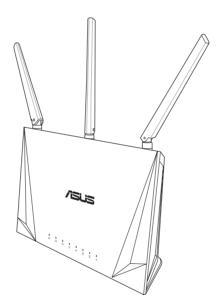
# **User Guide**

# **RT-AC2600**

### Wireless-AC2600 Dual Band Gigabit Router



The stylish RT-AC2600 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.



E16241 First Edition December 2019

#### Copyright © 2019 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	Getting to Know Your Wireless Router	6
1.1	Welcome!	6
1.2	Package contents	6
1.3	Your wireless router	7
1.4	Positioning your router	9
1.5	Setup Requirements	10
1.6	Router Setup	11
	1.6.1 Wired connection	11
	1.6.2 Wireless connection	12
2	Getting Started	14
2.1	Logging into the Web GUI	14
2.2	Quick Internet Setup (QIS) with Auto-detection	15
2.3	Connecting to your wireless network	19
3	Configuring the General Settings	20
3.1	Using the Network Map	20
	3.1.1 Setting up the wireless security settings	21
	3.1.2 Managing your network clients	22
	3.1.3 Monitoring your USB device	
3.2	Creating a Guest Network	25
3.3	Using the Traffic Manager	27
	3.3.1 Managing QoS (Quality of Service) Bandwidth	27
	3.3.2 Monitoring Traffic	
3.4	Setting up Parental Control	31
3.5	Using the USB Application	32
	3.5.1 Using AiDisk	
	3.5.2 Using Servers Center	

### Table of contents

Config	guring the Advanced Settings	39
Wirele	255	
4.1.1	General	
4.1.2	WPS	42
4.1.3	WDS	44
4.1.4	Wireless MAC Filter	46
4.1.5	RADIUS Setting	47
4.1.6	Professional	48
LAN		50
4.2.1	LAN IP	50
4.2.2	DHCP Server	51
4.2.3	Route	53
4.2.4	IPTV	54
WAN.		
4.3.1	Internet Connection	55
4.3.2	Port Trigger	58
4.3.3	Virtual Server/Port Forwarding	60
4.3.4	DMZ	63
4.3.5	DDNS	64
4.3.6	NAT Passthrough	65
IPv6		66
VPN S	erver	67
Firewa	all	
4.6.1	General	68
4.6.2	URL Filter	69
4.6.3	Keyword filter	70
4.6.4	Network Services Filter	71
Admii	nistration	72
4.7.1	Operation Mode	72
4.7.2	System	73

### Table of contents

	4.7.3 Firmware Upgrade	74
	4.7.4 Restore/Save/Upload Setting	74
4.8	System Log	75
5	Utilities	76
5.1	Device Discovery	76
5.2	Firmware Restoration	77
6	Troubleshooting	79
6.1	Basic Troubleshooting	79
6.2	Frequently Asked Questions (FAQs)	
App	pendices	92
Noti	ces	

## 1 Getting to Know Your Wireless Router

### 1.1 Welcome!

Thank you for purchasing an ASUS RT-AC2600 Wireless Router! The stylish RT-AC2600 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**

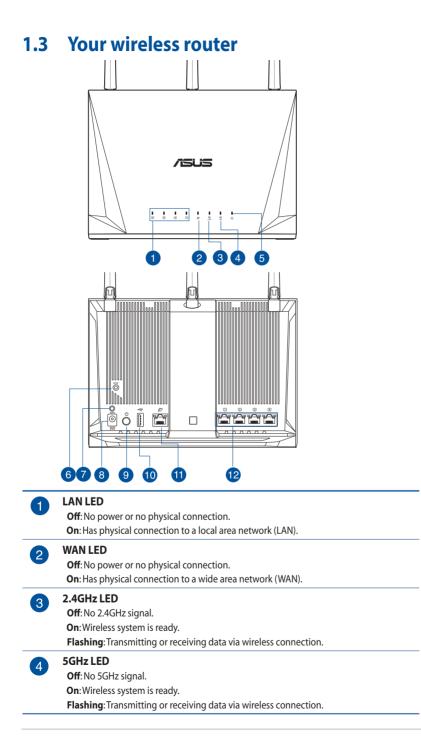
☑ RT-AC2600 Wireless Router

☑ Power adapter

☑ Network cable (RJ-45)

Quick Start Guide

- 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.



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

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

DC Power adapter	DC Output: +12V with max 2.5A current;		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

### **1.4 Positioning your router**

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

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



### 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 wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

- If your computer does not have built-in wireless capabilities, you may
  install an IEEE 802.11a/b/g/n/ac 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.
- If you are using only one computer with single band IEEE 802.11b/g/n WLAN adapter, you will only be able to use the 2.4GHz band.
- If you are using only one computer with dual band IEEE 802.11a/b/g/n/ac WLAN adapter, you will be able to use the 2.4GHz or 5GHz band.
- If you are using two computers with both IEEE 802.11a/b/g/n/ac WLAN adapters, you will be able to use both 2.4GHz and 5GHz bands simultaneously.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

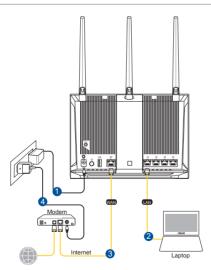
### 1.6 Router Setup

#### **IMPORTANT!**

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

### **1.6.1 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:

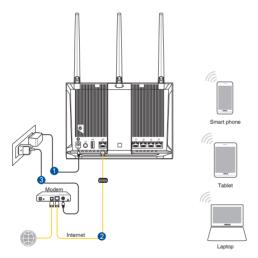
1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.

2. Using the bundled network cable, connect your computer to your wireless router's LAN port.

**IMPORTANT!** Ensure that the LAN LED is blinking.

- 3 Using another network cable, connect your modem to your wireless router's WAN port.
- 4. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.

### **1.6.2 Wireless connection**



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

- 1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.
- 2 Using the bundled network cable, connect your modem to your wireless router's WAN port.

- 3. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.
- 4. Install an IEEE 802.11a/b/g/n/ac WLAN adapter on your computer.

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

# 2 Getting Started

### 2.1 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 default user name (**admin**) and password (**admin**).
- 3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



#### Top command buttons

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

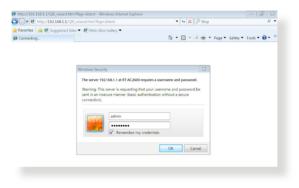
### 2.2 Quick Internet Setup (QIS) with Autodetection

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



- By default, the login username and password for your wireless router's Web GUI is admin. For details on changing your wireless router's login username and password, refer to section 4.7.2 System.
- The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

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

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

### for Automatic IP (DHCP)



### for PPPoE, PPTP, and L2TP

/ISUS Router			
Quick Internet Setup	Account Setting		$\bigcirc$
Check Connection	Please enter the req	uired information below.	
2 Internet Setup	User Name		
3 Router Setup	Password		
		Show password	
	Obtain the account na	ame and password from your ISP.	
		Previous Next	

### for Static IP

ng, and input the related information.
ss:
2
•
al) 🔅 MAC Clone
5

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.
- 3. Assign the wireless network name (SSID) and security key for your 2.4GHz and 5 GHz wireless connection. Click **Apply** when done.

/545	
Quick Intetnet Setup	Wireless Setting
Check Connection	Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.
Internet Setup	2.4GHz - Security Network Name(SSID) 2 ASUS
3 Router Setup	Security Key 2
	5GHz - Security Copy 2.4GHz to 5GHz settings.
	Network Name(SSID)  2 ASUS_SG
	Security Key 👔 🚥 🔹
	Арріу

- 4. Your Internet and wireless settings are displayed. Click **Next** to continue.
- 5. Read the wireless network connection tutorial. When done, click **Finish**.

	Completed Network Configuration Sur	nmary
Quick Internet Setup	System Time: Sat, Jan 01 (	00:02:51 2011 Change the time zone
Check Connection		
	Network Name(SSID)	ASUS-monkey
Internet Setup	Wireless Security	Open System
-		
3 Router Setup	Network Name(SSID)	ASUS_5G-monkey
	Wireless Security	Open System
	WAN Connection Type	Automatic IP
	WAN IP	192.168.123.23
	LAN IP	192.168.1.1
	MAC	20:CF:30:B6:C0:C0
		Next
_		MEXT

### 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.

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

## 3 Configuring the General Settings

### 3.1 Using the Network Map

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



### 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 **Security Level** dropdown list, select the encryption method for your wireless network.

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

- 5. 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 3.0 port for connecting USB devices 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 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. For more details, refer to the section **3.5.Using the USB Application** 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 3.5.2 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-AC2600 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.

The Guest Network provides Inte your Intranet.	ernet connection for guests but r	estricts access to
Enable	Enable	Enable
Enable	enable	Enable
Enable	Enable	Enable

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

Guess Network			
	st network can provide internet network.		hout accessing your
	ASUS_Guest1		
		Create	Create
	Limitless		
	Modify		
	ASUS_5G_Guest1		
		Create	Create
	Limitless		
	Modify		

- 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 Using the Traffic Manager

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

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

General	QeS Traffic Monitor Traffic Manager - QoS
<ul> <li>Guest Network</li> <li>Traffic Manager</li> <li>Parental Controls</li> <li>USB Application</li> </ul>	Cuality of Service (QoC) ensures bandwith for prioritized tasks and applications.
Advanced Settings	Enable QoS OFF
Wireless	Apply
WAN	

### 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.

- 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 low-priority 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.

### 3.3.2 Monitoring Traffic

The traffic monitor function allows you to access the bandwidth usage and speed of your Internet, wired, and wireless networks. It allows you to monitor network traffic even on a daily basis.

Quick Internet Setup	SSID: ASUS_A0_20	Operation Mode: <u>wireless</u> router Firmware Version: <u>3.0.0.4.382</u> 51599 SSID: Asus A0 2G ASUS A0 5G			App 🔏 🤤	•		
General	QoS Traffic Mo	nitor						
Network Map	Traffic Manag	er - Traffic M	onitor					
Guest Network	Traffic Monitor allow			utgoing packe	ts of the following			
🔿 Traffic Manager		Internet		Wired		Wirele	155	
Parental Controls	Reception							
🔊 USB Application	Transmission							
Advanced Settings	NOTE: Packets from Traffic Monitor FAC		evenly transmitte	d to the wired	and wireless dev	ices.		
Mireless	Internet Conne 48.83 KB/s	ection (Intern	et) Wired	Wireless				
🕎 LAN	10.03 KB/S			Internet				
💮 WAN	34.18 KB/s							_
<b>IPv6</b>								
VPN	24.41 KB/s							
Firewall								
Administration	12.21 KB/s							4
🛐 System Log							M	X
🔯 Network Tools	Curren	ıt	Averag	e	Maxi	mum	Total	
	2.39 KB		0.50 KB	/s	9.46	KB/s	302.43 KB	
								_

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

### 3.4 Setting up Parental Control

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

Quick Internet Setup	SSID: ASUS_AO_26_ASUS_AO_56
General	Parental Controls
💕 Network Map	Parental Controls allow you to set the time limit for a client's network usage. To use Parental Controls
💮 Guest Network	Parenial Controls: 1. In the [Clients Name] column, select the client whose network usage you want to
🔿 Traffic Manager	control. You may also key in the clients MAC address in the [Clients MAC Address] column.
😱 Parental Controls	2. In the [Add / Delete] column, click the plus(+) icon to add the client. 3. In the [Time Management] column, click the edit icon to edit the Active Schedule.
\delta USB Application	4. Select your time slot with a click. You can hold and drag to extend the duration.     5. Click [OK] to save the settings made.
Advanced Settings	Note: 1. Clients that are added to Parental Controls will have their internet access restricted
🔊 Wireless	by default. 2. Please disable NAT Acceleration for more precise scheduling control.
	Enable Parental Controls
WAN	

### To use the parental control function:

- 1. From the navigation panel, go to **General** > **Parental control**.
- 2. Click **ON** to enable Parental Control.
- 3. Select the client whose network usage you want to control. You may also key in the client's MAC address in the **Client MAC Address** column.

**NOTE:** Ensure that the client name does not contain special characters or spaces as this may cause the router to function abnormally.

- 4. Click 🙆 or 🖸 to add or delete the client's profile.
- 5. Set up the allowed time limit in **Time Management** map. Drag and drop a desired time zone to allow client's network usage.
- 6. Click **OK**.
- 7. Click **Apply** to save the settings.

### 3.5 Using the USB Application

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

**IMPORTANT!** To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 3.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <u>http://event.asus.com/2009/networks/disksupport/</u> for the file system support table.

### 3.5.1 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.

Quick Internet Setup	Operation Mode: Wireless SSID: ASUS A0 26 ASUS A	router Firmware Version: 3.0.0.4.382_51599 0_56		App 🛞	ē ◆
General		(2) $(3)$			
🜐 Guest Network		$\bigcirc$			
Traffic Manager	My FTP server is shared	.: Decide how to share your folders.			
Parental Controls	admin rights				
👸 USB Application	<ul> <li>limited access rights</li> <li>limitless access rights</li> </ul>				
Advanced Settings	Account	Password	Read	Write	
i Wireless	admin				
🕎 LAN					
🌐 WAN		Previous Next			
IPv6					

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



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.

### 3.5.2 Using Servers Center

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

#### **Using Media Server**

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

**NOTE**: Before using the DLNA Media Server function, connect your device to the RT-AC2600's network.

	Media Server Network Place (S	Samba) Share FTP Share
General	Media Server	
Metwork Map	Setup the iTunes and UPnP media se	erver.
🜐 Guest Network	iTunes Server	
Traffic Manager	Enable iTunes Server?	OFF
	Media Server	
Parental Controls	Enable UPnP Media Server	ON
🚲 USB Application	Media Server Name	RT-AC2600-54A0
Advanced Settings	Media Server Status	Idle
Wireless	Media Server Path Setting	All Disks Shared      ● Manual Media Server Path
E LAN		Apply
() WAN		
IPv6		
👥 VPN		
🚵 Firewall		

To launch the Media Server setting page, go to **General** > **USB application** > **Servers Center** > **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 directory**: Select your media server directory and click **Apply** to share files from the USB disk to media devices in the network.
- Media Server Status: Displays the status of the media server.

### Using Network Place (Samba) Share service

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

USB Application Advanced Settings Wireless	Allow guest login Device Name Work Group	OFE Username and password is necessary to log in network place(Samba) RT-AC2600-54A0 WORKGROUP
LAN WAN DIPV6	<b>^</b>	Apply

### To use Samba share:

1. From the navigation panel, go to **General** > **USB application** > **Servers Center**.

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 accountriace(S	iamba) Share / Clouc <mark>X</mark> D sl
New account has no re	ead/write access rights.
Account:	
Password:	
Retype password:	
	Add
RT-AC66U	

### 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.

The default access rights for a new folder is
read/write.
Folder Name:
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.

	Media Server Network P	Nace (Samba) Sha	re FTP Share				
General							
Network Map	USB Application - FTP	Share					
🙀 Guest Network	Set the account and permission	on of FTP service.					
🔿 Traffic Manager	Enable FTP		OFF				
Parental Controls	Allow anonymous login		OFF Username and p				
🗞 USB Application	Maximum number of concur connections	rrent 5					
	Character set on FTP Serve						
Advanced Settings			Apply				
Wireless			Apply				_
	⊕⊙⊘					4	
-	🔔 admin	RT-AC2600		R/W	w	No	
💮 WAN		JetFlash Tr	anscend 2GB				
1Pv6			Save Pe	rmission			
👥 VPN							
🛵 Firewall							

#### To use FTP Share service:

**NOTES:** Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.5.1 Using AiDisk**.

- 1. From the navigation panel, click **General** > **USB application** > **Servers Center** > **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.

# 4 Configuring the Advanced Settings

## 4.1 Wireless

### 4.1.1 General

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

General	General WPS WDS Wireless	MAC Filter RADIUS Setting Professional
Network Map	Wireless - General	
Guest Network	Set up the wireless related information t	below.
Traffic Manager	Band	
Parental Controls	Network Name (SSID)	ASUS_A0_5G
Parental Controls	Hide SSID	• Yes O No
USB Application	Wireless Mode	Auto •
Advanced Settings	Channel bandwidth	20/40/80 MHz *
Wireless	Control Channel	Auto    Current control channel: 149
LAN	Extension Channel	
ATTEN .	Authentication Method	
WAN 1Pv6		Apply

### To configure the basic wireless settings:

- 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 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.
- 7. 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.

- 8. Select any of these authentication methods:
  - Open System: This option provides no security.
  - 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).
  - 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.

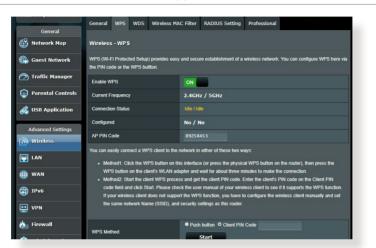
**NOTE:** Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto** and **encryption method** is **WEP** or **TKIP**.

- 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.



NOTE: Ensure that the devices support WPS.

### To enable WPS on your wireless network:

- 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.

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

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

- c. The wireless router will scan for any available WPS devices. If the wireless router does not find any WPS devices, it will switch to standby mode.
- 6. To set up WPS using the Client's PIN code, follow these steps:
  - a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.
  - b.Key in the Client PIN code on the text box.
  - c. Click **Start** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

### 4.1.3 WDS

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: wireless router Firmy SSID: ASUS_A0_2G_ASUS_A0_5G	vare Version: <u>3.0.0.4.382_51599</u>	Арр 🖄 🖻 🗲
General	General WPS WDS Wireless MAC	Fliter RADIUS Setting Professional	
Network Map	Wireless - Bridge		
Guest Network	Bridge (or named WDS - Wireless Distributio WDS may also be considered a repeater more		to connect to an access point wirelessly.
⊘ Traffic Manager	Note: The function only support [Open System		ntication method.
Parental Controls	To enable WDS to extend the wireless signal		
💏 USB Application	2. Ensure that this wireless router and th	nd add MAC address of APs in Remote AP L e AP you want to connect to use the same d te AP list and open the remote AP's WDS m	hannel.
Advanced Settings	4. To get the best performance, please g	o to Advanced Settings > Wireless > Genera sion channel to every router in the network.	al and assign the same channel
LAN	You are currently using the Auto channel You are currently using the Auto channel. Basic Config		
🌐 wan	2.4GHz MAC	04:09:F5:C7:54:A0	
IPv6	5GHz MAC		
•• VPN	Band		
	AP Mode		
irewall	Connect to APs in list		
😰 Administration	Remote AP List (Max Limit : 4)		
🛃 System Log	r	ternote AP List	Add / Delete
🙍 Network Tools			Ð
		No data in table.	
		Арріу	

To set up WDS:

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

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

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

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

NOTE: Channel availability varies per country or region.

 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.

General	General WPS WDS Wireless MAC Filter RADIUS Setting Professional
Network Map	Wireless - Wireless MAC Filter
	Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.
🔗 Traffic Manager	Basic Config Band 5GHz v
Parental Controls	Enable MAC Filter
👸 USB Application	Αρρίγ
Advanced Settings	
Wireless	

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

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
- 2. In the **Frequency** field, select the frequency band that you want to use for the Wireless MAC filter.
- 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.

Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382 51599</u> App         App         B         C         C           SSID: <u>ASUS A0.26</u> <u>ASUS A0.56</u> App         App
General	General WPS WDS Wireless MAC Filter RADIUS Setting Professional
Network Map	Wireless - RADIUS Setting
Guest Network	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".
🙆 Traffic Manager	Band 5GHz V
Parental Controls	Server IP Address
歲 USB Application	Server Port. 1812
Advanced Settings	Connection Secret
Wireless	Αρρίγ
🕎 LAN	
🌐 WAN	

#### 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.

Quick Internet Setup	Operation Mode: wireless router Firm SSID: <u>ASUS_A0_2G_ASUS_A0_2G</u>	ware Version: <u>3.0.0,4,382_51599</u> <b>2</b> App 🔏 🔁 🗲
General	General WPS WDS Wireless MAC	C Filter RADIUS Setting Professional
Network Map	Wireless - Professional	
Guest Network		set up additional parameters for wireless. But default values are recommended.
🔿 Traffic Manager	* Reminder: The System time zone is different for Band	SGHZ V
Parental Controls	Enable Radio	O Yes ● No
👸 USB Application	Enable wireless scheduler	● Yes O No
	Set AP Isolated	● Yes ♥ No
Advanced Settings	Roaming assistant	Disable •
Wireless	Enable IGMP Snooping	Disable •
🕎 LAN	Multicast Rate(Mbps)	Auto
🌐 wan	Preamble Type	Long •
1Pv6	RTS Threshold	2347
++ VPN	DTIM Interval	1
-	Beacon Interval	100
Kirewall	Enable TX Bursting	Enable •
Administration	Enable Packet Aggregation	Enable •
🛃 System Log	Enable WMM	Enable •
network Tools	Enable WMM No-Acknowledgement	Disable •
	Enable WMM APSD	Enable •
	Enable WMM DLS	Enable •
	Multi-User MIMO	Enable •
	802.11ac Beamforming	Enable •
	Region	China(Default) •
		Αρρίγ

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

- **Band**: Select the frequency band that the professional settings will be applied to.
- Enable Radio: Select Yes to enable wireless networking. Select No to disable wireless networking.
- Enable Wireless Scheduler: You can specify a time range when wireless networking is enabled during the weekend.

- Set AP isolated: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Enable IGMP Snooping**: When enabled, IGMP Snooping monitors IGMP communication among devices and optimizes wireless multicast traffic.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **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 Packet Aggregation: Select Enable to enable packet aggregation to increase the delivered bandwidth in your network.

- **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.
- **TX Power adjustment**: TX Power adjustment refers to the milliWatts (mW) needed to power the radio signal output of the wireless router. Enter a value between 0 to 100.

**NOTE**: Increasing the TX Power adjustment values may affect the stability of the wireless network.

## 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.

/1545	Logout	Reboot		English 🔻
Quick Internet	Operation Mode: Wireless rou	ter Firmware Version:	SSID: ASUS ASUS_SG	8 6 <del>4</del> 8
- Setup	LAN IP DHCP Server Route	IPTV Switch Control		
General				
Hetwork Map	LAN - LAN IP			
Suest Network	Configure the LAN setting of Router			
GBEST NELWORK	IP Address	192.168.1.1		
Manager Traffic Manager	Subnet Mask			
Parental control		Арг	ply	

### 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	
Network Map	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, RT-AC2600
🔊 Traffic Manager	supports up to 253 IP addresses for your local network. Manually Assigned IP around the DHCP list FAQ
Parental Controls	Basic Config
👸 USB Application	Enable the DHCP Server O Yes O No
	RT-AC2600's Domain Name
Advanced Settings	IP Pool Starting Address 192.168.50.2
<b></b> .	IP Pool Ending Address 192.168.50.254
	Lease time 86400
🌐 WAN	Default Gateway
1Pv6	DNS and WINS Server Setting
+ VPN	DNS Server
-	WINS Server
🚵 Firewall	Manual Assignment

#### 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 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.
- 7. In the **DNS and Server Settings** section, key in your DNS Server and WINS Server IP address if needed.
- 8. Your wireless router can also manually assign IP addresses to devices on the network. On the **Enable Manual Assignment** field, choose **Yes** to assign an IP address to specific MAC addresses on the network. Up to 32 MAC Addresses can be added to the DHCP list for manual assignment.

### 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.

General	LAN IP DHCP Server	Route IPT	V Switch Control			
Network Map	LAN - Route					
Guest Network	This function allows you to share the same connection		into RT-AC2600. It is useful if you o			
Traffic Manager	Basic Config					
Parental Controls	Enable static routes		• Yes O No			
3 USB Application	Static Route List (M:	ax Limit : 32)				
	Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
Advanced Settings				-		Ð
Wireless			No data in table.			
LAN			Apply			
) WAN						
1Pv6						

#### 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.

	LAN IP DHCP Server Route IPTV Switch Control
General	
Network Map	LAN - IPTV
🌐 Guest Network	Configure the IPTV setting of RT-AC2600.
Traffic Manager	LAN Port
	Select ISP Profile vone v
Parental Controls	Choose IPTV STB Port None v
歲 USB Application	Special Applications
Advanced Settings	Use DHCP routes Microsoft v
Wireless	Enable multicast routing (IGMP Proxy) Disable + (This feature only works on Primary WAN )
	Enable efficient multicast forwarding (IGMP Snooping) Disable ¥
	UDP Proxy (Udpxy) 0
() WAN	Apply
💏 IPv6	

## 4.3 WAN

### **4.3.1 Internet Connection**

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

	Operation Mode: Wireless router Firmw	vare Version: 3.0.0.4.382_51599	🛛 App 🛞 🔂 🍲
Quick Internet Setup	SSID: ASUS_A0_2G_ASUS_A0_5G		
General	Internet Connection Port Trigger Virts	ual Server / Port Forwarding DMZ 0	DDNS NAT Passthrough
Network Map			
метногк мар	WAN - Internet Connection		
Guest Network	RT-AG2600 supports several connection types beside WAN Connection Type. The setting fie		
Traffic Manager	Configure the Ethernet WAN settings of RT-AC	32600.	
Parental Controls	Basic Config		
A	WAN Connection Type	Automatic IP •	
👸 USB Application	Enable WAN	O Yes DNo	
Advanced Settings	Enable NAT	♥ Yes ● No	
Wireless	Enable UPnP UPnP FAQ	O Yes O No	
🕎 LAN	WAN DNS Setting		
🗰 wan	Connect to DNS Server automatically	O Yos ONO	
() IPv6	Account Settings		
	Authentication		
VPN	Special Requirement from ISP		
🚵 Firewall	Host Name		
Administration	MAC Address		IAC Clone
📝 System Log	DHCP query frequency		
<u></u>	Extend the TTL value	• Yes • No	
🔯 Network Tools	Spoof LAN TTL value	● Yes ♥ No	
		Apply	

#### To configure the WAN connection settings:

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

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

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

### 4.3.2 Port Trigger

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

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

Quick Internet Setup	Operation Mode: Wireless SSID: ASUS_A0_2G ASUS_A0		3.0.0.4.382_51	2222	P App 2	8 🔁 <del>4</del>
	Internet Connection Port	Trigger Virtual Server / P	ort Forwarding	DMZ DDNS	NAT Passthrough	
General				_		
💕 Network Map	WAN - Port Trigger					
Guest Network	Port Trigger allows you to temp two methods for opening incon					
Traffic Manager	the time and devices must use to the trigger port. Unlike port f	orwarding, port trigger does r	ot require static IF	addresses for LAP	devices. Port forwa	
Parental Controls	multiple devices to share a sing	gle open port and port trigger	only allows one cl	lient at a time to ac	cess the open port.	
Parental Controls	Port Trigger FAQ					
With the second	Port Trigger FAQ Basic Config	_				
•	and the second se	● Yes O N	•		-	
•	Basic Config	● Yes O N Please se		=	=	
💞 USB Application	Basic Config Enable Port Trigger	Please se				
USB Application	Basic Config Enable Port Trigger Well-Known Applications	Please se		Incoming Port	Protocol	Delete
WSB Application           Advanced Settings           Wireless	Basic Config Enable Port Trigger Well-Known Applications Trigger Port List ( Max Limit : 3	Please se 2) 🕀 Trigger Port		Incoming Port	Protocol	Delete

### 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.

### 4.3.3 Virtual Server/Port Forwarding

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

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

Quick Internet	Operation Mode: <u>wireless router</u> Firmware Version: <u>3.0.0.4.382_51599</u> App 🛞 🕞 😋
General	Internet Connection Port Trigger Virtual Server / Part Forwarding DM2 DDNS NAT Passthrough
Network Map	WAN - Virtual Server / Port Forwarding
Guest Network	Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a fuster connection, some P2P applications (such as BRToment), may also require that you set the port
⊘ Traffic Manager	forwarding setting. Flease refer to the F2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.
Parental Controls	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.
💰 USB Application	<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-AC2600's web user interface.</li> </ul>
Advanced Settings	<ul> <li>When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with RT- AC2800's native FTP server.</li> </ul>
i wireless	<u>Virtual Server / Port Forwarding FAQ</u>
🕎 LAN	Bankic Config Enable Pon Forwarding OFF
()) WAN	Port Forwarding List (Max Limit : 64)
IPv6	Service Name External Port Internal Port Internal IP Address Protocol Source IP Edit Delete
VPN	No data in table.
A Firewall	Add profile

#### 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 **Apply**.
  - **Enable Port Forwarding**: Choose **Yes** 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.

### 4.3.4 DMZ

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

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

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

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

Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.387</u> 51599 SSID: <u>Asus A0.26</u> <u>Asus A0.36</u>
General	Internet Connection Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough
Network Map	WAN - DMZ
Guest Network	Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertained incoming ports. Please use it carefully.
Traffic Manager	Special Applications:
Parental Controls	<ul> <li>Some applications require special handler against NAT. These special handlers are disabled in default.</li> <li>Please <u>add a rule</u> to port forwarding list for USB Disk access property on FTP service.</li> </ul>
👸 USB Application	DMZ FAQ
	Enable DMZ • Yes • No
Advanced Settings	Apply
Wireless	
👿 LAN	
()) WAN	

### 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**.

### 4.3.5 DDNS

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

Quick Internet Setup	Operation Mode: <u>wire</u> SSID: <u>ASUS_A0_2G</u>		Firmware Version: 3.0.0.4.3	<u>82_51599</u>		App 🖧 🔁
General	Internet Connection	Port Trigger	Virtual Server / Port Forward	ling DMZ	DDNS	NAT Passthrough
Network Map	WAN - DDNS					
Guest Network			n) is a service that allows netwo registered domain name. The w			e wireless router, even with a ad with the ASUS DDNS service
Traffic Manager	and other DDNS servic If you cannot use ASU:		s, please go to <u>http://iploo</u>	up.asus.co	m/nsloo	kup.php to reach your internet IP
Parental Controls	address to use this ser		• Yes O No			
\delta USB Application	Enable the DDNS Client		Apply	-		
Advanced Settings			(approximately)			
i wireless						
LAN						
() WAN						

### To set up DDNS:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DDNS** tab.
- 2. Configure the following settings below. When done, click **Apply**.
  - **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
  - Server and Host Name: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).

- If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.
- Enable wildcard: Enable wildcard if your DDNS service requires one.

#### NOTES:

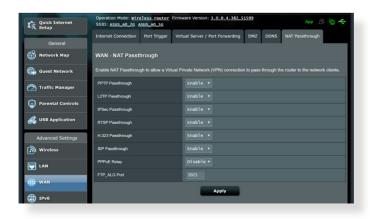
DDNS service will not work under these conditions:

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

### 4.3.6 NAT Passthrough

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

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



## 4.4 IPv6

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

Quick Internet Setup	Operation Mode: <u>Wireless router</u> F SSID: <u>ASUS_A0_2G_ASUS_A0_5G</u>	firmware Version: 3.0.	<u>0.4.382_51599</u>	Y App 🙈 🖻 🗲
General	IPv6			
Network Map	Configure the IPv6 Internet setting of RT-/	AC2600.		
Guest Network	<u>1PV6 PAQ</u>			
	Basic Config	_	_	
Traffic Manager	Connection type			
Parental Controls		Apply		
👸 USB Application				
Advanced Settings				
Mireless				
🌐 WAN				
() 19v6				

### 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 VPN Server

VPN (Virtual Private Network) provides a secure communication to a remote computer or remote network using a public network such as the Internet.

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

Quick Internet Setup	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382</u> 51599 SSID: <u>ASUS A0_26</u> <u>ASUS A0_56</u>	2	App 🖧 🔁 🔶
General	VPN Server VPN Client		
Network Map	VPN Server - PPTP	РРТР	OpenVPN
		<u> </u>	
Guest Network	Basic Config		
Traffic Manager	Enable PPTP VPN Server		
Parental Controls			
\delta USB Application			
Advanced Settings			
Wireless			
🕎 LAN			
() WAN			
(1) 1Pv6			
VPN			

### To set up access to a VPN server:

- 1. From the navigation panel, go to **Advanced Settings** > **VPN Server**.
- 2. On the Enable PPTP Server field, select Yes.
- 3. On the Network Place (Samba) Support field, select Yes.
- 4. Enter the user name and password for accessing the VPN server. Click the 
  button.
- 5. Click Apply.

**NOTE**: For advanced VPN server settings, click the **VPN Server** tab to configure broadcast support, authentication, MPPE Encryption, and Client IP address range.

## 4.6 Firewall

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

NOTE: The Firewall feature is enabled by default.

### 4.6.1 General

General	General URL Filter Keyword Filter	- Network Services Filter	
Network Map	Firewall		
	General		
🔗 Traffic Manager	Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.		
Parental Controls	DoS Protection FAQ		
<b>USB</b> Application	Enable Firewall	O Yes ● No	
Cost Application	Enable DoS protection	• Yes © No	
Advanced Settings	Logged packets type None		
🔊 Wireless	Respond ICMP Echo (ping) Request from WAN		
🕎 LAN	IPv6 Firewall		
() WAN	All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.		
() IPv6	You can leave the remote IP empty to allow traffic from any remote host. A subnet can also be specified. (2001:1111:2222:3333/64 for example)		
VPN	Basic Config		
📩 Firewall	Enable IPv6 Firewall	O Yes ● No	
	Famous Server List	Please select •	

### 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.

### 4.6.2 URL Filter

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

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

	General URL Filter Keyword Filte	r Network Services Filter	
General	Firewall - URL Filter		
	Key in the keywords for the sites that you For example, enter "XXX" in the list The U	want to block. RL filter will block the http://www.abcXXX.com, http://www.	XXXbbb.com and so on.
🔿 Traffic Manager	Basic Config		
Parental Controls	Enable URL Filter	Enabled ODisabled	
👸 USB Application	Filter table type	Black List ¥	
	URL Filter List: (Max Limit : 64)		
Advanced Settings		URL Filter List	Add / Delete
Wireless			Ð
🕎 LAN		No data in table.	
() WAN		Apply	
IPv6			
👥 VPN			
🚵 Firewall			

#### 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.

### 4.6.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

	General URL Filter Keyword Filter Network Services Filter	
General	Firewall - Keyword Filter	
	Keyword Filter allows you to block the clients' access to webpages containing Limitations of the filtering function ;	the specified keywords.
Traffic Manager	Compressed webpages that use HTTP compression technology canno	t be filtered. <u>See here for more details.</u>
Parental Controls	2. Https webpages cannot be filtered.	
👸 USB Application	Basic Config Enable Keyword Filter    Enabled	
Advanced Settings	Keyword Filter List (Max Limit : 64)	
Wireless	Keyword Filter List	Add / Delete
		€
() WAN	No data in table.	
() IPv6	Apply	
UPN VPN		
🚵 Firewall		

#### To set up a keyword filter:

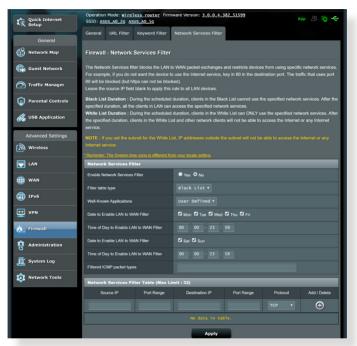
- 1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Keyword Filter** tab.
- 2. On the Enable Keyword Filter field, select **Enabled**.
- 3. Enter a word or phrase and click the Add button.
- 4. Click Apply.

#### 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.

### 4.6.4 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:

- 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**.

## 4.7 Administration

### 4.7.1 Operation Mode

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

C Quick Internet	Operation Mode: <u>kireless router</u> . Firmware Version: <u>3.0.0.4.382</u> .51599 App 🔏 🔁 🗲 SSID: <u>ASUS_A0_26</u> ASUS_A0_56
General	Operation Mode System Firmware Upgrade Restore/Save/Upload Setting Feedback Privacy
Network Map	Administration - Operation Mode
Guest Network	RT-AC2500 supports several operation modes to meet different requirements. Please select the mode that match your situation.
🔿 Traffic Manager	O Wireless router mode (Default)     ● Access Point(AP) mode
Parental Controls	In wireless router/ IP sharing mode, RTAC2600 connects to the Internet via PPPoE, DHCP, PPTP, L2TP, or Static IP and shares the wi release network to LAN clients or devices. In this mode, NAT, firewall, and DHCP server are enabled by default, UPAP and Dynamic D
👸 USB Application	NS are supported for SOHO and home users. Select this mode if you are a first-time user or you are not currently using any winedwir eless routers.
Advanced Settings	
Wireless	
🕎 LAN	
🌐 WAN	Save
🗱 1РV6	
irewall	
Reg Administration	

### To set up the operating mode:

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

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

# 4.7.2 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 or switch off wireless networking.
  - **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.

# 4.7.3 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**.

# 4.7.4 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 **Browse** to locate your file, then click **Upload**.

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

# 4.8 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

Quick Internet Setup	SSID: ASUS_A0_2G ASUS_A0_5G	
General	General Log Wireless Log DHCP lease	25 IPv6 Routing Table Port Forwarding Connections
Network Map	System Log - General Log	
Guest Network	This page shows the detailed system's activiti	ies.
Traffic Manager	System Time	Wed, Nov 27 07:30:05 2019
Parental Controls	Uptime Remote Log Server	0 days 4 hours 18 minute(s) 58 seconds Apply
USB Application	NOV 27 06:14:00 Kernel: WDEV Nov 27 06:14:00 kernel: WDEV	12:
Advanced Settings	Nov 27 06:14:00 kernel: WDEV Nov 27 06:14:00 kernel: WDEV Nov 27 06:14:00 kernel: WDEV	
Wireless	Nov 27 06:14:00 kernel:         WDEV           Nov 27 06:14:00 kernel:         WDEV           Nov 27 06:14:00 kernel:         WDEV           Nov 27 06:14:00 kernel:         WDEV	
LAN	Nov 27 06:14:00 kernel: Set_WiFiHWmat Nov 27 06:14:00 kernel: Set_WiFiHWmat Nov 27 06:14:01 miniupnpd[1495]: shut Nov 27 06:14:01 ntp: start NTP update	:_Proc ## Enable WiFi_HW_NAT .ting down MiniUPnPd
WAN	Nov 27 06:14:01 rc service: udhcpc 20 Nov 27 06:14:01 rc service: waitting Nov 27 06:14:01 nat: apply nat rules	34inotify_rc_stop_upnp "start_firewall" via_udhepc (/tmp/na_rulas_eth3_eth3)
IPv6		
VPN	Nov 27 06:14:02 rc sorvice: udhcpc 22 Nov 27 06:14:02 rc_service: waitting Nov 27 06:14:02 miniupnpd[211]: shut Nov 27 06:14:03 miniupnpd[2115]: vers	"stop upnp" via udhepe :ting down MiniUPnPd tion 1.9 started
Firewall		
Administration	Weby 27 Deriver by WAN Connection: WAN V	
System Log		Clear Save
Network Tools		

# 5 Utilities

#### NOTES:

- Download and install the wireless router's utilities from the ASUS website:
  - Device Discovery v1.4.7.1 at <u>http://dlcdnet.asus.com/pub/ASUS/</u> LiveUpdate/Release/Wireless/Discovery.zip
  - Firmware Restoration v1.9.0.4 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Rescue.zip</u>
- 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 > RT-AC2600 Wireless
 Router > Device Discovery.

/ISUS	RT-AC2600		1	-×
Device	SSID	IP Address	Subnet Mask	USB Device
RT-AC2600	ASUS	192.168.1.1	255.255.255.0	Ì
	<u>C</u> onfigure		<u>S</u> earch	<u>E</u> xit
Number of devic	ces found: 1			

**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.

Firmware Restor	ation		×
<u>F</u> ilename:			<u>B</u> rowse
Status After locating t	ne firmware file, click Uploa	ad.	
	<u>U</u> pload	Close	

**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 RT-AC2600 Wireless
   Router > Firmware Restoration.
- 5. Specify a firmware file, then click **Upload**.

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

# 6 Troubleshooting

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

<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.

	Operation Mode	System	Firmware Upgrade	Restore/Save/Upl	oad Setting	Feedback	Privacy	
General	Administration -	- Firmwai	re Upgrade					
Guest Network     Guest Network     Traffic Manager     Parental Controls     USB Application	<ol> <li>For a configure process.</li> <li>When the upg show correspondence of the show corres</li></ol>	ration parar rade fails, f onding sign	on includes previous upd neter existing both in the RT-AC2600 will enter the als. Please visit <u>ASUS D</u> ension from ASUS Suppo	old and new firmware emergency mode aut compload Center to d	omatically. The	LED in front		
Advanced Settings			_					
Wireless	Firmware Versi	on	_					
LAN	Product ID		RT-AC260					
	Firmware Version		3.0.0.4.382	_51599-gd18aeac	Check			
I WAN	New Firmware File		Browse		Upload			
1Pv6								
UPN VPN								
🚵 Firewall								
8 Administration								

- 2. If the latest firmware is available, visit the ASUS global website at <u>http://www.asus.com/Networking/RTAC2600/HelpDesk</u> <u>Download</u> to download the latest firmware.
- 3. From the **Firmware Upgrade** page, click **Browse** to locate the firmware file.
- 4. Click **Upload** to upgrade the firmware.

#### Restart your network in the following sequence:

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

#### Check if your Ethernet cables are plugged properly.

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

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

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

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

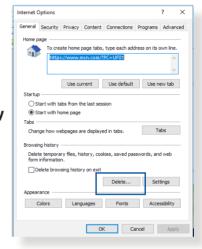
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.  Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You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



# 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 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.

/ISUS	Logout Rebo	ot	English 🔻
the second secon	Operation Mode: <u>Wireless router</u> F	irmware Version: SSID: ASUS ASUS SG	<u>8</u> 🔶 🖻
Setup	LAN IP DHCP Server Route IPTV	Switch Control	
General	LAN - DHCP Server		
船 Network Map		) is a protocol for the automatic configuration used on IP ne	hundre The DHCD constr
Guest Network		orms the client of the of DNS server IP and default gateway	
Manager Traffic Manager	Basic Config		
Parental control	Enable the DHCP Server	⊙ Yes ● No	
USB application	Router's Domain Name		
озваррисации	IP Pool Starting Address		
AiCloud	IP Pool Ending Address	192.168.1.254	
Advanced Settings	Lease Time	86400	
🛜 Wireless	Default Gateway		
	DNS and WINS Server Setting		
00	DNS Server		
💮 WAN	WINS Server		
🚳 IРv6	Enable Manual Assignment		
VPN Server	Enable Manual Assignment	● Yes ● No	
	Manually Assigned IP around the DHCP list(li		
Firewall	MAC address	IP Address	Add / Delete
Administration			•
System Log		No data in table.	
		Apply	

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

/ISUS	Logout Reboo	st English 🔻
Quick Internet	Operation Mode: <u>Wireless router</u> F	irmware Version: SSID: ASUS ASUS_SG 🛛 🛔 🔁 🔶 🖻
	General WPS Bridge Wireless MA	C Filter RADIUS Setting Professional
General	Wireless - General	
Retwork Map	Set up the wireless related information below	s
Guest Network	Frequency	2.4GHz 🔽
Yraffic Manager	SSID	ASUS
Parental control	Hide SSID	● Yes ◎ No
discrete USB application	Wireless Mode	Auto v 2 big Protection
AiCloud	Channel bandwidth	20/40 мнz 🗸 Алто 🗸
	Authentication Method	Open System
Advanced Settings	WEP Encryption	None
		Apply
💮 wan		
1Pv6		
VPN Server		
V Firewall		

- 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.

Ceneral         Operation Mode         System         Femware Upgrade         Restore/Save/Upload Setting           Ceneral         Administration - Restore/Save/Upload Setting         This lancion allows you to save current settings of Router to a life, or load settings from a life.           Main         Ceneral         Administration - Restore/Save/Upload Setting           Main         Restore         Save           Traffic Hanager         Save         Save           Save setting         Save         Save	/ISUS	Logout Rebo	ot	English
Central         Operation Mode         System         Fermurate Upgrade         Restore/Save/Upload         Setting           Image: Central Control         Administration - Restore/Save/Upload         Setting         Administration         Administration         Administration         Restore/Save/Upload         Setting         Image: Central Control         Image: Central Control         Image: Central Control         Restore         Restore         Image: Central Control         Image: Central Cont		Operation Mode: Wireless router	irmware Version: SSID: ASUS ASUS_SG	8 6 4 1
Network Map     Administration - Restore/SaveUU/boad Settings       Image: Setting Seting Setting Setting Setting Setting Setting Setting Sett	Setup	Operation Mode System Firmware	Upgrade Restore/Save/Upload Setting	
Network Map         This function allows you to save current satings of Roder to a life, or load satings from a life.           Const Network         Fadory debut         Restore           Traffic Menager         Save sating         Save           Perstal control         Reators sating         Lipbad         Const Sating	General	Administration Restore/Savell In	load Soffing	
Scuest Network         Factory datault         Restore           Troffic Manager         Sale setting         Sale           Parential control         Restore setting         Sale	品 Network Map			
Yraffic Manager         Save stilling           Parental control         Readore setting         Save	Suest Network	This function allows you to save current sett	ings of Router to a hie, or load settings from a hie.	
Parential control     Restore setting     Create a file     In the setting     Create a file     Ino the chosen	M	Factory default	Restore	
Restore setting Upload Choose File. No file chosen	Tranic Manager	Save setting	Save	
	Parental control	Restore setting	Upload Choose File No file chosen	
USB application	discrete dis			
AiCloud	AiCloud			

#### Internet is not accessible.

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



 The device has been blocked via the Parental Control function. Go to General > Parental 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.

/ISUS	Logout	Reboot			E	nglish	<b>v</b> ]
Quick Internet Setup	Operation Mode: Min	eless router Firmwa	re Version:	SSID: <u>ASUS</u> <u>ASUS</u>	<u>.sc</u> .8	<b>0</b> ~ 1	3
General	Parental control						
Retwork Map		Parental control allows y parental control:	ou to set the tin	ne limit for a client's	network usage.		
🕵 Guest Network		1. In the [Clients Na		lect the client whose le clients MAC addre			
挫 Traffic Manager	1 M	Address) column. 2. In the [Add / Dele			ss in the forein	5 MP1C	
Parental control	OFF	<ol> <li>Set up allowed tim desired day/time.</li> </ol>			nap. Drag and d	rop to	
🚓 USB application		<ol> <li>Click [OK] to save 5. <u>Click to open the</u></li> </ol>					
aiCloud					Time	Add /	
Advanced Settings		Clients Name	Clie	nts MAC Address	Management	Delete	4
察 Wireless		_	No data in table			Ð	
🚮 LAN			Apply				
🧐 VPN Server							
Firewall							
Administration							
System Log							
	Help & Support Man			FAQ			Q

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

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

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

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

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

The following are the factory default settings:

User Name:	admin
Password:	admin
Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	router.asus.com
Domain Name:	http://router.asus.com
Subnet Mask:	255.255.255.0
DNS Server 1:	router.asus.com
DNS Server 2:	(Blank)
SSID (2.4GHz):	ASUS
SSID (5GHz):	ASUS_5G

# Firmware upgrade failed.

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

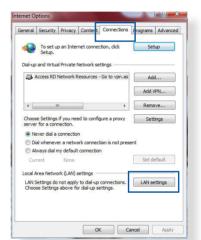
### **Cannot access Web GUI**

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.



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

Automatic configuration Automatic configuration ma use of manual settings, disa			
Automatically detect set	ttings		
Use automatic configura	ation script		
Address			
roxy server Use a proxy server for		e settings	will not apply to
dial-up or VPN connection	ons). Port:	80	Advanced
Bypass proxy serve	r for local addre	sses	

#### **MAC OS**

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

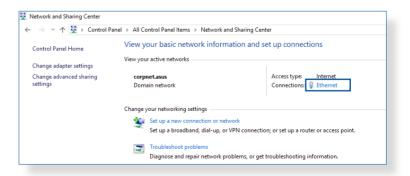
		utomatic uilt-in Ethernet	÷	
	TCP/IP PPPot	AppleTalk Pro	oxies Ethernet	
Select a pro	oxy server to config	ure: FTP Pn	oxy Server	
FTP Pro		n	:	
	oxy (HTTP) Web Proxy (HTTPS)	Pro:	xy server requires passw	vord
	ing Proxy (RTSP)	U	(Set Password)	
SOCKS		4		
Gophe	r Proxy	<b>T</b>		
	xy settings for & Domains:			
Use Pass	ive FTP Mode (PAS)	0		(?)

**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®

 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 Connectivi				Internet	
IPv6 Connectivi	ty:		No networ		
Media State:				Enabled	
Duration:				3:29:31	
Speed:			1	1.0 Gbps	
Details					
Activity					
	Sent —		— R	eceived	
Bytes:	71,424,646		70,	727,241	
Properties	Disable	Diag	nose		
Ethernet Propertie					×
Networking Authentio	cation				
Intel(R) Ethem	et Connection (2	2) I219-V			
			Config		
This connection uses		ems:	Coning	ure	
QoS Packet	Scheduler		_	^	
Internet Prot	ocol Version 4 (	TCP/IPv4)			
	twork Adapter		TOLOCO		
Microsoft LL	DP Protocol Dri ocol Version 6 (	ver TCP/IPv6)			
	opology Discov		der		
🗹 🔔 Link-Layer T	opology Discov				
<				>	
Install	Uninsta	1	Proper	ties	
Description					
Transmission Contr wide area network	rol Protocol/Inte	met Protoc	ol. The de	fault	
across diverse inte	rconnected net	works.	munication	'	
Internet Protocol Versi	on 4 (TCP/IPv4)	Properties			×
General Alternate Co	nfiguration				
You can get IP setting this capability. Otherv for the appropriate IP	vise, you need to	natically if yo ask your ne	our network twork adm	k supports inistrator	
Obtain an IP add		ly			
Use the following IP address:	JIP address:				
Subnet mask:					
Default gateway:					
Obtain DNS serv	er address auton	natically			
O Use the following	) DNS server add	resses:			
Preferred DN5 serv	er:		${\bf r}_{\rm eff} = {\bf r}_{\rm eff}$		
Alternate DNS serv	er:				
Validate setting					
	s upon exit		Ad	vanced	

### **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.

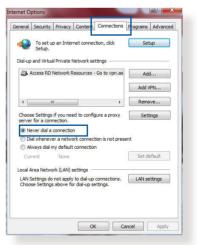
	Location: Automatic	:	
	Show: Built-in Ethernet	;	
T	CP/IP PPPoE AppleTalk	Proxies Ethernet	
Configure IP	4: Using DHCP	•	
IP Addre	ss: 192.168.182.103	Renew D	HCP Lease
Subnet Ma	sk: 255.255.255.0 DHC	P Client ID:	
Rout	er: 192.168.182.250	(If require	ed)
DNS Serve	rs: 192.168.128.10		(Optional)
Search Domain	ns:		(Optional)
IPv6 Addre	ss: fe80:0000:0000:0000:0211	24ff:fe32:b18e	
	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**

# Notices

# **ASUS Recycling/Takeback Services**

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <u>http://csr.asus.com/english/Takeback.htm</u> for the detailed recycling information in different regions.

# REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

#### http://csr.asus.com/english/index.aspx

# **Federal Communications Commission Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection

against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**WARNING!** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## **Prohibition of Co-location**

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

### **IMPORTANT NOTE:**

**Radiation Exposure Statement:** This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC exposure compliance requirement, please follow operation instruction as documented in this manual. **WARNING!** This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

# Compliance Statement of Innovation, Science and Economic Development Canada (ISED)

This device complies with Innovation, Science and Economic Development Canada licence exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

CAN ICES-3(B)/NMB-3(B)

# **Radio Frequency (RF) Exposure Information**

The radiated output power of the ASUS Wireless Device is below the Innovation, Science and Economic Development Canada radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This equipment should be installed and operated with a minimum distance of 20 cm between the radiator any part of your body.

This device has been certified for use in Canada. Status of the listing in the Innovation, Science and Economic Development Canada's REL (Radio Equipment List) can be found at the following web address:

http://www.ic.gc.ca/eic/site/ceb-bhst.nsf/eng/h\_tt00020.html

Additional Canadian information on RF exposure also can be

found at the following web:

https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

# Déclaration de conformité de Innovation, Sciences et Développement économique Canada (ISED)

Le présent appareil est conforme aux CNR d'Innovation, Sciences

et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La bande 5150 – 5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

CAN ICES-3(B)/NMB-3(B)

# Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par cet appareil sans fil est inférieure à la limite d'exposition aux fréquences radio d'Industrie Canada (IC). Utilisez l'appareil sans fil de façon à minimiser les contacts humains lors d'un fonctionnement normal.

Cet appareil a été évalué et démontré conforme aux limites de DAS (Débit d'absorption spécifique) d'IC lorsqu'il est installé dans des produits hôtes particuliers qui fonctionnent dans des conditions d'exposition à des appareils portables (Les antennes doivent être situées à plus de 20 cm de votre corps). L'utilisation de cet appareil est autorisée au Canada. Pour consulter l'entrée correspondant à l'appareil dans la liste d'équipement radio (REL - Radio Equipment List) d'Industrie Canada, rendez-vous sur: <u>http://www.ic.gc.ca/app/sitt/reltel/srch/</u> <u>nwRdSrch.do?lang=eng</u>

Pour des informations supplémentaires concernant l'exposition aux fréquences radio au Canada, rendez-vous sur: <u>http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html</u>

# **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