User Guide

RT-AC59U V2

Wireless-AC1500 Dual Band USB Router





E17524 First Edition November 2020

Copyright © 2020 ASUSTeK Computer Inc. All Rights Reserved.

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

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

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

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

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

Table of contents

1	Getting to know your wireless router	6
1.1	Welcome!	6
1.2	Package contents	6
1.3	Your wireless router	7
1.4	Positioning your router	9
1.5	Setup Requirements	
1.6	Router Setup	
	1.6.1 Wired connection	11
	1.6.2 Wireless connection	12
2	Getting started	14
2.1	Logging into the Web GUI	14
2.2	Quick Internet Setup (QIS) with Auto-detection	15
2.3	Connecting to your wireless network	
3	Configuring the General settings	20
3.1	Using the Network Map	
	3.1.1 Setting up the wireless security settings	21
	3.1.2 Managing your network clients	22
	3.1.3 Monitoring your USB device	23
3.2	Creating a Guest Network	
3.3	Using the Traffic Manager	
	3.3.1 Managing QoS (Quality of Service) Bandwidt	h28
	3.3.2 Monitoring Traffic	31
3.4	Setting up Parental Control	
3.5	Using the USB Application	
	3.5.1 Using Servers Center	
	3.5.2 3G/4G	35

Table of contents

4	Config	guring the Advanced Settings	37
4.1		255	
	4.1.1	General	
	4.1.2	WPS	40
	4.1.3	Wireless MAC Filter	42
	4.1.4	RADIUS Setting	43
	4.1.5	Professional	44
4.2	LAN		
	4.2.1	LAN IP	46
	4.2.2	DHCP Server	47
	4.2.3	Route	49
4.3	WAN		50
	4.3.1	Internet Connection	50
	4.3.2	Port Trigger	53
	4.3.3	Virtual Server/Port Forwarding	55
	4.3.4	DMZ	58
	4.3.5	DDNS	59
	4.3.6	NAT Passthrough	60
4.4	IPv6		61
4.5	VPN S	erver	62
4.6	Firewa	all	63
	4.6.1	General	63
	4.6.2	URL Filter	63
	4.6.3	Keyword filter	64
	4.6.4	Network Services Filter	65
4.7	Admi	nistration	67
	4.7.1	Operation Mode	67
	4.7.2	System	
	4.7.3	Firmware Upgrade	69

Table of contents

	4.7.4 Restore/Save/Upload Setting	69
4.8	System Log	70
5	Utilities	71
5.1	Device Discovery	71
5.2	Firmware Restoration	72
6	Troubleshooting	74
6.1	Basic Troubleshooting	74
6.2	Frequently Asked Questions (FAQs)	77
App	pendices	87
Noti	ces	
ASU	S Contact information	100

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS RT-AC59U V2 Wireless Router! The ultra-thin and stylish RT-AC59U V2 features a 2.4GHz and 5GHz dual bands for an unmatched concurrent wireless HD streaming; SMB server, and UPnP AV server for 24/7 file sharing.

1.2 Package contents

☑ RT-AC59U V2 Wireless Router

Power adapter

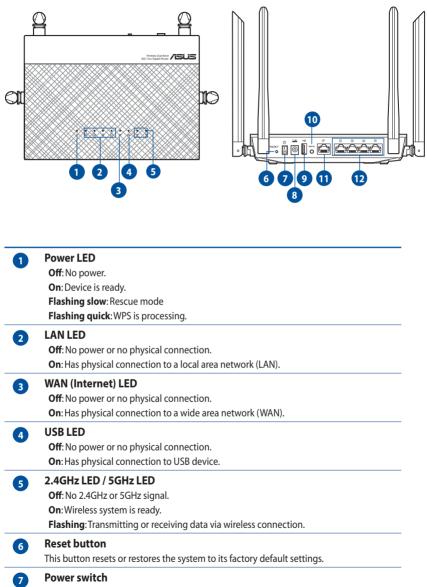
☑ Warranty card

☑ Network cable (RJ-45)

☑ Quick Start Guide

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

1.3 Your wireless router



Switch to power on or off the system.

8	Power (DC-IN) port Insert the bundled AC adapter into this port and connect your router to a power source.
9	USB port Insert a USB device such as USB hard disk or USB flash drive into the port. Insert your iPad's USB cable into the port to charge your iPad.
10	WPS button This button launches the WPS Wizard.
1	WAN (Internet) port Connect a network cable into this port to establish WAN connection.
12	LAN 1 ~ 4 ports Connect network cables into these ports to establish LAN connection.

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

DC Power adapter	DC Output: +12V with max 1.5A current;		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

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

- Place the wireless router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- Keep the device away from 802.11b/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 external antennas as shown in the drawing below.



1.5 Setup Requirements

To set up your wireless network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/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 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.

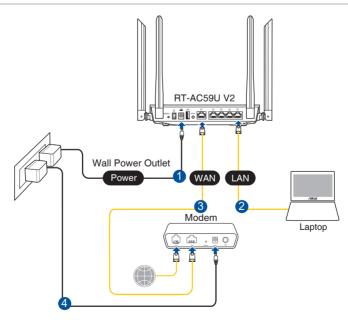
1.6 Router Setup

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.



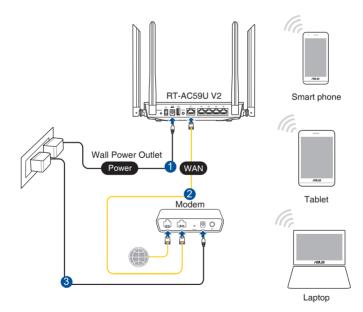
To set up your wireless router via wired connection:

- 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.
- 4. Install an IEEE 802.11a/b/g/n/ac WLAN adapter on your computer.

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

2 Getting started

2.1 Logging into the Web GUI

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

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

- On your web browser, manually key in the wireless router's default IP address: <u>192.168.1.1</u> or enter <u>http://router.asus.</u> <u>com</u>.
- 2. On the login page, key in the default user name (**admin**) and password (**admin**).
- 3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



Top command buttons

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

2.2 Quick Internet Setup (QIS) with Autodetection

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

NOTE: When setting the Internet connection for the first time, press the Reset button on your wireless router to reset it to its factory default settings.

To use QIS with auto-detection:

1. The QIS page launches automatically.



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

2. The wireless router automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP** 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

品 Skip Setup Wizard	Account Setting	
Quick Internet Setup Check Connection Internet Setup Router Setup	Please enter your username and password User Name 2 Password 2 Show password MAC Address(optional) 2 MAC Cone	Internet Connection Information Error Resource provide Account Name Pateriori
	Enable VPN client Special Requirement from ISP	User Name 2
	Previous Next	Enter the user name and password for your Internet connection information These settings were given by your Internet Service Provider (ISP).

- 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.

品 Skip Setup Wizard	Wireless Setting
	Do you want to use the previous wireless security settings?
Quick Internet Setup	Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.
Check Connection	2.4 GHz - Security
Internet Setup	Network Name (SSID) 3 ASUS_2.4G
	Network Key 👔
3 Router Setup	5 GHz - Security Copy 2.4 GHz to 5 GHz settings.
	Network Name (SSID)
	Network Key 🕐
	Enter a network key between 8 and 63 characters/letters, numbers or a combination) or 64 hex oligits. The default writeries security setting is WPA2-Pensonal AES. If you do not want to set the network recurity, leave the security key field blank, but this exposes your network to unauthorized access.
	Арріу

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

	npleted Network Configuration S	Summary
Skip Setup Wizard	ipietea network oomgalation a	,
	System Time: Mon, Feb 09 07:	59:03 2015 (GMT)
Quick Internet Setup		
Check	Network Name (SSID)	ASUS
U Connection	Wireless Security	Open System
Internet Setup		
anternet setup	Network Name (SSID)	ASUS_5G
(3) Router Setup	Wireless Security	Open System
Router Setup		
	WAN Connection Type	Automatic IP
	WAN IP	192.168.123.174
	LAN IP	192.168.50.1
	MAC	00:0C:43:26:60:40
		Next

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 2.4GHz 5GHz Status Wireless name(SSID) ASUS RT-AC59U_V2_2.4G Authentication Method WPA2-Personal WPA Encryption AES T WPA-PSK key Apply 192.168.50.1 **PIN code** 12345670 LAN MAC address 00:0C:43:E1:76:28 Wireless 2.4GHz MAC address 00:0C:43:E1:76:28

5GHz security settings

System Status
2.4GHz 5GHz Status
Wireless name(SSID)
ASUS RT-AC59U_V2_5G
Authentication Method
WPA2-Personal
WPA Encryption
AES V
WPA-PSK key
AiRadar
Apply
Арріу
LAN IP
LAN IP
LAN IP 192.168.50.1
LAN IP 192.168.50.1 PIN code
LAN IP 192.168.50.1 PIN code 12345670
LAN IP 192.168.50.1 PIN code 12345670 LAN MAC address
LAN IP 192.168.50.1 PIN code 12345670 LAN MAC address 00:0C:43:E1:76:28

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

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

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

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



3.1.2 Managing your network clients

To manage your network clients:

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

3.1.3 Monitoring your USB device

The ASUS Wireless Router provides a USB 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.

- For more details, refer to the section **3.5.1 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.

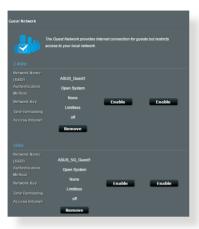
NOTE: RT-AC59U V2 supports up to six SSIDs (three 2.4GHz and three 5GHz SSIDs).

To create a guest network:

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

The Guest Network provides Int your Intranet.	ernel connection for guests but	t restricts access to
Enable	Enable	Enable
Enable	Enable	Enable

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



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

3.3 Using the Traffic Manager

3.3.1 Managing QoS (Quality of Service) Bandwidth

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

Quick Internet	Operation Mode: <u>Wireless row</u> SSID: <u>ASUS RT-AC</u> <u>ASUS RT</u> QoS Traffic Monitor		.0.0.4.378_6701	9 A	¢
General	Traffic Manager - QoS			QoS to configuration	
Retwork Map		The Quality of Service (QoS	S) ensures the network's s	peed performance. The default rule	
🔏 Guest Network		applications (peer-to-peer a	pplications such as BitTon	iority and are not influenced by P2P rent). To enable QoS function, Click and handwidth Folds. Cot the	
Manager	the QoS slide switch, and fill in the upload and download bandwith fields. Get the bandwith information from your ISP. If you want to prioritize specific network applications and network devices, select your				
Parental Controls		preferred priority from the U QoS FAQ	lser-defined QoS rules.		
SB Application	Enable Smart QoS	ON			
Advanced Settings	Upload Bandwidth		Mb/s		
🛜 Wireless	Download Bandwidth		Mb/s		
🔂 LAN			Apply		

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.



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

3.4 Setting up Parental Control

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

Quick Internet Setup	Operation Mode: Wireless. router Firmware Version: 3.9.0.4.378.5701 Q B G &		
General	Parental Controls		
🔠 Network Map	Parental Controls allow you to set the time limit for a client's network usage. To use Parental Controls:		
🚵 Guest Network	 In the [Clients Name] column, select the client whose network usage you want to control. You may also key in the clients MAC address in the [Clients MAC 		
🔆 Traffic Manager	Address) column. Address) column. () In the (Add / Delete) column. click the plus(+) icon to add the client.		
Parental Controls	2. In the (Add / Deletel calumn, click the plusif) icon to add the client. 3. In the [Time Management] column, click the edit icon to edit the Active Schedule. 4. Select the desired time stats for allowed access times. Drag and hold to create		
usb Application	 Clock in the durates time durates and the allowed durates they are they are the durates Click [OK] to save the settings made. 		
Advanced Settings	Click to open the tutorial video.		
察 Wireless	Note: Clients that are added to Parental Controls will have their internet access restricted by default.		
	Enable Parental Controls ON		
💮 wan	System Time Thu, Jan 01 08:32:51 201 *Reminder. The system time has not been synchronized with an NTP server.		
1Pv6	Client List (Max Limit : 16)		
Firewall	Clients Name Clients MAC Address Time Management Add / Delete		
& Administration	□ · · · ·		
System Log	No data in table.		
💫 Network Tools	Арріу		

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 Application function provides Servers Center.

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 Servers Center

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

Using Network Place (Samba) Share service

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

/ISLIS RT-AC59U	V2 Logout Rebo	×	English 👻	
C Quick Internet Setup	Operation Mode: Window center Firmware Network Place (Samba) Share FTP Sha	Version: <u>\$44.4.387 51585</u> SSID: <u>A818 (</u> F) A818 (F)	864	
🚯 Network Map	USB Application - Network Place (Samba) Share			
Guest Network	Sel Bie accurit and parministin of network plana(samba) service. Note: Byou are using WendowsB 10, use this (2AC) to anable SABAY Client to amoune you have access to Bien stoned within the material.			
Parental Controls	Enable Share			
USB Application	Allow guest login	OFF Usemame and password is necessary to log in t place(Sembel)	network	
	Device Name			
Wireless	Work Group	WORKGROUP		
		Apply		

To use Samba share:

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

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

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

To create a new account:

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

	Add new accountriace(Samba) Share / Clouc <mark>X</mark> a
	New account has no read/write access rights.
	Account:
	Password:
	Retype password:
	Add
l	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.

dd new folder in, sda e (Samba) Share / Cloud D	×
The default access rights for a new folder is read/write.	
Folder Name:	
Add	

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

3.5.2 3G/4G

3G/4G USB modems can be connected to RT-AC59U V2 to allow Internet access.

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

Quick Internet Setup	Operation Mode: <u>Wireless router</u> F SSID: <u>ASUS ASUS SG</u>	irmware Version: <u>3.0.0.4.260</u> & 🕒 🗲 🖻
General	USB Modem	S
🏪 Network Map	The current 3G/4G setting is set to 3G/4G Backup mode. If WAN port was disconnected, the network mode will automatically turn to 3G/4G mode.	
😤 Guest Network	Basic Config	
Traffic Manager	Enable USB Modem	© Yes ● No
	Location	Manual 🗸
Parental control	USB Modern	WCDMA (UMTS)
USB application	APN service(optional)	
AiCloud	Dial Number	
	PIN code	
Advanced Settings	Usemame	
🛜 Wireless	Password	
🔓 LAN	USB Adapter	auto
🕀 WAN		Apply

To set up 3G/4G internet access:

- 1. From the navigation panel, click **General** > **USB application** > **3G/4G**.
- 2. In the Enable USB Modem field, select Yes.
- 3. Set up the following:
 - Location: Select your 3G/4G service provider's location from

the dropdown list.

- **ISP**: Select your Internet Service Provider (ISP) from the dropdown list.
- **APN (Access Point Name) service (optional)**: Contact your 3G/4G service provider for detailed information.
- **Dial Number and PIN code**: The 3G/4G provider's access number and PIN code for connection.

NOTE: PIN code may vary from different providers.

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

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

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> Fi SSID: <u>ASUS RT-AC</u> <u>ASUS RT-AC</u>					
Setup	General WPS Wireless MAC Filter	RADIUS Setting Professional				
General						
品 Network Map	Wireless - General					
Suest Network	Set up the wireless related information be	łow.				
	Band	SGHz •				
Traffic Manager	SSID	ASUS RT-AC59U_V2_5G				
Parental Controls	Hide SSID	• Yes O No				
USB Application	Wireless Mode	Auto				
	Channel bandwidth	20/40/80 MHz *				
Advanced Settings	Control Channel	Auto •				
察 Wireless	Extension Channel	Auto -				
	Authentication Method	WPA2-Personal •				
💮 WAN	WPA Encryption	AES T				
🍪 IPv6	WPA Pre-Shared Key	44332211				
Firewall	Network Key Rotation Interval	3600				
Administration		Apply				

To configure the basic wireless settings:

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

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

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

Quick Internet	Operation Mode: Wireless router Fi SSID: ASUS RT-AC ASUS RT-AC	
	General WPS Wireless MAC Filter	RADIUS Setting Professional
General		
Retwork Map	Wireless - WPS	
🔉 Guest Network	WPS (Wi-Fi Protected Setup) provides eas via the PIN code or the WPS buttlon.	y and secure establishment of a wireless network. You can configure WPS here
Manager Traffic Manager	Enable WPS	
Parental Controls	Current Frequency	2.4GHz
USB Application	Connection Status	Idle
USB Application	Configured	Yes Reset
Advanced Settings	AP PIN Code	12345670
察 Wireless	You can easily connect a WPS client to the	network in either of these two ways:
		his interface (or press the physical WPS button on the router), then press the lapler and wait for about three minules to make the connection.
💮 wan		ess and get the client PIN code. Enter the client's PIN code on the Client PIN
		eck the user manual of your wireless client to see if it supports the WPS
🔯 1Pv6		not support the WPS function, you have to configure the wireless client Name (SSID), and security settings as this router.
Firewall	Hanvany and set the same network	Name (SSID), and security settings as this router.
	WPS Method:	Push button O Client PIN Code
D curture to a		Start
System Log		

To enable WPS on your wireless network:

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

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

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

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

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

4.1.3 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>3.0.0.4.378 6701</u> SSID: ASUS RT-AC, ASUS RT-AC	¥ @ ⊕ ↔			
Jour	General WPS Wireless MAC Filter RADIUS Setting Professional				
General					
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	Wireless LAN,			
	Basic Config				
Manager Traffic Manager	Enable MAC Filter O Yes O No				
Parental Controls	MAC Filter Mode Accept				
LISB Application	MAC filter list (Max Limit : 64)	and the second se			
	MAC filter list	Add / Delete			
Advanced Settings		Ð			
🛜 Wireless	No data in table.				
	Apply				
💮 wan					

To set up the Wireless MAC filter:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
- 2. In the **Frequency** field, select the frequency band that you want to use for the Wireless MAC filter.
- 3. In the MAC Filter Mode dropdown list, select either Accept or Reject.
 - Select Accept to allow devices in the MAC filter list to access to the wireless network.
 - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
- 4. On the MAC filter list, click the **Add** 💿 button and key in the MAC address of the wireless device.
- 5. Click Apply.

4.1.4 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 Setup	Operation Mode: <u>wireless router</u> Fir SSID: <u>ASUS RT-AC</u> <u>ASUS RT-AC</u>		₽ @ © ◆
	General WPS Wireless MAC Filter	RADIUS Setting Professional	
General			
🔠 Network Map	Wireless - RADIUS Setting		
🞊 Guest Network		parameters for authorizing wireless clients through RADIUS : "Wireless - General" as "WPA-Enterprise/ WPA2-Enterprise/	A CONTRACTOR OF A CONTRACTOR A
Manager	802.1X .		
D =====1	Band	5GHz ·	
Parental Controls	Server IP Address		
discrimination	Server Port.		
Advanced Settings	Connection Secret		
🛜 Wireless		Apply	

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.

Quick Internet Setup	Operation Mode: <u>Wireless router</u> Fi SSID: <u>ASUS RT-AC</u> <u>ASUS RT-AC</u> General WPS Wireless MAC Filter	
General	Wireless - Professional	NUIDS Setting Professional
Guest Network	Wireless Professional Setting allows you to * Reminder: The system time has not been	set up additional parameters for wireless. But default values are recommended. synchronized with an NTP server.
🚧 Traffic Manager	Band	5GHz
	Enable Radio	O Yes ● No
USB Application	Enable wireless scheduler	O Yes ● No <u>Time Selling</u>
SB Application	Set AP Isolated	• Yes O No
Advanced Settings	Enable IGMP Snooping	Disable *
🛜 Wireless	Multicast Rate(Mbps)	Auto
🚮 LAN	Preamble Type	Short •
() wan	AMPDU RTS	Enable
🙈 1Pv6	RTS Threshold	
1Pv6	DTIM Interval	
Firewall	Beacon Interval	
Administration	Enable TX Bursting	Enable
System Log	Enable Packet Aggregation	Enable
🕰 Network Tools	Enable WMM APSD	Enable
The work roots	Enable WMM DLS	Disable
		Apply

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

- **Band**: Select the frequency band that the professional settings will be applied to.
- Enable Radio: Select Yes to enable wireless networking. Select No to disable wireless networking.
- Enable Wireless Scheduler: You can set the time range when wireless networking is enabled during the week.
- Set AP isolated: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.

- **Enable IGMP Snooping:** When enabled, IGMP Snooping monitors IGMP communication among devices and optimizes multicast traffic.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- AMPDU RTS: Select Enable to enable RTS for every AMPDU.
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.
- Enable Packet Aggregation: Select Enable to increase the delivered bandwidth in your network.
- Enable WMM APSD: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
- Enable WMM DLS: Select Enable to set WMM Direct Link Setup.

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.

Quick Internet	Operation Mode: <u>Wireless rout</u> Version: 3.0.0.4.376_3792 SS LAN IP DHCP Server Route		8 8		
General					
船 Network Map	LAN - LAN IP				
Guest Network	Configure the LAN setting of RT-AC59U V2,				
Manager	IP Address	192.168.50.1			
A Parental	Subnet Mask	255.255.255.0			
Controls		Apply			
discrete Section USB Application		Арру			

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.

V Qui Set	ick Internet up	Operation Mode: <u>Winceless router</u> Firmware Version: <u>3.0.0.4.378.6701</u> SSID: <u>ASUS RT-AC</u> ASUS <u>RT-AC</u> LAN IP DHCD Server Route IPTV							
G	eneral								
品 Net	twork Map	LAN - DHCP Server	LAN - DHCP Server						
Sur Ret	est twork	DHCP (Dynamic Host Configuration networks. The DHCP server can ass							
	ffic nager	server IP and default gateway IP.RT							
	rental atrols	Basic Config							
📥 USI		Enable the DHCP Server O Yes No							
💽 Арр	olication	RT-AC59U V2's Domain Name							
Advanc	ed Settings	IP Pool Starting Address 192.168.50.2							
察 Wir	reless	IP Pool Ending Address 192.168.50.25							
🞧 LAI	4	Lease time	86400						
() wa	N N	Default Gateway							
	-6	DNS and WINS Server Setting							
- In .	N .	DNS Server							
🔽 Fire	ewall	WINS Server							
🔏 Adr	ninistration	Enable Manual Assignment							
📝 Sys	stem Log	Enable Manual Assignment	• Yes • No						
	work	Manually Assigned IP around	the DHCP list ((Max Limit : 64)					
No Too	ls	MAC address		IP Address	Add / Delete				
					Ð				
			No data in	table.					
			Appl	v					

To configure the DHCP server:

- 1. From the navigation panel, go to **Advanced Settings** > **LAN** > **DHCP Server** tab.
- 2. In the Enable the DHCP Server field, tick Yes.
- 3. In the **Domain Name** text box, enter a domain name for the wireless router.
- 4. In the **IP Pool Starting Address** field, key in the starting IP address.
- 5. In the **IP Pool Ending Address** field, key in the ending IP address.

6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

NOTES:

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

4.2.3 Route

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

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

Quick Internet Setup	Operation Mode: <u>Wire1ess</u> SSID: <u>ASUS_RT-AC</u> ASUS LAN IP DHCP Server Rou	5 RT-AC	n: <u>3.0.0.4.378_6701</u>		₽ 8	\$ <u>0</u> \$		
General	LAN - Route							
🚨 Guest Network	This function allows you to ad RT-AC59U V2 to share the sa			nnect seve	ral routers l	behind		
🚧 Traffic Manager	Basic Config							
Parental Controls	Enable static routes	Enable static routes • Yes • No						
at USB Application	Static Route List (Max Li	mit : 32)			_			
COD Application	Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete		
Advanced Settings					LAN	Ð		
察 Wireless	No data in table.							
			Apply					
💮 wan								

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 Setup	Operation Mode: <u>Wireless</u> rout SSID: ASUS RT-A ASUS RT- Internet Port Connection Trigger	er Firmware Version: <u>3.0.0.4.378.6701</u> B C + AC Virtual Server / Port Forwarding DMS NAT Passthrough
General Retwork Map	WAN - Internet Connection	
A Guest Network	selected from the dropdown menu	nnection types to WAN (wide area network). These types are beside WAN Connection Type. The setting fields differ
Manager	depending on the connection type	
Parental Controls	Configure the Ethernet WAN settin	gs of RT-AC59U V2.
distantion	Basic Config	
	WAN Connection Type	Automatic IP v
Advanced Settings	Enable WAN	© Yes ● No
🛜 Wireless	Enable NAT	© Yes ● No
🟠 LAN	Enable UPnP UPnP FAQ	© Yes ● No
💮 WAN	WAN DNS Setting	
IPv6	Connect to DNS Server automatically	o Yes ●No
T Firewall	Account Settings	
	Authentication	None
Administration	Special Requirement from IS	D
📝 System Log	Host Name	
Network Tools	MAC Address	00:0C:43:E1:76:28 MAC Clone
	DHCP query frequency	Aggressive Mode
	Extend the 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 fixed IP. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.

- Enable WAN: Select Yes to allow the router Internet access. Select No to disable Internet access.
- Enable NAT: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- Enable UPnP: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- Connect to DNS Server: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- Host Name: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.

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

4.3.2 Port Trigger

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

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

Quick Internet	Operation Mode: Wireless SSID: ASUS RT-AC ASU Internet Connection Por	IS RT-AC	are Version: <u>3.0.0.</u> Jal Server / Port For		DDNS	NAT Passthrou	¢+ ⊡ &		
General	WAN - Port Trigger	mporarily open d	lata ports when LAN	devices require u	nrestricted	access to the Ir	stemet. There are		
Guest Network	two methods for opening inc the time and devices must a access to the trigger port. U	use static IP add	resses. Port trigger	only opens the inc	oming port	when a LAN de	vice requests		
Traffic Manager Parental Controls	forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port. Port. Trigger. FAQ								
USB Application	Basic Config Enable Port Trigger	_	• Yes • No	_					
Advanced Settings	Well-Known Applications			•					
🛜 Wireless	Trigger Port List (Max L	imit : 32)	_	_		_			
🔂 LAN	Description	Trigger P	ort Protoco TCP		ig Port	Protocol	Add / Delete		
💮 wan		TCP TCP TCP U							
🚳 ІРV6			Арг	ly					

To set up Port Trigger:

- 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.

	rick Internet tup	Operation Mode: Wir- SSID: ASUS RT-AC			Version: 3.0.0.4.	.378_6	5701			<mark>9</mark> 8 ⊡ +
- Se		Internet Connection	Port Trigger	Virtual Se	rver / Port Forwar	ding	DMZ	DDNS	NAT Pas	sthrough
	General									
品 Ne	twork Map	WAN - Virtual Serv	er / Port For	warding						
🔉 Gu	iest Network	Virtual Server / Port forv area network (LAN). Fo	r a faster connec	tion, some f	P2P applications (su	ich as	BitTorre	nt), may a	Ilso require	that you set the
🚧 ти	affic Manager		port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.							
	rental ntrols	If you want to specify a 1 10200:10300), the LAN				er the S	Service 1	lame, the	Port Rang	e (e.g.
🔹 us	B Application	When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with RT-ACS9U V2's web user interface.								
Adva	nced Settings	 When you set 20:21 as RT-AC59U V2's native 		er's port rang	ge for your WAN set	up, the	en your F	TP serve	r would be	in conflict with
🛜 Wi	ireless	Virtual Server / P		ng FAQ						
្រុំ 🖬	N	Basic Config	_							
() w	A M	Enable Port Forwardin	g	• Yes	O No					
	20.1	Famous Server List			e select					
💮 IP	V6	Famous Game List				•				
🔽 Fir	rewall	FTP Server Port		2021						
🚨 🗚	ministration	Port Forwarding Li	st (Max Limit	: 32)	_		_		_	
📝 Sy	stem Log	Service Name	Po	rt Range	Local IP	•	Local		Protocol	Add / Delete
2 Ne	twork Tools			,	lo data in table	-				
					Apply	Ŋ.				

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 Internet Setup	Operation Mode: <u>Wireless</u> ro SSID: <u>ASUS_RT-AC</u> <u>ASUS_R</u> Internet Connection Port Trig		DDNS NAT Passthrough				
General	WAN - DDNS						
🔏 Guest Network		system) is a service that allows network clients to cor ugh its registered domain name. The wireless router					
🔆 Traffic Manager	service and other DDNS services If you cannot use ASUS DDNS se	rvices, please go to <u>http://iplookup.asus.com</u> ,	/nslookup.php to reach your internet				
Parental Controls	IP address to use this service. The wireless router currently uses a private WAN IP address,						
K USB Application	This router may be in the multiple	NAT environment and DDNS service cannot work in	n this environment.				
	Enable the DDNS Client	O Yes O No					
Advanced Settings	Server	WWW. ASUS. COM					
0	Host Name	RT-AC59U V2	.asuscomm.com				
🔂 LAN		Apply					
💮 wan							

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:

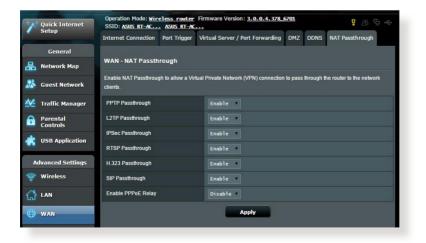
DDNS service will not work under these conditions:

- 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**.



4.4 IPv6

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

***	Quick Internet Setup	Operation Mode: <u>Wireless routor</u> Firmware Version: <u>3.0.0.4.378 6701</u> SSID: <u>ASIS RT-AC</u> ASIS RT-AC			
	General	IDuć			
品	Network Map	IPv6			
*	Guest Network	Configure the IPv6 Internet setting of RT-AC59U V2. IPv6 FAQ			
₩.	Manager Basic Config				
•	Parental Controls	Connection type	Disable		
		Auto Configuration Setting			
	USB Application	Enable Router Advertisement	Enable 🔻		
Advanced Settings Ap			Apply		
00)	Wireless				
	LAN				
٢	WAN				
	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 VPN Server

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

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

/6	545	Logout Reboo		English 🔻		
/	Quick Internet Setup		mware Version: SSID: <u>ASUS ASUS SG</u>	8648		
-	General	VPN Server VPN Details				
品	Network Map	VPN Server - Basic Config	VPN Server - Basic Config The VPN server allows you to access your home network anytime, anywhere. To use the VPN server. Plasse follow these steps.			
*	Guest Network	To use the VPN server. Please follow these s				
<u>*</u>	Traffic Manager	(1) Enable the PPTP VPN server (2) Set the IP pool for client IP. (Maximum 10 clients) (3) Set up the userame and password for VPN client.				
ß	Parental control	(d) Open the VFN connection program on your computer or smartphone. (e) Add a new FFTP VFN connection and the VFN server address is 0.0.0.0 (f) fly our VML in address is dynamic, <u>please click here to set the DDMS</u> . (f) <u>vpN Server FAQ</u>				
*	USB application					
\$	AiCloud	Basic Config				
_		Enable PPTP Server	● Yes O No			
A	dvanced Settings	Network Place (Samba) Support	● Yes O No			
	Wireless	Username and Password				
	LAN	User Name	Password	Add / Delete		
A				Ð		
Ð	WAN	No data in table.				
۲	IPv6	Αρρίγ				
×	VPN Server					

To set up access to a VPN server:

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

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

4.6 Firewall

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

NOTE: The Firewall feature is enabled by default.

4.6.1 General

To set up basic Firewall settings:

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

4.6.2 URL Filter

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

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

To set up a URL filter:

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

4.6.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

78	545	Logout Reboot	English 🔻		
+,+	Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>AS</u>	us Asus_sg 🔉 🖓 🔁 🚓 🖻		
	Setup	General URL Filter Keyword Filter Network Services Filter			
	General				
品	Network Map	Firewall - Keyword Filter Keyword Filter access to webpages containing the specified keywords. Limitations of the keyword filtering function :			
*	Guest Network				
<u> </u>	Traffic Manager	 Compressed webpages that use HTTP compression technology cannot be filtered. <u>See: here for more details.</u> Https webpages cannot be filtered. 			
D	Parental control	Basic Config			
e	USB application	Enable Keyword Filter Enabled Disabled			
		Keyword Filter List			
2	AiCloud	Keyword Filter List Add / Delet			
A	dvanced Settings		Ð		
(Î00	Wireless	No data in table.			
ដ	LAN				

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.

4.6.4 Network Services Filter

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



To set up a Network Service filter:

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

4.7 Administration

4.7.1 Operation Mode

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

/15U5	Logout Reboot English 🔻			
Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>ASUS ASUS -SG</u> <u>B</u> C C			
	Operation Mode System Firmware Upgrade Restore/Save/Upload Setting			
General				
Hetwork Map	Administration - Operation Mode			
Suest Network	Router supports several operation modes to meet different requirements. Please select the mode that match your situation.			
Manager	© Wireless router mode (Default) ● Access Point(AP) mode ● Media bridge			
Parental control	In wrekes rouker IP sharing mode, Router connects to the internet via PPPE, CHCP, PPTP, L2TP, or State, PF and shares the wrekess networks LNA idented or docks: In his mode, Hz (Freend), and DKCP sown are enabled by dockall. UTPP and Dynamic DKS are supported for SCHO and home users. Select this mode if you are a first-time user or you are not currently using any wiredwritelss routers.			
USB application				
AiCloud				
Advanced Settings				
🛜 Wireless	(III)			
🔂 LAN				
💮 wan				
IPv6	Save			

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.
 - **Media Bridge**: This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via ethernet.
 - Access Point mode: In this mode, the router creates a new wireless network on an exising network.
- 3. Click Apply.

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

4.7.2 System

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

To set up the System settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
- 2. You can configure the following settings:
 - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
 - **WPS button behavior**: The physical WPS button on the wireless router can be used to activate WPS.
 - **Time Zone**: Select the time zone for your network.
 - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
 - Enable Telnet: Click Yes to enable Telnet services on the network. Click No to disable Telnet.
 - Authentication Method: You can select HTTP, HTTPS, or both protocols to secure router access.
 - Enable Web Access from WAN: Select Yes to allow devices outside the network to access the wireless router GUI settings. Select No to prevent access.
 - **Only allow specific IP**: Click **Yes** if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
 - **Client List**: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked **Yes** in the **Only allow specific IP** item.
- 3. Click Apply.

4.7.3 Firmware Upgrade

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

To upgrade the firmware:

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

NOTES:

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

4.7.4 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

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

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

4.8 System Log

System Log contains your recorded network activities.

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

To view your system log:

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

ISUS	Logout	eboot English y		
+ Quick Internet Setup	Operation Mode: <u>Wireless router</u> General Log DHCP leases Wirel	Firmware Version: SSID: <u>ASUS_ASUS_SG</u> <u>&</u> <u>-</u>		
General				
Network Map		System Log - General Log		
Guest Network	This page shows the detailed system's a System Time	sat, Jan 01 00:49:51 2011		
Traffic Manager	Uptime	0 days 0 hours 49 minutes 50 seconds		
Parental control		adcom BCM4331 802.11 Wireless Controller 6.30.102.9 (r366174) adcom BCM4360 802.11 Wireless Controller 6.30.102.9 (r366174) h1 entered promiscuous mode		
USB application	Jan 1 00:31:27 kernel: wlc_phy_co Jan 1 00:31:27 kernel: br0: port	Jan 1 00:31:27 kernel: br0: port 2(eth1) entering listening state Jan 1 00:31:27 kernel: wlc_phy_cal_init_acphy: NOT Implemented		
AiCloud	Jan 1 00:31:27 kernel: br0: port Jan 1 00:31:27 kernel: device et Jan 1 00:31:27 kernel: br0: port			
Advanced Settings	Jan 1 00:31:27 kernel: br0: port Jan 1 00:31:27 kernel: device vil Jan 1 00:31:27 kernel: br0: port Jan 1 00:31:27 kernel: br0: topo:	0.1 entered promiscuous mode 4(w10.1) entering listening state		
Wireless	Jan 1 00:31:27 kernel: br0: port Jan 1 00:31:27 kernel: br0: port	3(eth2) entering forwarding state		
} LAN	Jan 1 00:31:39 dnsmasg-dhcp[510] Jan 1 00:31:39 dnsmasg-dhcp[510]	Jan 1 00:31:27 kernel: br0: port 4(w10.1) entering forwarding state Jan 1 00:31:39 dnsmasq-dhcp[510]: DHCPREQUEST(br0) 192.168.1.60 c4:6a:b7:89:8f:97		
WAN	Jan 1 00:32:12 dnsmasq-dhcp(510) Jan 1 00:33:08 dnsmasq-dhcp(510)			
IPv6	Jan 1 00:33:34 dnsmasq-dhep(510)			
VPN Server		III >		
Firewall				

5 Utilities

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
 - Device Discovery v2.0.0.0 at <u>https://www.asus.com/support/</u> <u>download-center</u>
 - Firmware Restoration v1.9.0.4 at <u>https://www.asus.com/</u> <u>support/download-center</u>

5.1 Device Discovery

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

To launch the Device Discovery utility:

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

/isus			TN	-×
Device	SSID	IP Address	Subnet Mask	Printer
RT-AC59U V2	ASUS	192.168.1.1	255.255.255.0	Ì
	<u>C</u> onfig	ure	<u>S</u> earch	<u>E</u> xit
Number of devices found: 1				

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

5.2 Firmware Restoration

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

Firmware Resto	ration	×
<u>F</u> ilename:		<u>B</u> rowse
Status		
After locating	the 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.

To launch the rescue mode and use the Firmware Restoration utility:

- 1. Unplug the wireless router from the power source.
- 2. Hold the Reset button at the rear panel and simultaneously replug the wireless router into the power source. Release the Reset button when the Power LED at the front panel flashes slowly, which indicates that the wireless router is in the rescue mode.

3. Set a static IP on your computer and use the following to set up your TCP/IP settings:

IP address: 192.168.1.x

Subnet mask: 255.255.255.0

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

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

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:

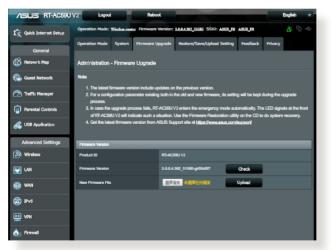
<u>https://www.asus.com/support</u> for more product information and contact details of ASUS Technical Support.

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.



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

Restart your network in the following sequence:

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

Check if your Ethernet cables are plugged properly.

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

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

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

Check if your network settings are correct.

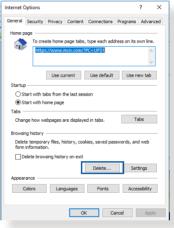
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network. Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You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



6.2 Frequently Asked Questions (FAQs)

I cannot access the router GUI using a web browser

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



NOTES:

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

The client cannot establish a wireless connection with the router.

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

- Out of Range:
 - Move the router closer to the wireless client.
 - Try to adjust antennas of the router to the best direction as described in section **1.4 Positioning your 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.



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

Quick Internet	Operation Mode: Wireless router Fir SSID: ASIS RT-AC ASUS RT-AC	
seup	General WPS Wireless MAC Filter	RADIUS Setting Professional
General		
H Network Map	Wireless - General	
😹 Guest Network	Set up the wireless related information belo	yw.
44	Band	SGHz
Manager	SSID	ASUS RT-AC59U_V2_5G
Parental Controls	Hide SSID	• Yes O No
🚓 USB Application	Wireless Mode	Auto
	Channel bandwidth	20/40/80 MHz
Advanced Settings	Control Channel	Auto *
💎 Wireless	Extension Channel	Auto
	Authentication Method	WPA2-Personal
🜐 WAN	WPA Encryption	AES =
🚳 IPv6	WPA Pre-Shared Key	44332211
Firewall	Network Key Rotation Interval	3600
V		Apply
Administration		

- 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.

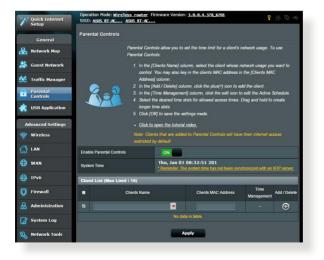
ASUS RT-AC59U	V2 Logout Rebo	ot English *
😥 Quick Internet Setup	Operation Mode: Wiedow.restor Firmware	Version: 144.432_5556 SSID: ASI3_F8 ASI3_F8 ASI3_F8
General	Operation Mode System Firmware U	Jpgrade Restore/Save/Upload Setting Feedback Privacy
🛞 Network Map	Administration - Restore/Save/Uplo	ad Setting
Guest Network	This function allows you to save current set	ings of RT-AC59UV2 to a file, or load settings from a file.
Traffic Hanager	Factory default	Restore
Parental Controls	Save setting	Save setting Citick on this checkbox if you want to share the config life for debugging. Since the original
🚲 USB Application		password in the config file will be removed, please do not import the file into your muter.
Advanced Settings	Restore setting	Upload
Mireless		
👿 LAN		
I WAN		
arv6		
👥 VAN		
🚵 Freval		
Reference Administration		

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.

How to restore the system to its default settings?

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

The following are the factory default settings:

- User Name: admin
- **Password:** admin
- Enable DHCP: Yes (if WAN cable is plugged in)
- IP address: 192.168.1.1
- **Domain Name:** (Blank)
- Subnet Mask: 255.255.255.0
- DNS Server 1: 192.168.50.1
- DNS Server 2: (Blank)
- SSID (2.4GHz) and SSID (5GHz) settings:

• For USA and Canada:

• 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

• For other regions:

- SSID (2.4GHz): ASUS
- SSID (5GHz): ASUS_5G

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".

Firmware upgrade failed.

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

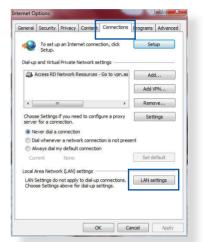
Cannot access Web GUI

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

A. Disable the proxy server, if enabled.

Windows®

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



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

	nay override manual settings. To ensure the isable automatic configuration.
Automatically detect se	ettings
Use automatic configur	iration script
Address	
roxy server Use a proxy server for dial-up or VPN connect	r your LAN (These settings will not apply to tions).
Address:	Port: 80 Advanced
Bypass proxy serve	ver for local addresses

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.

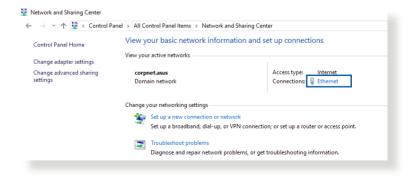
	Locat	ion: Automat	ic	;	
	Sh	ow: Built-in I	Ethernet	;	
_	TCP/IP	PPPoE Apr	leTalk Proxies	Ethernet	
Sele	ct a proxy server to	configure:	FTP Proxy S	erver	
	FTP Proxy		1		
_ ⊻	Web Proxy (HTTP) Secure Web Proxy (F		🗌 Proxy sei	ver requires pa	ssword
	Streaming Proxy (R1		6	et Password	
	SOCKS Proxy	517		et rassword	
Ä	Gopher Proxy		4 +		
Byp	ass proxy settings f	or			
	e Hosts & Domains				
V	Ise Passive FTP Mod	le (PASV)			(?)
					0

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

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

Windows®

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



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

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

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

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

5. Click **OK** when done.

General Connection IP-4 Connectivity: Internet IP-4 Connectivity: No network access Media State: Enabled Duration: 03:29:31 Speed: 1.0 Gbps Details Received Bytes: 71,424,646 Bytes: 71,424,646 Properties Disable Disable: Diagnose Ethernet Properties Disable Vetworking Automatication Connect using: Internet Properties Image: Internet Properties Vetworking Automatication Configure Configure This connection uses the following tems: Internet Protocol Version 4 (TCP/IPV6) Image: Internet Protocol Version 5 (TCP/IPV6) Internet Protocol Version 6 (TCP/IPV6) Image: Internet Protocol Version 6 (TCP/IPV6) Internet Protocol Version 7 (TCP/IPV6) Image: Internet Protocol Version 6 (TCP/IPV6) Internet Protocol Version 7 (TCP/IPV6) Image: Internet Protocol Version 4 (TCP/IPV6) Internet Protocol Version 7 (TCP/IPV6) Image: Internate Confi	Х
IPv4 Connectivity: Internet IPv6 Connectivity: No network access Media State: Enabled Duration: 03:29:31 Speed: 1.0 Gbps Details Details Activity	
BV4 Connectivity: Internet IPv6 Connectivity: No network access Media State: Enabled Duration: 03:29:31 Speed: 1.0 Gbps Details Details Activity	
IPv6 Connectivity: No network access Media State: Enabled Duration: 03:29:31 Specif: 1.0 Gbps Details Received Activity Sent — Properties Bytes: 71,424,646 Bytes: 71,424,646 Disable Dagnose Ethernet Properties Disable Dagnose Configure Connect using: Intel(R) Ethernet Connection (2) (219-V) Configure Configure This connection uses the following items: Intel(R) Ethernet Context of (2) (219-V) Configure Configure This connection uses the following items: Intel(R) Ethernet Context of (CP/IPV6) Intel Unital Properties	
Media State: Enabled Duration: 03:29:31 Speed: 1.0 Gbps Details Activity Sent Received Bytes: 71,424,646 70,727,241 Properties Disable Diagnose Ethernet Properties Disable Diagnose Install Configure Transmission Control Protocol Version 4 (TCP/IPV4) Meroach LLDP Protocol Oner Install Unstall Meroach LLDP Protocol/Internet Protocol Install Unstall Properties Description Transmission Control Protocol/Internet Protocol Install Use the following IP address:	
Duration: 03:29:31 Speed: 1.0 Gbps Details 1.0 Gbps Details Sent Activity	
Speed: 1.0 Gbps Details 1.0 Gbps Activity Sent — Received Bytes: 71,424,646 70,727,241 Image: Sent — Received Bytes: 71,424,646 70,727,241 Image: Sent — Sent — Received Bytes: 71,424,646 70,727,241 Image: Sent — Sent — Received Bytes: 71,424,646 70,727,241 Image: Sent — Sent & Sent	
Details Activity Sent Received Bytes: 71,424,646 70,727,241 Image: Sent Diagnose Ethernet Properties Diagnose Ethernet Properties Diagnose Ethernet Properties Diagnose Ethernet Properties Configure Configure Configure This connection uses the following items: Image: Configure Image: Protocol Version (CD/IP/4) Configure Image: Protocol Version (CD/IP/4) Image: Protocol Version (CD/IP/4) Image: Protocol Version (CD/IP/4) Properties Description Transmission Control Protocol/Internet Protocol Transmission Control Protocol/Internet Protocol Image: Protocol Version 4(CD/IP/4) Use and the following TP address:	
Activity	
Sent Received Bytes: 71,424,64 70,727,241 Image: Image	
Sent Received Bytes: 71,424,64 70,727,241 Image: Image	
Bytes: 71,424,646 70,727,241 Properties Plasable Dagnose Ethernet Properties Plasable Dagnose Ethernet Properties Plasable Dagnose Ethernet Properties Configure Configure Connect using: Intel(R) Ethemet Connection (2) 1219-V Configure This connection uses the following items: Orols Packet Scheduler Configure Intel (R) Ethemet Contocol Driver On Version (TCP/IPVI) Microsoft Ltervok Adapter Multipacer Frotocol Properties Intel	
Properties Diagnose Ethermet Properties Ethermet Properties etworking Authentication Connect using: Image: The (R) Ethermet Connection (2) (219-V Configure This connection uses the following items: Configure Image: The (R) Ethermet Connection (2) (219-V Configure This connection uses the following items: Configure Image: Construction Report Protocol Version 4 (TCP/IPV6) Marcasch LUP Protocol Driver Image: Construction Report Protocol Version 5 (TCP/IPV6) Properties Description Transmission Control Protocol/Intermet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Transmission Control Protocol/Intermet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Obtam an IP address automatically Use the following IP address: Use the following DN server addresses: O Obtam DNS server addressesutomatically	
Ethernet Properties Ethernet Properties Ethorized as a set of the appropriate process of the appropri	
etworking Authentication Connect using: Intel(R) Ethemet Connection (2) (219-V Configure This connection uses the following items: Consection textures Adapter Microard (TCP/IPv6) Microard LDP Protocol Uversion 4 (TCP/IPv6) Link-Layer Topology Discovery Mapper I/O Driver Discrete Alternate Configuration You can get IP setting: Discrete Protocol Version 4 (TCP/IPv4) Properties Def aud gateway: Def aud gateway: Discrete following DNS server addresses: Preferred DNS server: Alternate DNS server: Discrete DNS serve	
etworking Authentication Connect using: Intel(R) Ethemet Connection (2) (219-V Configure This connection uses the following items: Consection textures Adapter Microard (TCP/IPv6) Microard LDP Protocol Uversion 4 (TCP/IPv6) Link-Layer Topology Discovery Mapper I/O Driver Discrete Alternate Configuration You can get IP setting: Discrete Protocol Version 4 (TCP/IPv4) Properties Def aud gateway: Def aud gateway: Discrete following DNS server addresses: Preferred DNS server: Alternate DNS server: Discrete DNS serve	
Connect using: Intel(R) Ethemet Connection (2) /219-V Configure This connection uses the following items: Configure Con	×
Intel(R) Ethemet Connection (2) (219-V Configure This connection uses the following items: Microsoft LLDP Protocol Driver Link-Layer Topology Discovery Responder Link-Layer Topology Discovery Respond	
Configure This connection uses the following items: Configure This connection uses the following items: Configure Configure.	
This connection uses the following items:	
This connection uses the following items:	
Ocs Packet Scheduler Construction Constructi	
Install Uninitial Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Install Alternate Configuration You can get P settings assigned automatically if your network administrator for the appropriate IP settings. Otherwise, you need to ask your network administrator for the appropriate IP settings. Outer the following IP address: I address: Sobnet mask: Default gateway: Outer the following DNS server addresses: Preferred DNS server: Atternate DNS server:	
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Iternet Protocol Version 4 (TCP/IPv4) Properties General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Ouse the following IP address: UP	
Transmission Cortol Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
wide area network proceed that provides communication across diverse interconnected networks. termet Protocol Version 4 (TCP/IPv4) Properties Serveral Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP setting. Obtain an IP address automatically Outse the following IP address: IP address: Subnet mask: Def out gateway: Outse the following DNS server addresses: Preferred DNS server: Alternate DNS server: Alternate DNS server:	
across diverse interconnected networks.	
ternet Protocol Version 4 (TCP/IPv4) Properties Seneral Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Obtam an IP address automatically Use the following IP address: I address Subnet mask: Def out gateway: Obtam DNS server address automatically Outse the following DNS server addresses: Preferred DNS server: Atemate DNS server: Atemate DNS server: Atemate DNS server	
General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support of	
General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, your need to ask your network administrator for the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support of the appropriate IP settings. Image: Configuration of the support o	
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrators for the appropriate IP settings.	×
this capability. Otherwise, you need to ask your network administrator for the appropriate P settings. O Use the following IP address: P address: UP address: Def ault gateway: O Use the following DNS server addresses: Preferred DNS server: Akemate DNS server:	
O Use the following IP address: IP address: Subnet mask: Def ault gateway: O Use the following DNS server address automatically O Use the following DNS server addresses: Preferred DNS server: Alternate DNS server:	
O Use the following IP address: IP address: Subnet mask: Def ault gateway: O Use the following DNS server address automatically O Use the following DNS server addresses: Preferred DNS server: Alternate DNS server:	
Subnet mask: Default gateway: Obtain DNS server address automatically Oute the following DNS server: Preferred DNS server: Alternate DNS server:	
Obtault gateway: Obtault gateway: Obtaut DNS server address automatically Ouse the following DNS server: Preferred DNS server: Alternate DNS server:	
Obtain DNS server address automatically Use the following DNS server: Preferred DNS server: Alternate DNS server:	
OUse the following DNS server addresses: Preferred DNS server: Alternate DNS server:	
OUse the following DNS server addresses: Preferred DNS server: Alternate DNS server:	
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit Advanced	
OK Cancel	

MAC OS

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

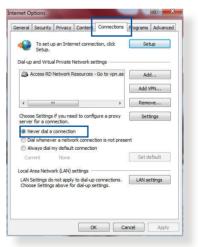
	Location: Automatic	:
	Show: Built-in Ethernet	;
	TCP/IP PPPoE AppleTalk Prox	cies Ethernet
Configura	IPv4: Using DHCP	
IP Add	ress: 192.168.182.103	Renew DHCP Lease
Subnet M	Mask: 255.255.255.0 DHCP Cl	
Ro	uter: 192.168.182.250	(If required)
DNS Ser	vers: 192.168.128.10	(Optional)
Search Dom	ains:	(Optional)
	ress: fe80:0000:0000:0000:0211:24f	f:fe32:b18e
IPv6 Add	1635. 1680.0000.0000.0000.0211.241	

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.

Industry Canada statement:

This device complies with RSS-247 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution:

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- (iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz

sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

- (ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- (iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

NCC 警語

低功率射頻器材技術規範

「取得審驗證明之低功率射頻器材,非經核准,公司、商號或使用者 均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率 射頻器材之使用不得影響飛航安全及干擾合法通信;經發現有干擾 現象時,應立即停用,並改善至無干擾時方得繼續使用。前述合法通 信,指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受 合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。」

*應避免影響附近雷達系統之操作。

電磁波曝露量 MPE 標準值 1mWcm²,送測產品實測值為: 0.409 mWcm²。

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. We include a copy of the GPL with every CD shipped with our product. 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

ASUS Contact information

ASUSTeK COMPUTER INC.

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