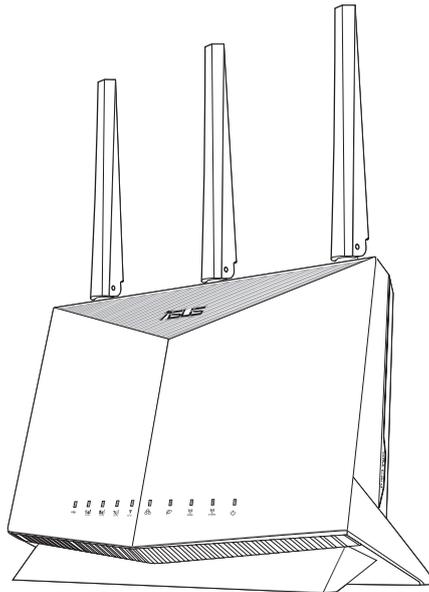


# User Guide

## 4G-AC86U

### Wireless-AC2600 Cat.12 LTE Router



E18231

First Edition

April 2021

**Copyright © 2021 ASUSTeK Computer Inc. All Rights Reserved.**

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

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification 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

|          |  |    |
|----------|--|----|
| <b>1</b> | <b>Getting to know your wireless router</b>          |    |
| 1.1      | Welcome! .....                                       | 7  |
| 1.2      | Package contents.....                                | 7  |
| 1.3      | Your wireless router .....                           | 8  |
| 1.4      | Positioning your router.....                         | 10 |
| 1.5      | Installing a Nano SIM card into your router .....    | 11 |
| <b>2</b> | <b>Getting started</b>                               |    |
| 2.1      | Router setup.....                                    | 12 |
|          | A. Wired connection.....                             | 13 |
|          | B. Wireless connection.....                          | 14 |
| 2.2      | Quick Internet Setup (QIS) with Auto- detection..... | 16 |
| <b>3</b> | <b>Configuring the General Settings</b>              |    |
| 3.1      | Using the Network Map .....                          | 21 |
|          | 3.1.1 Setting up the wireless security settings..... | 22 |
|          | 3.1.2 System Status .....                            | 23 |
|          | 3.1.3 Managing your network clients.....             | 24 |
|          | 3.1.4 Monitoring the Internet Status .....           | 26 |
|          | 3.1.5 Monitoring your USB device .....               | 27 |
| 3.2      | Guest Network.....                                   | 28 |
| 3.3      | AiProtection.....                                    | 30 |
|          | 3.3.1 Network Protection.....                        | 31 |
|          | 3.3.2 Setting up Parental Controls.....              | 35 |
| 3.4      | Adaptive QoS .....                                   | 39 |
|          | 3.4.1 Bandwidth Monitor.....                         | 39 |
|          | 3.4.2 QoS.....                                       | 40 |
|          | 3.4.3 Web History.....                               | 41 |

## Table of contents

|          |  |    |
|----------|--|----|
| 3.5      | Traffic Analyzer .....                   | 42 |
| 3.6      | Using the USB Application .....          | 43 |
| 3.6.1    | Using AiDisk .....                       | 43 |
| 3.6.2    | Using Servers Center.....                | 46 |
| 3.7      | Using iCloud 2.0 .....                   | 51 |
| 3.7.1    | Cloud Disk.....                          | 51 |
| 3.7.2    | Smart Access.....                        | 53 |
| 3.7.3    | Smart Sync.....                          | 53 |
| 3.7.4    | Sync Server .....                        | 55 |
| 3.7.5    | Settings.....                            | 58 |
| 3.8      | Using SMS.....                           | 59 |
| 3.8.1    | Sending Messages .....                   | 59 |
| 3.8.2    | Inbox.....                               | 60 |
| <b>4</b> | <b>Configuring the Advanced Settings</b> |    |
| 4.1      | Wireless.....                            | 61 |
| 4.1.1    | General.....                             | 61 |
| 4.1.2    | WPS .....                                | 63 |
| 4.1.3    | WDS.....                                 | 65 |
| 4.1.4    | Wireless MAC Filter .....                | 67 |
| 4.1.5    | RADIUS Setting .....                     | 68 |
| 4.1.6    | Professional .....                       | 69 |
| 4.2      | LAN.....                                 | 72 |
| 4.2.1    | LAN IP .....                             | 72 |
| 4.2.2    | DHCP Server.....                         | 73 |
| 4.2.3    | Route .....                              | 75 |
| 4.2.4    | IPTV .....                               | 76 |
| 4.2.5    | Switch Control.....                      | 76 |
| 4.3      | WAN .....                                | 77 |
| 4.3.1    | Internet Connection.....                 | 77 |

# Table of contents

|          |   |     |
|----------|---|-----|
| 4.3.2    | IPv6 (Internet Settings) .....                      | 85  |
| 4.3.3    | Dual WAN .....                                      | 86  |
| 4.3.4    | Port Trigger .....                                  | 88  |
| 4.3.5    | Virtual Server/Port Forwarding .....                | 90  |
| 4.3.6    | DMZ.....  | 93  |
| 4.3.7    | DDNS .....  | 94  |
| 4.3.8    | NAT Passthrough .....                               | 95  |
| 4.4      | IPv6 .....  | 96  |
| 4.5      | VPN Server.....                                     | 97  |
| 4.6      | Firewall.....                                       | 98  |
| 4.6.1    | General.....  | 98  |
| 4.6.2    | URL Filter .....                                    | 98  |
| 4.6.3    | Keyword filter .....                                | 99  |
| 4.6.4    | Network Services Filter .....                       | 100 |
| 4.6.5    | IPv6 Firewall .....                                 | 100 |
| 4.7      | Administration .....                                | 101 |
| 4.7.1    | Operation Mode .....                                | 101 |
| 4.7.2    | System.....   | 102 |
| 4.7.3    | Firmware Upgrade .....                              | 104 |
| 4.7.4    | Restore/Save/Upload Setting .....                   | 105 |
| 4.8      | System Log.....                                     | 106 |
| 4.9      | Ethernet WAN Mobile Broadband Function Support List | 107 |
| <b>5</b> | <b>Utilities</b>                                    |     |
| 5.1      | Device Discovery.....                               | 109 |
| 5.2      | Firmware Restoration .....                          | 110 |
| 5.3      | Setting up your printer server .....                | 112 |
| 5.3.1    | ASUS EZ Printer Sharing .....                       | 112 |
| 5.3.2    | Using LPR to Share Printer .....                    | 115 |
| 5.4      | Download Master .....                               | 120 |
| 5.4.1    | Configuring Bit Torrent download settings.....      | 122 |

|       |                     |     |
|-------|---------------------|-----|
| 5.4.2 | NZB settings.....   | 123 |
| 5.4.3 | eMule settings..... | 123 |

## **6 Troubleshooting**

|     |   |     |
|-----|---|-----|
| 6.1 | Basic Troubleshooting.....              | 124 |
| 6.2 | Frequently Asked Questions (FAQs) ..... | 127 |

## **Appendices**

|                               |     |
|-------------------------------|-----|
| Notices .....                 | 136 |
| ASUS Contact information..... | 150 |

# 1 Getting to know your wireless router

## 1.1 Welcome!

Thank you for purchasing an ASUS 4G-AC86U Wireless Router!

The powerful and stylish 4G-AC86U features 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

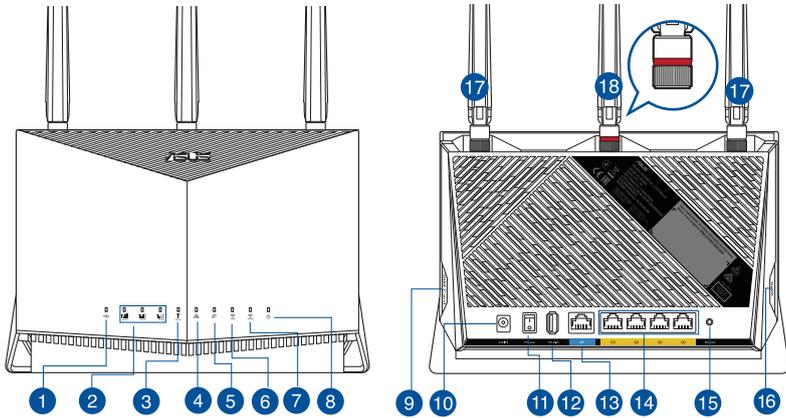
- |  |  |
|--|--|
| <input checked="" type="checkbox"/> 4G-AC86U Wireless Router | <input checked="" type="checkbox"/> AC adapter                         |
| <input checked="" type="checkbox"/> Network cable (RJ-45)    | <input checked="" type="checkbox"/> Quick Start Guide                  |
| <input checked="" type="checkbox"/> 2 x 3G/4G antennas       | <input checked="" type="checkbox"/> 1 x WiFi antenna (with a red ring) |

---

### NOTES:

- If any of the items is damaged or missing, contact your retailer or 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 USB LED**  
Off: No power or no physical connection.  
On: Has physical connection to USB devices.
- 
- 2 3G/4G signal strength LED**  
1 lit LED: Weak signal  
2 lit LEDs: Normal signal  
3 lit LEDs: Strong signal  
Purple light for 3G connection, blue light for 4G connection
- 
- 3 Mobile Broadband LED**  
White: 4G connection is established.  
Blue: 3G connection is established.  
Red: No mobile broadband connection.  
Off: No SIM card is detected.
- 
- 4 LAN LED**  
Off: No data activity or no physical connection.  
On: Ethernet connection is established.
- 
- 5 WAN (Internet) LED**  
Off: No data activity or no physical connection.  
On: Has physical connection to a wide area network (WAN).
- 
- 6 5GHz Wi-Fi LED**  
Off: No 5GHz signal.  
On: 5GHz wireless is ready.  
Flashing: Transmitting or receiving data via wireless connection.
- 
- 7 2.4GHz Wi-Fi LED**  
Off: No 2.4GHz signal.  
On: 2.4GHz wireless is ready.  
Flashing: Transmitting or receiving data via wireless connection.
-

- 
- 8 Power LED**  
 Off: No power.  
 On: Device is ready.  
 Flashing slow: Rescue mode  
 Flashing quick: WPS is processing.

---

  - 9 Nano SIM card slot**  
 Install a Nano SIM card into this slot to establish a Mobile Broadband Internet connection.

---

  - 10 Power (DCIN) port**  
 Insert the bundled AC adapter into this port and connect your router to a power source.

---

  - 11 Power button**  
 Press this button to power on or off the system.

---

  - 12 USB 2.0 port**  
 Insert USB 2.0 compatible devices such as USB hard disks or USB flash drives into this port.

---

  - 13 WAN (Internet) port**  
 Connect a network cable into this port to establish WAN connection.

---

  - 14 LAN (1~4) ports**  
 Connect network cables into these ports to establish LAN connection.

---

  - 15 Reset button**  
 This button resets or restores the system to its factory default settings.

---

  - 16 WPS button**  
 Long press the button to launch the WPS Wizard.

---

  - 17 Detachable LTE antennas**

---

  - 18 Detachable Wi-Fi antenna**

---

**NOTES:**

- Use only the adapter that came with your package. Using other adapters may damage the device.
  - Ensure to insert the Nano SIM card into the card slot before powering on the router.
- 

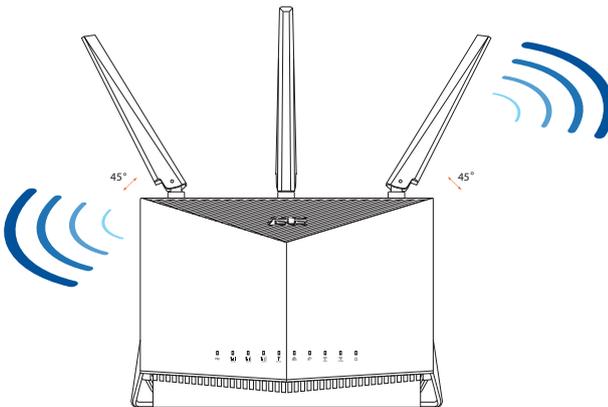
**Ambient conditions:**

|                              |                                 |                     |          |
|------------------------------|---------------------------------|---------------------|----------|
| <b>DC Power adapter</b>      | DC Output: +12V with 3A current |                     |          |
| <b>Operating Temperature</b> | 0~40°C                          | Storage Temperature | -40~70°C |
| <b>Operating Humidity</b>    | 10 ~ 95%                        | Storage Humidity    | 5 ~ 95%  |

## 1.4 Positioning your router

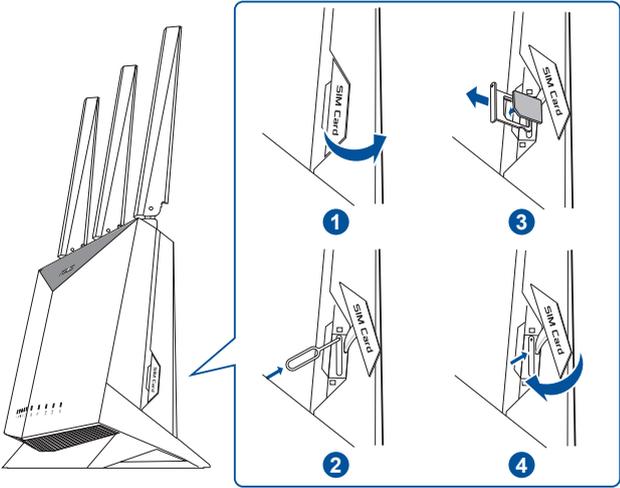
For the best wireless signal transmission between the wireless router and the network devices connected to it, ensure that you:

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



# 1.5 Installing a Nano SIM card into your router

- 1. Remove the cover from the Nano SIM card slot at the right side of your router.
- 2. Push a pin into the hole on the Nano SIM card tray to eject it.
- 3. Place a Nano SIM card on the tray.
- 4. Push the tray to close it.



# 2 Getting started

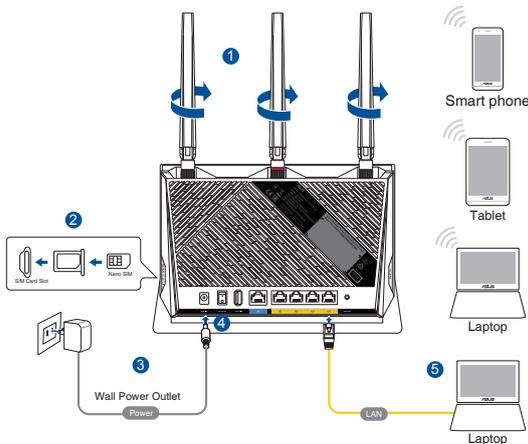
## 2.1 Router setup

### IMPORTANT!

- Use a wired connection when setting up your wireless router to avoid possible setup problems.
- Pinning down the location of your nearest cell tower will help you find the strongest signal.
- The default username and password for Web GUI are **admin** and **admin**.

### NOTES:

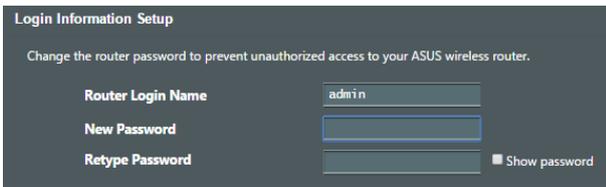
- The Mobile Broadband LED lights up after you power on your router with a Nano SIM card installed.
- Ensure that the Mobile Broadband LED lights up before setting up your router via the QIS Wizard (Quick Internet Setup Wizard).
- You can use either Mobile Broadband or Ethernet WAN for Internet access.
- The auto-detection of your ISP connection type takes place when you configure your Mobile Broadband router for the first time or when your Mobile Broadband router is reset to its default settings. During the QIS process, you may need to key in the PIN code of SIM card and APN (Internet Settings) information that you obtained from your Internet Service Provider (ISP).



## A. Wired connection

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

1. Connect two 3G/4G antennas to the left and right connectors, and the WiFi antenna to the center connector.
2. Insert a Nano SIM card into the Nano SIM card slot.
3. Insert the AC adapter of your router to the DCIN port and plug it to a power outlet.
4. Press the power button to turn on your Mobile Broadband router, and wait for a few minutes for Internet connection.
5. Connect your computer to the router using a wired Ethernet cable.
6. Set up your router via the QIS Wizard (Quick Internet Setup Wizard) after the Mobile Broadband LED  $\nabla$  lights up.
  - a. Open a web browser and enter <http://router.asus.com> to launch the web GUI. Follow onscreen instructions to complete the setup.
  - b. You can also choose ASUS Router app to set up your router. Download ASUS Router App to set up your router via your mobile devices.
7. Set up a password for your router to prevent unauthorized access.



Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New Password

Retype Password   Show password



ASUS  
Router



GET IT ON  
Google Play



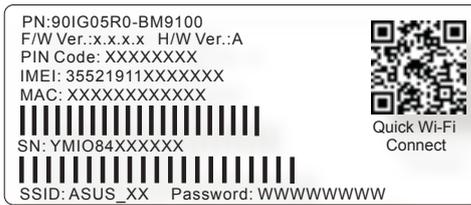
Download on the  
App Store

Q | ASUS Router

## B. Wireless connection

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

1. Connect two 3G/4G antennas to the left and right connectors, and the WiFi antenna to the center connector.
2. Insert a Nano SIM card into the Nano SIM card slot.
3. Insert the AC adapter of your router to the DCIN port and plug it to a power outlet.
4. Press the power button to turn on your Mobile Broadband router, and wait for a few minutes for Internet connection.
5. Connect to the wireless network with SSID shown on the product label on the back side of the router. You can connect by searching the SSID list or scanning the QR code to for quick connection.



\* **XX** refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back side of your router.

6. Set up your router via the QIS Wizard (Quick Internet Setup Wizard) after the Mobile Broadband LED  $\nabla$  lights up.
  - a. Open a web browser and enter <http://router.asus.com> to launch the web GUI. Follow onscreen instructions to complete the setup.
  - b. You can also choose ASUS Router app to set up your router. Download ASUS Router App to set up your router via your mobile devices.
7. Set up a password for your router to prevent unauthorized access.

---

## NOTES:

- For details on connecting to a wireless network, refer to the WLAN adapter's user manual.
  - To set up the security settings for your network, refer to **3.1.1 Setting up the wireless security settings** of this user manual.
- 

**Login Information Setup**

Change the router password to prevent unauthorized access to your ASUS wireless router.

|                   |   |
|-------------------|---|
| Router Login Name | <input type="text" value="admin"/>                              |
| New Password      | <input type="password"/>  |
| Retype Password   | <input type="password"/> <input type="checkbox"/> Show password |



ASUS  
Router



GET IT ON  
Google Play



Download on the  
App Store

🔍 | ASUS Router

## 2.2 Quick Internet Setup (QIS) with Auto-detection

### To set up your router using QIS (Quick Internet Setup):

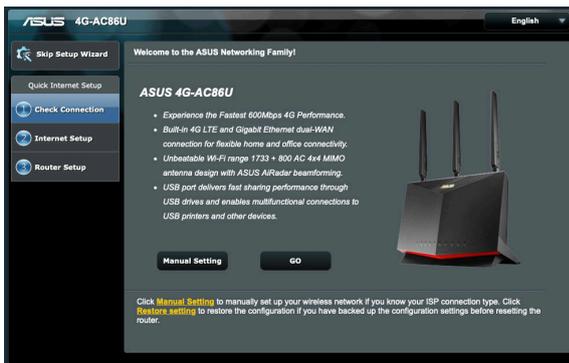
1. Ensure that the following LEDs light up:
  - Power LED
  - 2.4GHz Wi-Fi LED
  - WAN or Mobile Broadband LED
  - 5GHz Wi-Fi LED
2. Launch your web browser such as Internet Explorer, Firefox, Google Chrome, or Safari.

---

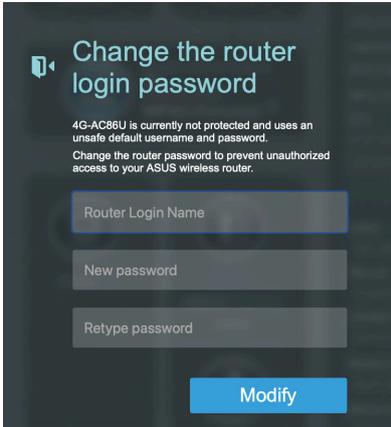
**NOTE:** If QIS does not launch automatically, enter <http://router.asus.com> in the address bar and refresh the browser again.

---

3. Log into the Web GUI. The QIS page launches automatically. By default, the login username and password for your router's Web GUI is "admin".

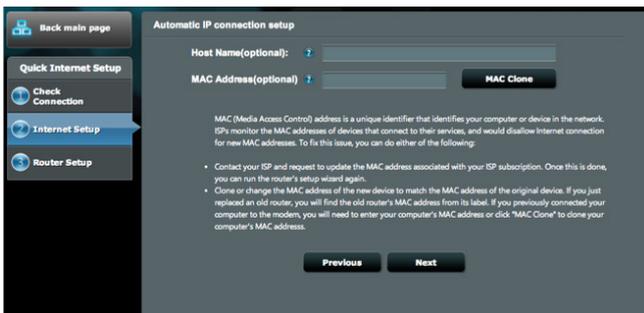


4. Assign your router login name and password and click **Next**. You need this login name and password to log into ASUS router to view or change the router settings. You can take note of your router login name and password for future use.

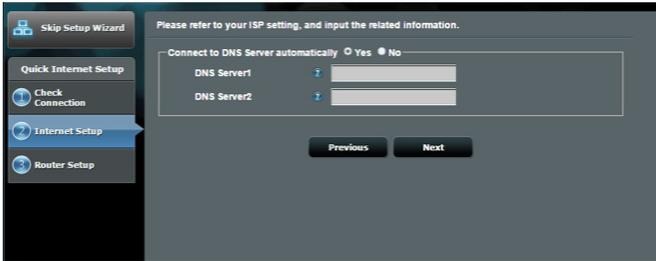


5. If the WAN port is connected, the wireless router's Quick Internet Setup (QIS) feature automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP**, **L2TP**, and **Static IP**. Please obtain the necessary information from your Internet Service Provider (ISP). If your connection type is Dynamic IP (DHCP), QIS wizard will automatically direct you to the next step.

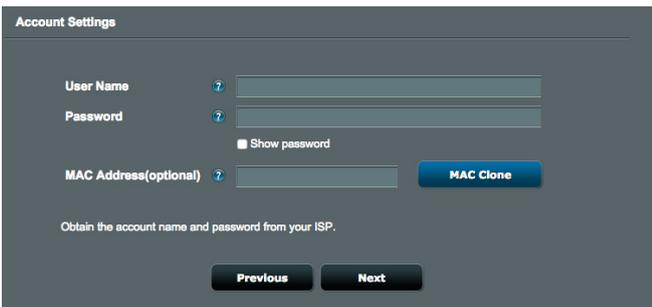
for Automatic IP (DHCP)



for PPPoE, PPTP, and L2TP



for Static IP

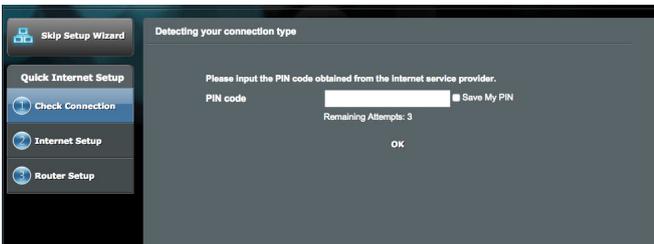


6. If a 3G/4G network is connected, the wireless router's Quick Internet Setup (QIS) feature automatically detects and applies the APN setting to connect to the wireless base station. If the QIS wizard failed to automatically apply the APN setting or the SIM card prompts for a PIN code, set up the APN setting manually.

---

**NOTE:** The PIN code may vary from different providers.

---





7. The dual WAN connection configuration result is displayed. Click **Next** to continue.

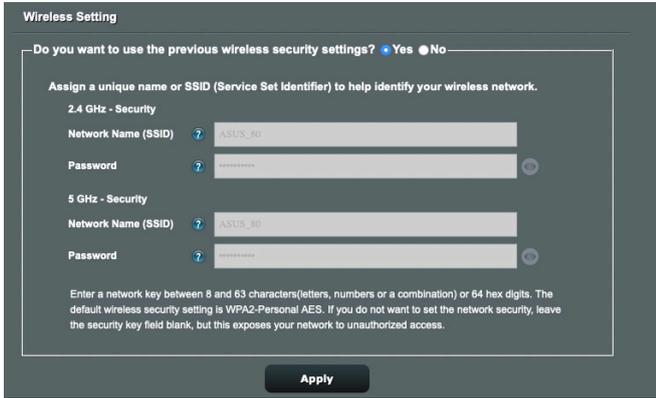
Mobile Broadband Connection is configured successfully



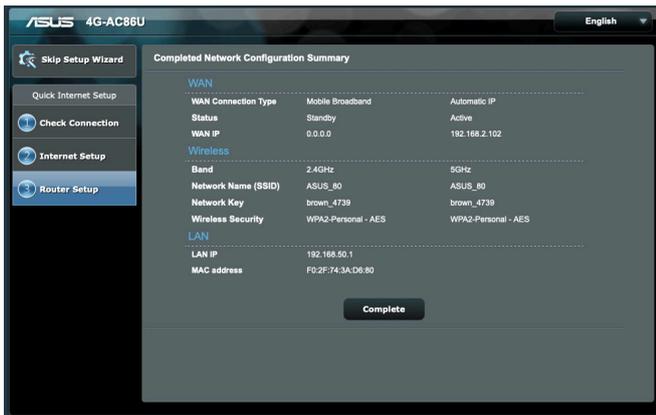
Ethernet WAN Connection is configured successfully



8. If both WAN are configured, go to next step to configure the wireless LAN settings.



9. Assign the network name (SSID) and security key for your 2.4GHz wireless connection. Click **Apply** when done.
10. Your Internet and wireless settings are displayed. Click **Next** to complete the QIS process.



11. The 3G/4G signal strength LED lights up and is steady after completing the 3G/4G network settings via QIS, indicating a successful Internet connection.

# 3 Configuring the General Settings

## 3.1 Using the Network Map

**Network Map** allows you to check the Internet connection status, 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, click System status icon . You can configure the wireless security settings such as **wireless name(SSID), authentication method, and encryption settings**.

#### 2.4GHz security settings



The screenshot shows the 'System Status' screen with the '2.4GHz' tab selected. The settings are as follows:

| Category                    | Value             |
|-----------------------------|-------------------|
| Network Name (SSID)         | ASUS_80           |
| Authentication Method       | WPA2-Personal     |
| WPA Encryption              | AES               |
| WPA-PSK key                 | *****             |
| LAN IP                      | 192.168.50.1      |
| PIN code                    | 31257367          |
| Yandex.DNS                  | Disabled          |
| LAN MAC address             | F0:2F:74:3A:D6:80 |
| Wireless 2.4GHz MAC address | F0:2F:74:3A:D6:80 |

#### 5GHz security settings



The screenshot shows the 'System Status' screen with the '5GHz' tab selected. The settings are as follows:

| Category                  | Value             |
|---------------------------|-------------------|
| Network Name (SSID)       | ASUS_80           |
| Authentication Method     | WPA2-Personal     |
| WPA Encryption            | AES               |
| WPA-PSK key               | *****             |
| LAN IP                    | 192.168.50.1      |
| PIN code                  | 31257367          |
| Yandex.DNS                | Disabled          |
| LAN MAC address           | F0:2F:74:3A:D6:80 |
| Wireless 5GHz MAC address | F0:2F:74:3A:D6:84 |

3. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.
4. From the **Authentication Method** dropdown list, select the authentication method for your wireless network.

If you select **WPA-Personal** or **WPA-2 Personal** as the authentication method, key in the WPA-PSK key or security passkey.

---

**IMPORTANT!** The IEEE 802.11n/ac standard prohibits using Low 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.

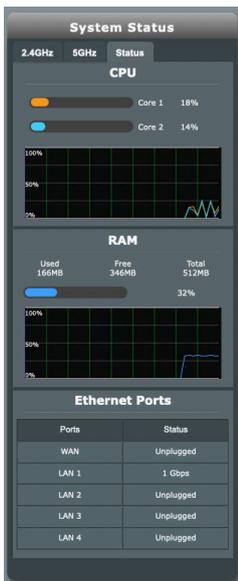
---

- 5 Click **Apply** when done.

### 3.1.2 System Status

**To monitor the system resources:**

1. From the navigation panel, go to **General > Network Map**.
2. On the Network Map screen, click the System status icon . you can find the information about CPU and memory usage.



### 3.1.3 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. On Client status table, click the device icon  to show the detailed profile of the device.

DHCP Logged-in User 



Name MacBook-Air-M1

IP 192.168.50.209

MAC 00:E0:4C:68:01:A2

Device REALTEK SEMICONDUCTOR CORP.

Default Change

Block Internet Access  OFF

Time Scheduling  OFF

### 3.1.4 Monitoring the Internet Status

#### To monitor your Internet status:

1. From the navigation panel, go to **General > Network Map** tab.
2. On the **Network Map** screen, select the Internet icon  to display your Internet configuration. You can also select Mobile Broadband icon  to display Mobile Broadband configuration.
3. To terminate WAN interface from your network, click **Switch** button on Cellular Data and Internet Connection.

#### Mobile Broadband

#### Mobile Broadband Status

Cellular Data

Enable Dual WAN

WAN Port  
Mobile Broadband

Dual WAN Mode  
Fail Over

Connection type  
TDD LTE

WAN IP  
100.76.54.161

Subnet Mask  
255.255.255.252

DNS  
210.200.211.193  
210.200.211.225

Gateway  
100.76.54.162

WAN setting

#### Ethernet WAN

#### Ethernet WAN Status

Internet Connection

WAN Port  
WAN

Dual WAN Mode  
Fail Over

Connection type  
Automatic IP

WAN IP  
0.0.0.0

Subnet Mask  
0.0.0.0

DNS

Gateway  
0.0.0.0

Lease time  
Renewing...

Lease expires  
Expired

Dual WAN setting

WAN setting

### 3.1.5 Monitoring your USB device

The ASUS wireless router provides one USB port for connecting USB devices or USB printer to allow you to share files and printer with clients in your network.

#### To monitor your USB device:

1. From the navigation panel, go to **General > Network Map** tab.
2. On the **Network Map** screen, select the USB Disk Status icon  to display your USB device's information.
3. On the **Media Server** field, click **GO** to set up an iTunes and DLNA server for local media file sharing.

---

**NOTE:** The wireless router works with most USB HDDs/Flash disks (up to 2 TB size) and supports read-write access for FAT16, FAT32, EXT2, EXT3, and NTFS.

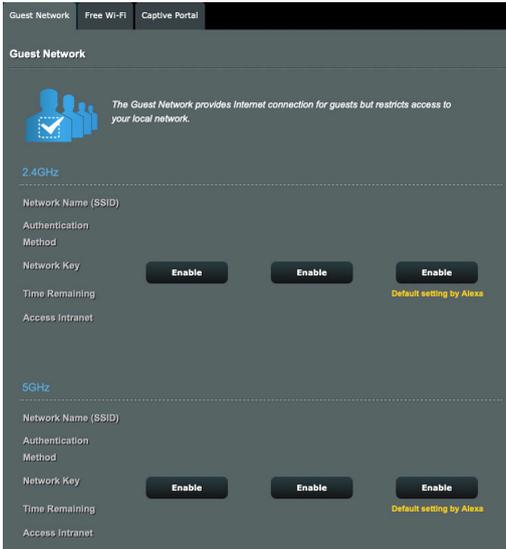
---

4. On the **AiDisk Wizard** field, click **GO** to set up an FTP server for Internet file sharing.
5. To eject USB Disk from USB interface, click **Remove** button on **Safely Remove disk** field. When the USB disk is ejected successfully, the USB status shows **Unmounted**.



## 3.2 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.



### To create a guest network:

1. From the navigation panel, go to **General** > **Guest Network**.
2. On the **Guest Network** screen, select 2.4Ghz and 5Ghz frequency band for the guest network that you want to create.
3. Click **Enable**.
4. Configure a guest's settings on pop-up screen
5. Assign a Network Name (SSID) for identify your guest network.
6. Select an Authentication Method.
7. If you select a WPA authentication method, select a WPA Encryption.
8. Specify the **Access time** or choose **Limitless**.

9. Select **Disable** or **Enable** on the **Access Intranet** item.
10. Select **Disable** or **Enable** on **Enable MAC Filter** item for your guest network.

**Guest Network**

 *The Guest Network provides Internet connection for guests but restricts access to your local network.*

|                       |   |
|-----------------------|---|
| Guest Network Index   | 1   |
| Hide SSID             | <input checked="" type="radio"/> Yes <input type="radio"/> No   |
| Network Name (SSID)   | ASUS_R0_2G_Guest  |
| Authentication Method | WPA2-Personal   |
| WPA Encryption        | AES   |
| WPA Pre-Shared Key    | brown_4739  |
| Access time           | <input checked="" type="radio"/> 0 days 0 hour(s) 0 minute(s)<br><input type="radio"/> Unlimited access |
| Bandwidth Limiter     | <input checked="" type="radio"/> Yes <input type="radio"/> No   |
| Access Intranet       | Disable   |
| Enable MAC Filter     | Disable   |

11. When done, click **Apply**.

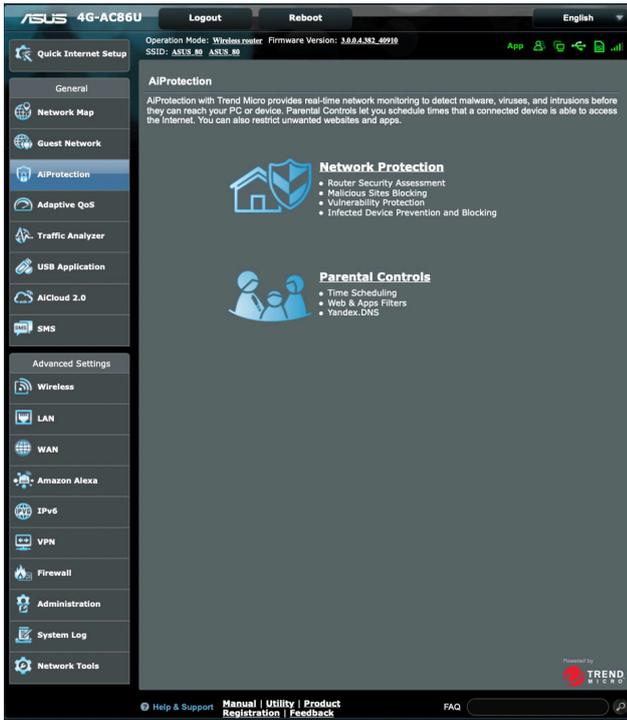
---

## NOTES:

- Visit <https://www.asus.com/support/FAQ/1034977/> to see **How to set up Captive Portal**.
  - Visit <https://www.asus.com/support/FAQ/1034971/> to see **How to set up Free Wi-Fi**.
-

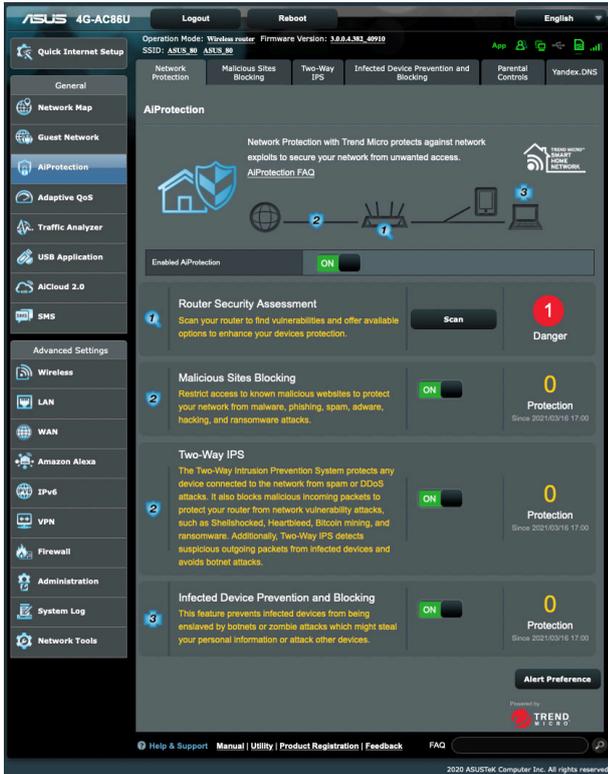
### 3.3 AiProtection

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



### 3.3.1 Network Protection

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

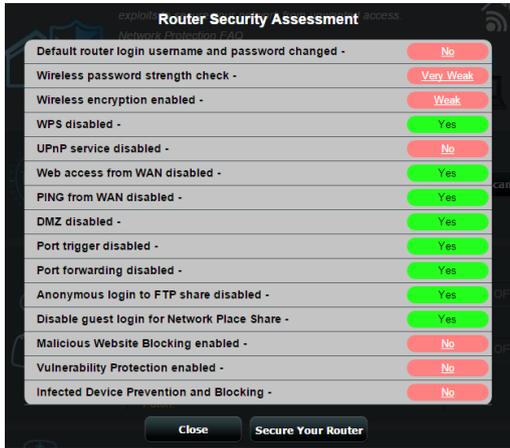


### Configuring Network Protection

To configure Network Protection:

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

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



---

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

---

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

---

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

---

- b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.
  - c. Go back to the **Router Security Assessment** page and click **Close** to exit the page.
5. To automatically configure the security settings, click **Secure Your Router**.
6. When a message prompt appears, click **OK**.

## Malicious Sites Blocking

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

---

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

---

### To enable Malicious Sites Blocking:

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

## Vulnerability protection

This feature resolves common exploits within the router configuration.

---

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

---

### To enable Vulnerability protection:

1. From the navigation panel, go to **General > AiProtection**.
2. From the **AiProtection** main page, click on **Network Protection**.
3. From the **Vulnerability protection** pane, click **ON**.

## Infected Device Prevention and Blocking

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

---

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

---

### To enable Infected Device Prevention and Blocking:

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

### To configure Alert Preference:

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

## 3.3.2 Setting up Parental Controls

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

To go to the Parental Controls main page:

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

The screenshot shows the ASUS AiProtection Web & Apps Filters configuration page. The interface includes a navigation sidebar on the left with options like General, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, USB Application, AiCloud 2.0, SMS, and Advanced Settings. The main content area is titled "AiProtection - Web & Apps Filters" and features a "Web & Apps Filters" toggle switch set to "ON". Below this, there is a table for "Client List (Max Limit: 16)" with columns for "Client Name (MAC Address)", "Content Category", and "Add / Delete". The table contains one entry for "PC (P2P-TR-ALL-0x00)". The "Content Category" column lists several categories: "Adult", "Instant Message and Communication", "P2P and File Transfer", and "Streaming and Entertainment", each with a brief description of the filtering rules. An "Apply" button is located at the bottom of the table. The footer of the page includes links for "Help & Support", "Manual", "Utility", "Product Registration", "Feedback", and "FAQ", along with the copyright notice "© 2020 ASUSTek Computer Inc. All rights reserved."

## Web & Apps Filters

Web & Apps Filters is a feature of **Parental Controls** that allows you to block access to unwanted web sites or applications.

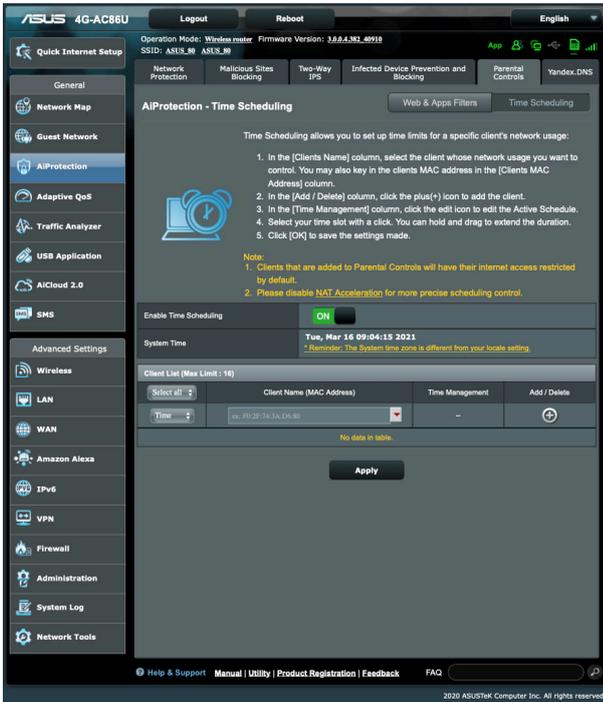
### To configure Web & Apps Filters:

1. From the navigation panel, go to **General > AiProtection**.
2. From the **AiProtection** main page, click on the **Parental Controls** icon to go to the **Parental Controls** tab.
3. From the **Web & Apps Filters** pane, click **ON**.
4. When the End Users License Agreement (EULA) message prompt appears, click **I agree** to continue.
5. From the **Client List** column, select or key in the client's name from the drop down list box.
6. From the **Content Category** column, select the filters from the four main categories: **Adult, Instant Message and Communication, P2P and File Transfer**, and **Streaming and Entertainment**.
7. Click  to add the client's profile.
8. Click **Apply** to save the settings.

## Time Scheduling

Time Scheduling allows you to set the time limit for a client's network usage.

**NOTE:** Ensure that your system time is synchronized with the NTP server.



### To configure Time Scheduling:

1. From the navigation panel, go to **General > AiProtection > Parental Controls > Time Scheduling**.
2. From the **Enable Time Scheduling** pane, click **ON**.
3. From the **Client Name (MAC Address)** column, select or key in the client's name from the drop down list box.

---

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

---

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

## 3.4 Adaptive QoS

### 3.4.1 Bandwidth Monitor

This feature allows you to monitor the bandwidth of WAN/LAN and displays the upload and download speed of your connection.



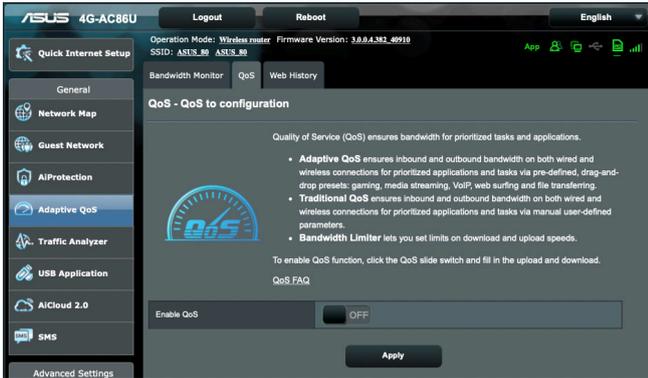
### Apps analysis

To enable Apps analysis function:

1. From the navigation panel, go to **General > Adaptive QoS > Bandwidth Monitor** tab.
2. From the **Apps Analysis** pane, click **ON**.

## 3.4.2 QoS

This feature ensures bandwidth for prioritized tasks and applications.



### To enable the QoS function:

1. From the navigation panel, go to **General > Adaptive QoS > QoS** tab.
2. From the **Enable QoS** pane, click **ON**.
3. Fill in the upload and download bandwidth fields.

---

**NOTE:** Get the bandwidth information from your ISP. You can also go to <http://speedtest.net> to check and get your bandwidth.

---

4. Select the QoS Type (Adaptive or Traditional) for your configuration.

---

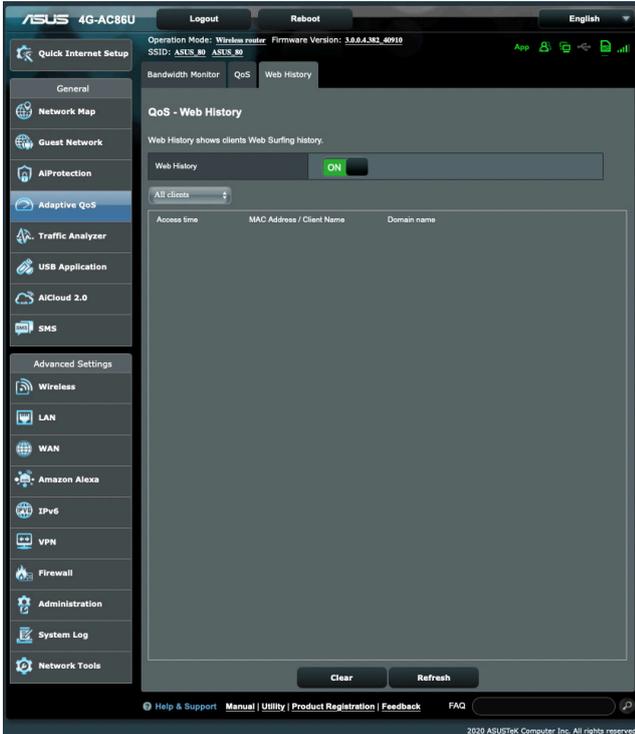
**NOTE:** The definition of the QoS Type is displayed on the QoS tab for your reference.

---

5. Click **Apply**.

### 3.4.3 Web History

This feature displays the history and details of the sites or URLs that the client visited.

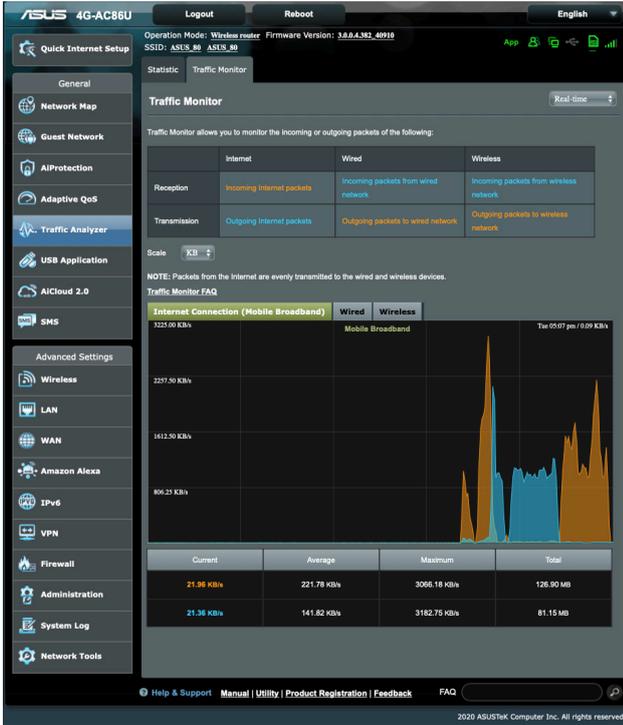


#### To view the Web History:

1. From the navigation panel, go to **General > Adaptive QoS > Web History** tab.
2. (Optional) Click **Refresh** to clear the list.

## 3.5 Traffic Analyzer

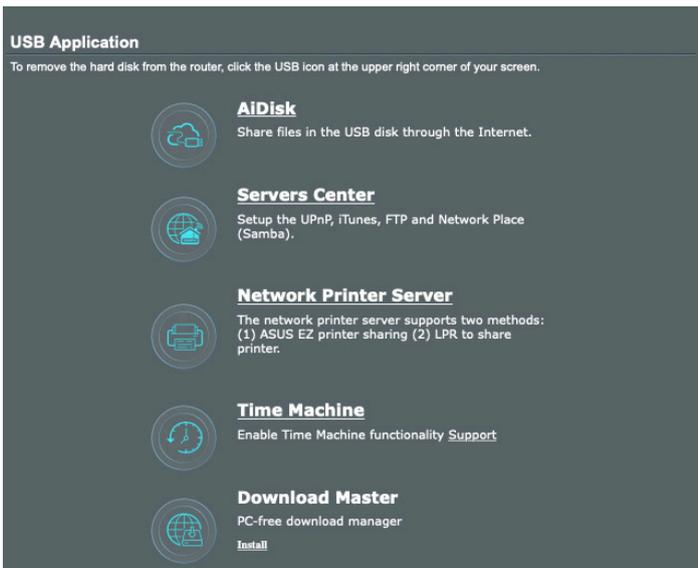
The traffic monitor feature allows you to access the bandwidth usage and speed of your Internet, wired, or wireless networks. It allows you to monitor network traffic in real-time or on a daily basis. It also offers an option to display the network traffic within the last 24 hours.



## 3.6 Using the USB Application

The USB Applications function provides AiDisk, Servers Center, Network Printer Server, Time Machine 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.



### 3.6.1 Using AiDisk

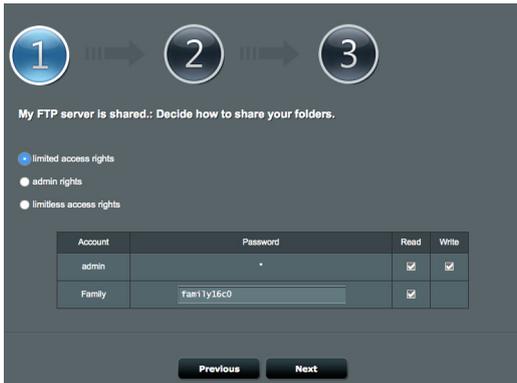
AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

#### To use AiDisk:

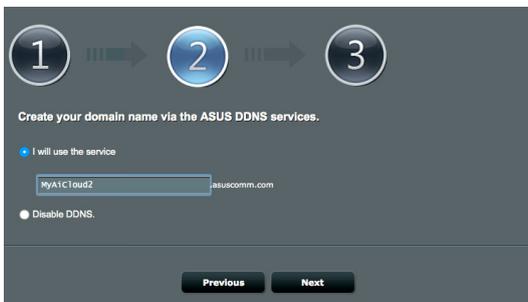
1. From the navigation panel, go to **General > USB application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.



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



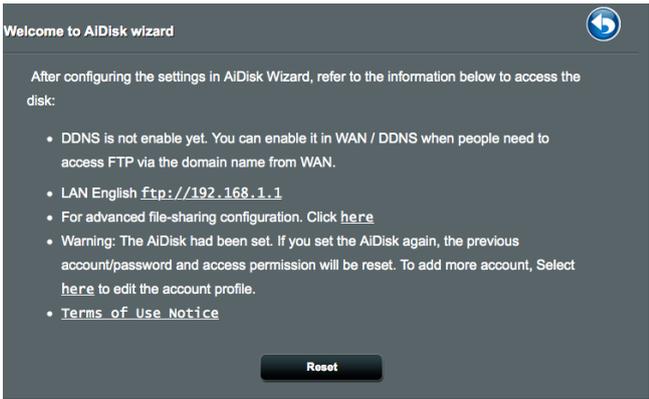
4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select **I will use the service** and key in your domain name. When done, click **Next**.





You can also select **Disable DDNS** 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.



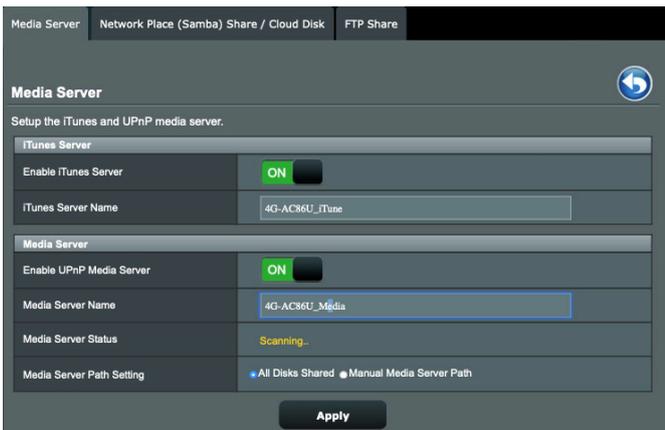
### 3.6.2 Using Servers Center

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 4G-AC86U's network.

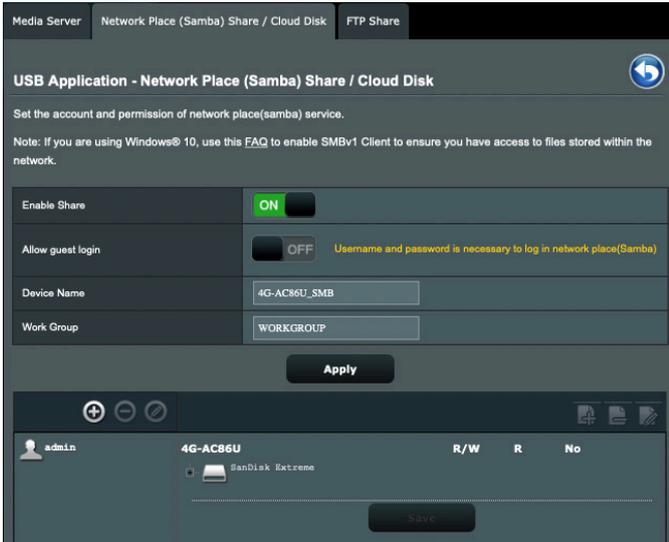


To launch the Media Server setting page, go to **General > USB application > Media Services and Servers > Media Server** tab. Refer to the following for the descriptions of the fields:

- **Enable iTunes Server:** Select ON/OFF to enable/disable the iTunes Server.
- **Enable UPnP Media Server:** Select ON/OFF to enable/disable the UPnP Media Server.
- **Media Server Status:** Displays the status of the media server.
- **Media Server Path Setting:** Select **All Disks Shared** or **Manual Media Server Path**.

### 3.6.3 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 > Media Services and Servers > Network Place (Samba) Share / Cloud Disk** tab.

---

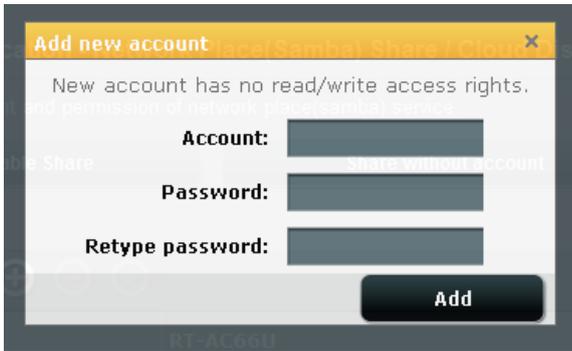
**NOTE:** Network Place (Samba) Share is enabled by default.

---

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

#### To create a new account:

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



### 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.

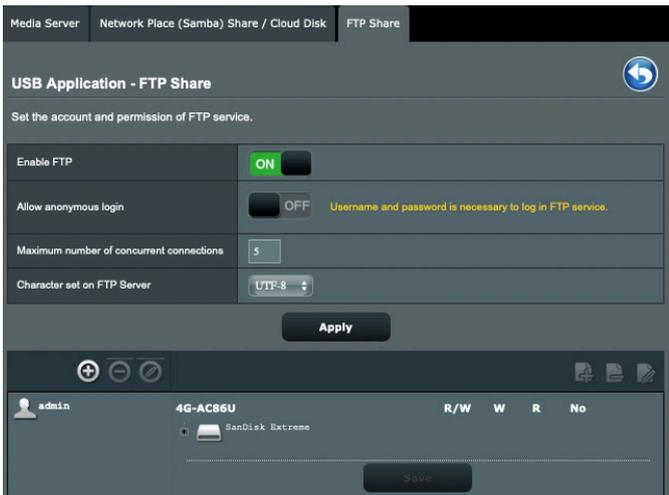
### 3.6.4 Using the FTP Share service

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 **3.1.5 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 **3.6.1 Using AiDisk**.

---

1. From the navigation panel, click **General > USB application > Media Services and Servers > FTP Share** tab.
2. From the list of folders, select the type of access rights that you want to assign for specific folders:
  - **R/W:** Select to assign read/write access for a specific folder.
  - **W:** Select to assign write only access for a specific folder.

- **R:** Select to assign read only access for a specific folder.
  - **No:** Select this option if you do not want to share a specific folder.
3. If you prefer, you can set the **Allow anonymous login** field to **ON**.
  4. In the **Maximum number of concurrent connections** field, key in the number of devices that can simultaneously connect to the FTP share server.
  5. Click **Apply** to confirm the changes.
  6. To access the FTP server, key in the ftp link **ftp://<hostname>.asuscomm.com** and your user name and password on a web browser or a third-party FTP utility.

## 3.7 Using AiCloud 2.0

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

The screenshot shows the AiCloud 2.0 web interface. At the top, there are navigation tabs: AiCloud 2.0, Smart Sync, Sync Server, Settings, and Log. Below the tabs, the title "AiCloud 2.0" is displayed. A paragraph explains that the service keeps users connected to their data wherever and whenever they have an Internet connection, linking to home networks and online storage services. Below this, there are three links: "Enter AiCloud 2.0 <https://router.asus.com>", "Find tutorial videos [GO](#)", and "Find FAQs [GO](#)". To the right of these links are logos for Google Play and the App Store. The interface then lists three features, each with an icon, a description, and a toggle switch:

- Cloud Disk:** Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device. The toggle is turned ON.
- Smart Access:** Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC. The toggle is turned ON.
- Smart Sync:** Enables synchronization of USB-attached storage with cloud services like ASUS Webstorage and other AiCloud 2.0-enabled networks. There is a "GO" button next to it.

### 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.

### 3.7.1 Cloud Disk

#### To create a cloud disk:

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

This image is a close-up of the "Cloud Disk" feature toggle. It shows the "USB" icon, a router icon, and a smartphone icon. The text reads: "Enables USB-attached storage devices to be accessed, streamed or shared through an internet-connected PC or device." The toggle switch is currently turned ON.

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.

---



### 3.7.2 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 **4.3.7 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.

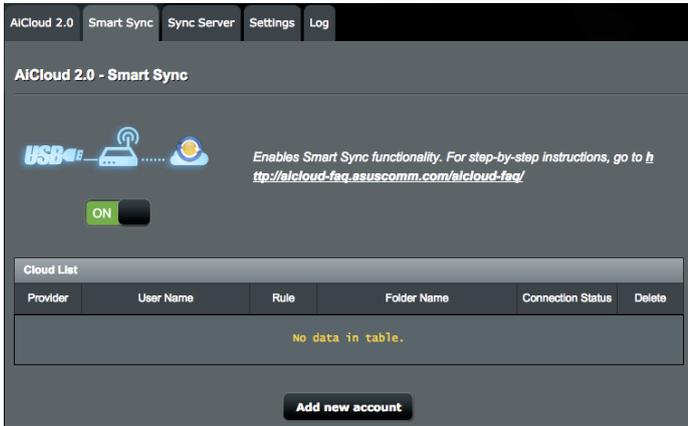
### 3.7.3 Smart Sync

#### To use Smart Sync:

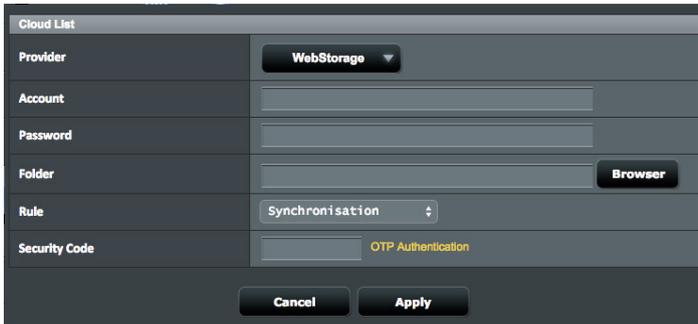
1. From the navigation panel, click **AiCloud 2.0 > AiCloud 2.0 > Smart Sync > Go**.



2. Select **ON** to enable Smart Sync.
3. Click **Add new account**.



4. Enter your ASUS WebStorage or Dropbox account password and select the directory that you want to sync with WebStorage.
5. Select Syn rules for the Smart sync task.
  - **Synchronization:** Selecting **Synchronization** allows you to sync a folder between two servers, which sync task always keeps your folder with the same files.
  - **Download to USB Disk:** Selecting **Download to USB Disk** allows you to replicate the remote files to the local folder on USB Disk.
  - **Upload to Cloud:** Selecting **Upload to Cloud** allows you to replicate the local files to the remote folder on **ASUS WebStorage**.



6. Click **Apply** to add the sync task .

## 3.7.4 Sync Server

AiCloud 2.0 Smart Sync Sync Server Settings Log

### AiCloud 2.0 - Sync Server

Smart Sync let you to sync your cloud disk with other AiCloud 2.0 account, fill the forms below then generate an invitation to your friend.

1. Fill the invitation form as below.
2. Select a way to get a security code.
3. Click "Generate" to get a invitation.
4. Copy the contents of invitation and mail to your friends.
5. You might not use smart sync with your friends due to ISP firewall issue, please contact your ISP. For advanced users, please enter a specific "Host name" below to use smart sync with your friends.



#### Invitation Generator

**Description**

**Host Name**

**Local sync folder**

**Rule**  ?

**Security Code**

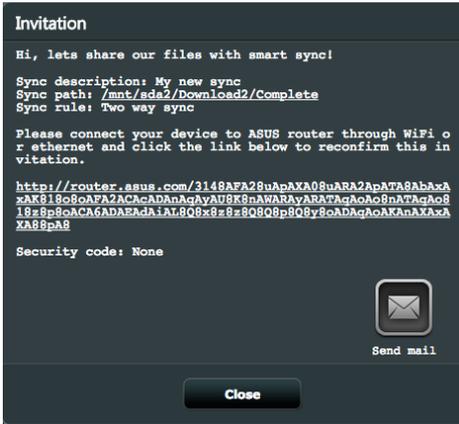


#### Sync List

| Provider          | Description | Rule | Local Sync Folder | Invitation | Delete |
|-------------------|-------------|------|-------------------|------------|--------|
| No data in table. |             |      |                   |            |        |

## To use Sync Server:

1. From the navigation panel, click **AiCloud 2.0 > Sync Server**.
2. Enter Sync Server configuration on **Invitation Generator** to enable **Smart Sync**.
3. Send your friend the sync invitation.



4. After a invitation is generated, you can check the sync task on **Sync List** table .



5. You can click Delete button  to terminate the task if you don't want sync task the folder with remote sync client anymore.
6. You can also check the activities of sync server by clicking **Check log** button or lick **Log** tab.

AiCloud 2.0 Smart Sync Sync Server Settings Log

### AiCloud 2.0 - Settings

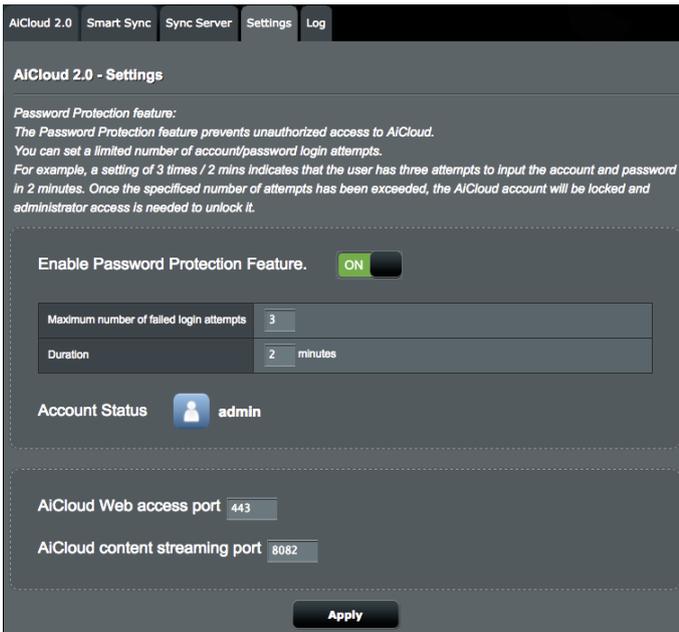
*This page displays a log of AiCloud's activities.*

**Refresh**

### 3.7.5 Settings

AiCloud 2.0 allows you to define a access policy to prevent unauthorized access, such as dictionary attack. When a host try to access the AiCloud and exceed the defined Maximum number of failed login attempts in the defined duration, the AiCloud service will be disabled automatically.

The Secure Socket Layer (SSL) is a protocol that provide an encrypted communication between web server and browsers for secure data transfer, which includes access password. User access the AiCloud web portal use a default port, 443, over https. The content delivering uses a default port, 8082, over http.



## 3.8 Using SMS

Short Message Service (SMS) is a text messaging service that allows you to send or receive messages from or on your wireless router.

### 3.8.1 Sending Messages

This function allows you to send short messages from your wireless router.

#### To send a new SMS message:

1. Click the **New** button .
2. Enter the recipient's phone number.
3. Compose your message.
4. Click **Send** to send the message.



The screenshot shows a dark-themed form for composing an SMS. At the top right is a close button (X). The form has two main sections: 'Phone Number' and 'Message (Max Limit : 70)'. The 'Phone Number' field contains '0988487210'. The 'Message' field contains the text 'Comment est ta journée, doux robot?'. At the bottom right of the message field is a green circular icon with a white 'G'. Below the message field are two buttons: 'Send' and 'Save'.

#### To save a draft message:

1. You can also save the draft message by clicking **Save**.
2. You will see the message listed in the table in **Draft**.
3. Click the edit icon  to edit and send the message, or tick it and click  to delete the draft message.



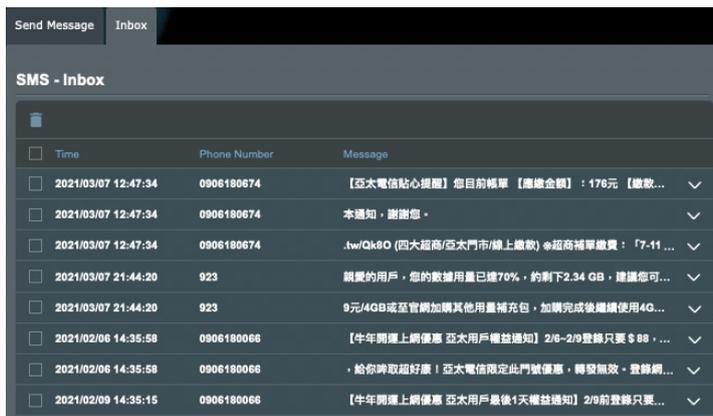
The screenshot shows a table titled 'SMS - Send Message'. The table has a header row: 'Draft (Max Limit : 5)' and a 'New' button with a plus icon. Below the header is a table with two columns: 'Phone Number' and 'Message'. The first row of data has '0988487210' in the 'Phone Number' column and 'Comment est ta journée, doux robot?' in the 'Message' column. There is a delete icon (trash) to the left of the first row and an edit icon (pencil) to the right of the second row.

| SMS - Send Message                  |                                     |
|-------------------------------------|-------------------------------------|
| Draft (Max Limit : 5)               |                                     |
| <input type="checkbox"/>            |                                     |
| Phone Number                        | Message                             |
| <input type="checkbox"/> 0988487210 | Comment est ta journée, doux robot? |

## 3.8.2 Inbox

Inbox allows you to view the received short messages saved in your device.

Click  to view more information, or tick a message and click  to delete it.



| <input type="checkbox"/> | Time                | Phone Number | Message                                     |   |
|--------------------------|---------------------|--------------|---|---|
| <input type="checkbox"/> | 2021/03/07 12:47:34 | 0906180674   | 【亞太電信貼心提醒】您目前帳單【應繳金額】：176元【繳款...            | ▼ |
| <input type="checkbox"/> | 2021/03/07 12:47:34 | 0906180674   | 本週知，謝謝您。                                    | ▼ |
| <input type="checkbox"/> | 2021/03/07 12:47:34 | 0906180674   | .tw/Qk8O (四大超商/亞太門市/線上繳款) *超商補單繳費：「7-11 ... | ▼ |
| <input type="checkbox"/> | 2021/03/07 21:44:20 | 923          | 親愛的用戶，您的數據用量已達70%，約剩下2.34 GB，建議您可...        | ▼ |
| <input type="checkbox"/> | 2021/03/07 21:44:20 | 923          | 9元/4GB或至官網加購其他用量補充包，加購完成後繼續使用4G...          | ▼ |
| <input type="checkbox"/> | 2021/02/06 14:35:58 | 0906180066   | 【牛年開運上網優惠 亞太用戶權益通知】2/6-2/9登錄只要 \$ 88，...    | ▼ |
| <input type="checkbox"/> | 2021/02/06 14:35:58 | 0906180066   | ，給你睇取超好康！亞太電信限定此門號優惠，轉發無效 - 登錄網...          | ▼ |
| <input type="checkbox"/> | 2021/02/09 14:35:15 | 0906180066   | 【牛年開運上網優惠 亞太用戶最後4天權益通知】2/9前登錄只要...          | ▼ |

# 4 Configuring the Advanced Settings

## 4.1 Wireless

### 4.1.1 General

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

| General  | WPS   | WDS | Wireless MAC Filter | RADIUS Setting | Professional |
|--|---|-----|---------------------|----------------|--------------|
| <b>Wireless - General</b>                      |   |     |                     |                |              |
| Set up the wireless related information below. |   |     |                     |                |              |
| Band   | 2.4GHz  |     |                     |                |              |
| SSID   | ASUS  |     |                     |                |              |
| Hide SSID                                      | <input type="radio"/> Yes <input checked="" type="radio"/> No |     |                     |                |              |
| Wireless Mode                                  | Auto <input checked="" type="checkbox"/> b/g Protection       |     |                     |                |              |
| Channel bandwidth                              | 40 MHz  |     |                     |                |              |
| Control Channel                                | 3   |     |                     |                |              |
| Extension Channel                              | Above   |     |                     |                |              |
| Authentication Method                          | WPA2-Personal   |     |                     |                |              |
| WPA Encryption                                 | AES   |     |                     |                |              |
| WPA Pre-Shared Key                             | 99999999  |     |                     |                |              |
| Network Key Rotation Interval                  | 3600  |     |                     |                |              |
| <b>Apply</b>                                   |   |     |                     |                |              |

#### To configure the basic wireless settings:

1. From the navigation panel, go to **Advanced Settings > Wireless > General** tab.
2. Configure wireless basic configuration for 2.4GHz or 5GHz frequency band.
3. In the **SSID** field, 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.

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. In the **Wireless Mode** field, 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, 802.11b and 802.11a 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.
  - **b/g Protection:** Tick b/g Protection to allow wireless router protect 802.11n transmissions performance from legacy devices with 802.11g, 802.11b connection.
6. In the **Control Channel** field, 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. In the **Channel bandwidth** field, select any of these channel bandwidth to accommodate higher transmission speeds:
  - **20/40MHz** (default): Select this bandwidth to automatically select the best bandwidth for your wireless environment. In 5GHz band, the default bandwidth **20/40/80MHz** is selected.
  - **80MHz:** Select this bandwidth to maximize the wireless throughput of 5GHz radio.
  - **40MHz:** Select this bandwidth to maximize the wireless throughput of 2.4GHz radio.
  - **20MHz:** Select this bandwidth if you encounter some issues with your wireless connection.
8. If **20/40/80MHz**, **20/40MHz**, **40MHz** or **80MHz** is selected, you can define a upper or lower adjacent channel in the **Extension Channel** field to be accommodated
9. In the **Authentication Method** field, select any of these authentication methods:

- **Open System:** This option provides no security.
- **WPA2-Personal / WPA Auto-Personal:** This option provides strong security. You can use either WPA2-Personal (with AES) or WPA Auto-Personal (with AES or TKIP + AES). If you select this option, you must enter the WPA Pre-Shared Key (network key).
- **WPA2 Enterprise / WPA Auto-Enterprise:** This option provides very strong security. It is with integrated EAP server or an external RADIUS back-end authentication server.

11. 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.

| General  | WPS                                     | WDS | Wireless MAC Filter | RADIUS Setting | Professional |
|--|---|-----|---------------------|----------------|--------------|
| <b>Wireless - WPS</b>  |   |     |                     |                |              |
| WPS (Wi-Fi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button. |   |     |                     |                |              |
| Enable WPS   | <input type="checkbox"/> OFF            |     |                     |                |              |
| Current Frequency  | 2.4GHz <a href="#">Switch Frequency</a> |     |                     |                |              |
| Connection Status  | Not used                                |     |                     |                |              |
| Configured   | Yes                                     |     |                     |                |              |
| AP PIN Code  | <input type="text" value="31257367"/>   |     |                     |                |              |

| General  | WPS                                   | WDS | Wireless MAC Filter | RADIUS Setting | Professional |
|--|---------------------------------------|-----|---------------------|----------------|--------------|
| <b>Wireless - WPS</b>  |                                       |     |                     |                |              |
| WPS (Wi-Fi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button. |                                       |     |                     |                |              |
| Enable WPS   | <input type="checkbox"/> OFF          |     |                     |                |              |
| Current Frequency  | 5GHz <a href="#">Switch Frequency</a> |     |                     |                |              |
| Connection Status  | Not used                              |     |                     |                |              |
| Configured   | Yes                                   |     |                     |                |              |
| AP PIN Code  | <input type="text" value="31257367"/> |     |                     |                |              |

## 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 and 5GHz radio separately.
4. You can use any of the following WPS methods for wireless connection pairing:
  - **PBC (Push Button Configuration) Mode:**
    - Hardware PBC on the router: Press the physical WPS button on wireless router, and then press WPS button on wireless client in three (3) minutes.
    - Software PBC on the router: Tick <Push button> on **WPS Method** field, click **Start**, and then press the WPS button on the wireless client in three (3) minutes.
  - **PIN Code Mode:**
    - Pairing from the wireless client: Press the WPS button on the wireless router, and then perform WPS connection process in PIN code mode and enter the **AP PIN Code** on the client device.
    - Pairing from the wireless router: Press the WPS button on wireless client, and then perform the WPS connection process in PIN code mode and enter the **Client PIN Code** on the **WPS Method > Client PIN Code** field. Check if the PIN code is correct and then click **Start** to pair with wireless client.

---

### NOTES:

- WPS supports authentication using Open System and WPA2-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Personal, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.
- Check your wireless device or its user manual for the location of the WPS button.
- During the WPS process, the wireless router scans for any available WPS devices. If the wireless router does not find any WPS devices, it switches to idle mode.
- The router's power LED indicators quickly flash three minutes until the WPS setup is completed.

### 4.1.3 WDS

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 > WDS** tab.

General WPS **WDS** Wireless MAC Filter RADIUS Setting Professional

#### Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your 4G-AC55U to connect to an access point wirelessly. WDS may also be considered a repeater mode. But with this method, the devices connected to the access point will only be able to use half of the access point's original wireless speed.

Note: The function only support [Open System/NONE, Open System/WEP] security authentication method.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

#### Basic Config

|                        |   |
|------------------------|---|
| 2.4GHz MAC             | AC:9E:17:56:6F:48   |
| 5GHz MAC               | AC:9E:17:56:6F:4C   |
| Band                   | 2.4GHz  |
| AP Mode                | AP Only   |
| Connect to APs in list | <input checked="" type="radio"/> Yes <input type="radio"/> No |

#### Remote AP List (Max Limit : 4)

| Remote AP List       | Add / Delete                     |
|----------------------|----------------------------------|
| <input type="text"/> | <input type="button" value="⊕"/> |

No data in table.

2. Select the band for the wireless bridge.
3. In the **AP Mode** field, select any of these options:
  - **AP Only**: Disables the WDS function.
  - **WDS Only**: Enables the WDS 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.
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. 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
6. Click **Apply**.

---

**NOTES:**

- In Hybrid mode, wireless devices connected to the ASUS wireless router only receives half the connection speed of the Access Point.
  - Any Access Point added to the list should be on the same Control Channel and the same fixed Channel bandwidth as the local ASUS wireless router. You can modify the Control Channel from **Advanced Settings > Wireless > General** tab.
-

## 4.1.4 Wireless MAC Filter

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

General WPS WDS **Wireless MAC Filter** RADIUS Setting Professional

### Wireless - Wireless MAC Filter

Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

**Basic Config**

Band: 2.4GHz

Enable MAC Filter:  Yes  No

MAC Filter Mode: Accept

MAC filter list (Max Limit : 64)

| MAC filter list | Add / Delete |
|-----------------|--------------|
|                 |              |

No data in table.

Apply

### To set up the Wireless MAC filter:

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

## 4.1.5 RADIUS Setting

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

The screenshot shows the 'RADIUS Setting' tab in a wireless router's configuration interface. The page title is 'Wireless - RADIUS Setting'. Below the title is a descriptive paragraph: 'This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise/ WPA2-Enterprise/ Radius with 802.1x".' The configuration fields are: 'Band' set to '2.4GHz', 'Server IP Address' (empty), 'Server Port' set to '1812', and 'Connection Secret' (empty). An 'Apply' button is located at the bottom right of the form.

### To set up the wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to **WPA-Auto-Enterprise** or **WPA2-Enterprise**.

---

**NOTE:** Please refer to section **4.1.1 General** 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 **Server Port** field, key in the server port.
6. In the **Connection Secret** field, assign the password to access your RADIUS server.
7. Click **Apply**.

## 4.1.6 Professional

The Professional screen provides advanced configuration options.

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

| General  | WPS   | WDS | Wireless MAC Filter | RADIUS Setting | Professional |
|--|---|-----|---------------------|----------------|--------------|
| <b>Wireless - Professional</b>   |   |     |                     |                |              |
| Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.<br><i>* Reminder: The System time zone is different from your locale setting.</i> |   |     |                     |                |              |
| Band   | 5GHz  |     |                     |                |              |
| Enable Radio   | <input checked="" type="radio"/> Yes <input type="radio"/> No |     |                     |                |              |
| Enable wireless scheduler  | <input type="radio"/> Yes <input checked="" type="radio"/> No |     |                     |                |              |
| Set AP Isolated  | <input type="radio"/> Yes <input checked="" type="radio"/> No |     |                     |                |              |
| Enable IGMP Snooping   | Disable   |     |                     |                |              |
| Multicast Rate(Mbps)   | Auto  |     |                     |                |              |
| Preamble Type  | Long  |     |                     |                |              |
| RTS Threshold  | 2347  |     |                     |                |              |
| DTIM Interval  | 1   |     |                     |                |              |
| Beacon Interval  | 100   |     |                     |                |              |
| Enable TX Bursting   | Disable   |     |                     |                |              |
| Enable Packet Aggregation  | Enable  |     |                     |                |              |
| Enable WMM   | Enable  |     |                     |                |              |
| Enable WMM No-Acknowledgement  | Disable   |     |                     |                |              |
| Enable WMM APSD  | Enable  |     |                     |                |              |
| Enable WMM DLS   | Disable   |     |                     |                |              |
| Airtime Fairness   | Disable   |     |                     |                |              |
| Multi-User MIMO  | Enable  |     |                     |                |              |
| 802.11ac Beamforming   | Enable  |     |                     |                |              |
| Universal Beamforming  | Disable   |     |                     |                |              |
| Tx power adjustment  | <input type="range"/> Performance                             |     |                     |                |              |
| <b>Apply</b>   |   |     |                     |                |              |

In the **Professional Setting** 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:** Select **Yes** to enable wireless networking by the following schedule rules. Select **No** to disable the schedule rules.
- **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 you want to create a public wireless network that only allow guests to access the Internet. Select **Yes** to enable this feature or select **No** to disable.
- **Roaming Assistant:** When your wireless environment has provisioned a several APs (access point) or wireless repeaters to cover all wireless dead zones. When a client that connected on AP1 moves from one place with better signal to another with poor signal, but there is an another signal from AP2. To prevent the client stick on AP1, you can enable Roaming Assistant, and set a minimal RSSI value as threshold. When the connection quality lower than the threshold, AP1 disconnect the wireless client so that it can reevaluate the wireless environment to select a AP with the best signal quality, such as AP2.
- **Enable IGMP Snooping:** When IGMP snooping is enabled, multicast traffic is only forwarded to wireless clients that are members of a specific multicast group.
- **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:** In 802.11n or 802.11ac using a method, A-MPDU, to aggregate short packet into a longer packet for the same MAC address. When a wireless device ready for transmission sends a RTS (Request to Send). After enabling AMPDU RTS, every AMPDU frame send with RTS process.
- **RTS Threshold:** Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval:** DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval:** Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting:** Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.
- **Enable WMM APSD:** WMM APSD (Automatic Power Save Delivery) is the enhancement to the legacy power saver mode. Enable WMM APSD, the wireless AP manages radio usage to help increase battery life for battery-powered wireless clients, such as smartphone and laptop. APSD automatically changes to use a longer beacon interval when the traffic does not require a short packet exchange interval.

## 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.

The screenshot shows the 'LAN - DHCP Server' configuration page. At the top, there are navigation tabs: LAN IP, DHCP Server (selected), Route, IPTV, and Switch Control. Below the tabs, the page title is 'LAN - DHCP Server'. A descriptive paragraph explains that DHCP (Dynamic Host Configuration Protocol) is used for automatic configuration on IP networks, allowing the server to assign IP addresses and inform clients of DNS server and default gateway IP addresses. A link for 'Manually Assigned IP around the DHCP list FAQ' is provided. The configuration is divided into several sections: 'Basic Config' with fields for 'Enable the DHCP Server' (radio buttons for Yes/No, 'Yes' is selected), '4G-AC55U's Domain Name' (text box), 'IP Pool Starting Address' (text box with '192.168.1.2'), 'IP Pool Ending Address' (text box with '192.168.1.254'), 'Lease time' (text box with '86400'), and 'Default Gateway' (text box). 'DNS and WINS Server Setting' includes 'DNS Server' and 'WINS Server' text boxes. 'Enable Manual Assignment' has 'Enable Manual Assignment' radio buttons (No is selected). Below this is a table for 'Manually Assigned IP around the DHCP list (Max Limit : 64)' with columns for 'MAC address', 'IP Address', and 'Add / Delete'. The table is currently empty, showing 'No data in table.' and an 'Apply' button at the bottom.

### 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 WINS 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.

LAN IP DHCP Server **Route** IPTV Switch Control

### LAN - Route

This function allows you to add routing rules into 4G-AC55U. It is useful if you connect several routers behind 4G-AC55U to share the same connection to the Internet.

**Basic Config**

Enable static routes  Yes  No

Static Route List (Max Limit : 32)

| Network/Host IP | Netmask | Gateway | Metric | Interface | Add / Delete |
|-----------------|---------|---------|--------|-----------|--------------|
|                 |         |         |        | LAN       | +            |

No data in table.

Apply

### 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.

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. The 'IPTV' tab is selected. Below the tabs, there is a title 'LAN - IPTV' and a note: 'To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.' The configuration area is divided into two sections: 'Port' and 'Special Applications'. In the 'Port' section, 'Select ISP Profile' is set to 'None' and 'Choose IPTV STB Port' is also set to 'None'. In the 'Special Applications' section, 'Use DHCP routes' is set to 'Microsoft', 'Enable multicast routing (IGMP Proxy)' is set to 'Disable', 'Enable efficient multicast forwarding (IGMP Snooping)' is set to 'Disable', and 'UDP Proxy (Udpsy)' is set to '0'. An 'Apply' button is located at the bottom right of the configuration area.

## 4.2.5 Switch Control

Switch Control tab enables you to configure NAT Acceleration and Jumbo frame to improve network performance. We recommend that you do not change the default route settings unless you have advanced knowledge.

The screenshot shows the 'LAN - Switch Control' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. The 'Switch Control' tab is selected. Below the tabs, there is a title 'LAN - Switch Control' and a note: 'Setting 4G-AC55U switch control.' The configuration area contains two settings: 'NAT Acceleration(IPv4 Only)' is set to 'Enable' and 'Enable Jumbo Frame' is set to 'Disable'. An 'Apply' button is located at the bottom right of the configuration area.

## 4.3 WAN

### 4.3.1 Internet Connection

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

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

#### WAN - Internet Connection

4G-AC55U supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

**WAN Index**

WAN Type: WAN

**Basic Config**

WAN Connection Type: Automatic IP

Enable WAN: Yes No

Enable NAT: Yes No

Enable UPnP: UPnP\_FAQ Yes No

**WAN DNS Setting**

Connect to DNS Server automatically: Yes No

**Account Settings**

Authentication: None

**Special Requirement from ISP**

Host Name: [Text Field]

MAC Address: [Text Field] **MAC Clone**

DHCP query frequency: Aggressive Mode

**Apply**

#### 4.3.1.1 WAN

**To configure the WAN connection settings:**

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

- **Enable WAN:** Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.
- **Enable NAT:** NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Enable UPnP:** UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- **Connect to DNS Server automatically:** 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.
- **DHCP query frequency:** Changes the DHCP Discovery interval settings to avoid overloading the DHCP server.

### 4.3.1.2 Mobile broadband

4G-AC86U has build in 3G/4G modem that allows you to use a Mobile Broadband connection for Internet access.

#### To set up your Mobile broadband Internet access:

1. From the navigation panel, go to **Advanced Settings > WAN > Internet Connection** tab, select the **Mobile Broadband** in **WAN Interface** field.

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

#### WAN - Mobile Broadband

4G-AC86U can establish Internet connection via Ethernet WAN, Mobile Broadband or LAN as WAN. Select the interface for your Internet connection from the WAN Interface dropdown list. You can enable the dual WAN connection and change the priorities of the WAN interfaces from the [Dual WAN] tab.

| WAN Index               |                  |
|-------------------------|------------------|
| WAN Interface           | Mobile Broadband |
| Enable Mobile Broadband | Enable           |

| Mobile Broadband Modem Information |   |
|------------------------------------|---|
| Modem software version             | EM12GPAR01A18M4G <span>Reset Modem</span> <span>Reboot Modem</span> |
| IMEI                               | 355219110000082   |

2. In the **Enable Mobile Broadband** field, select **Enable**.
3. Check that you have properly inserted the SIM card, and configure the mobile settings of your router.

|  |   |
|--|---|
| WAN Index  |   |
| WAN Interface  | Mobile Broadband ▾  |
| Enable Mobile Broadband                              | Enable ▾  |
| Mobile Broadband Modem Information                   |   |
| Modem software version                               | EM12GPAR01A21M4G <b>Reset Modem</b> <b>Reboot Modem</b>                                     |
| IMEI   | 355219110000084   |
| Configure the Mobile Broadband settings of 4G-AC86U. |   |
| Internet Connection                                  |   |
| Connection status                                    | Connected  |
| Network Type   | Auto ▾  |
| PDP Type   | IPv4 ▾  |
| LTE Band   | Auto ▾  |
| Roaming  | Disable ▾   |

#### 4. Internet Connection Configuration:

1) On **Network Type** field, select your preferred network:

- **Auto** (Default): Select **Auto** to allow the wireless router to automatically select the channel that has the available connection from 4G or 3G network.
- **4G only**: Select this option to automatically connect the wireless router to a 4G network only.
- **3G only**: Select this option to automatically connect the wireless router to a 3G network only.

2) **PDP Type**: The wireless router support several PDP Types, PPP, IPv4, IPv6, IPv6 to IPv4.

3) **LTE Band**: This field allows you to select the LTE band.

4) **Roaming** : When you travel to another country, you may use original SIM to access the local network if your ISP provider roaming service in the country. Enable this functions to allow you to access the local network.

- Click **Scan** to show all the available mobile networks.
- Select available mobile network and click **Apply** to connect to it.

---

#### NOTES:

- The LTE Router can detect your ISP based on the IMSI information of your SIM card. If the mobile network from your ISP is not found, connect to a roaming network of other ISPs.
  - Using a roaming service will incur additional charges. Inquire from your mobile service provider before using the roaming service.
-

| Data Usage Limitation |   |
|-----------------------|---|
| Data Usage            | 9.64 MBytes (Starting Day : 1) <span style="float: right;">Clear</span> |
| Cycle Start Day       | 1   |
| Data Usage Limit      | 0 Gbytes (Disable : 0)  |
| Data Usage Alert      | 0 Gbytes (Disable : 0)  |
| Send SMS Notification | Disable   |

## 5. Data Usage Limitation

- **Data Usage:** Show the data usage.
- **Cycle Start Day:** Select the day you wish the data usage to begin to accumulate. The data usage will be reset at the end of each cycle.
- **Data Usage Limit:** Set the monthly maximum volume of traffic (in GB) for Internet usage. When this limit is reached, an exclamation mark and pop-up alert message will show up when you login administration page, and Internet access is blocked.
- **Data Usage Alert:** Set the maximum volume of Internet traffic at which an exclamation mark and pop-up alert message will show up when you login administration page. When your Internet usage reaches this limit, Internet access is not blocked until the Usage Limit is reached.
- **Send SMS Notification:** Enable this function to send an SMS notification from your router to your mobile device once the Data Usage limit for Internet usage is reached.

| APN Profile           |      |
|-----------------------|------|
| APN Configuration     | Auto |
| APN Service(optional) | Gent |
| Dial Number           | *99# |
| Username              |      |
| Password              |      |
| Authentication        | None |

| APN Profile           |                |
|-----------------------|----------------|
| APN Configuration     | Manual Setting |
| Location              | Taiwan         |
| ISP                   | Far EastTone   |
| APN Service(optional) | Internet       |
| Dial Number           | *99#           |
| Username              |                |
| Password              |                |
| Authentication        | None           |

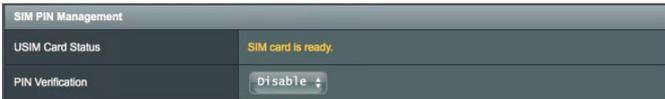
## 6. APN Configuration

- 1) **Auto** (Default): The system selects Auto APN setting by default.
- 2) **Manual**: If the automatic dial-up connection fails, select Manual to configure APN setting manually.
  - A. **Location**: Select your 3G/4G service provider's location from the dropdown list.
  - B. **ISP**: Select your Internet Service Provider (ISP) from the dropdown list.
  - C. **APN (Access Point Name) service (optional)**: Contact your 3G/4G service provider for detailed information.
  - D. **Dial number**: The 3G/4G provider's access number
  - E. **Username / Password**: Enter the username and password that your 3G/4G network provider has provided.

## 7. PIN Configuration

**PIN code:** Enter the 3G/4G provider's PIN code for connection on SIM PIN Management if the SIM card is required.

- The default PIN code may vary with different providers. If your ISP has disabled the PIN code verification by default, you can skip the setting.



| SIM PIN Management |                    |
|--------------------|--------------------|
| USIM Card Status   | SIM card is ready. |
| PIN Verification   | Disable            |

- If your ISP has enabled PIN code verification by default, you will see the SIM lock status icon  on the status icon area and are required to enter the PIN code.



Configure the Mobile Broadband settings of 4G-AC86U.

| SIM PIN Management    |  |
|-----------------------|--|
| USIM Card Status      | PIN code is required.  |
| PIN code              | 1234 <input checked="" type="checkbox"/> Save My PIN <input type="button" value="OK"/> |
| Remaining Attempts: 3 |  |

- You can manually enable the PIN code verification from your router's web GUI or your mobile phone. You are also required to enter the PIN code.



| SIM PIN Management |                                       |
|--------------------|---------------------------------------|
| USIM Card Status   | SIM card is ready.                    |
| PIN Verification   | Enable                                |
| PIN Modification   | <input type="button" value="Modify"/> |



**SIM PIN Management - PIN Verification**

Please input the PIN code obtained from the internet service provider.

|                        |                      |
|------------------------|----------------------|
| PIN code               | <input type="text"/> |
| PIN Remaining Attempts | 2                    |

# Mobile Connection Status

## To find Mobile broadband Information:

- 1. Click  to find the detailed information.

| Internet Connection |   |
|---------------------|---|
| Connection status   | Connected  |
| Network Type        | Auto  |
| PDP Type            | IPv4  |
| LTE Band            | Auto  |
| Roaming             | Disable   |

- 2. The **Mobile Connection Status** screen displays the detailed Mobile Broadband connection status.

### WAN - Mobile Connection Status

This page displays basic device information, internet connection status and internet usage.

| Product Information |                  |
|---------------------|------------------|
| Model Name          | 4G-AC86U         |
| IMSI                | 466056008449     |
| ICCID               | 8988605101902049 |
| Phone Number        | +88690697        |

| Wireless Status |             |
|-----------------|-------------|
| Cell ID         | 1B60134     |
| Connection Type | TDD LTE     |
| Band            | LTE BAND 38 |
| RSSI            | -58 dBm     |
| SINR            | 11 dB       |
| RSRP            | -94 dBm     |
| RSRQ            | -13 dBm     |

| Internet Usage    |   |
|-------------------|---|
| Connection Status |  Connected |
| SIM Provider      | KGT-Online  |
| Network Provider  | LTE GT  |
| Data Usage        | 212.514 MBytes  |
| Data Sent         | 8.841 MBytes  |
| Data Received     | 203.673 MBytes  |
| Data Sent/Sec     |   |
| Data Received/Sec |   |
| Connection Time   | 0 days 0 hour(s) 28 minute(s) 22 seconds  |

**Close**

### 4.3.2 IPv6 (Internet Settings)

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.

The screenshot shows the IPv6 configuration page for a 4G-AC86U router. The page is titled "IPv6" and includes a sub-header "Configure the IPv6 Internet setting of 4G-AC86U." and a link to "IPv6\_FAQ". The configuration is organized into several sections:

- Basic Config:** The "Connection type" is set to "Static IPv6".
- IPv6 WAN Setting:** Fields for "WAN IPv6 Address", "WAN Prefix Length", and "WAN IPv6 Gateway".
- IPv6 LAN Setting:** Fields for "LAN IPv6 Address", "LAN Prefix Length", and "LAN IPv6 Prefix". The "Auto Configuration Setting" is set to "Stateless".
- IPv6 DNS Setting:** Fields for "IPv6 DNS Server 1", "IPv6 DNS Server 2", and "IPv6 DNS Server 3".
- Auto Configuration Setting:** The "Enable Router Advertisement" option is checked.

An "Apply" button is located at the bottom of the page.

#### 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**.

---

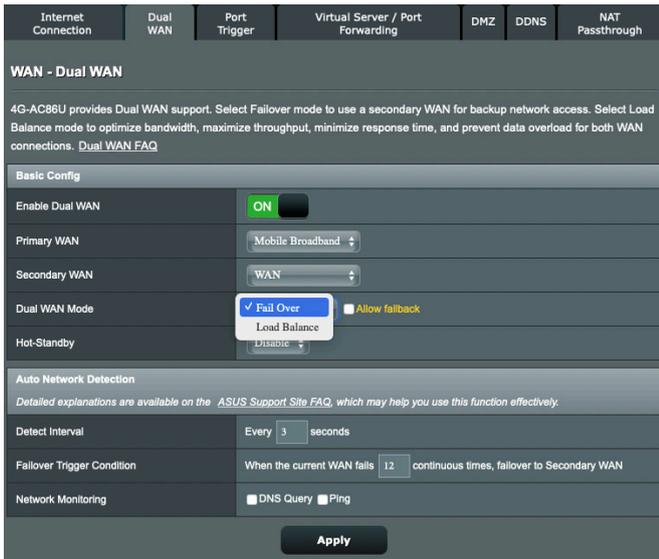
**NOTE:** Please refer to your ISP regarding specific IPv6 information for your Internet service.

---

### 4.3.3 Dual WAN

Your ASUS wireless router provides dual WAN support. You can set the dual WAN feature to any of these two modes:

- **Fail Over:** Select this mode to use the secondary WAN as the backup network access.
- **Load Balance:** Select this mode to allow concurrent use of dual WAN connections for improved bandwidth and reliability.
- **Allow failback:** Tick the checkbox to allow Internet connection switch back to primary WAN automatically when primary WAN becomes available.



- **Detect Interval:** Set the time interval (in seconds) between two ping packets.
- **Failover Trigger Condition:** Set the continuous times when the system triggers the failover or failback action after reaching the ping test counter and getting no response from the target IP address.

- **Network Monitoring**

- 1) **DNS Query:** Select this option if you want to periodically resolve target FQDN (Fully Qualified Domain Name).

|                       |   |
|-----------------------|---|
| Network Monitoring    | <input checked="" type="checkbox"/> DNS Query <input type="checkbox"/> Ping |
| Resolve Hostname      | <input type="text" value="dns.msftncs1.com"/>                               |
| Resolved IP Addresses | <input type="text" value="131.107.255.255 112.4.20.71 fd3e:4f5a:5b81::1"/>  |

- 2) **Ping:** Select this option if you want to periodically ping test packet domain or IP address.

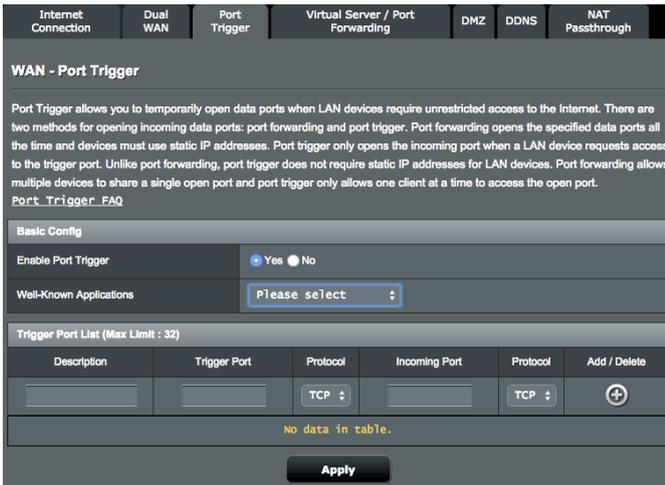
|                    |   |
|--------------------|---|
| Network Monitoring | <input type="checkbox"/> DNS Query <input checked="" type="checkbox"/> Ping |
| Ping Target        | <input type="text" value="www.facebook.com"/> ▼                             |

If internet connection issue occurs due to DHCP lease problem such as IP address being expired, you can enable DNS Query or Ping to alleviate the problem.

### 4.3.4 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. On the **Enable Port Trigger** field, tick **Yes**.
3. On the **Well-Known Applications** field, select the popular games and web services to add to the Trigger Port List.

4. On the **Trigger Port List** table, key in the following information:
  - **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.
5. Click the **Add**  button to enter the port trigger information to the list. Click the **Delete**  button to remove a port trigger entry from the list.
6. When done, click **Apply**.

---

**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.
-

### 4.3.5 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.

Internet Connection | Dual WAN | Port Trigger | **Virtual Server / Port Forwarding** | DMZ | DDNS | NAT Passthrough

#### WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the 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. 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.

- 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 4G-AC55U's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with 4G-AC55U's native FTP server.

[Virtual\\_Server / Port\\_Forwarding\\_FAQ](#)

#### Basic Config

Enable Port Forwarding:  Yes  No

Famous Server List:

Famous Game List:

FTP Server Port:

#### Port Forwarding List (Max Limit : 32)

| Service Name | Port Range | Local IP | Local Port | Protocol | Add / Delete                     |
|--------------|------------|----------|------------|----------|----------------------------------|
|              |            |          |            | TCP      | <input type="button" value="+"/> |

No data in table.

#### To set up Port Forwarding:

1. From the navigation panel, go to **Advanced Settings > WAN > Virtual Server / Port Forwarding** tab.
2. On the **Enable Port Forwarding** field, tick **Yes**.

3. On the **Famous Server List** field, select the type of service you want to access.
4. On the **Famous Game List** field, select the popular game that you want to access. This item lists the port required for your selected popular online game to work properly.
5. On the **Port Forwarding List** table, key in the following information:
  - **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**.

6. Click the **Add**  to enter the port trigger information to the list. Click the **Delete**  button to remove a port trigger entry from the list.
7. When done, click **Apply**.

### **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.

### 4.3.6 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.

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding **DMZ** DDNS NAT Passthrough

#### WAN - DMZ

Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertain incoming ports. Please use it carefully.  
Special Applications: Some applications require special handler against NAT. These special handlers are disabled in default.  
[DMZ\\_FAQ](#)

Enable DMZ  Yes  No

IP Address of Exposed Station

Apply

#### 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**.

### 4.3.7 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.

| Internet Connection  | Dual WAN  | Port Trigger | Virtual Server / Port Forwarding | DMZ | DDNS | NAT Passthrough |
|--|---|--------------|----------------------------------|-----|------|-----------------|
| <b>WAN - DDNS</b>  |   |              |                                  |     |      |                 |
| DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services. |   |              |                                  |     |      |                 |
| The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x).  |   |              |                                  |     |      |                 |
| This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.   |   |              |                                  |     |      |                 |
| Enable the DDNS Client   | <input checked="" type="radio"/> Yes <input type="radio"/> No |              |                                  |     |      |                 |
| Server   | www.asus.com  |              |                                  |     |      |                 |
| Host Name  | Key in the name .asuscomm.com                                 |              |                                  |     |      |                 |
| <b>Apply</b>   |   |              |                                  |     |      |                 |

#### 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.
-

## 4.3.8 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:

1. Go to the **Advanced Settings > WAN > NAT Passthrough** tab.
2. Select **Enable** or **Disable** for specific traffic pass through the NAT firewall.
3. When done, click **Apply**.

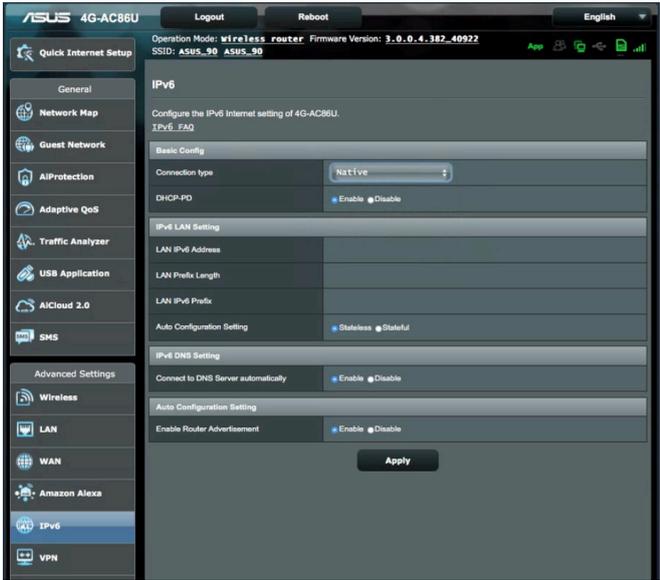
The screenshot shows the 'WAN - NAT Passthrough' configuration page. At the top, there are navigation tabs: 'Internet Connection', 'Dual WAN', 'Port Trigger', 'Virtual Server / Port Forwarding', 'DMZ', 'DDNS', and 'NAT Passthrough'. Below the tabs, the page title is 'WAN - NAT Passthrough'. A descriptive text reads: 'Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.' The main configuration area contains a table with the following settings:

|                   |         |
|-------------------|---------|
| PPTP Passthrough  | Enable  |
| L2TP Passthrough  | Enable  |
| IPSec Passthrough | Enable  |
| RTSP Passthrough  | Enable  |
| H.323 Passthrough | Enable  |
| SIP Passthrough   | Enable  |
| PPPoE Relay       | Disable |
| FTP_ALG Port      | 2021    |

At the bottom of the configuration area, there is an 'Apply' button.

## 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 for 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**.

---

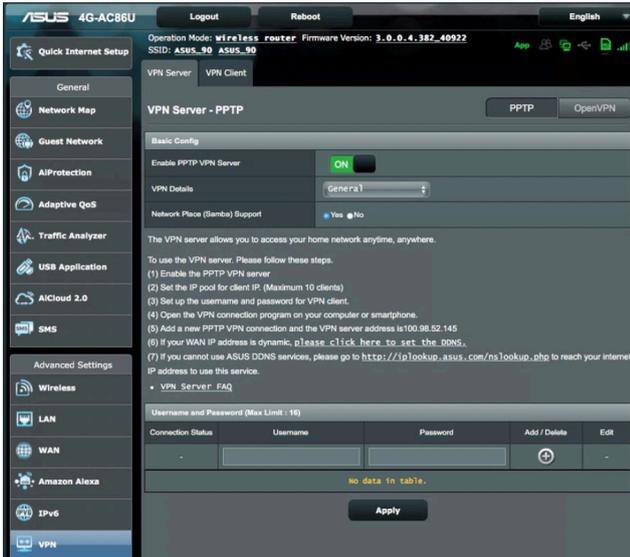
**NOTE:** Please refer to your ISP regarding specific IPv6 information for your Internet service.

---

## 4.5 VPN Server

VPN (Virtual Private Network) provides a secure communication to a remote computer or remote server 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 VPN Server** field, select **ON** to enable PPTP VPN Server.
3. On the **VPN Details** dropdown list, select **Advanced Settings** if want to configure advanced VPN settings such as broadcast support, authentication, MPPE Encryption, and Client IP address range.
4. On the **Network Place (Samba) Support** field, select **Yes**.
5. Enter the user name and password for accessing the VPN server. Click the  button.
6. Click **Apply**.

## 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.

#### To set up a keyword filter:

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

---

#### NOTES:

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

## 4.6.4 Network Services Filter

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

### To set up a Network Service filter:

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

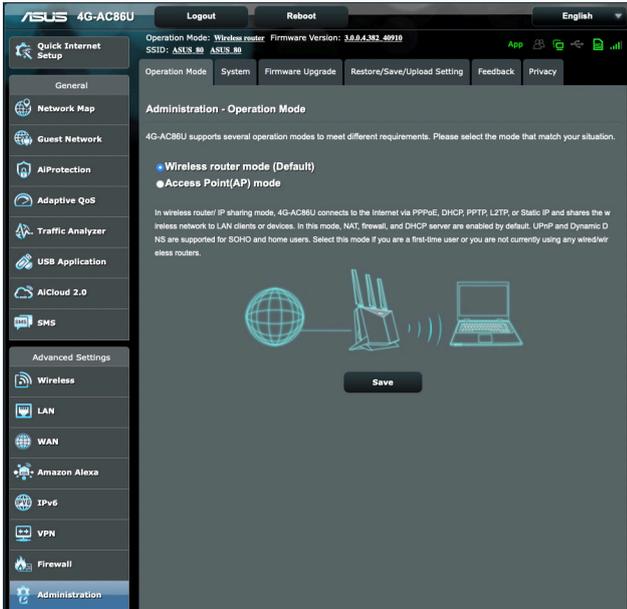
## 4.6.5 IPv6 Firewall

By default, your ASUS wireless router blocks all unsolicited incoming traffic. The IPv6 Firewall function allows incoming traffic coming from specified services to go through your network.

## 4.7 Administration

### 4.7.1 Operation Mode

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



#### To set up the operating mode:

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

---

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

---

## 4.7.2 System

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

| Operation Mode  | System   | Firmware Upgrade | Restore/Save/Upload Setting | Feedback | Privacy                  |
|---|--|------------------|-----------------------------|----------|--------------------------|
| <b>Administration - System</b>  |  |                  |                             |          |                          |
| Change the router login password, time zone, and NTP server settings. |  |                  |                             |          |                          |
| <b>Change the router login password</b>                               |  |                  |                             |          |                          |
| Router Login Name   | <input type="text" value="admin"/>   |                  |                             |          |                          |
| New password  | <input type="password"/>   |                  |                             |          |                          |
| Retype Password   | <input type="password"/> <input type="checkbox"/> Show password  |                  |                             |          |                          |
| Enable Login Captcha  | <input checked="" type="radio"/> Yes <input type="radio"/> No  |                  |                             |          |                          |
| <b>Basic Config</b>   |  |                  |                             |          |                          |
| Time Zone   | <input type="text" value="(GMT) Greenwich Mean Time"/> <input type="button" value="v"/><br><small>* Reminder: The System time zone is different from your locale setting.</small>                    |                  |                             |          |                          |
| NTP Server  | <input type="text" value="pool.ntp.org"/>  |                  |                             |          | <a href="#">NTP Link</a> |
| Network Monitoring  | <input checked="" type="checkbox"/> DNS Query <input type="checkbox"/> Ping  |                  |                             |          |                          |
| Auto Logout   | <input type="text" value="30"/> minute(s) (Disable : 0)  |                  |                             |          |                          |
| Enable WAN down browser redirect notice                               | <input checked="" type="radio"/> Yes <input type="radio"/> No  |                  |                             |          |                          |
| WPS Button behavior   | <input checked="" type="radio"/> Activate WPS <input type="radio"/> Toggle Radio <input type="radio"/> Turn LED On/Off   |                  |                             |          |                          |
| Enable Reboot Scheduler   | <input type="radio"/> Yes <input checked="" type="radio"/> No  |                  |                             |          |                          |
| <b>Service</b>  |  |                  |                             |          |                          |
| Enable Telnet   | <input checked="" type="radio"/> Yes <input type="radio"/> No<br><small>* Due to security concerns, we suggest using SSH instead of Telnet. SSH provides an encrypted network communication.</small> |                  |                             |          |                          |
| Enable SSH  | <input type="text" value="No"/> <input type="button" value="v"/>   |                  |                             |          |                          |
| Idle Timeout  | <input type="text" value="20"/> minute(s) (Disable : 0)  |                  |                             |          |                          |
| <b>Local Access Config</b>  |  |                  |                             |          |                          |
| Authentication Method   | <input type="text" value="HTTP"/> <input type="button" value="v"/>   |                  |                             |          |                          |
| <b>Remote Access Config</b>   |  |                  |                             |          |                          |
| Enable Web Access from WAN  | <input type="radio"/> Yes <input checked="" type="radio"/> No  |                  |                             |          |                          |
| Enable Access Restrictions  | <input type="radio"/> Yes <input checked="" type="radio"/> No  |                  |                             |          |                          |
| <input type="button" value="Apply"/>                                  |  |                  |                             |          |                          |

## 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 the router login password:** You can change the password and login name for the wireless router by entering a new name and password.
  - **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.
  - **Auto Logout:** System will auto log out the administration page after an idle period. To disable Auto logout, set the value in 0.
  - **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.
  - **Enable Access Restrictions:** Select Yes to set a whitelist which allows administrator to limit and control access only to trusted IP address.
    - a). **Allow only specified IP address:** Click Yes if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
    - b). **Specified IP Address:** Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This Client list allows you to add the maximum IP addresses of 4.
3. Click **Apply**.

## 4.7.3 Firmware Upgrade

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

| Firmware Version  |  |
|-------------------|--|
| Product ID        | 4G-AC86U   |
| Signature version | 2.220 Updated : 2021/03/16 17:01 <input type="button" value="Check"/>            |
| Firmware Version  | 3.0.0.4.382_40910-g755bc74 <input type="button" value="Check"/>                  |
| New Firmware File | <input type="button" value="選擇檔案"/> 尚未選取檔案 <input type="button" value="Upload"/> |

| 4G Modem Firmware      |  |
|------------------------|--|
| Modem Firmware version | EM12GPAR01A18M4G   |
| New Modem Firmware     | <input type="button" value="選擇檔案"/> 尚未選取檔案 <input type="button" value="Upload"/> |

### To upgrade the router or 4G modem firmware:

1. From the navigation panel, go to **Advanced Settings > Administration > Firmware Upgrade** tab.
2. In the **New Firmware File** or **New Modem Firmware** 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

|                |        |                  |                             |          |         |
|----------------|--------|------------------|-----------------------------|----------|---------|
| Operation Mode | System | Firmware Upgrade | Restore/Save/Upload Setting | Feedback | Privacy |
|----------------|--------|------------------|-----------------------------|----------|---------|

**Administration - Restore/Save/Upload Setting**

This function allows you to save current settings of 4G-AC86U to a file, or load settings from a file.

|                 |                     |   |
|-----------------|---------------------|---|
| Factory default | <b>Restore</b>      | <input type="checkbox"/> Initialize all the settings, and clear all the data log for AIProtection, Traffic Analyzer, and Web History.   |
| Save setting    | <b>Save setting</b> | <input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router. |
| Restore setting | <b>Upload</b>       |   |

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

1. 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 setting**, 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
  - Wireless Log
  - DHCP Leases
  - IPv6 (WAN and LAN network information)
  - Routing Table
  - Port Forwarding
  - Connections

General Log Wireless Log DHCP leases IPv6 Routing Table Port Forwarding Connections

### System Log - General Log

This page shows the detailed system's activities.

System Time **Tue, Mar 16 10:59:11 2021**

Uptime **0 days 0 hour(s) 49 minute(s) 58 seconds**

Remote Log Server

Remote Log Server Port  \* The default port is 514. If you reconfigured the port number, please make sure that the remote log server or IoT devices' settings match your current configuration.

**Apply**

```
Mar 16 10:24:29 kernel: [ 916.551820] McCmdChannelSwitch: control_ch1 = 9,control_ch2=0, central_ch1 = 9 DBDCId
Mar 16 10:24:29 kernel: [ 916.560873] BW = 0,TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:29 kernel: [ 916.707743] McCmdChannelSwitch: control_ch1 = 10,control_ch2=0, central_ch1 = 10 DBDCI
Mar 16 10:24:29 kernel: [ 916.718283] BW = 0,TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:29 kernel: [ 916.867717] McCmdChannelSwitch: control_ch1 = 11,control_ch2=0, central_ch1 = 11 DBDCI
Mar 16 10:24:29 kernel: [ 916.875003] BW = 0,TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.023715] McCmdChannelSwitch: control_ch1 = 12,control_ch2=0, central_ch1 = 12 DBDCI
Mar 16 10:24:30 kernel: [ 917.032866] BW = 0,TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.129716] McCmdChannelSwitch: control_ch1 = 13,control_ch2=0, central_ch1 = 13 DBDCI
Mar 16 10:24:30 kernel: [ 917.188880] BW = 0,TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.335788] scan_ch_restore : restore channel done in non-offchannel scan path
Mar 16 10:24:30 kernel: [ 917.344890] McCmdChannelSwitch: control_ch1 = 8,control_ch2=0, central_ch1 = 10 DBDCI
Mar 16 10:24:30 kernel: [ 917.353992] BW = 1,TXStream = 4, RXStream = 4, scan(0)
Mar 16 10:24:30 kernel: [ 917.362366] [DfsCacNormalStart] Normal start. Enable MAC TX
Mar 16 10:30:10 rc_services: httpd(210)notify_rc start_lockpin 0 0000
Mar 16 10:41:10 kernel: [ 917.437055] scan_ch_restore,central_ch=10,bw=1
Mar 16 10:41:10 kernel: [ 917.437055] #
Mar 16 10:43:28 kernel: [ 2055.628779] entry wcid 1 QosMapSupport=0
Mar 16 10:43:28 kernel: [ 2055.764733] AP SETKEYS DONE - AKMMap=WPA2-Personal, PairwiseCipher=AES, GroupCipher=AE
Mar 16 10:43:28 kernel: [ 2055.764733] #
Mar 16 10:43:28 kernel: [ 2055.778081] PTK:871aac461967aaec6ec12bda5d2c7683ac7193ca18d4016cd18d452381099b7f4d0ca1
Mar 16 10:43:28 kernel: [ 2055.857106] Rcv Wcid(1) AddDAReg
Mar 16 10:43:28 kernel: [ 2055.860358] Start Seq = 00000000
Mar 16 10:43:32 dnsmasq[2091]: failed to execute /sbin/dhpcp lease: No such file or directory
Mar 16 10:43:43 kernel: [ 2070.455804] Rcv Wcid(1) AddDAReg
Mar 16 10:43:43 kernel: [ 2070.459109] Start Seq = 00000002
```

**Clear Save**

## 4.9 Ethernet WAN Mobile Broadband Function Support List

The wireless router supports wired WAN and Mobile broadband WAN in failover and failback modes. The Mobile broadband WAN is used both as Internet access and WAN backup interface. LAN, WAN, VPN, and Firewall support different functions. See the comparison table below.

|   | Wired WAN | LAN as WAN | Mobile broadband |
|---|-----------|------------|------------------|
| <b>LAN</b>  |           |            |                  |
| IPTV  | V         | N/A        | N/A              |
| Switch Control >><br>NAT Acceleration (IPv4 Only) | V         | N/A        | N/A              |
| Switch Control >><br>Jumbo Frame                  | V         | N/A        | N/A              |
| <b>WAN</b>  |           |            |                  |
| IPv6  | V         | V          | V (1)            |
| Port Trigger                                      | V         | V          | V (2)            |
| Virtual Server / Port Forwarding                  | V         | V          | V (2)            |
| DMZ   | V         | V          | V (2)            |
| DDNS  | V         | V          | V (2)            |
| NAT Passthrough                                   | V         | V          | V (2)            |
| <b>Traffic Manager</b>                            |           |            |                  |
| QoS   | V         | V          | V                |
| <b>Firewall</b>                                   |           |            |                  |
| General   | V         | V          | V                |
| URL Filter  | V         | V          | V                |
| Keyword Filter                                    | V         | V          | V                |
| Network Services Filter                           | V         | V          | V                |
| IPv6 Firewall                                     | V         | V          | N/A              |
| <b>Administration</b>                             |           |            |                  |
| System >><br>Enable Web Access from WAN           | V         | V          | V (2)            |

| Applications               |   |   |       |
|----------------------------|---|---|-------|
| AiCloud<br>Access from WAN | V | V | V (2) |
| VPN Server                 | V | V | V (2) |
| FTP Server                 | V | V | V (2) |

---

**NOTES:**

V (1): Mobile WAN has separated configuration on its configuration page

V (2): In most of using case, Internet service provide dispatch the mobile broadband a private IP, that will cause the WAN service failed to access from WAN side.

---

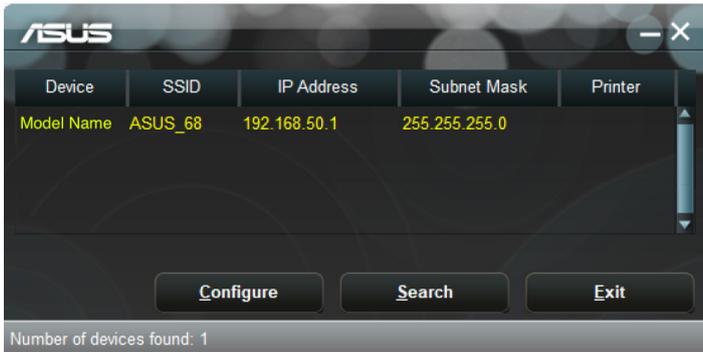
## 5 Utilities

**NOTE:** Download and install the wireless router's utilities from the ASUS website: <https://www.asus.com/support/Download-Center/>

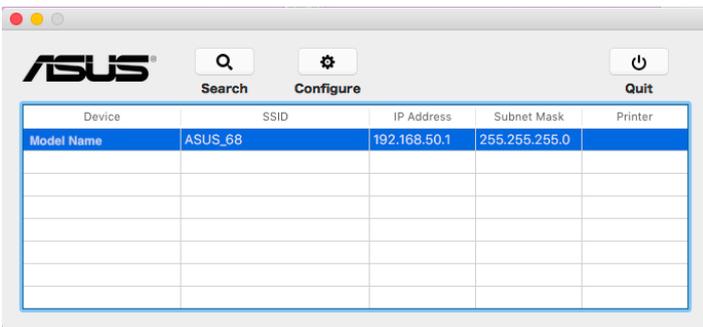
### 5.1 Device Discovery

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

#### Windows:



#### Mac OS:

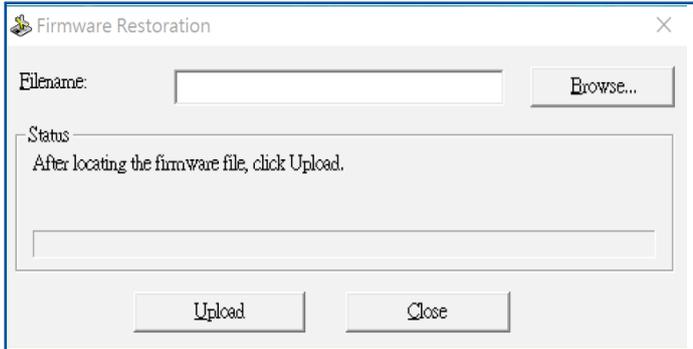


**NOTE:** When you set the router to Access Point mode, you need to use Device Discovery to get the router's IP address.

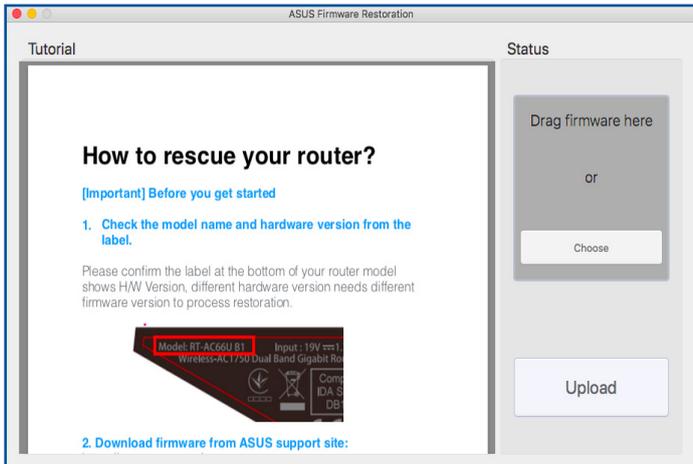
## 5.2 Firmware Restoration

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.

### Windows:



### Mac OS:



---

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

---

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

---

## 5.3 Setting up your printer server

### 5.3.1 ASUS EZ Printer Sharing

ASUS EZ Printing Sharing utility allows you to connect a USB printer to your wireless router's USB port and set up the print server. This allows your network clients to print and scan files wirelessly.



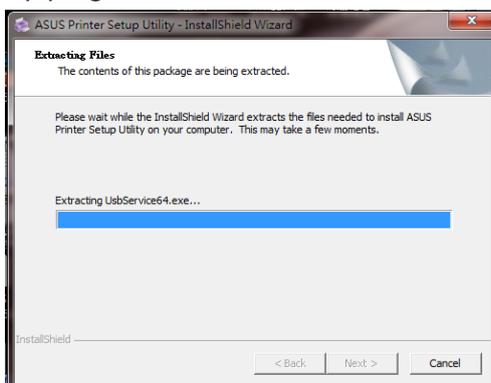
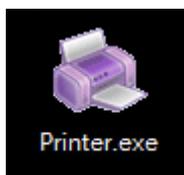
**To set up the EZ Printer sharing mode:**

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

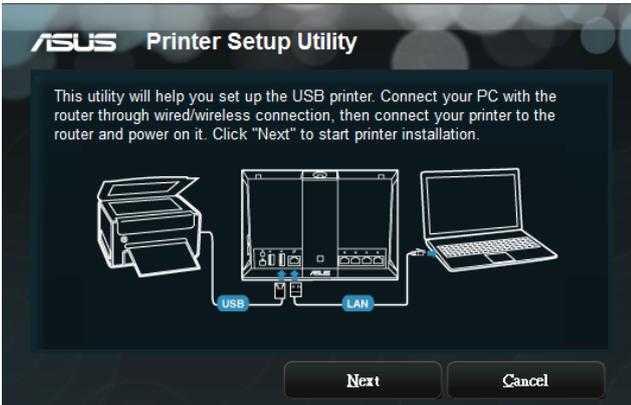


**NOTE:** Network printer utility is supported on Windows® XP, Windows® Vista, and Windows® 7 only. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

3. Unzip the downloaded file and click the Printer icon to run the network printer setup program.



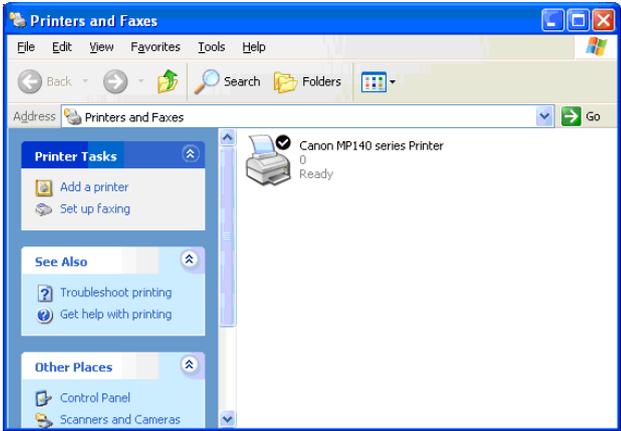
4. Follow the onscreen instructions to set up your hardware, then click **Next**.



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



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



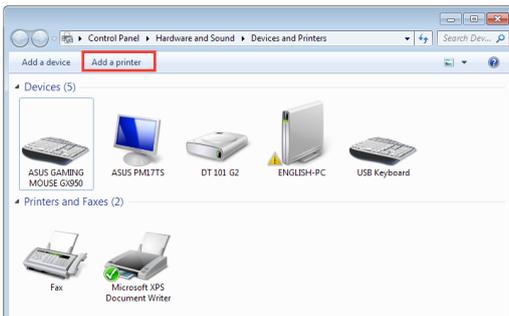
## 5.3.2 Using LPR to Share Printer

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

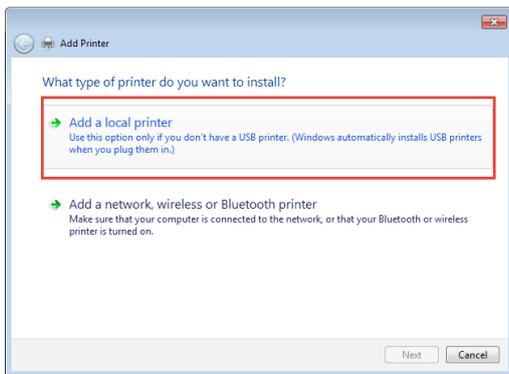
### Sharing your LPR printer

To share your LPR printer:

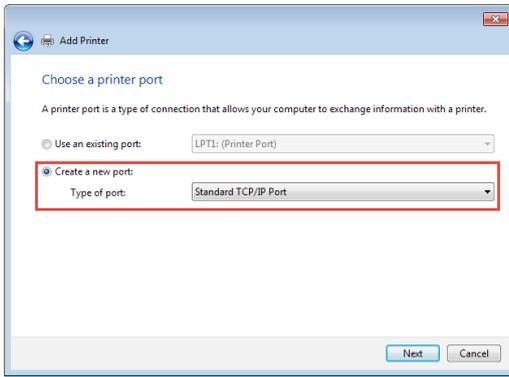
1. From the Windows® desktop, click **Start > Devices and Printers > Add a printer** to run the **Add Printer Wizard**.



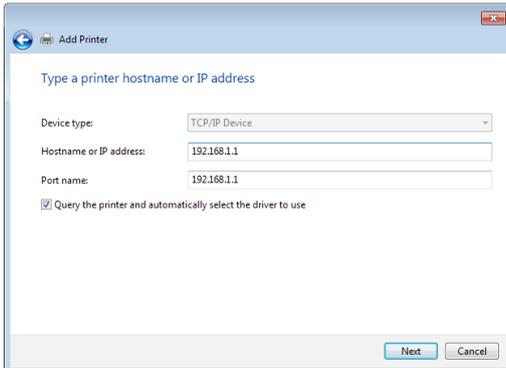
2. Select **Add a local printer** and then click **Next**.



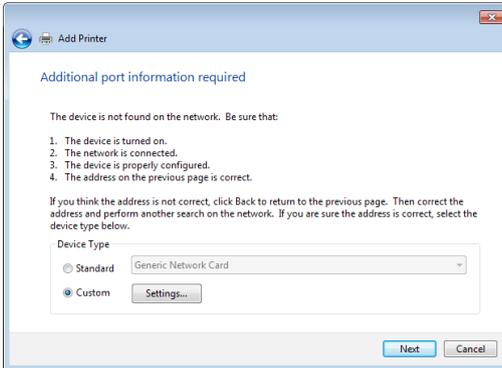
3. Select **Create a new port** then set **Type of Port** to **Standard TCP/IP Port**. Click **New Port**.



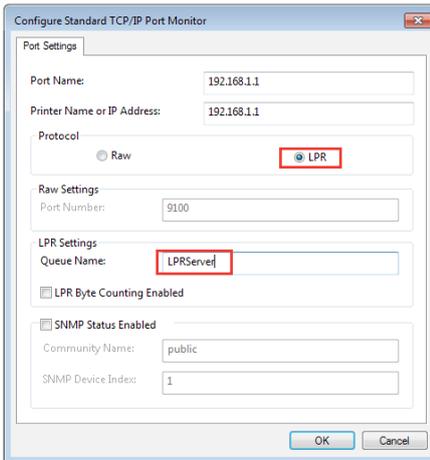
4. In the **Hostname or IP address** field, key in the IP address of the wireless router then click **Next**.



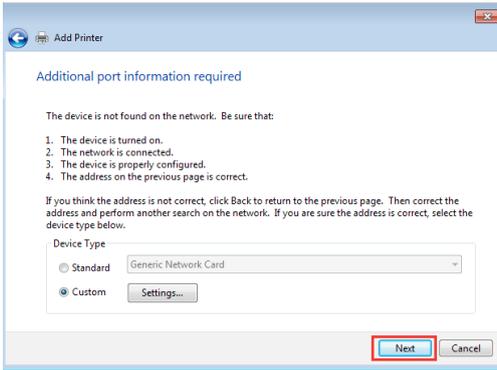
5. Select **Custom** then click **Settings**.



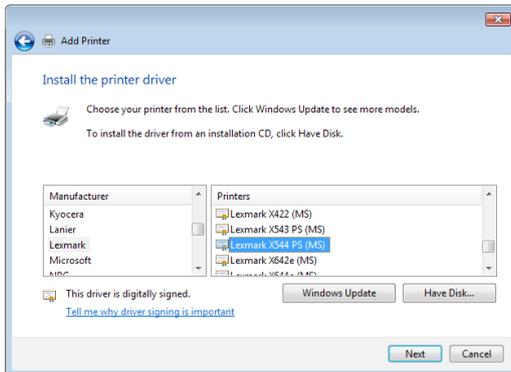
6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.



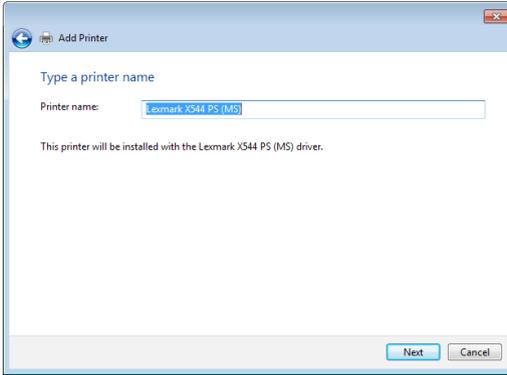
7. Click **Next** to finish setting up the standard TCP/IP port.



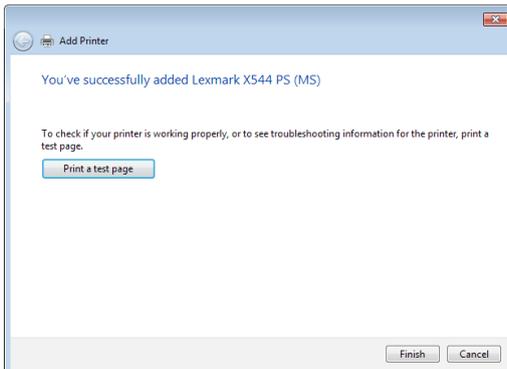
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.



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



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



## 5.4 Download Master

Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

---

**NOTE:** You need a USB device connected to the wireless router to use Download Master.

---

### To use Download Master:

1. Click **General > USB application > Download Master** to download and install the utility automatically.

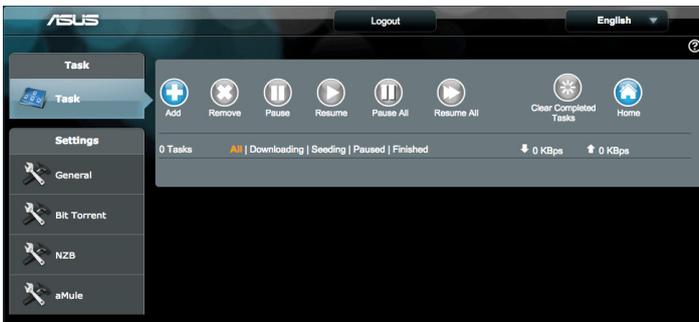
---

**NOTE:** If you have more than one USB drive, select the USB device you want to download the files to.

---



2. After the download process is finished, click the Download Master icon to start using the utility.
3. Click **Add** to add a download task.



4. Select a download type such as BitTorrent, HTTP, or FTP. Provide a torrent file or a URL to begin downloading.

---

**NOTE:** For details on Bit Torrent, refer to section **5.4.1 Configuring Bit Torrent download settings**.

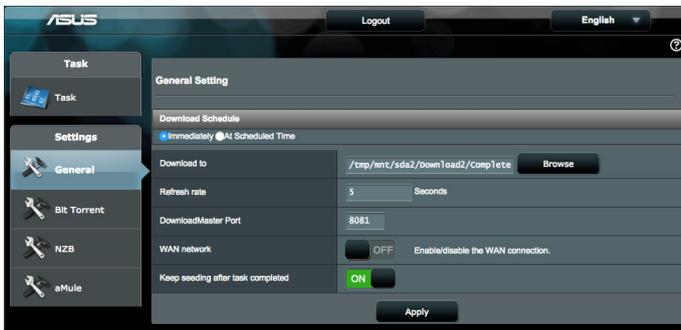
---

5. Use the navigation panel to configure the **General settings**.
  - You can define the download schedule by Selecting download **Immediately** or **At Scheduled Time**.

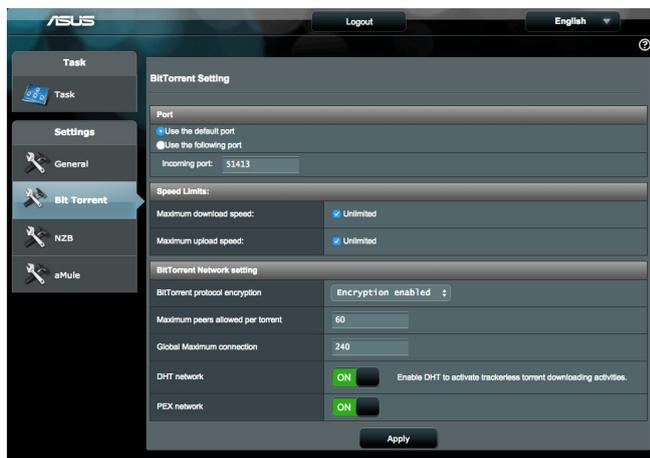
The screenshot shows a configuration window for download scheduling. At the top, there are two radio buttons: 'Immediately' (selected) and 'At Scheduled Time'. Below this, there are four rows of configuration options:

|                                     |   |
|-------------------------------------|---|
| Date to Enable Download (week days) | <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri |
| Time of Day to Enable Download      | 00 : 00 - 23 : 59   |
| Date to Enable Download (weekend)   | <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun   |
| Time of Day to Enable Download      | 00 : 00 - 23 : 59   |

- The download tasks information updates each 5 seconds in default. The options, **Refresh rate**, allow you to change the information updated period.
- You can select folder path from **Download to** field as download file repository.
- The default port number for **DownloadMaster** administration page is 8081. If the port number conflicts with other application you can change from here.
- To manage the **DownloadMaster** from Internet, you can slide **WAN network** to **ON**.
- If your network resource is tight, we recommend you disable Keep seeding after task completed by sliding the witch to **OFF**.



## 5.4.1 Configuring BitTorrent download settings

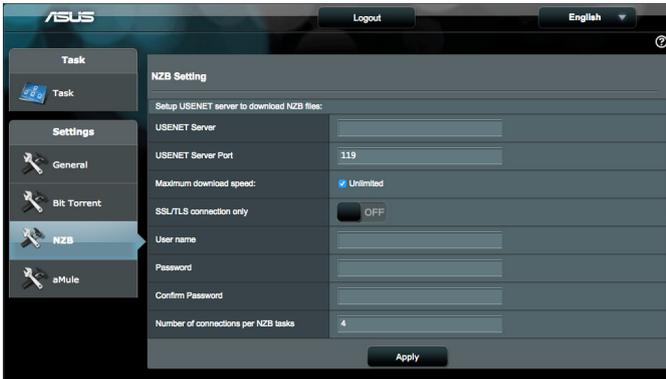


### To configure BitTorrent download settings:

1. From Download Master's navigation panel, click **Bit Torrent** to launch the **Bit Torrent Setting** page.
2. Select a specific port or use the default port for your download task.
3. To prevent network congestion, you can limit the maximum upload and download speeds under **Speed Limits**.
4. You can limit the maximum number of allowed peers and enable or disable file encryption during downloads.
5. Enable DHT (Distributed Hash Table) network can enhance download speeds and transfer rates by jointing a information sharing domain. To use the DHT network, your wireless router also needs to share some information with other member on the network,
6. Enable PEX (Peer Exchange) network to exchange peer information between two connected peers help you to gather more peers in the network.

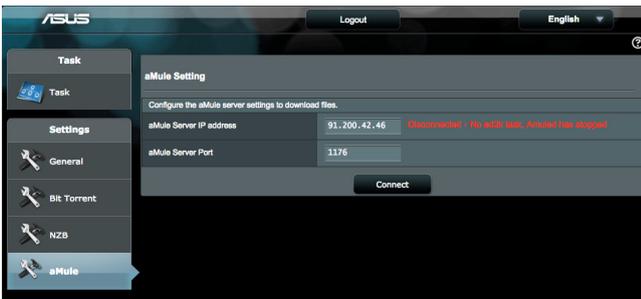
## 5.4.2 NZB settings

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



## 5.4.3 eMule settings

You can set up a eMule server to download file from eMule. After entering eMule settings, click **Apply**.



# 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: <https://www.asus.com/support> 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.

1. 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 <http://www.asus.com/support> 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 powered-on 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**.

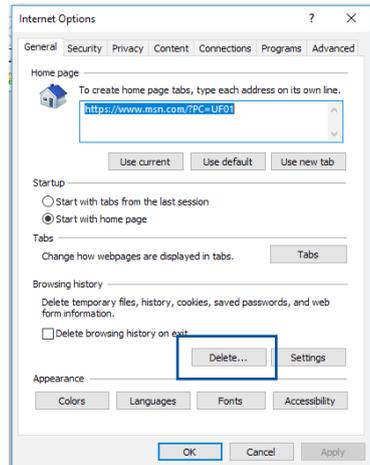


## 6.2 Frequently Asked Questions (FAQs)

### 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:

1. 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:**
  1. Launch the web GUI. Go to **General > Network Map > Clients** and search for the device that you want to connect to the router.
  2. 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**.
- 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**.

## Wired 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.

## Mobile broadband Internet is not accessible.

- Insert a SIM that with data plan subscription into the USIM card slot. The 3G/4G Mobile Broadband LED lights up, indicating that the SIM card is properly installed.
- The APN settings are not applied automatically. Obtain the APN service settings from your ISP, then follow the steps below to manually configure the APN settings.
  - Go to **Advanced Settings > WAN > Internet Connection** tab.
  - In the **WAN Type** field, select **Mobile broadband**.
- If APN is configured correct and Internet connection still failed, ensure that:
  - The frequency band is compatible with your ISP.

- The wireless router is placed close to the window for a strong 3G/4G signal.
- Port trigger, port forwarding, DDNS or DMZ service cannot work. Most ISPs provide a private IP address for a mobile broadband device. Hence some services, such as AiCloud, are not accessible. Please contact your ISP for assistance.

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

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

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

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

The following are the factory default settings:

**User Name:** admin

**Password:** admin

**Router's LAN IP address:** 192.168.50.1 / router.asus.com

**Wi-Fi Settings:**

**SSID (2.4GHz):** ASUS\_XX

**SSID (5GHz):** ASUS\_XX

**Default Wi-Fi Key:** Located on the label on the back of your router.

---

**NOTE:** XX refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back of your router.

---

## 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.

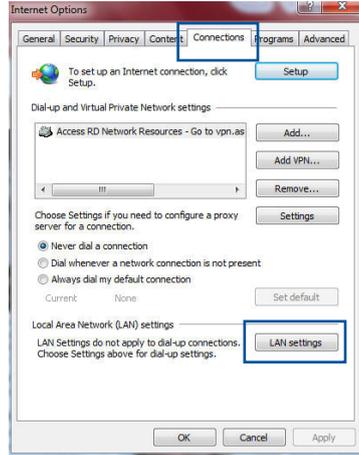
# Cannot access Web GUI

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

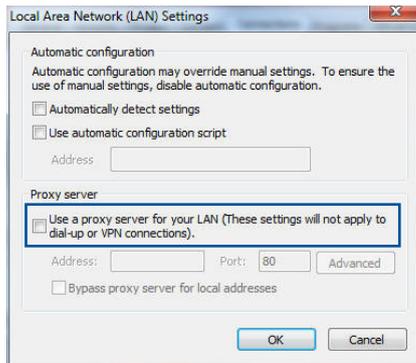
## A. Disable the proxy server, if enabled.

### Windows®

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

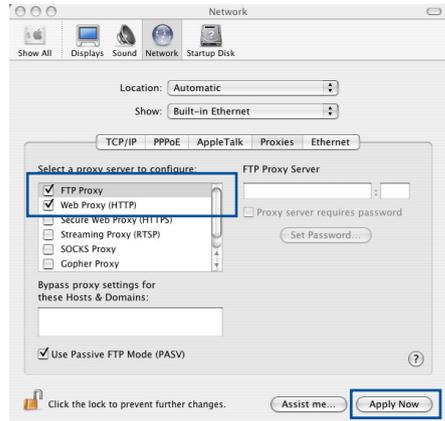


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



## MAC OS

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

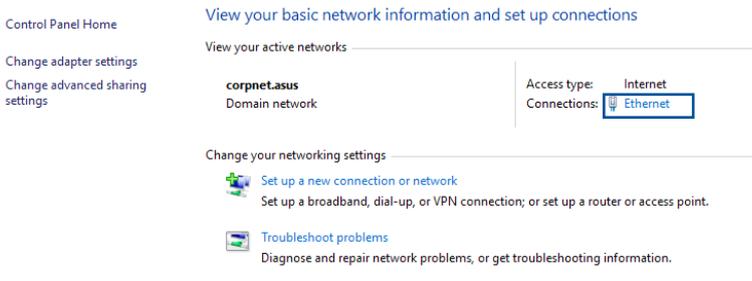


**NOTE:** Refer to your browser's help feature for details on disabling the proxy server.

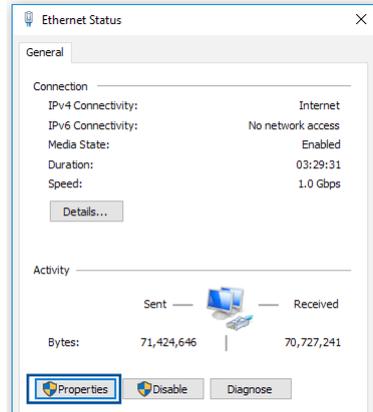
## B. Set the TCP/IP settings to automatically obtain an IP address.

### Windows®

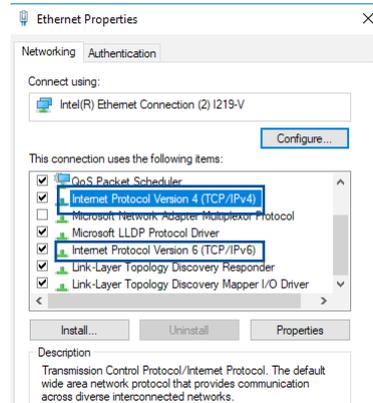
1. Click **Start > Control Panel > Network and Sharing Center**, then click the network connection to display its status window.



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



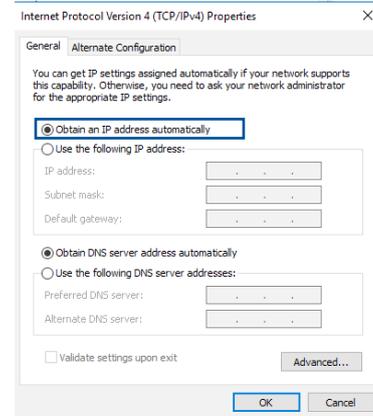
3. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



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

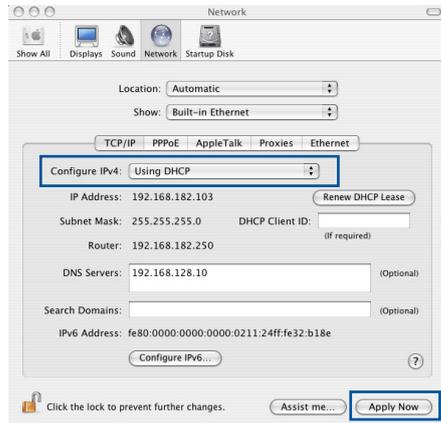
To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

5. Click **OK** when done.



## MAC OS

1. 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.

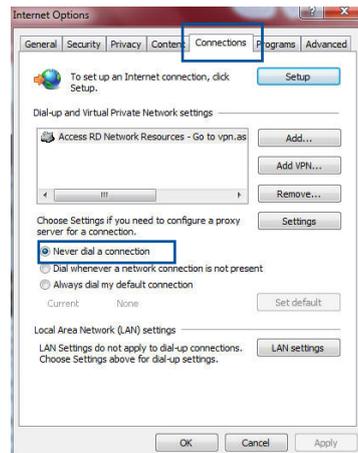


**NOTE:** Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

## 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 <http://csr.asus.com/english/Takeback.htm> 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 is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

---

---

**WARNING!**

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
  - Users must not modify this device. Modifications by anyone other than the party responsible for compliance with the rules of the Federal Communications Commission (FCC) may void the authority granted under FCC regulations to operate this device.
  - For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
-

## CE statement

### Simplified EU Declaration of Conformity

ASUSTek Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. Full text of EU declaration of conformity is available at <https://www.asus.com/support/>

### Declaration of Conformity for Ecodesign directive 2009/125/EC

Testing for eco-design requirements according to (EC) No 1275/2008 and (EU) No 801/2013 has been conducted. When the device is in Networked Standby Mode, its I/O and network interface are in sleep mode and may not work properly. To wake up the device, press the Wi-Fi on/off, LED on/off, reset, or WPS button.

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

All operational modes:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40) , 802.11n (HT80)

The frequency, mode and the maximum transmitted power in EU are listed below:

2412-2472MHz (802.11n HT40 MCS 8): 19.97 dBm

5180-5240MHz (802.11n HT40 MCS 8): 22.43 dBm

5260-5320MHz (802.11n HT40 MCS 8): 22.81 dBm

5500-5700MHz (802.11n HT20 MCS 8): 29.75 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

|   |    |    |    |    |    |    |    |
|---|----|----|----|----|----|----|----|
|  | AT | BE | BG | CZ | DK | EE | FR |
|   | DE | IS | IE | IT | EL | ES | CY |
|   | LV | LI | LT | LU | HU | MT | NL |
|   | NO | PL | PT | RO | SI | SK | TR |
|   | FI | SE | CH | UK | HR |    |    |

## Safety Notices

- Use this product in environments with ambient temperatures between 0°C(32°F) and 40°C(104°F).
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- DO NOT place on uneven or unstable work surfaces. Seek servicing if the casing has been damaged.
- DO NOT place or drop objects on top and do not shove any foreign objects into the product.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the modem during electrical storms.
- DO NOT cover the vents on the product to prevent the system from getting overheated.
- DO NOT use damaged power cords, accessories, or other peripherals.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.

## CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

## Radio Frequency (RF) Exposure Information

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 31 cm between the radiator & your body.

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 31 cm de distance entre la source de rayonnement et votre corps.

### Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux normes CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

Son utilisation est sujette aux deux conditions suivantes : (1) cet appareil ne doit pas créer d'interférences et (2) cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

### NCC 警語

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。

## 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 machine-readable 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

## For Turkey only

### Authorised distributors in Turkey:

#### **BOGAZICI BİL GİSAYAR SAN. VE TİC. A.S.**

**Tel. No.:** +90 212 3311000

**Address:** AYAZAGA MAH. KEMERBURGAZ CAD. NO.10  
AYAZAGA/İSTANBUL

#### **CİZGİ Elektronik San. Tic. Ltd. Sti.**

**Tel. No.:** +90 212 3567070

**Address:** CEMAL SURURI CD. HALİM MERİC İS MERKEZİ  
No: 15/C D:5-6 34394 MECİDİYEKOY/  
İSTANBUL

#### **KOYUNCU ELEKTRONİK BİLGİ İSLEM SİST. SAN. VE DİŞ TİC. A.S.**

**Tel. No.:** +90 216 5288888

**Address:** EMEK MAH.ORDU CAD. NO:18, SARİGAZİ,  
SANCAKTEPE İSTANBUL

#### **ENDEKS BİLİŞİM SAN VE DİŞ TİC LTD ŞTİ**

**Tel. No.:** +90 216 523 35 70 (pbx)

**Address:** Bulgurlu Mahallesi Alemdağ Caddesi No:56 /  
B-1 34696 Üsküdar/ İSTANBUL

AEEE Yönetmeliğine Uygundur.

## ASUS Contact information

### ASUSTeK COMPUTER INC.

Address 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan  
Telephone +886-2-2894-3447  
Fax +886-2-2893-1687  
Web site <https://www.asus.com>

#### Technical Support

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

### ASUS COMPUTER INTERNATIONAL (America)

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

#### Technical Support

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

### ASUS COMPUTER GmbH (Germany and Austria)

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

#### Technical Support

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