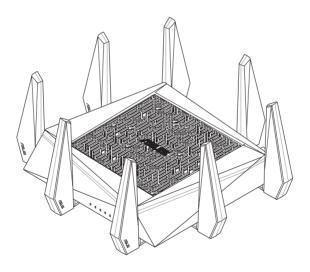
User Guide

RT-AC5300

Wireless-AC5300 Tri-band Gigabit Router





E15858 Revised Edition V3 August 2019

Copyright © 2019 ASUSTeK Computer Inc. All Rights Reserved.

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

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

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

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

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

Table of contents

1	Gettir	ng to know your wireless router	
1.1	Welco	ome!	7
1.2	Packa	ge contents	7
1.3	Your	vireless router	8
1.4	Positi	oning your router1	0
1.5	Setup	Requirements 1	1
1.6	Route	r Setup1	2
	1.6.1	Wired connection1	2
	1.6.2	Wireless connection1	3
2	Gettir	ng started	
2.1		ng into the Web GUI 1	5
2.2	Quick	Internet Setup (QIS) with Auto-detection	6
2.3	Conne	ecting to your wireless network1	9
3	Confi	guring the General settings	
3.1		the Network Map 2	0
	3.1.1	Setting up the wireless security settings2	1
	3.1.2	Managing your network clients2	3
	3.1.3	Monitoring your USB device2	4
3.2	Creati	ing a Guest Network2	7
3.3	AiProt	tection 2	9
	3.3.1	Network Protection	0
	3.3.2	Setting up Parental Controls	4
3.4	Adapt	tive QoS	8
	3.4.1	Bandwidth Monitor3	8
	3.4.2	QoS	9
	3.4.3	Web History4	0
	3.4.4	Traffic Monitor4	1

Table of contents

3.5	Usina	the USB Application	
		Using AiDisk	
		Using Servers Center	
	3.5.3	3G/4G	
3.6	Usina	AiCloud 2.0	
	3.6.1	Cloud Disk	
	3.6.2	Smart Access	
		AiCloud Sync	
4	Confi	guring the Advanced Settings	
4.1		255	55
	4.1.1	General	55
	4.1.2	WPS	57
	4.1.3	Bridge	59
	4.1.4	Wireless MAC Filter	61
	4.1.5	RADIUS Setting	62
	4.1.6	Professional	63
4.2	LAN		66
	4.2.1	LAN IP	66
	4.2.2	DHCP Server	67
	4.2.3	Route	69
	4.2.4	IPTV	70
4.3	WAN .		71
	4.3.1	Internet Connection	71
	4.3.2	Dual WAN	74
	4.3.3	Port Trigger	75
	4.3.4	Virtual Server/Port Forwarding	77
	4.3.4	DMZ	80
	4.3.5	DDNS	81
	4.3.6	NAT Passthrough	82

Table of contents

4.4	IPv6	
4.5	VPN S	erver
4.6	Firewa	all
	4.6.1	General85
	4.6.2	URL Filter85
	4.6.3	Keyword filter86
	4.6.4	Network Services Filter87
	4.6.5	IPv6 Firewall88
4.7	Admi	nistration 89
	4.7.1	Operation Mode89
	4.7.2	System
	4.7.3	Firmware Upgrade91
	4.7.4	Restore/Save/Upload Setting92
4.8	Syster	m Log
4.9	Smart	: Connect
	4.9.1	Setting up Smart Connect94
	4.9.2	Smart Connect Rule97
5	Utiliti	es
5.1	Devic	e Discovery100
5.2	Firmw	vare Restoration101
5.3	Settin	g up your printer server102
	5.3.1	ASUS EZ Printer Sharing 102
	5.3.2	Using LPR to Share Printer 106
5.4	Down	lload Master111
	5.4.1	Configuring Bit Torrent download settings 112
	5.4.2	NZB settings 113

6	Troubleshooting	
6.1	Basic Troubleshooting	114
6.2	Frequently Asked Questions (FAQs)	116
App	pendices	
Noti	ces	125
ASU	S Contact information	139

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS RT-AC5300 Wireless Router! The ultra-thin and stylish RT-AC5300 features 2.4GHz, 5GHz-1 and 5 GHz-2 triple 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% powersaving solution.

1.2 Package contents

- ☑ RT-AC5300 Wireless Router
- Network cable (RJ-45)
- ☑ AC adapter
- Quick Start Guide
- Support CD (Manual)

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

1.3 Your wireless router
Power button Press this button to power on or off the system.
 Power (DC-IN) port Insert the bundled AC adapter into this port and connect your router to a power source.
3 USB 3.0 port Insert USB 3.0 devices such as USB hard disks or USB flash drives into this port.
WAN (Internet) port Connect a network cable into this port to establish WAN connection.
5 LAN 1 ~ 4 ports Connect network cables into these ports to establish LAN connection.
6 Power LED Off: No power. On: Device is ready. Flashing slow: Rescue mode.
 2.4GHz LED Off: No 2.4GHz signal. On: Wireless system is ready. Flashing: Transmitting or receiving data via wireless connection.
 SGHz LED Off: No 5GHz signal. On: Wireless system is ready. Flashing: Transmitting or receiving data via wireless connection.

9	WAN (Internet) LED
	Red: No IP or no physical connection.
	On: Has physical connection to a wide area network (WAN).
10	LAN LED
	Off : No power or no physical connection.
	On: Has physical connection to a local area network (LAN).
A	WPS LED
	Off: WPS verification process is off or completed.
	Flashing: WPS verification process is activated.
12	USB 2.0 port
	Insert USB 2.0 devices such as USB hard disks or USB flash drives into this port.
13	LED On/Off button
	Press this button to turn on/off the LEDs on the panel.
14	WPS button
	This button launches the WPS Wizard.
15	Wi-Fi On/Off button
	Press this button to turn on /off the Wi-Fi connection.

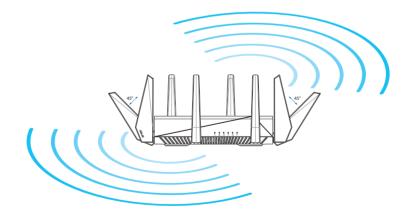
- Use only the adapter that came with your package. Using other adapters may damage the device.
- Specifications:

DC Power adapter	DC Output: +19V with max 3.42A current		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

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

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



1.5 Setup Requirements

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

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

- If your computer does not have built-in wireless capabilities, you may
 install an IEEE 802.11a/b/g/n/ac WLAN adapter to your computer to
 connect to the network.
- With its triple band technology, your wireless router supports 2.4GHz, 5GHz-1 and 5GHz-2 wireless signals simultaneously. This allows you to do Internet-related activities such as Internet surfing or reading/writing e-mail messages using the 2.4GHz band while simultaneously streaming high-definition audio/video files such as movies or music using the 5GHz band.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

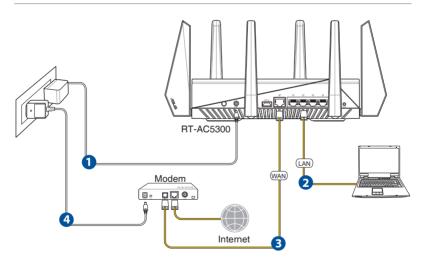
1.6 Router Setup

IMPORTANT!

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

1.6.1 Wired connection

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



To set up your wireless router via wired connection:

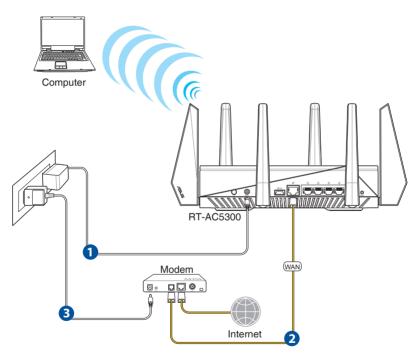
1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.

2. Using the bundled network cable, connect your computer to your wireless router's LAN port.

IMPORTANT! Ensure that the LAN LED is blinking.

- 3 Using another network cable, connect your modem to your wireless router's WAN port.
- 4. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.

1.6.2 Wireless connection



To set up your wireless router via wireless connection:

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

- 2 Using the bundled network cable, connect your modem to your wireless router's WAN port.
- 3. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.
- 4. Install an IEEE 802.11a/b/g/n/ac WLAN adapter on your computer.

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

2 Getting started

2.1 Logging into the Web GUI

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

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

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



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

Top command buttons

2.2 Quick Internet Setup (QIS) with Autodetection

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

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

To use QIS with auto-detection:

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

Windows Security					
The server 192.168.50.1 is asking for your user name and password. The server reports that it is from RT-AC88U.					
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.					
User name Password Remember my credentials					
OK Cancel					

- By default, the login username and password for your wireless router's Web GUI is admin. For details on changing your wireless router's login username and password, refer to section 4.6.2 System.
- The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

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

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

for Automatic IP (DHCP)



for PPPoE, PPTP and L2TP

🖁 Skip Setup Wizerd	Account Setting	
Quick Internet Setup Check Connection	Please enter your username and pase	word
Disternet Setup	Password 2	Pitamiel Correction Information
🗿 Router Setup	MAC Address(optional) 🔹	MAC Clonic
	Enable VPN client	User Name 2
	Special Requirement from ISP	Password 2
	Previous	ext Enter the user name and password for your internet covenaction information. These settings were given by your internet Service Provider (ISP).

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.
- 3. Assign the wireless network name (SSID) and security key for your 2.4GHz and 5 GHz wireless connection. Click **Apply** when done.

🐣 Skip Sctup Wizard	Wireless Setting	
Quick Internet Setup		
Statemet Setup	Assign a unique name or 8&D (Bervice Bet identifier) to help identify your wireless network.	
Router Selay	2.4 Gilly Security	
	Network Kene (SSIII) 🧃 ASUS	
	Network Kay 🙀	
	5 City 1 Security Di Capy 2 4 Gills asteody key to 5 Gills-1 wellings	
	Network Harris (\$500) 🧃 Assis_56-1	
	Nelwork Kay	
	a Lifer 2 Security ID Capy 5 Gi in 1 amends key to 5 Gills 2 settings	
	Network Name (SSIII) (AND Sec.)	
	Network Key 2	
	brine a nationsh koy belavaan ili and bit chandrandyklana, nombans on a condumationt in 64 has digita. The dahadi wanina weariny salitang is 1994/2 Penasani ACC. Ili you da nati, and to anti ha moteois waaring, ianve the wearing hey heid blank, juli dha vagama year an wearing the additionand sciona.	
	Αρρίγ	

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

	System Time Fri, Nay 15 07:	28:94 2019 (GMT)
uick Internet Setup		
Check	Network Name (5500)	
Connection	Nelwork Kay	and 234
6	Wireless Security	WPA2 Poisonal ACS
Internet Setup		
8	Network Hame (5510)	ASUS_931
Router Setup	Network Key	a33417714
	Wireless Security	WPA24Personal - AEB
	Network Hame (\$500)	
	Network Key	anno1234
	Wireless Security	WPA2Pervani - AFS
	WAN Connection Type	Amonte IP
	WAN B"	
	LAN IP	102 (00 1.1
	MAC address	M DD A9.6F.58.39
		Next
		ack .

2.3 Connecting to your wireless network

After setting up your wireless router via QIS, you can connect your computer or other smart devices to your wireless network.

To connect to your network:

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

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

3 Configuring the General settings

3.1 Using the Network Map

Network Map allows you to configure your network's security settings, manage your network clients, and monitor your USB device.



3.1.1 Setting up the wireless security settings

To protect your wireless network from unauthorized access, you need to configure its security settings.

To set up the wireless security settings:

- 1. From the navigation panel, go to **General** > **Network Map**.
- 2. On the Network Map screen and under **System status**, you can configure the wireless security settings such as SSID, security level, and encryption settings.

NOTE: You can set up different wireless security settings for 2.4GHz and 5GHz bands.

2.4GHz security settings



5GHz-2 security settings



5GHz-1 security settings



- 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 High Throughput with WEP or WPA-TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11g 54Mbps connection.

5 Click **Apply** when done.



3.1.2 Managing your network clients

To manage your network clients:

- 1. From the navigation panel, go to **General** > **Network Map** tab.
- 2. On the **Network Map** screen, select the **Clients** icon to display your network client's information.
- 3. Click View List below the **Clients** icon to display all the clients.
- 4. To block a client's access to your network, select the client and click the open lock icon.

3.1.3 Monitoring your USB device

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



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

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

To monitor your USB device:

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

- For more details, refer to the section **3.5.2 Using Servers Center** in this user manual.
- The wireless router works with most USB HDDs/Flash disks (up to 4TB size) and supports read-write access for FAT16, FAT32, NTFS, and HFS+.

Safely removing the USB disk

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

To safely remove the USB disk:

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



3.2 Creating a Guest Network

The Guest Network provides temporary visitors with Internet connectivity via access to separate SSIDs or networks without providing access to your private network.

NOTE: RT-AC5300 supports up to nine SSIDs (three 2.4GHz, three 5GHz-1 and three 5GHz-2).

To create a guest network:

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

Guest Network			
	est Network provides inte al network	met connection for goests be	l realificils accesa fo
Network Name (55ID)			
	Enable	Enable	Enable
Time Remaining			
Access Intranet			
Network Name (SSID)			
Authentication Method			
Network Key	Enable		Enable
Time Remaining	Enable	Enable	Enable
			· · · · · · · · · · · · · · · · ·
	Enable	Inable	Inable
Time Remaining Access Intranet			
Autors master			
		1 10 /	
Help & Support Manual Util	11	FAQ	

- 4. To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
- 5. Assign a wireless name for your temporary network on the Network Name (SSID) field.

Guest Network			
	uest Network provides k ocal network.	nternet connection for guests but re	estricts access to
2.4GHz			
Network Name (SSID)	ASUS_Guest1		
Authentication Method	Open System		
Network Key	None	Enable	Enable
Time Remaining	Umitiess		
Access Intranet			
	Remove		
5GHz-1			
Network Name (SSID)	ASUS_5G-1_Guest1		
Authentication Method	Open System		
Network Key	None	Enable	Enable
Time Remaining	Limitiess		
Access Intranet			
	Remove		
5GHz-2			
Network Name (SSID)	ASUS_5G-2_Guest1		
Authentication Method	Open System		
Network Key	None	Enable	Enable
Time Remaining	Umitless		
Access Intranet			
	Remove		
Help & Support Manual U	tility	FAG) <i>2</i>

- 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. 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.

	AlProtection				
General	A Destaction with	Tread Lines upon coal d	ina astundo manterias ta dat	net making utures and s	they interviewe
Retwork Map	able to access th	your PC or connected o niternel You can also	Ime network monitoring to det devices. Parental Controls let y restrict unwinited websites ar	ect maiware, viruses and c you schedule limes that a c vd apps	onnected device is
🞊 Guest Network					
Alprotection	•		Network Protectio Router Security Assessm Malicious Sites Blocking		
Maptive QoS			Malicious Sinas Blocking Vulnerability Protection Infected Device Preventi		
K USB Application					
aiCloud 2.0		o 📀	Parental Controls		
Advanced Settings		N91	 Time Scheduling Web & Apps Filters 		
🜍 Wineless					
🔂 LAN					
💮 WAN					
😂 1Pv6					
🤹 VPN					
V Firewall					
Administration					
System Log					
💫 Network Tools					Bernath
	Help & Support	Manual Utility		FAQ	P

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.

	Router Security Assessment		ลโ
	Default router login username and password changed -	(<u>No</u>	
	Wireless password strength check -	Very Weak	
	Wireless encryption enabled -	Weak	
	WPS disabled -	Yes	
	UPnP service disabled -		
-7	Web access from WAN disabled -	Yes	
3	PING from WAN disabled -	Yes	CIR
	DMZ disabled -	Yes	
	Port trigger disabled -	Yes	
	Port forwarding disabled -	Yes	
d	Anonymous login to FTP share disabled -	Yes	OFF
ľ	Disable guest login for Network Place Share -	Yes	
r	Malicious Website Blocking enabled -	<u>No</u>	OFF
Ч	Vulnerability Protection enabled -	<u>No</u>	
	Infected Device Prevention and Blocking -	No	
	Close Secure Your Router		

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.

/islis	Logout	Reboot		English 🔻		
W Quick Internet Setup	Operation Mode: Wirelway real Network Protection Parental Cont		i: SSID: Asus Asus_ng	9864B		
Ceneral Retwork Map	AiProtection - Time Schedul		Web & Apps Filters	Time Scheduling		
🚵 Guest Network	June Schecktung alkows you to set the time hind for a ceen'ts network usage. Yo use Time Schecktung 1. In the (Clents Name) catum, select the Clent whose network usage you want to control. You may also sey in the clents MAC address in the (Clents MAC Address) cotum. 2. In the (MaC / Detelly column, cleck the plun(1) count add the core! 3. In the (Time (Time) and column) cleck the plun(1) count add the core!					
AlProtection						
Maptive QoS						
USB Application	Solicit the desired time stats for allowed access times. Drag and hold to create Nonger time stats					
AiCloud 2.0	- c	 Click (OK) to save the settings made. Click to open the hitorial video 				
Advanced Settings		: Clients that are added it ucled by default		e they offernet access		
💝 Wireless	Enable Time Scheduling					
	System Time	Wed, Nov 12 10: Round: The Bake	11:39 2014 n line zone is different from your	iscale settre.		
WAN	Client List (Max Limit : 16)					
1Pv6	Clients N:	ame	Clients MAC Address	Time Add / Delete Management		
🤹 VPN	-	💌	Indu	- 🕀		
Firewall						
Administration		Appl				
System Log						
Network tools						
	O Help & Support Manual Utility		FAQ) e		

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 log 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.

/ISUS	Logout Reboot		English 🔻
Quick Internet Setup	Operation Mode: <u>wineless router</u> F	Firmware Version: SSID: Abub Abub	هد 🚽 🖧 🧧 مد
Setup	Bandwidth Nonitor QoS Web History Traff	tic Monitor	
General	Adaptive QoS - WAN/LAN Bandwidth	Monitor A	pps analysis
Retwork Map			
Suest Network	Upload	Download	11.
AiProtection	nu 200 sau Se shaperpaced 30	The state of the	au
Adaptive QoS	· · · · · · · · · · · · · · · · · · ·		700
USB Application	20.03	36.4	7 🔨
AICloud 2.0		lgliest 🧕 ligh 🥚 Medum 🧶 Law	Lowest Limply
Advanced Settings	Jiewing-58	-	5.5 Hb 🔻
😴 Window	Jiening-PC		G.0 Mb 🔺
🚮 LAN		_	11.0 Mb 🔺
WAN	ZiemingdeKBP		20.1 Mb 🔻
🚳 IPv6			
VPN			
Firewall			
& Administration			
System Log			
Network Tools			
	WANI AN Bandwidh Monitor FAQ	Apply	
4	Help & Support Manual Utility	FAQ) (P)

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.

/ISUS	Logout Reboot English *
Ouick Internet Setup	Operation Model: Vicelana, cuudure Firmware Version: SSID: Adub Abib_AG 😦 🔗 🕞 🥪 🗈 Bandwidth Monitor (Boll Web History Traffic Nentor
General	Adaptive QoS - QoS to configuration
📇 Network Map	Quality of Sarvice (QoS) ansures bandwidth for prioritorial tasks and applications
🔉 Guest Network	 Adaptive QoS assume indound and outbound bandwith on both wired and weeks connections for prioritized applications and tasks via pre-defined, drag and
AiProtection	dap prevents genning, media stawming. VolP and sufficient and the transferring • Traditional QSE ensures intexnal and unbiased benchistor and beach and the transferring weaks comparison for promotion dampingtonic and takes in a meaning used defined
Adaptive QoS	(ECGS) parameters.
💼 USB Application	To enable (EpS function, click the CoS shale switch, and fit in the upload and download Gat the bandwidth information from ISP or go to <u>http://soccedbot.net</u> to check bandwidth.
AlCloud 2.0	QuS FAQ
Advanced Settings	Fraible Smart QoS
💝 Wireless	Apply
🔂 LAN	
🜐 WAN	
🚱 IPVG	

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 <u>http://speedtest.net</u> to check and get your bandwidth.

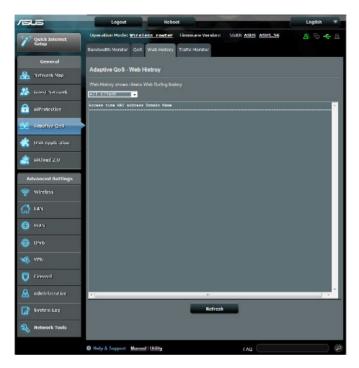
4. Select the QoS Type (Adaptive or Traditional) for your configuration.

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** > **Traffic Analyzer**> **Traffic Monitor** tab.
- 2. (Optional) Click **Refresh** to clear the list.

3.4.4 Traffic Monitor

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.

JS	Logout	1		Reboot						E	nglish
🗖 Quick Internet	Operation Mode	: Winele		ter Fin	nware Versio	in: SSID: A	SUS A	<u>sus se</u>	Ŧ	8	6 *
Setup	Bandwidth Monito	r QoS	Web Histo	ory Traffe	: Monitor						
	Traffic Manag	jer - Traf	tic Mon	itor						val-1	tine
Network Map	Traffic Monitor allow	vis visu to m	onite the i	incomina or	oufooine packe	ts of the following					
Guest Network		Internet			Wred			Wreless			
AiProtection	Reception										
Adaptive Qo%	Transmission										
USB Application	NOTE: Packets for	n Die Interni	et are ever	nly bansmith	ed to the wired a	and wireless davi					
	Traffic Monitor FA										
AiCloud 2.0					ss (2.4GHz)	Wireless ()					
AiCloud 2.0	Ethernet WAN 85.45 KB/s	(WAN)	Wired	white	aa (<i>2.4</i> aniz)					_	_
AiCloud 2.0		(WAN)	Wired	W D GIS	25 (2.4616)						
	85.45 KB/s	(WAN)	Wired								
Advanced Settings		(WAN)	Wired	- WITCH							
dvanced Settings Wireless	85.45 KB/s 59.81 KB/s	(WAN)	Wind								
dwanced Settings Wireless LAN WAN	85.45 KB/s	(WAN)	Levi W								
dvanced Settings Wireless	85.45 KB/s 59.81 KB/s	(WAN)	Wired								
dwanced Settings Wireless LAN WAN	85.45 KB/s 59.81 KB/s		Wind								
udvanced Settings Wireless LAN WAN IPv6	85.45 KB/s 59.81 KB/s 42.72 KB/s		Wind								
dvanced Settings Wireless LAN WAN IPv6 VPN	85.45 KR(5 59.81 KR)s 42.22 KR)s 21.36 KR)s										
dwanced Settings Winkess LAN WAN IPv6 VPN Firewall	85.45 KB/s 59.81 KB/s 42.72 KB/s	1		Average		Hour Z B k				Total	

To configure Traffic Monitor:

- 1. From the navigation panel, go to **General** > **Traffic Analyzer**> **Traffic Monitor** tab.
- 2. (Optional) From the **Traffic Manager Traffic Monitor** pane, select an option (**Real-Time, Last 24 Hours,** or **Daily**) from the drop down list box.

3.5 Using the USB Application

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

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

3.5.1 Using AiDisk

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

To use AiDisk:

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



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



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.

General	
品 Network Map	
🚨 Guest Network	Create your domain name via the ASUS DDNS services.
AiProtection	I will use the service and accept
Maptive QaS	key in the name assocomm.com
USB Application	Oreside DONS
AiCloud 2.0	
Advanced Settings	Previous Next

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

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

3.5.2 Using Servers Center

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

Using Media Server

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

NOTE: Before using the DLNA Media Server function, connect your device to the RT-AC5300's network.

/ISUS	Logout	Reboot	English 🔻
guick Internet	Operation Mode: Wireless row	ter: Firmware Version: SSID: ASUS ASUS 39	¶8 @ € 8
Setup	Hedia Server Network Place (Samb	a) Share / Cloud Disk. FTP Share	
General	Media Server		6
船 Network Map	Set up the iTunes and DLNA media se		
🞎 Guest Network	ITunes Server Enable ITunes Server?	OFF	
AiProtection	Media Server		
Adaptive QoS	Enable DLNA Media Server		
	Media Server Name		
USB Application	Media Server Status		
AiCloud 2.0	Media Server Path Setting	O Ali Disks Shared 🔍 Manual Media Server Path	
Advanced Settings		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.

Using Network Place (Samba) Share service

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

🥖 Šetup	Media Server Network Pla	ace (Samba) Share / Cloud Disk	FTP Share	
General	-	vork Place (Samba) Share		G)
Buest Network	Enable Share	ON		
AiProtection	Allow guest legin			stary to log in a elwork place
Maptive Qus	Device Name			
USB Application	Work Group	VORKGROUP Disable		-
AiCloud 2.0			npty.	,
💡 Wireless	⊕⊙⊘			R 2 R
🚮 lan	L admin	Router	R/W	R No
🜐 wan			Save Permission	

To use Samba share:

 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.

Add new account lace(s	amba) Share / Cloud <mark>X</mark> D s
New account has no re	ead/write access rights.
Account:	
Password:	
Retype password:	
	Add
RT-AC66U	

To delete an existing account:

- a) Select the account that you want to delete.
- b) Click \varTheta.
- c) When prompted, click **Delete** to confirm the account deletion.

To add a folder:

- a) Click 🖳
- b) Enter the folder name, and click **Add**. The folder that you created will be added to the folder list.

The default access rights for a new folder is read/write.
able Share with account Folder Name:
Add

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

Using the FTP Share service

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

IMPORTANT:

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

/ISUS	Logout Reboot	English 💌
Ulick Internet	Operation Mode: <u>Mineless router</u> Firmwa	are Version: SSID: ASUS ASUS SG 🧧 🔠 🔶 🛎
Setup	Media Server Network Place (Samba) Share / Ch	oud Disk FTP Strare
General		
🔒 Network Map	USB Application - FTP Share	
an second study	Set the account and permission of FTP service	
Suest Network	Enable FTP ON	
oiProtection	Allow anothericus login	DFF Commanies and conservation responsions for that print 10 services
Maptive QoS	Maximum number of concurrent connections	
USB Application	Character set on FTP Server	
aithud 2.0		Apply
Advanced Settings	⊕⊙⊘	R R #
💎 Wineless	🔔 admin Rooter	R/W R No
🚮 lan		Save Permission
1000		

To use FTP Share service:

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

- 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.
- 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.

3.5.3 3G/4G

3G/4G USB modems can be connected to RT-AC5300 to allow Internet access.

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

To set up 3G/4G internet access:

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

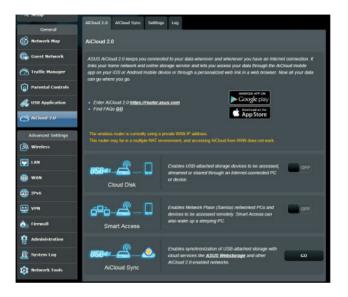
NOTE: PIN code may vary from different providers.

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

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

3.6 Using AiCloud 2.0

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



To use AiCloud:

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

3.6.1 Cloud Disk

To create a cloud disk:

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

USB - Cloud Disk	Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.	OFF
ن اللہ کے الے Smart Access	Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.	OFF
AiCloud Sync	Enables synchronization of USB-atlached storage with cloud services like <u>ASUS Webstorage</u> and other AiCloud 2.0-enabled networks.	GO

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

ć	AiCloud 🗂	
	Welcome. Who's coming home?	
	Your Name.	
	Your Password.	
	9	

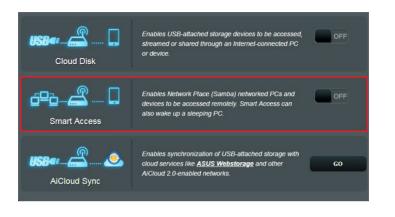
4. You can now start accessing Cloud Disk files on devices connected to the network.

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.

📕 semir — ("abys empryseriet.ev)	Failest IP (181) 80	Teglikk
ക്ക്ASUS AiCloud		
	seent an available device from the list on the left panel to start using AlCloud.	
2 201 241 GB / 745 GB]	• 🔆 🖵 🗖	
ANNEL_CHEN-NB1		
ut Setting C Robush		plante Anglianse

3.6.2 Smart Access

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



NOTES:

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

3.6.3 AiCloud Sync

/ISUS	Logo	nt Rebo	ot	-	En	glish 👻
Quick Internet General Bill Network Map Guest Network Indific Manager Parental Controls XUSB Application	AiCloud 2.0 A	Miceless couter Firm ICloud Sync Settings AiCloud Sync	log	STD: ASIAS ASIAS_S6 d Sync functionality. For st		90 fo
	Cloud List					
Aitloud 2.0	Provider	Usemane	Rule	Folder Name	Connection Status	Delete
Advanced Settings			No data	in table.		
EAN			Add net	waccount		

To use AiCloud Sync:

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

4 Configuring the Advanced Settings

4.1 Wireless

4.1.1 General

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

The Quick Internet	Operation Mode: Mineless route	r Firmware Version: SSID: Asus Asus_3G 🧧 🤔 🥵 🚍 🔶 🖴		
🦉 Setup	General WPS WDS Windows	MAC Filter RADBUS Setting Professional		
General	Wireless - General			
品 Network Map	Set up the wireless related information	below		
🥂 Guest Network	Enabled Smart Connect			
AiProtection	Band	2.4692		
🕋 Adaptive QoS	SSID			
Mainter Traffic Analyzer	Hide SSID	• Yes O No		
	Wireless Mode	Auto 🖉 Optimized for Xbox 🖾 big Protection		
USB Application	Channel bendwidth	20/40 инг.		
AiCloud 2.0	Control Channel	Auto		
Advanced Settings	Extension Channel	Auto		
In the second	Authentication Method	MPA2-Personal		
😴 Wireless	WPA Encryption	ACS I		
🟠 lan	WPA Pre-Shared Key			
🜐 wan	Protected Management Frames	Disable		
30 10v6	Network Key Rotation Interval	3500		

To configure the basic wireless settings:

- From the navigation panel, go to Advanced Settings > Wireless > General tab.
- 2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
- 3. If you want to use the Smart Connect function, move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band 2.4GHz or 5GHz for optimal speed.

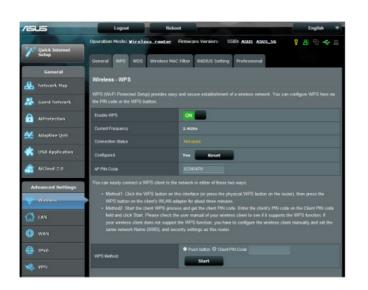
4. Assign a unique name containing up to 32 characters for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

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

- 5. 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.
- 6. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
 - **Auto:** Select Auto to allow 802.11ac, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
 - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
 - **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.
- 7. Select the operating/control channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
- 8. Select the channel bandwidth to accommodate higher transmission speeds.
- 9. Select the authentication method.
- 10. When done, click **Apply**.

4.1.2 WPS

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



NOTE: Ensure that the devices support WPS.

To enable WPS on your wireless network:

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

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

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

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

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

4.1.3 Bridge

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

guick Internet	Operation Model: Wiceless	router Fimware	Version: SSID:	ASUS ASUS_SG	8 9 4 5
5etup	General WPS Bridge 1	Wireless MAC Filter	RADIUS Setting	Professional	
General	Wireless - Bridge				
📇 Network Map					
🚵 Guest Network	Bridge (or named WDS - Wirele WDS may also be considered a able to use half of the access po	repeater mode. Hut w oint's original wireless	th this method, the speed.		
🔒 AiProtection	To enable WDS to extend the w 1. The function only support			P1 security authentication	method
Adaptive QoS	 Select [WDS Only] or [I h Ensure that this wireless 	lybrid] mode and add N router and the AP you	AC address of APs want to connect to	in Remote AP List. use the same channel.	
💼 USB Application	 Key in the remote AP ma mute's MAC eddress 	ic in the remote AP lis	t and open the remo	te AP's WDS managemer	it interface, key in the this
aicloud 2.0	(2.4CHz MAC) 10/8F 48:08: (SGHz MAC) 10/8F 48:08:49 5. You are currently using th	97C			
Advanced Settings	Basic Config				
💡 wireless	Frequency		12 💌		
ᠿ LAN	AP Noda		ılγ 💌		
	Connect to APs in list	• Yes	No		
(D) WAN	Remote AP List				
🚳 ТРиб		Remote AF	*List		Add / Delete
VPN Server			-		Ð
Firewall					
Firewall			Apply		
Administration					

To set up the wireless bridge:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WDS** tab.
- 2. Select the frequency band for the wireless bridge.

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

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

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

You can modify the **Control Channel** from **Advanced Settings** > **Wireless** > **General** tab.

NOTE: Channel availability varies per country or region.

 On the Remote AP List, key in a MAC address and click the Add button (1) to enter the MAC address of other available Access Points.

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

7. Click **Apply**.

4.1.4 Wireless MAC Filter

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

/ISUS	Logout Ret	boot	Logiish 🔻
Ouick Internet Setup	Operation Mode: <u>Wireless router</u>		8 🕤 🔶 B
Ceneral	General WPS WDS Wireless MAC	Filter RADIUS Setting Professional	
Retwork Map	Wireless - Wireless MAC Filter	packets from devices with specified MAC address in your)	Wroless LAN.
Suest Network	Basec Config		
AlProtection	Enable MVC Filter		
Maptive QoS	MAC Filler Mode	Accept +	
dSB Application	MAC filter list (Max Limit : 64)	MAC ther list	Add / Dolote
AiCloud 2.0			Ð
Advanced Settings		We data in table.	
💡 Window		Apply	

To set up the Wireless MAC filter:

- 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.

/ISUS	Logout	Heboot		English 🔻
Ouick Internet	Operation Mode: Wineless r	rautor Firmware Version:	SSID: ASUS ASUS 50	8 6 4 8
Serup	General WPS WDS Wird	less MAC Filter RADIUS Setting	Professional	
Ceneral			Ne al-	
🔠 Network Map	Wireless - RADIUS Setting			
Suest Nelwork	This section allows you to set up a while you select "Authentication M	additional parameters for authorizin Aethod" in "Wineless - General" as '		
AlProtection	Frequency	2.4GH2 *		
	Server IP Address			
Adaptive QoS	Server Part.			
dis Application	Connection Secret			
AlCloud 2.0		Apply		
Advanced Settings				
💝 Windows				

To set up 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** section for configuring your wireless router's Authentication Mode.

- 2. From the navigation panel, go to **Advanced Settings** > **Wireless** > **RADIUS Setting**.
- 3. Select the frequency band.
- 4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
- 5. In the **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.

5.15	Logate R	ebest	Erglich *
flack latened Scho	Internet water surgical matter		18642
Grand	Defined With Mith Withhold	science and a second second	
🐣 Hirbaark Mey	Winsings - Protessional		
	Wheters Technologic Kelling aloos pre		
2 Gerst Milwork	There is a balance of the		
Alfredaction	Property	2.3042	
Matthe Des	bachas	0-10 ® Ho	
	Endlesin levislinint	0-m @Ho	
🚮 USO Application	Duk is Drabik Radie (weik durch	Cheen Citys Citys Citys City	
dis beekin 🏫	Time of Device Crucke Facility	<u>ve ve 21 24</u>	
Advanced realings	Date to Cracke Radio (weekend)	Con Con	
Ser Winder	Time of Day to Gradue Radio		
~	Sector Review	• xn 0 H/	
(i) i #	History Costant	picesie -	
😳 wav	Print and a state of the sping	for same a	
🖨 194	Million Reis Miles	4413	
VPN	thereafting the second s	Long	
NSN VAN	AMEDITE	And is	
Unwell	RTD Treat and	2.917	
🤮 Administration	OT M INNER		
Mattern Lag	the acce internal		
TS against	Professional Contractions	route	
🗞 Helmark laak	Period in Vision Anna	FOR P	
	Private in the second second	Mante -	
	Rolate 15530 Ministers	pisiple -	
	Colimics AMPOU approaches	planeta -	
	Tato GWI	Anally .	
	exploreantening	ensile	
	the statements	eratio	
	Transference and advant	100 N	•
	1	Assty	
	O Holo & Saport Manual Unity	740 /	10

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

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

- Date to Enable Radio (weekend): You can specify which days of the weekend wireless networking is enabled.
- **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the weekend.
- Set AP isolated: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- Roaming Assistant: In network configurations that involve multiple Access, Points or wireless repeater, wireless clients sometimes cannot connect automatically to thefts available AP because they are still connected to the main wireless router. Enable this setting so that the client will disconnect from the main wireless router if the signal strength is under a specific threshold and connect to a stronger signal.
- **Enable IGMP Snooping:** Enable this function allows the IGMP (Internet Group Management Protocol) to be monitored among devices and optimizes wireless multicast traffic.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **AMPDU RTS**: Enable this function allows to build a group of frames before they are transmitted and use RTS for every AMPDU for communication among 802.11g and 802.11b devices.
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.

- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.
- **Enable WMM APSD**: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
- **Reducing USB 3.0 interference**: Enable this function ensures the best wireless performance on the 2.4 GHz band. Disabling this feature increase USB 3.0 port's transmission speed and may affect the 2.4 GHz wireless range.
- **Optimize AMPDU aggregation**: Optimize the max number of MPDUs in an AMPDU and avoid packets get lost or corrupted during transmission in error-prone wireless channels
- **Optimize ack suppression**: Optimize the max number of ack to suppress in a raw.
- **Turbo QAM**: Enable this function allows to support 256-QAM (MCS 8/9) on the 2.4GHz band to achieve better range and throughput on that frequency.
- Airtime Fairness: With airtime fairness, the speed of the network is not determined by the slowest traffic. By allocating time equally among clients, Airtime Fairness allows every transmission to move at its highest potential speed.
- **Explicit Beamforming**: The client's WLAN adapter and router both support beam forming technology. This technology allows these device to communicate the channel estimation and steering direction to each other to improve download and uplink speed.

- **Universal Beamforming**: For legacy wireless network adapter that do not support beam forming, the router estimates the channel and determines the steering direction to improve the downlink speed.
- **TX Power adjustment**: TX Power adjustment refers to the milliWatts (mW) needed to power the radio signal output of the wireless router. Enter a value between 0 to 100.

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

4.2 LAN

4.2.1 LAN IP

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

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

/isus	Logout	Reboot		English 🔻
guick Internet	Operation Mode: Mineless	router Firmware Version:	SSID: ASUS ASUS 56	8 9 4 8
Setup	LAN IP DHCP Server Rou	te IFTV Switch Control		
General	Netter Street B			
🚠 Network Map	LAN - LAN IP			
•1	Configure the LAN setting of R1	-AC3200.		
Guest Network	IP Address			
AiProtection	Subnet Mask			
Maptive QoS		Appl	×	
disk Application				

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.

Terret	Operation Mode: Mirel	eaa_router F	innware Version:	SSID: ASUS ASUS_SG	8 6 4 8
Setup	LAN IP DHCP Server	Route IPTV	Switch Control		
General					
📇 Network Map	LAN - DHCP Server				
😹 Guest Network		IP address and infi	orms the client of the	automatic configuration used on IP n of DNS server IP and default gateway <u>limit:32) FAQ</u>	
AiProtection	Basic Config				1
Adaptive Qu5	Enable the DHCP Server		© Yes ● No		
	Router's Domain Name				
USB Application	IP Pool Starting Address				
AiClaud 2.0	P Pool Ending Address				
Advanced Settings	Lease Time				
Se Wireless	Default Galeway				
•	DHS and WHS Server Setting				
🞧 1AN	DNS Server				1
💮 WAN	WNS Server				
🙈 1Pv6	Enable Manual Assignment	4			
	Enable Manual Assignmen		● Yes ◎ No		
VPN Server	Manually Assigned IP around the COCP Int(Int lane:32)				
💟 Firewall	MAC ad	dress		IP Address	Add/Delete
& Administration					Ð
	No data in kakin.				
System Log			Арр	ty	

To configure the DHCP server:

- 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.

12 Quick Internet	Operation Mode: <u>Whrele</u>	ss router H	imware Version:	SSID: ASUS ASUS 5	<u>s</u> 8	₽ ♣ ₫
Setup	LAN IP DHCP Server	Route IPTV	Switch Control			
General			a 10			
品 Network Map	LAN - Route					
🞎 Guest Network	This function allows you to a same connection to the inte		nto Router. It is usef	ul if you connect several	muters behind Router I	o share the
AiPmtertion	Basic Config	_	-	_	_	_
	Enable static routes		🗢 Yes 🔍 No			
Adaptive Qo5	Static Route List					
de USB Application	Network/Host I		Netmask	Galeway	Metric Interface	Add / Delete
		•			LAN 💌	Ð
AiClaud 2.0			No data in	i table.		
Advanced Settings			Арр	ly		
察 wireless						

To configure the LAN Routing table:

- 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.

/ISUS	l ogout Rebo	st	English 🔻
Oulck Internet	Operation Mode: Wireless router	Firmware Version: SSID: ASUS ASUS 56	8 🕤 🗢 🖻
Sellip	LAN IP DHCP Server Route IPTV	Switch Control	
General			
品 Network Map	LAN - IPTV		-
🎊 Guest Network	To watch IPTV, the WAN port must be com assigned to primary WAN.	ected to the Internet. Please go to <u>WAN - Dual WAN</u> to confi	irm that WAN port is
AiProtection	Port		
	Select ISP Profile	None	
Maptive QoS	Choose IPTV STB Port	None	
disk Application	Special Applications		
AiCloud 2.0	Use OHCP roules	Microsoft	
AICIOUU 2.0	Enable multicast routing (IGMP Proxy)	Disable	
Advanced Settings	Enable efficient multicast forwarding (IGMP Snooping)	utsable -	
🛜 Wireless	UDP Proxy (Lidpry)		
🚮 lan		Αυρίγ	1

4.3 WAN

4.3.1 Internet Connection

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

7 Quick Internet Schup	Operation Mode: <u>Wireless router</u>	irmware Version: SSED: ASUS ASUS ASUS ASU
	Internet Connection Port Inigger Vi	tual Server / Port Forwarding DM2 DDNS NAT Pasethrough
General		
📇 Network Map	WAN - Internet Connection	
😹 Guest Network		WAN (wide ane network) These types are selected from the dmpthen menu heside ler depending on the connection type you selected.
AiProtection	Basic Config	
APProtection	WAN Connection Type	AUTOMATIC TP
Adaptive QoS	Enable WAN	O Yes 🗣 No
🔹 USB Application	Enable NAT	O Yes O No
AiGland 2.8	Enable UPhP UPeP FAQ	© Yes ● No
	WAR DRS Setting	
Advanced Settings	Connect to DNS Server automatically	© Yes ● No
察 Wireless	Account Setting	
	Authenticstion	konc
() WAN	Password	
	Special Requirement from ESP	
S IPV6	HostName	
VPN Server	NAC Address	MAC Clone
💭 Firewall		Λρμίγ

To configure the WAN connection settings:

- 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.

4.3.2 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.
- Load Balance Mode: Select this mode to optimize bandwidth, minimize response time and prevent data overload for both primary and secondary WAN connections.

/545	Logout Raba	ot	Lnglish 🔻
Quick Internet	Operation Mode: Wireless router	Firmware Version: SSID: <u>ASUS_SG</u>	8548
General	Internet. Dual Po Connection WAN The WAN - Dual WAN	rt Virtual Server / Port DMZ DDNS ver Forwarding	NAT Passthrough
Sinest Vetourk	Basic Config		
Manaphive Ques	Enable Cual WAN		
🔹 USB Application	Secondary WAN	USB .	
Advanced Settings	Duzi WAN Node Pring Time Watch Dog	Fall Over 🗹 🖬 Alter Setters	
💡 Wineless	Interval Overay	s seconds	
C LAN	Fail Count Enable Watch Dog	12 • Yes © No	
🚳 TPvi		Apply	

4.3.3 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.

/SUS	Logout		Reboot	-				Engli	sh 🔻
+2 Quick Internet	Operation Mode:)	tireless	router Firmy	are Version:	SSID: ASUS	ASUS_S	G	8 6	* 🖻
Setup	Internet Connection	Dual WAN	Port Trigger	Virtual Ser Forma		DN7	DONS	NA1 Passthrou	gh
General	1		18 - AS						16
📇 Nelwork Map	WAN - Port Trigg	ger							
💑 Guest Network	Port Trigger allows yo two methods for open the time and devices	ing incoming	data ports: port fo	ewarding and po	rt trigger. Port for	varding o	pens the sp	ecified data	ports all
AiProtection	access to the trigger forwarding allows mul								
Maptive QoS	Port Trigger FAC	þ							
Maptive QoS)							
USB Application	Port Trigger FAC	2	• Ye	s O No	=				
	Port Trigger FAC			a O No Se Select	•				
USB Application	Port Trigger FAC Base Config Enable Port Ingger	- 	Ple		•				
IUSB Application	Port Trigger FAV Basic Config Enable Port Ingger Well-Known Applicatio	- 	Ple		Incoming Pr	ərt	Protocol	Add i	Dekate
USB Application AiCloud 2.0 Advanced Settings Windox	Port Tr igger FAC Basis Config Enable Port Ingger Well-Known Applicatio Trigger Port List (I	- 	P1ea 32)	se select	incoming Pr	ort	Protocol		Delote Delote
USB Application	Port Tr igger FAC Basis Config Enable Port Ingger Well-Known Applicatio Trigger Port List (I	- 	P1ea 32)	se select Protocol		nt			

To set up Port Trigger:

- 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** 💮 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**.

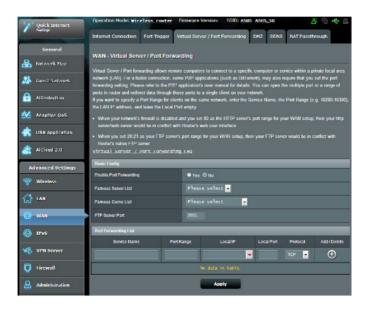
NOTES:

- 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.

4.3.4 Virtual Server/Port Forwarding

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

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



To set up Port Forwarding:

- From the navigation panel, go to Advanced Settings > WAN > Virtual Server / Port Forwarding tab.
- 2. 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.

4.3.4 DMZ

Virtual DMZ exposes one client to the Internet, allowing this client to receive all inbound packets directed to your Local Area Network.

Inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. In a DMZ configuration, one network client receives all inbound packets.

Setting up DMZ on a network is useful when you need incoming ports open or you want to host a domain, web, or e-mail server.

CAUTION: Opening all the ports on a client to the Internet makes the network vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.

To set up DMZ:

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

To remove DMZ:

- 1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
- 2. When done, click **Apply**.

4.3.5 DDNS

Setting up DDNS (Dynamic DNS) allows you to access the router from outside your network through the provided ASUS DDNS Service or another DDNS service.

/ISUS	Logout		Reboot				English 🔻
Terret Quick Internet	Operation Mode: 1	tireless	router firm	ware Version:	SSID: ASUS	ASUS_56	8 6 4 8
Setup	Internet Connection	Dual WAN	Port Trigger	Virtual Serv Forward		DM2 DONS	NAT Passthrough
General							
📇 Network Map	WAN - DDNS						
😹 Guest Network		ldress, throug					ess muter, even with a he ASUS DDNS service
AiProtection	The winders router o This router may be in						
Adaptive QoS	Enable the DDNS CI	ent	• Y	res • No			
USB Application				Apply			
AiCloud 2.0							

To set up DDNS:

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

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

NOTES:

DDNS service will not work under these conditions:

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

4.3.6 NAT Passthrough

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

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

/ISUS	Logout Re	boot	English 🔻
Quick Internet	Operation Mode: Wireless rowter	Firmware Version: SSID: Asus	xsus_xe 78 @ ≪ ≘
Setup		Port Virtual Server / Port risser Forwarding	DMZ DDNS NAT Passthrough
General	WAN - NAT Passthrough		
🚠 Network Map	WAN-NAT Fassurough		
Suest Network	Enable NAT Passthrough to allow a Virtu		s through the router to the network clients
Geest Network	PPTP Passthrough	Enable 🔜	
AiProtection	L2TP Passtbrough	snable 💌	
Maptive QoS	PSec Pasathrough	Enable 🗾	
JUSB Application	RTSP Passtmugh	cnable 💌	
	H 323 Passthrough	Enable 🗾	
AiCloud 2.0	SIP Passthrough	Enable 📕	
Advanced Settings	Enable PPPoE Relay	Disable 🗧	
💝 Wireless		Apply	
🔛 LAN			
() - 99AN			

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.

/ISUS	Logout	Reboot	English 🔻
Quick Internet	Operation Mode: Mireless, route	er Firmware Version: SSID: <u>ASUS ASUS SG</u>	8 % 4 8
General			
品 Network Map	IPv6		
😹 Guest Netsvork	Configure the IPv6 Internet setting of R IPv6_FAQ	outer	
AiProtection	Basic Config		
	Connection type	Disable	
Adoptive QoS	Auto Configuration Setting		
dist USB Application	Enable Router Advertisement	Enable	
AiClaud 2.0		Apply	

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.

SUS	Logout	Reboot		English 🔻
A	Operation Mode: Minel	Ins. router Firmware Version:	SSID: ASUS ASUS_35	
Quick Internet Setup	VPN Server VPN Client			
General			The second second	
Network Map	VPN Server - PPTP		рртр	OpenVPN
Guest Network	Basic Config	<i></i>		
Guest Network	Enable VPN Server			
AiProtection	VPN Details			
Adaptive QoS	Network Place (Samba) Su	ipport 🗢 Yas 🛇 No		
USB Application	The VPN server allows you To use the VPN server. Plo (1) Enable the PPTP VPN			
AiCloud 2.0	(2) Set the IP pool for client (3) Set up the username an	nt IP. (Maximum 10 clients) nd pessword for VPN client.		
		ion program on your computer or smarth connection and the VPN server address		
	(5) If your WAN IP addres	ss is dynamic, <u>please_click_he</u>	re to set the pows.	
👌 LAN	Username and Password	(Max Limet : 16)		
WAN	Connection Status	UserName	Password	Add / Delate
Pv6				Ð
2 IN 19		No data se	tahīe.	

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:

- 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:

- 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.

//SUS	Logout	Reboot		English 🔻
Quick Internet	Operation Mode: Mineless	rauter Firmware Version:	SSID: ASUS ASUS_SG	2 8 @ 4 8
Sector	General URL Filter Keyword	Filter Network Services Filter	IPv6 Firewall	
General	en and a state of the state of			
🔠 Network Map	Firewall - Keyword Filter			
Suest Network	Keyword Filter ellows you to block Limitations of the filtering function		containing the specified keywords	l.
AiProtection	1. Compressed webpages that 2. Https webpages cannot be	use HITP compression technolo iltered.	gy cannot be tiltered <u>see her e</u>	for more details.
Adaptive QoS	Basic Config			
🐇 USB Application	Enable Keyword Filter	Enabled O Disable	ed	
	Keyword Filter List			
aiClaud 2.0		Keyword Filter List		Add / Delete
Advanced Settings				Ð
😪 Wireless		Ku data in t	able.	
🕼 LAN		Apply	-	

To set up a keyword filter:

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

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

NOTES:

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

4.6.4 Network Services Filter

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

Contraction of Contra	Logaut Hab	vat		reglish
💭 Quick Internet	Operation Hode: Hineless router	Finnware Version:	5540: ASIS ASIS 55	1 8 B 🗢 i
Solup	Central URL Filter Keyword Filter	Network Service Filter	IPv8 Citized	
General	Firewall - Network Services Filter		0	
helmork Nep	Les and the second second second second			
🕹 Gunst Network	The Network Services Filer blocks the LAN services.			
Aimotection	For example, if you do not want the device .00 will be blocked Leave the source IP field blank to apply thi		, sey in do in the destination	port. The Native That uses p
🛓 Adaptive QoS	Black List Duration - During the scheduler the specified duration, all the efforts in LV			fed network services. Alter
USB Application	White List Duration : During the schedule After the specified duration, clients in the 'i Internet service.			
aicford 2.0	NOTE off you and the subset for the Welle Interest assets.			
Advanced Settings	- Restance for Byggen Line 2015 & other of the			
Window	Network Services Piller			
	Proble Helwork Services Filler			
1.8.9	and a second sec	Disk List		
£	Filler lable igne	FLOOR FLOOR		
	Well Known Applications	user perfined		
а Э wax	- Andrew Street -		1 55 (m) 15 m	
WAN	Well Known Applications	user teffinel	15 mu 5 m	
WAN	Well Rower Associations Definite Drawline LAN is WAR Disc	user befined S Non S for S we		
WAN	Well Known Applications Date to Fradels LAN to WAR Filter Tanc of Day to Castle LAN to WAR Filter	Discr Defined		
) WAR IPVS UPH Iffcwulf	Wolf Rower Additions Debuts Franks I An Is WAR Film Three silbey to camble LAN to WAR Film Date to Franks I An Is wash Film	User Defined Sinten Since Siver So Sal Sise	30	
WAR Prof UPH Fircoulf Administration	We Hoven Adams Alone Data Is Franks (Als Is Mol Plan Inter Hiller In Lands) (Mar Han Date Is Franks (Als Is Mol Plan Date Is Franks (Als Is Mol Plan Harved Tale) Is Casta (Als Is Mol Plan Harved Tale) (Service) (Mar Tale)	User usfined D Hor D Ive D Yes 00 00 23 D Set D Set 00 00 21 Hot 23	50	
WAR WAR FIFUS FIFUS FIFUS Administration Systems Log	NOT FORMER ADDRESSENS Franks Pradie LAN IS KON FRAN The office for an above LON to WINN Franc The office for an above LON to WINN Franc The office for the second Franc Frank of the formation of the the second Frank Hallows KOM resolutions	User Lisffied S Mar S Lis S Ver 00 00 23 S Sa S San 00 00 24	10 19 Parl Resge Pro	ked Add/Easter
WAR WAR FIFUS FIFUS FIFUS Administration Systems Log	We Hoven Adams Alone Data Is Franks (Als Is Mol Plan Inter Hiller In Lands) (Mar Han Date Is Franks (Als Is Mol Plan Date Is Franks (Als Is Mol Plan Harved Tale) Is Casta (Als Is Mol Plan Harved Tale) (Service) (Mar Tale)	LIGER Defined 1 Diver Defined 2 Diver Diver Diver 00 00 23 Diver Diver 00 00 23 Diver 00 00 00 00 Diver 00 00	19 Se Pat Resge Pro	ked Ale/Table
WAR Prof UPH Filewal Administration Systems Log	We Hoven Adams Alone Data Is Franks (Als Is Mol Plan Inter Hiller In Lands) (Mar Han Date Is Franks (Als Is Mol Plan Date Is Franks (Als Is Mol Plan Harved Tale) Is Casta (Als Is Mol Plan Harved Tale) (Service) (Mar Tale)	User usfined D Hor D Ive D Yes 00 00 23 D Set D Set 00 00 21 Hot 23	19 Se Pat Resge Pro	

To set up a Network Service filter:

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

4.6.5 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.

/ISUS	Logout	Reb	xot.			English 🔻
Quick Internet	Operation Mode:)	fireless router	Firmware Version:	SSID: ASUS ASUS SG	8	
Sctup	General URL Filte	r Keyword Filter	Network Services Filter	1Pv6 Firewall		
General						
🔒 Network Map	Firewall - IPv6 Fi	rewall				
Suest Network	must be specifically a	lowed here.		well as related inbound traffi		
f AiProtection	for example)	note IP empty to allow	i traffic from any remote ne	st. A subnet can also be spe	oned (2001-1	11/222/20064
Maptive QoS	Basic Config					
	Enable IPv0 Firewall		🔍 Yes 🔍 No			
disa Application	Famous Server List		Please select 💌			
🙈 Aicloud 2.0	Inbound Firewall Rule	s (Max Limit : 128)				
	Service Name	Remote IP/CICR	Local IP	PortRange	Protocol	Add / Delete
Advanced Settings					тер 💌	Ð
💎 Wireless			No deta in te	ste.	and the second s	
😭 IAN			Apply			

4.7 Administration

4.7.1 Operation Mode

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

/645	Logout Reboot	English *
Ouick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>ASUS ASUS S6</u>	8 % 4 8
and the second s	Operation Mode System Firmware Upgrade Restore/Save/Upload Setting	
General		
🚠 Network Map	Administration - Operation Mode	
😹 Guest Network	Router supports several operation modes to meet different requirements. Please safect the mode that mat	ch your situation.
🔒 AiProtection	O Wireless router mode (Default) Access Point(AP) mode Media brid	
💒 Adaptive QoS	In weeks to outser 19 sharing mode, Routar connects to the internative PPPer, DHCP, PPTP, L2TP, or State witness network to LAK dents or devices, in this mode, NAT, firewall, and DHCP series are enabled by deb Dynamic LOK's an supported by SDHO and home users. Select this mode if you are a fractime user or you a	
dis USB Application	any wiredwirelies routers.	
AiCloud 2.0	— … —	
Advanced Settings		
💝 Wireless		
😭 LAN		
🖨 wan		
🚱 ІРче	Save	

To set up the operating mode:

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

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 to prevent access.

- 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.
- Client List: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked Yes in the Only allow specific IP item.
- 3. Click **Apply**.

4.7.3 Firmware Upgrade

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

To upgrade the firmware:

- 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**.

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

4.8 System Log

System Log contains your recorded network activities.

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

To view your system log:

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

/345	Logout Reboot	English 👻
12 Quick Internet	Operation Mode: <u>Wineless nutter</u> Firmware Version: SSID: <u>ASUS ASUS 56</u>	8 5 4 5
Setup	General Log DHCP leases Wireless Log Port Forwarding Routing Table	
General	System Log - General Log	
🚠 Network Map		
🚨 Guest Network	This page shows the detailed system's activities. System Time Set, Jan 01 00749:51 2011	
🔒 AlProtection	Uptime 0 daes () hours (1) minutes 10 seconds	
💒 Adaptive QoS	Tan 1 00:31:27 kernel: ethi: Broadcom ECH4321 003 11 Wireless Controller 6.30 102 Jun 1 00:31:27 kernel: ethi: Micoudoms SCH4930 002.11 Maceleys Controller 6.30.102 Tan 1 0:31:27 kernel: device schi anceseg Schaftande mode	
💼 USB Application	Jam 1 00 M1 27 kernel n00, put 2 (200M) entering tradeting pickle Jam 1 00:11:37 kernel: wie pig_ai int sephy: NOT Implemented Jam 10:01:47 27 kernel n00 put 2 (200M) entering terring state	
AICIOUD 2.0	Then 1 (0:81:27 kernel: hrft: part 2(ath) entering forwarding state den 1 (0:31:27 kernel: device with writewed promissionar mode Tan 1 (0:31:27 kernel: hrft: part 2(ath) a unscring literating state	
Advanced Settings	Jun 3.00.31.27 herms. http://www.setains.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.	
💡 Wireless	Jon 1 00:34:27 kernel: b01 part 8/pth02 estering forwarding state Jam 1 00:31:27 kernel: b02: port 6/e10.1) entering learning state Jam 1 60:31:27 kernel: b02: spolary shange detected, propagating	
🚮 LAN	Jun: 3.00.32127 hermal: http://publicline.org/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipation/anticipa	aug-65080582dL684285
😫 WAN	[40] 1. Collection and an energy adopting the function (and) in the list of a control of the list of the	
0V91 🚱	Jan 1 00:33:34 downaweg-doep/5127: 100004069000710500 152.100.1.3 3c-dd:62:0e-11:74 Ten 1 00:33:84 downaweg-doep[510]: TGCDAGE[br0] 150 150 1.3 3c-dd:60:be-f1:74 (Phon	A48.
VPN Server	d dear Save Refresh	
Firewall		

4.9 Smart Connect

Smart Connect is designed to automatically steer clients to one of three radios (one 2.4 GHz, one lowband 5 GHz, one high-band 5 GHz) to maximize total wireless throughput use.

4.9.1 Setting up Smart Connect

You can enable Smart Connect from the Web GUI through the following two ways:

- Via the Wireless screen
- 1. On your web browser, manually key in the wireless router's default IP address: <u>http://router.asus.com</u>.
- 2. On the login page, key in the default user name (**admin**) and password (**admin**) and click **OK**. The QIS page launches automatically.
- 3. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
- 4. Move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band for optimal speed.

• Quick Internet Setup	Operation Mode: <u>wincless route</u>	Firmware Version: SSID: Asus Asus SG 🛛 🛂 🖄 🕞 🔶 🖻		
Semp	General WPS WDS Wireless M	IAC Filter RADIUS Setting Professional		
General	Wireless - General			
Network Map	Set up the wireless related information	below		
Guest Network	Enabled Smart Connect	OFF		
AiProtection	Band	2.4GHz		
Adaptive QoS	SSID			
Traffic Analyzer	Hide SSID	Yas O No		
	Wireless Mode	Auto 🔹 🗖 Optimized for Xbox 🖾 big Protection		
USB Application	Channel bandwidth	20/40 мнz +		
AiCloud 2.0	Control Channel	AUTO		
	Extension Channel	AUEO		
Advanced Settings	Authentication Method	WPA2-Personal		
and the second	WPA Encryption	AES. •		
S LAN	WPA Pre-Shared Key			
WAN	Protected Management Frames	Disable		
IPv6	Network Key Rotation Interval			

- Via the Network Map screen
- 1. Follow the first two steps in the above section to log into the Web GUI.
- 2. From the navigation panel, go to **General** > **Network Map**.
- 3. On the Network Map screen and under **System status**, move the slider to **ON** in the **Smart Connect** field.

5GHz-1	5GHz-2	Status
:t:	OFF	
ie(SSID)		
n Method		
onal	*	
tion		
y		
	n Method onal tion	n Method ona 1

After Smart Connect is enabled, you can check Smart Connect status on the Network Map screen. If you want to change more wireless configurations, click **On/Off** to go to the settings page.



When Smart Connect is enabled, your router will automatically adjust the wireless mode, channel bandwidth, control bandwidth and extension channel settings according to your networking conditions. You can check the changes from the Wireless screen.

Quick Internet	Operation Mode: wireless router SSID: Alen-AC68 General WPS WDS Wireless M	AC Filter RADIUS Setting Professional		
General	Wireless - General			
🞊 Guest Network	Enabled Smart Connect			
AlProtection	SSID	A1en-AC3200		
Adaptive Qo5	Hide SSID	• Yes O No		
Main Traffic Analyzer	Wineless Mode	Auto :		
USB Application	Channel bandwidth	Awto :		
AlCloud 2.0	Edension Channel	Auto :		
	Authentication Method	WPA2-Personal \$		
Advanced Settings	WPA Encryption			
Wireless	WPA Pre-Shared Key	qwas1234		
🚮 LAN	Protected Management Frames			
💮 wan	Network Key Rotation Interval	3600		
IPv6		Арріу		

4.9.2 Smart Connect Rule

ASUSWRT provides default condition settings to trigger switching mechanism. You can also change the trigger conditions according to your networking surroundings. To change the settings, go to the Smart Connect Rule tab on the Network Tools screen.

2 Quick Internet	Operation Mode: W1 N SSID: ASUSPH-Public	less router Himware ver	10n: <u>3.0.0.4.3/8_41/9</u>	28 🔁 🔶 🖴
Setup	Network Analysis N	etstat Wake on LAN Sma	int Connect Rule	
General	Wireless - Smart (Connect Rule		
Retwork Map	Sel up the Smart Conn	ect related information below.		
🞊 Guest Network	Steering Trigger Cond	tion		
AlProtection	Band	2.4GHz	5GHz-1	5GHz-2
Adaptive QoS	Bandwidth Utilization	0	80%	l−−−− ∞
(M) Mashave doo	Enable Load Balance	• Yes 📀 No	🔿 Yes 🙁 No	🔿 Yes 🙁 No
Traffic Analyzer	RSSI	Greater : -58 dBm	Less 💠 D dBm	Less 🗧 0 dBm
USB Application	PHY Rate Loss	Disable	< 54 Mbps	< 433 Mbps
AlCloud 2.0	PHY Rate Greater	> 110 Mops		0 Disable
	VHT			¢ ITA
Advanced Settings	8TA Selection Policy			
🛜 Wireless	RSSI	Greater : -58 dBm	Less ‡ -76 dBm	Less ‡ 0 cBm
	PHY Rate Loss	Disable	Diseble	< 433 Mbps
💮 WAN	PHY Rate Greater	- > 110 Mbps	> 433 Mbpe	Disable
IPv6	VHT			A11 ¢
	Interface Select and Q	alify Procedures		
VPN	Target Band	1: 5GHz-2 ; 2: 5GHz-1	\$ 1: 5GHz-2 \$ 2: 2.4GHz \$	1: 5GHz-1 ; 2: 2.4GHz ;
Firewall	Bandwidth Utilization	0 0%		8 0%
Administration	Bounce Detect			2
_	Window Time	180 seconds		
System Log	Counts			
	Dwell Time	1800 seconds		
		Defau	it Apply	

Smart Connect Rule controls are divided into four sections:

- Steering Trigger Condition
- STA Selection Policy
- Interface Select and Qualify Procedures
- Bounce Detect

Steering Trigger Condition

This set of controls sets the criteria to initiate band steering.

Band	2.4GHz	5GHz-1	5GHz-2
Bandwidth Utilization	0%	 80%	0%
Enable Load Balance	🔵 Yes 💽 No	🔿 Yes 💿 No	•Yes •No
RSSI	Greater ‡ -58 dBm	Less 💠 0 dBm	Less 🛟 0 dBm
PHY Rate Less	Disable	54 Mbps	433 Mbps
PHY Rate Greater	> 110 Mbps		Disable
VHT	A11 \$	¢ [[A]]	¢ 11A

Bandwidth Utilization

When bandwidth use exceeds this percentage, steering will be initiated. Broadcom's documentation does not say how utilization is measured.

Enable Load Balance

This controls load balancing. Broadcom's documentation does not indicate how balancing is done.

RSSI

If the received signal level of any associated client meets this criteria, steering will be triggered.

• PHY Rate Less / PHY Rate Greater

These controls determine STA link rates that trigger band steering.

• VHT

This controls determines how 802.11ac and non-ac clients are handled.

- ALL (default) means any type of client can trigger steering.
- AC only means a client must support 802.11ac to trigger steering.
- **Not-allowed** means only non-802.11ac clients will trigger steering, i.e. 802.11a/b/g/n.

STA Selection Policy

Once steering has been triggered, ASUSWRT will follow the STA Selection Policy to select a client(STA) that is going to be steered to the most appropriate band.

RSSI	Greater ‡ -58 dBm	Less 💠 -76 dBm	Less 🛟 0 dBm
PHY Rate Less	Disable	Disable	<433 Mbps
PHY Rate Greater	> 110 Mbps	> 433 Mbps	Disable
VHT	A11 +	A11 ÷	A11 ÷

Interface Select and Qualify Procedures

These controls determine where the steered client will end up. The **Target Band** controls specify first and second choice of steering targets. Clients meeting the STA selection policy criteria for the radio will be steered to the first target if that radio's **Bandwidth Utilization** is less than the set value. Otherwise, the client will be sent to the second **Target Band** radio.



Bounce Detect

This set of controls determines how often a client can be steered. This is intended to prevent clients from constantly moving around. It does not, however, prevent clients from disconnecting on their own, or counting them as bounces if they do. Each client can be steered N **Counts** within the **Window Time**. When the Count limit is hit, the client will not be steered again for **Dwell Time**.

Bounce Detect	
Window Time	180 seconds
Counts	
Dwell Time	1800 seconds

5 Utilities

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
 - Device Discovery v1.4.7.1 at <u>http://dlcdnet.asus.com/pub/ASUS/ LiveUpdate/Release/Wireless/Discovery.zip</u>
 - Firmware Restoration v1.9.0.4 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Rescue.zip</u>
 - Windows Printer Utility v1.0.5.5 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Printer.zip</u>
- 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 > RT-AC5300 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.

limware Restor	ation	×
<u>F</u> ilename:		<u>B</u> rowse
Status After locating t	he firmware file, click Upload.	
	<u>U</u> pload <u>C</u> lose	

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

NOTE: This feature is not supported on MAC OS.

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

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

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

IP address: 192.168.1.x

Subnet mask: 255.255.255.0

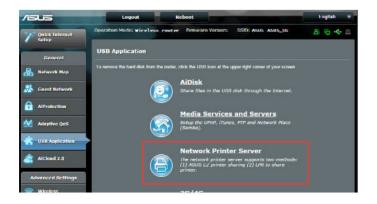
- From your computer's desktop, click
 Start > All Programs > ASUS Utility RT-AC5300 Wireless
 Router > Firmware Restoration.
- 5. Specify a firmware file, then click **Upload**.

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.



NOTE: The print server function is supported on Windows® XP, Windows® Vista, and Windows® 7.

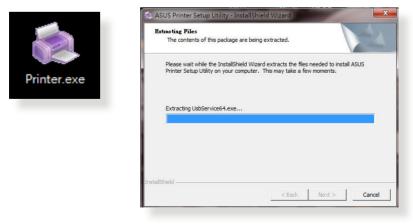
To set up the EZ Printer sharing mode:

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

Quick Internet	Operation Model Virelex conter Firmware Version: SSID: Asias Asia_sa	8 6 4 8
General	Network Printer Server	5
🔠 Network Map	The network printer server supports two methods. (1) ASUS EZ printer sharing (2) LPR to share printer	
Suest Network	ASUS EZ printer sharing (Windows OS only) EAQ Download Now! Use LPR protocol to sharing printing LAQ (Windows)	
f AiProtection	Use LPR protocol to sharing printing FAQ (MAC)	
Adaptive Qo5		
🔹 USB Application		

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**.

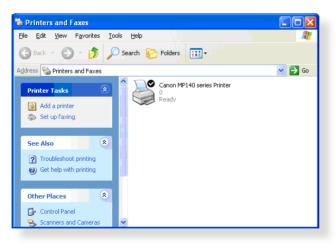


- 5. Wait a few minutes for the initial setup to finish. Click **Next**.
- 6. Click **Finish** to complete the installation.

7. Follow the Windows[®] OS instructions to install the printer <u>driver</u>.



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

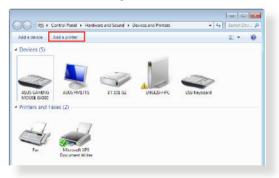


5.3.2 Using LPR to Share Printer

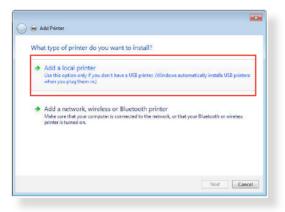
You can share your printer with computers running on Windows[®] and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

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.

Choose a printer port		
A printer port is a type of con	nection that allows your computer to exchange information with a	orinter.
Use an existing port:	LPT1: (Printer Port)	12
Oreate a new port:		
Type of port:	Standard TCP/IP Port	
A STREET OF STREET		

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

🕝 🖶 Add Printer		
Type a printer hostnar	ne or IP address	
Device type:	TCP/IP Device	v
Hostname or JP address:	192.168.1.1	
Port name:	192.168.1.1	
🗹 Query the printer and auto	ematically select the driver to use	
	Next	Cancel

- 5. Select **Custom** then click **Settings**.
 - Add Printer

 Additional port information required

 The device is not found on the network. Be sure that:

 The device is not found on the network. Be sure that:

 The device is not found on the network. Be sure that:

 The device is properly configured.

 The device is properly configured.

 The device is not found on the network. Be sure that:

 Type think the address is mot context, click Back to reform to the previous page. Then correct the device type below.

 Device Type
 Stendard General Network Cont

 Custom Sattings.

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

Configure Standard TCP/IP Po	ort Monitor
Port Settings	
Port Name:	192.168.1.1
Printer Name or IP Address	s: 192.168.1.1
Protocol	
Raw	LPR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	LPRServer
LPR Byte Counting Er	nabled
SNMP Status Enabled	1
Community Name:	public
SNMP Device Index:	1
	OK Cancel

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

	t information required	
The device is not	found on the network. Be sure that	
1. The device is		
 The network i The device is 	s connected. properly configured.	
	n the previous page is correct.	
	ddress is not correct, click Back to return to the p orm another search on the network. If you are su v.	
Device Type		
() Standard	Generic Network Card	-

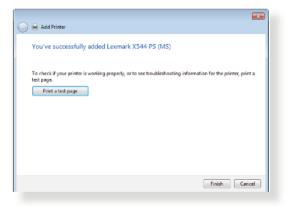
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.

Install the printer drive	r.		
Choose your printer	from the list. Click	Windows Update to see more models.	
To install the driver	from an installation	CD, click Have Disk.	
Manufacturer	* Printers		
Kyocera	Lem	ark X422 (MS)	
Lanier	🗌 🗔 Lem	ark X543 PS (MS)	
Lesmark	In Learn	ark XS44 PS (MS)	
Microsoft		ark X64Ze (MS)	
sinc	The Party of Street of Str	J. Veral, mars	
This driver is digitally sig	and the second sec	Windows Update	Have Disk

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 the Bit Torrent download settings**.

- Task
 General Selling

 Sattings
 Refresh fat:

 Sattings
 Apply

 Ceneral
 Apply

 States
 Apply
- 5. Use the navigation panel to configure the advanced settings.

5.4.1 Configuring Bit Torrent download settings

/ISUS		
Task	Bit Torrent Setting	
🧱 Task	Put	
Settings	Use the default port Use the following port Incoming port	
Seneral	Speed Limits:	
	Naulmum download speed:	KENS
Bit Torrent	Hadmum upload speed:	Keis
	Billioment Network setting	
N78	BillTorrent protocol encryption	Encryption disabled 👱
	Max poors allowed per torrent	100 Enable DHT to activate tracticess forment download
	DHT network	Phase LPT I I SCHOOL TROCESS INTERFORMULAD
		Apply

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 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.

5.4.2 NZB settings

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

Task			
	NZB Setting		
Task	Setup USENET server to download NZB files:		
	USENET Server		
Settings			
	USENET Server Port	119	
Seneral	Maximum download speed	KB/S	
it Torrent	SSL/TLS connection only		
	User name		
B	Password		
	Contrm Password		
	Number of connections per NZB tasks	2	
		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:

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

6.1 Basic Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

Upgrade Firmware to the latest version.

- Launch the Web GUI. Go to Advanced Settings > Administration > Firmware Upgrade tab. Click Check to verify if the latest firmware is available.
- 2. If the latest firmware is available, visit the ASUS global website at <u>http://www.asus.com/Networks/Wireless_Routers/</u><u>RTAC5300/#download</u> to download the latest firmware.
- 3. From the **Firmware Upgrade** page, click **Browse** to locate the firmware file.
- 4. Click **Upload** to upgrade the firmware.

Restart your network in the following sequence:

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

Check if your Ethernet cables are plugged properly.

- When the Ethernet cable connecting the router with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your 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 mehtod, and password are correct.

Check if your network settings are correct.

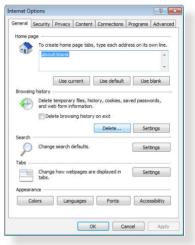
- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. 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:
 - Launch Internet Explorer 8, then click Tools > Internet Options.
 - 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:
 - Launch the web GUI. Go to General > Network Map> Clients and search for the device that you want to connect to the router.
 - If you cannot find the device in the Network Map, go to Advanced Settings > LAN > DHCP Server, Basic Config list, select Yes on the Enable the DHCP Server.

/sus	Logout Rebool		English 🔻
Quick Internet	Operation Mode: <u>Wireless</u> router Fi	mware Version: SSID: <u>ASUS ASUS SG</u> Switch Control	8 단 속 요
General	LAN - DHCP Server		
Guest Network		is a protocol for the automatic configuration used on IP ne rms the client of the of DNS server IP and default gateway HCP_list(list_limit;32).FAQ	
AiProtection	Basic Config		
Adaptive Qo5	Enable the DHCP Server	© Yes ● No	
	Router's Domain Name		
TSB Application	IP Pool Starting Address		
AiClaud 2.0	IP Pool Ending Address		
Advanced Settings	Lease Time	86400	
😪 Wireless	Detault Galeway		
	DNS and WINS Server Setting		
70255	DNS Server		
💮 wan	WINS Server		
1Pv6	Enable Manual Assignment	14000000000	
VPN Server	Enable Manual Assignment	• Yes O No	
Tirewall	Namually Assigned IP around the DACP listics	P Addresa	Add/Delete
×			(f)
Administration		No data in table,	
📝 System Log		Apply	

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

/ISUS	Logout Rebu	oot	English 💌
Quick Interact Schup	Operation Mode: <u>Wireless</u> router	Firmware Version: SSID: <u>ASUS ASUS 36</u> IAC Filter RADIUS Setting Professional	8 6 4 8
General	Wireless - General		
🔏 Guest Netwurk	Set up the wireless related information belo	w. 2,46Hz -	
AiProtection	SSID	ASUS	
🚧 Adaptive Qo5	Hide SSID	● Yes ◎ No	
de USB Application	Wireless Node	Auto 💌 🖬 sig Projection	
	Channel bandwidth	20/40 MHz 💌	
AiClaud 2.0	Control Channel	Auto 💌	
Advanced Settings	Authentication Nethod	Open System 🗾	
💡 Windess	WEP Encryption	Norhi	
		Apply	

- 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.

/1545	Logout	Reboot			English
Ten Quick Internet	Operation Mode: wirelie	s router Firmware	Version: SS	ID: ASUS_ASUS_NG	8 G 🔶 E
Setup	Operation Mode System	Ermware Upgrade	Restore/Sav	e/Upload Setting	
General			1952		
🔒 Network Mop	Administration - Rest	ore/Save/Upload Se	ling		
	This function allows you to s	ave current settings of Ho	uter to a tile, or i	inad settings from a file	
auest Network	Factory default	Real Property in the International P	estore		
AiProtection	Save setting		Save		
Maptive OoS			Pave		
and woodprove data	Restore setting		pload	Chanse Fiel No file chosen	
📩 USB Application					
AiCloud 2.0					

Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to General> Network Map, and check the Internet Status.
- If your router cannot connect to your ISP's WAN IP address, try restarting your network as described in the section **Restart your network in following sequence** under **Basic Troubleshooting**.



- The device has been blocked via the Parental Control function. Go to General > Parental Control and see if the device is in the list. If the device is listed under Client Name, remove the device using the Delete button or adjust the Time Management Settings.
- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.
- Check the status indicators on the ADSL modem and the wireless router. If the WAN LED on the wireless router is not ON, check if all cables are plugged properly.

You forgot the SSID (network name) or network password

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

How to restore the system to its default settings?

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

The following are the factory default settings:

User Name:	admin
Password:	admin
Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	http://router.asus.com (or 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
SSID (5GHz):	ASUS_5G

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

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

0	o set up an I	L	action allak	_	Setu	
	ietup.	itemet conne	ection, cick		Setu	
ial-up an	d Virtual Priva	ate Network s	ettings			
😂 Aco	ess RD Netwo	rk Resources	- Go to vpn.	as	Add.	ù 👘
					Add VP	N
4	III			•	Remov	e
erver fo Neve Dial v	ettings if you r a connectio r dial a conne vhenever a n	n. ction etwork conne	ction is not p		Settin	igs
Alway	ys dial my def	ault connection	on	_		
Curren	it No	ne			Set def	ault
ocal Area	Network (LA	N) settings -				3
LAN Set	tings do not a Settings abov	pply to dial-up e for dial-up s	p connection settings.	s.	LAN set	tings

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

utomatic cor	figuration figuration m l settings, di			ngs. To ensure the ation.
Automatic	ally detect se	ettings		
Use autom	natic configur	ration script		
Address				
roxy server				
Use a prop	ky server for VPN connect		hese setting	s will not apply to
			1	
		P	ort: 80	Advanced
Address:	s proxy serv			Advanced
Address:	s proxy serv			Advanced
Address:	s proxy serv			Advanced

MAC OS

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

Proxies Ethernet Proxy Server Proxy Server requires pass (Set Password)	
Proxy Server	
: Proxy server requires pass	
Proxy server requires pass	
Proxy server requires pass	
(Jer Password)	

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.

Connect using:		
Realtek PCIe G	BE Family Controller	
		Configure
This connection uses t	the following items:	
Client for Micr		
QoS Packet :		10000 /001
	er Sharing for Microsoft DIS 6.X SPR Protocol E	
	col Version 6 (TCP/IP	
	col Version 4 (TCP/IP	
	pology Discovery Map	
	opology Discovery Res	ponder
		Properties
Link-Layer To	opology Discovery Res	
Link-Layer To Install Description Transmission Control	Uninstall	Properties tocol. The default
Link-Layer To Instal Description Transmission Contro wide area network p	upology Discovery Res	Properties tocol. The default
Link-Layer To Instal Description Transmission Contro wide area network p	Uninstall	Properties tocol. The default
Link-Layer To Instal Description Transmission Contro wide area network p	Uninstall	Properties tocol. The default

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.

eneral	Alternate Configuration				
this cap	n get IP settings assigned autor ability. Otherwise, you need to appropriate IP settings.				
() ()	otain an IP address automatical	ly:			
- () Us	e the following IP address:				
IP ad	ldress:			2	
Subr	et mask:	*	10	х	
Default gateway:		i.	141	3	
() O	otain DNS server address autor	natically			
OU	e the following DNS server add	resses:			
Pref	erred DNS server:				
Alter	nate DNS server:	•	19		
V	alidate settings upon exit			Adv	anced
			ОК		Cancel

MAC OS

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

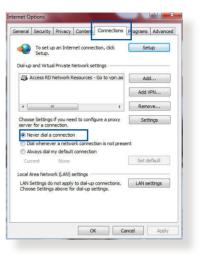
	Location: Automatic + Show: Built-in Ethernet +	
	TCP/IP PPPoE AppleTalk Proxies Etherne	<u> </u>
Configure	IPv4: Using DHCP	
IP Ad	dress: 192.168.182.103	W DHCP Lease
Subnet	Mask: 255.255.255.0 DHCP Client ID:	
R	iff rec outer: 192.168.182.250	(uired)
DNS Se	nvers: 192.168.128.10	(Optional)
Search Dor	nains:	(Optional)
IPv6 Ad	dress: fe80:0000:0000:0000:0211:24ff;fe32:b18e	
	Configure (Pvb)	(7)

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 <u>http://csr.asus.com/english/Takeback.htm</u> for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

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

IMPORTANT! This device is restricted for indoor use.

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.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

Safety Information

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

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements - Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

Operate the device in 5150-5250 MHz frequency band for indoor use only.

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.

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

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

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

WARNING!

- This radio transmitter (3568A-RTGZ00) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.
- Le présent émetteur radio (3568A-RTGZ00) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur

able for filed antenna						
Antenna Brand		Medel Name	Antenna Type	Connector	Gain (dBi)	
Antenna	branu	Model Name	Antenna Type	Connector	2.4GHz	5GHz
1	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
2	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
3	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
4	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
5	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
6	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47
7	PSA	RFDPA131000SBLB805	Dipole Antenna	Reversed-SMA	2.32	3.47

PSA

For product available in the USA/Canada market, only channel 1~11 • can be operated. Selection of other channels is not possible.

RFDPA131000SBLB805 Dipole Antenna Reversed-SMA 2.32

- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and it's antennas(s) must not be co-located or operating . in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
- Cet appareil et son antenne (s) ne doit pas être co-localisés • ou fonctionnement en association avec une autre antenne ou transmetteur.
- The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Hz

3.47

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. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose

authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

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

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

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

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

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear

that any patent must be licensed for everyone's free use or not licensed at all.

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

Terms & conditions for copying, distribution, & modification

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

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

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

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

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of

these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License. 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machinereadable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any

attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

- 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

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

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

- 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9. The Free Software Foundation may publish revised and/ or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

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

10. If you wish to incorporate parts of the Program into other free

programs whose distribution conditions are different, write to the author to ask for permission.

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

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

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.

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

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

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

ENDEKS BİLİŞİM SAN VE DIŞ 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	https://www.asus.com/support/

ASUS COMPUTER INTERNATIONAL (America)

Address	48720 Kato Rd., Fremont, CA 94538, USA
Telephone	+15107393777
Fax	+15106084555
Website	usa.asus.com
Online support	https://www.asus.com/support/

ASUS COMPUTER GmbH (Germany and Austria)

ny

Technical Support

+49-2102-5789555
+49-2102-5789557
+43-820-240513
+49-2102-959911
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	ASUS Computer GmbH		
representative	Address:	HARKORT STR. 21-23, 40880	
in Europe:		RATINGEN, GERMANY	