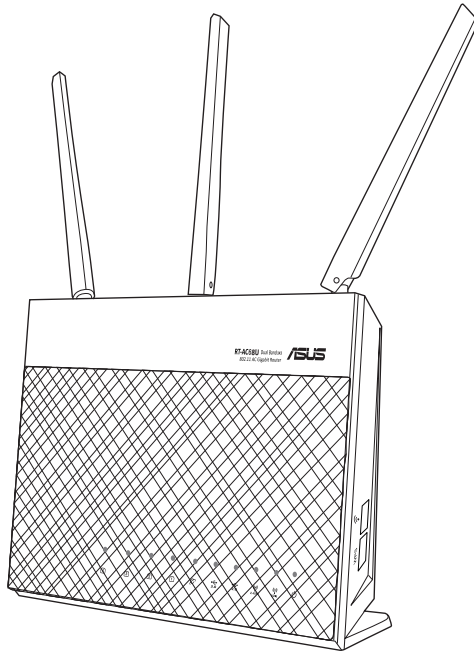


User Guide

RT-AC68U Dual Band

3x3 Wireless-AC 1900 Gigabit Router



ASUS[®]
IN SEARCH OF INCREDIBLE

E16205

Revised Edition V7

December 2019

Copyright © 2019 ASUSTeK Computer Inc. All Rights Reserved.

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

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

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

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

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

Table of contents

1	Getting to know your wireless router	6
1.1	Welcome!	6
1.2	Package contents	6
1.3	Your wireless router	7
1.4	Positioning your router	9
1.5	Setup Requirements	10
1.6	Router Setup	11
	1.6.1 Wired connection	11
	1.6.2 Wireless connection	12
2	Getting started	14
2.1	Logging into the Web GUI	14
2.2	Quick Internet Setup (QIS) with Auto-detection	15
2.3	Connecting to your wireless network	19
3	Configuring the General settings	20
3.1	Using the Network Map	20
	3.1.1 Setting up the wireless security settings	21
	3.1.2 Managing your network clients	22
	3.1.3 Monitoring your USB device	23
3.2	Creating a Guest Network	26
3.3	Using the Traffic Manager	28
	3.3.1 Managing QoS (Quality of Service) Bandwidth	28
	3.3.2 Monitoring Traffic	31
3.4	Setting up Parental Control	32
3.5	Using the USB Application	33
	3.5.1 Using AiDisk	33
	3.5.2 Using Servers Center	35
	3.5.3 3G/4G	41

Table of contents

3.6	Using AiCloud 2.0.....	43
3.6.1	Cloud Disk.....	44
3.6.2	Smart Access.....	46
3.6.3	AiCloud Sync.....	47
4	Configuring the Advanced Settings	48
4.1	Wireless.....	48
4.1.1	General.....	48
4.1.2	WPS	51
4.1.3	Bridge	53
4.1.4	Wireless MAC Filter	55
4.1.5	RADIUS Setting	56
4.1.6	Professional	57
4.2	LAN.....	59
4.2.1	LAN IP	59
4.2.2	DHCP Server.....	60
4.2.3	Route	62
4.2.4	IPTV	63
4.3	WAN	64
4.3.1	Internet Connection.....	64
4.3.2	Port Trigger.....	67
4.3.3	Virtual Server/Port Forwarding	69
4.3.4	DMZ.....	72
4.3.5	DDNS	73
4.3.6	NAT Passthrough	74
4.4	IPv6.....	75
4.5	VPN Server	76
4.6	Firewall.....	77
4.6.1	General.....	77
4.6.2	URL Filter	77
4.6.3	Keyword filter	78

Table of contents

4.6.4	Network Services Filter	79
4.7	Administration	81
4.7.1	Operation Mode	81
4.7.2	System.....	82
4.7.3	Firmware Upgrade	83
4.7.4	Restore/Save/Upload Setting	83
4.8	System Log	84
5	Utilities	85
5.1	Device Discovery	85
5.2	Firmware Restoration	86
5.3	Setting up your printer server	87
5.3.1	ASUS EZ Printer Sharing	87
5.3.2	Using LPR to Share Printer	91
5.4	Download Master.....	96
5.4.1	Configuring Bit Torrent download settings	97
5.4.2	NZB settings.....	98
6	Troubleshooting	99
6.1	Basic Troubleshooting	99
6.2	Frequently Asked Questions (FAQs)	102
	Appendices	112
	Notices	112
	ASUS Contact information	126
	Networks Global Hotline Information.....	127

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS RT-AC68U Wireless Router!

The ultra-thin and stylish RT-AC68U features a 2.4GHz and 5GHz dual bands for an unmatched concurrent wireless HD streaming; SMB server, UPnP AV server, and FTP server for 24/7 file sharing; a capability to handle 300,000 sessions; and the ASUS Green Network Technology, which provides up to 70% power-saving solution.

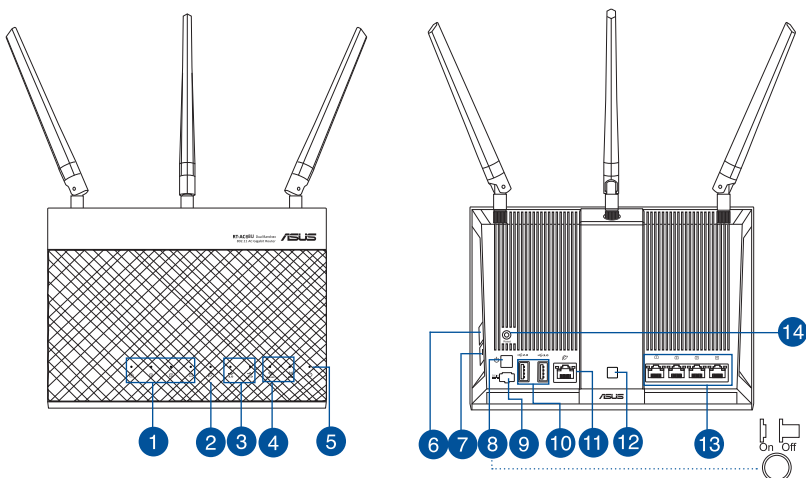
1.2 Package contents

- | | |
|--|---|
| ☒ RT-AC68U Wireless Router | ☒ Network cable (RJ-45) |
| ☒ Power adapter | ☒ Quick Start Guide |
| ☒ Support CD (Manual) | |

NOTES:

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

1.3 Your wireless router



-
- 1 LAN 1~4 LED**
Off: No power or no physical connection.
On: Has physical connection to a local area network (LAN).
-
- 2 WAN (Internet) LED**
Off: No power or no physical connection.
On: Has physical connection to a wide area network (WAN).
-
- 3 USB 3.0 / 2.0 LED**
Off: No power or no physical connection.
On: Has physical connection to USB 3.0 / 2.0 devices.
-
- 4 2.4GHz LED / 5GHz LED**
Off: No 2.4GHz or 5GHz signal.
On: Wireless system is ready.
Flashing: Transmitting or receiving data via wireless connection.
-
- 5 Power LED**
Off: No power.
On: Device is ready.
Flashing slow: Rescue mode
Flashing quick: WPS is processing.
-
- 6 WPS button**
This button launches the WPS Wizard.
-

7 Wi-Fi On/Off button

Press this button to turn on /off the Wi-Fi connection.

8 Power button

Press this button to power on or off the system.



9 Power (DC-IN) port

Insert the bundled AC adapter into this port and connect your router to a power source.

10 USB 3.0 / 2.0 ports

Insert USB 3.0 / 2.0 devices such as USB hard disks or USB flash drives into these ports. Insert your iPad's USB cable into one of these ports to charge your iPad.

11 WAN (Internet) port

Connect a network cable into this port to establish WAN connection.

12 LED On/Off button

Press this button to turn on/off the backlight LED on the panel.

13 LAN 1 ~ 4 ports

Connect network cables into these ports to establish LAN connection.

14 Reset button

This button resets or restores the system to its factory default settings.

NOTES:

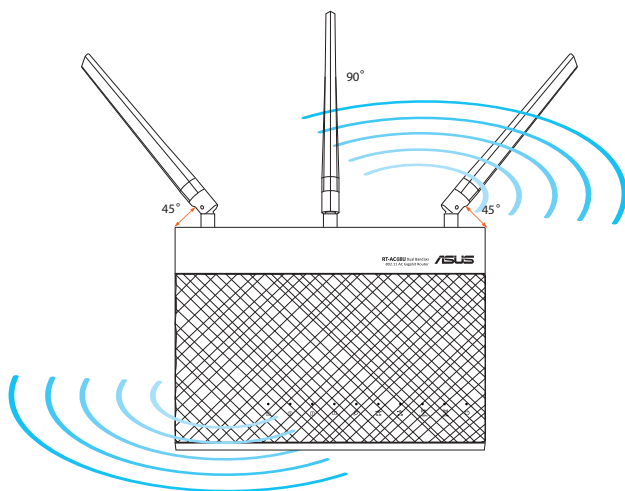
- Use only the adapter that came with your package. Using other adapters may damage the device.
- **Specifications:**

DC Power adapter	DC Output: +19V with max 1.75A current;		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

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

- Place the wireless router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- Keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at <http://www.asus.com> to get the latest firmware updates.
- To ensure the best wireless signal, orient the three detachable antennas as shown in the drawing below.



1.5 Setup Requirements

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

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000BaseTX)
- IEEE 802.11a/b/g/n/ac wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

NOTES:

- If your computer does not have built-in wireless capabilities, you may install an IEEE 802.11a/b/g/n/ac 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.
-

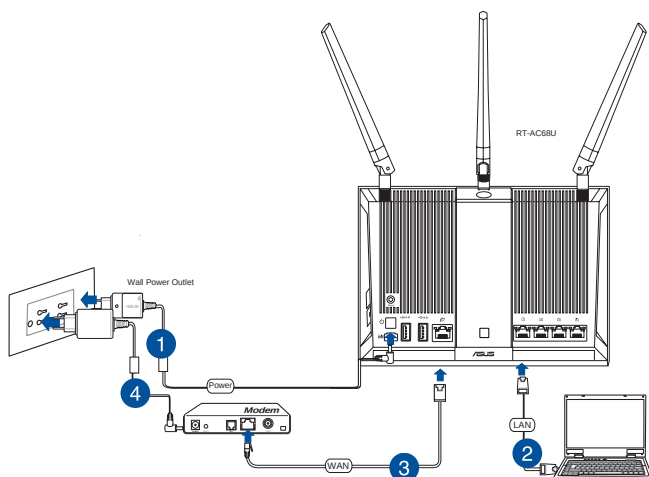
1.6 Router Setup

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:

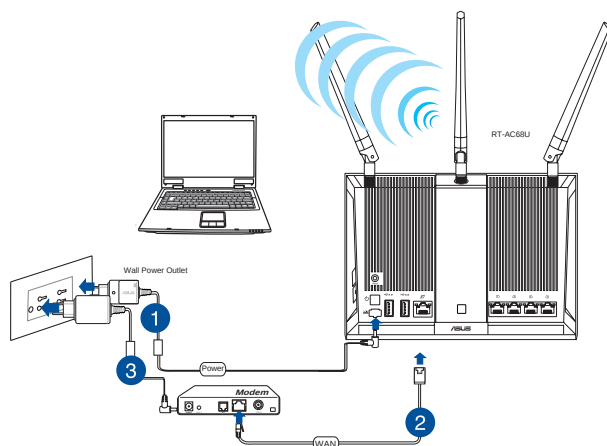
1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.

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.

NOTES:

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

2 Getting started

2.1 Logging into the Web GUI

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

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

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



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

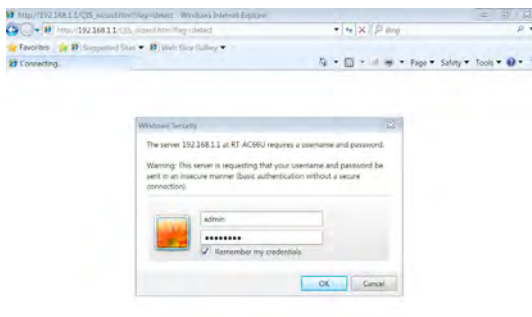
2.2 Quick Internet Setup (QIS) with Auto-detection

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

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

To use QIS with auto-detection:

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



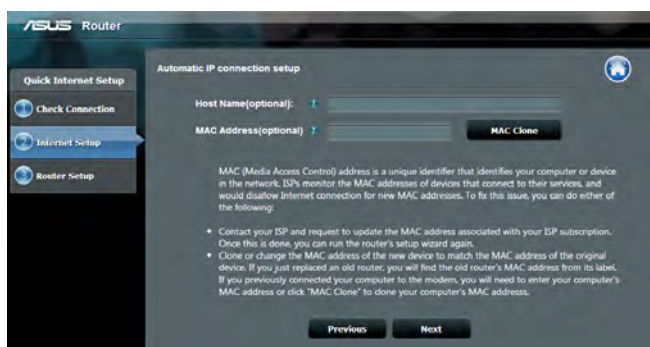
NOTES:

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

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

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

for Automatic IP (DHCP)



for PPPoE, PPTP, and L2TP



for Static IP



The image shows the 'Quick Internet Setup' screen of an ASUS Router. On the left, there is a sidebar with three options: 'Check Connection', 'Internet Setup' (which is highlighted with a blue arrow), and 'Router Setup'. The main area has a title 'Please refer to your ISP setting, and input the related information.' Below this, there are two sections. The first section is 'Use the following IP address:' and contains three input fields: 'IP Address' with the value '0.0.0.0', 'Subnet Mask' with '0.0.0.0', and 'Default Gateway' with '0.0.0.0'. The second section is 'DNS Servers' and contains two input fields: 'DNS Server1' and 'DNS Server2'. Below these is a 'MAC Address(optional)' input field and a 'MAC Clone' button. At the bottom, there are 'Previous' and 'Next' buttons.

NOTES:

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.

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



The image shows the 'Wireless Setting' screen of an ASUS Router. On the left, there is a sidebar with three options: 'Quick Internet Setup', 'Internet Setup', and 'Router Setup' (which is highlighted with a blue arrow). The main area has a title 'Wireless Setting' and a subtitle 'Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.' Below this, there are two sections. The first section is '2.4GHz - Security' and contains two input fields: 'Network Name(SSID)' with the value 'ASUS' and 'Security Key' with '*****'. The second section is '5GHz - Security' and contains two input fields: 'Network Name(SSID)' with the value 'ASUS_5G' and 'Security Key' with '*****'. There is a checkbox labeled 'Copy 2.4GHz to 5GHz settings' which is checked. At the bottom, there is an 'Apply' button.

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



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

NOTES:

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

3 Configuring the General settings

3.1 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

The screenshot shows the 'System Status' window with the '2.4GHz' tab selected. The 'Wireless name(SSID)' field contains 'ASUS'. The 'Authentication Method' dropdown is set to 'Open System'. The 'WEP Encryption' dropdown is set to 'None'. An 'Apply' button is located below these settings. Below the wireless settings, the LAN IP is 192.168.1.1, the PIN code is 72013502, the LAN MAC address is 10:BF:48:D8:49:78, and the Wireless 2.4GHz MAC address is 10:BF:48:D8:49:78.

5GHz security settings

The screenshot shows the 'System Status' window with the '5GHz' tab selected. The 'Wireless name(SSID)' field contains 'ASUS_5G'. The 'Authentication Method' dropdown is set to 'Open System'. The 'WEP Encryption' dropdown is set to 'None'. An 'Apply' button is located below these settings. Below the wireless settings, the LAN IP is 192.168.1.1, the PIN code is 72013502, the LAN MAC address is 10:BF:48:D8:49:78, and the Wireless 5GHz MAC address is 10:BF:48:D8:49:7C.

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

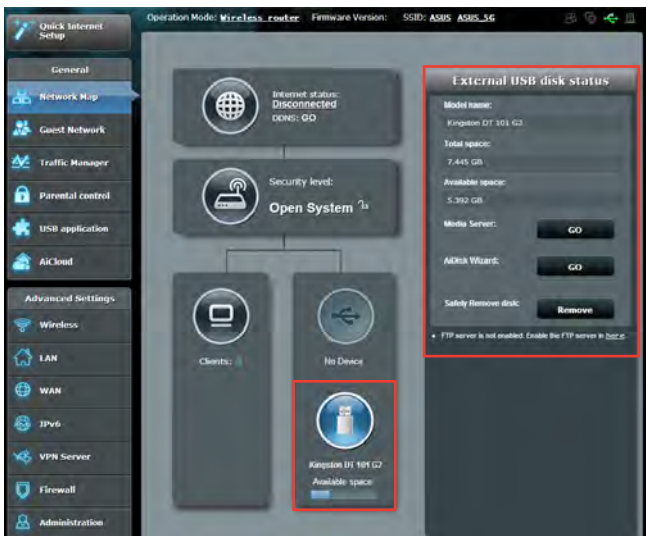


To manage your network clients:

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 two USB ports for connecting USB devices or USB printer to allow you to share files and printer with clients in your network.



NOTES:

- To use this feature, you need to plug a USB storage device, such as a USB hard disk or USB flash drive, to the USB 3.0/2.0 ports on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the Plug-n-Share Disk Support List at <http://event.asus.com/networks/disksupport>
- The USB ports support two USB drives or one printer and one USB drive at the same time.

IMPORTANT! You first need to create a share account and its permission /access rights to allow other network clients to access the USB device via an FTP site/third-party FTP client utility, Servers Center, Samba, or AiCloud. For more details, refer to the section **3.5.Using the USB Application** and **3.6 Using AiCloud** in this user manual.

To monitor your USB device:

1. From the navigation panel, go to **General > Network Map**.
2. On the Network Map screen, select the **USB Disk Status** icon to display your USB device's information.
3. On the AiDisk Wizard field, click **GO** to set up an FTP server for Internet file sharing.

NOTES:

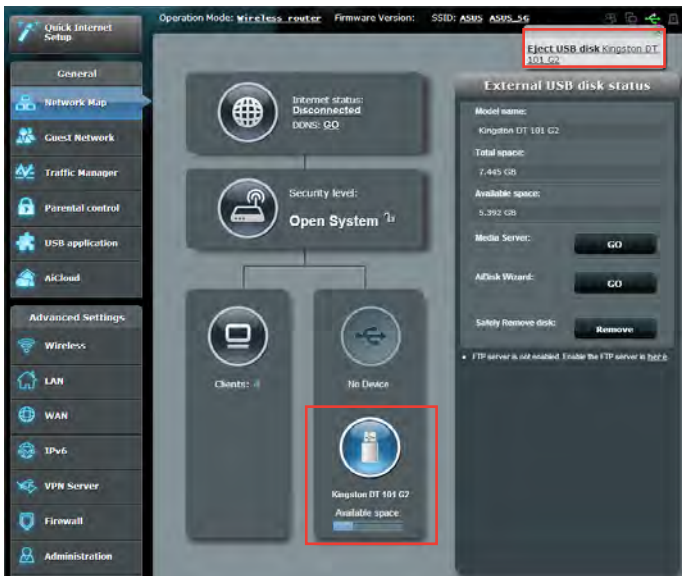
- For more details, refer to the section **3.5.2 Using Servers Center** in this user manual.
 - The wireless router works with most USB HDDs/Flash disks (up to 2TB size) and supports read-write access for FAT16, FAT32, EXT2, EXT3, and NTFS.
-

Safely removing the USB disk

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

To safely remove the USB disk:

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



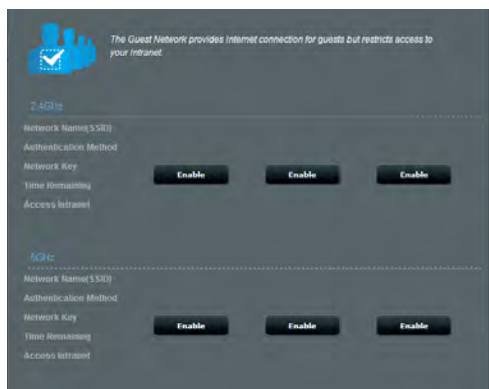
3.2 Creating a Guest Network

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-AC68U 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**.



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

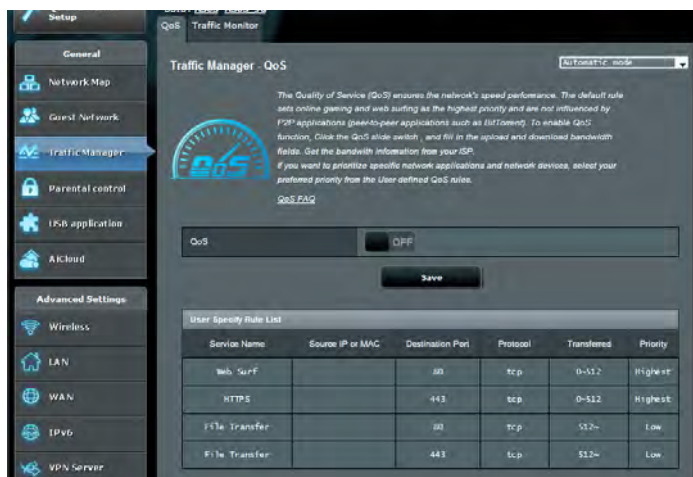
The screenshot shows a 'Guest Network' configuration window. At the top, there is a blue icon of three people and a text box stating: 'The guest network can provide internet connectivity for temporary visitors without accessing your private network.' Below this, there are two sections: '24GHz' and '5GHz'. Each section contains the following fields: 'Network name:' (with values 'ASUS_Guest' and 'ASUS_5G_Guest' respectively), 'Wireless Security:' (both set to 'Open System'), 'Security key:' (both set to 'None'), 'Access Time:' (both set to 'Limitless'), and 'Access Intranet:' (both set to 'off'). Each section also has a 'Modify' button at the bottom and two 'Create' buttons next to the 'Security key:' field.

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.



To set up bandwidth priority:

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

NOTE: Get the bandwidth information from your ISP.

3. Click **Save**.

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

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

NOTES

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

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

NOTES:

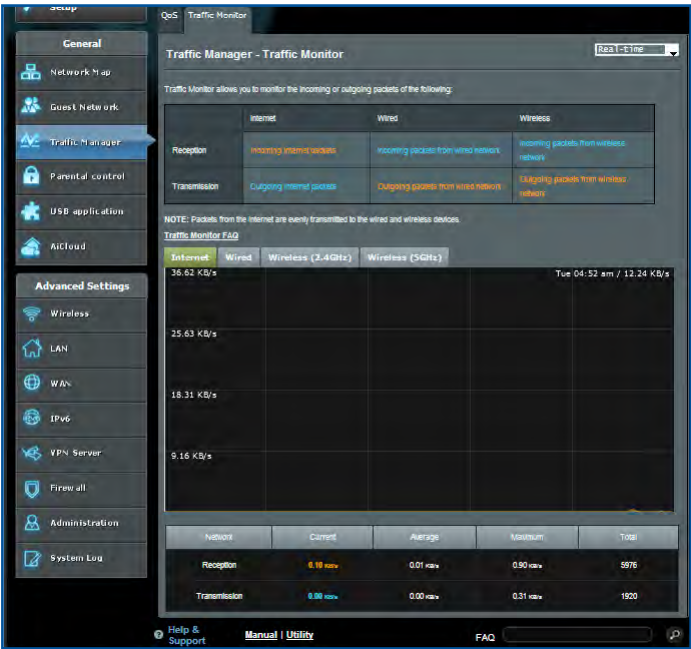
- Low-priority packets are disregarded to ensure the transmission of high-priority packets.
 - Under **Download Bandwidth** table, set **Maximum Bandwidth Limit** for multiple network applications in corresponding order. The higher priority upstream packet will cause the higher priority downstream packet.
 - If there are no packets being sent from high-priority applications, the full transmission rate of the Internet connection is available for low-priority packets.
-

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

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

3.3.2 Monitoring Traffic

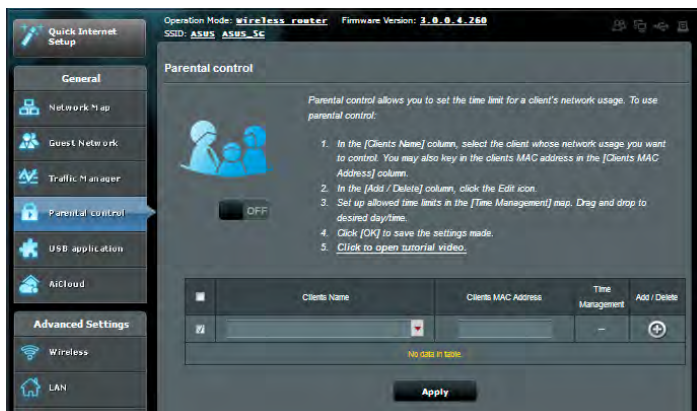
The traffic monitor function allows you to access the bandwidth usage and speed of your Internet, wired, and wireless networks. It allows you to monitor network traffic even on a daily basis.



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.



To use the parental control function:

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

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

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

3.5 Using the USB Application

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

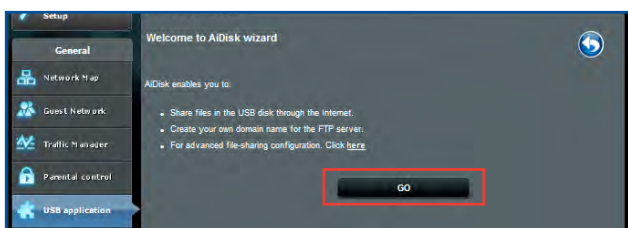
IMPORTANT! To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <http://event.asus.com/2009/networks/disksupport/> for the file system support table.

3.5.1 Using AiDisk

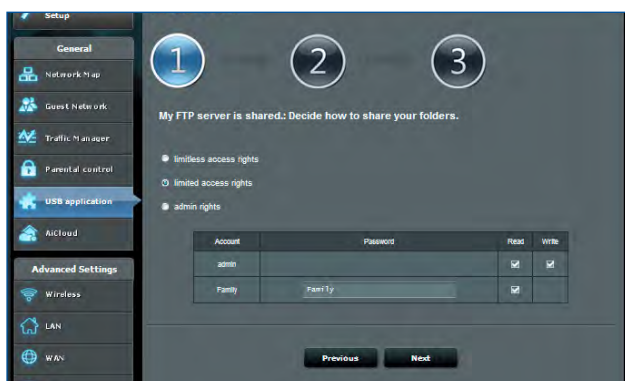
AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

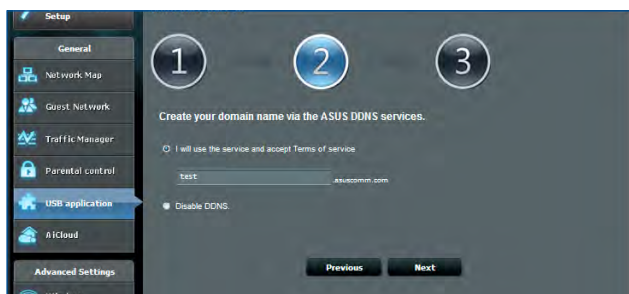
1. From the navigation panel, go to **General > USB application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.



3. Select the access rights that you want to assign to the clients accessing your shared data.



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



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

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

3.5.2 Using Servers Center

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

Using Media Server

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

NOTE: Before using the DLNA Media Server function, connect your device to the RT-AC68U's network.

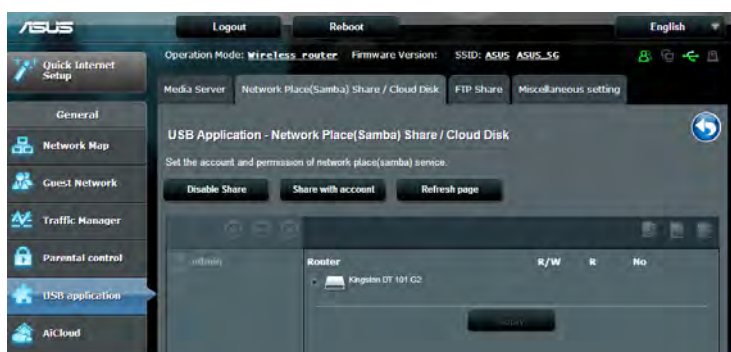


To launch the Media Server setting page, go to **General > USB application > Servers Center > Media Servers** tab. Refer to the following for the descriptions of the fields:

- **Enable DLNA Media Server:** Select ON/OFF to enable/disable the DLNA Media Server.
- **Enable iTunes Server?:** Select ON/OFF to enable/disable the iTunes Server.
- **Media server directory:** Select your media server directory and click **Apply** to share files from the USB disk to media devices in the network.
- **Media Server Status:** Displays the status of the media server.

Using Network Place (Samba) Share service

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



To use Samba share:

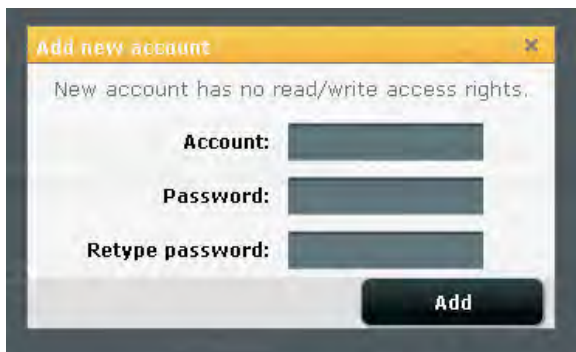
1. From the navigation panel, go to **General > USB application > Servers Center**.

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.

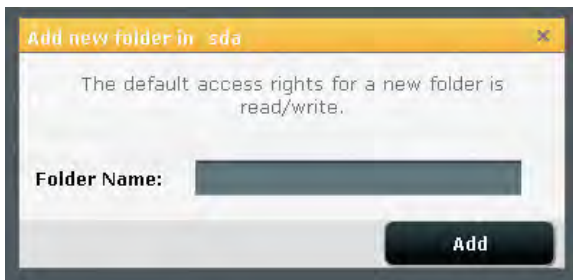


To delete an existing account:

- a) Select the account that you want to delete.
- b) Click .
- 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.



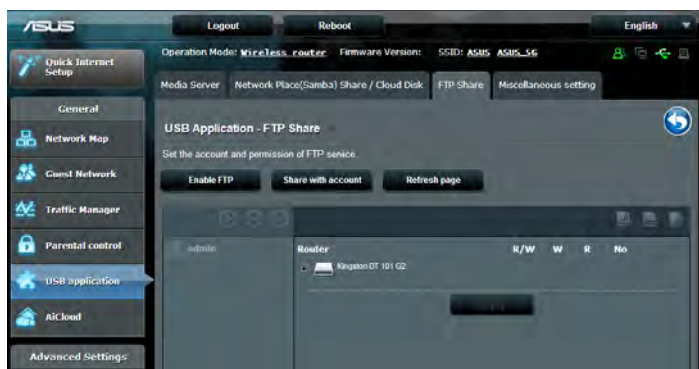
3. From the list of folders, select the type of access permission that you want to assign for specific folders:
 - **R/W**: Select this option to assign read/write access.
 - **R**: Select this option to assign read-only access.
 - **No**: Select this option if you do not want to share a specific file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

Using the FTP Share service

FTP share enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

IMPORTANT:

- Ensure that you safely remove the USB disk. Incorrect removal of the USB disk may cause data corruption.
 - To safely remove the USB disk, refer to the section **Safely removing the USB disk** under **3.1.3 Monitoring your USB device**.
-



To use FTP Share service:

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

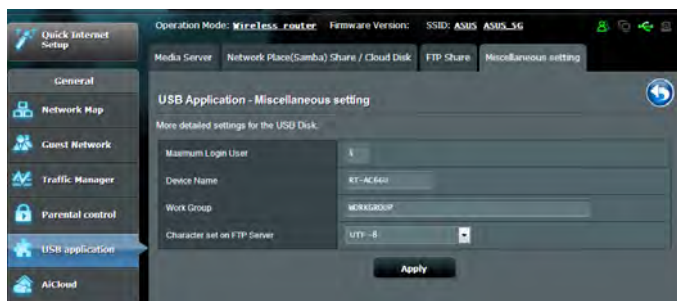
1. From the navigation panel, click **General > USB application > Servers Center > FTP Share** tab.
2. From the list of folders, select the type of access rights that you want to assign for specific folders:
 - **R/W:** Select to assign read/write access for a specific folder.
 - **W:** Select to assign write only access for a specific folder.
 - **R:** Select to assign read only access for a specific folder.
 - **No:** Select this option if you do not want to share a specific folder.
3. Click **Apply** to confirm the changes.
4. To access the FTP server, key in the ftp link **ftp://<hostname>.asuscomm.com** and your user name and password on a web browser or a third-party FTP utility.

Miscellaneous setting

Miscellaneous setting allows you to configure other settings for the USB disk, including the maximum number of user logins, the device name, work group, and character set used on the FTP server.

To configure Miscellaneous settings:

1. From the navigation panel, click **General > USB application > Servers Center > Miscellaneous setting** tab.



2. Configure the following settings:

- **Maximum Login User**

Set the maximum number of concurrent connections of the Network Neighborhood or FTP Server.

NOTE: Some FTP clients may establish more than one connection. Setting this number too low will lead to login failures.

- **Device Name**

Assigns the name of the device as shown on the network. For example, for a device with the name ABC, enter //ABC on the Internet Explorer address bar to access the Network Place service.

- **Work Group**

Assigns the name of the local RT-AC68U network as seen in Network Neighborhood.

NOTE: For **Device Name** and **Work Group**, the standard input characters include letters (a-z, A-Z), digits (0-9), space, underscores(_), and hyphens(-). The first and last character should not contain any spaces. An invalid workgroup name makes it harder for other devices to find your device in the network.

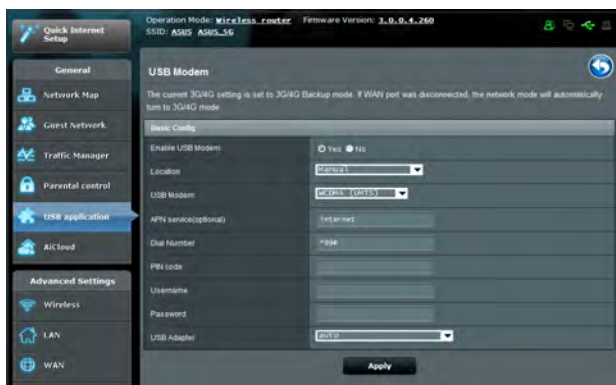
- **Character set on FTP Server**

Select the appropriate encoding used during data exchange on the FTP server.

3.5.3 3G/4G

3G/4G USB modems can be connected to RT-AC68U to allow Internet access.

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



To set up 3G/4G internet access:

1. From the navigation panel, click **General > USB application > 3G/4G**.
2. In the **Enable USB Modem** field, select **Yes**.
3. Set up the following:
 - **Location:** Select your 3G/4G service provider's location from the dropdown list.
 - **ISP:** Select your Internet Service Provider (ISP) from the dropdown list.
 - **APN (Access Point Name) service (optional):** Contact your 3G/4G service provider for detailed information.
 - **Dial Number and PIN code:** The 3G/4G provider's access number and PIN code for connection.

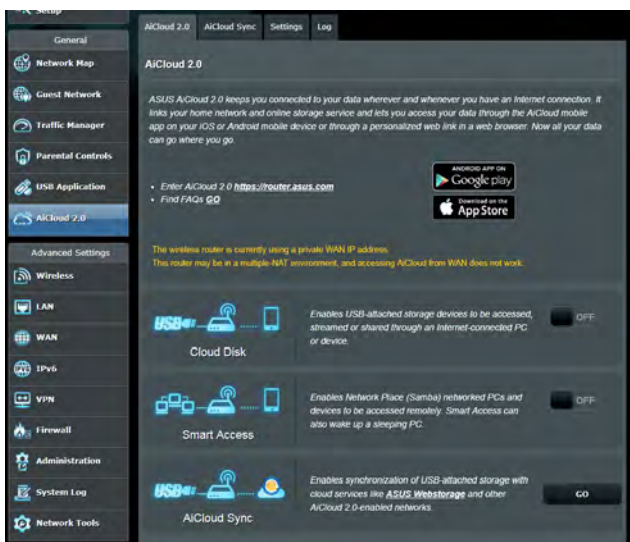
NOTE: PIN code may vary from different providers.

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

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

3.6 Using AiCloud 2.0

AiCloud 2.0 is a cloud service application that allows you to save, sync, share, and access your files.



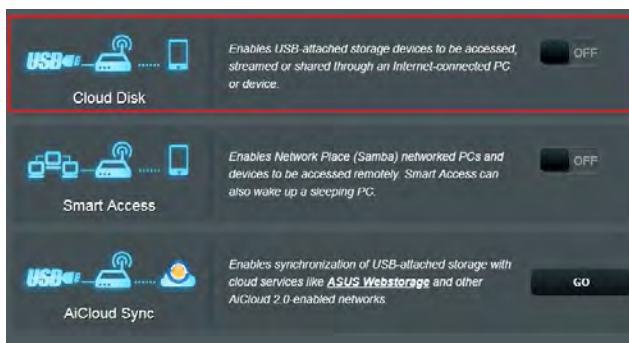
To use AiCloud:

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

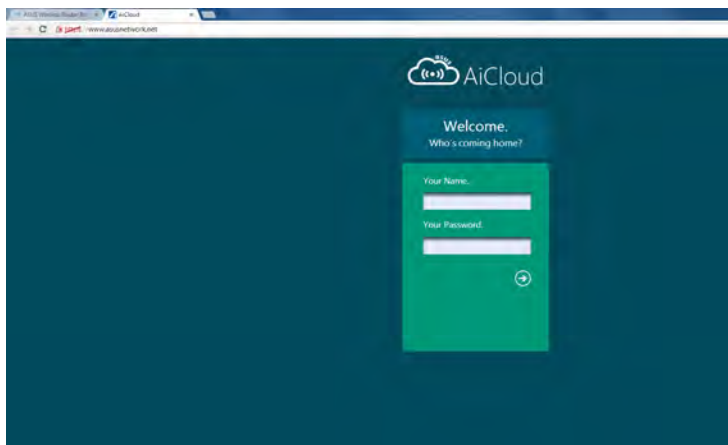
3.6.1 Cloud Disk

To create a cloud disk:

1. Insert a USB storage device into the wireless router.
2. Turn on **Cloud Disk**.

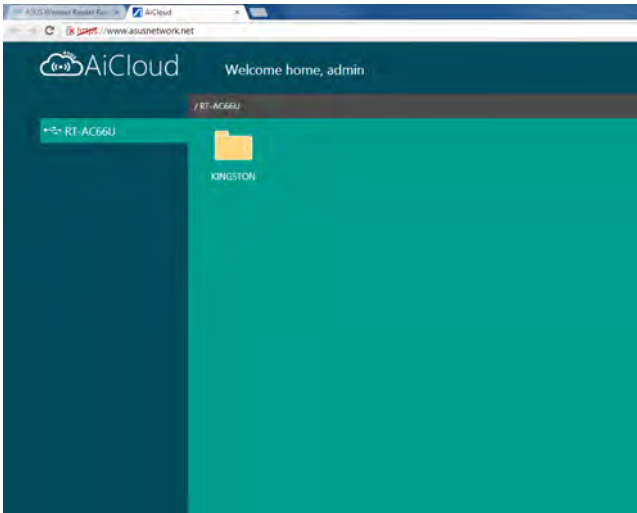


3. Go to <https://router.asus.com> and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.



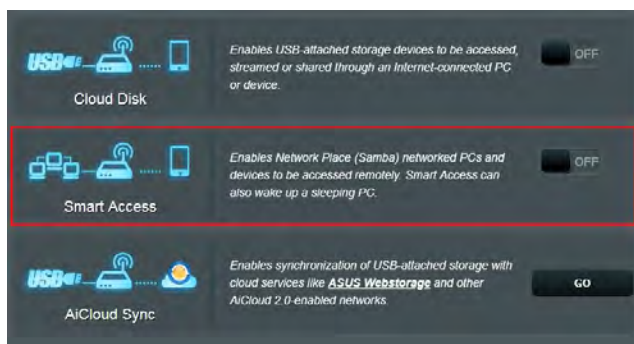
4. You can now start accessing Cloud Disk files on devices connected to the network.

NOTE: When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud for security reason.



3.6.2 Smart Access

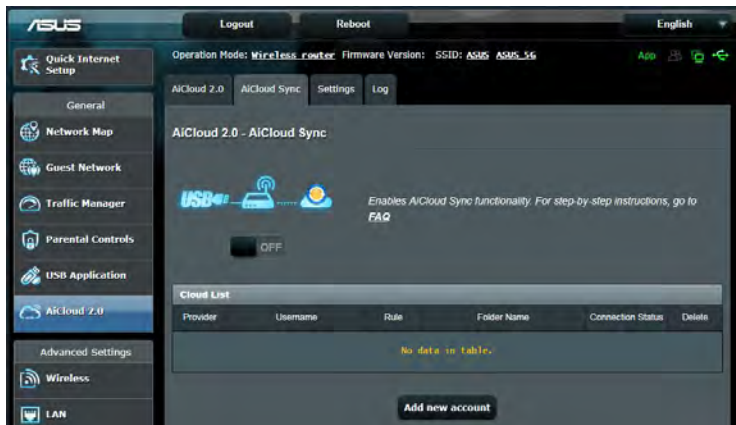
The Smart Access function allows you to easily access your home network via your router's domain name.



NOTES:

- You can create a domain name for your router with ASUS DDNS. For more details, refer to section **4.3.5 DDNS**.
 - By default, AiCloud provides a secure HTTPS connection. Key in [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) for a very secure Cloud Disk and Smart Access usage.
-

3.6.3 AiCloud Sync



To use AiCloud Sync:

1. Launch AiCloud, click **AiCloud Sync** > **Go**.
2. Select **ON** to enable AiCloud Sync.
3. Click **Add new account**.
4. Enter your ASUS WebStorage account password and select the directory that you want to sync with WebStorage.
5. Click **Apply**.

4 Configuring the Advanced Settings

4.1 Wireless

4.1.1 General

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



To configure the basic wireless settings:

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

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

4. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
5. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
 - **Auto:** Select **Auto** to allow 802.11AC, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
 - **Legacy:** Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
 - **N only:** Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
6. Select the operating channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
7. Select any of these channel bandwidth to accommodate higher transmission speeds:
 - 40MHz:** Select this bandwidth to maximize the wireless throughput.
 - 20MHz (default):** Select this bandwidth if you encounter some issues with your wireless connection.
8. Select any of these authentication methods:
 - **Open System:** This option provides no security.
 - **Shared Key:** You must use WEP encryption and enter at least one shared key.

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

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

9. Select any of these WEP (Wired Equivalent Privacy) Encryption options for the data transmitted over your wireless network:

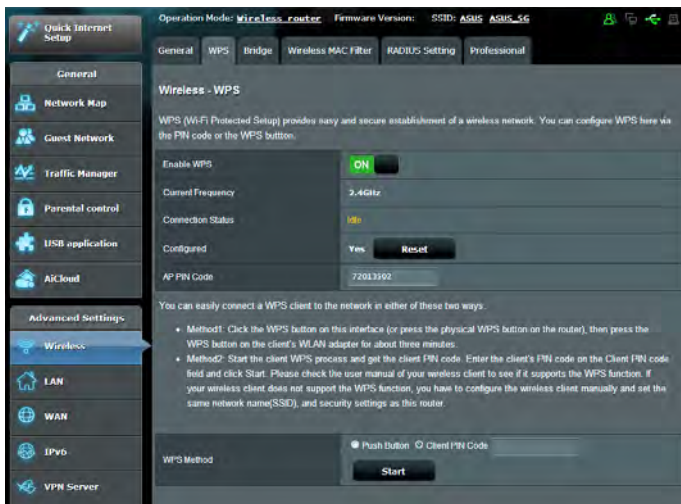
- **Off:** Disables WEP encryption
- **64-bit:** Enables weak WEP encryption
- **128-bit:** Enables improved WEP encryption.

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

4.1.2 WPS

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

NOTE: Ensure that the devices support WPS.



To enable WPS on your wireless network:

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

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

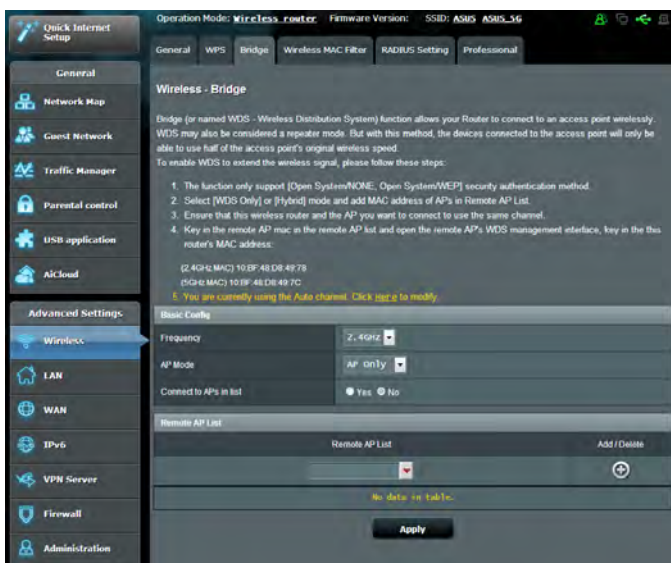
3. In the WPS Method field, select **Push Button** or **Client PIN** code. If you select **Push Button**, go to step 4. If you select **Client PIN** code, go to step 5.
4. To set up WPS using the router's WPS button, follow these steps:
 - a. Click **Start** or press the WPS button found at the rear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

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

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

4.1.3 Bridge

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



To set up the wireless bridge:

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

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

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

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

NOTE: Channel availability varies per country or region.

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

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

7. Click **Apply**.

4.1.4 Wireless MAC Filter

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

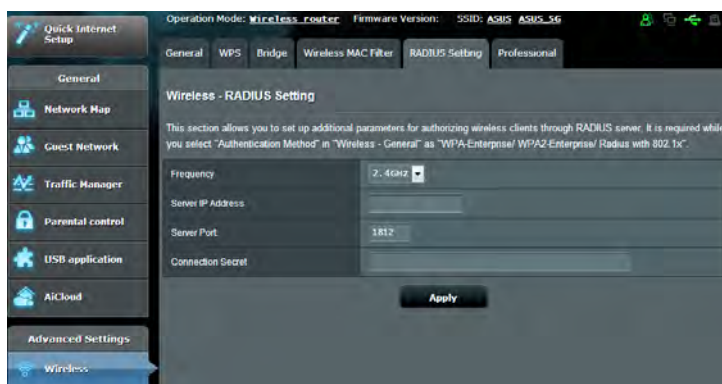


To set up the Wireless MAC filter:

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

4.1.5 RADIUS Setting

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



To set up wireless RADIUS settings:

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

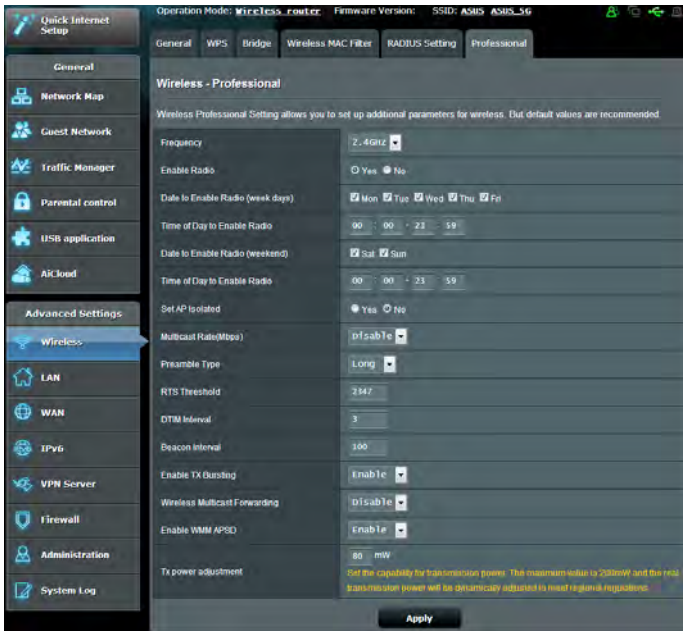
NOTE: Please refer to section **4.1.1 General** section for configuring your wireless router's Authentication Mode.

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

4.1.6 Professional

The Professional screen provides advanced configuration options.

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



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

- **Frequency:** Select the frequency band that the professional settings will be applied to.
- **Enable Radio:** Select **Yes** to enable wireless networking. Select **No** to disable wireless networking.
- **Date to Enable Radio (weekdays):** You can specify which days of the week wireless networking is enabled.
- **Time of Day to Enable Radio:** You can specify a time range when wireless networking is enabled during the week.

- **Date to Enable Radio (weekend):** You can specify which days of the weekend wireless networking is enabled.
- **Time of Day to Enable Radio:** You can specify a time range when wireless networking is enabled during the weekend.
- **Set AP isolated:** The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Multicast rate (Mbps):** Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type:** Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **RTS Threshold:** Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval:** DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval:** Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting:** Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.

- **Wireless multicast forwarding:** Select **Enable** to allow the wireless router to forward multicast traffic to other wireless devices that support multicast. Select **Disable** to prevent the router from forwarding multicast transmissions.
- **Enable WMM APSD:** Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
- **TX Power adjustment:** TX Power adjustment refers to the milliWatts (mW) needed to power the radio signal output of the wireless router. Enter a value between 0 to 100.

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

4.2 LAN

4.2.1 LAN IP

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

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

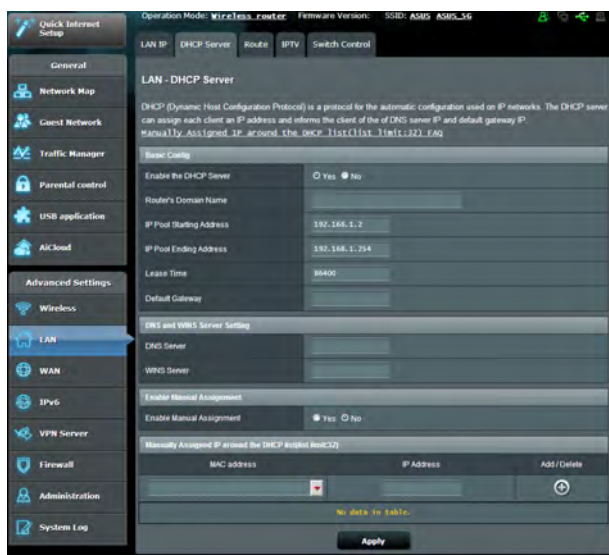


To modify the LAN IP settings:

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.



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:

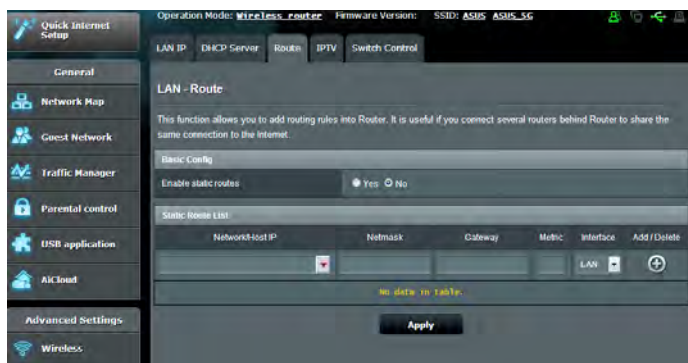
- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
 - An IP Pool Starting Address should not be greater than the IP Pool Ending Address.
-

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.



To configure the LAN Routing table:

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

4.2.4 IPTV

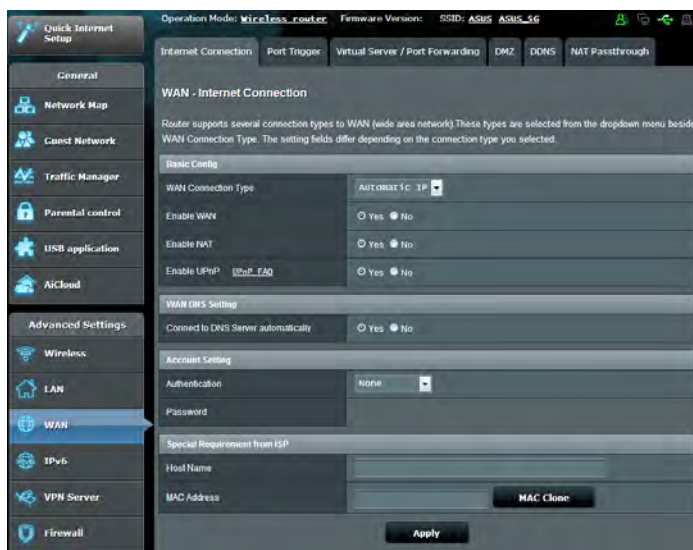
The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.



4.3 WAN

4.3.1 Internet Connection

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



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.

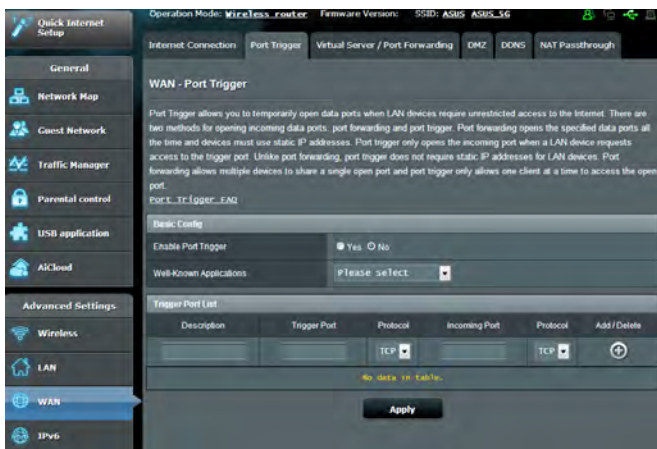
- **Enable NAT:** NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Enable 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.



To set up Port Trigger:

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

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

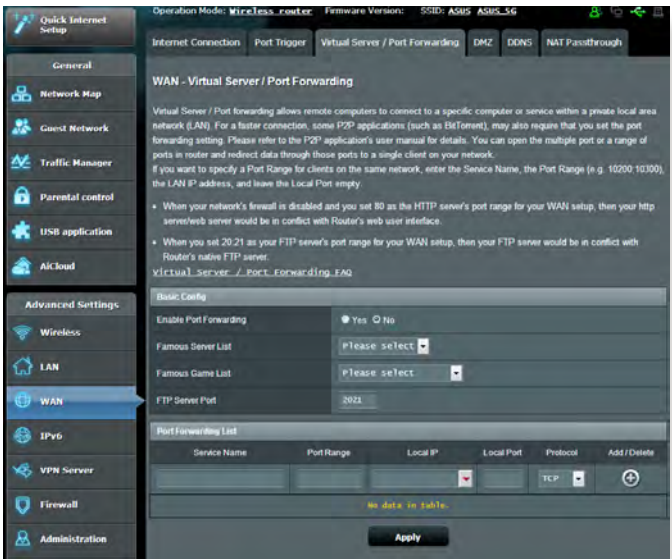
NOTES:

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

4.3.3 Virtual Server/Port Forwarding

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

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



To set up Port Forwarding:

1. 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:

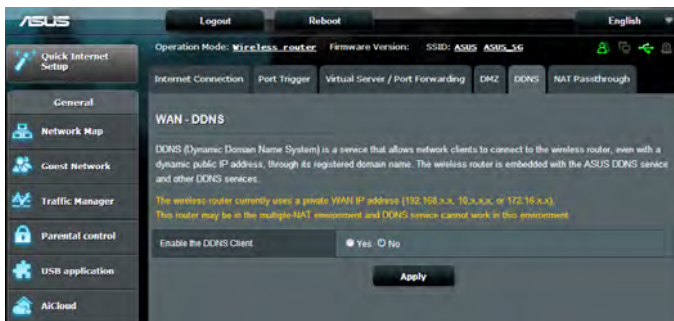
1. From the navigation panel, go to **Advanced Settings > WAN > DMZ** tab.
2. Configure the setting below. When done, click **Apply**.
 - **IP address of Exposed Station:** Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client 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.



To set up DDNS:

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

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

NOTES:

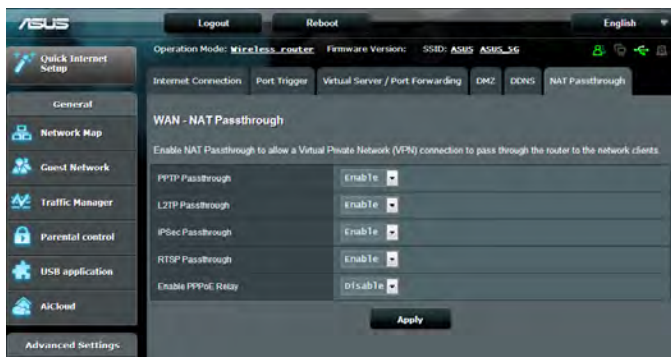
DDNS service will not work under these conditions:

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

4.3.6 NAT Passthrough

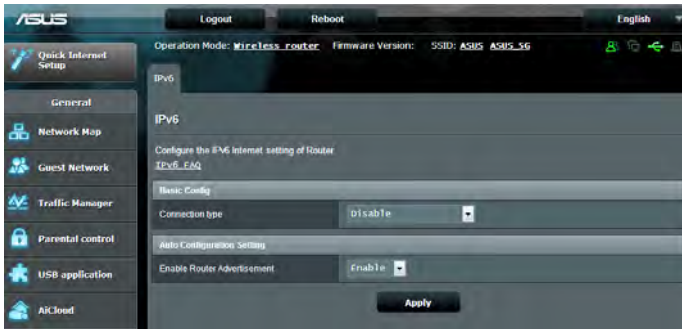
NAT Passthrough allows a Virtual Private Network (VPN) connection to pass through the router to the network clients. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough and RTSP Passthrough are enabled by default.

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



4.4 IPv6

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



To set up IPv6:

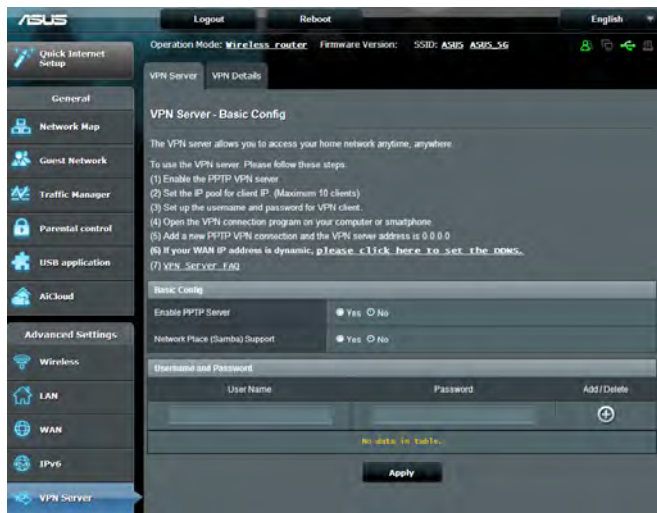
1. From the navigation panel, go to **Advanced Settings > IPv6**.
2. Select your **Connection Type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

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.



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.
