# **User Guide**

# ZenWiFi BT10

# **BE18000 Tri Band WiFi Router**





E23864 First Edition June 2024

#### Copyright © 2024 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	Getti	ng to know your wireless router
1.1	Welco	me!6
1.2	Packa	ge contents6
1.3	Your v	vireless router7
1.4		oning your wireless router8
1.5		Requirements9
2	Getti	ing started
2.1		r Setup 10
	A.	Wired connection11
	В.	Wireless connection12
2.2	Quick	Internet Setup (QIS) with Auto-detection
2.3	Conne	ecting to your wireless network
3	Confi	iguring the General and Advanced settings
3.1		ng into the Web GUI
	3.1.1	Setting up the wireless security settings
	3.1.2	Managing your network clients
	3.1.3	Monitoring your USB device
3.2	Adapt	tive QoS
	3.2.1	Managing QoS (Quality of Service) Bandwidth24
3.3	Admiı	nistration
	3.3.1	Operation Mode27
	3.3.2	System
	3.3.3	Firmware Upgrade
	3.3.4	Restore/Save/Upload Setting
3.4	AiClou	Jd 2.0
	3.4.1	Cloud Disk
	3.4.2	Smart Access

# Table of contents

3.5	AiProte	ection	
	3.5.1	Network Protection	
	3.5.2	Setting up Parental Controls	37
3.6	Firewa	II	
	3.6.1	General	40
	3.6.2	URL Filter	41
	3.6.3	Keyword filter	42
	3.6.4	Network Services Filter	43
3.7	Guest	Network and Smart Home Master	
	3.7.1	Guest Network	45
	3.7.2	Smart Home Master	47
3.8	IPv6		51
3.9	LAN		
	3.9.1	LAN IP	52
	3.9.2	DHCP Server	53
	3.9.3	Route	55
	3.9.4	IPTV	56
3.10	System	n Log	57
3.11	Traffic	Analyzer	
3.12	USB A	pplication	
	3.12.1	Using AiDisk	60
	3.12.2	Using Servers Center	62
	3.12.3	3G/4G	67
3.13	WAN		
	3.13.1	Internet Connection	69
	3.13.2	Dual WAN	72
	3.13.3	Port Trigger	73
	3.13.4	Virtual Server/Port Forwarding	75
	3.13.5	DMZ	78
	3.13.6	DDNS	79

# Table of contents

	3.13.7	NAT Passthrough	80
3.14	Wirele	SS	. 81
	3.14.1	General	81
	3.14.2	WPS	84
	3.14.3	Bridge	86
	3.14.4	Wireless MAC Filter	88
	3.14.5	RADIUS Setting	89
	3.14.6	Professional	90

# 4 Utilities

4.1	Device	e Discovery	
4.2	Firmw	are Restoration	
4.3	Settin	g up your printer server	
	4.3.1	ASUS EZ Printer Sharing	96
	4.3.2	Using LPR to Share Printer	100
4.4	Down	load Master	105
	4.4.1	Configuring Bit Torrent download settings	106
	4.4.2	NZB settings	107

# 5 Troubleshooting

5.1	Basic Troubleshooting	108
5.2	Frequently Asked Questions (FAQs)	

# Appendices

Safety Notices	129
Service and Support	131

# 1 Getting to know your wireless router

# 1.1 Welcome!

Thank you for purchasing an ASUS ZenWiFi BT10 Wireless Router! The stylish ZenWiFi BT10 features a 2.4GHz, 5GHz and 6GHz tri 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**

- ZenWiFi BT10 Wireless Router
- ☑ Network cable (RJ-45)

☑ Power adapter

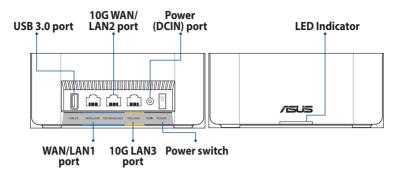
☑ Quick Start Guide

☑ Warranty card

#### NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support. Refer to Service and Support 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**



#### WAN/LAN1 port, 10G WAN/LAN2 port

Connect your optical modem to either WAN/LAN1 port or 10G WAN/LAN2 port with a network cable.

#### 10G LAN3 port

Connect your PC to a LAN port with a network cable.

#### Specifications:

DC Power adapter	DC Output: +12V with max 3A current		
<b>Operating Temperature</b>	0~40°C	Storage	0~70°C
<b>Operating Humidity</b>	50~90%	Storage	20~90%

# **1.4 Positioning your wireless router**

For optimal wireless transmission between the wireless router and connected wireless devices, ensure that you:

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

# 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/ax wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

#### NOTES:

- If your computer does not have built-in wireless capabilities, you may
  install an IEEE 802.11a/b/g/n/ac/ax WLAN adapter to your computer
  to connect to the network.
- With its tri band technology, your wireless router supports 2.4GHz, 5GHz and 6GHz 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.

#### **IMPORTANT!**

- Some wireless adapters might have connectivity issues to 802.11ax WiFi APs.
- If you're experiencing such issue, please ensure you update the driver to the latest version. Check your manufacturer's official support site where software drivers, updates, and other related information can be obtained.
  - Realtek: <u>https://www.realtek.com/en/downloads</u>
  - Mediatek: <u>https://www.mediatek.com/products/connectivity-</u> <u>and-networking/broadband-wifi</u>
  - Intel: <u>https://downloadcenter.intel.com/</u>

# 2 Getting started

# 2.1 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).

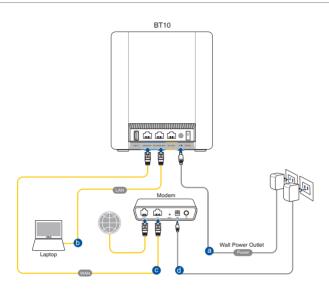


# WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
- 1. Insert your wireless router's AC adapter to the DCIN port.
- 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 DCIN port.

# A. 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:

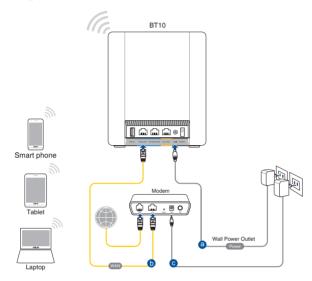
- 1. Power on your router and use a network cable to connect your computer to your wireless router's LAN port.
- 2. The web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <u>http://www.asusrouter.com</u>.
- 3. Set up a password for your router to prevent unauthorized access.

<b>Q</b> 4	Sign In ZenWiFi BT10 Sign in with your ASUS router account	
	Sign In	1994 - 1995 - 11 - 11 - 11 - 11 - 11 - 11 -

# **B.** Wireless connection

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

1. Plug your router into a power outlet and power it on.



2. Connect to the network name (SSID) shown on the product label on the back side of the router. For better network security, change to a unique SSID and assign a password.

Wi-Fi Name (SSID): ASUS\_XX

- \* XX refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back of your router.
- 3. Once connected, the web GUI launches automatically when you open a web browser. If it does not auto-launch, enter <u>http://www.asusrouter.com</u>.
- 4. Set up a password for your router to prevent unauthorized access.

#### NOTES:

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

hange the router password to prevent un	authorized access to your ASI	JS wireless router.
Router Login Name	admin	
New Password		
Retype Password		Show password

# 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. Launch a web browser. You will be redirected to the ASUS Setup Wizard (Quick Internet Setup). If not, key in <u>http://www.asusrouter.com</u> manually.



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

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

#### NOTES:

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

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

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network. Network Name (SSID)		
Wireless Security	8	
Previous App	bly	

4. On the **Login Information Setup** page, change the router's login password to prevent unauthorized access to your wireless router.

Login Username / Password Settings	Change the router password to prevent unauthorized access to your ASUS wireless router.	
	New password Retype Password	
	Previous	

**NOTE:** The wireless router's login username and password is different from the wireless 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 wireless network name (SSID) and security key allows Wi-Fi devices to log in and connect to your wireless network.

# 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.

#### NOTES:

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

# 3 Configuring the General and Advanced settings

# 3.1 Logging into the Web GUI

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

NOTE: The features may vary with different firmware versions.

# To log into the web GUI:

- 1. On your web browser, manually key in the wireless router's default IP address: <u>http://www.asusrouter.com</u>.
- 2. On the login page, key in the user name and password that you have set in 2.2 Quick Internet Setup (QIS) with Autodetection.



3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



#### \* The image is for reference only.

**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.

# 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**.
- 2. On the Network screen and under **Main Network**, you can configure the wireless security settings such as SSID, security level, and encryption settings.

	0
Main Network	Û
Network	Clients
General	~
Network Name (SSID) ZenWiFi_BT10	0:0 0:0
WiFi Band 2.4GHz GGHz	<mark>∕</mark> 5GHz
Security Open Password	RADIUS Setting
Authentication Method WPA2/WPA3-Personal	~ ⑦
Wireless Security	8
WIFi Scheduling	•
Enable MAC Filter Disable	~
Advanced Settings	>
Арріу	

#### Wireless security settings

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

4. From the **WEP Encryption** dropdown list, select the encryption method for your wireless network.

**IMPORTANT!** The IEEE 802.11n/ac/ax 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.

Internet status: Connected WAN IP: 192.168.66.8 DDNS: GO	Client status Online Wired (1) Jiesing-PC 192.168.58.129 06:08:08:08:08:09
Security level: WPA2-Personal	Refresh
Clients: 1 View List	
AiMesh Node: 0	

# 3.1.2 Managing your network clients

# To manage your network clients:

- 1. From the navigation panel, go to **General** > **Network Map**.
- 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 a USB port for connecting a USB device or a USB printer to allow you to share files and printer with clients in your network.

	LACCIMALC	JSB disk s	status
Internet status: Connected WAN IP: 192.168.66.8	Information	Health Scanner	Format
DDNS: GO	Model Name:		
	Hitachi HDP7250	25GLAT80	
	Available space:		
	232.749 GB		
	Total space:		
Security level:	232.883 GB		
WPA2-Personal	Media Server:	6	ю
	AiDisk Wizard:		io
	Safely Remove dis	k: Ren	nove
	USB Mode		8.0 🔻
Clients: 1 USB 3.0 No Device		Apply	
View LSA AlMesh Node: 0 USB 3.0 Hitachi HDP7255 v			

\* The image is for reference only.

**NOTE:** To use this feature, you need to plug a USB storage device, such as a USB hard disk or a USB flash drive, to the USB 3.0 port 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>.

**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 2.0. For more details, refer to the section **3.12 USB Application** and **3.4 AiCloud 2.0** in this user manual.

#### To monitor your USB device:

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

#### NOTES:

- For more details, refer to the section 3.12.2 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.

Internet status: Connected WAN IP: 192.168.66.8 DDNS: <u>GO</u>	External EfectUSB disk Hitachi H09725025GLAT80
Security level: WPA2-Personal	Available space: 232.749 GB Total space: 232.883 GB Media Server: GO
	AiDisk Wizard: CO Safely Remove disk: Remove USB Mode USB 3.0 *
Clients: 1 View List View List AiMesh Node: 0 USB 3.0 USB 3.0 USB 3.0 Hittachi HDP7255 *	Αρρίγ

\* The image is for reference only.

# 3.2 Adaptive QoS

# 3.2.1 Managing QoS (Quality of Service) Bandwidth

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

QoS - QoS to configuration	
To a	<ul> <li>ality of Service (QoS) ensures bandwidth for prioritized tasks and applications.</li> <li>Adaptive QoS ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via pre-defined, drag-and-drop presets: gaming, media streaming, VoIP, web surfing and file transferring.</li> <li>Traditional QoS ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via manual user-defined parameters.</li> <li>Bandwidth Limiter lets you set limits on download and upload speeds.</li> <li>enable QoS function, click the QoS slide switch and fill in the upload and download.</li> <li><u>SLFAQ</u></li> </ul>
Enable GeForce NOW QoS UPr control	P O Yes ● No
Enable QoS	OFF
	Apply

# To set up bandwidth priority:

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

NOTE: Get the bandwidth information from your ISP.

#### 3. Click Apply.

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

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

#### NOTES:

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

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

#### NOTES:

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

# 3.3.1 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.
- 2. Select any of these operation modes:
  - Wireless router mode (default): In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
  - Access Point mode: In this mode, the router creates a new wireless network on an existing network.
  - **AiMesh Node**: You can set ZenWiFi BT10 as an AiMesh node to extend an existing AiMesh routers WiFi coverage.
- 3. Click Save.

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

# 3.3.2 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**.
- 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 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.
- 3. Click Apply.

# 3.3.3 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.
- 2. In the **Firmware Version** field, click **Check** 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 4.2 Firmware Restoration.

# 3.3.4 Restore/Save/Upload Setting

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

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

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

# 3.4 AiCloud 2.0

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

AiCloud 2.0		0
links your home network and online st	ed to your data wherever and whenever you have an Internet connection orage service and lets you access your data through the AiCloud mobile vice or through a personalized web link in a web browser. Now all your d	
<ul> <li>Enter AiCloud 2.0 <u>https://www.asu</u></li> <li>Find FAQs <u>GO</u></li> </ul>	srouter.com	
The wireless router is currently using a p This router may be in a multiple-NAT env	rivate WAN IP address. /ironment. and accessing AlCloud from WAN does not work.	
USBer [] Cloud Disk	Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.	OFF
Smart Access	Enables Network Place (Samba) networked PCs and devices to be accessed remolely. Smart Access can also wake up a sleeping PC.	OFF

# To use AiCloud 2.0:

- 1. From Google Play Store or Apple Store, download and install the ASUS AiCloud 2.0 app to your smart device.
- 2. Connect your smart device to your network. Follow the instructions to complete the AiCloud 2.0 setup process.

# 3.4.1 Cloud Disk

#### To create a cloud disk:

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

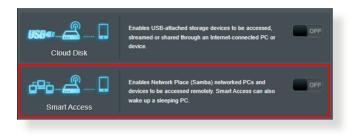


- 3. Go to <u>http://www.asusrouter.com</u> and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.
- 4. You can now start accessing Cloud Disk files on devices connected to the network.

**NOTE:** When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud 2.0 for security reason.

# 3.4.2 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 3.13.6 DDNS.
- By default, AiCloud 2.0 provides a secure HTTPS connection. Key in <u>https://[yourASUSDDNSname].asuscomm.com</u> for a very secure Cloud Disk and Smart Access usage.

# 3.5 AiProtection

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

# **3.5.1 Network Protection**

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

AiPro	tection	
ĺ	Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access. <u>AProtection FAO</u>	
Enab	led AiProtection OFF	
Ø	Router Security Assessment Scan your router to find vulnerabilities and offer available options to enhance your devices protection.	<b>1</b> Danger
2	Malicious Sites Blocking Restrict access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking, and ransomware attacks.	0 Protection
2	Two-Way IPS The Two-Way Intrusion Prevention System protects any device connected to the network from spann or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability flacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outging packets from infected devices and avoids bolnet attacks.	0 Protection
3	Infected Device Prevention and Blocking This feature prevents infected devices from being enslaved by bolnets or zombie attacks which might steal your personal information or attack other devices.	0 Protection
		Alert Preference

# **Configuring Network Protection**

# **To configure Network Protection:**

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

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

Default router login usernan	ne and password changed -	
Wireless password strength	check -	Very Weak
Wireless encryption enabled	i.	Strong
WPS Disabled -		
UPnP service disabled -		
Web access from WAN disat	oled -	Yes
PING from WAN disabled -		Yes
DMZ disabled -		Yes
Port trigger disabled -		Yes
Port forwarding disabled -		Yes
Anonymous login to FTP sh	are disabled -	Yes
Disable guest login for Netw	ork Place Share -	Yes
Malicious Website Blocking	enabled -	
Vulnerability Protection enal	bled -	
Infected Device Prevention a	and Blocking -	

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

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

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

b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.

- c. Go back to the **Router Security Assessment** page and click **Close** to exit the page.
- 5. To automatically configure the security settings, click **Secure Your Router**.
- 6. When a message prompt appears, click **OK**.

# **Malicious Sites Blocking**

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

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

# To enable Malicious Sites Blocking:

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

# **Two-Way IPS**

Two-Way IPS (Intrusion Prevention System) protects your router from network attacks by both blocking malicious incoming packets and detecting suspicious outgoing packets.

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

# To enable Two-Way IPS:

- 1. From the navigation panel, go to **General** > **AiProtection**.
- 2. From the **AiProtection** main page, click on **Network Protection**.
- 3. From the **Two-Way IPS** pane, click **ON**.

# **Infected Device Prevention and Blocking**

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

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

# To enable Infected Device Prevention and Blocking:

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

# **To configure Alert Preference:**

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

# 3.5.2 Setting up Parental Controls

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

To go to the Parental Controls main page:

From the navigation panel, go to **General** > **Parental Controls**.

Parental Controls -	Web & Apps Filters
	Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:
E	<ol> <li>In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.</li> <li>Check the unwanted content categories</li> <li>Click the plus (+) icon to add rule then click apply.</li> <li>If you want to disable the rule temporarily, uncheck the check box in front of rule. <u>Parental Controls FAQ</u></li> </ol>
Web & Apps Filters	OFF

### Web & Apps Filters

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

#### To configure Web & Apps Filters:

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

- 6. Click **(a)** to add the client's profile.
- 7. Click **Apply** to save the settings.

Pare	ntal Controls - Web & Apps Filters		
(	web & apps Fillers: . In the [Clients Nam control. The client in 2. Check the univarile 3. Click the plus (+) io	you to block access to unwanted websites and apps. e] column, select the client whose network usage you ame can be modified in network map client list. d content cleoprises on to add rule then click apply. rule temporarily, uncheck the check box in front of rule	want to
100.00	& Apps Filters ON		
Clier	nt List (Max Limit : 64) Client Name (MAC Address)	Content Category	Add / Delete
8		Adult Block adult/mature content to prevent children from violing sates that contain material of a securit, violent; and llegal nature.     Instant Message and Communication Block instant communication software and messaging apes to prevent children from becoming addicted to social networking sites.     P2P and File Transferring you can make sure your indvork has a better quality of data transmission.     Streaming and Entertainment services you can limit the time your children spend online.	۲
		No data in table.	
		Apply	

## **Time Scheduling**

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

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

By enabling Block All Device	s, all of the connected devices will be b	locked from Internet access.	
Enable block all devices	OFF		
	his feature allows you to set up a scheo 1. In [Client Name] column, select a manually key in MAC address in IU 2. In the [Add / Delete] column, click 3. In [Time Management] column, cli 4. Click [Apply] to save the configura	device you would like to man his column. the plus(+) icon to add the cl sk the edit icon to set a sche	age. You can also ient.
Enable Time Scheduling	ON		
System Time	Thu, Sep 21 12:34:41	2023	
Client List (Max Limit : 64			
Select all∨	Client Name (MAC Address)	Time Management	Add / Delete
	45 (7) (5) - (7) (6) (4)	-	Ð
	No data in table.		

## To configure Time Scheduling:

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

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

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

# 3.6 Firewall

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

NOTE: The Firewall feature is enabled by default.

# 3.6.1 General

Firewall			
General			
Enable the firewall to protect your local area packets based on the filter rules. <u>DoS Protection FAQ</u>	network against attacks from hackers. T	The firewall filters the incomin	g and outgoing
Enable Firewall	O Yes O No		
Enable DoS protection	O Yes O No		
Logged packets type	None 🗸		
Respond ICMP Echo (ping) Request from WAN	• Yes O No		
Basic Config			
Enable IPv4 inbound firewall rules	• Yes O No		
Inbound Firewall Rules (Max Limit : 1)	28)		
Source IP	Port Range	Protocol	Add / Delete
		TCP 🗸	۲
	No data in table.		
IPv6 Firewall All outbound traffic coming from IPv6 hosts must be specifically allowed here. You can leave the remote IP blank to allow t (2001::1111:2222:3333/04 for example)			nbound traffic
Basic Config		_	
Enable IPv6 Firewall	O Yes O No		
Famous Server List	Please select 🗸		
Inbound Firewall Rules (Max Limit : 1)	28)		
Service Name Remote IP/CIDR	Local IP	Port Range Protocol	Add / Delete
		TCP 🗸	• •
	No data in table.		
	Apply		

#### To set up basic Firewall settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **General**.
- 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.

# 3.6.2 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.

Key in the keywords for the sites	that you want to block. list The URL filter will block the http://www.abcXXX.com,	http://www.VVVhbh.com.ond.co.on
or example, enter XXX in the	IST THE OKE IIIEF WIII DIOCK THE HUP J/WWW.abCAAA.com,	http://www.XXX.bbb.com and so on.
Basic Config		
Enable URL Filter		
Filter table type		
URL Filter List: (Max Limit :	64)	
	URL Filter List:	Add / Delete
		Ð
	Apply	

#### To set up a URL filter:

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

# 3.6.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

Firewall - Keyword Filter		
Keyword Filter allows you to block th	e clients' access to webpages containing the specified key	/words.
Limitations of the filtering function :		
<ol> <li>Compressed webpages that to 2. Https webpages cannot be fill</li> </ol>	use HTTP compression technology cannot be filtered. <u>See</u> lered.	<u>here for more details.</u>
Basic Config		
Enable Keyword Filter	Enabled      Disabled	
Keyword Filter List (Max Limit	: 64)	
	Keyword Filter List	Add / Delete
		Ð
	No data in table.	
	Арріу	

#### To set up a keyword filter:

- From the navigation panel, go to Advanced Settings > Firewall > Keyword Filter.
- 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.

## 3.6.4 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.

Firewall - Network	Services Filter				_
The Network Services filt For example, if you do no 80 will be blocked (but htt Leave the source IP field	t want the device to ps can not be block	use the Internet service, ed).			
Deny List Duration : Dur specified duration, all the Allow List Duration : Du	clients in LAN can a	access the specified netwo	ork services.		
NOTE : If you set the sub Internet service.	net for the Allow Lis	t, IP addresses outside th	e subnet will not be		nternet or any
Network Services Filt	er	_			
Enable Network Services F	Filter	🔍 Yes 🙁 No			
Filter table type		Deny List 🗸			
Well-Known Applications		User Defined 🗸			
Date to Enable LAN to WA	N Filter	🗹 Mon 🗹 Tue 🗹 Wed	🏹 Thu 🔽 Fri		
Time of Day to Enable LAM	to WAN Filter				
Date to Enable LAN to WA	N Filter	🗹 Sat 🗹 Sun			
Time of Day to Enable LAM	to WAN Filter				
Filtered ICMP packet types					
Network Services Fill	er Table (Max Lir	nit : 32)			
Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
					Ð
		No data in tal	ole.		
		Apply			

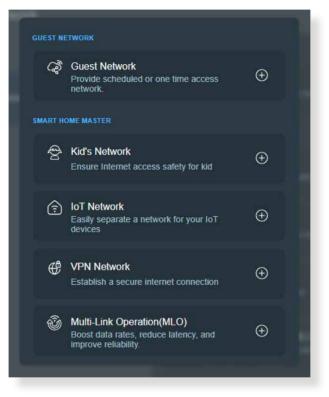
### To set up a Network Service filter:

- 1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Network Service Filter**.
- 2. On the Enable Network Services Filter field, select Yes.
- 3. Select the Filter table type. **Deny** blocks the specified network services. **Allow** 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.

# 3.7 Guest Network and Smart Home Master

## 3.7.1 Guest Network

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



#### To create a guest network:

- 1. From the navigation panel, go to General > Network.
- 2. Select **Guest Network** and assign a network name for your temporary network in the **Network Name (SSID)** field.
- 3. Select an authentication method under Security.

- 4. Specify the access time or choose **Scheduled** to add an online schedule profile.
- 5. Select the **WiFi Band** for the guest network that you want to create.
- 6. Enable or disable the **Bandwidth Limiter**.
- 7. Enable or disable the **Access Intranet**.
- 8. When done, click **Apply**.

Guest Network	0
Network Name (SSID)	
Security	
Open System	Password
WiFi Scheduling	
Scheduled <b>One Time Access</b>	
30 mins 1 hr(s)	2 hr(s)
4 hr(s) 6 hr(s)	Custom
More Config	^
WiFi Band	
2.4GHz / 5GHz	<u> </u>
AiMesh	^
ZenWiFi BT10 192.168.50.1	24 3 6
Bandwidth Limiter	
Access Intranet	
Apply	

# 3.7.2 Smart Home Master

Smart Home Master is a powerful and user-friendly tool for network segmentation. It simplifies the process of creating and managing advanced subnetworks scenarios like creating a dedicated SSID for your children's devices, connecting to a VPN through a dedicated subnetwork, or even creating one secure SSID for all your IoT devices.

#### To create a Kid's Network:

- 1. From the navigation panel, go to **General** > **Network**.
- 2. Select **Kid's Network** and assign a network name and security key in the **Network Name (SSID)** and **Wireless Security** fields.
- 3. Customize Internet access time in the **Online schedule** field.
- 4. Select the **WiFi Band** for the kid's network that you want to create.
- 5. Enable or disable the **Bandwidth Limiter**.
- 6. Enable or disable the Access Intranet.
- 7. When done, click **Apply**.

Kid's Network	0
Network Name (SSID)	i
Wireless Security	Ø
WiFi Scheduling	
Online schedule	$\oplus$
WEEKDAY(S) 17:00 - 21:00	<b></b> <sup>†</sup>
WEEKEND 16:00 - 22:00	•
More Config	~
WiFi Band	
2.4GHz / 5GHz	٣)
AiMesh	^
ZenWiFi BT10 192.188.50.1	24 3 8
Bandwidth Limiter	
Access Intranet	-
Apply	

### To create an IoT Network:

- 1. From the navigation panel, go to **General** > **Network**.
- 2. Select **IoT Network** and assign a network name and security key in the **Network Name (SSID)** and **Wireless Security** fields.
- 3. Select the **WiFi Band** for the IoT network that you want to create.
- 4. Customize Internet access time by enabling **WiFi Scheduling**.
- 5. When done, click **Apply**.

IoT Network	٥
Network Name (SSID)	
Wireless Security	
	8
Use same subnet as main network	
More Config	^
WiFi Band	
2.4GHz	~
AilMesh	~
ZenWiFi BT10 192.188.50.1	24 5 8
WIFi Scheduling	
Apply	

#### To create a VPN Network:

- 1. From the navigation panel, go to **General** > **Network**.
- 2. Select **VPN Network** and assign a network name and security key in the **Network Name (SSID)** and **Wireless Security** fields.
- 3. If you haven't set up a VPN profile for the VPN server or VPN client, click **Go Setting** to create a VPN profile.
- 4. Select the **WiFi Band** for the VPN network that you want to create.
- 5. Customize Internet access time by enabling WiFi Scheduling.
- 6. Enable or disable the **Bandwidth Limiter**.
- 7. Enable or disable the Access Intranet.
- 8. When done, click **Apply**.

VPN Network	٥
Network Name (SSID)	
Wireless Security	<u> </u>
	Ø
VEN CLIENT There is no VPN profile now. Click [Go S VPN setting page and create.	
Go Setting →	
VPN SERVER WireGuard VPN	
Go Setting →	
More Config	
More Config WiFi Band 2.4GHz / 5GHz	
WiFi Band	
WiFi Band 2.4GHz / 5GHz	^ ~ ^ 2 8 8
WiFi Band 2.4GHz / 5GHz AilMesh ZenWiFi BT10	^ ~ ^ & & & & & & & & & & & & & & & & & & &
WIFI Band 2.4GHz / 5GHz AiMesh ZenWiFi BT10 192.168.50.1	

# 3.8 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.

Configure the IPv6 Internet setting. <u>IPv6_FAQ</u>	
Basic Config Connection type Disable •	

## 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.

# 3.9 LAN

# 3.9.1 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.

LAN - LAN IP		
Configure the LAN setting of ASUS Router.		
Host Name	ASUS Router	
ASUS Router's Domain Name		
IP Address	192.168.50.1	
Subnet Mask	255.255.255.0	
Apply		

### To modify the LAN IP settings:

- 1. From the navigation panel, go to **Advanced Settings** > **LAN** > **LAN IP**.
- 2. Modify the IP address and Subnet Mask.
- 3. When done, click **Apply**.

# 3.9.2 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.

LAN - DHCP Server		
Basic Config		
Enable the DHCP Server	O Yes ● No	
ASUS Router's Domain Name		
IP Pool Starting Address	192.168.50.2	
IP Pool Ending Address	192.168.50.254	
Lease time	86400	
Default Gateway		
DNS and WINS Server Setting		
DNS Server 1		
DNS Server 2		
Advertise router's IP in addition to user- specified DNS	O Yes ● No	
WINS Server		
Manual Assignment		
Enable Manual Assignment	• Yes • No	
Manually Assigned IP around the DHC	P list (Max Limit : 64)	
Client Name (MAC Address)	IP Address DNS Server (Optional) Host Name (Optional) Add / Delete	
ex: 017712424040		
	No data in table.	
Apply		

### To configure the DHCP server:

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

# 3.9.3 Route

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

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

LAN - Route					
This function allows you to a to the Internet.	idd routing rules i	into. It is useful if you connect several	I routers behind I	to share the sar	ne connection
Basic Config		_			
Enable static routes • Yes • No					
Static Route List (Max L	.imit : 32) Netmask	Gateway	Metric	Interface	Add / Delete
			<b>.</b>		Ð
		No data in table.			
		Apply			

### To configure the LAN Routing table:

- 1. From the navigation panel, go to **Advanced Settings** > **LAN** > **Route**.
- 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**.

# 3.9.4 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.

LAN - IPTV	
o watch IPTV, the WAN port must be cor issigned to primary WAN.	nnected to the Internet. Please go to $\underline{WAN}$ - Dual $\underline{WAN}$ to confirm that WAN port is
LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None v
Special Applications	
Use DHCP routes	Microsoft •
Enable multicast routing (IGMP Proxy)	Disable v
	0

# 3.10 System Log

System Log contains your recorded network activities.

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

#### To view your system log:

- 1. From the navigation panel, go to **Advanced Settings** > **System Log**.
- 2. You can view your network activities in any of these tabs:
  - General Log
  - Wireless Log
  - DHCP Leases
  - IPv6
  - Routing Table
  - Port Forwarding
  - Connections

System Log - General Log		
This page shows the detailed system's activit	ties.	
System Time	Thu, Aug 23 07:15:34 2018	
Uptime	0 days 1 hours 18 minute(s) 11 seconds	
Remote Log Server	Apply	
Aug 23 06:38:28 kernel: [(0:33 41m] Aug 23 06:58:58 kernel: [(0:33 41m] Aug 23 06:58:58 kernel: [(0:33 41m] Aug 23 06:58:58 kernel: [(0:33 41m] Aug 23 06:58:55 kernel: [(0:33 41m] Aug 23 06:58:55 kernel: [(0:33 41m] Aug 23 06:58:55 kernel: [(0:33 41m] Aug 23 06:58:57 kernel: [(0:33 41m] Aug 23 07:07:14 minupad[768]; ker Aug 23 07:07:14 minupad[778]; ker Aug 23 07:07:15 minupad[772]; ker	P listening on port 53102 tening for NAT-MEYPCF traffic on port 5351 PATHSTAT] path add fidw ASSERT: (encoute_pathkey != PATH_IX_INVAL PATHSTAT] path_add fidw ASSERT: (encoute_pathkey != PATH_IX_INVAL PATHSTATI path_add fidw ASSERT: (encoute_pathkey != PATH_IX_INVAL PATHSTATI PATH_ADA Ling dow MinIUPATH PATHSTATI PATHSTATH IX_INVAL PATHSTATH_ADA PATHSTATH PATHANA PATHSTATH_ADA PATHSTATH PATHANA PATHSTATH PATHANA PATHSTATH_ADA PATHSTATH PATHANA PATHSTATH PATHANA PATHSTATHANA PATHSTATHANA PATHSTATHANA PATHSTATH_ADA PATHSTATHANA PATHSTATHA	

# 3.11 Traffic Analyzer

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

raffic Monito	or				
affic Monitor allow	rs you to monitor the incoming or (	outgoing packets	of the following:		
	Internet	Wired		Wireless	
Reception					packets from wireless
Transmission					
cale KB 🗸					
DTE: Packets from affic Monitor FA	n the Internet are evenly transmitt	ed to the wired a	nd wireless devices.		
		Wireless			
9.47 MB/s		WAN			Thu 02:44 pm / 0.03 MB/s
6.63 MB/s					
4.74 MB/s					
2.37 MB/s					
				Ä	
Currer	nt Avera	ge	Maximum		Total
			9.47 MB/s	_	98.32 MB
0.07 ME	3/s 0.16 M	B/S	5.47 MD/S		ALL CONTRACTOR

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

# 3.12 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 a USB flash drive, in the USB 3.0 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.



# 3.12.1 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.

1		2	3)	
O admin ● limite	n rights d access rights ss access rights	ed.: Decide how to share your folders.		
	Account	Password •	Read	Write
	· · · · · · · · · · · · · · · · · · ·	Previous Next	)	

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

$\bigcirc 1 $	2 3
Create your domain name via t	the ASUS DDNS services.
• I will use the service	
Key in the name	.asuscomm.com
Disable DDNS.	
N	Previous Next

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

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

# 3.12.2 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 ZenWiFi BT10's network.



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

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

## Using Network Place (Samba) Share service

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

USB Application - Network Place (Samba) Share / Cloud Disk				
Set the account and permission	of network place(samba) service.			
Enable Share	ON			
Allow guest login	OFF Usemame and password is necessary to log in network place(Samba)			
Device Name				
Work Group	WORKGROUP			
Maximum number of concurrent	connections 5			
	Apply			
⊕ ⊝ ⊘				
	ASUS Router R/W R No			
	Save			
		_		

#### To use Samba share:

1. From the navigation panel, go to General > USB application > Servers Center > Network Place (Samba) Share / Cloud Disk.

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

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

#### To create a new account:

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

Add new account	×
New account has no read/write a	ccess rights.
Account:	00-0E
Password:	
Retype password:	
	Add

#### 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	1 ×
The default access righ	nts for a new folder is read/write.
Folder Name:	
roider Name.	
addel	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.

USB Application - FTP Sh	iare 🕥
Set the account and permission of	of FTP service.
Enable FTP	OFF
Enable WAN access	OFF
Allow anonymous login	OFF Usemane and password is necessary to log in FTP service.
Enable TLS support	O Yes ● No
Maximum number of concurrent cor	nnections 5
Character set on FTP Server	
	Арріу
$\odot \bigcirc \bigcirc$	R 2 🕅
в	NB878A175D4A6FD54D2E6 ID51950B5EF7.asuscomm. R/W W R No om

#### To use FTP Share service:

**NOTE:** Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.12.1 Using AiDisk**.

- 1. From the navigation panel, click **General** > **USB application** > **Servers Center** > **FTP Share**.
- 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.

# 3.12.3 3G/4G

3G/4G USB modems can be connected to ZenWiFi BT10 to allow Internet access.

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

USB Modem / USB Tethering		
Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem.		
Basic Config		
Enable USB Mode		
Select USB Device	Auto 🗸 🖓	
APN Configuration		
Telecommunications Standards	WCDMA (UMTS) / LTE V	
APN Service(optional)	internet	
Dial Number	*99#	
Username		
Password		
Authentication		
PIN code		
USB Adapter		
USB MTU		
Special Requirement from ISP		
Extend the TTL value	● Yes O No	
Spoof LAN TTL value	● Yes ● No	

#### 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.

# 3.13 WAN

## **3.13.1 Internet Connection**

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

WAN - Internet Connection		
ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu baside WAN Connection Type. The setting fields differ depending on the connection type you selected.		
Configure the Ethernet WAN settings of ASUS Router.		
Basic Config		
WAN Connection Type	Automatic IP ~	
Enable WAN	O Yes ● No	
Enable NAT	O Yes ● No	
Enable UPnP UPnP FAQ	O Yes ● No	
Enable WAN Aggregation	● Yes: ● No WAN Aggregation combines have network connections to increase your WAN speed up to 2006p. Connect your router's WAN port and I.NA 4 port to your modern's LAM ports (ensure you use two cables with the same specification) <u>WAN Appropriate EAQ</u>	
WAN DNS Setting		
DNS Server	Default status : Get the DNS IP from your ISP automatically Assign a DNS service to improve security, block advertisement and gain faster performance.	
Forward local domain queries to upstream DNS	● Yes O No	
Enable DNS Rebind protection	• Yes O No	
Enable DNSSEC support	● Yes <sup>O</sup> No	
Prevent client auto DoH	Autov	
DNS Privacy Protocol	None	
DHCP Option		
Class-identifier (Option 60):		
Client-identifier (Option 61):		
Class-Identifier (Option 60):		
Client-identifier (Option 61):		
Account Settings		
Authentication	None ~	
PPP Echo Interval	6	
PPP Echo Max Failures	10	
Special Requirement from ISP		
Host Name		
MAC Address	MAC Clone	
DHCP query frequency	Aggressive Mode 🗸	
Extend the TTL value	● Yes O No	
Spoof LAN TTL value	• Yes O No	
Apply		

### To configure the WAN connection settings:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection**.
- 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.

## 3.13.2 Dual WAN

The Dual WAN allows you to select two ISP connections to your router, a primary WAN and a secondary WAN.

### To configure Dual WAN:

- 1. From the navigation panel, go to **Advanced Settings > WAN**.
- 2. Go to **Dual WAN** field, turn **ON**.
- 3. Choose your **Primary WAN** and **Secondary WAN**. There are WAN, USB, Ethernet LAN and 2.5G WAN for your options.
- 4. Choose Fail Over or Load Balance.
- 5. Click Apply.

**NOTE:** Detailed explanations are available on the ASUS Support Site FAQ <u>https://www.asus.com/support/FAQ/1011719</u>.

WAN - Dual WAN		
ASUS Router provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connection. Dual WAN FAQ To enable WAN Aggregation go to the WAN-Internet Connection page.		
Basic Config		
Enable Dual WAN	ON	
Primary WAN	WAN V	
Secondary WAN	US8 V	
Dual WAN Mode	Fail Over 🗸 🗖 Allow failback	
Auto Network Detection Detailed explanations are available on the <u>ASUS Support Sile FAQ</u> which may help you use this function effectively:		
Detect Interval	Every 5 seconds	
Failover Trigger Condition	When the current WAN fails 12 continuous times, failover to Secondary WAN	
Network Monitoring	DNS Query Ping	

# 3.13.3 Port Trigger

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

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

WAN - Port Trigger					
Port Trigger allows you to temporar two methods for opening incoming , the time and devices must use stati- to the trigger port. Unlike port forwa multiple devices to share a single of <u>Port_Trigger_EAQ</u>	data ports: port forwardir c IP addresses. Port trigg rding, port trigger does n	ng and port trigger ger only opens the not require static IF	: Port forwarding opens e incoming port when a P addresses for LAN de	the specified da LAN device requ vices. Port forwa	ita ports all iests access
Basic Config					
Enable Port Trigger	🔍 Yes 🔍 Ni				
Well-Known Applications					
Trigger Port List (Max Limit : 32 )	Ð				
Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
		Apply			

#### To set up Port Trigger:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Port Trigger**.
- 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.

### 3.13.4 Virtual Server/Port Forwarding

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

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

WAN - Virtual S	erver / Port For	warding					
network (LAN). For forwarding setting. F ports in router and r	a faster connection, Please refer to the P edirect data through iy a Port Range for c	some P2P applica 2P application's us those ports to a si lients on the same	o connect to a specific tions (such as BitTorre er manual for details. ) ngle client on your net network, enter the Ser	nt), may als /ou can ope work.	o require that you se In the multiple port o	et the por r a range	t • of
			as the HTTP server's perver's perver's perver		pr your WAN setup, I	then you	r http
When you set 20     ASUS Server's na		ver's port range for	your WAN setup, then	your FTP s	erver would be in co	nflict with	h
<u>Virtual Server</u>	/ Port Forward	ing_FAQ					
Basic Config	_	_		_	_	_	_
Enable Port Forward	ling	OF					
Port Forwarding	List (Max Limit : 6	;4)		_		_	
Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
			Add profile				

#### To set up Port Forwarding:

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

- 2. Configure the following settings below. When done, click **ON**.
  - Enable Port Forwarding: Turn ON 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 **3.9 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.

# 3.13.5 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.

WAN - DMZ	
	expose one computer to the Internet, so that all the inbound packets will be redirected to the computer you run some applications that use uncertained incoming ports. Please use it carefully.
Special Applications:	
<ul> <li>Some applications</li> </ul>	require special handler against NAT. These special handlers are disabled in default.
<ul> <li>Please add a rule</li> </ul>	o port forwarding list for USB Disk access properly on FTP service.
DMZ_FAQ	
Enable DMZ	• Yes • No
	Apply

#### To set up DMZ:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DMZ**.
- 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**.

# 3.13.6 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.

WAN - DDNS		
dynamic public IP address, through its regis and other DDNS services.	a service that allows network clients to connect to the wireless stered domain name. The wireless router is embedded with the ease go to <u>https://iploekup.asus.com/nslookup.php</u>	ASUS DDNS service
The wireless router currently uses a private This router may be in the multiple-NAT envi	WAN IP address. ironment and DDNS service cannot work in this environment.	
WAN. Use "[hostname] asuscomm.com" to	re the port forwarding or DMZ settings to allow other WAN clien	
Server	WWW.ASUS.COM V Deregister	
Host Name	A8878A175D4A6FD54D2E6BD6195DB5EF7	.asuscomm.com
DDNS Status		
DDNS Registration Result	Registration is successful.	
HTTPS/SSL Certificate	Free Certificate from Let's Encrypt     Import Your Own Cert	ificate O None
	Apply	

#### To set up DDNS:

- 1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DDNS**.
- 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.

# 3.13.7 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**. When done, click **Apply**.

VAN - NAT Passthrough	
nable NAT Passthrough to allow a Virtual	Private Network (VPN) connection to pass through the router to the network clients.
PPTP Passthrough	
L2TP Passthrough	
IPSec Passthrough	
RTSP Passthrough	
H.323 Passthrough	Enable 🗸
SIP Passthrough	Enable 🗸
PPPoE Relay	
FTP ALG port	
	Арріу

# 3.14 Wireless

## 3.14.1 General

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

Wireless - General	
Set up the wireless related information belo	W.
Enable Smart Connect	OFF
Band	2.4 GHz 🗸
Network Name (SSID)	LIAO
Hide SSID	● Yes O No
Wireless Mode	Auto 🗸 🖌 b/g Protection 🗖 Disable 11b
802.11ax / WiFi 6 mode	Enable v If compatibility issue occurs when enabling 802.11ax / WiFI 6 mode, please check EAQ
WiFi Agile Multiband	Disable 🗸
Target Wake Time	Disable 🗸
Channel bandwidth	20/40 mHz 🗸
Control Channel	Auto V Current Control Channel: 6
Extension Channel	Auto 🗸
Authentication Method	WPA2-Personal v 🕜
WPA Encryption	AES 🛩
WPA Pre-Shared Key	Weak
Group Key Rotation Interval	3600
	Apply

#### To configure the basic wireless settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General**.
- 2. Select 2.4GHz, 5GHz or 6GHz 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, 5GHz and 6GHz 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.
  - **Nonly**: Select **Nonly** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
- 6. 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.

- 7. 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.
- 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**.

# 3.14.2 WPS

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

NOTE:	Ensure that the device	es support WPS.
-------	------------------------	-----------------

Wireless - WPS	
WPS (WiFi Protected Setup) provides easy a PIN code or the WPS buttton.	ind secure establishment of a wireless network. You can configure WPS here via the
Enable WPS	ON
Current Frequency	2.4 GHz
Connection Status	ldle
Configured	Reset Enabled Pressing the reset fulfion resets the network name (SSID) and WPA encryption key.
AP PIN Code	51246044
button on the client's WLAN adapter a • Method2: Start the client WPS proces field and click Start. Please check the	s interface (or press the physical WPS button on the router), then press the WPS nd walt for about three minutes to make the connection. s and get the client PIN code. Enter the client? PIN code on the Client PIN code user manual of your writeless client to see if it supports the WPS function. If your PS function, you have to configure the wireless client manually and set the same
WPS Method	Push button     Client PIN Code  Start

#### To enable WPS on your wireless network:

- From the navigation panel, go to Advanced Settings > Wireless > WPS.
- 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 or 6GHz, 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.

# 3.14.3 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.

Wireless - Bridge		
Bridge (or named WDS - Wireless Distribut wirelessly. WDS may also be considered a	ion System) function allows your ASUS Router to connect to an repeater mode.	n access point
	en/NONE, Open System/WEP] security authentication metho please select Legacy as your wireless mode first. his <u>FAQ</u> for more details.	
To enable WDS to extend the wireless sig	nal, please follow these steps :	
<ol> <li>Ensure that this wireless router and</li> <li>Key in the remote AP mac in the re router's MAC address.</li> <li>To get the best performance, pleas</li> </ol>	e and add MAC address of APs in Remote AP List. I the AP you want to connect to use the same channel. mote AP list and open the remote AP's WDS management int e go to Advanced Settings > Wireless > General and assign t tension channel to every router in the network.	
You are currently using the Auto chan	nel. Click <u>Here</u> to modify.	
Basic Config		
2.4 GHz MAC		
5 GHz MAC	C8:7F:54:12:69:CC	
Band	2.4 GHz ∨	
AP Mode	AP Mode AP only v	
Connect to APs in list   Yes  No		
Remote AP List (Max Limit : 4)		
	Remote AP List	Add / Delete
	<b>*</b>	Ð
	No data in table.	
	Apply	
	Арру	

To set up the wireless bridge:

- 1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WDS**.
- 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.

# 3.14.4 Wireless MAC Filter

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

Wireless - Wireless MAC Filter		
Wireless MAC filter allows you to control pac	kets from devices with specified MAC address in	your Wireless LAN.
Basic Config		
Band	2.4GHZ *	
Enable MAC Filter	O Yes ● No	
MAC Filter Mode	Accept •	
MAC filter list (Max Limit : 64)		
Client	Name (MAC Address)	Add / Delete
		Ð
	Apply	

#### To set up the Wireless MAC filter:

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

## 3.14.5 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.

	tional parameters for authorizing wireless clients through RADIUS server. It is required whil "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".
Band	2.46Hz *
Server IP Address	
Server Port:	
Connection Secret	

#### 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 **3.14.1 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.

# 3.14.6 Professional

The Professional screen provides advanced configuration options.

Band	to set up additional parameters for wireless. But default values are recommended.
Enable Radio	O Yes ● No
Enable wireless scheduler	● Yes O No
Set AP Isolated	• Yes • • No
Roaming assistant	Eriab Te V Disconnect clients with RSSI lower than : -70 dBm
Bluetooth Coexistence	Disable 🗸
Enable IGMP Snooping	Enable 🗸
Multicast Rate(Mbps)	Auto 🗸
Preamble Type	Long 🗸
AMPDU RTS	Enable 🗸
RTS Threshold	2347
DTIM Interval	
Beacon Interval	100
Enable TX Bursting	Enable 🗸
Enable WMM	Enable 🗸
Enable WMM No-Acknowledgement	Disable 🗸
Enable WMM APSD	Enuble 🗸
Optimize AMPDU aggregation	Disable 🗸
Modulation Scheme	Up to MC5 11 (NitroQAM/1024-QAM) 🗸
Airtime Fairness	Disable 🗸
Multi-User MIMO	Enable 🗸
OFDMA/802.11ax MU-MIMO	Disable 🗸
Explicit Beamforming	Enable 🗸
Universal Beamforming	Enable 🗸
Tx power adjustment	Performance

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

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

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

• Enable wireless scheduler: You can choose clock format as 24-hour or 12-hour. The color in the table indicates Allow or Deny. Click each frame to change the settings of the hour of the weekdays and click **OK** when done.

inder: The Sys	atem time zone is	different from yo	ur locale setting				
lock ormat	24-hour 🔻	Allow		Deny [			
Active Sche	iule						
System Time			Thu, Aug	23 06:59:27 2	018		
Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00~01					ĺ		
01 ~ 02							
02~03							
03~04							
04~05							
05~06							
06~07							
07~08							
08~09							
09~10							
10~11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14~15							
15~16							
16~17							
17 ~ 18							
18~19							
19 ~ 20					j,		
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

- 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.
- 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.

# 4 Utilities

#### NOTES:

- Download and install the wireless router's utilities from the ASUS website:
  - Device Discovery v1.4.8.3 at <u>https://dlcdnets.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Discovery.zip</u>
  - Firmware Restoration v2.1.0.3 at <u>https://dlcdnets.asus.com/</u> pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
  - Windows Printer Utility v1.0.5.5 at <u>http://dlcdnet.asus.com/pub/</u> ASUS/LiveUpdate/Release/Wireless/Printer.zip
- The utilities are not supported on MAC OS.

# 4.1 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 > 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.

# 4.2 Firmware Restoration

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



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

NOTE: This feature is not supported on MAC OS.

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

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

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

**IP address**: 192.168.1.x

Subnet mask: 255.255.255.0

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

**NOTE**: This is not a firmware upgrade utility and cannot be used on a working ASUS Wireless Router. Normal firmware upgrades must be done through the web interface. Refer to **Chapter 3: Configuring the General and Advanced Settings** for more details.

# 4.3 Setting up your printer server

## 4.3.1 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 $^{\circ}$  10 and Windows $^{\circ}$  11.

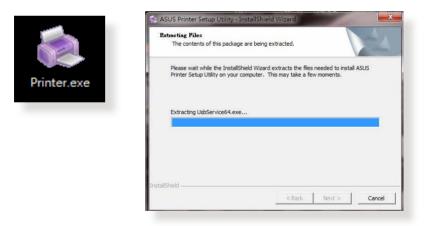
#### To set up the EZ Printer sharing mode:

- 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<sup>®</sup> 10 and Windows<sup>®</sup> 11 only. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

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



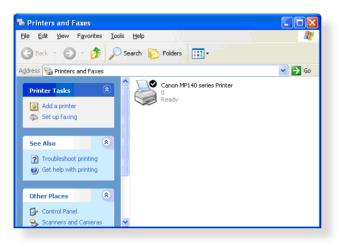
4. Follow the onscreen instructions to set up your hardware, then click **Next**.



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

Found New Hardware W	izard
	Welcome to the Found New Hardware Wizard Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission). Read our privacy policy
	Can Windows connect to Windows Update to search for software? Yes, this time only Yes, now and every time I connect a device No, not this time
	Click Next to continue.
	< Back Next > Cancel

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

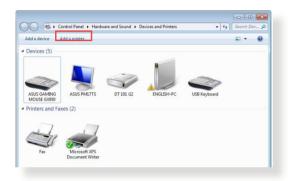


## 4.3.2 Using LPR to Share Printer

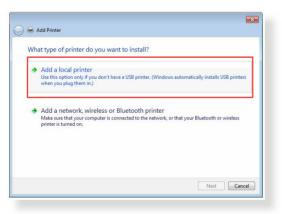
You can share your printer with computers running on Windows<sup>®</sup> and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

#### Sharing your LPR printer To share your LPR printer:

1. From the Windows<sup>\*</sup> 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:	LPT1: (Printer Port)
Oreate a new port:	20 20
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**.

e		
e		
e driver to use		
	e driver to use	: driver to use

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

	information required	
The device is not	found on the network. Be sure that:	
1. The device is t		
2. The network i	s connected. properly configured.	
	n the previous page is correct.	
	ddress is not correct, click Back to return to the prev orm another search on the network. If you are sure	
device type below		
device type below		*

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	55: 192.168.1.1
Protocol	
C Raw	LPR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	LPRServer
E LPR Byte Counting E	inabled
SNMP Status Enable	d
Community Name:	public
SNMP Device Index:	1
	OK Cancel

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

	information required	
The device is not	found on the network. Be sure that:	
1. The device is		
2. The network i		
	properly configured. n the previous page is correct.	
address and perfo device type below	erm another search on the network. If you are sur	re the address is correct, select the
Device Type		
	Generic Network Card	*
Standard	Generic Network Card	

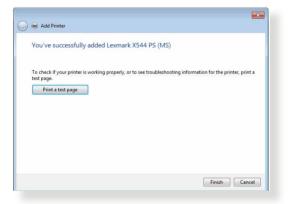
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.

Manufacturer  Printers Kyocen Lanier Lamier Lamark Emarkk Printers	The second se	the list. Click Windows Update to see more models. an installation CD, click Have Disk.
	Kyocera Lanier	Lexmark X422 (MS)
Microsoft Carl Convert Mode (MS)		

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



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



# 4.4 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 **4.4.1 Configuring Bit Torrent download settings**.

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

Task	General Setting	
	Download Schedule	
Settings	Immediately     At Scheduled Time     Remind: The System lime zone is difference	
General	Download to	/tmp/mnt/sdal/Download2/Complete Browse
Bit Torrent	Refresh rate	5 Seconds
NZB	DownloadMaster Port	8061
•	Download Master Https Port	8481
🗙 aMule	WAN network	OFF Enable/disable the WAN connection.
	Keep seeding after task completed	ON
		Apply

### 4.4.1 Configuring Bit Torrent download settings

Task	BitTorrent Setting	
	Port	
Settings	OUse the default port Use the following port	
Seneral	Incoming part: 51413	
Bit Torrent	Speed Limits:	
Bit forrent	Maximum download speed:	Unlimited
X NZB	Maximum upload speed:	C Unlimited
aMule	BitTorrent Network setting	
~	BitTorrent protocol encryption	Encryption enabled *
	Maximum peers allowed per torrent	60
	Global Maximum connection	240
	DHT network	ON Enable DHT to activate trackerless torrent downloading activities.
	PEX network	
		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.

## 4.4.2 NZB settings

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

/islis		Logout	English 🔻
A CONTRACTOR			0
Task	NZB Setting		
🛃 Task	Setup USENET server to download NZB files:		
Settings	USENET Server		
General	USENET Server Part		
	Maximum download speed:	Unlimited	
Bit Torrent	SSL/TLS connection only	OFF	
NZB NZB	User name		
aMule	Password		
•	Confirm Password		
	Maximum number of simultaneous connections to this server		
		Apply	
		2018 AS	SUSTeK Computer Inc. All rights reserved

# 5 Troubleshooting

This chapter provides solutions for issues you may encounter with your router. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at:

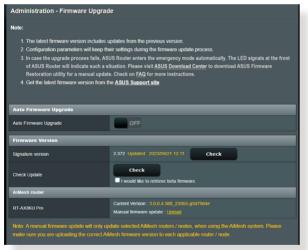
<u>https://www.asus.com/support/</u> for more product information and contact details of ASUS Technical Support.

# 5.1 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. Click Check to verify if the latest firmware is available.



- 2. If the latest firmware is available, visit the ASUS global website at <u>https://www.asus.com/networking-iot-servers/whole-</u> <u>home-mesh-wifi-system/zenwifi-wifi-systems/asus-zenwifi-</u> <u>BT10/helpdesk\_bios/?model2Name=ASUS-ZenWiFi-BT10</u> to download the latest firmware.
- 3. From the **Firmware Version** page, click **Check** 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 router.

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

#### Check if your network settings are correct.

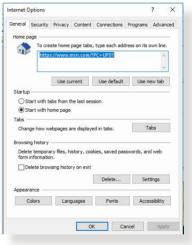
 Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.  Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You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

Internet status: Connected Wan IP: 192.168.66.8 DDNS: <u>GO</u>	Client status Online Wired (1)  Jiening-PC  192.166.59.129  90:90:00:00:00:00
Scurty level: WRA2-Personal C Clerts: 1 Verw List Verw L	Refresh

# 5.2 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. Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer, follow these steps:
  - Launch Internet Explorer, then click Tools > Internet Options.
  - 2. In the General tab, under Browsing history, click Delete..., select Temporary Internet files and website files and Cookies and website data then click Delete.



#### NOTES:

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

# The client cannot establish a wireless connection with the router.

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

- Out of Range:
  - Move the router closer to the wireless client.
- 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.

LAN - DHCP Server				
DHCP (Dynamic Host Configuration Protocol server can assign each client an IP address a supports up to 253 IP addresses for your loc Manually Assigned IP around the DHCP	nd informs the client o al network.			
Basic Config				
Enable the DHCP Server	🔾 Yes 🔍 No			
ASUS Router's Domain Name				
IP Pool Starting Address	192.168.50.2			
IP Pool Ending Address	192.168.50.254			
Lease time	86400			
Default Gateway				
DNS and WINS Server Setting	_			
DNS Server 1				
DNS Server 2				
Advertise router's IP in addition to user- specified DNS	OYes ⊙No			
WINS Server				
Manual Assignment			_	
Enable Manual Assignment	•Yes •No			
Manually Assigned IP around the DHC	P list (Max Limit : 6	:4)		
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
641 (68)/7C76411234691CE				€
	No data in	table.		
	Аррі	ły		

 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.

Wireless - General	
Set up the wireless related information belo	w.
Enable Smart Connect	OFF
Band	2.4 GHz ~
Network Name (SSID)	LIAO
Hide SSID	• Yes O No
Wireless Mode	Auto 🗸 🗹 big Protection 🖿 Disable 11b
802.11ax / WIFi 6 mode	Enable v If compatibility issue occurs when enabling 802.11ax / WIFi 6 mode, please check: EAQ
WiFi Agile Multiband	Disable 🗸
Target Wake Time	Disable 🗸
Channel bandwidth	20/40 MHz 🗸
Control Channel	Auto V Current Control Channel: 5
Extension Channel	Auto 🗸
Authentication Method	WPA2-Personal v 🕜
WPA Encryption	AES 🗸
WPA Pre-Shared Key	Weak
Group Key Rotation Interval	3600
	Apply

- If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. If not, adjust the channel, channel bandwidth, and wireless mode.
- If you still cannot connect to the router wirelessly, you can reset your router to factory default settings. In the router GUI, click Administration > Restore/Save/Upload Setting and click Restore.

Administration - Restore/Save/Up	load Setting	
This function allows you to save current setti	ngs of ASUS Router to	a file, or load settings from a file.
Factory default	Restore	Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.
Save setting	Save setting	Click on this checkbox if you want to share the contig file for debugging. Since the original password in the contig file will be removed, please do not import the file into your order. Transfer ASUS DDNIS name
Restore setting	Upload	)

#### 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 Controls 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.

Parental Controls - V	Neb & Apps Filters
	Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:
E	<ol> <li>In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.</li> <li>Check the unwanted content categories</li> <li>Click the plus (+) icon to add rule then click apply.</li> <li>If you want to disable the rule temporarily, uncheck the check box in front of rule. <u>Parential Controls FAQ</u></li> </ol>
Web & Apps Filters	OFF

- 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.

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

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

#### Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **4.2 Firmware Restoration** on how to use the Firmware Restoration utility.

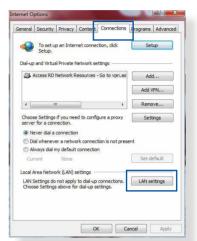
# **Cannot access Web GUI**

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

# A. Disable the proxy server, if enabled.

#### Windows®

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



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

	on on may override man Is, disable automatic (		
Automatically dete	ect settings		
Use automatic cor	figuration script		
Address			
Use a proxy serve dial-up or VPN con	er for your LAN (Thes inections).	e settings	will not apply to
Address:	Port:	80	Advanced
Address,			
	server for local addre	sses	
	server for local addre	sses	

#### **MAC OS**

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

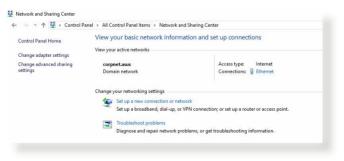
		utomatic uilt-in Ethernet	÷)
_	TCP/IP PPPoE	AppleTalk Pro	kies Ethernet
Bypa	t a proxy server to config FTP Proxy Web Proxy (HTTP) Secure Web Proxy (HTTP) Streaming Proxy (RTSP) SOCKS Proxy Gopher Proxy copher Proxy ss proxy settings for e Hosts & Domains:	ñ	y server y server requires password Set Password
⊻u	se Passive FTP Mode (PAS)	n	(?

**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®

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



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

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

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

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

5. Click **OK** when done.

eneral		
Connection		
IPv4 Connectivit	y: Intern	et
IPv6 Connectivit	y: No network acce	ss
Media State:	Enable	ed
Duration:	03:29:	31
Speed:	1.0 Gb	ps
Details		
Activity		
ictivity ———	Sent — 🦳 — Receive	ed
lotivity ———— Bytes:	Sent — Receive	
Bytes:	and the second s	

tworking Authentication		
mucrorfucduori		
onnect using:		
Intel(R) Ethemet Connection (	2) 1219-V	
	Cont	igure
his connection uses the following it		
QoS Packet Scheduler		^
Internet Protocol Version 4		
Microsoft Network Adapter		
Internet Protocol Version 6	(TCP/IPv6)	
<ul> <li>Link-Layer Topology Discov</li> <li>Link-Layer Topology Discov</li> </ul>		ar v
<	iciy mapper i/o bity	>
Install Uninsta	Prop	erties
Description	nop	
Transmission Control Protocol/Inte		
wide area network protocol that p		on
across diverse interconnected net	works.	
	OK	
	OK	Cancel
	OK	Cancel
	UN	Cancel
rnet Protocol Version 4 (TCP/IPv4)		Cancel
neral Alternate Configuration	Properties	×
neral Alternate Configuration ou can get IP settings assigned autor is capability. Otherwise, you need to	Properties natically if your networ	× k supports
neral Alternate Configuration ou can get IP settings assigned autor is capability. Otherwise, you need to	Properties natically if your networ	× k supports
neral Alternate Configuration ou can get IP settings assigned autor is capability. Otherwise, you need to	Properties natically if your network adm	× k supports
Alternate Configuration ou can get IP settings assigned auton is capability. Otherwise, you need to or the appropriate IP settings.	Properties natically if your network adm	× k supports
eral Alternate Configuration ou can get IP settings assigned autor is capability. Otherwise, you need to or the appropriate IP settings. Obtain an IP address automatical	Properties natically if your network adm	× k supports
Alternate Configuration       ou can get IP settings assigned autom       is capability. Otherwise, you need to       of the appropriate IP settings.       Obtain an IP address automatical       Use the following IP address:	Properties natically if your network adm ask your network adm	× k supports
Use the following IP address:	Properties natically if your network adm ask your network adm	× k supports
Alternate Configuration           ou can get IP settings assigned auton is capability. Otherwise, you need to the appropriate IP settings.           O bean an IP address automatical           Use the following IP address:           Biohert mask:           Default gateway:	Properties hatically if your network address address your network address your network address you have been you h	× k supports
erell Alternate Configuration ou can get IP settings assigned autom is capability. Otherwise, you need to it the appropriate Pertings. © Obtain an IP address automatical O Use the following IP address: IP address: Default gateway: © Obtain DNS server address autom	Properties Properties Properties	× k supports
Alternate Configuration           ou can get IP settings assigned autom is capability. Otherwise, you need to it the appropriate Pretitings.           Image: Contain an IP address automatical Oute the following IP address:           IP address:           Subnet mask:           Default patway:           Othan DNS server address autom           Othat the following IP address:	Properties abtcally if your network adn	× k supports
Alternate Configuration           ou can get IP settings assigned auton is capability. Otherwise, you need to it the appropriate Petitings.           ID do the following IP address:           Dube the following IP address:           Subnet mack:           Default gatewayr:           ID obtain DNS server address auton           O Use the following IP address:           Default gatewayr:           ID obtain DNS server address auton           O Use the following IPS server add           Preferred DNS server:	Properties Properties Properties	× k supports
Alternate Configuration           ou can get IP settings assigned autom is capability. Otherwise, you need to it the appropriate Pretitings.           Image: Contain an IP address automatical Oute the following IP address:           IP address:           Subnet mask:           Default patway:           Othan DNS server address autom           Othat the following IP address:	Properties abtcally if your network adn	× k supports
Alternate Configuration           ou can get IP settings assigned auton is capability. Otherwise, you need to it the appropriate Petitings.           ID do the following IP address:           Dube the following IP address:           Subnet mack:           Default gatewayr:           ID obtain DNS server address auton           O Use the following IP address:           Default gatewayr:           ID obtain DNS server address auton           O Use the following IPS server add           Preferred DNS server:	Properties	× k supports
Alternate Configuration           ou can get JP settings assigned autom is capability. Otherwise, you need to it the appropriate Pretitings.           O Lot an an IP address automatical O Use the following JP address:           P address:           Subnet make:           Default optionaries           O Obtain DNS server address autom Preferred DNS server:           Alternate DNS server:	Properties	k supports inistrator
Alternate Configuration     or can get IP settings assigned autom     is capability. Otherwise, you need to     the appropriate Petitings.     Obtain an IP address automatical     Use the following IP address:     Sobnet make     Default gatoway!     Obtain DNS server address autom     Obtain DNS server:     Alternate DNS server:	Properties	k supports inistrator

## **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. Click **Apply Now** when done.

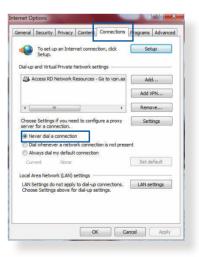
Le	ocation: Automatic	•
	Show: Built-in Ethernet	•
TCP/	IP PPPoE AppleTalk Proxies	Ethernet
Configure IPv4:	Using DHCP	•
IP Address:	192.168.182.103	(Renew DHCP Lease)
Subnet Mask:	255.255.255.0 DHCP Client	
Router:	192.168.182.250	(If required)
DNS Servers:	192.168.128.10	(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:0211:24ff:fe	32:b18e
	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®

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

# **GNU General Public License**

## **Licensing information**

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

# **GNU GENERAL PUBLIC LICENSE**

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

# Preamble

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

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

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

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

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

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations. Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

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

#### Terms & conditions for copying, distribution, & modification

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

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

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

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

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

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

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

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

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

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

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

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

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

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

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

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

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

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

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

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

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

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

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

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

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

#### **NO WARRANTY**

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

# **Safety Notices**

When using this product, always follow the fundamental safety precautions, including, but not limited to the following:



## WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
- Read the operational guidelines and the temperature range provided before using the product.
- Pay particular attention to the personal safety when using this device in airports, hospitals, gas stations and professional garages.
- Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products to reduce the risk of interference.
- Kindly use ASUS products in good reception conditions to minimize the radiation's level.
- Keep the device away from pregnant women and the lower abdomen of the teenager.
- DO NOT use this product if visible defects can be observed or it has been wet or damaged or modified. Seek servicing for assistance.



#### WARNING!

- DO NOT place on uneven or unstable work surfaces.
- DO NOT place or drop objects on the top of the product. Avoid exposing the product to mechanical shock such as crushing, bending, puncturing or shredding.
- DO NOT disassemble, open, microwave, incinerate, paint, or shove any foreign objects into this product.
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- Keep the product away from fire and heat sources.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the product during electrical storms.
- Connect the PoE output circuits of this product exclusively to PoE networks, without routing to external facilities.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- Only use accessories that have been approved by the device manufacturer to work with this model. The use of other types of accessories may invalidate the warranty or violate local regulations and laws, and may pose safety risks. Contact your local retailer for the availablity of authorized accessories.
- Use of this product in a way not recommended in the provided instructions may result in a risk of fire or personal injury.

# **Service and Support**

Visit our multi-language website at https://www.asus.com/support.

