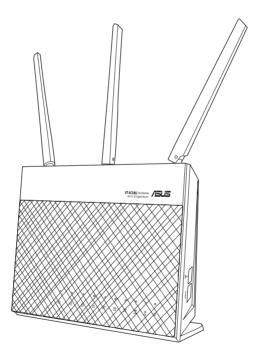
User Guide

RT-AC68U Dual Band

3x3 Wireless-AC 1900 Gigabit Router





E9493 Revised Edition v3 June 2014

Copyright © 2014 ASUSTeK Computer Inc. All Rights Reserved.

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

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

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

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

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

Table of contents

1	Getting to know your wireless router	6
1.1	Welcome!	6
1.2	Package contents	6
1.3	Your wireless router	7
1.4	Positioning your router	9
1.5	Setup Requirements	10
1.6	Router Setup	11
	1.6.1 Wired connection	11
	1.6.2 Wireless connection	12
2	Getting started	14
2.1	Logging into the Web GUI	14
2.2	Quick Internet Setup (QIS) with Auto-detection	15
2.3	Connecting to your wireless network	19
3	Configuring the General settings	20
3.1	Using the Network Map	
	3.1.1 Setting up the wireless security settings	21
	3.1.2 Managing your network clients	22
	3.1.3 Monitoring your USB device	23
3.2	Creating a Guest Network	
3.3	Using the Traffic Manager	
	3.3.1 Managing QoS (Quality of Service) Bandwid	th28
	3.3.2 Monitoring Traffic	31
3.4	Setting up Parental Control	
3.5	Using the USB Application	
	3.5.1 Using AiDisk	
	3.5.2 Using Servers Center	35
	3.5.3 3G/4G	41

Table of contents

3.6	Using	AiCloud	43
	3.6.1	Cloud Disk	44
	3.6.2	Smart Access	46
	3.6.3	Smart Sync	47
4	Config	guring the Advanced Settings	48
4.1	Wirele	2SS	48
	4.1.1	General	48
	4.1.2	WPS	51
	4.1.3	Bridge	53
	4.1.4	Wireless MAC Filter	55
		RADIUS Setting	
		Professional	
4.2	LAN		59
	4.2.1	LAN IP	59
	4.2.2	DHCP Server	60
	4.2.3	Route	62
		IPTV	
4.3	WAN .		64
	4.3.1	Internet Connection	64
	4.3.2	Port Trigger	
	4.3.3	Virtual Server/Port Forwarding	69
	4.3.4	DMZ	72
		DDNS	
		NAT Passthrough	
4.4	IPv6		75
4.5	VPN S	erver	76
4.6	Firewa	all	77
	4.6.1	General	77
	4.6.2	URL Filter	77
	4.6.3	Keyword filter	78

Table of contents

	4.6.4	Network Services Filter	79
4.7	Admiı	nistration	
	4.7.1	Operation Mode	81
	4.7.2	System	82
	4.7.3	Firmware Upgrade	83
	4.7.4	Restore/Save/Upload Setting	83
4.8	Syster	n Log	
5	Utiliti	es	85
5.1	Devic	e Discovery	
5.2	Firmw	vare Restoration	
5.3	Settin	g up your printer server	
	5.3.1	ASUS EZ Printer Sharing	
	5.3.2	Using LPR to Share Printer	91
5.4	Down	load Master	
	5.4.1	Configuring Bit Torrent download settin	gs97
	5.4.2	NZB settings	98
6	Troub	leshooting	99
6.1	Basic	Troubleshooting	
6.2	Frequ	ently Asked Questions (FAQs)	
	oendice		112
ASUS	S Contact	t information	
Netw	vorks Glo	bal Hotline Information	

1 Getting to know your wireless router

1.1 Welcome!

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

1.2 Package contents

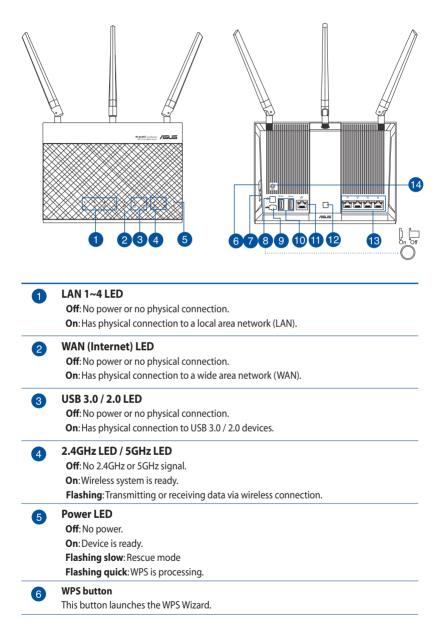
☑ RT-AC68U Wireless Router

Network cable (RJ-45)Quick Start Guide

- Power adapter
- Support CD (Manual)

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

1.3 Your wireless router



7	WI-FI On/Off button Press this button to turn on /off the Wi-Fi connection.
8	Power button Image: Comparison of the stystem. Press this button to power on or off the stystem. Image: Comparison of the stystem.
9	Power (DC-IN) port Insert the bundled AC adapter into this port and connect your router to a power source.
10	USB 3.0 / 2.0 ports Insert USB 3.0 / 2.0 devices such as USB hard disks or USB flash drives into these ports. Insert your iPad's USB cable into one of these ports to charge your iPad.
1	WAN (Internet) port Connect a network cable into this port to establish WAN connection.
12	LED On/Off button Press this button to turn on/off the backlight LED on the panel.
13	LAN 1 ~ 4 ports Connect network cables into these ports to establish LAN connection.
14	Reset button This button resets or restores the system to its factory default settings.

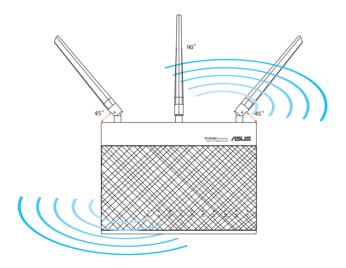
- Use only the adapter that came with your package. Using other adapters may damage the device.
- Specifications:

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

1.4 Positioning your router

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

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



1.5 Setup Requirements

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

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

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

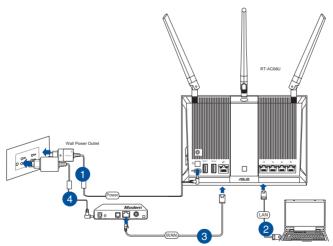
1.6 Router Setup

IMPORTANT!

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

1.6.1 Wired connection

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



To set up your wireless router via wired connection:

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

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

IMPORTANT! Ensure that the LAN LED is blinking.

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

1.6.2 Wireless connection

To set up your wireless router via wireless connection:

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

- 3. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.
- 4. Install an IEEE 802.11a/b/g/n/ac WLAN adapter on your computer.

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

2 Getting started

2.1 Logging into the Web GUI

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

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

- 1. On your web browser, manually key in the wireless router's default IP address: **192.168.1.1** or enter <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.



Top command buttons

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

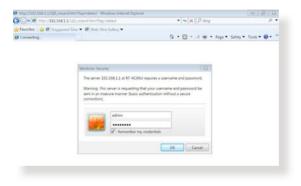
2.2 Quick Internet Setup (QIS) with Autodetection

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

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

To use QIS with auto-detection:

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



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

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

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

for Automatic IP (DHCP)

ASUS Router	And the second second	
Quick Internet Setup	Automatic IP connection setup	٦
() Check Connection	Host Name(optional): 👔	
Internet Setup	MAC Address(optional) 1	HAC Clone
Router Setup	 MAC (Media Access Control) address is a unique identifier that ide in the network. SPh monitor the MAC addresses of devices that of the blowing. Contrata your IB and request to update the MAC address that Does this is done, you can run the router's setup ward again. Once this is done, you can run the router's setup ward again. Once or change the MAC address of the new device to match the device. If you just replaced an oil router, you will find the oil mous purported to the setup and runter of the one device the model. 	conect to their services, and this issue, you can do either of ted with your ISP subscription, e MAC address of the original ter's MAC address from its label, ill need to erter your computer's

for PPPoE, PPTP, and L2TP

/ISUS Router		A DESCRIPTION OF	
Quick Internet Setup	count Setting		٢
Check Connection	Please enter the requ	uired information below.	
Internet Setup	User Name		
Router Setup	Password		
		Show pasaword	
_	Obtain the account na	anse and password from your ISP.	
_		Previous Next	

for Static IP

Please refer to your ISP setting.	and	I input the related infon	mation.	0
on Use the following IP address:				
IP Address				
Subnet Mask				
Default Gateway				
-DNS Servers				
DNS Server1				
DNS Server2	*			
MAC Address(optional)			MAC Clone	
		Previous Ne	1	

- 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.

Quick Internet Setup Wireless Setting Internet Setup Assign a unique name or SSID (Service Set Identifier) to help identify your 2.240% - Security Internet Setup Network Name(SSID) 2 Rowter Setup Security Key Stift - Security Coxy 2.40% - setings.	\odot
Assign a unique name or SSID (Service Set Identifier) to help identify your Z4GHz - Security Network Name(SSID) Koster Setup Security Key z	
Router Setup Network Name(SSID) 2 A005 Router Setup Security Key 2	ireless network.
accumy ney	
5GHz - Security Copy 2.4GHz to 5GHz settings.	
Network Name(\$SID) 3 ASUS_56	
Security Key 2	
Apply	

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

Quick Internet Setup	Sustem Time: Sat. Jan 01 (00:02:51 2011 Change the Line zong
Check Connection	Wireless (24GHz)	
	Network Name(SSID)	ASUS-monikey
Internet Setup	Wireless Security	Open System
Router Setup	Network Name(SSID)	ASUS_5C-monkey
	Wireless Security	Open System
	WAN Connection Type	Automatic IP
	WAN IP	192 168 123 23
	LANIP	192.16E.1.1
	MAC	20 CF 30 B6 C0 C0
		Next

2.3 Connecting to your wireless network

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

To connect to your network:

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

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

3 Configuring the General settings

3.1 Using the Network Map

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



3.1.1 Setting up the wireless security settings

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

To set up the wireless security settings:

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

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

2.4GHz security settings



5GHz security settings



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

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

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

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

3.1.2 Managing your network clients



To manage your network clients:

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

3.1.3 Monitoring your USB device

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



- 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 2TB size) and supports read-write access for FAT16, FAT32, EXT2, EXT3, and NTFS.

Safely removing the USB disk

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

To safely remove the USB disk:

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



3.2 Creating a Guest Network

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

NOTE: RT-AC68U supports up to six SSIDs (three 2.4GHz and three 5GHz SSIDs).

To create a guest network:

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

The Quest Network provides Internet connection for guests but restricts access to your Intranet.	
Network Key Enable Enable Enable	
Linable Linable Linable Linable	
Network Koy	
Time Remaining Enable Enable Enable	1

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

Guess Network			
Ta pa		et connectivity for temposity visitors w	ittout accessing your
	ASUS_Quest1		
		Create	Create
	Lindess		
	Modify		
	ASUS_50_Over1		
	Open System		
		Create	Create
	Linitese		
	Medify		

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

3.3 Using the Traffic Manager

3.3.1 Managing QoS (Quality of Service) Bandwidth

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

Setup							
1997/0985	QoS Traffic I	Monitor					
Ceneral	Traffic Mar	nager - QoS	3			Automatic ec	4
Ne two rk: Map	Traine mar						
Guest Network	5111		r Quality of Service (QoS) s online gaming and web P applications (peer-lo-pe ction, Cilck the QoS slide	surfing as the highest p er applications such as	snonty and are n Difforrentj. To e	of influenced by nable GoS	
Traffic Manager		/ nel	als. Get the bandwith info	mation from your ISP.			
Parental control		pre	formed priority from the Usi <u>S.F.A.Q</u>				
USB application		9.7	_	Prop.	_		_
	0.5						
AiCloud	0.5			OFF	1		
	0.5			5460	ļ		
AiCloud dvanced Settings Wireless		rolly Rule List		5460	l		
lvanced Settings	User Spi	esity Rule List rice Name	Source IP or MAC	5460	Protocol	Transferred	Priority
Ivanced Settings	User Spe Serv			Save	Protocol	Transferred 0~512	Priority
ivanced Settings Wireless	Utier Spe Serv	vice Name		Suve Destination Port		AND STREET	
lvanced Settings Wireless LAN	Uter Spe Ser	vice Name Ib Surf		Save Destination Port 80	tep	0-512	Highest

To set up bandwidth priority:

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

NOTE: Get the bandwidth information from your ISP.

3. Click Save.

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

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

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

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

NOTES:

- Low-priority packets are disregarded to ensure the transmission of high-priority packets.
- Under Download Bandwidth table, set Maximum Bandwidth Limit for multiple network applications in corresponding order. The higher priority upstream packet will cause the higher priority downstream packet.
- If there are no packets being sent from high-priority applications, the full transmission rate of the Internet connection is available for lowpriority packets.
- 6. Set the highest priority packet. To ensure a smooth online gaming experience, you can set ACK, SYN, and ICMP as the highest priority packet.

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

3.3.2 Monitoring Traffic

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

aernh	QoS Traffic Monitor				
General	Traffic Manager - T	raffic Monitor		Real-ti	me 🚽
Retwork Map	Traffic Monitor allows you to mo	nitor the incoming or outgoing	a cackets of the following:		
😹 Guest Network	Intern		Wired	Wireless	
🚧 Traffic Manager	Reception Incom			incoming packets from wireless network	
Parental control	Transmission Outgr			Outgoing packets from wireless network	-
USB application	NOTE: Packets from the interne	et are evenly transmitted to the	wired and wireless devices.		
AiCloud		Wireless (2.4GHz)	Wireless (SGHz)		
Advanced Settings	36.62 KB/s			Tue 04:52 am / 12	.24 KB/s
察 Wireless					
	25.63 KB/s				
() w an	18.31 KB/s				
IPv6					
VPN Server	9.16 KB/s				
Firew all					
& Administration	Network	Current	Alerage	Maximum Tota	
System Log	Reception	L11 res	0.01 каза	0.90 kasa 597	
	Transmission	0.00 xex	0.00 man	0.31 kale 192	
	O Help & Manu Support Manu	al <u>Utility</u>	FAQ		0

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

3.4 Setting up Parental Control

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

Quick Internet Setup	Operation Mode: Wi SSID: ASUS ASUS	<u>ireless router</u> Firmware Version: <u>SC</u>	3.0.0.4.260	8	6 4 E
General	Parental contro	bl			
Network Map			u to set the time limit for a client's	network usage.	To use
		parental control:			
🐇 Guest Network			e] column, select the client whose		
		to control. You may Address] column.	also key in the clients MAC addr	ess in the [Olient	's MAC
Traffic Manager] column, click the Edit icon.		
Parental control		OFF 3. Set up allowed time desired day/time.	limits in the [Time Management] m	ap. Drag and dro	op to
	_	4. Click [OK] to save	the settings made.		
USB application		5. Click to open tuto	vrial video.		
AiCloud	10-10				_
•	•	Clients Name	Cilents MAC Address	Time Management	Add / Delete
Advanced Settings	2				Ð
Wireless Wireless					
U CAN			Apply		

To use the parental control function:

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

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

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

3.5 Using the USB Application

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

IMPORTANT! To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <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.

Setup					
General	1	(2) (3)	١		
品 Network Map	」	\mathbf{C})		
🞊 Guest Network 🕅	/ FTP server is shar	red.: Decide how to share your folders.			
Manager Traffic Manager					
Parental control	limitless access rights limited access rights				
•	admin rights				
AiCloud	Account	Password	Read	Write	
Advanced Settings	admin				
察 Wireless	Family	Family			
💮 wan		Previous Next			
A					

 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.

Setup	
General	
Retwork Map	
Suest Network	Create your domain name via the ASUS DDNS services.
Manager	○ I will use the service and accept Terms of service
Parental control	test ssuscomm.com
USB application	Disable DDNS.
A iCloud	
Advanced Settings	Previous Next
🗇 Wineless	

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-AC68U's network.

- Hereit	Media Server	Network Place(Samba) S	hare / Cloud Disk	FTP Share	Miscellaneous setting	
General	Media Server					
🏯 Network Hap		iTunes, FTP and Network	Place (Samba) serv			
Seest Network	Enable DLNA Me	ta Canar	ON			-
Manager Traffic Hanager	Enable (Tunes Se			F		
Parental control	Media server de		/1mp/eet		Apply	Y III
K USB application	Media Server Sta	den j	lde			
Aicloud						
Advanced Settings						
💡 Wireless						
😭 LAN	1	1				
💮 wan	•	ł				
Bv6					Digital Media Player	
VPN Server	L L					
💟 Firewall	Digi	tal Media Server				
& Administration						
System Log			1		Digital Media Player	

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

• Enable DLNA Media Server: Select ON/OFF to enable/ disable the DLNA Media Server.

Enable iTunes Server?: Select ON/OFF to enable/disable the iTunes Server.

- **Media server directory**: Select your media server directory and click **Apply** to share files from the USB disk to media devices in the network.
- Media Server Status: Displays the status of the media server.

Using Network Place (Samba) Share service

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

/ISUS	Logout Reboot	English 🔻
Ouick Internet	Operation Mode: Wireless router Firmware Version: SSID: ASUS ASUS SG	8648
Setup	Media Server Network Place(Samba) Share / Cloud Disk FTP Share Miscellaneous setting	
General		
品 Network Map	USB Application - Network Place(Samba) Share / Cloud Disk	
•	Set the account and permission of network place(samba) service.	
Guest Network	Disable Share Share with account Refresh page	
💒 Traffic Manager	000	RER
Parental control	edmin Router R/W R	No
usb application	C Cogston DT 101 G2	
AiCloud	Aaaday.	
AK JUBU		

To use Samba share:

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

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

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

To create a new account:

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

a	Add new account lace(Samba) Share / Clour,*)
L	New account has no read/write access rights.
L	Account:
L	Password:
Į.	Retype password:
ł	Add
ł,	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.

Add new folder in: sda _{e of} Samba) Share / Cloud D <mark>X</mark> I
The default access rights for a new folder is read/write.
Folder Name:
Add

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

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.

/BUS	Logout	Reboot			-		E	nglish	•
Ouick Internet	Operation Mode: 🖬	reless router Firmware Version:	SSID: ASUS	ASUS_SG			8		€ 🗉
Ścłup	Media Server Net	work Place(Samba) Share / Cloud Disk	FTP Share	Miscelland	ous se	tting			
General									
Retwork Map	USB Application	- FTP Share							9
	Set the account and p	permission of FTP service.							
💑 Gaest Network	Enable FTP	Share with account Refr	esh page						
Yraffic Manager	(20					E.	. 19.	B
Parental control	admin	Router		R/W	w	R	No		
USB application		Kingston DT 101 G2							
A			. 44	μiγ.					
AiCloud									
Advanced Settings									

To use FTP Share service:

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

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

Miscellaneous setting

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

To configure Miscellaneous settings:

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

guick Inter	Operation M	ode: Wireless router	Firmware Vension:	SSID: ASUS	ASUS_SG	8 6 4 8
Setup	Media Serve	Network Place(Samb	a) Share / Cloud Disk	FTP Share	Miscellaneous setting	
General		-				
🔒 Network M	P	ication - Miscellaneo				V
Suest Netw		settings for the USB Disk				
Guest Netw	Maximum L	ogin User				
Man Traffic Man	iger Device Nar	•				
Parental co	work Group		MORKGROUP			
		et on FTP Server		•		
use applic	tion		Αρι			
AlCloud						
		_	_	_		

2. Configure the following settings:

Maximum Login User

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

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

Device Name

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

Work Group

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

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

Character set on FTP Server

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

3.5.3 3G/4G

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

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

Quick Internet Setup	Operation Mode: Wireless ro SSID: Asus Asus so	uter Firmware Version: 3,0.0.4.260	8 🗟 🔶 🛛
General	USB Modem		5
Network Map	The current 3G/4G setting is set to turn to 3G/4G mode.		
🐣 Guest Network	Basic Costly		_
Z Traffic Manager	Enable USB Modern	O Yes O No	
	Location	Pranua 1	
Parental control	USB Noders	WEDMAL (UMTS)	
US8 application	APN sentce(optional)		
Aicloud	Dial Number		
	PtH code		
Advanced Settings	Usemane		
Y Wireless	Password		
🚮 LAN	USB Adapter	auto 🗸	
🗊 wan		Apply	
	-		

To set up 3G/4G internet access:

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

NOTE: PIN code may vary from different providers.

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

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

3.6 Using AiCloud

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



To use AiCloud:

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

3.6.1 Cloud Disk

To create a cloud disk:

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



3. Go to <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**.

C (b pert / www.assortwok.net	AiCloud
	Welcome. Wha's coming home?
	You Name. You Password.
	●

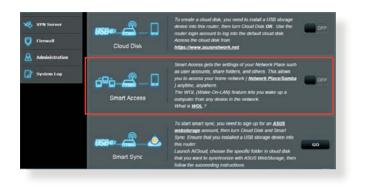
4. You can now start accessing Cloud Disk files on devices connected to the network.

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.

ACC Western Router Root X V 💽 ArClevel C 🕼 کوهلزا که ArClevel کوهلزا	× [m]
ക്ഷ്Cloud	Welcome home, admin
	пт-Асеби
•15+ RT-AC66U	
	KINGSTON

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 Smart Sync

/545	Logos	4	Reboot		English
V Quick Internet Setup	Operation Mode		er Firmware Version:	SSID: ASUS ASUS SG	8641
General					
🏪 Network Map	AiCloud - Sm	art Sync			
🥵 Guest Network		£&		you need to sign up for an &	
	U5841-6	<u> </u>	nt, then turn Cloud I B storage device int	Disk and Smart Sync. Ensure o this router	that you installed a US
🔀 Traffic Hanager	ALCONG STORE			oose the specific folder in clo	od disk that you want to
Traffic Hanager Parental control	0		Launch A/Cloud, chi		
			Launch AlCloud, chi synchronize with AS	oose the specific folder in clo	
Parental control			Launch AlCloud, chi synchronize with AS	oose the specific folder in clo	
Parental control	0		Launch AlCloud, chi synchronize with AS	oose the specific folder in clo	
Parental control	Court List		Launch AlCloud, ch synchronize with AS ons. Rule	oose the specific folder in do US WebStorage, then follow	the succeeding instructi
Parental control Parental control Alcloud	Court List		Launch AlCloud, ch synchronize with AS ons. Rule	oose the specific folder in clo US WebStorage, then follow Folder	the succeeding instructi

To use Smart Sync:

- 1. Launch AiCloud, click **Smart Sync** > **Go**.
- 2. Select **ON** to enable Smart 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.

V Quick Internet	Operation Mode: <u>Wireless</u> rout	er Firmware Version: SSID: ASUS ASUS_SG	8 @ 4 8
setup	General WPS Bridge Wire	less MAC Filter RADIUS Setting Professional	
General			
品 Network Hap	Wireless - General		
Suest Network	Set up the wireless related informatio	n below.	
Guest Network	Frequency	2.4GHZ -	
🔆 Traffic Manager	SSID		
Parental control	Hide SSID	• Yes O No	
USB application	Wireless Node	Auto 💽 🖾 big Printection	
nan abhurannan	Channel bandwidth	20/40 MHz -	
AiCloud	Control Channel	Auto 💌	
Advanced Settings	Authentication Method	Open System	
😽 Wireless	WEP Encryption	None:	
🖨 LAN		Apply	

To configure the basic wireless settings:

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

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

- 4. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
- 5. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
 - Auto: Select Auto to allow 802.11AC, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
 - **Legacy**: Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
 - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
- 6. Select the operating channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
- 7. Select any of these channel bandwidth to accommodate higher transmission speeds:

40MHz: Select this bandwidth to maximize the wireless throughput.

20MHz (default): Select this bandwidth if you encounter some issues with your wireless connection.

- 8. Select any of these authentication methods:
 - Open System: This option provides no security.
 - **Shared Key**: You must use WEP encryption and enter at least one shared key.

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

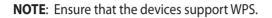
NOTE: Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto** and **encryption method** is **WEP** or **TKIP**.

- 9. Select any of these WEP (Wired Equivalent Privacy) Encryption options for the data transmitted over your wireless network:
 - **Off**: Disables WEP encryption
 - 64-bit: Enables weak WEP encryption
 - **128-bit**: Enables improved WEP encryption.

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

4.1.2 WPS

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



Ouick Internet	Operation Mode: <u>Wireless rout</u>	er Firmware Version: SSID: ASUS_ASUS_SG 🔠 🕂 🕂
 Setup 	General WPS Bridge Wirele	ass MAC Filter RADIUS Setting Professional
General	Wireless - WPS	
A Network Map		
🞊 Guest Network	the PIN code or the WPS button.	a easy and secure establishment of a wireless network. You can configure WPS here via
Manager	Enable WPS	ON
Parental control	Current Frequency	2.4Gitz
Parental control	Connection Status	kde
USB application	Configured	Ves. Reset
AiCloud	AP FIN Code	72013102
Advanced Settings Wireless LAN	Method1: Click the WPS button WPS button on the client's WL Method2: Start the client WPS field and click Start. Please ch your wraless client does not as	to the network in either of these two ways. n on this interface (or press the physical WPS button on the routed), then press the AN adapter for about these mentes: process and of the cleant PN code. Enter the cleant's PN code on the Cleant PN code exh the user manual of your eventses cleant to see if a supports the WPS function. If upport the WPS function, you have to configure the wireless cleant manually and set the d socurity settings as this router.
1Pv6	WPS Method	Push Button O Citerif 194 Code
VPN Server		

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.

Quick Internet	Operation Mode: Mireless	router Firmware	Version: SSID:	ASUS ASUS_5G	8 6 4 8
Swirdh	General WPS Bridge	Wireless MAC Filter	RADIUS Setting	Professional	
General					
🔒 Network Map	Wireless - Bridge				
🞎 Gaest Network	Bridge (or named WDS - Wirel WDS may also be considered able to use half of the access	a repeater mode. But v	with this method, the		
💒 Traffic Manager	To enable WDS to extend the 1. The function only suppo			Pl security authentication	mathod
Parental control	 Select [WDS Only] or [Ensure that this weeks 	Hybrid] mode and add f	WAC address of APs	in Remote AP List	
🔹 USB application	 Key in the remote AP in router's MAC address: 	nac in the remote AP li	st and open the remo	te AP's WDS managemen	t interface, key in the this
a AiCloud	(2.4GHz MAC) 10.8F.48.0 (5GHz MAC) 10.8F.48.08 5. You are currently using	49.70	Here to modify.		
Advanced Settings	Basic Config				
🐨 Windess	Frequency		HZ 💌		
	AP Mode		nly 💌		
	Connect to APs in list	• Yes	No No		
() WAN	Remote AP List	_	_	_	
1Pv6		Remole A	P List		Add/Delete
VPN Server					۲
V Firewall			Apply	i i i i i i i i i i i i i i i i i i i	
Administration					

To set up the wireless bridge:

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

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

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

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

NOTE: Channel availability varies per country or region.

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

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

7. Click Apply.

4.1.4 Wireless MAC Filter

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

Quick Internet	Operation Mode: wireless ro	wter Firmware Version: SSID	2: ASUS ASUS_SG	8 10 4 10
	General WPS Bridge Wi	reless MAC Filter RADIUS Setting	g Professional	
General				
Network Map	Wireless - Wireless MAC Fi	iter		
	Wireless MAC liter allows you to o	control packets from devices with spec	cilied MAC address in your W	freless LAN.
Guest Network	Basic Config			
🛃 Traffic Manager	Frequency	2.4GHZ 💌		
Parental control	MAC Filter Mode	Disabled 💌		
	MAC filter list		_	
USB application		MAC filter ltat		Add/Delete
AiCloud				۲
Advanced Settings				
Windess		Apply		

To set up the Wireless MAC filter:

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

4.1.5 RADIUS Setting

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

Quick Internet	Operation Mode: <u>Wireless</u> router	Firmware Version: SSID: ASUS ASUS 55 🛛 🗿 😌 🔶 🖴					
Serup	General WPS Bridge Wireles	s MAC Filter RADIUS Setting Professional					
General							
Hetwork Hap	Wireless - RADIUS Setting						
Guest Network		nal parameters for authorizing wireless clients through RADRUS server. It is required while Wireless - Generall" as "WPA-Enterprise/ WPA2-Enterprise/ Radius with 802.1x".					
Manager	Frequency	2. 46HZ -					
Parental control	Server IP Address						
	Server Port.	1812					
USB application	Connection Secret						
AiCloud		Apply					
Advanced Settings	1						
💎 Wireless							

To set up wireless RADIUS settings:

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

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

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

4.1.6 Professional

The Professional screen provides advanced configuration options.

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

Quick Internet Setup		Operation Mode: <u>Vircless router</u> Firmware Version: SSID: ASUS ASUS_SG						
	General WPS Bridge Wireles	s MAC Filter RADIUS Setting Professional						
General	Wireless Professional							
Network Map		Wireless - Professional						
Guest Network	Wireless Professional Setting allows yo	Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.						
	Frequency	2.4GIZ						
Traffic Manager	Enable Radio	© Yes ● No						
Parental control	Date to Emable Radio (week days)	121 Mon 121 Tue 121 Wed 121 Thu 121 Fill						
USB application	Time of Day to Enable Radio							
Constant of the second states	Date to Enable Radio (weekend)	12 Sat 12 Sun						
AiCloud	Time of Day to Enable Radio							
Advanced Settings	Set AP Isolated	• Yes O No						
Wireless	Mulbcast Rate(Mbps)	pisable -						
E LAN	Preamble Type	Long -						
	RTS Threshold							
WAN	DTIM Interval							
IPv6	Beacon Interval							
VPN Server	Enable TX Bursting	Enable 👤						
	Wintess Multicast Forwarding	Disable <mark>-</mark>						
Firewall	Enable WMM APSD	Enable -						
Administration								
System Log	Tx power adjustment	Set the capatality for transmission power. The maximum value is 200mW and the real transmission power will be dynamically adjusted to meet regional regulations.						
Meeting .		Apply						

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

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

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

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

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

4.2 LAN

4.2.1 LAN IP

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

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

/islus	Logout	Reboot		English 🔻
guick Internet	Operation Mode: Wireles	ss router Firmware Version:	SSID: ASUS ASUS SG	8 5 4 8
Setup	LAN IP DHCP Server	Route IPTV Switch Control		
General				
Hetwork Map	LAN - LAN IP			
-	Configure the LAN setting of	Router.		
Goest Network	IP Address			
Manager Traffic Manager	Subnet Mask			
🔒 Parental control		Aps	sty	

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.

Quick Internet		Operation Mode: Winnless	router F	entware Version:	SSID: ASUS ASUS_SG	8 9 4 8			
	Secur	LAN IP DHCP Server Ro	ste IPTV	Switch Control					
ſ.	General	LAN - DHCP Server							
*	Network Hap								
*	Guest Network	DFCP (byname: hist Configuration Protocol) is a protocol for the automatic configuration used on P rotworks. The DFCP server can assign each client an P address and informs the client of the of DFS server P and default gateway P. Harwarilly, Assigned, JP, arcound: the DFCP. List (Clist. Link).222_FA0							
丝	Traffic Manager	Resic Config							
	Parental control	Enable the DHOP Server		O Yes No					
-		Router's Domain Name							
•	USB application	IP Pool Starting Address							
4	Aicload	IP Pool Ending Address							
-	dvanced Settings	Lease Time							
-	Wireless	Default Galeway							
		DRS and WRS Server Setting		_					
ស	LAN	DHS Server							
0	WAN	WINS Server							
	IPv6	Enable Manual Assignment							
		Enable Manual Assignment		Tes D No					
	VPN Server	Manually Assigned IP around the DIKCP Bal(bot Hmit.32)							
D	Firewall	MAC 20311			IP Address	Add/Delete			
8	Administration					Ð			
	System Log	No data to table.							
La		Apply							

To configure the DHCP server:

- 1. From the navigation panel, go to **Advanced Settings** > **LAN** > **DHCP Server** tab.
- 2. In the Enable the DHCP Server field, tick Yes.

- 3. In the **Domain Name** text box, enter a domain name for the wireless router.
- 4. In the **IP Pool Starting Address** field, key in the starting IP address.
- 5. In the **IP Pool Ending Address** field, key in the ending IP address.
- 6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

NOTES:

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

4.2.3 Route

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

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

wick Internet	Operation Mode: Wireless re	auter Fin	nware Version:	SSID: ASUS ASUS	G	8	© ♣ @
Setup	LAN IP DHCP Server Rout	e IPTV	Switch Control				
General	1.0000000000						
Hetwork Map	LAN - Route						
Suest Network	This function allows you to add ro same connection to the Internet.	iting rules in	to Router. It is usef	ul if you connect severa	l routers be	hind Router to	share the
A	Basic Config						
Traffic Manager	Enable static routes		• Yes O No				
Parental control	Static Route List						
dist use application	Network/Host IP		Netmask	Cateway	Metric	Interface	Add / Delete
AiCloud						LAN 🝷	⊕
AiCloud				n table.			
Advanced Settings			Арр	ły			
💎 Wireless							

To configure the LAN Routing table:

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

4.2.4 IPTV

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

Quick Internet	Operation Mode: Wireless router	Firmware Version: SSID: ASUS_ASUS_ASUS_ASUS_ASUS_ASUS_ASUS_ASUS	E.
	LAN IP DHCP Server Route IPT	V Switch Control	
General			
	LAN - IPTV		
	Configure the IPTV setting of Router.		
Geest Network	Port		
💒 Traffic Hanager	Select ISP Profile	None	
Parental control	Choose IPTV STB Port	None	
	Special Applications		
USB application	Use DHCP routes	Microsoft 🗾	
AiCloud	Enable multicast routing	Disable 💽	
Advanced Settings	Enable efficient multicast forwarding	Disable 💌	
S Windess	UDP Prox(Udpxy)		
A Mussics		Apply	

4.3 WAN

4.3.1 Internet Connection

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

Cuick Internet	Operation Mode: Wireless router	Firmware Version: SSID: ASUS ASUS_SG 🔗 🗇 🐟 🖻
	Internet Connection Port Trigger	Virtual Server / Port Forwarding DMZ DDNS NAT Passtbrough
General	WAN - Internet Connection	
Guest Network		s to WAN (wide area network). These types are selected from the dropdown menu beside s differ depending on the connection type you selected.
AN	Basic Config	
Traffic Manager	WAN Connection Type	Automatic IP -
Parental control	Enable WAN	O Yes SNO
dist use application	Enable NAT	© Yes ● No
AiCloud	Enable UPnP UPnP FAQ	O Yes No
	WAN DNS Setting	
Advanced Settings	Connect to DNS Server automatically	© Yes ● No
🚏 Wireless	Account Setting	
🚮 LAN	Authentication	None
WAN	Password	
	Special Requirement from ISP	
5 IPv6	Host Name	
VPN Server	MAC Address	MAC Clone
V Firewall		Аррђу

To configure the WAN connection settings:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.
- 2. Configure the following settings below. When done, click **Apply**.
 - WAN Connection Type: Choose your Internet Service Provider type. The choices are Automatic IP, PPPoE, PPTP, L2TP or fixed IP. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
 - **Enable WAN**: Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.

- Enable NAT: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- Enable UPnP: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- Connect to DNS Server: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- Host Name: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.

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

4.3.2 Port Trigger

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

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

Quick Internet	Operation Mode: WireTe	ss router	Firmware Version	SSID: ASI	IS ASUS_SG		8 6 4 1
	Internet Connection Pe	ort Trigger V	firtual Server / Po	rt Forwarding	DMZ DONS	NAT Pass	through
General							
📇 Network Hap	WAN - Port Trigger						-
🞎 Guest Network	Port Trigger allows you to te two methods for opening inc the time and devices must u	coming data port	ts: port forwarding a	and port trigger.	Port forwarding o	pens the spec	ifed data ports all
Manager Traffic Manager	access to the trigger port. U forwarding allows multiple de	inlike port forwar	rding, port trigger d	oes not require	static IP address	es for LAN des	ices. Port
Parental control	port. Port_Trigger_FAQ						
USB application	Besic Config						
	Enable Port Tripper		• Yes © No				
a AiCloud	Well-Known Applications			ict 💽			
Advanced Settings	Trigger Port List			_			
S Wireless	Description	Trigger	Port Prot	acal inc	coming Port	Protocol	Add/Delete
				•		TCP •	Ð
			No.elett	in table.			10000
🛈 WAN				pply			-
1Pv6							

To set up Port Trigger:

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

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

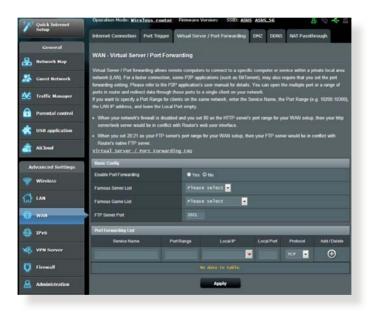
NOTES:

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

4.3.3 Virtual Server/Port Forwarding

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

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



To set up Port Forwarding:

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

- 2. Configure the following settings below. When done, click **Apply**.
 - **Enable Port Forwarding**: Choose **Yes** to enable Port Forwarding.
 - Famous Server List: Determine which type of service you want to access.
 - **Famous Game List**: This item lists ports required for popular online games to work correctly.
 - **FTP Server Port**: Avoid assigning the port range 20:21 for your FTP server as this would conflict with the router's native FTP server assignment.
 - Service Name: Enter a service name.
 - **Port Range**: If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty. Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,3021).

NOTES:

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with the router's web user interface.
- A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.

• Local IP: Key in the client's LAN IP address.

NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **4.2 LAN** for information.

- Local Port: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
- Protocol: Select the protocol. If you are unsure, select BOTH.

To check if Port Forwarding has been configured successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

4.3.4 DMZ

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

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

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

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

To set up DMZ:

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

To remove DMZ:

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

4.3.5 DDNS

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

/SUS	Logout	R	aboot		Engli	sh 🔻
Quick Internet Setup	Operation Mode: Mire	eless router	Firmware Version: SSID: ASU	S ASUS_SG	a a	* 🗈
	Internet Connection	Port Trigger	Virtual Server / Port Forwarding	DHZ DO	NS NAT Passtbrough	
General				-		
🔒 Network Map	WAN - DDNS					
Guest Network		ss, through its n) is a service that allows network clien ogistered domain name. The wireless			
🙋 Traffic Manager			ate WAN IP address (192.168 x x, 10, microment and DDNS service cannot			
Parental control	Enable the DONS Client		• Yes O No			
USB application			Apply			

To set up DDNS:

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

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

NOTES:

DDNS service will not work under these conditions:

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

4.3.6 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	Reboot English *
Quick Internet	Operation Mode: Wireless r	outer Firmware Version: SSID: ASUS ASUS_SG 8: 🔁 🔶 🖴
Setup	Internet Connection Port Tri	gger Virtual Server / Port Forwarding DM2 DDNS NAT Passtbrough
General		
Network Map	WAN - NAT Passthrough	
	Enable NAT Passthrough to allow	a Virtual Private Network (VPN) connection to pass through the router to the network clients.
Guest Network	PPTP Passtbrough	Crable 🐱
Yraffic Manager	L2TP Passthrough	Enable
Parental control	IPSec Passthrough	Enuble
USB application	RTSP Passthrough	Enable -
USB application	Enable PPPoE Relay	Disable 💌
AiCloud		
		Αρρίγ
Advanced Settings		

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.

Logout	Reboot		English 🔻
Operation Mode: <u>Wireless</u> route	r Firmware Version: S	ISTO: <u>Asus asus sg</u>	8 6 4 8
No. of Concession, Name			
IPv6			
Configure the EV6 Internet setting of Ro <u>TPv6_FAQ</u>	suter		
Basic Config			
Connection type		•	
Auto Configuration Setting			
Enable Router Advertisement	Enable -		
	Apply		
	Operation Mode: <u>VireTess route</u> Brv6 IPv6 Configue the BV6 Internet setting of R <u>ZPv6_EN0</u> Basic Coeffig Correction hppe Auto Coeffiguration Setting	Operation Mode: Wireless couter Permutate Version: IPv6 IPv6 Configura the IPv6 Internet setting of Router. Table. Could Table. Could Auto Configuration Setting Couble Router Advertisement	Operation Mode: Vircless_router Fermivale Version: SSID: ASUS_ASUS_ASUS_ASUS_ASUS_ASUS_ASUS_ASUS

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.

/545	Logout	Reboot		English 🔻
V Quick Internet	Operation Mode: <u>Wireless</u> route	E Firmware Version:	SSID: ASUS ASUS_SG	8648
General	VPN Server - Basic Config The VPN server allows you to access	vaur horne network amfin	so amultere	
Suest Network	To use the VPN server. Please follows (1) Enable the PPTP VPN server			
We Traffic Manager	(2) Set the IP pool for client IP. (Maxim (3) Set up the username and password	for VPN client.		
Parental control	(4) Open the VPN connection program (5) Add a new PFITP VPN connection	and the VFN server addre		
dist use application	(6) If your WAN IP address is dynam (7) <u>YPN_SECVEC_EAQ</u>	nic,please_click_h	ere to set the DONS.	
AiCloud	Elesic Config	_		
	Enable PPTP Server	• Yes O No		
Advanced Settings	Network Place (Samba) Support	• Yes O No		
🛜 Wireless	Username and Password			
🕼 LAN	User Name		Password	Add/Delete
🖨 wan				Ð
U 100				
IPv6		A	Ply	
VPN Server				

To set up access to a VPN server:

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

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

4.6 Firewall

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

NOTE: The Firewall feature is enabled by default.

4.6.1 General

To set up basic Firewall settings:

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

4.6.2 URL Filter

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

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

To set up a URL filter:

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

4.6.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

/ISUS	Logout	Reboot	English 🔻
Quick Internet	Operation Mode: Mireless row	ter Firmware Version: SSID: ASUS ASUS SG	8 @ < 8
	General URL Filter Keyword	Filter Network Services Filter	
General	Coursell, Managered Cities		
Retwork Map	Firewall - Keyword Filter		
😹 Gaest Network	Keyword Filter allows you to block the Limitations of the keyword filtering fu	he clients' access to webpages containing the specified keywo inction :	rds.
Manager Traffic Hanager	1. Compressed webpages that s 2. Https webpages cannot be fill	use HTTP compression technology cannot be filtered. <u>See her</u> tered.	e for more details.
Parental control	Basic Config		
use application	Enable Keyword Filter	Enabled Disabled	
A	Keyword Filter List.		
AiCloud		Keyword Filter List	Add / Delete
Advanced Settings			Ð
察 Wireless			
🚮 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.



To set up a Network Service filter:

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

4.7 Administration

4.7.1 Operation Mode

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



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

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

4.7.2 System

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

To set up the System settings:

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

4.7.3 Firmware Upgrade

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

To upgrade the firmware:

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

NOTES:

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

4.7.4 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

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

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

/SUS	Logout	Reboot	English
Quick Internet	Operation Mode: Wireless. row	ter Firmware Version: SSID: ASUS ASUS 55	8 6 4 1
General	General Log DHCP leases W	Areless Log Port Forwarding Routing Table	
	System Log - General Log		
Network Map	This page shows the detailed system	n's activities.	
Guest Network	System Time	Sat, Jan 01 00:49:51 2011	
🖆 Traffic Manager	Uptime	0 days 0 hours 49 minutes 50 seconds	
Parental control	Jan 1 00:31.27 kernel: eth2:	Broadcom BCM4331 802 11 Wireless Controller 6.30 10 Broadcom BCM4360 807 11 Wireless Controller 6.30.10 e131 enternal promiseruous mode	
USB application	Jan 1 00:31:27 kernel: br0; p Jan 1 00:31:27 kernel: wic_ph Jan 1 00:31:27 kernel: br0; p	ort 2(eth1) entering listening state y_cal_init_acpby: NOT Implemented ort 2(eth1) entering learning state opology change detected, propagating	
AiCloud	Jan 1 00:31:27 kernel: br0: p Jan 1 00:31:27 kernel: device Jan 1 00:31:27 kernel: device	ort 2(eth1) entering forwarding state eth2 entered promiscuous mode ort 3(eth2) entering listening state	
Advanced Settings	Jan 1 00:31:27 kernel: device Jan 1 00:31:27 kernel: br0: p	ort 3(eth2) entering learning state w10.1 entered promiscuous mode ort 4(w10.1) entering listening state opology change detected, propagating	
Wireless Vireless	Jan 1 00:31:27 kernel: br0: p Jan 1 00:31:27 kernel: br0: p	opology change detected, propagating ort 3(wth2) entering forwarding state ort 4(w10.1) entering learning state opology change detected, propagating	
👌 lan	Jan 1 00:31:27 kurnel: hr0: p Jan 1 00:31:39 dnsmang-dbcp15 Jan 1 00:31:39 dnsmang-dbcp15	ort 4(V10.1) entering forwarding state 10]: DHCREAGUEST(br0) 192.168.1.60 c4:6a:b7:89:8f:1 10]: DHCRACK(br0) 192.168.1.60 c4:6a:b7:89:8f:97 ar	dro1d-b3d00032df634239
🕑 WAN	Jan 1 00:32:12 dnamaseg-dhcp(5 Jan 1 00:33:00 dnamaseg-dhcp(5	10): DHEPTHYDRH(br0) 192 168.1.197 10:bf:48:4e:b9:4 10): DHEPHEK(br0) 192 168.1.197 10:bf:48:4e:b9:40 10): DHEPHEQUERT(br0) 192 168.1.189 b0(me:71:me:67 30): DHEPHEQUERT(br0) 192 168.1.189 b0(me:71:me:67 30): DHEPHEK(br0) 193 168.1.189 b0(me:73:me:67):me	OUIE-CHAVEI
🗿 1Pv6	Jan 1 00:33:34 dnmasg-dhep15	10]: IMCERNEQUEST(br0) 192,168,1.3 le:d0:f8:be:11:7d 10]: IMCERACK(br0) 192,160,1.3 le:d0:f8:be:11:7d 1Ph	
🍕 VPN Server		Clear Save Refresh	,
Firewall		Crean Save Refresh	

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-AC68U Wireless
 Router > Device Discovery.



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

5.2 Firmware Restoration

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

<u>F</u> ilename:	I		<u>B</u> rowse
Status After locating	the firmware file, click U	Jpload.	

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-AC68U Wireless
 Router > Firmware Restoration.
- 5. Specify a firmware file, then click **Upload**.

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

5.3 Setting up your printer server

5.3.1 ASUS EZ Printer Sharing

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



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

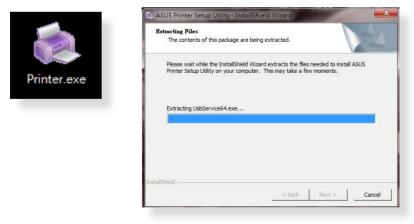
To set up the EZ Printer sharing mode:

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



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**.



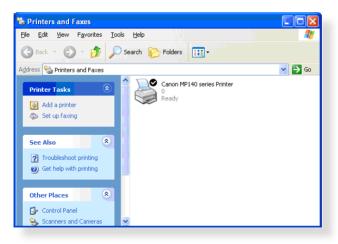
- 5. Wait a few minutes for the initial setup to finish. Click **Next**.
- 6. Click **Finish** to complete the installation.

/ISUS Printer S	Setup Utility
You have connected to the direction to install printer of	e following wireless router. Please follow Windows Iriver now.
IP Address:	192.168.1.1
Wireless Router:	RT-AC68U
Please follow the Windows OS	's directions to install printer driver.
	Einish

7. Follow the Windows[®] OS instructions to install the printer driver.



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

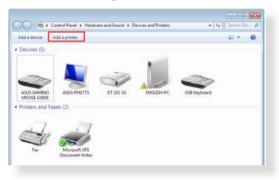


5.3.2 Using LPR to Share Printer

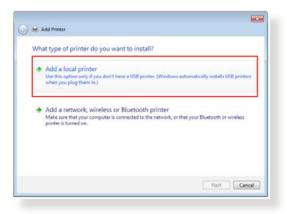
You can share your printer with computers running on Windows[®] and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

Sharing your LPR printer To share your LPR printer:

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



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



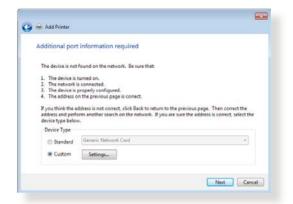
3. Select Create a new port then set Type of Port to Standard TCP/IP Port. Click New Port.

Choose a printer port		
A printer port is a type of con	nection that allows your computer to exchange	information with a printer.
🖱 Use an existing port:	[LPTI: (Printer Port)	
Create a new port:	52	
Type of port:	Standard TCP/IP Port	-

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 hostnan	ne or IP address	
Device type:	TCP/IP Device	
Hostname or IP address:	192.168.1.1	
Port name:	192.168.1.1	
Query the printer and auto	matically select the driver to use	
		Next Cancel

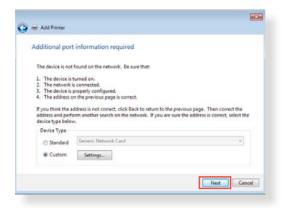
5. Select **Custom** then click **Settings**.



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

ort Settings	
Port Name:	192.168.1.1
Printer Name or IP Addres	ss: 192.168.1.1
Protocol	
Raw	LPR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	LPRServer
LPR Byte Counting E	nabled
SNMP Status Enable	d
Community Name:	public
SNMP Device Index	1

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



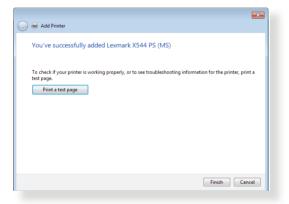
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.

Install the printer dr	iver		
Choose your pri	nter from the list. Click	Windows Update to see more mo	odels.
To install the dri	ver from an installation	CD, click Have Disk.	
Manufacturer	* Printers		-
Kyocera		erk X422 (MS)	
Lanier Lexmark		rk X543 PS (MS)	10
Microsoft		ark X642e (M5)	
kin/		L. VELL AND	-
This driver is digitally	signed.	Windows Update	Have Disk_
-	oning is important		

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**.

5. Use the navigation panel to configure the advanced settings.



5.4.1 Configuring Bit Torrent download settings

/SUS		
Task	Bit Torrent Setting	
🌆 Task	Port	
Settings	Use the default port Use the following port	
K General	Incoming port	
	Maximum download speed. Maximum upload speed.	KB/S
Kit Torrent	GillTorrant Network setting	
X 120	BitTorrent protocol encryption	Encryption disabled
	Max peers allowed performent	00
	DHT network	Enable DHT to activate trackless toment download
		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	30.4 2024.55	
Task	NZB Setting	
124	Setup USENET server to download NZB tiles:	
Settings	USENET Server	
50 2	USENET Server Port	119
General	Maximum download speed	Kas
Bit Torrent	SSL/TLS connection only	
	User name	
428	Password	
	Contrm Password	
	Number of connections per N20 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>http://support.asus.com/</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.

7 Quick Internet	ration Model Wireleas now	eter Fernivare Version: 3.0.0.4.260 SSID: ASUS ASUS B 🖯 🔶 🕮
	ation Mode System Fir	mware Upgrade Restore/Save/Upload Setting
General		11
🐣 Network Map	ninistration - Firmware (Upgrade
2 Guest Network		(Http://support.axus.com.) to get the latest firmware.
		REACHU
Manager Part		3.9.8.4.240 Check
Perrotal control	e Ferrovane File	Artest
🔹 LISB application		Upload
		e existing both in the sid and new timeware, its setting will be kept during the segrade process
Advanced Settings		falo, NT ACIIIU enters the emergency mode automatically. The LED signals at the tort at NT- alton. Use the Ferneare Restoration utility on the CD to do system recovery.
😵 Wireless		
🕼 un		
🔁 wan		
🚭 IPv6		
🤹 VPN Server		
💟 Firewall		
Atomistation		

- 2. If the latest firmware is available, visit the ASUS global website at <u>http://www.asus.com/Networks/Wireless_Routers/RTAC68U/</u> <u>#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 poweredon computer with the router is plugged in properly, the corresponding LAN LED will be on.

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

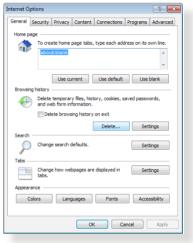
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network. Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You 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.
 - 2. In the **General** tab, under **Browsing history**, click **Delete...**, select **Temporary Internet Files** and **Cookies** then click **Delete**.



NOTES:

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

The client cannot establish a wireless connection with the router.

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

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

Seick Internet Centeral LN D Centeral Cen	/545	Logout Rebo	ot	English 🔻
Interview Interview IAN - DHCP Server Image: Interview DHSP (p)-process that an P address and nhorm the cating that of the address and other if the CATE process and other and the CATE process and proces and the CATE process and the CATE process and process an	Voick Internet Setup			8 6 4 5
BC Guest Network DFGP (Dynamic Ised Configuration Plottice)) is a protocol for the admandance configuration scaled on P anterohis. The DFGP sever many scale of the P advises and rifering is even P and sched field of DES and P and and field DES and P	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	LAN - DHCP Server		
		can assign each client an IP address and in	forms the client of the of DNS server IP and default gat	
Image: Parential control Prod/25 drains / Address Image: Voltage Address 195:185.11.21 Image: Address 195:185.11.	Manager	Basic Config		
•••••••••••••••••••••••••••••••	A Parental control	Enable the DHCP Server	O Yes ● No	
		Router's Domain Name		
Advanced Settings Lasts Time 54400 Wrieless Lasts Time 54400 Image: Settings Image: Settings Image: Settings	USB application	IP Pool Starting Address		
Advanced Setting: Twind: Wieless Defad Catway It AM Defad Catway It Sam Wath Server Setting Defad Catway It MA Defad Server It Makes Defad Server It Makes Tradic Manual Assignment It Table Manual Assignment It was an Wath Server It forwall McC appress It Forwall McC appress Advanishtration It was date in table. It system Log We date in table.	aiCloud	IP Pool Ending Address		
Wireless Drhaft Calency Wireless Ens and West Sover Safting Dr YAN Drist Sover WAN Well Sover WAN Well Sover WAN Table Manual Assignment Urbs Sover Enable Manual Assignment Dr YPN Sorver Table Manual Assignment Facewall MA2 address Adsolubitration MA2 address System Log No dats in table.	Advanced Settings	Lease Time		
Image: Springer Station		Default Gateway		
Unit Dirty Stever IP Vol. Franklik Manual Assignment! IP Vol. Franklik Manual Assignment! Vol. VPN Server Indire Manual Assignment! IP Top Firewalt MAC address IM Administration Image: Sprates Log		DNS and WINS Server Setting		
IPvo Findle Manual Assignment Trable Manual Assignment Vru © No VPM Server Manualy Assigned P annual the (MCP letited inec.2g) Firewall MC address P Address Addrifted MC address P Address Addrifted MC address No det s in table.	La un	DNS Server		
BYPD Enable Manual Assignment If Yes: © 160 VPN Server Manual Assignment If Yes: © 160 Frewall MAC address If Address Administration If System Log If address	💮 wan	WINS Server		
VPH Server Hansally Assigned P around the (HCP indice investor) Frewall MC2 address Administration Image: Comparison of the ChCP indice investor System Log No data in tables.	🔒 19v6	Enable Manual Ansignment		
Taxwall MAX2 a59 msd BP A59 ms3 Addribits Administration Image: System Log Image: System Log Image: System Log		Enable Manual Assignment	● Yes O No	
Administration Septemblag	VPN Server	Manually Assigned IP around the DHCP list()	ist limit:37)	
Administration No deta in table.	V Firewall	MAC address	EP Address	Add/Delete
📝 System Log	Administration		•	Ð
	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.

//545	Logost Reb	iot	Erglish *
Quick Internet	Operation Mode: Wireless router	Firmware Version: SSID: ASUS ASUS_36	8 % * 5
Settap	General WPS Bridge Windess H	WC Filter RUDIUS Setting Professional	
General	Wireless - General		
🚠 Network Map	Set up the westess related information belo	-	
Caest Network	frequency	2.400 .	
💒 Traffic Hanager	5560		
Parental control	Hide SSD		
de USB application	Wireless Mode	Auto • 🖬 by Probins	
Alched	Channel bandwidth	20/49 ##2	
AL NO	Control Channel	Auto 💽	
Advanced Settings	Authentication Method	Open System	
Wireless	WEP Encryption	kone	
🚮 LAN		Apply	
🖨 wan			
1Pv6			
VPN Server			
Firewall			

- 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	Rebool		English
Quick Internet	Operation Mode: Wireless rout	er: Firmware Version:	SSID: ASHS ASHS_SG	864
Setup	Operation Mode System Firm	ware Upgrade Restore	/Save/Upload Setting	
General	and the second second	dist state		
品 Network Map	Administration - Restore/Sav	e/Upload Setting		
Guest Network	This function allows you to save curre	nt settings of Router to a M	e, or load settings from a file.	
Gaest Network	Factory default	Restore		
🜿 Traffic Manager	Save setting	Save		
Parental control				
ter a second	Restore setting	Upload	Choose File Tild Tile Chosen	
USB application				
AiCloud				

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.

/505	Logost	Rebo	Firmware Version:	(010) APRIL 100		nglish Canada an	ľ
Quick Internet Setup	operation Model 1	Trefess Fouter	Ferning of Version.	5510: K305 K30	<u>.</u>	0 -0 1	1
General	Parental control						
Retwork Map		Parental cont parental cont	rol allows you to set the rol	time limit for a client's	s network usage.	To use	
👫 Guest Network	2.5		Clients Name/ column, rol. You may also key ir				
Manager Traffic Manager	1 M	Addres	nic. roli may also key i is) column. (Add / Delete) column, c		eas in the funers	3.6610	
Parental control		ITT 3. Set up	allowed time limits in th I day/time.		map. Drag and d	hap to	
🔹 USB application		4. Click /	OK] to save the setting: to open the tutorial vid				
AiCloud	1000				Time	Add/	
Advanced Settings		Clients Name		Dients MAC Address	Management	Delete	
💎 Wireless	-		No data in ta	din .		Ð	
🚮 LAN	1		Apply				
📵 wan							
🚯 1Pv6							
VPN Server							
👽 Firewall							
Administration							
🕜 System Log							

- 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:	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

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



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

utomatic con		nay override man sable automatic		gs. To ensure the ion.
Automatica	ally detect s	ettings		
Use autom	atic configu	ration script		
Address				
	y server for /PN connect	r your LAN (Thes tions).	e settings	will not apply to
Address:		Port:	80	Advanced
Bypass	proxy serv	er for local addre	esses	
o ypuss				

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.

	LOC	ation: AL	itomatic	•	
	1	Show: Bu	ilt-in Ethernet	•	
	TCP/IP	PPPoE	AppleTalk Pro	xies Ethernet	
Select a	Droxy server	to configu	re: FTP Pr	oxy Server	
🗹 FTF	Proxy		0		1
	Proxy (HTTP) are Web Proxy		Pro	xy server requires	password
	aming Proxy (J	Set Password	-
	KS Proxy		Ϋ́.		
	her Proxy	-	1		
	roxy setting: osts & Domai				
-					

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.

Networking Authentication	on	
Connect using:		
Realtek PCle GBB	E Family Controller	
		Configure
This connection uses the	following tame	Configure
Client for Micros		
QoS Packet Sc		
File and Printer		Networks
Rawether NDIS		
Internet Protoco	Version 6 (TCP/IP	v6)
Market Protoco	ol Version 4 (TCP/IP	v4)
💌 🛥 Link-Layer Topo		
Ink-Layer Topo	ology Discovery Res	ponder
Instal	Uninstall	Properties
Description Transmission Control F	Protocol/Internet Pro	tocol. The default
Description Transmission Control F wide area network pro	tocol that provides o	
Description Transmission Control F	tocol that provides o	
Description Transmission Control F wide area network pro	tocol that provides o	
Description Transmission Control F wide area network pro	tocol that provides o	
Description Transmission Control F wide area network pro	tocol that provides o	

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.

neral Alternate Conf	iguration				
ou can get IP settings his capability. Otherwis					
or the appropriate IP s	ettings.				
Obtain an IP addre	ess automatical	y.			
O Use the following I	IP address:				
IP address:					
Subnet mask:		кс.	34	- 20	
Default gateway:		- K.	14	з <u>т</u>	
Obtain DNS server	address autom	atically			
O Use the following [ONS server add	esses:			
Preferred DNS serve	ri				
Alternate DNS server	r)	*.)	(\mathbf{r})		
Validate settings i	upon exit			Adv	anced

MAC OS

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

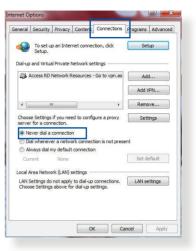
	:	ocation: Automatic	Lo	
	•	Show: Built-in Ethernet		
	Proxies Ethernet	IP PPPoE AppleTalk	TCP/I	_
	•	Using DHCP	Configure IPv4: (C.
ICP Lease	(Renew DH	192.168.182.103	IP Address:	
	P Client ID: 0/ required	255.255.255.0 DHC	Subnet Mask:	
20	ui required.	192.168.182.250	Router:	
(Optional)		192.168.128.10	DNS Servers:	
(Optional)		1	Search Domains:	Sea
1.02.0440	24ff.fe32.b18e	fe80:0000:0000:0000:0211:	IPv6 Address: 1	
		(Configure IPv6)		

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.

CAUTION: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels in not possible.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

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.

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 Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

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

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng

Additional Canadian information on RF exposure also can be found at the following web: http://www.ic.gc.ca/eic/site/smt-gst. nsf/eng/sf08792.html

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes

canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent a ecter son fonctionnement.

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。

電池波曝露量 MPE 標準值 1mWcm2,送測產品實測值 為:0.529 mWcm2。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

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

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

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get

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.

Tel. No.:	+90 212 3567070	
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.

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

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

AEEE Yönetmeliğine Uygundur.

ASUS Contact information

ASUSTeK COMPUTER INC. (Asia Pacific)

Address15 Li-Te Road, Peitou, Taipei, Taiwan 11259Websitewww.asus.com.tw

Technical Support

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

ASUS COMPUTER INTERNATIONAL (America)

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

ASUS COMPUTER GmbH (Germany and Austria)

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

Technical Support

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

Networks Global Hotline Information

Region	Country	Hotline Number	Service Hours
	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
		0049-1805010920	
	<i>c</i>	0049-1805010923	09:00-18:00 Mon-Fri
	Germany	(component support)	10:00-17:00 Mon-Fri
		0049-2102959911 (Fax)	
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
Europe	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	0046-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	0044-8448008340	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Networks Global Hotline Information

Region	Country	Hotline Numbers	Service Hours
	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri
		0000-1252/6/	09:00-17:00 Sat-Sun
		0081-473905630	09:00-18:00 Mon-Fri
		(Non-Toll Free)	09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717	09:00-18:00 Mon-Fri
Asia-Pacific		1800-8525201	
	Singapore	0065-64157917	11:00-19:00 Mon-Fri
		0065-67203835	11:00-19:00 Mon-Fri
		(Repair Status Only)	11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
	India(WL/NW)	1800-2090505	09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000	09:30-17:00 Mon-Fri
		500128 (Local Only)	9:30 – 12:00 Sat
	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
Americas	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
	Canada	1-012-202-2/0/	9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri
			08:00-15:00 CST Sat

Networks	Global	Hotline	Information
	erenar		

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

NOTE: For more information, visit the ASUS support site at: http://support.asus.com

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 in Europe:	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY