# **User Guide**

# **RT-ACRH17**

## Wireless-AC1700 Dual Band Gigabit Router





E17880 Revised Edition v4 April 2021

#### Copyright © 2021 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	
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	
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	18
3	Configuring the General settings	
3.1	Using the Network Map	19
	3.1.1 Setting up the wireless security settings	20
	3.1.2 Managing your network clients	21
	3.1.3 Monitoring your USB device	22
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	30
3.4	Setting up Parental Control	31
3.5	Using the USB Application	32
	3.5.1 Using AiDisk	32
	3.5.2 Using Servers Center	34

## Table of contents

4	Config	guring the Advanced Settings	
4.1	Wirele	255	39
	4.1.1	General	
	4.1.2	WPS	42
	4.1.3	Wireless MAC Filter	44
	4.1.4	RADIUS Setting	45
	4.1.5	Professional	46
4.2	LAN		48
	4.2.1	LAN IP	48
	4.2.2	DHCP Server	49
	4.2.3	Route	51
4.3	WAN		52
	4.3.1	Internet Connection	52
	4.3.2	Port Trigger	55
	4.3.3	Virtual Server/Port Forwarding	57
	4.3.4	DMZ	60
	4.3.5	DDNS	61
	4.3.6	NAT Passthrough	62
4.4	IPv6		63
4.5	Firewa	all	64
	4.5.1	General	64
	4.5.2	URL Filter	64
	4.5.3	Keyword filter	65
	4.5.4	Network Services Filter	66
4.6	Admi	nistration	68
	4.6.1	Operation Mode	68
	4.6.2	System	69
	4.6.3	Firmware Upgrade	70
	4.6.4	Restore/Save/Upload Setting	70

## **Table of contents**

4.7	System Log	71
<b>5</b> 5.1	<b>Utilities</b> Firmware Restoration	72
<b>6</b> 6.1	Troubleshooting Basic Troubleshooting	73
6.2	Frequently Asked Questions (FAQs)	76
Anr	pendices	

## Appendices

Notices	85
ASUS Contact information	98
Networks Global Hotline Information	99

# 1 Getting to know your wireless router

## 1.1 Welcome!

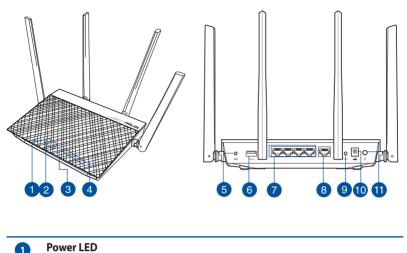
Thank you for purchasing an ASUS RT-ACRH17 Wireless Router! The ultra-thin and stylish RT-ACRH17 features both 2.4GHz and 5GHz dual bands which delivers super fast gigabit wireless-AC speeds up to 1400 Mbps on the 5 GHz band & 300 Mbps on the 2.4 GHz band concurrently.

## **1.2 Package contents**

☑ RT-ACRH17 Wireless Router
 ☑ Power adapter
 ☑ 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.

## **1.3 Your wireless router**



	Off: No power. On: Device is ready. Flashing slow: Rescue mode Flashing quick: WPS is processing.
2	<ul> <li>2.4GHz LED / 5GHz LED</li> <li>Off: No 2.4 GHz or 5 GHz signal.</li> <li>On: Wireless system is ready.</li> <li>Flashing: Transmitting or receiving data via wireless connection.</li> </ul>
3	WAN (Internet) LED Off: No power or no physical connection. On: Has physical connection to a wide area network (WAN).
4	LAN LED Off: No power or no physical connection. On: Has physical connection to a local area network (LAN).
5	WPS button This button launches the WPS Wizard.
6	<b>USB 3.0 port</b> Insert a USB 3.0 device such as USB hard disks or USB flash drives into this port.



#### LAN 1 ~ 4 ports

Connect network cables into these ports to establish LAN connection.

8	WAN (Internet) port Connect a network cable into this port to establish WAN connection.
9	<b>Reset button</b> This button resets or restores the system to its factory default settings.
10	<b>Power (DC-IN) port</b> Insert the bundled AC adapter into this port and connect your router to a power source.
1	<b>Power button</b> Press this button to power on or off the system.

- 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 2A 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 802.11b/g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at <u>http://www.asus.com</u> to get the latest firmware updates.
- To ensure the best wireless signal, orient the four antennas as shown in the drawing below.
- DO NOT mount this equipment higher than 2 meters.



## 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/1000Base-TX)
- 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.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

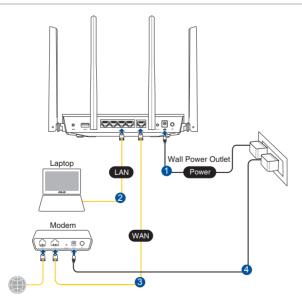
## 1.6 Router Setup

#### **IMPORTANT!**

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

## **1.6.1 Wired connection**

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

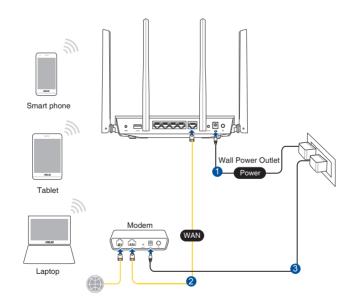


## To set up your wireless router via wired connection:

- 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.

- 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

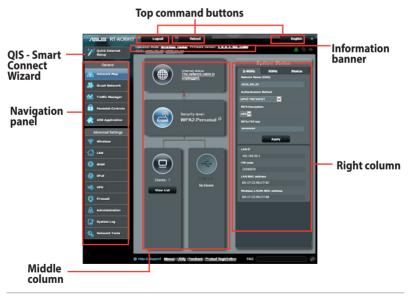
## 2.1 Logging into the Web GUI

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



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

## 2.2 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 4.6.2 System.
- The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

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

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

## for Automatic IP (DHCP)



## for PPPoE, PPTP and L2TP

Skin Setun Wizard	Account Settings		
Quick Internet Setup         Quick Internet Setup         Check Connection         Internet Setup         Router Setup	Please enter your usernam Username	e and password. 2 2 Show password Next	Evenedian file file     evening     e
			Hillet user's dient number is soccocco@whet net

- 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.

*** Skip Setup Wizard	Wireless Setting	
Quick Internet Setup	Do you want to use the previ	ious wireless security settings? • Yes O No
Check Connection	Assign a unique name or SS	SID (Service Set Identifier) to help identify your wireless network.
Check Connection	2.4 GHz - Security	
Internet Setup	Network Name (SSID)	ASUS_68_2G
	Password	• •••••
3 Router Setup	5 GHz - Security	
	Network Name (SSID)	ASUS 68 5G
	Password	
	Password	•
	default wireless security sett	n 8 and 63 charactersfletters, numbers or a combination) or 64 hex digits. The ing is WPA2-Personal AES. If you do not want to set the network security, leave the this exposes your network to unauthorized access.
		Apply

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

ternet Setup	System Time: Tue, Feb 14 09: * Reminder: The system time has a WAN	58:17 2017 (GMT+08:00) tol been synchronized with an NTP server.	
onnection	WAN Connection Type	Automatic IP	
up	Network Name (SSID)	ASUS_68_2G	
	Wireless Security	Open System	
IP			
	Network Name (SSID)	ASUS_68_5G	
	Wireless Security	Open System	
	LAN IP	192.168.50.1	
	MAC address		
		Complete	
Becom	e an ASUS Member and receive the	latest product information. Sign Up Now!	

## 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

System Status	System Status		
2.4GHz 5GHz Status	2.4GHz 5GHz Status		
Network Name (SSID)	Network Name (SSID)		
ASUS_68_2G	ASUS_68_5G		
Authentication Method	Authentication Method		
Open System 🔽	Open System 🗸		
Apply	Apply		
LAN IP	LAN IP		
192.168.50.1	192.168.50.1		
PIN code PIN code			
12345670	12345670		
LAN MAC address	LAN MAC address		
D0:17:C2:E6:C7:6C	D0:17:C2:E6:C7:6C		
Wireless 2.4GHz MAC address	Wireless 5GHz MAC address		
D0:17:C2:E6:C7:68	D0:17:C2:E6:C7:6C		

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

## **5GHz security settings**

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 port for connecting USB devices to allow you to share files 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 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, or Samba. 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.

- 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-ACRH17 supports up to six SSIDs (three 2.4GHz and three 5GHz SSIDs).

#### To create a guest network:

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

Guest Network	
	The Guest Network provides Internet connection for guests but restricts access to your local network.
Network Name	
(SSID)	
Authentication Method	
Network Key	Enable Enable Enable
Time Remaining	3
Access Intranet	٤
Network Name	
(SSID)	
Authentication	
Method	
Network Key	Enable Enable Enable
Time Remaining	3
Access Intranet	:

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

Guest Network			
	The Guest Network provides Interne your local network.	t connection for guests but re	stricts access to
Network Name (SSID)	ASUS_68_2G_Guest		
Authentication Method	Open System		
Network Key	None	Enable	Enable
Time Remaining	Unlimited access		
	Remove		
Network Name (SSID)	ASUS_68_5G_Guest		
Authentication Method	Open System		
Network Key		Enable	Enable
Time Remaining	Unlimited access	Chirole	Chable
	Remove		

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

## 3.3 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.

Quick Internet	Operation Mode: <u>Wireless router</u> Firmw SSID: <u>ASUS 68 2G</u> <u>ASUS 68 5G</u>	vare Version: 3.0.0.4.382_1180	2 🕹 😳 🔶
General	QoS Traffic Monitor		
品 Network Map	Traffic Manager - QoS		QoS to configuration 🔽
Guest Network		rvice (QoS) ensures bandwidth for tional QoS ensures inbound and o	prioritized tasks and applications. outbound bandwidth on both wired and
🚧 Traffic Manager	wirele param		ations and tasks via manual user-defined
Parental Controls		width Limiter lets you set limits o oS function, click the QoS slide swit	n download and upload speeds. ch and fill in the upload and download.
discrimination	QoS FAQ		
Advanced Settings	Enable QoS	ON	
🛜 Wireless	QoS Type	O Traditional QoS O Bandwidth	Limiter
	Upload Bandwidth	40 Mb/s	<ul> <li>Get the bandwidth information from ISP or go to http://speedtest.net to check</li> </ul>
🕀 wan	Download Bandwidth	100 Mb/s	bandwidth.
IPv6		Apply	
🧐 VPN			

## 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 lowpriority packets.
- 6. Set the highest priority packet. To ensure a smooth online gaming experience, you can set ACK, SYN, and ICMP as the highest priority packet.

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

## 3.3.2 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.

Setup	oS Traffic Mo	nitor				
General Network Map	Traffic Manage	er - Traffic Mo	onitor			Real-time 🔻
	raffic Monitor allo	ws you to monito	or the incoming or outgo	ing packets of the follo	wing:	
Guest Network		Internet	Wired		Wireless	
	Reception					ts from wireless
Parental Controls	Transmission					
N	OTE: Packets fro		re evenly transmitted to	the wired and wireless	s devices.	
	Internet W 5383.30 KB/s	ired Wirel	ess (2.4GHz) Wi	reless (5GHz)		
LAN						
IPv6	8768.31 KB/s					
VPN	2691.65 KB/s					
Firewall						
Administration	1345.83 KB/s					
System Log					Wed	11:27 m / 46, 14 KB/s
Network Tools	Curren	t I	Average	Maximur	n	Total
	2.84 KB	l/s	133.33 KB/s	5370.79 K	B/s	78.12 MB
	1.48 KB		100.95 KB/s	4555.63 K		59.15 MB

**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	Operation Mode: <u>•</u> SSID: <u>ASUS 68 2</u>		ware Version: <u>3. 0. 0. 4. 382 1</u>	1802	&⊡ ↔
General	Parental Contr	ols			
🔒 Network Map		Parental Cont Parental Cont	rols allow you to set the time li rols:	imit for a client's network	usage. To use
Guest Network			Clients Name] column, select t		
Manager Traffic Manager	_	Addres	You may also key in the clien s] column.		
Parental Controls		<ol> <li>In the [.</li> </ol>	Add / Delete] column, click the Time Management] column, cl	ick the edit icon to edit th	he Active Schedule.
USB Application		longer t	the desired time slots for allow time slots. KJ to save the settings made.	ea access times. Drag a	na nola to create
Advanced Settings		Note: 1, Clients tha	at are added to Parental Contro	ols will have their interne	t access restricted
🛜 Wireless					
🔂 LAN	Enable Parental Co	ntrols	ON		
💮 wan	System Time		Tue, Feb 14 08:21:07 201 Reminder. The system time has		h an NTP server.
IPv6	Client List (Max	Limit : 16)			
VPN	-	Client Name (		Time Management	Add / Delete
Firewall	<b>Z</b>	ex: D0:17:C2:E6:C	7:6C 🗾	-	Ð
Administration		AA170020 78:24:AF:		Ø	Θ
System Log			Apply		

## 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 and Servers Center submenus.

**IMPORTANT!** To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <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	Operation Mode: Wireless SSID: ASUS_68_26 ASUS_6	router Firmware Version: <u>3.0.0.4.382 11802</u> 8 <u>5</u> 5			& ⊡ ↔
General					
Hetwork Map		<pre>&gt;(2) =&gt; (3)</pre>			
Suest Network		$\sim$			
Manager Traffic Manager	My FTP server is sha	red.: 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					
🛜 Wireless	Account	Password	Read	Write	
	admin				
	Family				
💮 wan					
🚳 ІРvб					
VPN		Previous Next			

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

Quick Internet	Operation Mode: <u>WiceLess router</u> Finnware Version: <u>3.9.8.4.387_11892</u> & © ← SSID: <u>Asir, et. 26</u> Asir, <u>et. 36</u> ←
General	$1 \longrightarrow 2 \longrightarrow 3$
Guest Network	Create your domain name via the ASUS DDNS services.
Parental Controls	O 1 will use the service test
Advanced Settings	Orable DDNS
🟠 LAN	Previous Next

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

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

## 3.5.2 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 UPnP-supported devices to access multimedia files from the USB disk connected to your wireless router.

**NOTE**: Before using the UPnP Media Server function, connect your device to the RT-ACRH17's network.

Quick Internet	Operation Mode: <u>Wireless router</u> Firmu SSID: <u>ASUS_68_26</u> <u>ASUS_68_56</u>	vare Version: <u>3.0.0.4.382 11802</u> <u>&amp; </u>
General	Media Server Network Place (Samba) Sl	hare FTP Share
Retwork Map	Media Server	<b>S</b>
🚨 Guest Network	Setup the UPnP media server. Media Server	
Manager Traffic Manager	Enable UPnP Media Server	
Parental Controls	Media Server Name	RT-ACRH17-C768
USB Application	Media Server Status	lde
To a ship in the second	Media Server Path Setting	O All Disks Shared O Manual Media Server Path
Advanced Settings		Арріу

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

Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382 11802</u> SSID: <u>ASUS 68 26 ASUS 68 36</u>
General	Media Server Network Place (Samba) Share FTP Share
Retwork Map	USB Application - Network Place (Samba) Share
Guest Network	Set the account and permission of network place(samba) service.
Manager	Enable Share
Parental Controls	Allow guest login Username and password is necessary to log in network place (Samba)
USB Application	Device Name RT-ACRH17-C768
Advanced Settings	Work Group WORKGROUP
🛜 Wireless	Арріу
() wan	Landmin RT-ACRH17-C768 R/W R No
🛞 ІРvб	Save Permission
VPN	

## 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 account lace(Se	ımba) Share / Clouc <mark>×</mark> Disi
New account has no rea	ad/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.	
able Share with account 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.

+*	Quick Internet Setup		e: <u>Wireless r</u> 8_2G_ASUS_68		vare Ve	ersion: ]	3.0.0.	4.382_1	11802				8	è .«	
H	General	Media Server	Network Plac	e (Samba) Sl	nare	FTP SH	nare								
	General														
品	Network Map	USB Applic	ation - FTP	Share										9	E.
*	Guest Network	Set the account	Set the account and permission of FTP service.						II.						
1	Traffic Manager	Enable FTP				OFF									
ß	Parental Controls	Allow anonymo	ous login			OFF									
	USB Application	Maximum num	iber of concurrent	connections											II.
		Character set of	on FTP Server			-8 🗸	·								II.
A	dvanced Settings						Apply								
1	Wireless						Appis								
	LAN	(	€⊝⊘												
-		👤 admin		RT-ACRH1						R/W		No			
۲	WAN			. — К.	пдтаж										
	IPv6							Save	e Perm	ission					

#### To use FTP Share service:

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

Quick Internet	Operation Mode: <u>Wireless router</u> Firmw SSID: <u>ASUS 68 2G</u> <u>ASUS 68 5G</u>	are Version: <u>3.0.0.4.382 11802</u> 🔗 🔁 🗲				
General	General WPS WDS Wireless MAC F	Iter RADIUS Setting Professional				
Hetwork Map	Wireless - General					
🞊 Guest Network	Set up the wireless related information below.					
Manager	Band	2.4GHz 🛩				
Parental Controls	Network Name (SSID)	A5U5_68_2G				
Parental Controls	Hide SSID	Ves ON0				
USB Application	Wireless Mode	Auto 🔽 🗖 Optimized for Xbox 🗹 b/g Protection				
Advanced Settings	Channel bandwidth	20/40 MHz Y				
🛜 Wireless	Control Channel	Auto 🛩 Current control channel: 1				
	Extension Channel	Auto Y				
wan	Authentication Method	open System 🖌				
💮 wan		Αρρίγ				
IPv6						
VPN						

#### To configure the basic wireless settings:

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

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

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

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

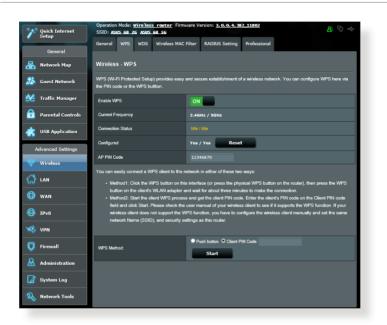
**NOTE:** Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto** and **encryption method** is **WEP** or **TKIP**.

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

10. When done, click Apply.

## 4.1.2 WPS

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



NOTE: Ensure that the devices support WPS.

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

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

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

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

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

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

## 4.1.3 Wireless MAC Filter

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

Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.387_11802</u> SSID: <u>ASUS_68_26_ASUS_68_56</u>	& ⊡ ↔				
General	General WPS WDS Wireless MAC Filter RADIUS Setting Professional					
品 Network Map	Wireless - Wireless MAC Filter					
🞎 Guest Network	Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wirel	ess LAN.				
Manager	Basic Config Band 2.4GHz V					
Parental Controls	Enable MAC Filter O Yes © No					
usb Application						
Advanced Settings	MAC filter list (Max Limit : 64)					
🛜 Wireless	Client Name (MAC Address)	Add / Delete				
	<u> </u>	Ð				
ស <sup>LAN</sup>	No data in table.					
💮 wan	Apply					
1Pv6						
VPN						

### To set up the Wireless MAC filter:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
- 2. In the **Band** 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.

## 4.1.4 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	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382 11802</u> SSID: <u>ASUS 68 26</u> ASUS <u>68 56</u>					
General	General WPS WDS Wireless MAC Filter RADIUS Setting Professional					
Han 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".					
Manager	Band 2.4GHz					
Parental Controls	Server IP Address					
discrete USB Application	Server Port. 1812					
Advanced Settings	Connection Secret					
🛜 Wireless	Apply					
🚮 LAN						
💮 wan						
🚳 IPv6						

#### 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.

## 4.1.5 Professional

The Professional screen provides advanced configuration options.

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

🏯 Network Map	Wireless - Professional				
👭 Guest Network	Wintess Professional Setting allows you to set up additional parameters for wheless. But default values are recommended.				
Manager Traffic Hanager	C Barrinder. The system time has not been sy Band				
Parental Controls	Enable Radio	© Yes ■No			
at USB Application	Enable winkes schotuler	Ci Yes Cillo Inc. Entre			
	Set AP Incluted	■Yes ●No			
Advanced Settings	Poarring assistant	of sale			
Wireless	Enable KIMP Secoping	ofsable V			
🚮 LAN	Multicast Rate(Maps)	Auto			
🕒 wan	Preamble Type	Long M			
🚯 IPv6	RTS Threshold				
	OTIM Interval				
VPN	Bascon Interval				
👽 Firewall	Enable TX Bunking	enuble 💟			
& Administration	Enable WININ APSD	muble 🔽			
📝 System Log	Reducing USB 3.0 interference	muble M			
2 Network Tools	216 QAM	of sale			
	Aistine Faimeas	■ afdeato			
	Explicit Beamforming	enable 🗸			
	Implicit beamforming	efsable 🔽			
	Tx power adjustment	Performance			
		Apply			

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

- **Band**: Select the frequency band that the professional settings will be applied to.
- Enable Radio: Select Yes to enable wireless networking. Select No to disable wireless networking.
- **Time setting**: You can specify which days of the week wireless networking is enabled.

You can specify a time range when wireless networking is enabled during the week.

You can specify which days of the weekend wireless networking is enabled.

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.
- **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.

- Wireless multicast forwarding: Select Enable to allow the wireless router to forward multicast traffic to other wireless devices that support multicast. Select **Disable** to prevent the router from forwarding multicast transmissions.
- 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.

ISUS RT-ACRH			
Quick Internet Setup	Operation Mode: <u>Whreless router</u> I SSID: <u>ASUS_C8_26</u> <u>ASUS_C8_56</u>	Firmware Version: 3.0.0.4.382_11811	
General	LAN IP DHCP Server Route Swit	ch Control	
Network Map	LAN - LAN IP		
Guest Network	Configure the LAN setting of RT-ACRH17.		
🖉 Traffic Manager	IP Address	192.168.50.1	
Parental Controls	Subnet Mask	255.255.255.0	
USB Application		Apply	
Advanced Settings			
Wireless			
LAN			
🗊 wan			

### 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.

/ISLIS RT-ACRH1	7 Logout Rel	boot		English 🔻			
Quick Internet Setup General	SSID: ASUS_C8_2G ASUS_C8_50	Operation Mode: Wireless. router Firmware Version: 3.0.0.4.382_11811 SSID: ASUS_C8_26_ASUS_C8_56 LAN IP DHCP Server Route Switch Control					
Retwork Map	LAN - DHCP Server						
👭 Guest Network	DHCP (Dynamic Host Configuration F						
挫 Traffic Manager		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-ACRH17 supports up to 253 IP addresses for your local network.					
Parental Controls	Basic Config						
at USB Application	Enable the DHCP Server	O Yes ● No					
	RT-ACRH17's Domain Name						
Advanced Settings	IP Pool Starting Address						
🛜 Wireless	IP Pool Ending Address						
🔂 LAN	Lease time	86400					
💮 WAN	Default Gateway						
IPv6	DNS and WINS Server Setting			-			
Firewall	DNS Server						
Firewall	WINS Server						
Administration	Enable Manual Assignment						
📝 System Log	Enable Manual Assignment	• Yes • No					
💫 Network Tools	Manually Assigned IP around	the DHCP list (Max Limit	: 64)	-			
	Client Name (MAC	IP Address	Add / Delete				
	lex::10:78:44:9E:8	Alec 🖌		Ð			
		No data in table.	8				
		Apply					
	Help & Manual   Utility   F Support Registration	eedback   Product	FAQ	P			
		2017 AS	USTeK Computer Inc. All ri	ahts reserved.			

#### 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.
- 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.

/ISUS RT-ACRH1	7 Logout	Reb	oot	-		E	nglish 🔻
Quick Internet Setup General	Operation Mode: <u>W</u> SSID: <u>ASUS_C8_2G</u> LAN IP DHCP Serv	ASUS_C8_5G	<u>er</u> Firmware V Gwitch Control	ersion: <u>3.0.0</u>	).4.382 <u>11</u> 8	<u>11</u> 7	8 G ¢
品 Network Map	LAN - Route						
😤 Guest Network	This function allows yo RT-ACRH17 to share t				ul if you conne	ct several rou	ters behind
🞽 Traffic Manager							
Parental Controls	Basic Config Enable static routes	• Yes • No					
USB Application	Static Route List	(Max Limit : :	32)				
Advanced Settings	Network/Host IP	Netmask		Gateway	Metric	Interface	Add / Delete
🛜 Wireless					-	LAN V	Ð
	No data in table.						
🗊 wan	Apply						
🗟 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.

## 4.3 WAN

## 4.3.1 Internet Connection

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

+ Quick Internet	Operation Mode: <u>wireless</u> router Firm	ware Version: 3. 0. 0. 4. 332 11802
Setup		ual Server / Port Forwarding DMZ DDNS NAT Passthrough
General	Internet Connection Port Ingger Vin	Cual Server / Port Forwarding DM2 DDN5 NA1 Passenrough
Retwork Map	WAN - Internet Connection	
Suest Network		es to WAN (wide area network).These types are selected from the dropdown menu elds differ depending on the connection type you selected.
Manager Traffic Manager	Configure the Ethernet WAN settings of RT-/	ACRH17.
Parental Controls	Basic Config	
•	WAN Connection Type	Automatic IP 🔽
K USB Application	Enable WAN	O Yes O No
Advanced Settings	Enable NAT	O Yes 🔍 No
🛜 Wireless	Enable UPnP UPnP_FAQ	O Yes ● No
🚮 LAN	WAN DNS Setting	
💮 wan	Connect to DNS Server automatically	O Yes O No
6 IPv6	Account Settings	
1940	Authentication	None 👱
🌾 VPN	Host-Uniq (Hexadecimal)	
Firewall	Special Requirement from ISP	
Administration	Host Name	
System Log	MAC Address	78:24:af:ea:41:0b MAC Clone
	DHCP query frequency	Aggressive Mode 🗹
Network Tools	Extend the TTL value	• Yes O No
	Spoof LAN TTL value	• Yes • No
		Apply

### To configure the WAN connection settings:

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

- Enable WAN: Select Yes to allow the router Internet access. Select No to disable Internet access.
- Enable NAT: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- Enable UPnP: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- Connect to DNS Server: 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	Operation Mode: Wireless roo SSID: ASUS 68 2G ASUS 68 5		ware Version: 3	.0.0.4.382_1	1802		8	\$ © ↔
General	Internet Connection Port Trig	jger Vir	tual Server / Po	t Forwarding	DMZ	DDNS N	IAT Passthrough	
品 Network Map	WAN - Port Trigger							
🞎 Guest Network	Port Trigger allows you to tempor two methods for opening incomin							
Manager	anager the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows							
Parental Controls	multiple devices to share a single Port_Trigger_FAQ	open port	and port trigger o	nly allows one o	lient at a	time to acces	ss the open port.	
USB Application	Basic Config		_					
	Enable Port Trigger		🔍 Yes 🔍 No					
Advanced Settings	Well-Known Applications			ect 🔽				
🛜 Wireless	Trigger Port List ( Max Limit : 32 )	Ð						
🚮 LAN	Description	Тл	gger Port	Protocol	Inco	ming Port	Protocol	Delete
💮 wan	No data in table.							
🚳 1Рvб	Apply							
VPN								

### 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.

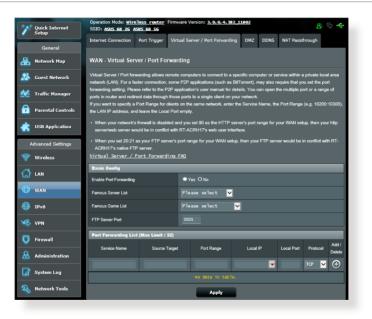
#### NOTES:

- 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.



#### 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.

### 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 I Setup Gen	internet eral	Operation Mode: Wireless router Firm SSID: ASUS_68_2G_ASUS_68_5G Internet Connection Port Trigger Via	ware Version: <u>3.0.0.4.382_11802</u> tual Server / Port Forwarding DMZ DDNS	AT Passthrough
品 Networ	rk Map	WAN - DDNS		
🚨 Guest I	Network		a service that allows network clients to connect to the lered domain name. The wireless router is embedder	
Martine Traffic	Manager	and other DDNS services. If you cannot use ASUS DDNS services, ple	ase go to <u>http://iplookup.asus.com/nslook</u>	up , php to reach your internet
🔒 Parents	al Controls	IP address to use this service.		
-		Enable the DDNS Client	● Yes ● No	
Advanced	pplication Settings		Αρρίγ	
🛜 Wireles	ss			

### To set up DDNS:

- 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**.

Quick Internet	Operation Mode: <u>Wireless router</u> Firm SSID: <u>ASUS 68 2G</u> <u>ASUS 68 5G</u>	ware Version: <u>3.0.0.4.382 11802</u> & 🚊 🗲				
General	Internet Connection Port Trigger Vie	tual Server / Port Forwarding DMZ DDNS NAT Passthrough				
船 Network Map	WAN - NAT Passthrough					
🞊 Guest Network	Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.					
Manager	PPTP Passthrough	Enable M				
Parental Controls	L2TP Passthrough	Enable M				
-	IPSec Passthrough	Enable 🔽				
USB Application	RTSP Passthrough	Enable 🖌				
Advanced Settings	H.323 Passthrough	Enable 🔽				
察 Wireless	SIP Passthrough	Enable 🖌				
🚮 LAN	Enable PPPoE Relay	Disable <mark>V</mark>				
🕕 wan		Αρρίγ				
IPv6						

## 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	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382 11802</u> SSID: <u>ASUS 68.26</u> <u>ASUS 68.56</u>			
	Internet Connection Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough			
General				
Hetwork Map	WAN - NAT Passthrough			
🞊 Guest Network	Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.			
Manager Traffic Manager	PPTP Passthrough Enable			
•	L2TP Passthrough Enable 🔽			
Parental Controls	IPSec Passttrough Enable 🔽			
usb Application	RTSP Passthrough Enable M			
Advanced Settings	H.323 Passthrough Enable 🗹			
🛜 Wireless	SIP Passthrough Enable			
🚮 lan	Enable PPPoE Relay Disable 🔽			
🕕 wan	Apply			
IPv6				

### To set up IPv6:

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

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

## 4.5 Firewall

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

NOTE: The Firewall feature is enabled by default.

## 4.5.1 General

#### To set up basic Firewall settings:

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

## 4.5.2 URL Filter

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

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

### To set up a URL filter:

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

## 4.5.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: <u>3.0.0.4.382_11802</u> SSID: <u>ASUS_68_26_ASUS_68_SG</u>	& ⊡ ↔			
General	General URL Filter Keyword Filter Network Services Filter IPv6 Firewall				
品 Network Map	Firewall - Keyword Filter				
🔉 Guest Network	Keyword Filter allows you to block the clients' access to webpages containing the specified keywords. Limitations of the filtering function :				
Manager Traffic Manager	Lumations of the Internity function : 1. Compressed webpages that use HTTP compression technology cannot be filtered <u>see here for more details.</u> 2. Https webpages cannot be filtered Basic Config Bas				
Parental Controls					
SB Application	Enabled © Disabled				
Advanced Settings	Settings Keyword Filter List (Max Limit : 64)				
🛜 Wireless	Keyword Filter List	Add / Delete			
		Ð			
4	No data in table.				
💮 wan	Apply				
🚳 ІРV6					
🧐 VPN					
V Firewall					

### To set up a keyword filter:

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

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

#### NOTES:

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

## 4.5.4 Network Services Filter

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

General						
品 Network Map	Firewall - Network Services Filter					
🞎 Guest Network	The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port					
Manager	80 will be blocked. Leave the source IP field blank to apply this rule to all LAN devices.					
Parental Controls	Black List Duration : During the scheduled duration, clients in the Black List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.					
USB Application	the specified duration, clients in the White Lis	White List Duration : During the scheduled duration, clients in the White List can CNLY use the specified network services. After the specified duration, clients in the White List and other network clients will not be able to access the Internet or any Internet				
Advanced Settings		service. NOTE : If you set the subnet for the White List, IP addresses outside the subnet will not be able to access the Internet or any				
察 Wireless	Internet service.	Internet service.				
	Network Services Filter	*Reminder: The system time has not been synchronized with an NTP server. Network Service's Filter				
💮 wan	Enable Network Services Filter	• Yes • No				
•	Filter table type	Black List 🔽				
1Pv6	Well-Known Applications	User Defined 🔽				
🧐 VPN	Date to Enable LAN to WAN Filter	Fiber Sillion Si Tue Sillion Si Thu Si Fri				
Firewall	Time of Day to Enable LAN to WAN Filter	Time of Day to Enable LAN to WAN Filter 00 : 00 - 23 : 59				
& Administration	Date to Enable LAN to WAN Filter	🖾 Sat 🖾 Sun				
System Log	Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59				
-	Filtered ICMP packet types					
Network Tools	Network Services Filter Table (Max Lir	Network Services Filter Table (Max Limit : 32)				
	Source IP Port Range	Destination IP Port Range Protocol Add / Delete				
		TCP   _ ⊕				
		No data in table.				

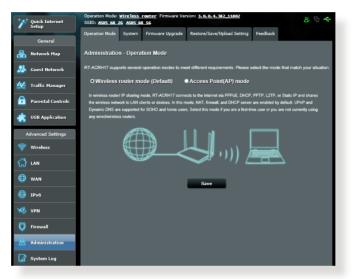
#### To set up a Network Service filter:

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

## 4.6 Administration

## 4.6.1 Operation Mode

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



### To set up the operating mode:

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

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

## 4.6.2 System

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

### To set up the System settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
- 2. You can configure the following settings:
  - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
  - **WPS button behavior**: The physical WPS button on the wireless router can be used to activate WPS 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**.

## 4.6.3 Firmware Upgrade

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

#### To upgrade the firmware:

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

#### NOTES:

- When the upgrade process is complete, wait for some time for the system to reboot.
- If the upgrade process fails, the wireless router automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly. To recover or restore the system, refer to section 5.1 Firmware Restoration.

## 4.6.4 Restore/Save/Upload Setting

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

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

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

## 4.7 System Log

System Log contains your recorded network activities.

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

#### To view your system log:

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

ternet	Operation Mode: <u>wireless router</u> Firm SSID: ASUS 68 26 ASUS 68 56	ware Version: <u>3.0.0.4.332 11802</u> 🔗 🕒 🔶			
Setup	General Log Wireless Log DHCP lea	es IPv6 Routing Table Port Forwarding Connections			
General					
Retwork Map	System Log - General Log				
Suest Network	This page shows the detailed system's activities.				
Manager	System Time	Tue, Feb 14 09:11:56 2017			
Parental Controls	Uptime Feb 14 08:00:41 kernel: Set wait done	0 days 1 hours 11 minute(s) 55 seconds			
USB Application	Tab 10 88:00.41 kansal: Sat frag vap 1 stop sand + cbbc8000         A           Tab 10 88:00.41 kansal: Sat frag vap 1 stop sand + cbbc8000         Fab 10 88:00.41 kansal: Sat vait dosscbbc8000           Tab 10 88:00.41 kansal: Sat vait dosscbbc8000         Fab 10 88:00.41 kansal: Sat vait dosscbbc8000           Fab 10 88:00.41 kansal: Sat vait dosscbbc8000         Fab 10 88:00.41 kansal: Sat vait dosscbbc8000				
Advanced Settings	Two 14 88:00141 kawalı osif_wap_ist: foan in peogees. Cansalling it. sap: Owchoe8000 Two 14 88:00146 kawalı cançıdar_dara_mon_ind_itr for sap 0 (ccf50000) Two 14 88:00146 kawalı Cu vap_stara ordinanı. Two 14 88:00146 kawalı CU vap_stara				
🛜 Wireless	The 14 defended business (c) -gg/mat - The 14 defended business) c) -gg/mat - The 14 defended business) c) -gg/mat - The 14 defended business) - gg/mat - The 14 defended business - gg/mat - The 14 defended busine				
🚮 LAN					
💮 wan	Feb 14 08:00:43 Marmal: sand wama update cod non llw: Feb 14 08:00:43 Marmal: su bise 1 mu bise 0 su bise 1 mu bise 1 impl bf 0 sounding dim 3 Feb 14 08:00:43 Marmal: sand_wdaw_upi_cmd_non_thr for wap 0 (acf30000)				
🚱 ІРvб	Teb 16 06105(45 Bareaks,Lease00011_wast_att_init: Bast Astesna functions are not registered !!! Pab 16 06105(45 Bareaks) 0.1_cont_itatsaft_pab for up1 1(051000) Pab 16 06105(45 Bareaks) andwast_att_indt_pam_Liv Deb 16 06105(40 Bareaks) andwast_att_att_att_indt_pam_Liv Deb 16 06105(40 Bareaks) andwast_att_att_att_att_att_att_att_att_att_				
VPN	Pab 14 08:06:23 nmbd(859): [2017/02/14 Fab 14 08:06:23 nmbd(859): Samba nam	00:85:23, 0) nmbd/nmbd_become_lnb.c:become_local_master_stage2(392) : server RT-ACREI7-C768 is now a local master browser for workgroup WORM↓			
Firewall	Clear	Save Refresh			
Administration					
System Log					
💫 Network Tools					

# 5 Utilities

## 5.1 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.

Se Firmware Restoration				
<u>F</u> ilename:		<u>B</u> rowse		
Status After locating t	he firmware file, click Upload.			
	<u>U</u> pload <u>C</u> lose			

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

**NOTE:** This feature is not supported on MAC OS.

# 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.

***	Quick Internet Setup	Operation Mode: <u>wireless router</u> Firm SSID: <u>AGUS 68 26 AGUS 68 56</u>			8 © ↔	
	General	Operation Mode System Firmware U	pgrade Restore/Save/Upload Set	ing Feedback		
*	Network Map	Administration - Firmware Upgrad	le			
*	Guest Network	Note:				
₩	Traffic Manager	<ol> <li>The latest firmware version include updates on the previous version.</li> <li>For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.</li> </ol>				
£	Parental Controls	<ol> <li>In case the upgrade process fails, RT RT-ACRH17 will indicate such a situa</li> </ol>				
٠	USB Application	<ol> <li>Get the latest firmware version from A</li> </ol>			ajalan koovay.	
A	idvanced Settings	Firmware Version	_	_		
	Wireless	Product ID				
ដ	LAN	Firmware Version	3.0.0.4.382_11802-g15f08f0	Check	Get Beta Firmware	
۲	WAN	New Firmware File	312	Upload		
8	ІРуб					
	VPN					
Q	Firewall					
&	Administration					

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

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

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

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

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

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

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

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

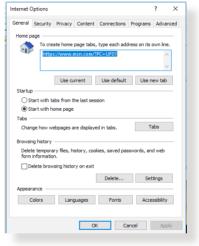
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.  Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You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



## 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.

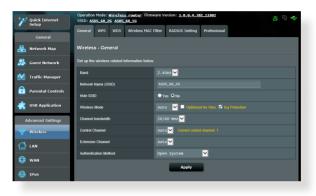
# The client cannot establish a wireless connection with the router.

**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.

*** Quick Internet	Operation Mode: wireless router Firms SSID: ASUS 68 26 ASUS 68 56	ware Version: 3.0.0.4.382 11	102	8 🖻 🗲		
Setup	LAN IP DHCP Server Route IPTV	Switch Control				
Retwork Map	LAN - DHCP Server					
Suest 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-ACR417				
Manager	supports up to 253 IP addresses for your local network.					
Parental Controls	Basic Config Enable the DHCP Server	O Yes O No	_			
USB Application	RT-ACRH17's Domain Name					
Advanced Settings	IP Pool Starting Address	192.168.50.2				
🛜 Wireless	IP Pool Ending Address	192.168.50.254				
	Lease time Default Gateway	86400				
🕀 wan	Describer Calenay					
IPv6	DNS Server					
🍫 VPN	WINS Server					
C Firewall	Enable Manual Assignment					
× ·····	Enable Manual Assignment	O Yes O No				
Administration	Manually Assigned IP around the DHCI	P list (Max Limit : 64)				
System Log	Client Name (MAC A	Client Name (MAC Address)				
💫 Network Tools	6	×		Ð		
		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.



- 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.

Operation Mode: Wireless router Fir SSID: ASUS_68_2G_ASUS_68_5G	8 ⊡ ⇔	
Operation Mode System Firmware	Upgrade Restore/Save/Upload Setting Feedback	
Administration - Restore/Save/L	Jpload Setting	
This function allows you to save current se	ettings of RT-ACRH17 to a file, or load settings from a file.	
Factory default	Restore	
Save setting	Save	
Restore setting	Upload 泡觉	
	SID: <u>Aus</u> <b>ce</b> <u>76</u> <u>Aus</u> <del>ce</del> <u>76</u> Operation Mode System Firmward Administration - Restore/Save/L This function allows you to save current s Factory default Save setting	Operation Mode         System         Firmware Upgrade         Reattory/Save/Upload         Setting         Feedback           Administration - Restore/Save/Upload         Setting         Feedback         Feedback         Feedback           This function allows you to save current settings of RT-ACIBHT7 to a file, or load settings from a file.         Feedback         Feedback         Feedback           Packing detail         Restore         Save setting         Save         Save         Save

#### 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.



- 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
IP address:	router.asus.com
SSID (2.4GHz):	Refer to the label at the bottom of the router
SSID (5GHz):	Refer to the label at the bottom of the router

### Firmware upgrade failed.

. .

- -

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **5.1 Firmware Restoration** on how to use the Firmware Restoration utility.

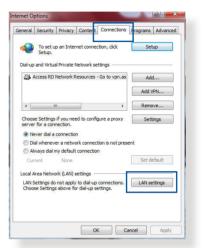
## **Cannot access Web GUI**

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.

	figuration ma	ay override man able automatic o		gs. To ensure the
Automatic	ally detect se	ttings		
Use autom	atic configura	ation script		
Address				
oxv server				
			e settings	will not apply to
Use a prov	y server for VPN connection		e settings	
Use a prov dial-up or ' Address:	VPN connection	ons). Port:	80	will not apply to
Use a prov dial-up or ' Address:	VPN connection	ons).	80	
Use a prov dial-up or '	VPN connection	ons). Port:	80	
Use a prov dial-up or '	VPN connection	ons). Port:	80	

#### **MAC OS**

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

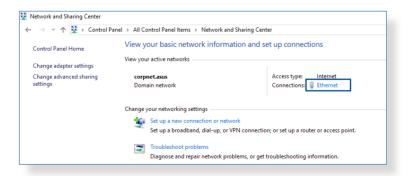
		Automatic	•	
		Built-in Ethernet	;	\ \
	TCP/IP PPP		Proxies Ethernet	)
Select a p	roxy server to conf	Gure: FTP	Proxy Server	
	Proxy (HTTP)		roxy server requires	
	e Web Proxy (HTTPS)			
	ming Proxy (RTSP) S Proxy	2	Set Password.	
	er Proxy	4 7		
	oxy settings for ts & Domains:			
-				
	ssive FTP Mode (PA	SV)		(?)

**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.

General				×
General				
Connection				
IPv4 Connectiv	ity		1	nternet
IPv6 Connectiv		Ne	network	
Media State:	icy.	146		Enabled
Duration:				3:29:31
Speed:				.0 Gbps
				.0 00ps
Details				
Activity				
Activity				
	Sent		— R	eceived
Bytes:	71,424,646	Ĩ	70,3	727,241
Properties	Disable	Diagno	ise	
🖗 Ethernet Properti	es			×
Networking Authenti	cation			
Connect using:				
Intel(R) Ethem	et Connection (2	) I219-V		
This connection uses	s the following ite	ms:	Config	ure
QoS Packe				^
	tocol Version 4 (1	TCP/IPv4)	1	
	etwork Adapter N		otocol	
	DP Protocol Driv		_	
	tocol Version 6 (1			
	Fopology Discove Fopology Discove			
<	opology Discove	ay mapper i	O Driver	*
-				>
In shall	Hereitel		D	>
Install	Uninstal		Propert	
Description				ies
Description Transmission Cont	rol Protocol/Inter	net Protocol	. The def	ies ault
Description	rol Protocol/Inter	net Protocol	. The def	ies
Description Transmission Cont wide area network across diverse inte	rol Protocol/Inter protocol that pro erconnected netw	net Protocol ivides comm iorks.	. The def	ault
Description Transmission Cont wide area network across diverse inte	rol Protocol/Inter protocol that pro erconnected netw	net Protocol ivides comm iorks.	. The def	ies ault
Description Transmission Cont wide area network	rol Protocol/Inter protocol that pro econnected netw ion 4 (TCP/IPv4)	net Protocol ivides comm iorks.	. The def	ault
Description Transmission Cont wide area network across diverse inte across diverse inte Internet Protocol Versi General Alternate Co	rol Protocol/Inter protocol that pro erconnected netw ion 4 (TCP/IPv4) nfiguration	net Protocol vides comm vorks. Properties	. The defunication	ault ×
Description Transmission Cont wide area network across diverse inte	rol Protocol/Inter protocol that pro rconnected netw ion 4 (TCP/IPv4) nfiguration gs assigned autom	net Protocol wides comm vorks. Properties atically if you	. The def unication	ault X
Description Transmission Cont wide area network across diverse inte Internet Protocol Versi General Alternate Co You can get IP settin this capability. Other for the appropriate IP () Obtain an IP add	rol Protocol/Inter protocol that pro- proconnected networks ion 4 (TCP/IPv4) infiguration gs assigned autom vise, you need to * settings. dress automatically	net Protocol vides comm rorks. Properties atically if you ask your net	. The def unication	ault X
Description Transmission Cont wide area network across divense inte Internet Protocol Versi General Alternate Co You can get IP settin this capabily. Other for the appropriate IP @ Obtain an IP add O Use the followin	rol Protocol/Inter protocol that pro- proconnected networks ion 4 (TCP/IPv4) infiguration gs assigned autom vise, you need to * settings. dress automatically	net Protocol vides comm rorks. Properties atically if you ask your net	. The def unication	ault X
Description Transmission Cort wide area network across diverse inte Internet Protocol Versi General Alternate Co You can get IP setting this capabily. Other for the appropriate IP @ Obtain an IP add O Use the followin IP address:	rol Protocol/Inter protocol that pro- proconnected networks ion 4 (TCP/IPv4) infiguration gs assigned autom vise, you need to * settings. dress automatically	net Protocol vides comm vorks. Properties atically if you ask your net	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across diverse inte Internet Protocol Versi General Alternate Co You can get IP setting this capability. Other for the appropriate IP Obse the followin IP address: Subnet mask:	rol Protocol/Inter protocol that pro- proconnected networks ion 4 (TCP/IPv4) infiguration gs assigned autom vise, you need to * settings. dress automatically	net Protocol vides comm rorks. Properties atically if you ask your net	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across diverse inte control of the second second control of the second second the capability. Other for the appropriate IR Ouse the followin IP address: Subnet mask: Default gateway:	rol Protocol/inter protocol that pro reconnected netw ion 4 (TCP/IPv4) nfiguration ga sagiqued automise, you need to settings. these automatically IP address:	net Protocol vides comm orks. Properties atically if you ask your net	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across diverse inte Internet Protocol Versi General Altemate Cont You can get IP setting this capability. Other for the appropriate IP Could the appropriate IP Could and IP address Subnet mask: Default gatoway: © Otain NDS servi-	rol Protocol/inter roornected network ion 4 (TCP/IPv4) infguration gassigned autom settings. dress automatically g IP address:	net Protocol vides comm properties atically if you ask your net , , , , , , , , , , , , , , , , , , ,	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across divense inte Internet Protocol Versi General Alternate Co You can get P setting this capability. Other for the appropriate II @ Obtain n. IP add Def bottain n. IP add Def setting active Subnet mask: Def sout gateway: @ Obtain NDS serv. . Use the following	rol Protocol/inter protocol that pro rconnected netw ion 4 (TCP/IP-4) infiguration ps assigned autom insety you need to settings. dress automatical g IP address: er address autom g DNS server addr	net Protocol vides comm properties atically if you ask your net , , , , , , , , , , , , , , , , , , ,	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across diverse inte Internet Protocol Versi General Altemate Cont You can get IP setting this capability. Other for the appropriate IP Could the appropriate IP Could and IP address Subnet mask: Default gatoway: © Otain NDS servi-	rol Protocol/inter protocol that pro rconnected netw ion 4 (TCP/IP-4) infiguration ps assigned autom insety you need to settings. dress automatical g IP address: er address autom g DNS server addr	net Protocol vides comm properties atically if you ask your net , , , , , , , , , , , , , , , , , , ,	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across divense inte Internet Protocol Versi General Alternate Co You can get P setting this capability. Other for the appropriate II @ Obtain n. IP add Def bottain n. IP add Def setting active Subnet mask: Def sout gateway: @ Obtain NDS serv. . Use the following	rol Protocol/inter protocolthat protocolthat protocolthat protocolthat pro- reconnected networks ion 4 (TCP/IPv4) infiguration grassing automatical grass automatical graddress: er address autom g DNS server address	net Protocol vides comm properties atically if you ask your net , , , , , , , , , , , , , , , , , , ,	. The def unication r network work admi	ault X
Description Transmission Cont wide area network across divense inte Internet Protocol Versi General Alternate Co You can get IP settin this capability. Other for the appropriate IJ Obtain an IP add Obtain An IP add Def ault gateway: Obtain task: Def ault gateway: Obtain DAS ser Obtain DAS ser	rol Protocol/inter protocolthat protocolthat protocolthat protocolthat pro- reconnected networks in a 4 (TCP/IPv4) in 4 (TCP/IPv4) in gassigned autom settings. dress automatically produces automatically pro	net Protocol vides comm properties atically if you ask your net , , , , , , , , , , , , , , , , , , ,	r network	ault X

#### **MAC OS**

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

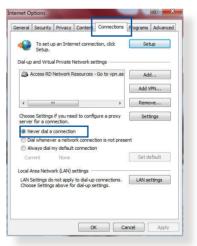
	L	ocation: Aut	omatic		•	
		Show: Buil	t-in Ethernet		;	
	ТСР	/IP PPPoE	AppleTalk	Proxies Et	nernet	
Confi	aure IPv4:	Using DHCF	•	:		
	P Address:	192.168.18	2.103	6	Renew DH0	P Lease
Sub	onet Mask:	255.255.25	5.0 DHC	P Client ID:		
	Router:	192.168.18	2.250		(If required)	
DN	IS Servers:	192.168.12	8.10			(Optional)
Search	Domains:					(Optional)
IPve	5 Address:	fe80:0000:00	000:0000:0211	:24ff:fe32:b1	8e	
		Configure I	Pv6)			(?)

**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.

**IMPORTANT!** This device within the 5.15 ~ 5.25 GHz is restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

**CAUTION**: 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.

## **Safety Information**

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

## **GNU General Public License**

#### **Licensing information**

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

### **GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not

price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

- 2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
  - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

- 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a) Accompany it with the complete corresponding machinereadable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this

License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9. The Free Software Foundation may publish revised and/or new

versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### **NO WARRANTY**

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## **Safety Notices**

- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- DO NOT place on uneven or unstable work surfaces. Seek servicing if the casing has been damaged.
- DO NOT place or drop objects on top and do not shove any foreign objects into the product.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the modem during electrical storms.
- DO NOT cover the vents on the product to prevent the system from getting overheated.
- DO NOT use damaged power cords, accessories, or other peripherals.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.

### For Turkey only

#### Authorised distributors in Turkey:

#### BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel. No.:	+90 212 3311000
Address:	AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
	AYAZAGA/ISTANBUL

#### CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.:	+90 212 3567070
Address:	CEMAL SURURI CD. HALIM MERIC IS MERKEZI
	No: 15/C D:5-6 34394 MECIDIYEKOY/

#### ISTANBUL KOYUNCU ELEKTRONIK BILGI ISLEM SIST. SAN. VE DIS TIC. A.S.

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

## **ASUS Contact information**

#### **ASUSTeK COMPUTER INC. (Asia Pacific)**

Address	1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112,
	TAIWAN
Telephone	+886-2-2894-3447
Fax	+886-2-2890-7798
Web site	https://www.asus.com

#### **Technical Support**

Telephone	+86-21-38429911
Online support	https://qr.asus.com/techserv

#### **ASUS COMPUTER INTERNATIONAL (America)**

Address	48720 Kato Rd., Fremont, CA 94538, USA
Telephone	+1-510-739-3777
Fax	+1-510-608-4555
Web site	https://www.asus.com/us/

#### **Technical Support**

Support fax	+1-812-284-0883
Telephone	+1-812-282-2787
Online support	https://qr.asus.com/techserv

#### ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkortstrasse 21-23, 40880 Ratingen, Germany
Web site	https://www.asus.com/de
Online contact	https://www.asus.com/support/Product/
	ContactUs/Services/questionform/?lang=de-de

#### **Technical Support**

Telephone (DE) Telephone (AT) Online support +49-2102-5789557 +43-1360-2775461 https://www.asus.com/de/support

#### NOTES:

- UK support e-mail: <u>network support uk@asus.com</u>
- For more information, visit the ASUS support site at: <u>https://www.asus.com/support/</u>

#### SUPPORT HOTLINE

#### **USA/ CANADA**

Hotline Number: 1-812-282-2787 Language: English

Availability: Mon. to Fri. 8:30-12:00am EST (5:30am-9:00pm PST)

> **Sat. to Sun.** 9:00am-6:00pm EST (6:00am-3:00pm PST)

#### BRAZIL

Hotline Number: 4003 0988 (Capital) / 0800 880 0988 (demais localidades) Language: Portuguese

Availability: **Mon. to Fri.** 

9:00am-18:00

#### Manufacturer

#### **ASUSTeK Computer Inc.**

Tel: +886-2-2894-3447 Address: 1F, No. 15, LIDE RD., BEITOU DIST., TAIPEI CITY 112, TAIWAN

#### Authorised representative in Europe

ASUS Computer GmbH Address: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

#### Authorised distributors in Turkey

#### BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel: +90 212 3311000 Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL

#### CIZGI Elektronik San. Tic. Ltd. Sti.

Tel: +90 212 3567070Address: CEMAL SURURI CD. HALIM MERIC IS MERKEZI No: 15/C D:5-6 34394 MECIDIYEKOY/ ISTANBUL

#### KOYUNCU ELEKTRONIK BILGI ISLEM SIST. SAN. VE DIS TIC. A.S.

Tel: +90 216 5288888 Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZI, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.