

# Contents

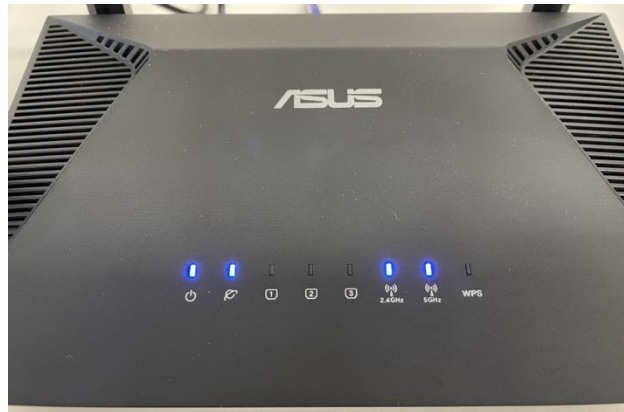
<b>1</b>	<b>Connect Router</b>	<b>2</b>
<b>2</b>	<b>Router Setup</b>	<b>3</b>
<b>1</b>	<b>Router Configuration</b>	<b>3</b>
<b>2</b>	<b>Set new login password</b>	<b>6</b>
<b>3</b>	<b>Optional: Change your Wi-Fi name (SSID) and password</b>	<b>6</b>
<b>4</b>	<b>Advanced settings</b>	<b>7</b>
<b>6</b>	<b>Adding mesh AP by AiMesh (option)</b>	<b>11</b>
<b>7</b>	<b>Appendice</b>	<b>12</b>



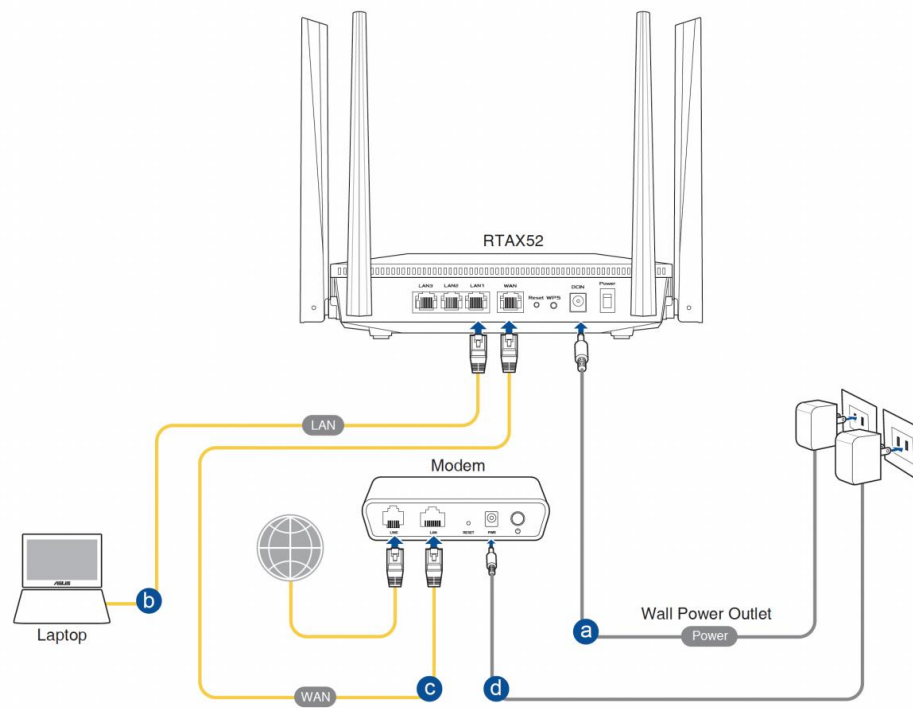
# 1 Connect Router

1.1 Power up the router with the power adapter, wait for all lights to be stable.

1.1.1 The power light and 2.4GHz & 5GHz Wi-Fi lights should be solid on after power on the router.



1.2 Connect the **WAN port** to the correct port (most likely will be **LAN 1/UNI-D1**) of the fibre box (i.e., nbn / OptiComm / RedTrain NTD) via the **Ethernet cable** (Cat5E or above).



## 2 Router Setup

There are two methods to connect with your router:

- **Option one - Ethernet cable connection:** Connect your **laptop/PC** to any of **LAN ports** via **Ethernet cable**.
- **Option two - Wi-Fi Connection:** Connect your **device** (laptop, iPad, or mobile phone) to the router's Wi-Fi.

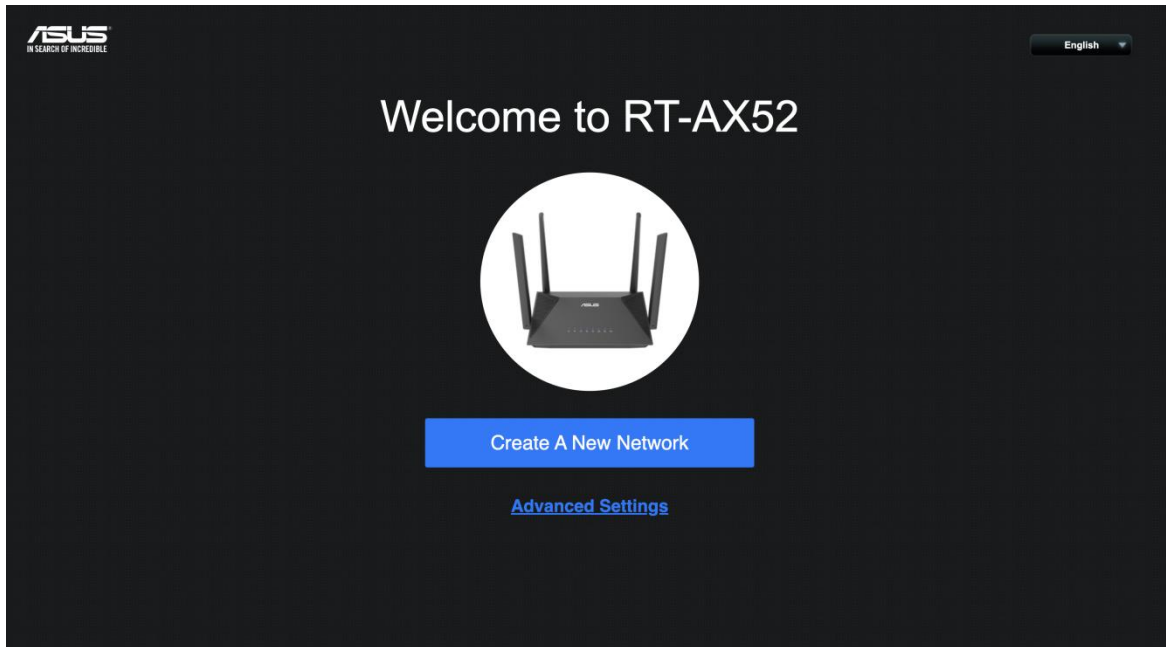
Check the Wi-Fi details:

- Find the **Wi-Fi Setup Card** or the sticker on the bottom of the router.
- You can find the Wi-Fi name (SSID), Wi-Fi password and the router login username and password.

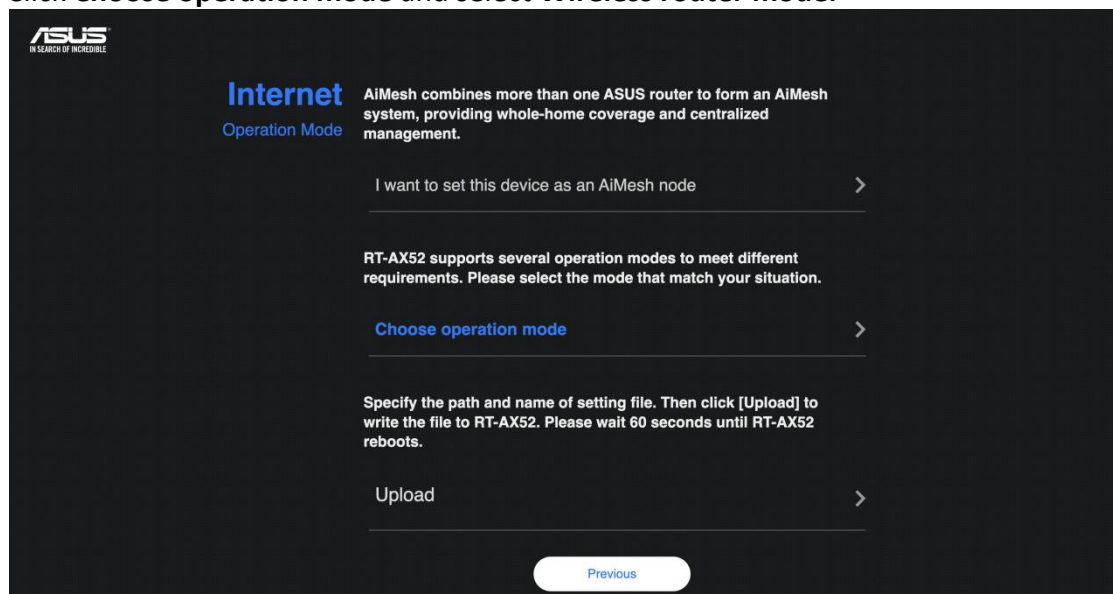


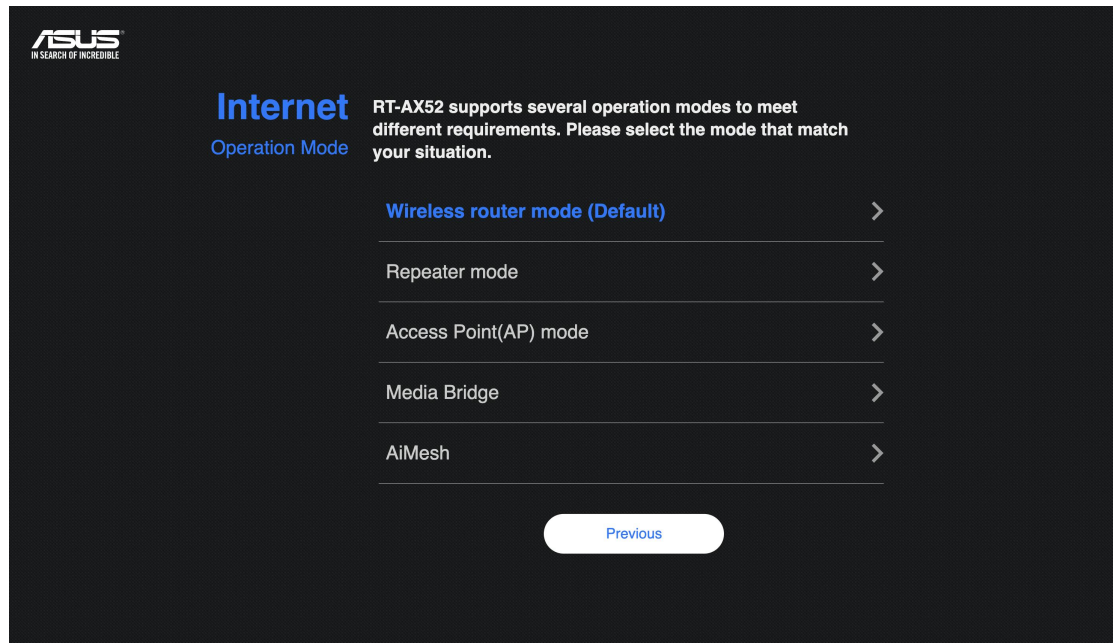
## 1 Router Configuration

Open the Internet browser (e.g., Google Chrome, Safari, etc.) and input <http://192.168.50.1/> in the address bar to visit the router's configuration page. Click Advanced Settings.

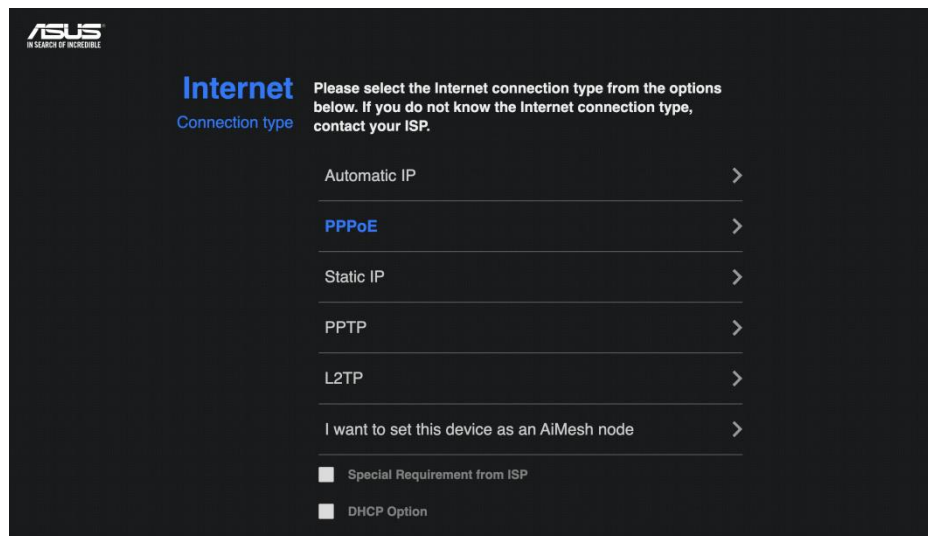


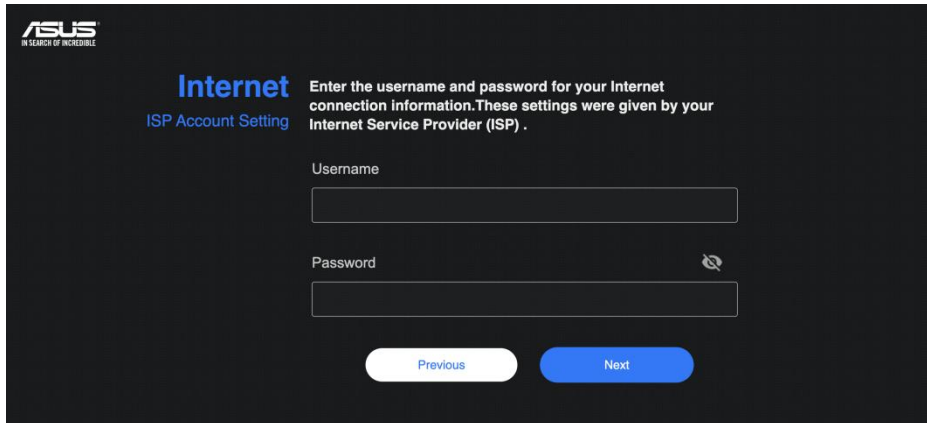
**1.1 Click Choose operation mode and select Wireless router mode.**





- 1.2 Select **PPPoE** and Input the PPPoE username and password provided by the ISP, then click Next.





ASUS  
IN SEARCH OF INCREDIBLE

## Internet

ISP Account Setting

Enter the username and password for your Internet connection information. These settings were given by your Internet Service Provider (ISP).

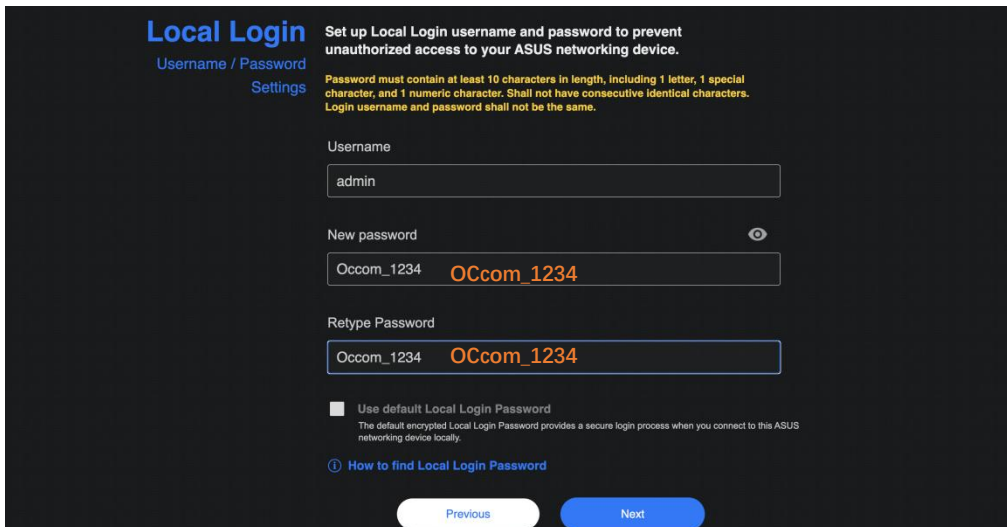
Username

Password

Previous Next

## 2 Set new login password

Input new login username and password as “OCcom\_1234”



## Local Login

Username / Password Settings

Set up Local Login username and password to prevent unauthorized access to your ASUS networking device.

Password must contain at least 10 characters in length, including 1 letter, 1 special character, and 1 numeric character. Shall not have consecutive identical characters. Login username and password shall not be the same.

Username

New password

OCcom\_1234

Retype Password

OCcom\_1234

☐ Use default Local Login Password  
The default encrypted Local Login Password provides a secure login process when you connect to this ASUS networking device locally.

[How to find Local Login Password](#)

Previous Next

## 3 Optional: Change your Wi-Fi name (SSID) and password

- 3.1 Enable **Separate 2.4 GHz and 5GHz**. You can enter your preferred Wi-Fi name and password in this page. Click **Apply** after changing.

**Wireless Settings**

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

2.4 GHz Network Name (SSID)  
 Change Wi-Fi name here

2.4 GHz Wireless Security  
  
Strong Change Wi-Fi password here

5 GHz Network Name (SSID)

5 GHz Wireless Security  
  
Strong

☒ Separate 2.4 GHz and 5 GHz

[How to find WiFi Password](#)

[Previous](#) [Apply](#)

**\*Careful:** Once you change your Wi-Fi name or password, your device needs to reconnect with Wi-Fi by using the new Wi-Fi name and password.

## 4 Advanced settings

### 5.1 Check the PPPoE details

If the router has already been configured and we need to check or modify the PPPoE information, select WAN and modify the information under Account settings.

**WAN Settings**

Basic Config  
 WAN Connection Type:   
 Enable WAN: ☒ Yes ☐ No  
 Enable NAT: ☒ Yes ☐ No  
 Enable UPnP: ☒ Yes ☐ No

WAN IP Setting  
 Get the WAN IP automatically: ☒ Yes ☐ No

WAN DNS Setting  
 Default status: Get the DNS IP from your ISP automatically.  
 Assign a DNS service to improve security, block advertisement and gain faster performance. [Assign](#)  
 DNS Server:   
 Forward local domain queries to upstream DNS: ☒ Yes ☐ No  
 Enable DNS Rebind protection: ☒ Yes ☐ No  
 Prevent client auto DoH:   
 DNS Privacy Protocol:

Account Settings  
 Username:   
 Password:  [Show password](#)  
 PPP Authentication:   
 Disconnect after time of inactivity (in seconds):   
 MTU:   
 MRU:   
 Service Name:   
 Access Concentrator Name:

## 5.2 Enable Remote Access via WAN IP

Administration>System> Remote Access Config, select **Yes** to enable remote access the setting page via WAN IP.

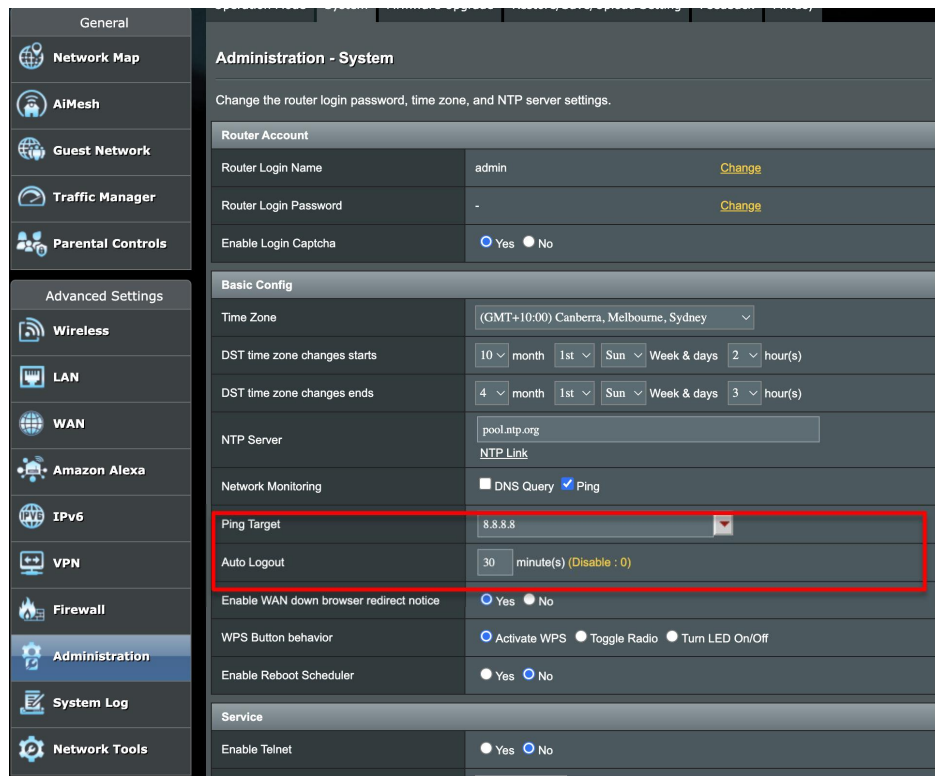
The screenshot shows the 'Remote Access Config' section of a network device's web interface. The left sidebar contains 'Firewall', 'Administration', 'System Log', and 'Network Tools'. The main content area is divided into several sections: 'Service' (with 'Enable Telnet' and 'Enable SSH'), 'Local Access Config' (with 'Authentication Method', 'HTTPS LAN port', and 'Download Certificate'), and 'Remote Access Config'. In the 'Remote Access Config' section, the 'Enable Web Access from WAN' option is highlighted with a red box and is set to 'Yes'. Below it, a note states 'Only HTTPS is supported when accessing the web UI from WAN. FAQ'. The 'HTTPS Port of Web Access from WAN' is set to 8443. The 'Enable Access Restrictions' option is set to 'No'. An 'Apply' button is at the bottom right.

Enable WAN down browser redirect notice	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS Button behavior	<input checked="" type="radio"/> Activate WPS <input type="radio"/> Toggle Radio <input type="radio"/> Turn LED On/Off
Enable Reboot Scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
<b>Service</b>	
Enable Telnet	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable SSH	No
Idle Timeout	20 minute(s) (Disable : 0)
<b>Local Access Config</b>	
Authentication Method	Default
HTTPS LAN port	8443 Access setting page via <a href="https://10.10.9.141:8443">https://10.10.9.141:8443</a> * Please use port 1024-65535.
Download Certificate	<button>Export</button> <button>Renew</button> <a href="#">FAQ</a>
<b>Remote Access Config</b>	
Enable Web Access from WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No Only HTTPS is supported when accessing the web UI from WAN. <a href="#">FAQ</a>
HTTPS Port of Web Access from WAN	8443 <a href="https://10.10.9.141:8443">Access setting page via https://10.10.9.141:8443</a>
Enable Access Restrictions	<input type="radio"/> Yes <input checked="" type="radio"/> No
<button>Apply</button>	

## 5.3 Enable Remote ping

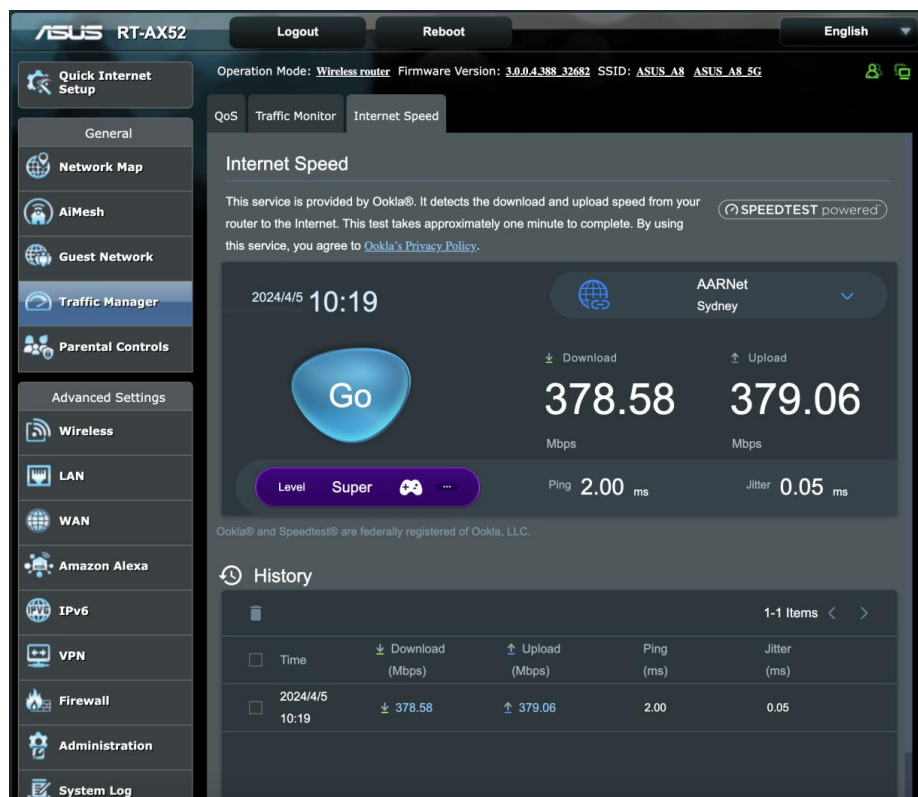
Administration>System>Basic Config, enable **Ping** under Network Monitoring to enable remote ping.





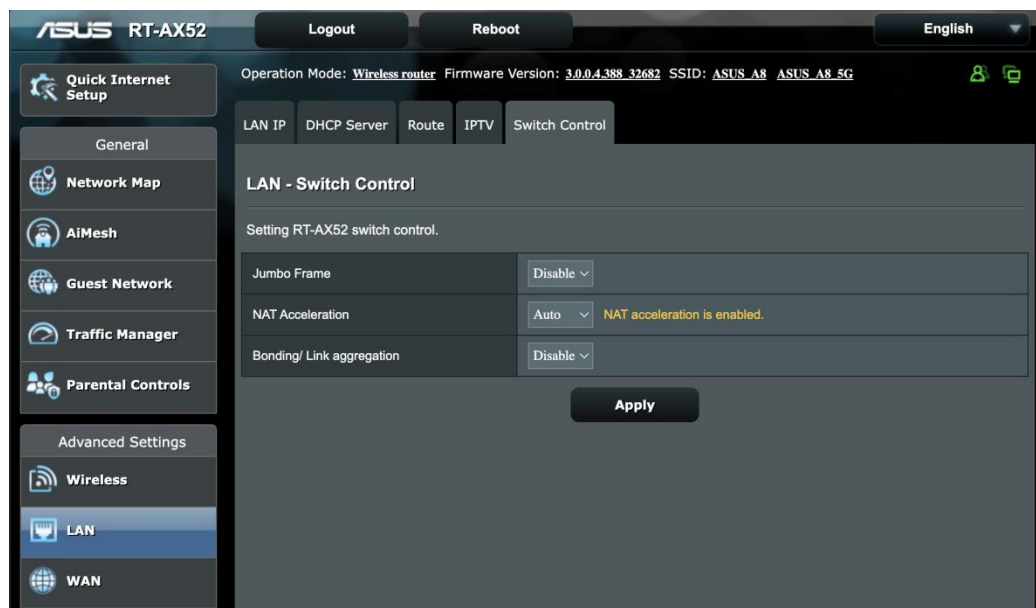
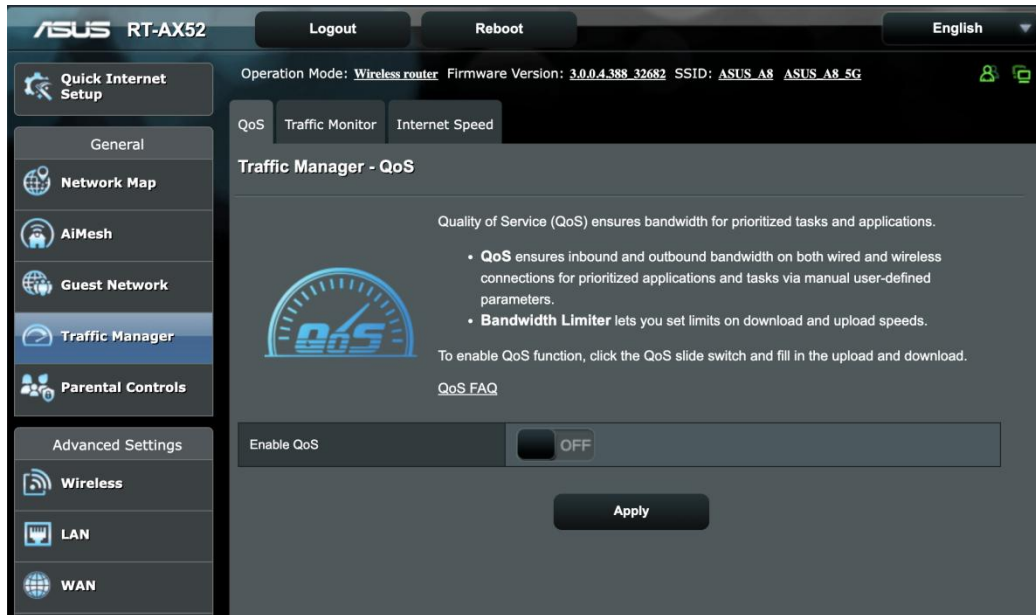
## 5.4 CPE Build-in Speed Test

Click **Internet Speed** under **Traffic Manager**, and then click **Go** to run the speed test.



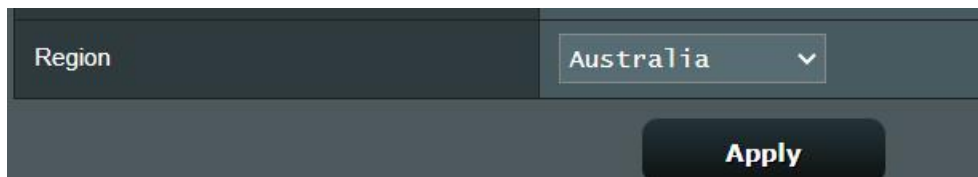
## 5.5 QoS and NAT acceleration

Ensure any form of QoS function remains OFF, and NAT acceleration function is enabled (default):





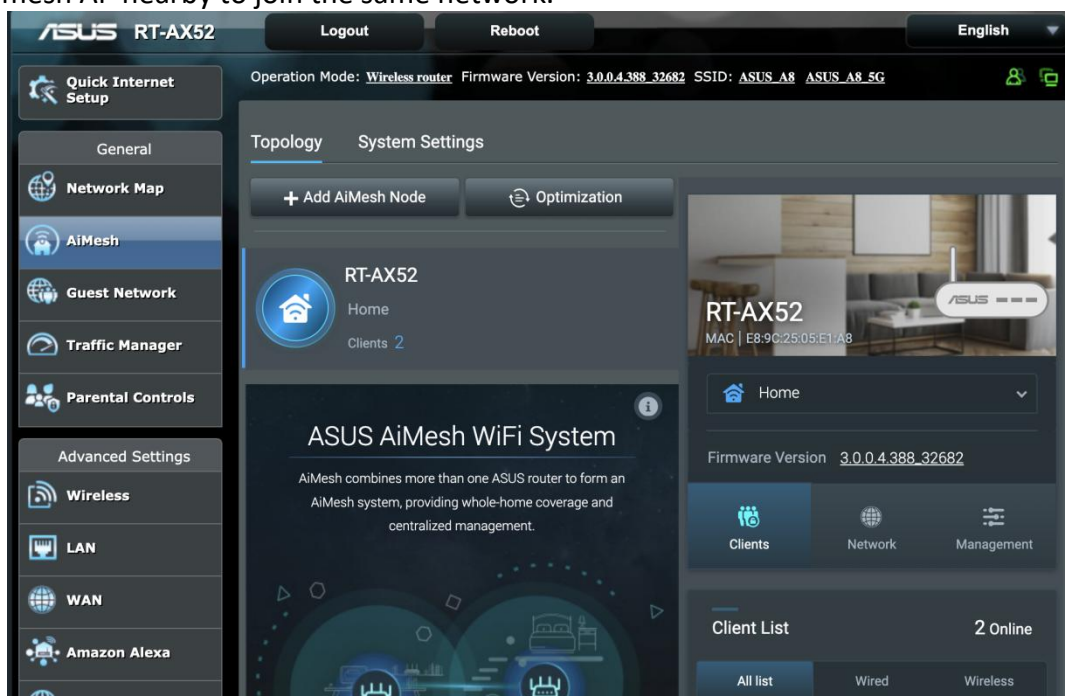
Keep Smart connect OFF

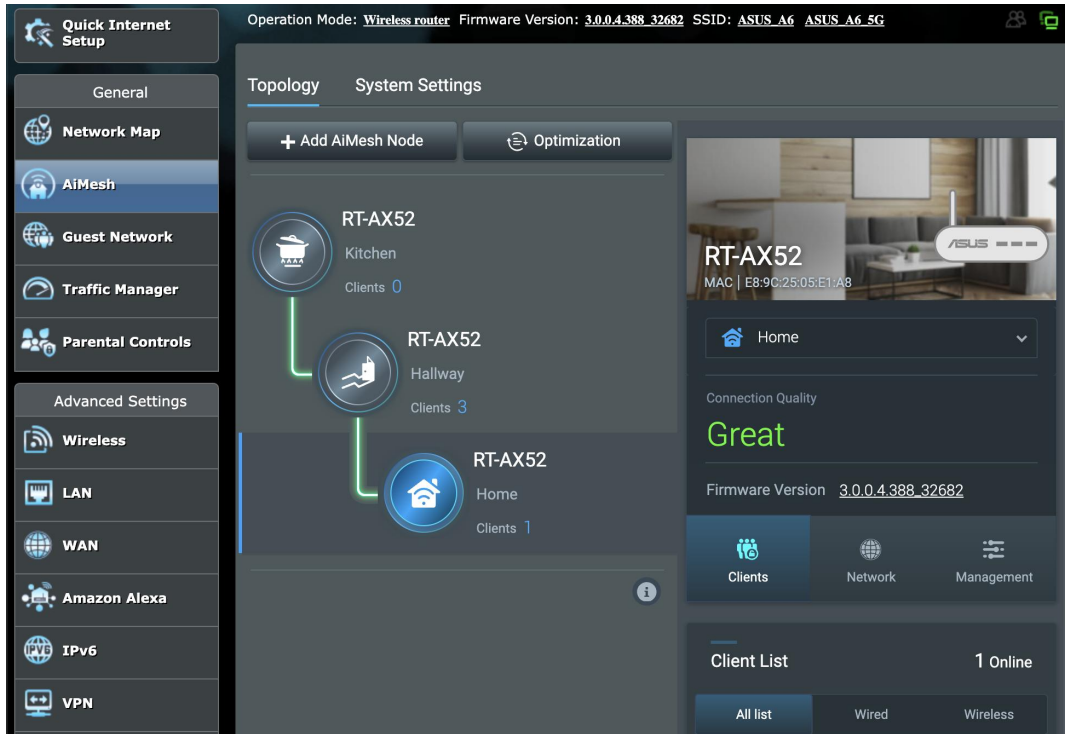
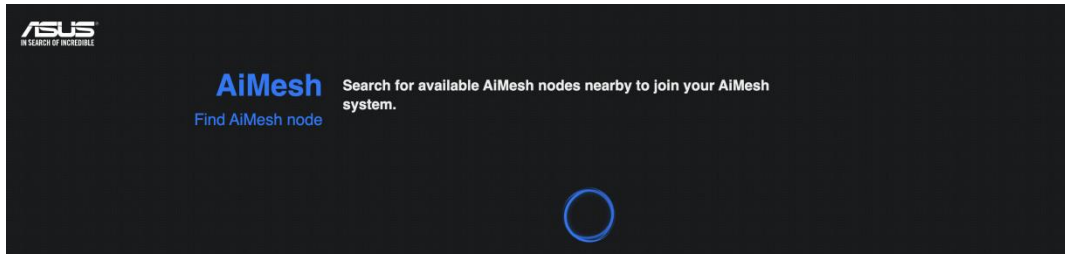


Change the Region in wifi setting: Australia

## 6 Adding mesh AP by AiMesh (option)

Power on the AP, and then click **+Add AiMesh Node** under **AiMesh** within the configuration page of the primary router, then the primary router will search for available Aimesh AP nearby to join the same network.





## 7 Appendice

Some official videos about Asus RT-AX52

- Asus support reference:

<https://www.asus.com/au/support/faq/1011715/>

[https://www.youtube.com/playlist?list=PLS\\_9rTR7el1ZmINE0Hxr-6lag3BspTzBI](https://www.youtube.com/playlist?list=PLS_9rTR7el1ZmINE0Hxr-6lag3BspTzBI)