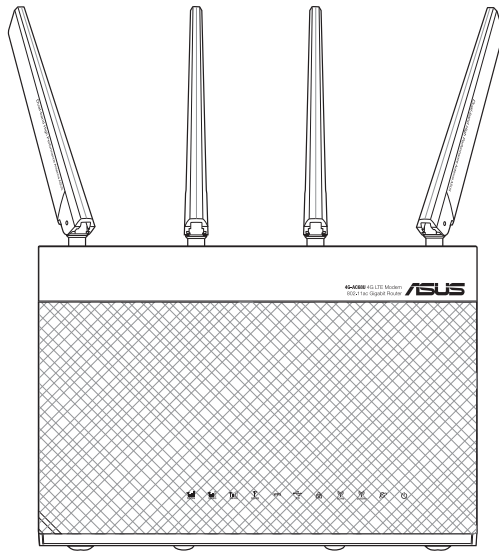


User Guide

4G-AC68U

Dual-Band Wireless-AC1900 LTE Modem Router



ASUS[®]
IN SEARCH OF INCREDIBLE

E13374

First Edition

August 2017

Copyright © 2017 ASUSTeK Computer Inc. All Rights Reserved.

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

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

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

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

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

Table of contents

1	Getting to know your wireless router	
1.1	Welcome!	7
1.2	Package contents.....	7
1.3	Your wireless router	8
1.4	Device Properties.....	10
1.5	Positioning your router.....	11
1.6	Installing your router	12
1.6.1	Prepare the setup requirements.....	12
1.6.2	Set up your LTE wireless router.	13
2	Getting started	
2.1	Quick Internet Setup (QIS) with Auto- detection	15
3	Configuring the General Settings	
3.1	Using the Network Map	20
3.1.1	Setting up the wireless security settings.....	21
3.1.2	System Status	22
3.1.3	Managing your network clients.....	23
3.1.4	Monitoring the Internet Status	25
3.1.5	Monitoring your USB device	26
3.2	Guest Network	27
3.3	AiProtection	29
3.3.1	Network Protection	30
3.3.2	Setting up Parental Controls.....	34
3.4	Adaptive QoS	38
3.4.1	Bandwidth Monitor	38
3.4.2	QoS.....	39
3.4.3	Web History.....	40

Table of contents

3.5	Traffic Analyzer	41
3.6	Using the USB Application	42
3.6.1	Using AiDisk	42
3.6.2	Using Servers Center.....	45
3.7	Using iCloud 2.0	50
3.7.1	Cloud Disk.....	51
3.7.2	Smart Access.....	52
3.7.3	Smart Sync.....	53
3.7.4	Sync Server	54
3.7.5	Settings.....	57
4	Configuring the Advanced Settings	
4.1	Wireless.....	58
4.1.1	General.....	58
4.1.2	WPS	60
4.1.3	WDS.....	62
4.1.4	Wireless MAC Filter	64
4.1.5	RADIUS Setting	65
4.1.6	Professional	66
4.2	LAN.....	69
4.2.1	LAN IP	69
4.2.2	DHCP Server.....	70
4.2.3	Route	72
4.2.4	IPTV	73
4.2.5	Switch Control.....	73
4.3	WAN	74
4.3.1	Internet Connection.....	74
4.3.2	IPv6 (Internet Settings)	83
4.3.3	Dual WAN	84
4.3.4	Port Trigger.....	85

Table of contents

4.3.5	Virtual Server/Port Forwarding	87
4.3.6	DMZ.....	90
4.3.7	DDNS	91
4.3.8	NAT Passthrough.....	92
4.4	IPv6	93
4.5	VPN Server.....	94
4.6	Firewall.....	95
4.6.1	General.....	95
4.6.2	URL Filter	95
4.6.3	Keyword filter	96
4.6.4	Network Services Filter	96
4.6.5	IPv6 Firewall	97
4.7	Administration	98
4.7.1	Operation Mode	98
4.7.2	System.....	99
4.7.3	Firmware Upgrade.....	101
4.7.4	Restore/Save/Upload Setting	102
4.8	System Log.....	103
4.9	Ethernet WAN Mobile Broadband Function Support List	104
5	Utilities	
5.1	Device Discovery.....	106
5.2	Firmware Restoration	107
5.3	Setting up your printer server.....	108
5.3.1	ASUS EZ Printer Sharing	108
5.3.2	Using LPR to Share Printer	112
5.4	Download Master	117
5.4.1	Configuring Bit Torrent download settings.....	119
5.4.2	NZB settings.....	120
5.4.3	eMule settings.....	120

6 Troubleshooting

6.1	Basic Troubleshooting.....	121
6.2	Frequently Asked Questions (FAQs)	123

Appendices

Notices 132

ASUS Contact information..... 146

Networks Global Hotline Information..... 147

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS 4G-AC68U Wireless Router!

The powerful and stylish 4G-AC68U 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.

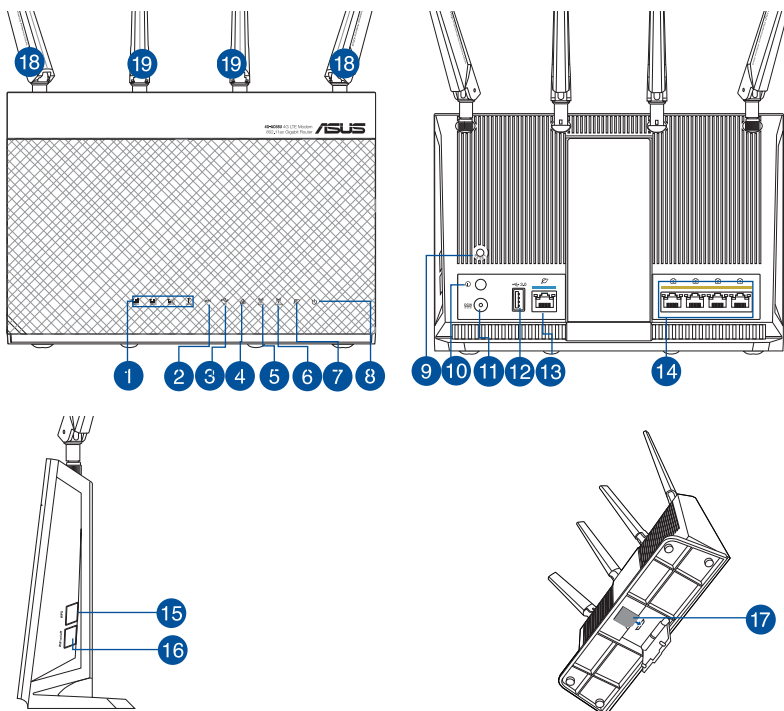
1.2 Package contents

- 4G-AC68U Wireless Router
- AC adapter
- Network cable (RJ-45)
- Quick Start Guide
- 2 x 3G/4G antennas

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 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

 - 2 WPS LED**
 - Off: WPS is not processing.
 - Flashing quick: WPS is processing.

 - 3 USB 3.0 LED**
 - Off: No power or no physical connection.
 - On: Has physical connection to USB 3.0 devices.

 - 4 LAN LED**
 - Off: No data activity or no physical connection.
 - On: Ethernet connection is established.
-

-
- 5 5GHz Wi-Fi LED**
Off: No 5GHz signal.
On: 5GHz wireless is ready.
Flashing: Transmitting or receiving data via wireless connection.
-
- 6 2.4GHz Wi-Fi LED**
Off: No 2.4GHz signal.
On: 2.4GHz wireless is ready.
Flashing: Transmitting or receiving data via wireless connection.
-
- 7 WAN (Internet) LED**
Off: No data activity or no physical connection.
On: Has physical connection to a wide area network (WAN).
-
- 8 Power LED**
Off: No power.
On: Device is ready.
Flashing slow: Rescue mode
Flashing quick: WPS is processing.
-
- 9 Reset button**
This button resets or restores the system to its factory default settings.
-
- 10 Power on/off button**
Press this button to power on or off the system.
-
- 11 Power (DC-In) port**
Insert the bundled AC adapter into this port and connect your router to a power source.
-
- 12 USB 3.0 port**
Insert USB 3.0 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 WPS button**
Long press the button to launch the WPS Wizard.
-
- 16 Wi-Fi On/Off button**
Press this button to turn on /off the Wi-Fi connection.
-
- 17 Micro SIM/USIM card slot**
Install a Micro SIM/USIM card into this slot to establish a Mobile Broadband Internet connection.
-
- 18 Detachable LTE antennas**
-
- 19 Fixed Wi-Fi antennas**
-

NOTES:

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

1.4 Device Properties

Power Consumption:

- Input: AC 100~240V / 50~60Hz, DC 19V /2.37A (EU)
Input: AC 100~240V / 50~60Hz, DC 19V /3.42A (UK)
- Maximum power consumption: 25.8 W
- Average power consumption: 10.3 W
- The average power consumption was determined at room temperature (23 °C to 27 °C) with the following load:
 - Active Mobile Broadband connection
 - Wireless LAN on; no devices are connected to the wireless LAN
 - One network device is connected to a LAN port; no data transfer; no network devices are connected to the other LAN ports

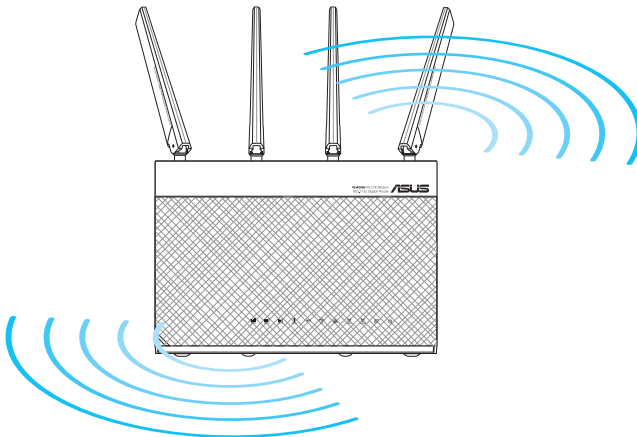
Ambient conditions:

DC Power adapter	DC Output: +19V with max 2.37A current ; DC Output: +19V with max 3.42A current		
Operating Temperature	0~40°C	Storage Temperature	0~70°C
Operating Humidity	10 ~ 90%	Storage Humidity	10 ~ 90%

1.5 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 LTE router near a window to receive the best quality for maximum wireless upstream performance with an LTE base station.
- Keep the device away from metal obstructions and away from direct sunlight.
- Place the router horizontally.
- Do not place the Wireless LTE Router in a dusty or wet environment.
- To prevent signal loss, keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment.
- Always update to the latest firmware. Visit the ASUS website at <http://www.asus.com/Networking/4G-AC68U/HelpDesk/Download/> to get the latest firmware updates.
- To ensure the best wireless signal, orient the antennas as shown in the drawing below.



1.6 Installing your router

1.6.1 Prepare the setup requirements.

To set up your wireless network, you need to meet the following requirements:

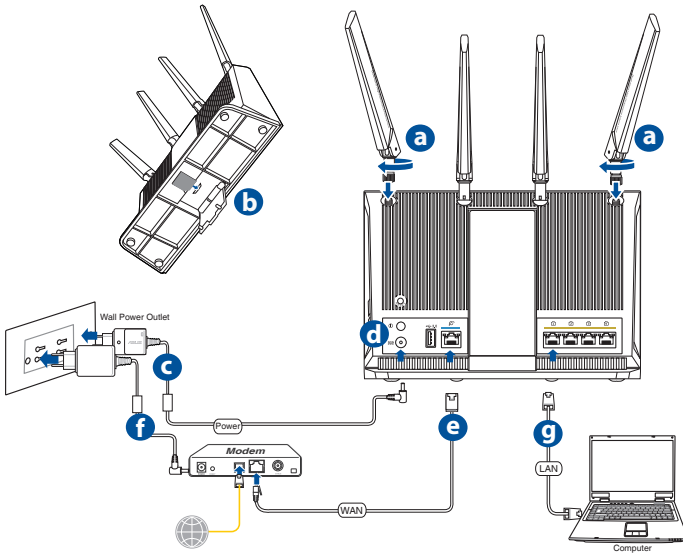
- A Micro SIM/USIM card with WCDMA and LTE subscription

IMPORTANT! Ensure that your Micro SIM/USIM card is subscribed to WCDMA and LTE services. Contact your mobile service provider about these services.

CAUTION! Use only a standard Micro SIM/USIM card on your router. Using a different form of SIM card type, such as mini or nano SIM card, may result to a stuck SIM card and may damage your router.

- An ADSL/cable modem with Internet subscription
- A computer with Ethernet RJ-45 (LAN) port (10/100/1000 Base-TX) or a Wi-Fi-enabled device with a 2.4 GHz and 5 GHz 802.11 a/b/g/n/ac wireless interface
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

1.6.2 Set up your LTE wireless router.



- a. Attach the two 3G/4G antennas.
- b. Insert the Micro SIM/USIM card into the Micro SIM/USIM card slot. When the Micro SIM/USIM card is properly installed, the Mobile Broadband LED lights up and flashes slowly after power on. See **Install Micro SIM/USIM card into your router**.
- c. Insert the AC adapter of your router to the DC-IN port and plug it to a power outlet.
- d. Turn on your router.
- e. Using a network cable, connect your modem to the WAN port of your router. When the network cable is properly connected, the WAN LED lights up.
- f. Insert the AC adapter of your modem to the DC-IN port and plug it to a power outlet.

NOTE: You can use either 3G/4G or wired Ethernet connection for Internet access.

- g. Using the bundled network cable, connect your computer to the LAN port of your router.

Manually connecting to a wireless network

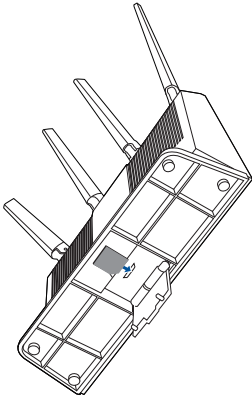
NOTE: Ensure that you press the Wi-Fi button on your router.

1. Enable the Wi-Fi function on your wireless client for it to automatically scan for wireless networks.
 2. Select the wireless network named “ASUS_XX_2G” or “ASUS_XX_5G”, which is the default wireless network name (SSID) of ASUS wireless routers.
-

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.

Installing Micro SIM/USIM card into your router

1. Find the Micro SIM/USIM card slot on the bottom of the router and lift the cover.
2. Insert the Micro SIM/USIM card.



2 Getting started

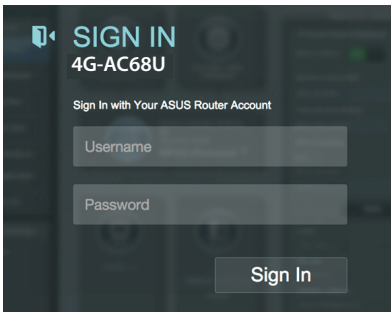
2.1 Quick Internet Setup (QIS) with Auto-detection

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

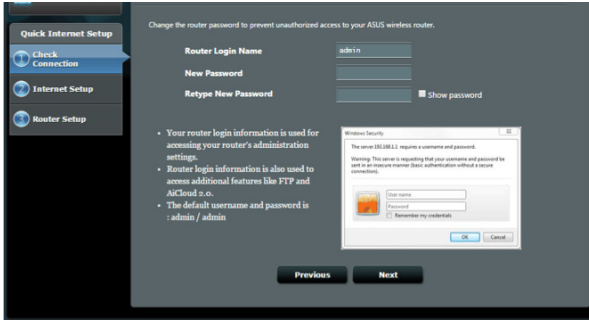
1. Press the power button at the back of your router. Ensure that the following LEDs light up:
 - Power LED
 - 2.4GHz Wi-Fi LED
 - WAN or Mobile Broadband LED
 - 5GHz Wi-Fi LED
2. Launch your web browser such as Internet Explorer, Firefox, Google Chrome, or Safari.

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".

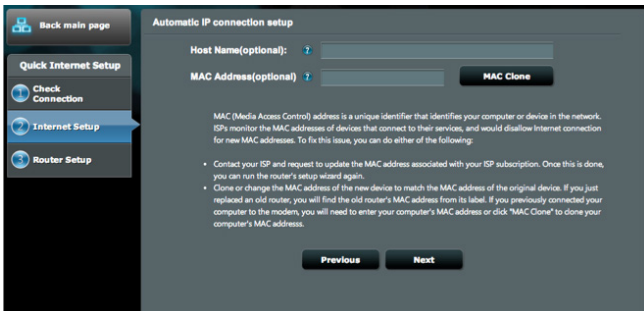


4. Assign your router login name and password and click **Next**. You need this login name and password to log into ASUS router to view or change the router settings. You can take note of your router login name and password for future use.

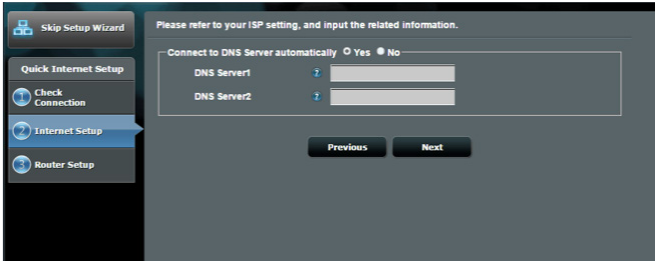


5. If the WAN port is connected, the wireless router's Quick Internet Setup (QIS) feature automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP**, **L2TP**, and **Static IP**. Please obtain the necessary information from your Internet Service Provider (ISP). If your connection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

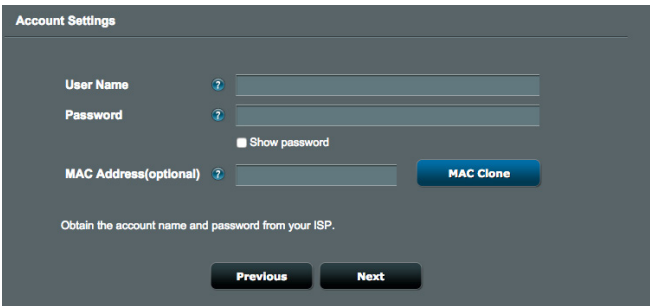
for Automatic IP (DHCP)



for PPPoE, PPTP, and L2TP

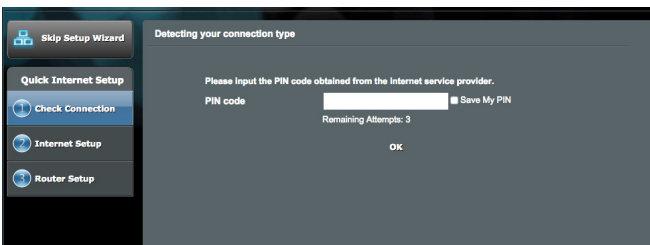


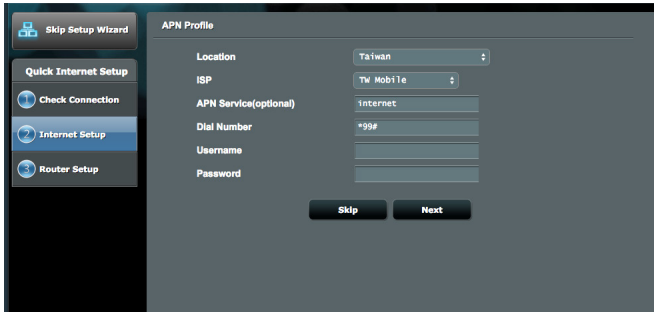
for Static IP



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.

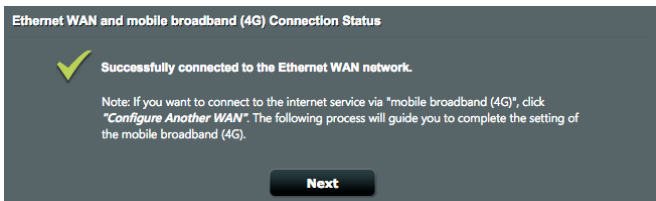
NOTE: The PIN code may vary from different providers.



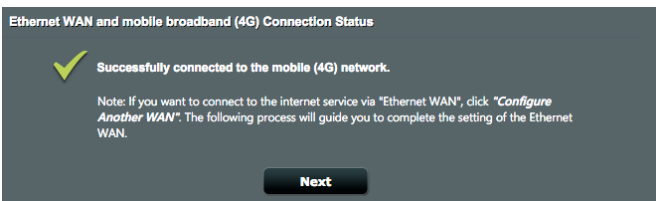


7. The dual WAN connection configuration result is displayed. Click **Next** to continue.

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.

Wireless Setting

Do you want to use the previous wireless security settings? Yes No

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

2.4 GHz - Security

Network Name (SSID)

Network Key

5 GHz - Security Copy 2.4 GHz to 5 GHz settings

Network Name (SSID)

Network Key

Enter a network key between 8 and 63 characters(letters, numbers or a combination) or 64 hex digits. The default wireless security setting is WPA2-Personal AES. If you do not want to set the network security, leave the security key field blank, but this exposes your network to unauthorized access.

Apply

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.

Completed Network Configuration Summary

System Time: **Mon, Jul 06 10:55:50 2015** (GMT+08:00)

Wireless

Band	2.4GHz	5GHz
Network Name (SSID)	ASUS_4GAC55U	ASUS_4GAC55U_5G
Network Key	99999999	99999999
Wireless Security	WPA2-Personal - AES	WPA2-Personal - AES

WAN

WAN Connection Type	Mobile Broadband	Automatic IP
Status	Active	Inactive
WAN IP	10.181.40.163	0.0.0.0

LAN

LAN IP	192.168.1.1
MAC address	AC:9E:17:56:5F:8C

Finish

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, and manage your network clients.



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' app with the '2.4GHz' tab selected. The settings are as follows:

Field	Value
Wireless name(SSID)	ASUS
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA-PSK key	*****
LAN IP	192.168.1.1
PIN code	62867566
LAN MAC address	AC:9E:17:56:6F:4C
Wireless 2.4GHz MAC address	AC:9E:17:56:6F:48

5GHz security settings



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

Field	Value
Wireless name(SSID)	ASUS_5G
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA-PSK key	*****
LAN IP	192.168.1.1
PIN code	62867566
LAN MAC address	AC:9E:17:56:6F:4C
Wireless 5GHz MAC address	AC:9E:17:56:6F:4C

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.

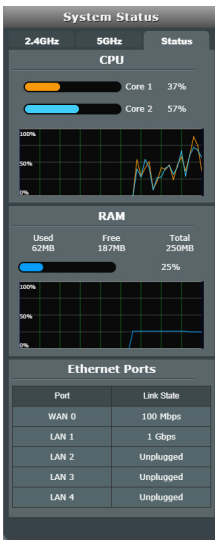
5. Click **Apply** when done.

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:

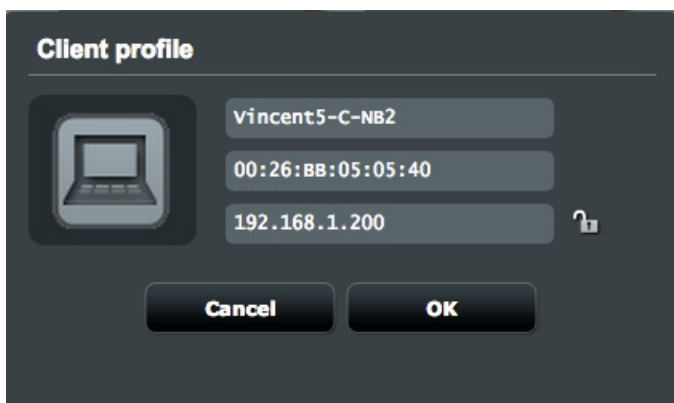
1. From the navigation panel, go to **General > Network Map** tab.
2. On the **Network Map** screen, select the Client Status icon



to display your network client's information.





3. On Client status table, click the device icon  to show the detailed profile of the device. To block a client's access to your network, select the client and click block icon  .



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 **Disable** button on Terminate WAN Interface.

Primary WAN

Primary WAN status	
Terminate WAN Interface	Disable
WAN Port	
WAN	
Dual WAN Mode	
Fail Over	
Connection type	
Static IP	
WAN IP	
192.168.201.77	
Subnet Mask	
255.255.255.0	
DNS	
168.95.1.1	
168.95.192.1	
Gateway	
192.168.201.1	
Dual WAN setting	GO
WAN setting	GO


Secondary WAN

Secondary WAN status	
Terminate WAN Interface	Disable
WAN Port	
USB	
Dual WAN Mode	
Fail Over	
Connection type	
USB Modem	
WAN IP	
100.91.231.153	
Subnet Mask	
255.255.255.252	
DNS	
61.31.233.1	
168.95.1.1	
Gateway	
100.91.231.154	
Dual WAN setting	GO
WAN setting	GO

3.1.5 Monitoring your USB device

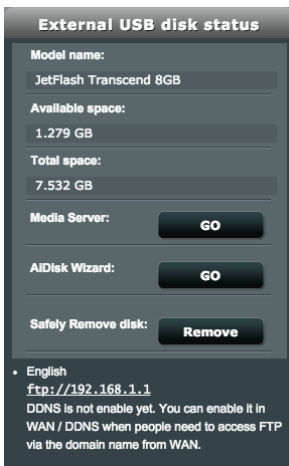
The ASUS wireless router provides one USB port for connecting USB devices or USB printer to allow you to share files and printer with clients in your network.

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.

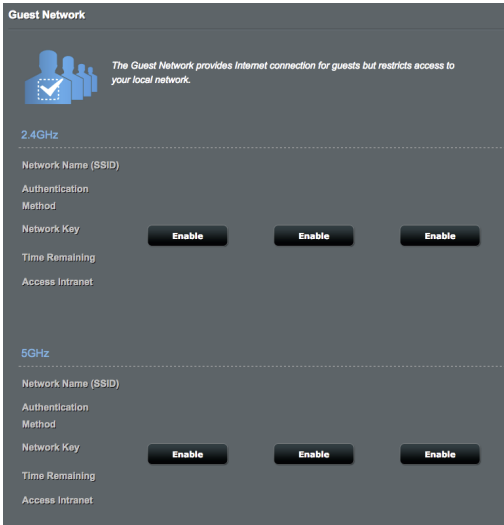
NOTE: The wireless router works with most USB HDDs/Flash disks (up to 2 TB size) and supports read-write access for FAT16, FAT32, EXT2, EXT3, and NTFS.

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.




The screenshot displays the 'Guest Network' configuration page. At the top, there is a header 'Guest Network' and a descriptive icon of people with a checkmark, accompanied by the text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' Below this, the interface is divided into two sections: '2.4GHz' and '5GHz'. Each section contains the following fields: 'Network Name (SSID)', 'Authentication Method', and 'Network Key'. The 'Network Key' field in both sections has three 'Enable' buttons. Below these fields are 'Time Remaining' and 'Access Intranet' options.

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 **No** or **Yes** on **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
Network Name (SSID)	ASUS_Guest1
Authentication Method	Open System
Access time	<input type="radio"/> hours <input type="radio"/> minutes <input checked="" type="radio"/> Unlimited
Access Intranet	Disable
Enable MAC Filter	No <small>You must go to enable Wireless MAC Filter</small>

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

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.

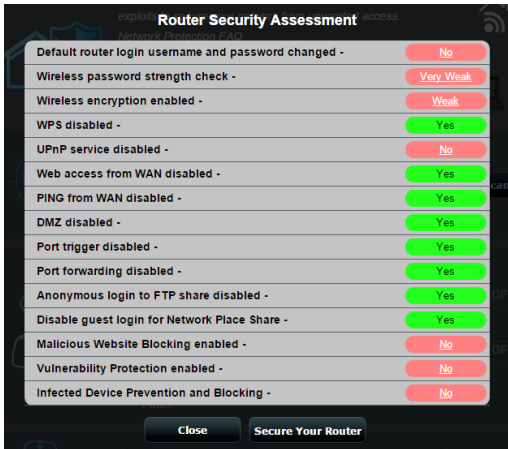


Configuring Network Protection

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 Vulnerability protection:

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.



Web & Apps Filters

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

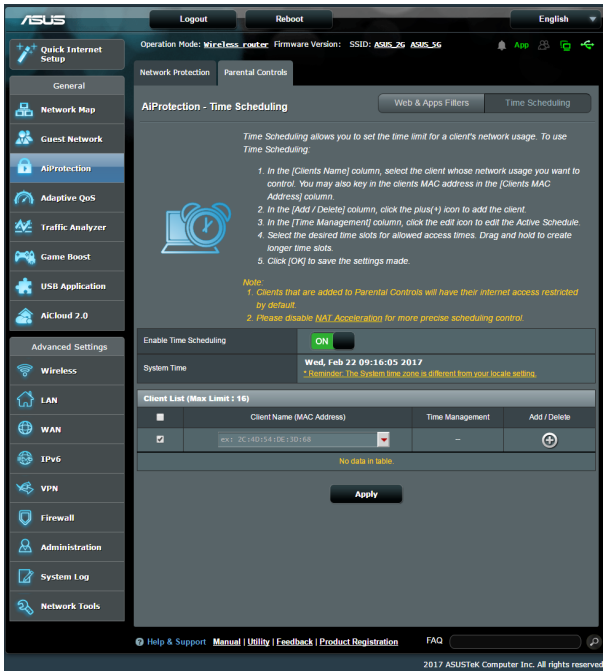
To configure Web & Apps Filters:

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 **Enable 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 **Clients Name** 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 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.



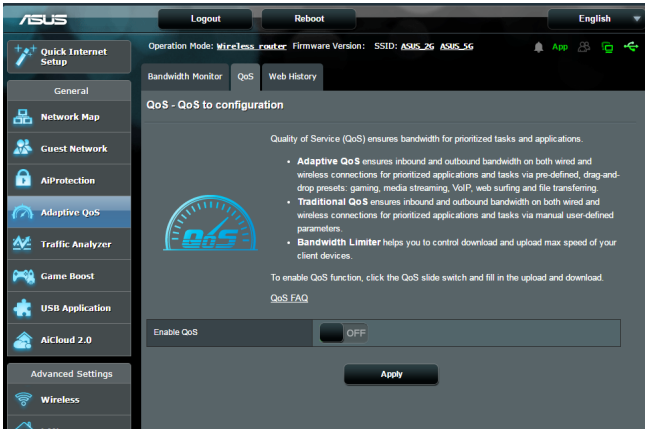
Apps analysis

To enable Apps analysis:

From the **Bandwidth Monitor** tab, go to 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 Smart 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.

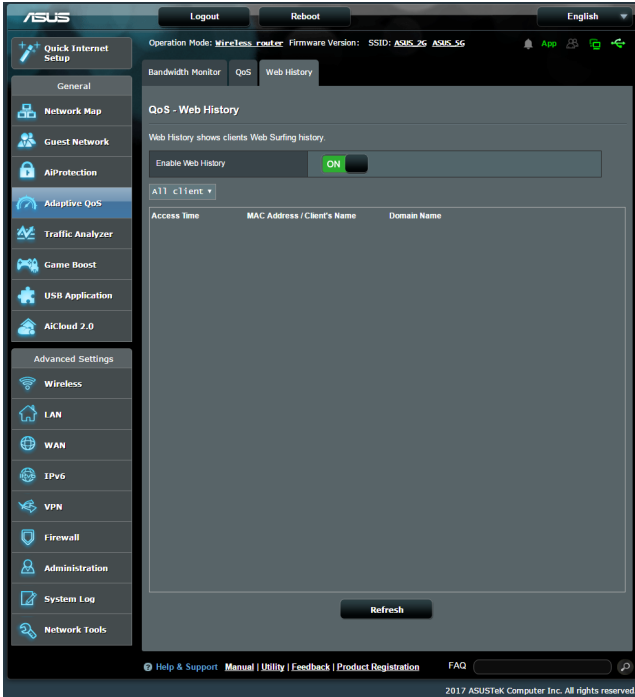
4. Select the QoS Type (Adaptive or Traditional) for your configuration.

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.

ASUS

Logout Reboot English

Operation Mode: Wireless router Firmware Version: SSID: ASUS_26 ASUS_56

Statistic Traffic Monitor

QoS - Traffic Monitor Real-time

Traffic Monitor allows you to monitor the incoming or outgoing packets of the following:

	Internet	Wired	Wireless
Reception	Incoming Internet packets	Incoming packets from wired network	Incoming packets from wireless network
Transmission	Outgoing Internet packets	Outgoing packets to wired network	Outgoing packets to wireless network

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

Traffic Monitor FAQ

Ethernet WAN (WAN)	Wired	Wireless (2.4GHz)	Wireless (5GHz)
305.18 KB/s			
213.62 KB/s			
152.59 KB/s			
76.29 KB/s			

Current	Average	Maximum	Total
0.91 KB/s	0.80 KB/s	238.84 KB/s	480.94 KB
0.68 KB/s	0.04 KB/s	9.70 KB/s	21.40 KB

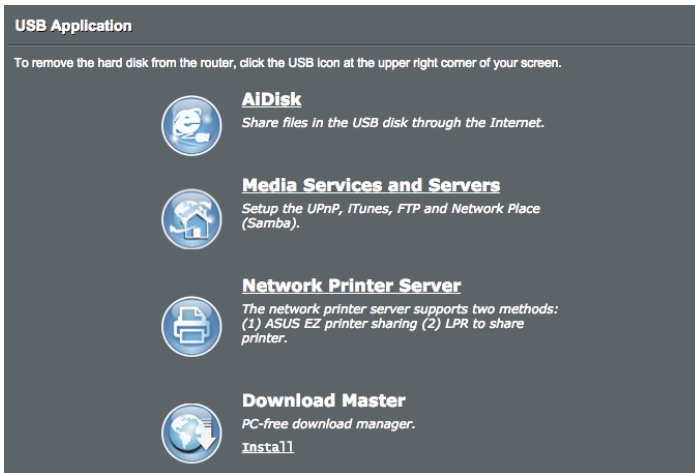
Help & Support Manual | Utility | Feedback | Product Registration FAQ

2017 ASUS/ASUSTek Computer Inc. All rights reserved.

3.6 Using the USB Application

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

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

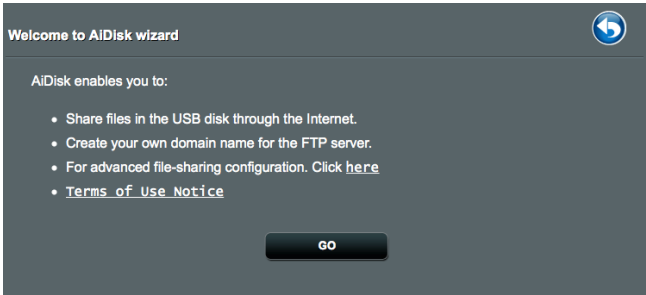


3.6.1 Using AiDisk

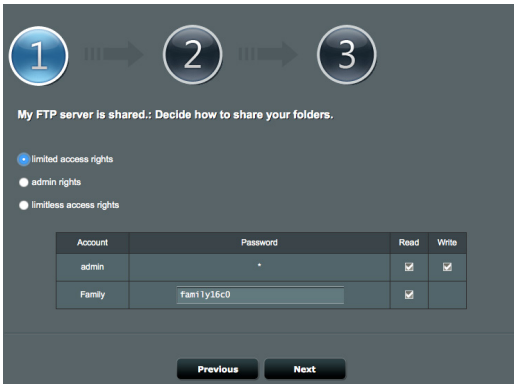
AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

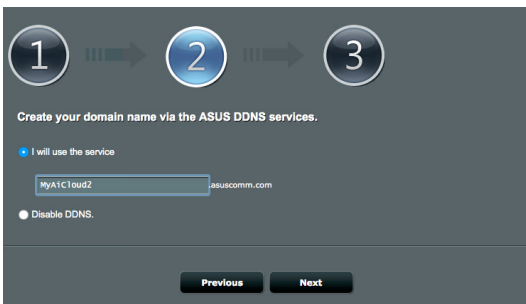
1. From the navigation panel, go to **General > USB application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.

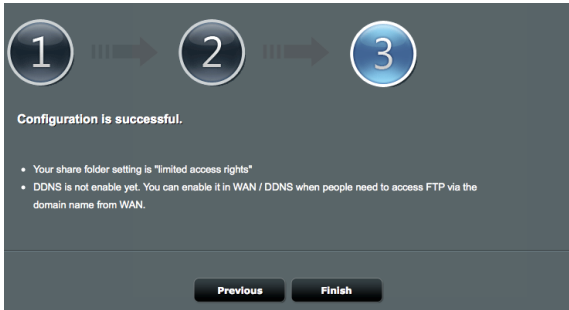


3. Select the access rights that you want to assign to the clients accessing your shared data.



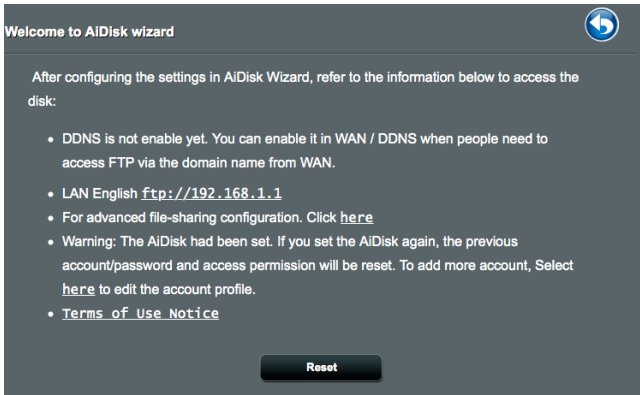
4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select **I will use the service and accept the Terms of service** and key in your domain name. When done, click **Next**.





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

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



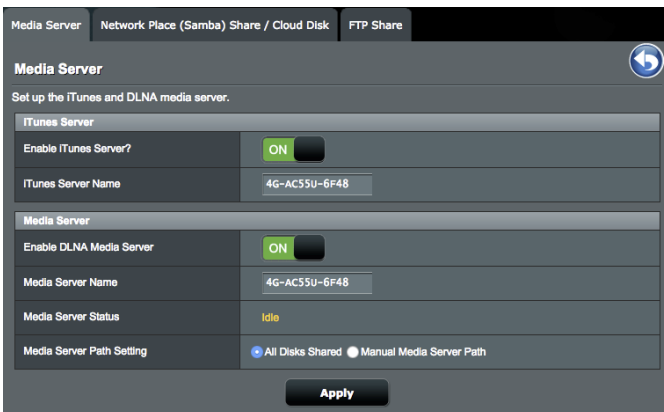
3.6.2 Using Servers Center

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-AC68U's network.



The screenshot shows the 'Media Server' configuration page. At the top, there are three tabs: 'Media Server' (selected), 'Network Place (Samba) Share / Cloud Disk', and 'FTP Share'. Below the tabs, the page title is 'Media Server' with a help icon. The main heading is 'Set up the iTunes and DLNA media server.' There are two main sections: 'iTunes Server' and 'Media Server'. The 'iTunes Server' section has a toggle for 'Enable iTunes Server?' set to 'ON' and a text field for 'iTunes Server Name' containing '4G-AC55U-6F48'. The 'Media Server' section has a toggle for 'Enable DLNA Media Server' set to 'ON', a text field for 'Media Server Name' containing '4G-AC55U-6F48', a 'Media Server Status' field showing 'Idle', and a 'Media Server Path Setting' with radio buttons for 'All Disks Shared' (selected) and 'Manual Media Server Path'. An 'Apply' button is at the bottom.

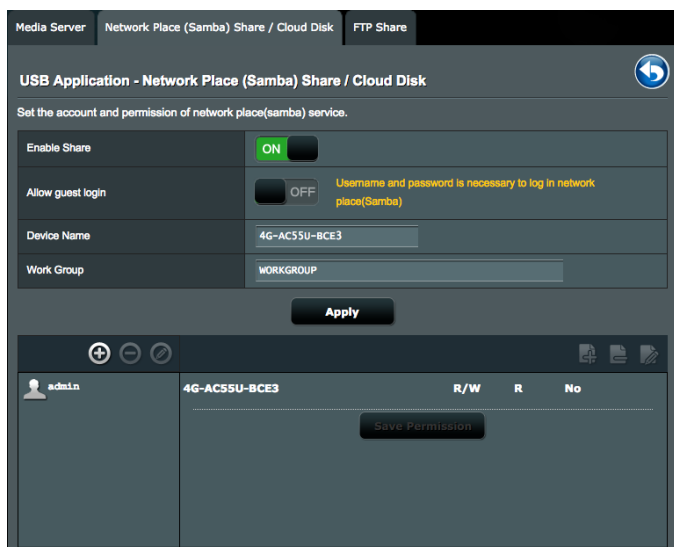
Media Server	
Set up the iTunes and DLNA media server.	
iTunes Server	
Enable iTunes Server?	<input checked="" type="checkbox"/> ON
iTunes Server Name	4G-AC55U-6F48
Media Server	
Enable DLNA Media Server	<input checked="" type="checkbox"/> ON
Media Server Name	4G-AC55U-6F48
Media Server Status	Idle
Media Server Path Setting	<input checked="" type="radio"/> All Disks Shared <input type="radio"/> Manual Media Server Path
Apply	

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

- **Enable iTunes Server:** Select ON/OFF to enable/disable the iTunes Server.
- **Enable DLNA Media Server:** Select ON/OFF to enable/disable the DLNA 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:

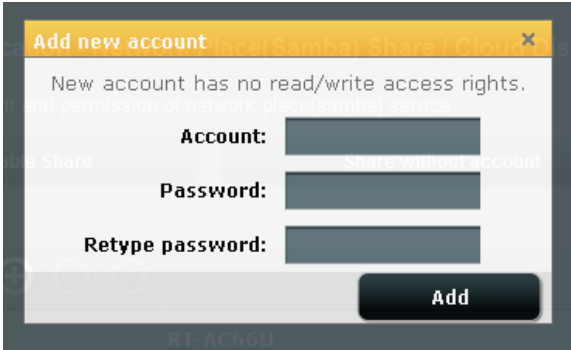
1. From the navigation panel, go to **General > USB application > Media Services and Servers > Network Place (Samba) Share / Cloud Disk** tab.

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.



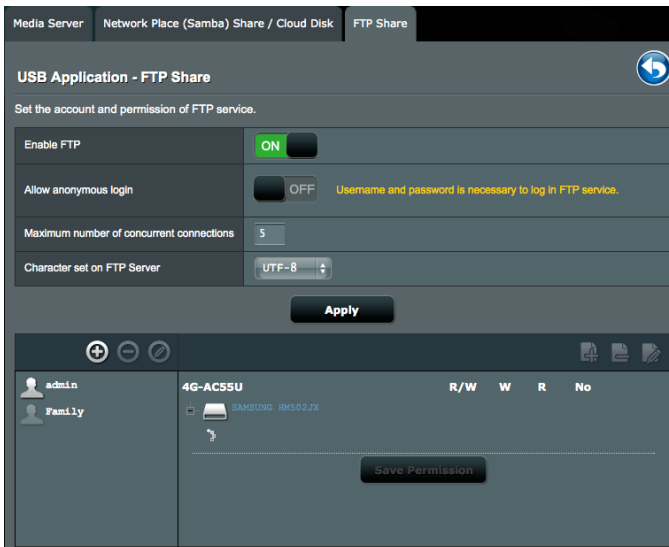
3. From the list of folders, select the type of access permission that you want to assign for specific folders:
 - **R/W**: Select this option to assign read/write access.
 - **R**: Select this option to assign read-only access.
 - **No**: Select this option if you do not want to share a specific file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



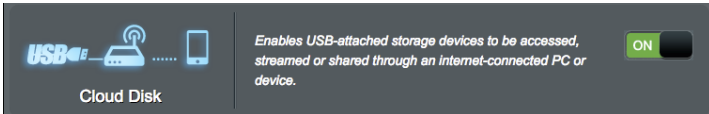
To use AiCloud:

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.

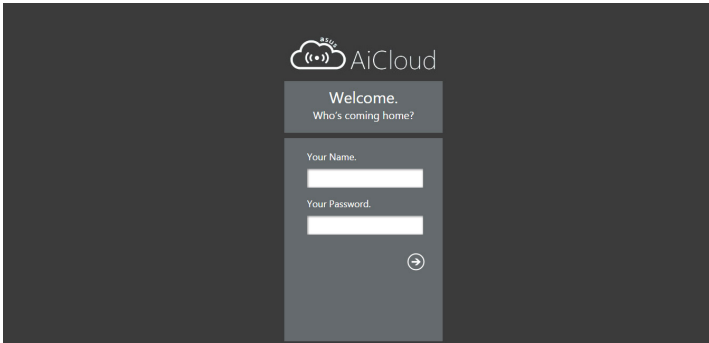
3.7.1 Cloud Disk

To create a cloud disk:

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

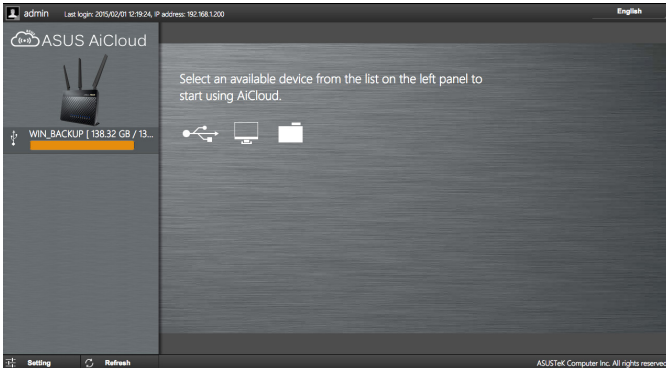


3. Go to <https://router.asus.com> and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.



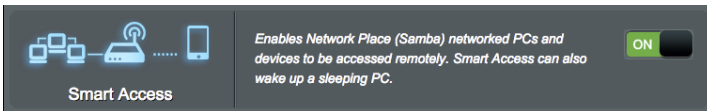
4. You can now start accessing Cloud Disk files on devices connected to the network.

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.



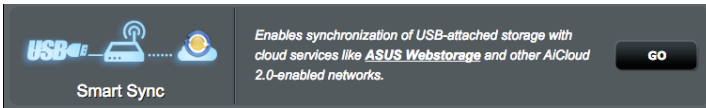
NOTES:

- 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.

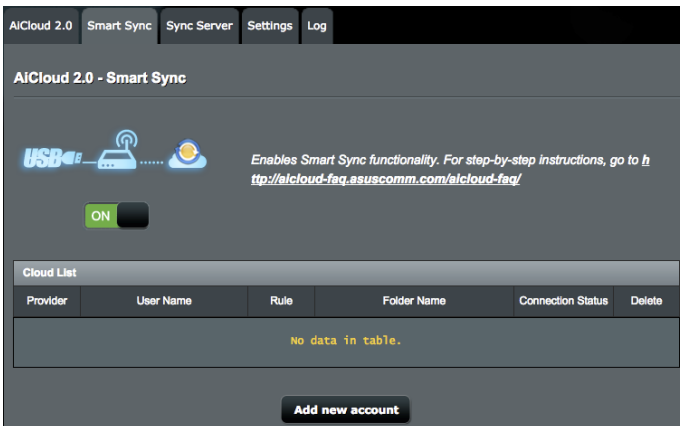
3.7.3 Smart Sync

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**.

Cloud List	
Provider	WebStorage
Account	<input type="text"/>
Password	<input type="password"/>
Folder	<input type="text"/> Browser
Rule	Synchronisation
Security Code	<input type="text"/> OTP Authentication
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

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 **Browser**

Rule ?

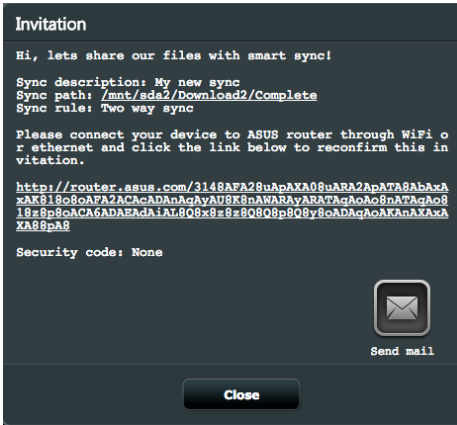
Security Code



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.

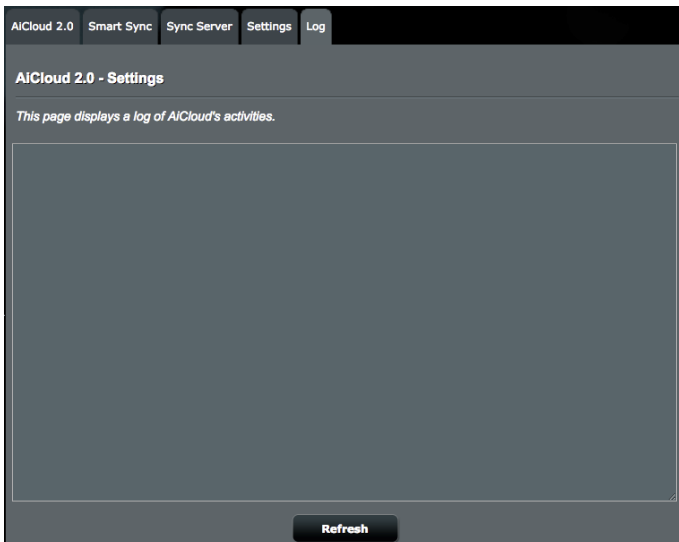


4. After a invitation is generated, you can check the sync task on **Sync List** table .

Sync List					
Provider	Description	Rule	Local Sync Folder	Invitation	Delete
	My new sync		/sda2/download2/Complete	View	

[Check log](#)

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.



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.

The screenshot shows the 'AiCloud 2.0 - Settings' page. At the top, there are navigation tabs: 'AiCloud 2.0', 'Smart Sync', 'Sync Server', 'Settings', and 'Log'. The 'Settings' tab is active. Below the tabs, the page title is 'AiCloud 2.0 - Settings'. A section titled 'Password Protection feature:' contains the following text: 'The Password Protection feature prevents unauthorized access to AiCloud. You can set a limited number of account/password login attempts. For example, a setting of 3 times / 2 mins indicates that the user has three attempts to input the account and password in 2 minutes. Once the specified number of attempts has been exceeded, the AiCloud account will be locked and administrator access is needed to unlock it.'

Below this text, there is a dashed-line box containing the following settings:

- 'Enable Password Protection Feature.' with a toggle switch set to 'ON'.
- 'Maximum number of failed login attempts' with a text input field containing '3'.
- 'Duration' with a text input field containing '2' and the unit 'minutes'.
- 'Account Status' with a user icon and the name 'admin'.

Below the dashed-line box, there are two more settings:

- 'AiCloud Web access port' with a text input field containing '443'.
- 'AiCloud content streaming port' with a text input field containing '8082'.

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

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
Wireless - General					
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				
Apply					

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
Wireless - WPS					
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 checked="" type="checkbox"/> ON				
Current Frequency	2.4GHz / 5GHz				
Connection Status	Idle / Idle				
Configured	Yes / Yes <input type="button" value="Reset"/>				
AP PIN Code	<input type="text" value="6286756"/>				
You can easily connect a WPS client to the network in either of these two ways:					
<ul style="list-style-type: none"> • Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter for about three minutes. • Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router. 					
WPS Method:	<input type="radio"/> Push button <input checked="" type="radio"/> Client PIN Code <input type="text"/>				
	<input type="button" value="Start"/>				

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 concurrently.
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.	

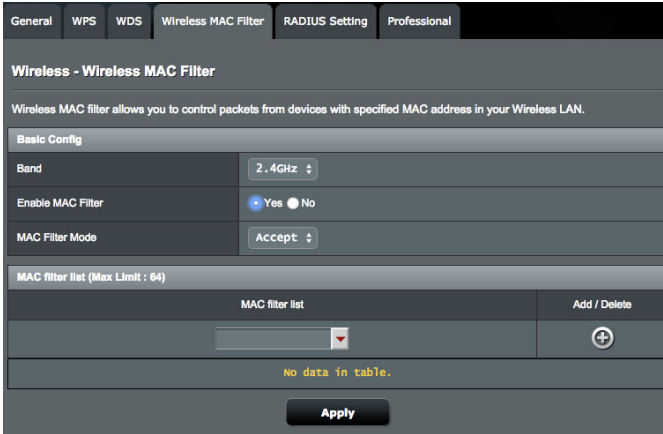
2. Select the band for the wireless bridge.
3. In the **AP Mode** field, select any of these options:
 - **AP Only**: Disables the WDS function.
 - **WDS Only**: Enables the WDS feature but prevents other wireless devices/stations from connecting to the router.
 - **HYBRID**: Enables the Wireless Bridge 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.

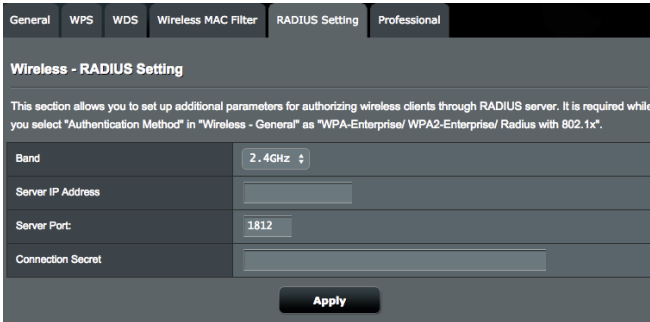


To set up the Wireless MAC filter:

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-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
Wireless - Professional					
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.					
Band	5GHz				
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Enable wireless scheduler	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Date to Enable Radio (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 Radio	00 : 00 - 23 : 59				
Date to Enable Radio (weekend)	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun				
Time of Day to Enable Radio	00 : 00 - 23 : 59				
Set AP Isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Roaming assistant	Disable				
Enable IGMP Snooping	Disable				
Multicast Rate(Mbps)	Auto				
Preamble Type	Long				
AMPDU RTS	Enable				
RTS Threshold	2347				
DTIM Interval	1				
Beacon Interval	100				
Enable TX Bursting	Enable				
Enable WMM APSD	Enable				
Apply					

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

- **Frequency:** Select the frequency band that the professional settings will be applied to.
- **Enable Radio:** Select **Yes** to enable wireless networking. Select **No** to disable wireless networking.

- **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 client that are members of the 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.



The screenshot shows the LAN IP configuration interface. At the top, there is a navigation bar with tabs for LAN IP, DHCP Server, Route, IPTV, and Switch Control. Below the navigation bar, the title is "LAN - LAN IP". Underneath, it says "Configure the LAN setting of RT-AC3200." There are two input fields: "IP Address" with the value "192.168.1.1" and "Subnet Mask" with the value "255.255.255.0". At the bottom center, there is an "Apply" button.

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 DHCP and provides a link to a FAQ. The configuration is divided into three sections: 'Basic Config', 'DNS and WINS Server Setting', and 'Manually Assigned IP around the DHCP list (Max Limit : 64)'. In the 'Basic Config' section, 'Enable the DHCP Server' is set to 'Yes', and the 'IP Pool Starting Address' is '192.168.1.2'. The 'DNS and WINS Server Setting' section has empty fields for 'DNS Server' and 'WINS Server'. The 'Manually Assigned IP' section has a table with columns for 'MAC address', 'IP Address', and 'Add / Delete', and a message 'No data in table.' at the bottom. An 'Apply' button is at the very bottom.

Basic Config	
Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
4G-AC55U's Domain Name	<input type="text"/>
IP Pool Starting Address	<input type="text" value="192.168.1.2"/>
IP Pool Ending Address	<input type="text" value="192.168.1.254"/>
Lease time	<input type="text" value="86400"/>
Default Gateway	<input type="text"/>

DNS and WINS Server Setting	
DNS Server	<input type="text"/>
WINS Server	<input type="text"/>

Manually Assigned IP around the DHCP list (Max Limit : 64)		
MAC address	IP Address	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>
No data in table.		

To configure the DHCP server:

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

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

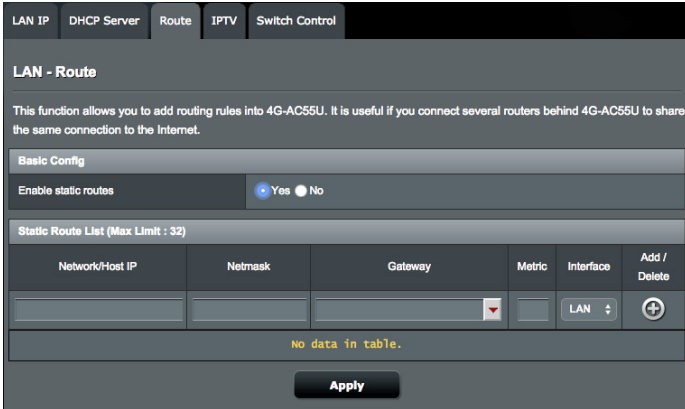
NOTES:

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



4.2.3 Route

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

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



To configure the LAN Routing table:

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

4.2.4 IPTV

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

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. Below the tabs, the page title is 'LAN - IPTV'. A note states: '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 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 (Udpxy)' 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'. Below the tabs, the page title is 'LAN - Switch Control'. A note states: 'Setting 4G-AC55U switch control.' The configuration is divided into two sections: 'NAT Acceleration(IPv4 Only)' and 'Enable Jumbo Frame'. '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 Input]

MAC Address: [Text Input] 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-AC68U 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 Type** field.

The screenshot shows the 'WAN - Mobile Broadband' configuration page. At the top, there are navigation tabs: 'Internet Connection', 'Dual WAN', 'Port Trigger', 'Virtual Server / Port Forwarding', 'DMZ', 'DDNS', and 'NAT Passthrough'. The main title is 'WAN - Mobile Broadband'. Below it, a subtitle reads 'Configure the Mobile Broadband setting of 4G-AC68U.' The configuration area is divided into three sections: 'WAN Index' with a 'WAN Type' dropdown set to 'Mobile Broadband'; 'Enable Mobile Broadband' with a dropdown set to 'Enable'; and 'SIM PIN Management' with a 'USIM Card Status' field showing 'SIM card is not inserted.' An 'Apply' button is located at the bottom center of the page.


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 ▾
Configure the Mobile Broadband settings of 4G-AC55U.	
Internet Connection	
Connection status	Connected ?
Network Type	Auto ▾
PDP Type	IPv4 ▾
Roaming	Disable ▾

4. Set up the following:

- **Location:** Select your 3G/4G service provider's location from the dropdown list.
- **ISP:** Select your Internet Service Provider (ISP) from the dropdown list.
- **APN (Access Point Name) service** (optional): Contact your 3G/4G service provider for detailed information.
- **Dial Number:** The 3G/4G provider's access number
- **PIN code:** Enter the 3G/4G provider's PIN code for connection on SIM PIN Management if the SIM card is required.

NOTE:

- The default PIN code may vary with different providers.
 - When you set up for the first time or reboot your router, you need to enter the PIN code in any of the two scenarios:
 - Your ISP enabled the PIN code verification by default.
 - You manually enabled the PIN code verification from your router's web GUI or your mobile phone.
 - If PIN code verification is enabled, you will see the SIM lock status icon  on the status icon area.
-

WAN Index	
WAN Interface	Mobile Broadband ▾
Enable Mobile Broadband	Enable ▾
Configure the Mobile Broadband settings of 4G-AC55U.	
SIM PIN Management	
USIM Card Status	PIN code is required.
PIN code	<input type="text"/> Save My PIN <input type="button" value="OK"/>
Remaining Attempts: 3	
<input type="button" value="Apply"/>	

- **Username / Password:** Enter the username and password that your 3G/4G network provider has provided.
- **Idle Time:** Enter the time (in minutes) when the router goes into sleep mode when there is no activity in the network.

APN Profile	
Location	Taiwan ▾ <small>* If APN setting cannot be automatically configured, you must manually configure APN parameters.</small>
ISP	TW Mobile ▾
APN Service(optional)	internet
Dial Number	*99#
Username	admin
Password	*****

Internet Connection Configuration

Internet Connection	
Connection status	Connected ?
Network Type	Auto ▾
Connection type	Always Connected ▾
PDP Type	IPv4 ▾
Roaming	Disable ▾

To configure your mobile broadband connection:

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, 3G and 2G network.

- **3G/4G:** Select 3G/4G to allow the wireless router to automatically connect to a 3G or 4G 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.
 - **2G only:** Select this option to automatically connect the wireless router to a 2G network only.
2. **Connection Type:** This field allows you to define your connection policies.
 3. **PDP Type:** The wireless router support several PDP Types, PPP, IPv4, IPv6, IPv6 to IPv4.
 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.
-

Traffic Limitation

Data Usage Limitation	
Data Usage	3.039 MBytes (Starting Day : 1) Clear
Cycle Start Day	1
Data Usage Limit	0 GBytes (Disable : 0)
Data Usage Alert	0 GBytes (Disable : 0)
Send SMS Notification	Enable
Mobile Phone Number	

To configure the Data Usage settings:

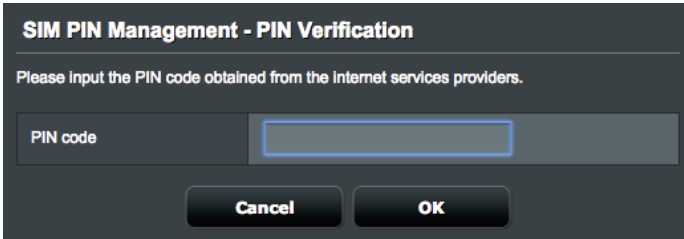
1. **Data usage:** Show the data usage.
2. **Cycle Start Day:** Select the day you wish the data usage to begin to accumulate. The data usage will be reset at the end of each cycle.
3. **Data Usage Limit:** Set the monthly maximum volume of traffic (in GB) for Internet usage. When this limit is reached, an exclamation mark and pop-up alert message will show up when you login administration page, and Internet access is blocked.
4. **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.
5. **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.
6. **Mobile Phone Number:** Enter the mobile number that is going to receive the SMS notification.

Note: The SMS fee is charged to your Micro SIM/USIM card of your router.

7. Click **Apply**.

Configure PIN Code

Enter PIN code if SIM card is required you to enter a PIN Code before apply APN connection.



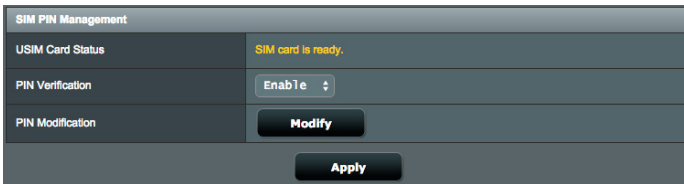
SIM PIN Management - PIN Verification

Please Input the PIN code obtained from the internet services providers.

PIN code

Cancel **OK**

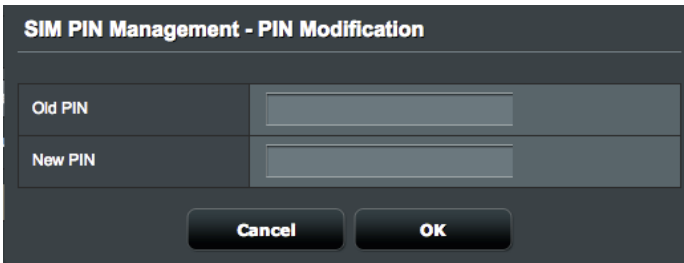
You can also click Modify button to change PIN code when PIN code authentication is enable.



SIM PIN Management

USIM Card Status	SIM card is ready.
PIN Verification	Enable ▾
PIN Modification	Modify

Apply



SIM PIN Management - PIN Modification


Old PIN

New PIN

Cancel **OK**

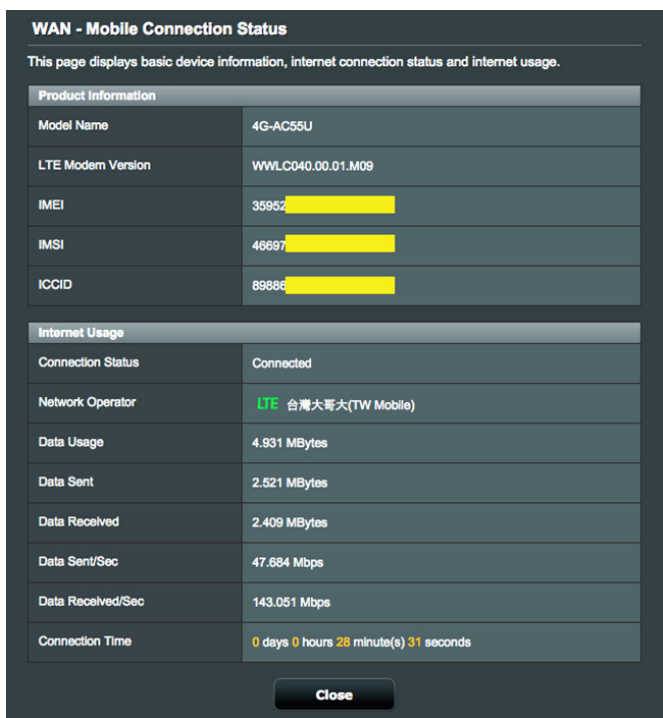
Mobile Connection Status

To find Mobile broadband Information:

1. Click  to find the detail information.

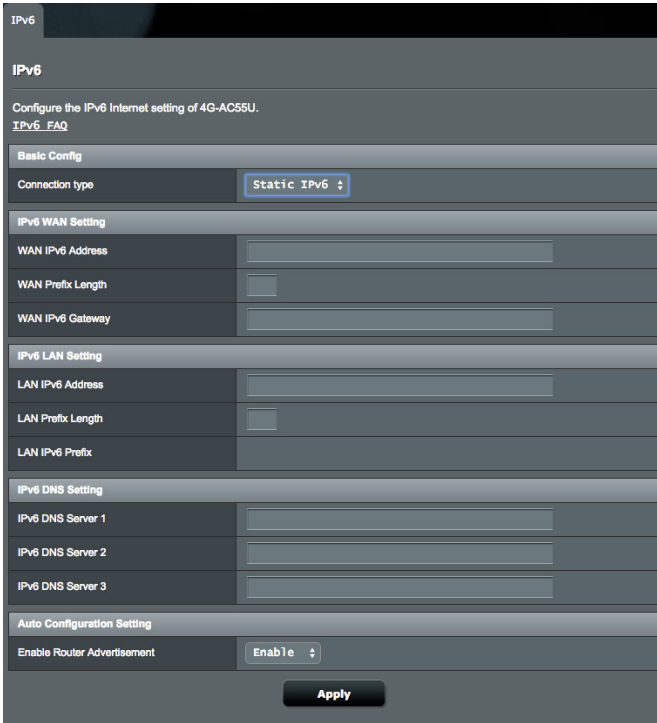


2. The **Mobile Connection Status** screen displays the detailed Mobile Broadband connection status.



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. At the top, it says "IPv6" and "Configure the IPv6 Internet setting of 4G-AC55U." Below that is a link for "IPv6_FAQ". The "Basic Config" section has a "Connection type" dropdown menu set to "Static IPv6". The "IPv6 WAN Setting" section includes fields for "WAN IPv6 Address", "WAN Prefix Length", and "WAN IPv6 Gateway". The "IPv6 LAN Setting" section includes fields for "LAN IPv6 Address", "LAN Prefix Length", and "LAN IPv6 Prefix". The "IPv6 DNS Setting" section includes three fields for "IPv6 DNS Server 1", "IPv6 DNS Server 2", and "IPv6 DNS Server 3". The "Auto Configuration Setting" section has an "Enable Router Advertisement" dropdown menu set to "Enable". At the bottom, there is an "Apply" button.

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:

- **Failover Mode:** Select this mode to use the secondary WAN as the backup network access.
- **Allow Failback:** Tick the checkbox to allow Internet connection switch back to primary WAN automatically when primary WAN becomes available.

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

WAN - Dual WAN

4G-AC55U provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. If the primary WAN connection fails, the secondary WAN automatically brings up a new connection.

Basic Config

Enable Dual WAN	<input checked="" type="checkbox"/> ON
Primary WAN	WAN
Secondary WAN	Mobile Broadband
Dual WAN Mode	Fail Over <input checked="" type="checkbox"/> Allow failback
Hot-Standby	Disable

Ping Time Watch Dog

First Time Delay	0 seconds
Retry Interval	3 seconds <small>*A minimum ping packet consumes approximately 126 bytes per interval. Therefore, the ping detector will consume 106 MBytes per month.</small>
Failover Retry Count	12 (Failover Detection Time: 36 seconds)
Enable User-Defined Target	<input checked="" type="radio"/> Yes <input type="radio"/> No

Apply

- **First time delay:** Set the time delay (in seconds) before the first ping packet is sent out.
- **Retry interval:** Set the time interval (in seconds) between two ping packets.
- **Failover Retry Count:** Set the time (in seconds) when the system triggers the failover or failback action after reaching

the ping test counter and getting no response from the target IP address.

- **Enable User-defined Target:** Select Yes when you want to manually define the target IP address or FQDN (Fully Qualified Domain Name) for the ping test packet.

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.

The screenshot shows the 'WAN - Port Trigger' configuration page. At the top, there is a navigation bar with tabs for Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ, DDNS, and NAT Passthrough. The 'Port Trigger' tab is selected. Below the navigation bar, the page title is 'WAN - Port Trigger'. A descriptive paragraph explains that Port Trigger allows temporarily opening data ports when LAN devices require unrestricted access to the Internet. It notes that there are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port. A link for 'Port_Trigger_FAQ' is provided. Below the description is a 'Basic Config' section with 'Enable Port Trigger' set to 'Yes' (selected) and 'No' (unselected). There is a 'Well-Known Applications' dropdown menu currently showing 'Please select'. Below that is a 'Trigger Port List (Max Limit : 32)' table. The table has columns for Description, Trigger Port, Protocol, Incoming Port, Protocol, and Add / Delete. The table is currently empty, with a message 'No data in table.' at the bottom. An 'Apply' button is located at the bottom of the page.



Description	Trigger Port	Protocol	Incoming Port	Protocol	Add / Delete
		TCP ↓		TCP ↓	+

No data in table.

Apply

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 Port Trigger 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**.
5. 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.
 6. 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 inbound packets will be redirected to the computer you set. It is useful while you run some applications that use unsecured 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
WAN - DDNS						
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					
Apply						

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.

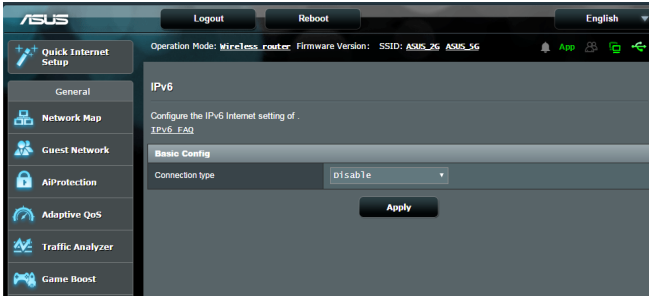
To enable / disable the NAT Passthrough settings:

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**.

Internet Connection	Dual WAN	Port Trigger	Virtual Server / Port Forwarding	DMZ	DDNS	NAT Passthrough
WAN - NAT Passthrough						
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.						
PPTP Passthrough	Enable ▾					
L2TP Passthrough	Enable ▾					
IPSec Passthrough	Enable ▾					
RTSP Passthrough	Enable ▾					
H.323 Passthrough	Enable ▾					
SIP Passthrough	Enable ▾					
Enable PPPoE Relay	Disable ▾					
Apply						

4.4 IPv6

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



To set up IPv6:

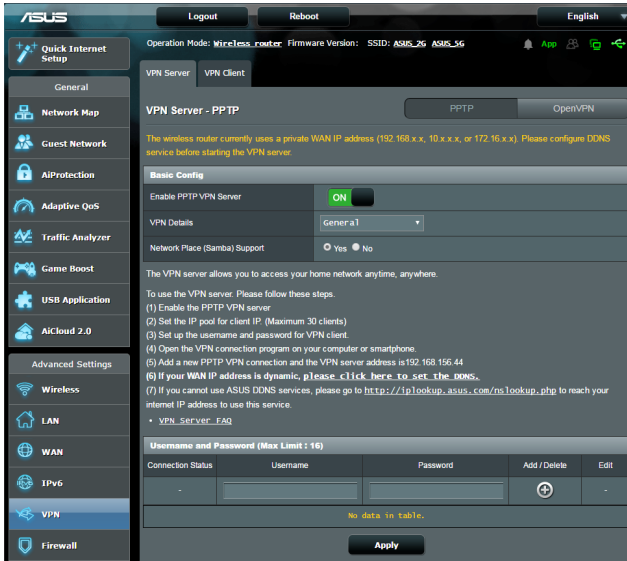
1. From the navigation panel, go to **Advanced Settings > IPv6**.
2. Select your **Connection Type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

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


4.5 VPN Server

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

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



To set up access to a VPN server:

1. From the navigation panel, go to **Advanced Settings > VPN Server**.
2. On the **Enable VPN Server** field, select **Yes**.
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**.

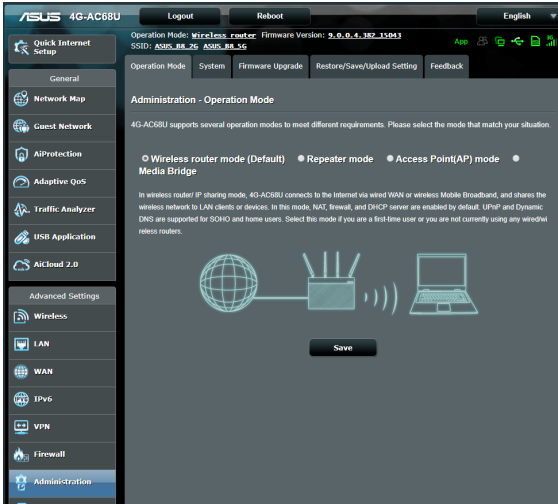
4.6.5 IPv6 Firewall

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.
 - **Repeater Mode:** In Repeater mode, your wireless router wirelessly connects to an existing wireless network to extend the wireless coverage. In this mode, the firewall, IP sharing, and NAT functions are disabled.
 - **Access Point mode:** In this mode, the router creates a new wireless network on an existing network.
 - **Media Bridge:** This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via Ethernet.

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.

The screenshot shows the 'System' configuration page of a router. At the top, there are tabs for 'Operation Mode', 'System', 'Firmware Upgrade', and 'Restore/Save/Upload Setting'. The 'System' tab is selected, and the page title is 'Administration - System'. Below the title, there is a sub-header 'Change the router login password, time zone, and NTP server settings.' and a section 'Change the router login password' with fields for 'Router Login Name' (admin), 'New Password', and 'Retype New Password' (with a 'Show password' checkbox). The 'Miscellaneous' section includes 'Remote Log Server', 'Time Zone' (GMT Greenwich Mean Time), 'NTP Server' (pool.ntp.org), 'Enable Telnet' (Yes/No), 'Authentication Method' (HTTP), 'Enable Web Access from WAN' (Yes/No), 'Auto Logout' (30 minutes), 'Enable WAN down browser redirect notice' (Yes/No), and 'Allow only specified IP address' (Yes/No). Below this is a table for 'Specified IP address (Max Limit : 4)' with columns for 'Client List' and 'Add / Delete'. The table is currently empty, showing 'No data in table.' and an 'Apply' button at the bottom.

Administration - System			
Change the router login password, time zone, and NTP server settings.			
Change the router login password			
Router Login Name	admin		
New Password			
Retype New Password			Show password
Miscellaneous			
Remote Log Server			
Time Zone	(GMT) Greenwich Mean Time		
	* Reminder: The System time zone is different from your locale setting.		
NTP Server	pool.ntp.org		NTP Link
Enable Telnet	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Authentication Method	HTTP		
Enable Web Access from WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Auto Logout	30 minutes (Disable : 0)		
Enable WAN down browser redirect notice	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Allow only specified IP address	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Specified IP address (Max Limit : 4)			
	Client List		Add / Delete
			<input data-bbox="721 1125 739 1152" type="button" value="+"/>
No data in table.			
<input data-bbox="438 1193 534 1214" 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 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.
 - **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.
 - **Auto Logout:** System will auto log out the administration page after an idle period. To disable Auto logout, set the value in 0.
 - **Enable WAN down browser redirect notice:** When WAN connection is down, the system will pop up a screen to guide to how to configure the WAN connection. If you don't like to see this notice, select No to disable the notice.
 - **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.
 - **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/Networking/4G-AC68U/HelpDesk_Download/

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting
Administration - Firmware Upgrade			
Note:			
1. The latest firmware version include updates on the previous version.			
2. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.			
3. In case the upgrade process fails, 4G-AC55U enters the emergency mode automatically. The LED signals at the front of 4G-AC55U will indicate such situation. Use the Firmware Restoration utility on the CD to do system recovery.			
Get the latest firmware version from ASUS Support site at http://www.asus.com/support/			
Product ID	4G-AC55U		
Firmware Version	3.0.0.4_376_6058-gd176ad0 <input type="button" value="Check"/>		
The router cannot connect to ASUS server to check for the firmware update. After reconnecting to the Internet, go back to this page and click Check to check for the latest firmware updates.			
New Firmware File	<input type="button" value="選擇檔案"/> 未選擇任何檔案		
<input type="button" value="Upload"/>			

To upgrade the firmware:

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

NOTES:

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

4.7.4 Restore/Save/Upload Setting



To restore/save/upload wireless router settings:

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**, 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**.

Note: 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)
 - Wireless Log
 - Port Forwarding
 - Routing Table
 - Connection

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	Sat, Jan 31 09:08:39 2015
Uptime	0 days 0 hours 48 minutes 11 seconds

```
Jan 31 09:04:20 iTunes: daemon is stopped
Jan 31 09:04:20 FTP Server: daemon is stopped
Jan 31 09:04:20 Samba Server: smb daemon is stopped
Jan 31 09:04:21 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:21 rc_service: hotplug 32676:notify_rc restart_nasapps
Jan 31 09:04:21 rc_service: waiting "restart_nasapps" via ...
Jan 31 09:04:21 iTunes: daemon is stopped
Jan 31 09:04:21 FTP Server: daemon is stopped
Jan 31 09:04:21 Samba Server: smb daemon is stopped
Jan 31 09:04:22 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:22 iTunes: daemon is stopped
Jan 31 09:04:25 FTP Server: daemon is stopped
Jan 31 09:04:25 Samba Server: smb daemon is stopped
Jan 31 09:04:27 kernel: scsi 2:0:0:0: Direct-Access AGMT 2105 0 PQ: 0 ANSI: 6
Jan 31 09:04:27 kernel: sd 2:0:0:0: Attached scsi generic sgd type 0
Jan 31 09:04:27 kernel: sd 2:0:0:0: [sda] 250099680 512-byte logical blocks: (128 GB/119 GiB)
Jan 31 09:04:27 kernel: sd 2:0:0:0: [sda] Write Protect is off
Jan 31 09:04:27 kernel: sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DTP
Jan 31 09:04:27 kernel: sd 2:0:0:0: [sda] Attached SCSI disk
Jan 31 09:04:27 kernel: FAT-fs (ada2): utf8 is not a recommended IO charset for FAT filesystems, filelay
Jan 31 09:04:27 kernel: FAT-fs (ada3): utf8 is not a recommended IO charset for FAT filesystems, filelay
Jan 31 09:04:27 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:28 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:30 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:44 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:04:54 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
Jan 31 09:05:48 HTTP login: Detect abnormal logins at 5 times. The newest one was from 192.168.1.200.
```

Clear Save Refresh

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 supports different functions. See the comparison table below.

	Wired WAN	LAN as WAN	Mobile broadband
LAN			
IPTV	V	N/A	N/A
Switch Control >> NAT Acceleration(IPv4 Only)	V	N/A	N/A
Switch Control >> Jumbo Frame	V	N/A	N/A
WAN			
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)
Traffic Manager			
QoS	V	V	V
Firewall			
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
Administration			
System >> Enable Web Access from WAN	V	V	V (2)

		Applications	
AiCloud 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

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
 - Device Discovery v1.4.7.1 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
 - Firmware Restoration v1.9.0.4 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Windows Printer Utility v1.0.5.5 at <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
 - The utilities are not supported on MAC OS.
-

5.1 Device Discovery

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

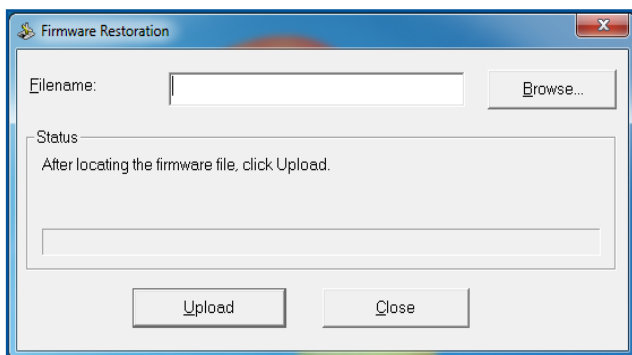
To launch the Device Discovery utility:

- From your computer's desktop, click **Start > All Programs > ASUS Utility > 4G-AC68U Wireless Router > Device Discovery.**

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.



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

NOTE: This feature is not supported on MAC OS.

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

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

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

IP address: 192.168.1.x

Subnet mask: 255.255.255.0

4. From your computer's desktop, click **Start > All Programs > ASUS Utility 4G-AC68U 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.



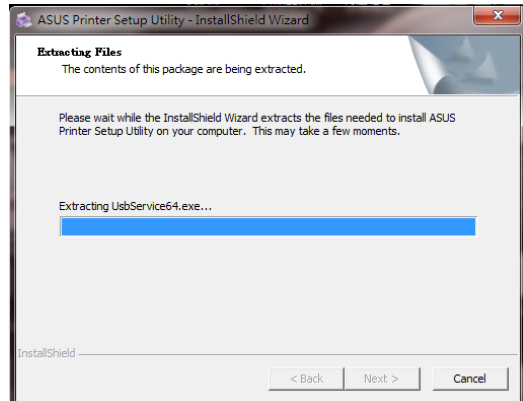
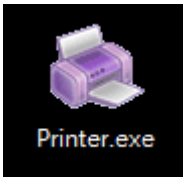
To set up the EZ Printer sharing mode:

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

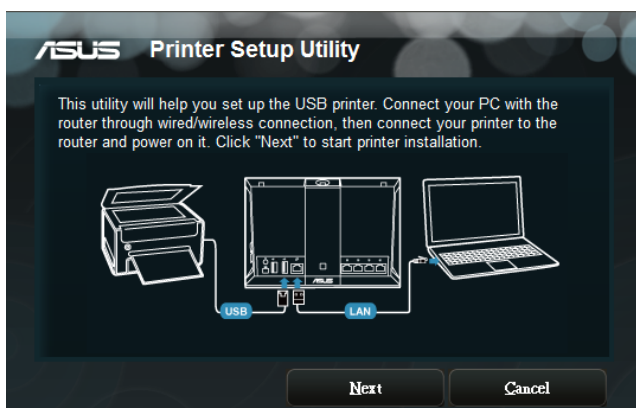


NOTE: Network printer utility is supported on Windows® XP, Windows® Vista, and Windows® 7 only. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

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

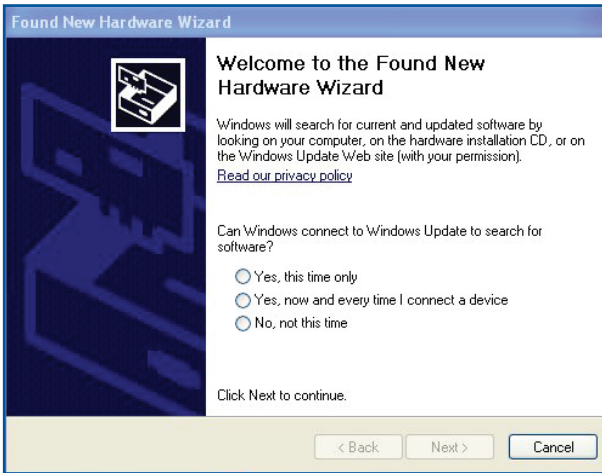


4. Follow the onscreen instructions to set up your hardware, then click **Next**.

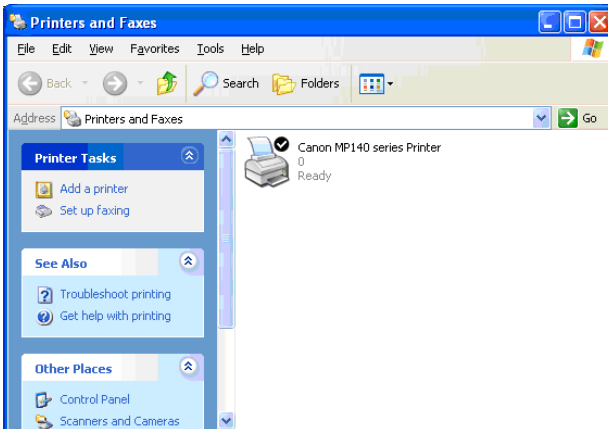


5. Wait a few minutes for the initial setup to finish. Click **Next**.
6. Click **Finish** to complete the installation.

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.



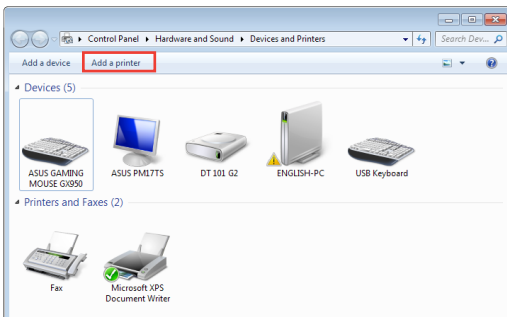
5.3.2 Using LPR to Share Printer

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

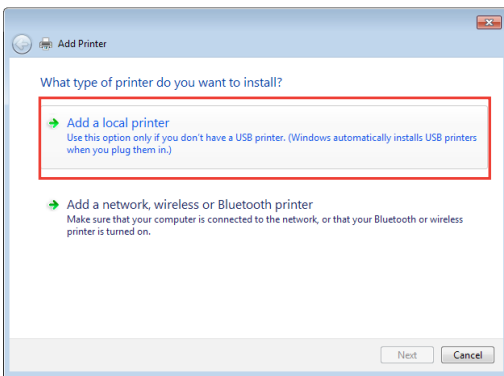
Sharing your LPR printer

To share your LPR printer:

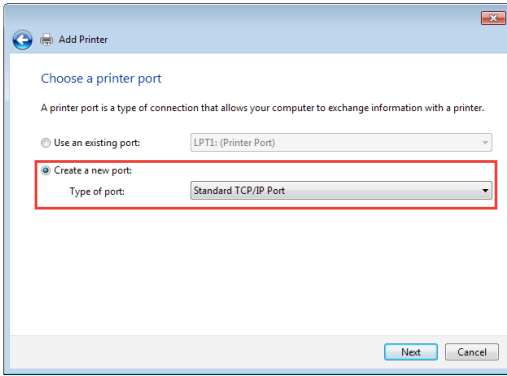
1. From the Windows® desktop, click **Start > Devices and Printers > Add a printer** to run the **Add Printer Wizard**.



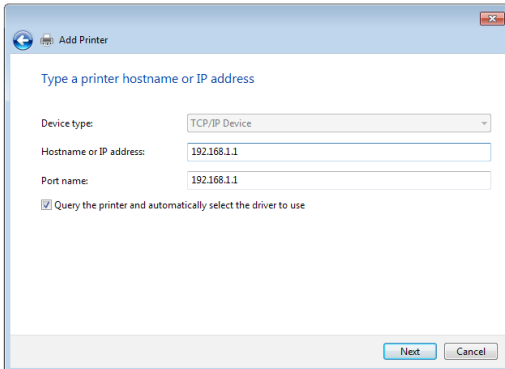
2. Select **Add a local printer** and then click **Next**.



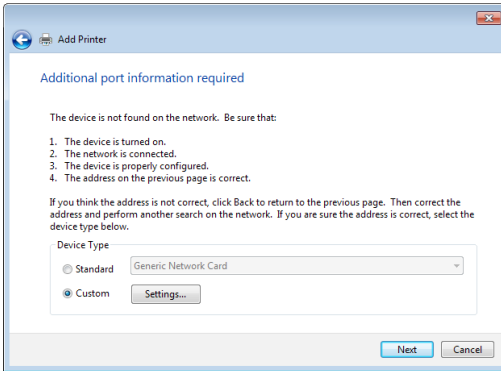
3. Select **Create a new port** then set **Type of Port** to **Standard TCP/IP Port**. Click **New Port**.



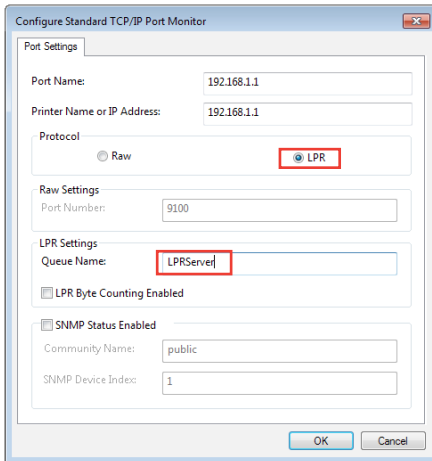
4. In the **Hostname or IP address** field, key in the IP address of the wireless router then click **Next**.



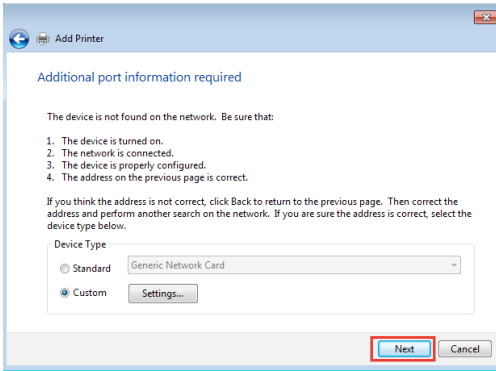
5. Select **Custom** then click **Settings**.



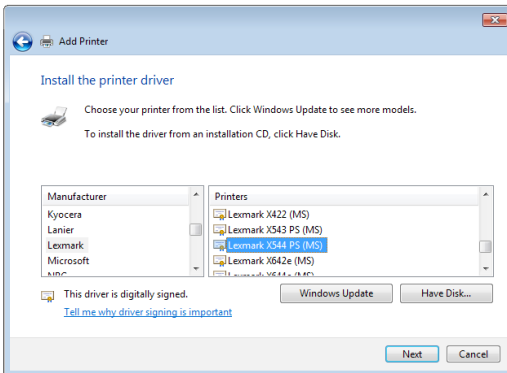
6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.



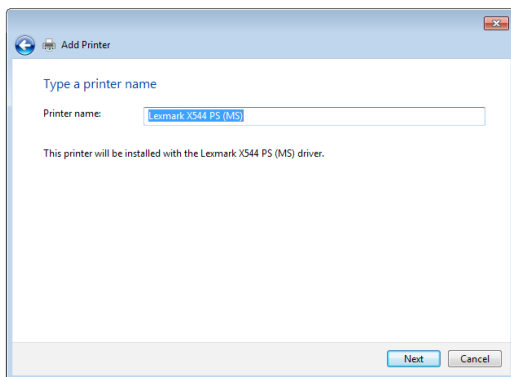
7. Click **Next** to finish setting up the standard TCP/IP port.



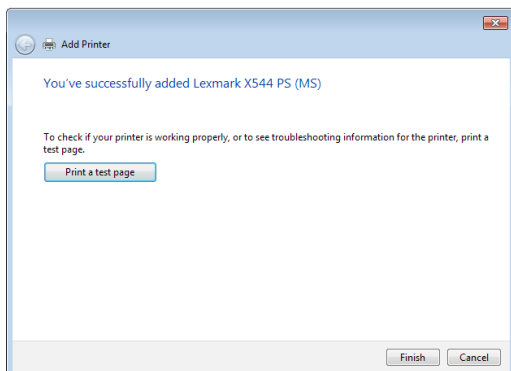
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.



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



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



5.4 Download Master

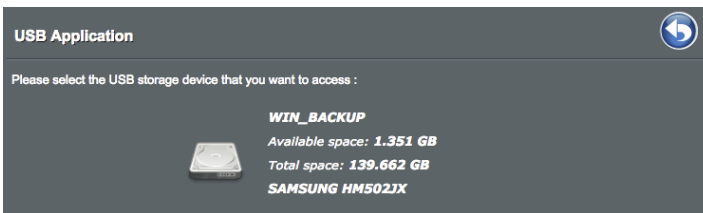
Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

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

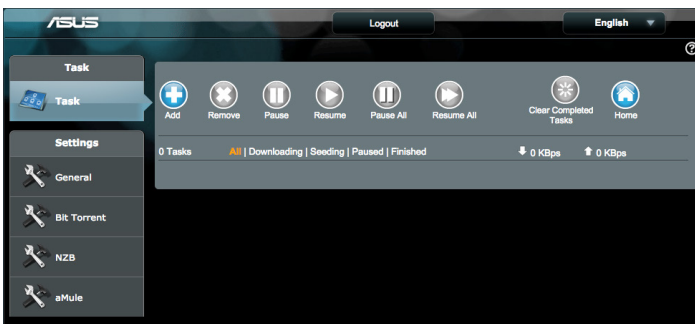
To use Download Master:

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.



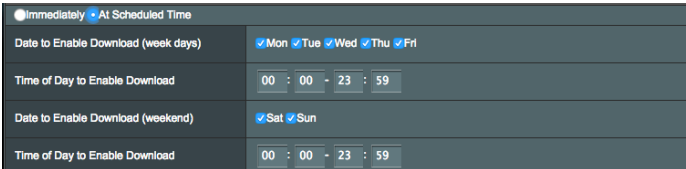
2. After the download process is finished, click the Download Master icon to start using the utility.
3. Click **Add** to add a download task.



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”.

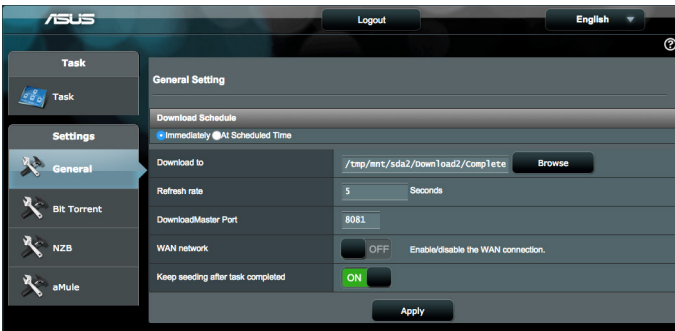
5. Use the navigation panel to configure the **General settings**.
 - You can define the download schedule by Selecting download **Immediately** or **At Schedule Time**.



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**.

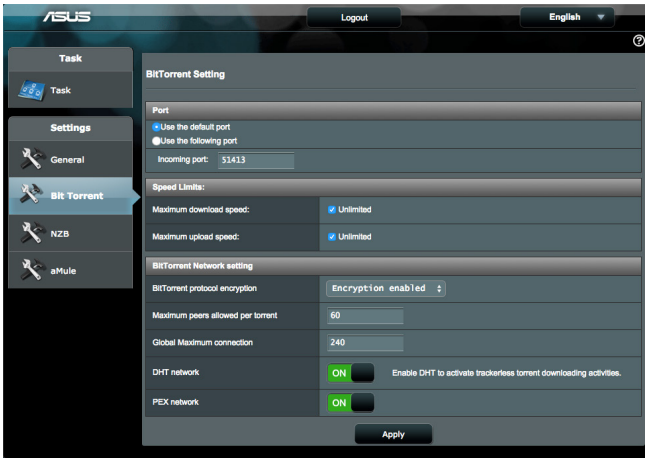


The screenshot shows the ASUS DownloadMaster web interface. On the left is a navigation menu with "Task" and "Settings" sections. The "Settings" section is expanded to show "General". The main content area is titled "General Setting" and contains the following configuration options:

Download Schedule	<input checked="" type="radio"/> Immediately <input type="radio"/> At Scheduled Time
Download to	/tmp/mnt/sda2/download/complete <input type="button" value="Browse"/>
Refresh rate	5 Seconds
DownloadMaster Port	8081
WAN network	<input type="checkbox"/> OFF Enable/disable the WAN connection.
Keep seeding after task completed	<input checked="" type="checkbox"/> ON

An "Apply" button is located at the bottom of the configuration area.

5.4.1 Configuring BitTorrent download settings

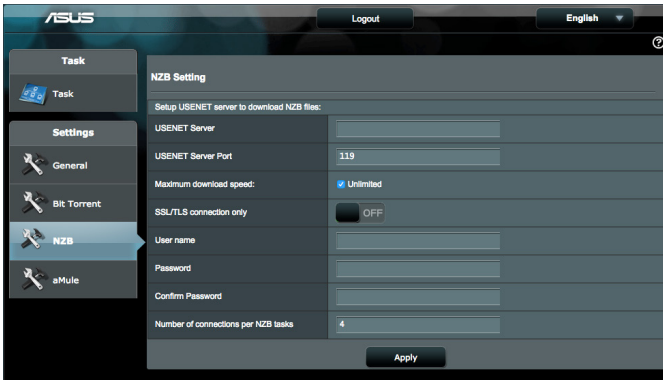


To configure BitTorrent download settings:

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.

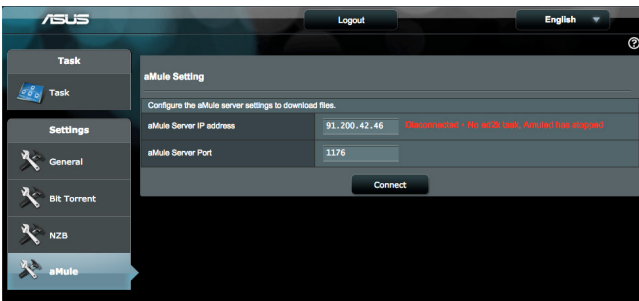
5.4.2 NZB settings

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: <http://support.asus.com/> 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/Networking/4G-AC68U/HelpDesk/Download/> 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 computer.

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

Check if your network settings are correct.

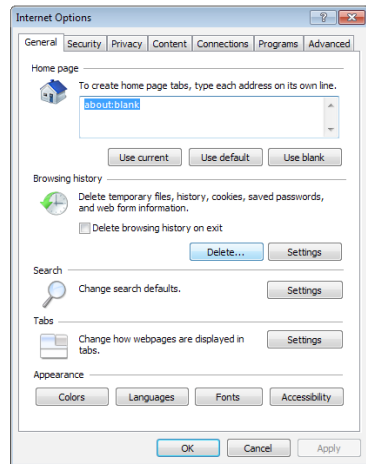
- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account.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

6.2 Frequently Asked Questions (FAQs)

I cannot access the router GUI using a web browser

- If your computer is wired, check the Ethernet cable connection and LED status as described in the previous section.
- Ensure that you are using the correct login information. The default factory login name and password is “admin/admin”. Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer 8, follow these steps:

1. Launch Internet Explorer 8, then click **Tools > Internet Options**.
2. In the **General** tab, under **Browsing history**, click **Delete...**, select **Temporary Internet Files** and **Cookies** 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
Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	192.168.1.1
Domain Name:	(Blank)
Subnet Mask:	255.255.255.0
DNS Server 1:	192.168.1.1
DNS Server 2:	(Blank)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz):	ASUS_XX_5G

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.

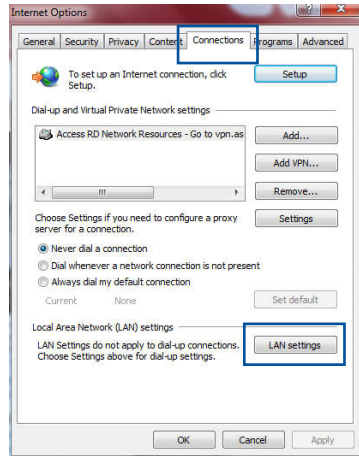
Cannot access Web GUI

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

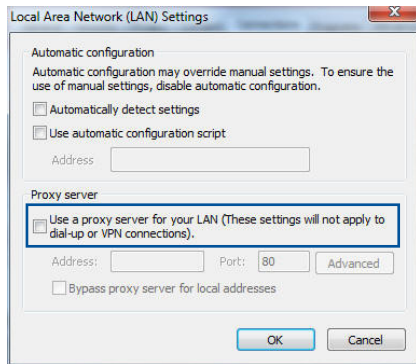
A. Disable the proxy server, if enabled.

Windows® 7

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

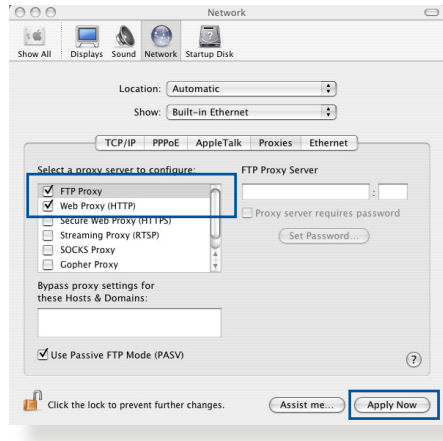


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



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.

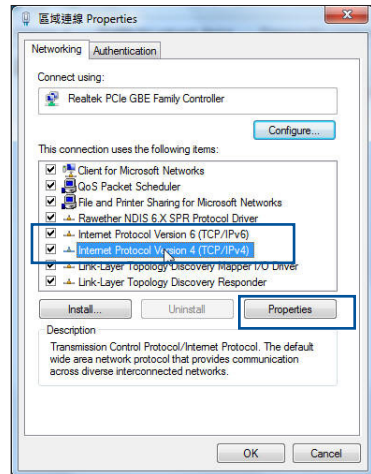


NOTE: Refer to your browser's help feature for details on disabling the proxy server.

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

Windows® 7

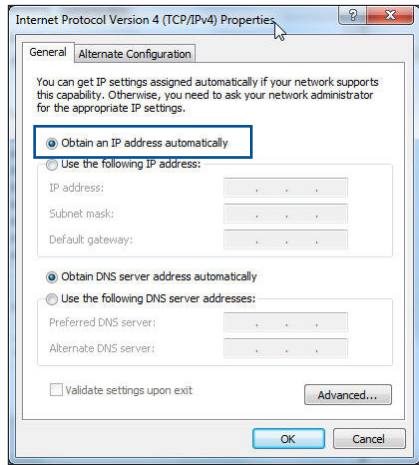
1. Click **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections.**
2. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties.**




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

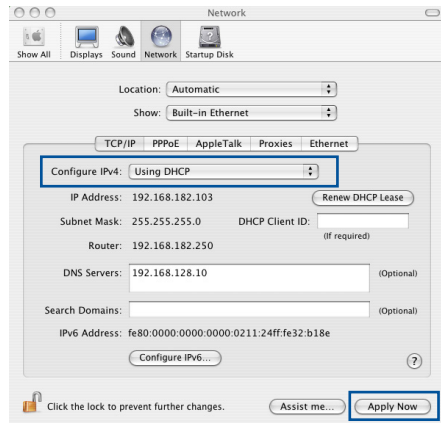
To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

4. 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.

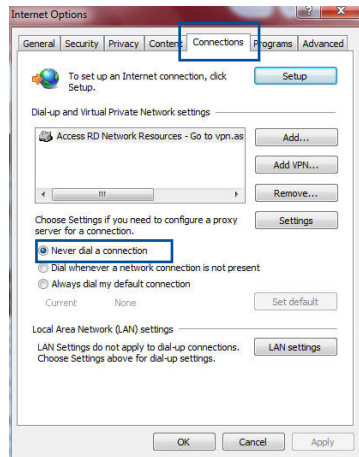


NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

C. Disable the dial-up connection, if enabled.

Windows® 7

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

經型式認證合格之低功率射頻電機，非經許可，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。低功率射頻電機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。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機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 BIL GISAYAR SAN. VE TIC. A.S.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

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

KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİŞ TİC. A.S.

Tel. No.: +90 216 5288888

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

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. (Asia Pacific)

Address 15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Website www.asus.com.tw

Technical Support

Telephone +886228943447
Support Fax +886228907698
Online support support.asus.com

ASUS COMPUTER INTERNATIONAL (America)

Address 800 Corporate Way, Fremont, CA 94539, USA
Telephone +15107393777
Fax +15106084555
Website usa.asus.com
Online support support.asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address Harkort Str. 21-23, D-40880 Ratingen, Germany
Support Fax +49-2102-959931
Website asus.com/de
Online contact eu-rma.asus.com/sales

Technical Support

Telephone (Component) +49-2102-5789555
Telephone Germany
(System/Notebook/Eee/LCD) +49-2102-5789557
Telephone Austria
(System/Notebook/Eee/LCD) +43-820-240513
Support Fax +49-2102-959911
Online support support.asus.com

Networks Global Hotline Information

Region	Country	Hotline Number	Service Hours	
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	France	0033-170949400	09:00-18:00 Mon-Fri	
	Germany	0049-1805010920		
		0049-1805010923 (component support)		09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
		0049-2102959911 (Fax)		
	Hungary	0036-15054561	09:00-17:30 Mon-Fri	
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Austria	0043-820240513	09:00-18:00 Mon-Fri	
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri	
	Belgium	0032-78150231	09:00-17:00 Mon-Fri	
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri	
	Sweden	0046-858769407	09:00-18:00 Mon-Fri	
	Finland	00358-969379690	10:00-19:00 Mon-Fri	
	Denmark	0045-38322943	09:00-18:00 Mon-Fri	
	Poland	0048-225718040	08:30-17:30 Mon-Fri	
	Spain	0034-902889688	09:00-18:00 Mon-Fri	
	Portugal	00351-707500310	09:00-18:00 Mon-Fri	
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri	
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri	
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri	
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri	
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri	
	United Kingdom	+44-1442265548	09:00-17:00 Mon-Fri	
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri	
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri	
Ukraine	0038-0445457727	09:00-18:00 Mon-Fri		

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787 0081-570783886 (Non-Toll Free)	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
			09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917 0065-67203835 (Repair Status Only)	11:00-19:00 Mon-Fri
			11:00-19:00 Mon-Fri 11:00-13:00 Sat
	Malaysia	1300-88-3495	9:00-18:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
	India(WL/NW)		09:00-21:00 Mon-Sun
Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri	
		9:30 – 12:00 Sat	
Vietnam	1900-555581	08:00-12:00	
		13:30-17:30 Mon-Sat	
Hong Kong	00852-35824770	10:00-19:00 Mon-Sat	
Americas	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
	Canada		9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri 08:00-15:00 CST Sat

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800 *9770/00972-35598555	08:00-17:00 Sun-Thu 08:30-17:30 Sun-Thu
Balkan Countries	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
Slovenia		00368-59045400 00368-59045401	08:00-16:00 Mon-Fri
Baltic Countries	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTE: For more information, visit the ASUS support site at:
<https://www.asus.com/support>

Manufacturer:	ASUSTeK Computer Inc.	
	Tel:	+886-2-2894-3447
	Address:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe:	ASUS Computer GmbH	
	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY