advanced Settings	Арріу				

#### To set up the Wireless MAC filter:

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

# 4.1.5 RADIUS Setting

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

/1545	Logout Reboo	ot	English 🔻	
Quick Internet	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS 26</u> <u>ASUS 56</u>	ware Version: <u>3.0.0.4.384.4360</u>	App 🔏 🖻 🔶	
General	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roaming Block I	List	
Network Map	Wireless - RADIUS Setting			
	This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise (WPA2-Enterprise".			
AiProtection	Band			
Adaptive QoS	Server IP Address			
🕼. Traffic Analyzer	Server Port:			
📇 🕼 Game	Connection Secret			
USB Application		Арріу		

#### To set up wireless RADIUS settings:

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

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

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

# 4.1.6 Professional

The Professional screen provides advanced configuration options.

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

	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roaming Block List		
General	Wireless - Professional			
Guest Network		set up additional parameters for wireless. But default values are recommended.		
AiProtection	* Reminder: The System time zone is different fr Band	om your locale setting, 2.4GHz +		
Adaptive QoS	Enable Radio	O Yes ● No		
Traffic Analyzer	Enable wireless scheduler	● Yes O No		
Game	Set AP Isolated			
👸 USB Application	Roaming assistant Bluetooth Coexistence	Enable   Disconnect clients with RSSI lower than -55 dBm Disable		
AiCloud 2.0	Enable IGMP Snooping	Disable •		
Advanced Settings	Multicast Rate(Mbps)	Auto V		
Mireless	Preamble Type	Long V		
	AMPDU RTS RTS Threshold	Enable •		
()) WAN	DTIM Interval	3		
🚑 Alexa & IFTTT	Beacon Interval	100		
19v6	Enable TX Bursting	Enable •		
VPN	Enable WMM	Enable •		
tirewall	Enable WMM No-Acknowledgement	Disable ▼		
Administration	Enable WMM APSD Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM) *		
System Log	Airtime Fairness	Enable •		
2 Network Tools	Multi-User MIMO	Enable •		
	Explicit Beamforming	Enable •		
	Universal Beamforming	Enable •		
		Apply		

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

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

Quick Internet Setup	Operation Mode: SSID: ASUS_2G		er Firmware V	ersion: 3.0.0	0.4.384_4360		Ар	8 @ +
	General WPS	WDS Wire	less MAC Filter	RADIUS Se	etting Profe	ssional Ro	aming Block List	:
General	_							
Network Map	Wireless - Prof	essional						
💮 Guest Network	* Reminder: The Sys							
AiProtection	Clock Format	24-hour 🔻	Allow		Deny		]	
Adaptive QoS	Active Sched	ule	_	_				
Adaptive QoS	System Time			Thu, Aug 2	23 06:59:27 2	2018		
A. Traffic Analyzer	Select All	Sun	Mon	Tue	Wed	Thu		Sat
(V.	00 ~ 01							
😂 Game	01 ~ 02							
	02 ~ 03							
ở USB Application	03 ~ 04							
	04 ~ 05							
AiCloud 2.0	05 ~ 06							
	06 ~ 07							
Advanced Settings	07 ~ 08							
	08 ~ 09							
Mireless	09~10							
	10~11							
E LAN	11 ~ 12							
<i>m</i>	12 ~ 13							
WAN WAN	13 ~ 14							
Alexa & IFTTT	14 ~ 15							
	15~16							
1Pv6	16~17							
<b>W</b>	17 ~ 18							
++ VPN	18~19							
	19 ~ 20							
📩 Firewall	20 ~ 21							
0.41	21 ~ 22							
Administration	22 ~ 23							
<u>u</u>	23 ~ 24							
🛃 System Log								
🔯 Network Tools			c	ancel	ок			

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

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

# 4.2 LAN

# 4.2.1 LAN IP

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

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

/ISUS	Logout Reboot	English
Quick Internet Setup	Operation Mode: <u>Mircless router</u> Firmware Version: <u>3.0.0.4.384</u> 4360 SSID: <u>ASUS 26 ASUS 56</u>	App 💩 🔁 🗲
General	LAN IP DHCP Server Route IPTV Switch Control	
Network Map	LAN - LAN IP	
🜐 Guest Network	Configure the LAN setting of RT-AX82U.	
AiProtection	IP Address 192.168.50.1	
Adaptive QoS	Subnet Mask 255.255.0	
Multive dos	Apply	
🙀. Traffic Analyzer		

#### To modify the LAN IP settings:

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

## 4.2.2 DHCP Server

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

	LAN IP DHCP Server Route IPTV	Switch Control		
General	LAN - DHCP Server			
Guest Network	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 supports up to			
AiProtection	253 IP addresses for your local network. Manually Assigned IP around the D	HCP list FAQ		
Adaptive QoS	Basic Config			
🞊, Traffic Analyzer	Enable the DHCP Server	O Yes ● No		
A. Home many cer	Domain Name			
Game	IP Pool Starting Address	192.168.50.2		
\delta USB Application	IP Pool Ending Address	192.168.50.254		
AiCloud 2.0	Lease time	86400		
Advanced Settings	Default Gateway			
ເລີ wireless	DNS and WINS Server Setting			
In makes	DNS Server			
LAN LAN	WINS Server			
I WAN	Manual Assignment			
🚔 Alexa & IFTTT	Enable Manual Assignment	● Yes O No		
(m) 1Pv6	Manually Assigned IP around the DHCF	P list (Max Limit : 64)		
	Client Name (MAC Address) IP Address Add / Delete			
	ex: 18:31:8F:31:31:30	•		
irewall	No data in table.			
Administration	Apply			

#### To configure the DHCP server:

- 1. From the navigation panel, go to **Advanced Settings** > **LAN** > **DHCP Server** tab.
- 2. In the Enable the DHCP Server field, tick Yes.

- 3. In the **Domain Name** text box, enter a domain name for the wireless router.
- 4. In the **IP Pool Starting Address** field, key in the starting IP address.
- 5. In the **IP Pool Ending Address** field, key in the ending IP address.
- 6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

#### NOTES:

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

## 4.2.3 Route

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

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

/ISUIS	Logout	Reboot			English 🔻
Quick Internet	Operation Mode: <u>Wireless</u> SSID: <u>ASUS_2G_ASUS_5G</u>	router Firmware Version	: 3.0.0.4.384_4360	Ap	- 8 @ <del>*</del>
General	LAN IP DHCP Server R	oute IPTV Switch C	ntrol		
Network Map	LAN - Route				
Guest Network	This function allows you to add to the Internet.	l routing rules into. It is use	ul if you connect several ro	uters behind to share the s	ame connection
AiProtection	Basic Config	Basic Config			
Adaptive QoS	Enable static routes	• Yes •			
🕅 Traffic Analyzer	Static Route List (Max Lin	nit : 32)			
C. Traine Analyzer	Network/Host IP	Netmask	Gateway	Metric Interface	Add / Delete
Game			•	LAN T	Ð
% USB Application			data in table.		
AiCloud 2.0	Apply				
Advanced Settings					

## To configure the LAN Routing table:

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

## 4.2.4 IPTV

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

/ISUS	Logout Reboo	English 🔻		
Quick Internet	Operation Mode: Wireless router Firm SSID: ASUS_2G_ASUS_5G	vare Version: <u>3.0.0.4.384_4360</u> App 🛞 🔁 🗲		
General	LAN IP DHCP Server Route IPTV	Switch Control		
Metwork Map	LAN - IPTV			
Guest Network	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.			
AiProtection	LAN Port			
Adaptive QoS	Select ISP Profile	None •		
🙀. Traffic Analyzer	Choose IPTV STB Port	None v		
	Special Applications			
Game	Use DHCP routes	Microsoft •		
👸 USB Application	Enable multicast routing (IGMP Proxy)	Disable •		
AiCloud 2.0	UDP Proxy (Udpxy)	0		
Advanced Settings		Apply		
(in) Wireless				

# 4.3 WAN

#### **4.3.1 Internet Connection**

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

General		ort Virtual Server / Port DMZ DDNS NAT gger Forwarding Passthrough		
Network Map	WAN - Internet Connection			
🌐 Guest Network		ses to WAN (wide area network). These types are selected from the dropdown setting fields differ depending on the connection type you selected.		
(a) AiProtection	Configure the Ethernet WAN settings of R1			
Adaptive QoS	Basic Config			
🕼. Traffic Analyzer	WAN Connection Type	Automatic IP v		
	Enable WAN	OYes ●No		
Game	Enable NAT	O Yes ● No		
📸 Open NAT	Enable UPnP UPnP FAQ	O Yes ● No		
📸 USB Application		Yes O No     WAN Aggregation combines two network connections to increase your WAN		
AiCloud 2.0	Enable WAN Aggregation	speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification).		
Advanced Settings	WAN Aggregation FAQ			
Wireless	WAN DNS Setting			
<b>_</b>	Connect to DNS Server automatically	O Yes ● No		
LAN LAN	Account Settings			
()) WAN	Authentication	None		
Alexa & IFTTT	Special Requirement from ISP			
() IPv6	Host Name			
e VPN	MAC Address	MAC Clone		
-	DHCP query frequency	Aggressive Mode v		
hirewall	Extend the TTL value	●Yes ONo		
Reg Administration	Spoof LAN TTL value	• Yes O No		
👿 System Log		Apply		

#### To configure the WAN connection settings:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.
- 2. Configure the following settings below. When done, click **Apply**.
  - WAN Connection Type: Choose your Internet Service Provider type. The choices are Automatic IP, PPPOE, PPTP, L2TP or fixed IP. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
  - Enable WAN: Select Yes to allow the router Internet access. Select No to disable Internet access.

- Enable NAT: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- Enable UPnP: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- Enable WAN Aggregation: WAN Aggregation combines two network connections to increase your WAN speed up to 2 Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports.
- **Connect to DNS Server**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- Host Name: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.

- MAC Address: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:
  - Contact your ISP and update the MAC address associated with your ISP service.
  - Clone or change the MAC address of the ASUS wireless router to match the MAC address of the previous networking device recognized by the ISP.

# 4.3.2 Dual WAN

The Dual WAN allows you to select two ISP connections to your router, a primary WAN and a secondary WAN.

#### To configure Dual WAN:

- 1. From the navigation panel, go to Advanced Settings > WAN.
- 2. Go to Dual WAN field, turn ON.
- 3. Choose your **Primary WAN** and **Secondary WAN**. There are WAN, USB, Ethernet LAN and 2.5G WAN for your options.
- 4. Choose Fail Over or Load Balance.
- 5. Click Apply.

**NOTE:** Detailed explanations are available on the ASUS Support Site FAQ <u>https://www.asus.com/support/FAQ/1011719</u>

General	Internet Connection	Dual WAN	Port Trigger	Virtual Server / Port Forwarding	DMZ	DDNS	NAT Passthrough
Network Map	WAN - Duai WAN						
Guest Network				rer mode to use a secondary WAN t ughput, minimize response time, and			
AiProtection	connections. <u>Dual WAM</u> To enable WAN Aggreg		e <u>WAN-Internet</u>				
Adaptive QoS	Basic Config						
🚯. Traffic Analyzer	Enable Dual WAN						
Came	Primary WAN						
Open NAT				Apply			

# 4.3.3 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.

Quick Internet	Operation Mode: Mire SSID: ASUS_2G ASUS		E Firmware Ve	rsion: <u>3.0.0.4.384_4</u>	360		8 🖻 🔶		
General	Internet Connection	Dual WAN	Port Trigger	Virtual Server / Forwarding	Port DMZ	DDNS Pa	NAT issthrough		
Network Map	WAN - Port Trigge								
Guest Network				s when LAN devices req rwarding and port trigge					
AiProtection		two methods for opening incoming data ports, port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static. IP addresses for LAN devices Port forwarding allows							
Adaptive QoS	multiple devices to share a single open port and port trigger only allows one client at a time to access the open port. Port. Trigger FAQ								
🞊. Traffic Analyzer	Basic Config					_			
	Enable Port Trigger		• Ye	● Yes ♥ No					
Game	Well-Known Application								
👸 USB Application	Trigger Port List ( Max	.imit : 32 ) 🤆	•						
AiCloud 2.0	Description		Trigger Port	t Protocol	Incoming Port	Protocol	Delete		
Advanced Settings									
i Wireless				Apply					
EAN									
() WAN									

#### To set up Port Trigger:

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

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

#### NOTES:

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

# 4.3.4 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.

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

General	Internet Connection	Dual WAN	Port Trigger	Virtual Server / Port Forwarding	DMZ	DDNS	NAT Passthro	ugh
🛞 Network Map	WAN - Virtual Se	erver / Port Fo	orwarding					
🛞 Guest Network				o connect to a specific o ations (such as BitTorrer				
AiProtection	forwarding setting. P	elevork (LAN). For a faster connection, some P2P applications (such as BRTorrent), may also require that you set the port orwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of not is nouter and referict data through those ports to a single client on your network.						
🔿 Adaptive QoS	If you want to specify the LAN IP address,			e network, enter the Ser	vice Name, the	Port Range (e	.g. 10200:'	10300),
🕼. Traffic Analyzer		<ul> <li>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 RT-AX82U's web user interface.</li> </ul>						
Game	When you set 20:2     AX86U's native F1		erver's port range fo	r your WAN setup, then	your FTP serve	r would be in a	conflict with	RT-
💑 Open NAT	<u>Virtual Server</u>	/ Port Forwar	ding_FAQ					
A	Basic Config							
👸 USB Application	Enable Port Forward	ng	•					
AiCloud 2.0	Port Forwarding	List (Max Limit :	: 64)					
Advanced Settings	Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
Wireless		No data in table.						
M wieless				Add profile				
wan								

### To set up Port Forwarding:

From the navigation panel, go to Advanced Settings > WAN > Virtual Server / Port Forwarding tab.

- 2. Configure the following settings below. When done, click ON.
  - Enable Port Forwarding: Turn ON to enable Port Forwarding.
  - **Famous Server List**: Determine which type of service you want to access.
  - **Famous Game List**: This item lists ports required for popular online games to work correctly.
  - **FTP Server Port**: Avoid assigning the port range 20:21 for your FTP server as this would conflict with the router's native FTP server assignment.
  - 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 **4.2 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.

#### To check if Port Forwarding has been configured successfully:

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

#### Differences between port trigger and port forwarding:

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

# 4.3.5 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 tab.
- 2. Configure the setting below. When done, click **Apply**.
  - IP address of Exposed Station: Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.

#### To remove DMZ:

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

# 4.3.6 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.

/ISUS	Logout		Reboot				English 🔻
Quick Internet	Operation Mode: Wir SSID: ASUS_2G ASU		er Firmware Ver	sion: 3.0.0.4.384_4360			Арр 🔏 🔁 🗲
General	Internet Connection	Dual WAN	Port Trigger	Virtual Server / Port Forwarding	DMZ	DDNS	NAT Passthrough
Network Map	WAN - DDNS						
🌐 Guest Network				that allows network clients to con nain name. The wireless router is			
AiProtection	and other DDNS servi			http://iplookup.asus.co			
🔿 Adaptive QoS	IP address to use this The wireless router cu						
🖗. Traffic Analyzer				nd DDNS service cannot work in			
😂 Game	Enable the DDNS Clie	nt	• Yes	• No			
USB Application				Apply			

#### To set up DDNS:

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

• **Enable wildcard**: Enable wildcard if your DDNS service requires one.

#### NOTES:

DDNS service will not work under these conditions:

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

### 4.3.7 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** tab. When done, click **Apply**.

	Logout	Reboot			English 🔻
Quick Internet	Operation Mode: Wireless r SSID: ASUS_2G ASUS_5G	outer Firmware Ve	rsion: <u>3.0.0.4.384_4360</u>		Арр 🔏 🔁 🗲
General	Internet Dual Connection WAN		Virtual Server / Port Forwarding	DMZ DDNS	NAT Passthrough
Network Map	WAN - NAT Passthrough				
🛞 Guest Network	Enable NAT Passthrough to alk	w a Virtual Private Ne	twork (VPN) connection to pass	through the router to	the network clients.
AiProtection	PPTP Passthrough				
Adaptive QoS	L2TP Passthrough				
	IPSec Passthrough				
🕼. Traffic Analyzer	RTSP Passthrough				
Game	H.323 Passthrough				
📸 USB Application	SIP Passthrough				
AiCloud 2.0	Enable PPPoE Relay				
	-		Apply		
Advanced Settings					

# 4.4 IPv6

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

/1545	Logout Rebo	t English 🔻
Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS 2G</u> <u>ASUS 5G</u>	rare Version: <u>3. 0. 0. 4. 384_4360</u> App 🔏 🕞 🔶
General	IPv6	
Network Map	Configure the IPv6 Internet setting.	
Guest Network	Basic Config	
AiProtection	Connection type	Disable •
Adaptive QoS		Αρρίγ
🗼. Traffic Analyzer		
🙈 Game		

### To set up IPv6:

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

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

# 4.5 Firewall

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

NOTE: The Firewall feature is enabled by default.

# 4.5.1 General

#### To set up basic Firewall settings:

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

# 4.5.2 URL Filter

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

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

### To set up a URL filter:

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

# 4.5.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

/islis	Logout Reboot	English 🔻
Quick Internet	Operation Mode: <u>wireless router</u> Firmware Version: <u>3,0,0,4,384_4360</u> SSID: <u>ASUS_26_ASUS_56</u>	App 🔏 🖻 🔶
General	General URL Filter Keyword Filter Network Services Filter	
Network Map	Firewall - Keyword Filter	
Guest Network	Keyword Filter allows you to block the clients' access to webpages containing the specified keywords.	
AiProtection	Limitations of the filtering function : 1. Compressed webpages that use HTTP compression technology cannot be filtered. <u>see her e</u>	for more details.
Adaptive QoS	2. Https webpages cannot be filtered. Basic Config	
🗼. Traffic Analyzer	Enabled O Disabled	
Game	Keyword Filter List (Max Limit : 64)	
🔊 USB Application	Keyword Filter List	Add / Delete
AiCloud 2.0		Ð
C_S Alcious 2.0	No data in table.	
Advanced Settings	Apply	
i Wireless		

### To set up a keyword filter:

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

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

#### NOTES:

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

# 4.5.4 Network Services Filter

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



#### To set up a Network Service filter:

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

# 4.6 Administration

# 4.6.1 Operation Mode

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

General	Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Network Map	Administration	n - Opera	tion Mode			
Guest Network	RT-AX86U support	ts several o	peration modes to meet	different requirements. Please sel	ect the mode	that match your situation.
AiProtection			ode / AiMesh Rout mode / AiMesh Ro			
Adaptive QoS	<ul> <li>Repeater</li> <li>Media Bri</li> </ul>					
👯. Traffic Analyzer	AiMesh N	ode				
Game				functionality, which connects to the in s or devices. In this mode, NAT, firewa		
🖏 Open NAT	rently using any w	vired/wireles:	s routers.	and home users. Select this mode if yo	ou are a first-tin	ne user or you are not cur
👸 USB Application	You can add AiMe	ash nodes to	form an AiMesh WiFi sys	tem to provide extra WIFI coverage.		
AiCloud 2.0		ŀ				
Advanced Settings		N.		-{(( ( ' [] `))) 🖉		
Wireless						
				Save		
🌐 WAN						

### To set up the operating mode:

- From the navigation panel, go to Advanced Settings > Administration > Operation Mode tab.
- 2. Select any of these operation modes:
  - Wireless router mode (default): In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
  - Access Point mode: In this mode, the router creates a new wireless network on an exising network.
  - **Repeater mode**: This mode turns the router into a wireless repeater to extend the range of your signal.
  - **Media Bridge**: The Media Bridge mode provides the fastest Wi-Fi connection for multiple media devices simultaneously. To set up the Media Bridge mode, you need two RT-AX86S: one configured as the Media station and the other as a router.
  - **AiMesh Node**: You can set RT-AX86S as an AiMesh node to extend an existing AiMesh routers WiFi coverage.

#### 3. Click Save.

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

# 4.6.2 System

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

#### To set up the System settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
- 2. You can configure the following settings:
  - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
  - **WPS button behavior**: The physical WPS button on the wireless router can be used to activate WPS.
  - Time Zone: Select the time zone for your network.
  - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
  - 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.
  - **Only allow specific IP**: 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.

# 4.6.3 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 tab.
- 2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
- 3. Click Upload.

#### NOTES:

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

# 4.6.4 Restore/Save/Upload Setting

#### To restore/save/upload wireless router settings:

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

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

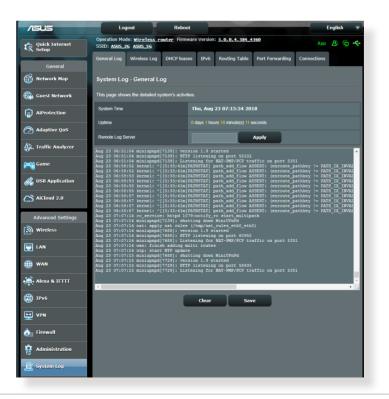
# 4.7 System Log

System Log contains your recorded network activities.

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

#### To view your system log:

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



# 5 Utilities

### NOTES:

- Download and install the wireless router's utilities from the ASUS website:
  - Device Discovery v1.4.7.1 at <u>https://www.asus.com/</u> <u>Networking/RT-AX86S/HelpDesk\_Download/</u>
  - Firmware Restoration v1.9.0.4 at <u>https://www.asus.com/</u> <u>Networking/RT-AX86S/HelpDesk\_Download/</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.

# 5.1 Device Discovery

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

# To launch the Device Discovery utility:

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



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

# 5.2 Firmware Restoration

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



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

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 > Wireless Router > Firmware Restoration.
- 5. Specify a firmware file, then click **Upload**.

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

# 5.3 Setting up your printer server

# 5.3.1 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<sup>®</sup> 7, Windows<sup>®</sup> 8, Windows<sup>®</sup> 8.1, and Windows<sup>®</sup> 10.

#### To set up the EZ Printer sharing mode:

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



**NOTE:** Network printer utility is supported on Windows<sup>®</sup> 7, Windows<sup>®</sup> 8, Windows<sup>®</sup> 8.1, and Windows<sup>®</sup> 10 only. 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 📃 🗾
	Extracting Files The contents of this package are being extracted.
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

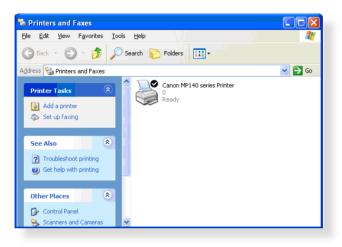
4. Follow the onscreen instructions to set up your hardware, then click **Next**.



- 5. Wait a few minutes for the initial setup to finish. Click Next.
- 6. Click **Finish** to complete the installation.
- 7. Follow the Windows<sup>®</sup> OS instructions to install the printer driver.

Found New Hardware Wiz	ard
	Welcome to the Found New Hardware Wizard         Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update web site (with your permission).         Read our privacy policy         Can Windows connect to Windows Update to search for software?         Yes, this time only         Yes, now and every time I connect a device         No, not this time         Click Next to continue.
	<back next=""> Cancel</back>

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

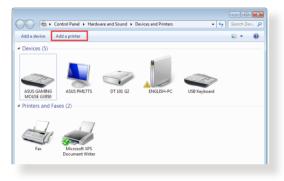


# 5.3.2 Using LPR to Share Printer

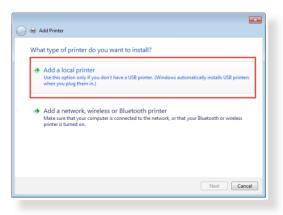
You can share your printer with computers running on Windows<sup>®</sup> and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

#### Sharing your LPR printer To share your LPR printer:

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



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



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

🇿 🖶 Add Printer		×
Choose a printer port		
A printer port is a type of cor	nection that allows your computer to exchange informat	tion with a printer.
Use an existing port:	LPT1: (Printer Port)	~
Oreate a new port:		
Type of port:	Standard TCP/IP Port	•
		lext 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 hostname or IP address						
Device type:	TCP/IP Device	Ŧ				
Hostname or IP address:	192.168.1.1					
Port name:	192.168.1.1					
Query the printer and auto	prmatically select the driver to use					
	Next	ancel				

- 5. Select **Custom** then click **Settings**.
  - Add Printer

     Additional port information required

     The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. Be sure that:

     1. The device is not found on the network. By our are sure the address is correct, select the device type below.

     Device Type
     Standard 
     Center(
     Standard
     Custom 
     Settings\_

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

Port Name:	192.168.1.1
Printer Name or IP Addres	55: 192.168.1.1
Protocol	
Raw	LPR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	LPRServer
LPR Byte Counting E	inabled
SNMP Status Enable	d
Community Name:	public
	1
SNMP Device Index:	

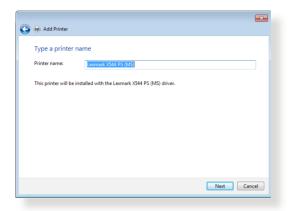
7. Click **Next** to finish setting up the standard TCP/IP port.

🚱 🚔 Add Printer Additional port	information required
The device is not 1. The device is 1 2. The network i 3. The device is	found on the network. Be sure that: turned on.
If you think the a	ddress is not correct, click Back to return to the previous page. Then correct the rm another search on the network. If you are sure the address is correct, select the
Standard	Generic Network Card *
Custom	Settings
	Next Cancel

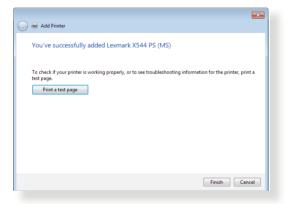
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.

🖶 Add Printer	
	m the list. Click Windows Update to see more models. n an installation CD, click Have Disk.
Manufacturer Kyocera Lanier Lemark Microsoft Microsoft Tell me why driver signing is	
	Next Cancel

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



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



# 5.4 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 **General** > **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 **5.4.1 Configuring Bit Torrent download settings**.

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

Task					
task	Seneral Setting Download Schedule				
Settings	Oimmediately  At Scheduled Time * Remind: The System time zone is different from your locate setting.				
General	Download to	/tmp/mnt/sda1/Download2/Complete Browse			
Bit Torrent	Refresh rate	5 Seconds			
NZB	DownloadMaster Port	8081			
	Download Master Https Port	8481			
aMule	WAN network	OFF Enable/disable the WAN connection.			
	Keep seeding after task completed	ON			
		Apply			

# 5.4.1 Configuring Bit Torrent download settings

Task	BitTorrent Setting					
	Port	Port				
Settings	OUse the default port					
100		Use the following port				
General	Incoming port 51413	Incoming port: 51413				
Bit Torrent	Speed Limits:					
~	Maximum download speed:	2 Unlimited				
NZB	Maximum upload speed:	🖬 Unlimited				
aMule	BitTorrent Network setting	BitTorrent Network setting				
~ 5	BitTorrent protocol encryption	Encryption enabled •				
	Maximum peers allowed per torrent	60				
	Global Maximum connection	240				
	DHT network	ON Enable DHT to activate trackerless torrent downloading activities.				
	PEX 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.

# 5.4.2 NZB settings

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

/ISUS		Logout	English
			0
Task	NZB Setting		
🌆 Task	Setup USENET server to download NZB files:		
Settings	USENET Server		
General	USENET Server Port		
35	Maximum download speed:	Unlimited	
Bit Torrent	SSL/TLS connection only	OFF	
NZB	User name		
A aMule	Password		
	Confirm Password		
	Maximum number of simultaneous connections to this server		
		Apply	
			2018 ASUSTeK Computer Inc. All rights reserved.

# 6 Troubleshooting

This chapter provides solutions for issues you may encounter with your router. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at:

<u>https://www.asus.com/support/</u> for more product information and contact details of ASUS Technical Support.

# 6.1 Basic Troubleshooting

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

### Upgrade Firmware to the latest version.

 Launch the Web GUI. Go to Advanced Settings > Administration > Firmware Upgrade tab. Click Check to verify if the latest firmware is available.

/ISUS	Logout		Reboot			E	inglish	•
Quick Internet	Operation Mode: SSID: ASUS_2G		outer Firmware Ver	sion: <u>3.0.0.4.384_4360</u>		Арр	8 6	÷
General	Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy		
Network Map	Administration - Firmware Upgrade							
Guest Network	Note:							
AiProtection	The latest firmware version include updates on the previous version.     For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process							
Adaptive QoS	<ol> <li>In case the upgrade process fails, enters the emergency mode automatically. The LED signals at the front will indicate such a situation. Use the Firmware Restoration utility on the CD to do system recovery.</li> </ol>							
🚯. Traffic Analyzer	social a susance, use the limit and e resolution using on the cub to us gradent recursy. 4. Get the latest firmware version from ASUS Support site at <u>http://www.asus.com/support/</u>							
Game	Firmware Versio	on	_	_	-	-	-	1
👸 USB Application	Check Update			Check				
AiCloud 2.0	AiMesh router	_						
Advanced Settings				Version : 3.0.0.4.384_4360 ge5799c firmware update : U <u>doad</u>				
Wireless				cted AiMesh routers / nodes, whe ware version to each applicable ro				
🕎 LAN	a na cana a papa cana na cana n							
WAN								
• Alexa & IFTTT								
() IPv6								
VPN								
📩 Firewall								
Administration								

- 2. If the latest firmware is available, visit the ASUS global website at <u>https://www.asus.com/Networking/RT-AX86S/HelpDesk/</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 router.

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

#### Check if your network settings are correct.

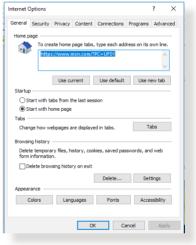
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.  Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the web GUI, Network Map > Clients page, and hover the mouse pointer over your device in Client Status.



# 6.2 Frequently Asked Questions (FAQs)

### I cannot access the router GUI using a web browser

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



#### **NOTES:**

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

# The client cannot establish a wireless connection with the router.

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

- Out of Range:
  - Move the router closer to the wireless client.
  - Try to adjust antennas of the router to the best direction as described in section 1.4 Positioning your wireless router.
- DHCP server has been disabled:
  - Launch the web GUI. Go to General > 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.

Auick Internet	Operation Mode: Wireless router Firms	ware Version: 3.0.0.4.384_4360 App 🛞 🕞 🔶
Setup	SSID: ASUS_2G_ASUS_5G	
General	LAN IP DHCP Server Route IPTV	Switch Control
Metwork Map	LAN - DHCP Server	
Guest Network		) is a protocol for the automatic configuration used on IP networks. The DHCP and informs the client of the of DNS server IP and default gateway IP, supports up to
(a) AiProtection	253 IP addresses for your local network. Manually Assigned IP around the D	<u>HCP list FAQ</u>
Adaptive QoS	Basic Config	
A. Traffic Analyzer	Enable the DHCP Server	O Yes ● No
W. Hume Support	Domain Name	
Game	IP Pool Starting Address	192.168.50.2
\delta USB Application	IP Pool Ending Address	192.168.50.254
AiCloud 2.0	Lease time	86400
Advanced Settings	Default Gateway	
Wireless	DNS and WINS Server Setting	
in whereas	DNS Server	
LAN	WINS Server	
() WAN	Manual Assignment	
Alexa & IFTTT	Enable Manual Assignment	● Yes O No
() 1Pv6	Manually Assigned IP around the DHCP	Plist (Max Limit : 64)
	Client Name (MAC Ac	ddress) IP Address Add / Deinte
VPN		•
🚵 Firewall		No data in table.
Administration		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.

Quick Internet	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS_26</u> <u>ASUS_56</u>	ware Version: <u>3.0.0.4.384.4360</u> App <u>8</u> C ++
General	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional Roaming Block List
Metwork Map	Wireless - General	
Guest Network	Set up the wireless related information below	ι.
AiProtection	Enable Smart Connect	OFF
Adaptive QoS	Band	2.4GHz *
	Network Name (SSID)	ASUS_2G
Traffic Analyzer	Hide SSID	● Yes O No
Came Game	Wireless Mode	Auto 🔹 🗖 Optimized for Xbox 🖾 big Protection
👸 USB Application	Channel bandwidth	20/40 MHz •
AiCloud 2.0	Control Channel	Auto   Current Control Channel: 4
	Extension Channel	AUTO *
Advanced Settings	Authentication Method	WPA2-Personal •
Wireless	WPA Encryption	AES T
EAN LAN	WPA Pre-Shared Key	12345678
() WAN	Protected Management Frames	Disable 🔻
Alexa & IFTTT	Group Key Rotation Interval	3600
• 1Pv6		Apply

- 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.

/ISUS	Logout Reboo	t	English 🔻
Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmu SSID: <u>ASUS 26</u> <u>ASUS 56</u>	vare Version: <u>3.0.0.4.384_4360</u>	Арр 🔏 🖻 🔶
General	Operation Mode System Firmware U	pgrade Restore/Save/Upload Setting	Feedback Privacy
Network Map	Administration - Restore/Save/Upl	oad Setting	
Guest Network	This function allows you to save current setting	ngs to a file, or load settings from a file.	
AiProtection	Factory default	Restore Initialize	
Adaptive QoS	Save setting	Save	
🖗. Traffic Analyzer	Restore setting	Upload 选择磁来 未选择	任何勉強
Came Game			
👸 USB Application			
AiCloud 2.0			

### Internet is not accessible.

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



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



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

#### You forgot the SSID (network name) or network password

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

#### How to restore the system to its default settings?

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

#### Firmware upgrade failed.

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

## **Cannot access Web GUI**

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

## A. Disable the proxy server, if enabled.

#### Windows®

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

	To set u	o an Inte	rnet conne	ction, dick		Set	up
-	Setup.						
Dial-up	and Virtua	Private	Network s	ettings —			
(1) A	ccess RD	Network I	Resources	- Go to vpr	.as	Add	i ]
					(	Add V	PN
	r	1			•	Remo	ve
<ul><li>Ne</li><li>Dia</li></ul>		connectio er a netw		ction is not p	presen	t	
Curr	ent	None			(	Set de	fault
Local A	ea Netwo	rk (LAN)	settings -				
			y to dial-up or dial-up s	connection settings.	ns. [	LAN se	ttings

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

	ation ation may override man ngs, disable automatic		
Automatically d		Janan	
Use automatic o	onfiguration script		
Address			
	ver for your LAN (Thes onnections).	e settings	will not apply to
Use a proxy ser		e settings 80	will not apply to
Use a proxy ser dial-up or VPN of Address:	onnections).	80	7
Address:	onnections). Port:	80	7

#### **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.

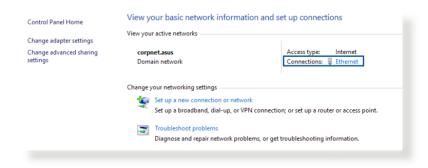
	Location:	Automatic	:	
	Show:	Built-in Ethernet	:	
Select a prox	TCP/IP PPPo		ies Ethernet	
✓ FTP Pro>	KY XY (HTTP)	n .		
	Veb Proxy (HTTPS) 1g Proxy (RTSP)	Prox)	Set Password	ord
SOCKS P		Ŭ,	Set Password	
	Proxv	Ŧ		
Gopher				
	y settings for			

**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.

Ethernet Status		×
General		
Connection		
IPv4 Connectivity	: Intern	et
IPv6 Connectivity	: No network acce	ss
Media State:	Enable	ed
Duration:	03:29:	31
Speed:	1.0 Gb	ps
Details		
Activity		
Acuvity	<b>*</b> ****	
	Sent — Neceive	ed
Bytes:	71,424,646 70,727,2	41
Properties	Oisable Diagnose	
	Cle	ose

Ethernet Properties	×
Networking Authentication	
Connect using:	
Intel(R) Ethernet Connection	(2) I219-V
This connection uses the following i  Construction uses the following i  Construction of the second	(TCP/IPv4) Multiplexor Protocol
<ul> <li>Internet Protocol Version 6</li> <li>Internet Protocol Version 6</li> <li>Internet Protocol Version 6</li> </ul>	(TCP/IPv6)
Link-Layer Topology Disco	
Install Uninst	
Description Transmission Control Protocol/Int wide area network protocol that p across diverse interconnected ne	rovides communication
	OK Cancel
Internet Protocol Version 4 (TCP/IPv4	) Properties X
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to for the appropriate IP settings.	matically if your network supports a ask your network administrator
Obtain an IP address automatica	ly
O Use the following IP address:	
Subnet mask:	
Default gateway:	
Obtain DNS server address autor	
O Use the following DNS server add Preferred DNS server:	
Alternate DNS server:	<u> </u>
Validate settings upon exit	
	Advanced
	Advanced OK Cancel

### **MAC OS**

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

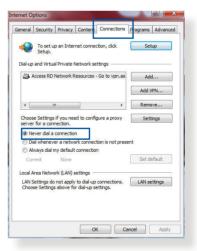
L	ocation: Automatic	•
	Show: Built-in Ethernet	•
ТСР	/IP PPPoE AppleTalk Proxies	Ethernet
Configure IPv4:	Using DHCP :	9
IP Address:	192.168.182.103	Renew DHCP Lease
Subnet Mask:	255.255.255.0 DHCP Client ID:	
Router:	192.168.182.250	(If required)
DNS Servers:	192.168.128.10	(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:0211:24ff:fe32:h	18e
	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 tab.
- 3. Tick Never dial a connection.
- 4. Click **OK** when done.



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

## **Appendices**

## **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

## **Service and Support**

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

