



User Guide

300Mbps Wireless N 4G LTE Router

MB110-4G

CE Mark Warning



This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

OPERATING FREQUENCY (the maximum transmitted power)

2400 MHz - 2483.5 MHz (20dBm)

WCDMA: B1/B8 (24dBm+1/-3dBm)

LTE: B1/B3/B7/B8/B20/B28/B38/B40 (23dBm±2dBm)

EU Declaration of Conformity

Mercusys hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU Declaration of Conformity may be found at <http://www.mercusys.com/en/ce>.

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

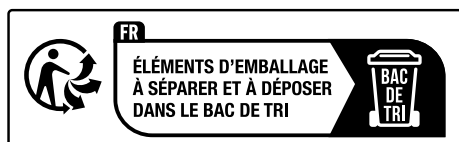
The device complies with RF specifications when the device is used at 20 cm from your body.

UK Declaration of Conformity



Mercusys hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at <https://www.mercusys.com/support/ukca/>



Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

限用物質含有情況標示聲明書

設備名稱：300Mbps Wireless N 4G LTE Router			型號（型式）：MB110-4G			
Equipment name			Type designation (Type)			
單元 Unit	限用物質及其化學符號					
	Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電 源 供 應 器	—	○	○	○	○	○
其 他 及 其 配 件	—	○	○	○	○	○

備考 1. “超出 0.1 wt %” 及 “超出 0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值

Note 1: “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考 2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2: “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考 3. “—” 係指該項限用物質為排除項目。

Note 3: The “—” indicates that the restricted substance corresponds to the exemption.



Продукт сертифіковано згідно з правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.



Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.
- Operating Temperature: 0°C~40°C (32°F~104°F)
- This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please

use this product with care and operate at your own risk.

Explanation of the symbols on the product label

The product label is at the bottom of the device. Symbols may vary from products.

Symbol	Explanation
	Class II equipment
	Class II equipment with functional earthing
	Alternating current
	DC voltage
	Polarity of output terminals
	Indoor use only
	Dangerous voltage
	Caution, risk of electric shock
	Energy efficiency Marking
	Protective earth
	Earth
	Frame or chassis
	Functional earthing
	Caution, hot surface
	Caution
	Operator's manual

	Stand-by
	"ON"/"OFF" (push-push)
	Fuse
	Fuse is used in neutral N
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.
	Caution, avoid listening at high volume levels for long periods
	Disconnection, all power plugs
m	Switch of mini-gap construction
μ	Switch of micro-gap construction (for US version) Switch of micro-gap / micro-disconnection construction (for other versions except US)
ε	Switch without contact gap (Semiconductor switching device)

Contents

Conventions	01
Chapter 1. Introduction	02
1. 1. Product Overview.....	02
1. 2. Panel Layout.....	02
1. 2. 1.Side Panel.....	02
1. 2. 2.Rear and Side Panels.....	03
Chapter 2. Quick Setup	05
2. 1. Position Your Router	05
2. 2. Plug & Play with SIM Card	05
2. 3. Set Up the Router in Wireless Router Mode.....	06
2. 4. Install External Antennas.....	07
Chapter 3. Log In to the Router.....	08
Chapter 4 Mercusys Cloud Service.....	09
4.1 Register a Mercusys ID	09
4.2 Manage the User Mercusys IDs	10
4. 1. 1. Add Mercusys ID to Manage the Router	10
4. 1. 2. Remove Mercusys ID(s) from Managing the Router	11
Chapter 5. Network Security	12
5. 1. Protect the Network from Cyber Attacks	12
5. 2. Service Filtering	12
5. 3. Access Control	13
5. 4. IP & MAC Binding	15
5. 5. Set up IPv6 Firewall Rules	16
Chapter 6. Parental Controls	18
Chapter 7. SMS	21
7. 1. View Messages.....	21
7. 2. Edit and Send a New Message	21
7. 3. View Sent Messages.....	22
7. 4. View Drafts	22

7. 5.	SMS Settings	22
-------	--------------------	----

Chapter 8. Guest Network. 24

8. 1.	Create a Network for Guests	24
8. 2.	Customize Guest Network Options.....	24

Chapter 9. NAT Forwarding. 26

9. 1.	Translate Address and Port by ALG.....	26
9. 2.	Share Local Resources in the Internet by Virtual Server.....	27
9. 3.	Open Ports Dynamically by Port Triggering.....	29
9. 4.	Make Applications Free from Port Restriction by DMZ	30
9. 5.	Make Xbox Online Games Run Smoothly by UPnP	31

Chapter 10. Specify Your Network Settings 32

10. 1.	Create a Connection Profile.....	32
10. 2.	Upgrade Your ISP Information.....	33
10. 3.	PIN Management	34
10. 4.	Data Settings	35
10. 5.	LAN Settings	36
10. 5. 1.	Change the LAN IP Address	36
10. 5. 2.	Use the 4G LTE Router as a DHCP Server	36
10. 5. 3.	Reserve LAN IP Addresses	37
10. 6.	Wireless Settings.....	38
10. 6. 1.	Specify Basic Wireless Settings	38
10. 6. 2.	Use WPS for Wireless Connection	40
10. 6. 3.	Schedule Your Wireless Function	41
10. 6. 4.	View Wireless Information	42
10. 6. 5.	Advanced Wireless Settings.....	43
10. 7.	Set Up a Dynamic DNS Service Account	44
10. 8.	Create Static Routes.....	45
10. 9.	IPv6 Tunnel	47
10. 10.	USSD.....	47

Chapter 11. Administrate Your Network 49

11. 1.	Set System Time	49
11. 2.	Control LEDs	50
11. 3.	Test Internet Connectivity	51
11. 4.	Update the Firmware.....	51
11. 4. 1.	Online Upgrade.....	52

11. 4. 2. Local Upgrade.....	52
11. 5. Back up and Restore Configuration Settings	52
11. 6. Reboot the Router	53
11. 7. Change the Administrator Account.....	54
11. 8. Local Management	55
11. 9. Remote Management.....	56
11. 10. ICMP Ping	57
11. 11. System Log.....	57
11. 12. CWMP.....	59
FAQ	61

Conventions

This guide is a complement to Quick Installation Guide. The Quick Installation Guide instructs you on quick internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

Features available in this router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

More Info

Specifications and the latest software can be found at the product page at the official website <http://www.mercusys.com>.

The Quick Installation Guide can be found where you find this guide or inside the package of the router.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput, wireless coverage, and number of connected devices are not guaranteed and will vary as a result of network conditions, client limitations, and environmental factors, including building materials, obstacles, volume and density of traffic, and client location.

Chapter 1. Introduction

1.1. Product Overview

The 4G LTE Router shares the latest generation 4G LTE network with multiple Wi-Fi devices, anywhere you want.

Working as a 4G router, the MB110-4G uses 4G LTE technology to achieve super fast speeds up to 150 Mbps download and 50 Mbps upload. It can also share a Wi-Fi network with maximum speed of 300 Mbps on 2.4 GHz for gaming, streaming, and more.

1.2. Panel Layout

1.2.1. Side Panel



The router's LEDs are located on the side panel. You can check the router's working status by following the LED Explanation table.

LED	Status	Indication
	Blinking Green	The router is starting up, upgrading firmware, or establishing WPS connection.
	Solid Green	The router is working properly.
	Solid Orange	Wi-Fi is off.
	Off	Power is off.

LED	Status	Indication
	On	Device is connected.
	Blinking	Device is connecting.
	Off	No device is connected.
	On	Indicates the signal strength received from the mobile internet network. More lit LEDs signify a better signal strength.
	Off	There is no mobile internet signal.

1.2.2. Rear and Side Panels



The following items are located on the rear and bottom panels.

Item	Description
4G/3G External Antenna Ports	Connect external antennas (if any) to strengthen the LTE network.
WPS/RESET Button	Press and hold this button for more than 5 seconds to reset the router. Press for 1 second to use the WPS function.
Ethernet Port 1	LAN port only. Used to connect a local device.
Ethernet Port 2	LAN/WAN port. By default, this port is used as the LAN port to connect a local device. When the router is set to Wireless Router mode, it can be used as the WAN port to connect the DSL/cable Modem or Ethernet outlet. To change to this mode, refer to <u>Set Up the Router in Wireless Router Mode</u> .

Item	Description
POWER Socket	Connect the power adapter. Please use the power adapter provided with this router.
Nano SIM Card Slot	Insert the nano SIM card.

Chapter 2. Quick Setup

2. 1. Position Your Router

With the router, you can access your network from anywhere within the wireless network coverage. However, the wireless signal strength and coverage varies depending on the actual environment where your router is in. Many obstacles may limit the range of the wireless signal, for example, concrete structures, thickness and number of walls.

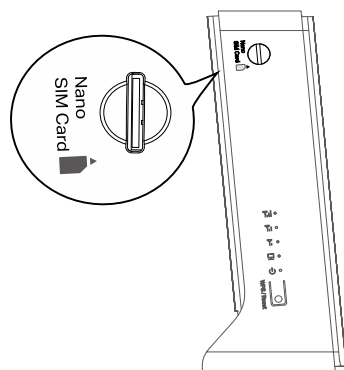
For your security and best Wi-Fi performance, please:

- Do not locate the router in the place where it will be exposed to moisture or excessive heat.
- Keep away from strong electromagnetic radiation source and electromagnetic-sensitive devices.
- Place the router in a location where it can be connected to the various devices as well as to a power source.
- Place the router in a location where it can receive a strong mobile internet signal.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.

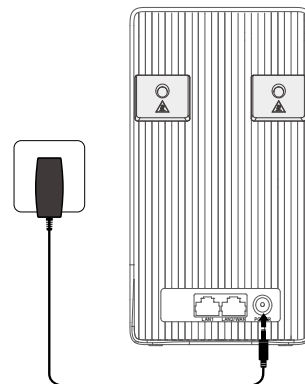
2. 2. Plug & Play with SIM Card

The router support two operation modes: 3G/4G Router mode and Wireless Router mode. By default, it works in 3G/4G Router mode. You can insert a SIM card to share the internet immediately.

Step 1



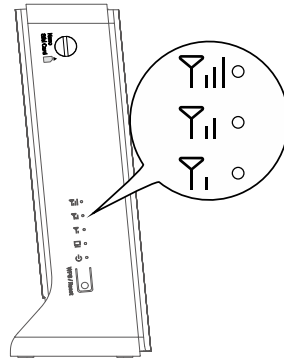
Step 2



1. Insert your Nano SIM card into the slot until you hear a click.

2. Connect the power adapter to the router.
3. Wait until the LED turns on. Your router is connected to the internet successfully.

Note: For better internet connection, make sure 2 or 3 bars of the LED are lit. Otherwise, try relocating the router to a spot that may receive a stronger mobile network signal, such as near a window.



4. Enjoy the Internet!

- **Wired**

Connect your computer to the router via an Ethernet cable.

- **Wireless**

Connect your computer to the router wirelessly. The default wireless network name (SSID) and password are printed on the label at the bottom of the router.

Note: If you want to customize router settings, log in to the web management page (<http://mwlogin.net>), and go to Quick Setup to complete the initial configuration.

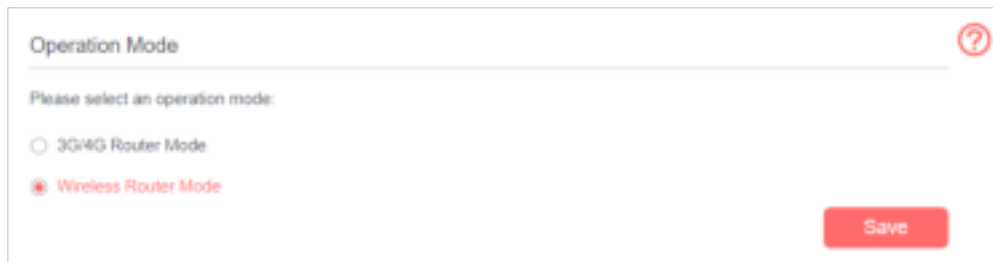
2.3. Set Up the Router in Wireless Router Mode

The router support two operation modes: 3G/4G Router Mode and Wireless Router mode. If you already have a modem or your internet comes via an Ethernet outlet, you can set up the router as a regular wireless router to share the internet.

1. Connect your router's **Ethernet Port 2** to the modem or Ethernet outlet.
2. Visit <http://mwlogin.net>, and log in with password you set for the router.
3. Go to **Advanced > Operation Mode** page.
4. Select the **Wireless Router Mode** option and save the settings.
5. Go to Quick Setup and follow the step-by-step instructions to complete the setup.

Tip:

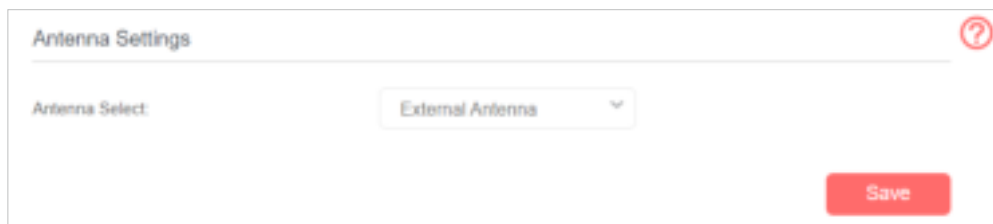
In wireless router mode, you can use 3G/4G network as a backup solution for internet access. With **3G/4G Backup** enabled, your router will connect to the 3G/4G network in case the original network service fails. To enable or disable **3G/4G Backup**, go to **Advanced > Network > Internet**.



2. 4. Install External Antennas

If you have external antennas, you can install them to strengthen the LTE Network.

1. Open the back cover.
2. Connect your external antennas.
3. Log in to the web page (<http://mwlogin.net>), then go to **Advanced > Wireless > Antenna Settings** to select external antennas.



Note:

External antennas are not provided. If you want to buy ones to strengthen the LTE Network, please check the recommended specifications below:

4G Antennas	
Connector	SMA Male Connector
Frequency Range	Includes 698-960 MHz&1710-2170 MHz&2300-2700 MHz

Chapter 3. Log In to the Router

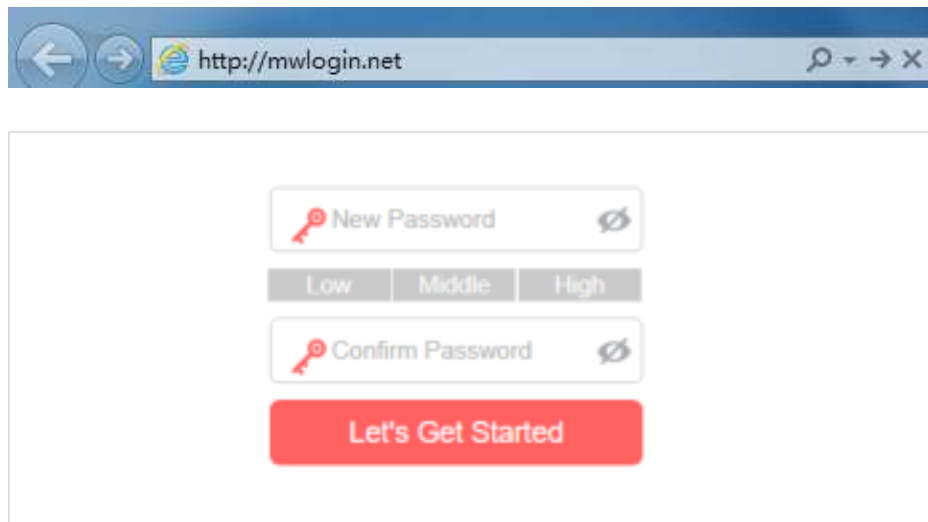
With the web-based utility, it is easy to configure and manage the router. The web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft the Internet Explorer, Mozilla Firefox or Apple Safari.

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your computer.
2. Visit <http://mwlogin.net>. Create a password for future logins.

Note:

If the login window does not appear, please refer to the **FAQ** section.



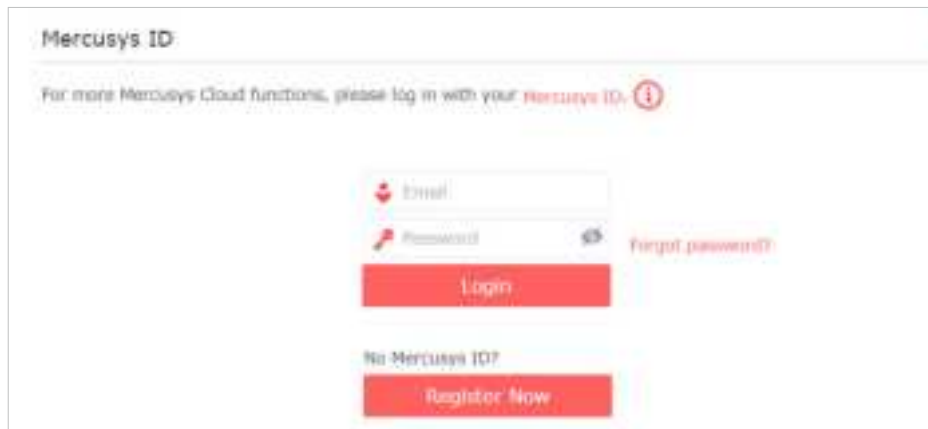
Chapter 4 Mercusys Cloud Service

Mercusys Cloud service lets you remotely monitor your network in real-time, access and manage your Mercusys devices from the Internet at anytime and anywhere.

4.1 Register a Mercusys ID

When you log in after initial setup, the web page will ask whether you need Mercusys Cloud service. You can also access the Mercusys Cloud settings as follows:

1. Visit **<http://mwlogin.net>**, and log in with the password you set for the router.
2. Go to **Basic > Mercusys Cloud**.
3. Click **Register Now** and follow the instructions to register a Mercusys ID.



4. After activating your Mercusys ID, come back to the Mercusys ID page to log in. The Mercusys ID used to log in to the router for the first time will be automatically bound as an **Admin**.

The screenshot displays the Mercusys Cloud Service web interface. It is divided into three main sections:

- Account Information:** Contains fields for 'Email' and 'Password', each with a red eye icon for toggling visibility.
- Device Information:** Shows the 'Model' as 'MR3020' and the 'Status' as 'Being managed by [email]'. A red 'Unbind' button is located to the right.
- Bound Accounts:** Features a table with columns for ID, Email, Binding Date, and Role. Above the table are 'Bind' and 'Unbind' buttons. The table contains one entry with ID '1', Email '[email]', Binding Date '11/02/2022', and Role 'Admin'.

ID	Email	Binding Date	Role
1	[email]	11/02/2022	Admin

4.2 Manage the User Mercusys IDs

The Mercusys ID used to log in to the router for the first time will be automatically bound as the **Admin** account.

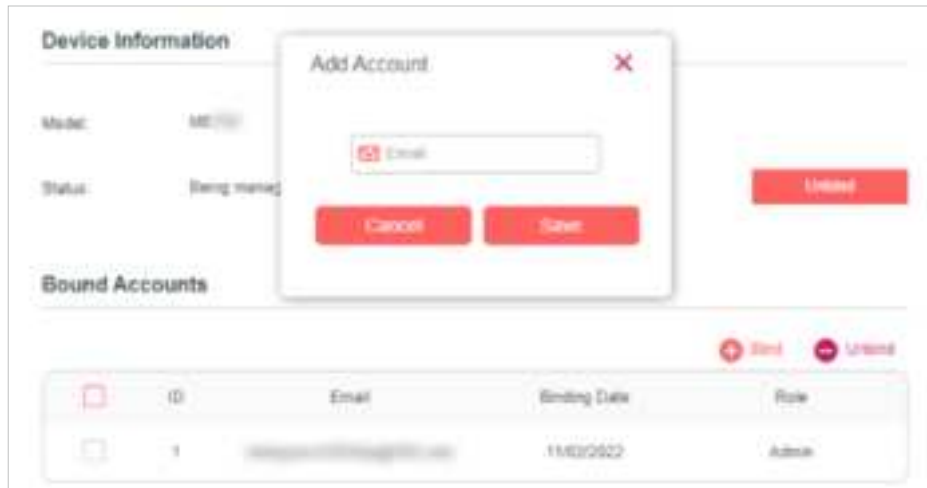
An admin account can add or remove other Mercusys IDs to or from the same router as **User** accounts.

All accounts can monitor and manage the router locally or remotely, but **User** accounts cannot:

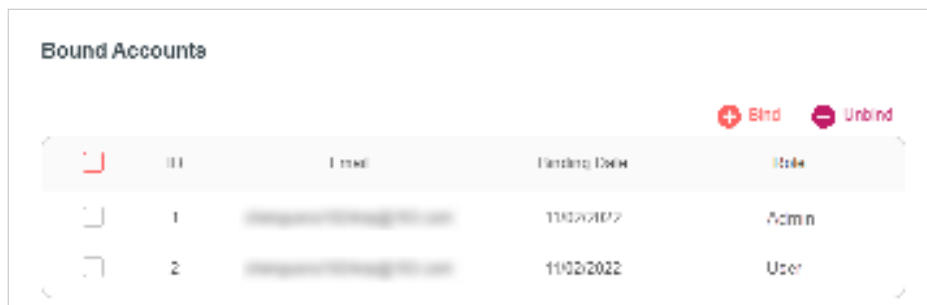
- Reset the router to its factory default settings either on the web management page or in the Mercusys app.
- Add/remove other Mercusys IDs to/from the router.

4.1.1. Add Mercusys ID to Manage the Router

1. Visit <http://mwlogin.net>, and log in with your Mercusys ID.
2. Go to **Settings > Mercusys ID**, and focus on the **Bound Accounts** section.
3. Click **Bind**, enter another Mercusys ID as needed and save the settings.

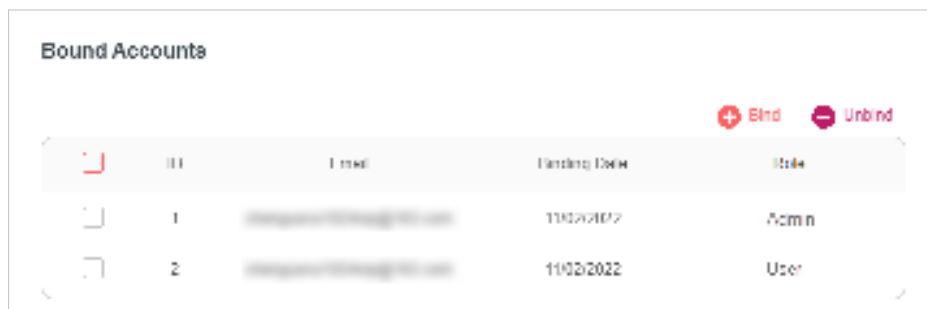


4. The new Mercusys ID will be displayed in the Bound Accounts table as a **User**.



4. 1. 2. Remove Mercusys ID(s) from Managing the Router

1. Visit <http://mwlogin.net>, and log in with your Mercusys ID.
2. Go to **Settings > Mercusys ID**, and focus on the **Bound Accounts** section.
3. Tick the checkbox(es) of the Mercusys ID(s) you want to remove and click **Unbind**.



Chapter 5. Network Security

5. 1. Protect the Network from Cyber Attacks

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it's recommended to keep the default settings.

Follow the steps below to configure Firewall.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Security > Firewall**.



3. Enable **IPv4 SPI Firewall**.

5. 2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, even block internet access completely.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Security > Service Filtering** and enable **Service Filtering**.

3. Click **Add**.

Service Filtering

Service Filtering ☒

Filtering List

ID	Service Type	Port	IP Address	Status	Enable
1	Any(ALL)	1 (14553)	65535 (146032)	Any(ALL)	☒

Service Type: Any(ALL)

Protocol: TCP/UDP

Starting Port: 1 (14553)

Ending Port: 65535 (146032)

Service Type: Any(ALL)

Filter Service For: ☐ Single IP Address ☐ IP Address Range ☒ All IP Addresses

Cancel Save

4. Select a service type from the drop-down list and the following four fields will be auto-populated. Select **Custom** when your desired service type is not listed, and enter the information manually.
5. Specify the IP address(es) that this filtering rule will apply to.
6. Click **Save**.

5.3. Access Control

Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

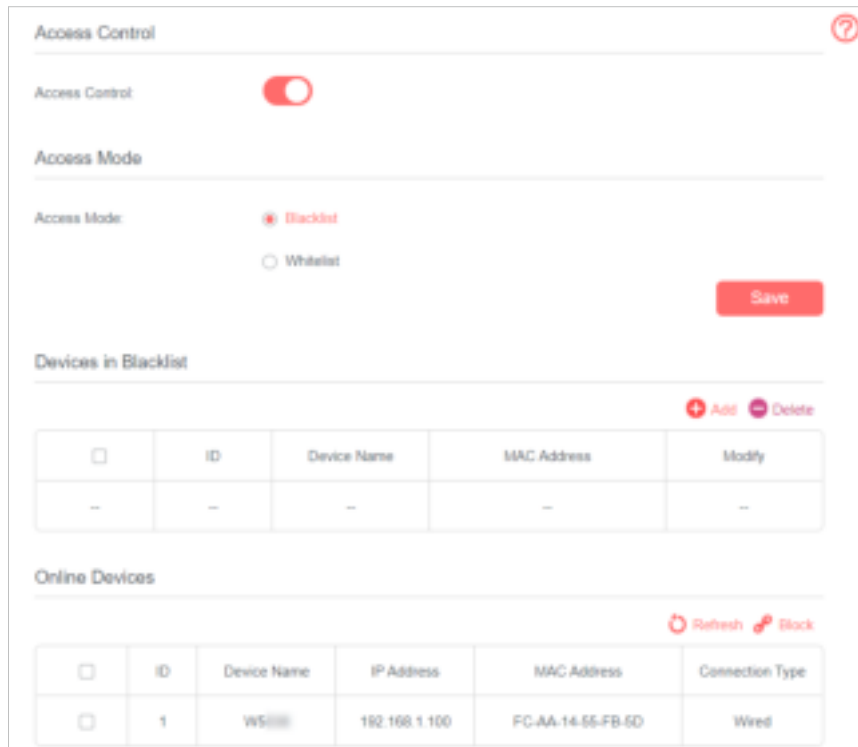
I want to:

Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Security > Access Control** and enable **Access Control**.
3. Select the access mode to either block (recommended) or allow the device(s) in the list.

To block specific device(s)



The image shows a web interface for 'Access Control'. At the top, there's a toggle switch for 'Access Control' which is turned on. Below it, the 'Access Mode' is set to 'Blacklist' (indicated by a red dot) and 'Whitelist' (indicated by a grey dot). A red 'Save' button is on the right. Below this, there's a section for 'Devices in Blacklist' with a table that has columns for ID, Device Name, MAC Address, and Modify. Above the table are '+ Add' and '- Delete' buttons. Below the table is a section for 'Online Devices' with a table that has columns for ID, Device Name, IP Address, MAC Address, and Connection Type. Above the table are 'Refresh' and 'Block' buttons. The 'Online Devices' table has one row with ID 1, Device Name WS1000, IP Address 192.168.1.100, MAC Address FC-AA-14-55-FB-6D, and Connection Type Wired.

Access Control

Access Control ☒

Access Mode

Access Mode: ☒ Blacklist ☐ Whitelist

Save

Devices in Blacklist

+ Add - Delete

☐	ID	Device Name	MAC Address	Modify
☐	--	--	--	--

Online Devices

Refresh Block

☐	ID	Device Name	IP Address	MAC Address	Connection Type
☐	1	WS1000	192.168.1.100	FC-AA-14-55-FB-6D	Wired

- 1) Select **Blacklist** and click **Save**.
- 2) Select the device(s) to be blocked in the **Online Devices** table.
- 3) Click **Block** above the **Online Devices** table. The selected devices will be added to **Devices in Blacklist** automatically.

To allow specific device(s)

Access Control

Access Control: ☒

Access Mode:

Access Mode: ☐ Blacklist ☒ Whitelist

Save

Devices in Whitelist

ID	Device Name	MAC Address	Modify
1	WH000	FC-AA-14-55-FB-5D	

Online Devices

ID	Device Name	IP Address	MAC Address	Connection Type
1	WH000	192.168.1.100	FC-AA-14-55-FB-5D	Wired

- 1) Select **Whitelist** and click **Save**.
- 2) Click **Add**.
- 3) Click **Scan** and select the device that you want to add in the whitelist, then the **Device Name** and **MAC Address** will be automatically filled in. Or enter the **Device Name** and **MAC Address** manually.
- 4) Click **Save**.

Done!

Now you can block or allow specific client devices to access your network (via wired or wireless) using the **Blacklist** or **Whitelist**.

5. 4. IP & MAC Binding

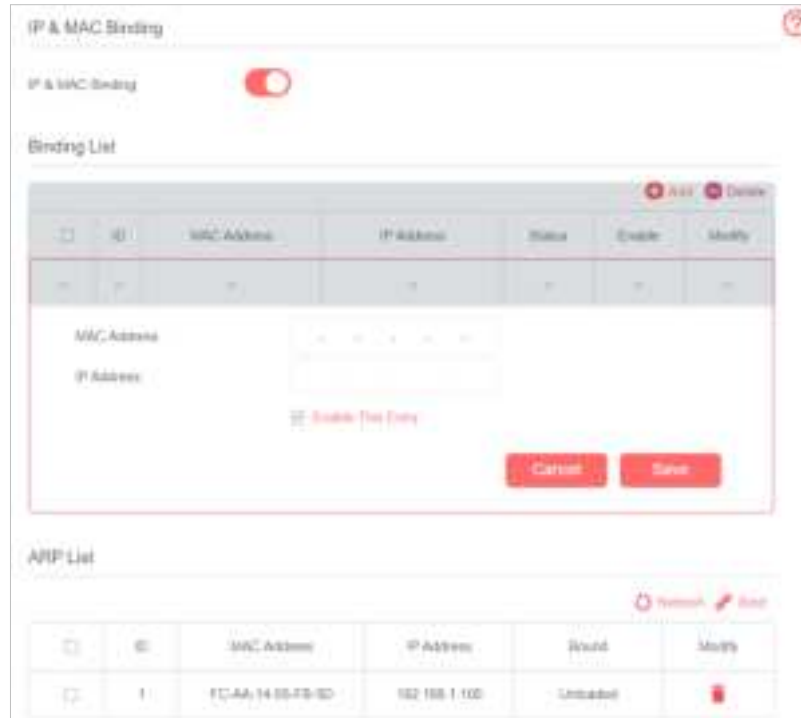
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and other ARP attacks.

How can I do that?

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Security > IP & MAC Binding** and enable **IP & MAC Binding**.



3. Bind your device(s) according to your needs.

To bind the connected device(s)

- 1) Select the device(s) to be bound in the **ARP List**.
- 2) Click **Bind** to add to the **Binding List**.

To bind the unconnected device

- 1) Click **Add**.
- 2) Enter the **MAC Address** and **IP Address** that you want to bind.
- 3) Select the checkbox to enable the entry and click **Save**.

Done!

Now you don't need to worry about ARP spoofing and other ARP attacks.

5. 5. Set up IPv6 Firewall Rules

IPv6 Firewall protects your IPv6 network by preventing access from the internet. However, when you are hosting a service, such as a file sharing server in your local network, you can choose to allow access to the server from the internet by adding

entries on this page. This feature is available only when you've set up an IPv6 connection.

1. Visit <http://mwlogin.net>, and log in with your Mercusys ID or the password you set for the router.
2. Go to **Advanced > Security > IPv6 Firewall**, and locate the **Inbound Firewall Rules** section.
3. Click **Add**.
4. Select a service from the drop-down list of **Service Type**. The **Port** and **Protocol** will be automatically filled in. It is recommended to keep the default **Port** and **Protocol** if you are unsure about which to use. If the service is not listed, please manually enter the **Service Type**, and specify the **Port** and **Protocol**.

Interface Name: LTE

Internal IP: Scan

Service Type: Scan

Port: (XX or XX-XX, XX=1-65535)

Protocol: ALL

☒ Enable This Entry

Cancel Save

5. Specify a **Service Name** for the rule.
6. In the **Internal IP** field, enter a valid IPv6 address to run the service. You can click **Select from clients**, choose a local host device, and its IPv6 address will be automatically filled in as the Internal IP.
7. Click **SAVE**, and the newly created IPv6 firewall rule will appear in **Inbound Firewall Rules**.

Inbound Firewall Rules

	ID	Service Type	Port	Internal IP	Protocol	Status	Modify
	1	DNS	53	2409:8B55:3124:2162:2409:2:3C17:7315::edw	ALL		

Chapter 6. Parental Controls

I want to:

Control the time of day my children or other home network users are allowed to access the internet and even types of websites they can visit.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access **<https://www.mercusys.com>** and **<https://www.wikipedia.org>** from 18:00 (6PM) to 22:00 (10PM) on weekdays only.

How can I do that?

1. Visit **<http://mwlogin.net>**, and log in with the password you set for the router.
2. Go to **Basic** or **Advanced** > **Parental Controls** and enable **Parental Controls**.

Parental Controls

Parental Controls: ☒

Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

Refresh Add Delete

☐	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
☐	--	--	--	--	--	--	--

Content Restriction

Content Restriction: ☒

Restriction Policy: ☒ Blacklist ☐ Whitelist

+ Add a New Keyword

Save

3. Click **Add**.

ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
	Device Name	MAC Address	Effective Time	Description		

☐ Enable This Entry

4. Click **Scan** and select the device to be controlled. Or enter the **Device Name** and **MAC Address** manually.
5. Click the Clock icon to set the **Effective Time**. Drag the cursor over the appropriate cell(s) and click **OK**.

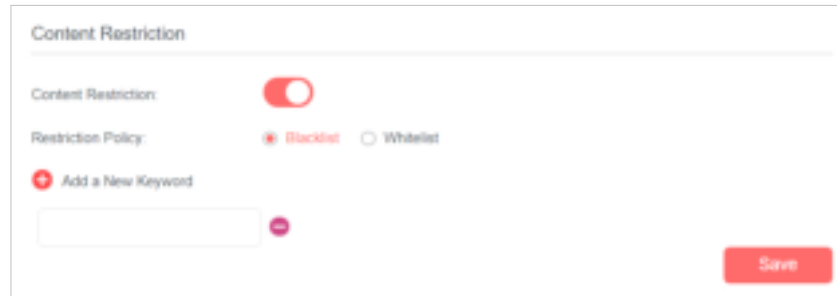
System Time: 01/10/2018 00:10:20

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

☐ Effective Time

6. Enter a **Description** for the entry.
7. Select the checkbox to enable this entry and click **Save**.
8. Select the restriction type.
 - 1) With **Blacklist** selected, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.

- 2) With **Whitelist** selected, the controlled devices can only access websites containing the specified keywords during the Effective Time period.

The screenshot shows a 'Content Restriction' settings window. At the top, the title 'Content Restriction' is displayed. Below it, there is a toggle switch for 'Content Restriction' which is currently turned on. Underneath the toggle, the 'Restriction Policy' is set to 'Blacklist', indicated by a red dot and the word 'Blacklist' in red, while 'Whitelist' is unselected, indicated by a grey dot and the word 'Whitelist' in grey. Below the policy selection, there is a red circular button with a plus sign and the text 'Add a New Keyword'. Under this button is a text input field. To the right of the input field is a small red circular button with a minus sign. In the bottom right corner of the window is a red rectangular button with the text 'Save'.

9. Click **Add a New Keyword**. You can add up to 200 keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.
 - 1) Enter a web address (e.g. **www.mercusys.com**) or a web address keyword (e.g. **wikipedia**) to only allow or block access to the websites containing that keyword.
 - 2) If you wish to block all internet browsing access, do not add any keyword to the **Whitelist**.
10. Enter the keywords or websites you want to add and click **Save**.

Done!

Now you can control your children's internet access according to your needs.

Chapter 7. SMS

7.1. View Messages

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > SMS > Inbox** page.



3. Click the envelope icon to unfold and read the content of the message.

7.2. Edit and Send a New Message

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > SMS > New Message** page.

3. Enter the receiver's phone number in the **Phone Number** field.
4. Enter your message in the **Message** field.

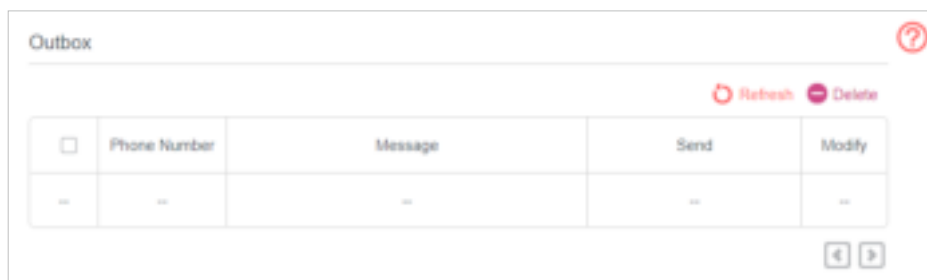
Tips:

You can enter up to 160 letters or numbers, and any exceeding characters will be sent in the next message. You can send up to 5 messages each time.

- Click **Send** to send the message or click **Save** to save the message to the Drafts.

7.3. View Sent Messages

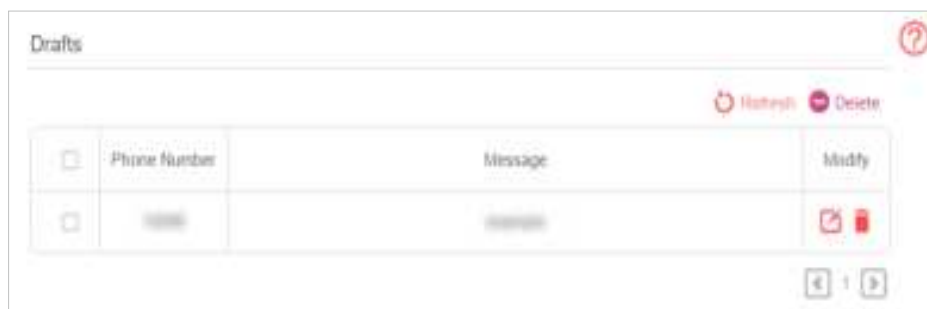
- Visit <http://mwlogin.net>, and log in with the password you set for the router.
- Go to **Advanced > SMS > Outbox** page. All the messages you sent are listed in the **Outbox** table.



	Phone Number	Message	Send	Modify
☐	--	--	--	--

7.4. View Drafts

- Visit <http://mwlogin.net>, and log in with the password you set for the router.
- Go to **Advanced > SMS > Drafts** page. All the unsent messages are listed in the **Drafts** table.



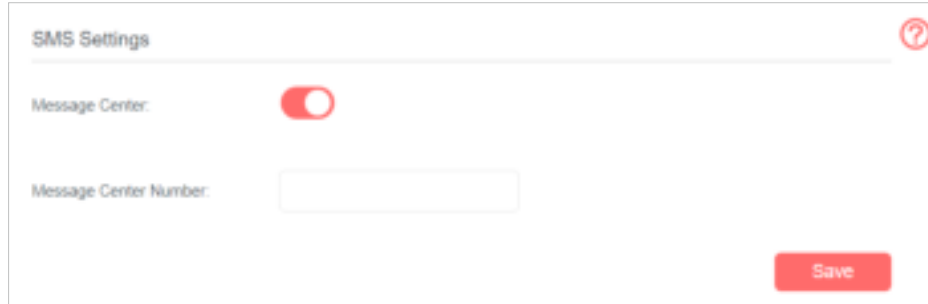
	Phone Number	Message	Modify
☐	--	--	--

7.5. SMS Settings

SMS Settings allows you to configure the Message Center. When the Message Center is enabled, you can change the Message Center Number via which messages will be sent. It is not recommended to change it for a wrong message center number will affect the SMS function of the router.

- Visit <http://mwlogin.net>, and log in with the password you set for the router.

2. Go to **Advanced > SMS > SMS Settings** page and enable **Message Center**.



The screenshot shows the 'SMS Settings' page. At the top, there is a header 'SMS Settings' with a red question mark icon to its right. Below the header, there is a section for 'Message Center' with a red toggle switch that is currently turned on. Below this, there is a label 'Message Center Number:' followed by an empty text input field. At the bottom right of the form, there is a red 'Save' button.

3. The **Message Center Number** is auto-populated. Change it according to your needs.

Chapter 8. Guest Network

This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security, privacy, and fluency.

8.1. Create a Network for Guests

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced** > **Guest Network**. Locate the **Wireless** section.
3. Create a guest network.
 - 1) Enable the guest network.
 - 2) Customize the SSID. Don't select **Hide SSID** unless you want your guests to manually input the SSID for guest network access.
 - 3) Set **Security** to **WPA/WPA2 Personal**, keep the default **Version** and **Encryption** values, and customize your own password.

The screenshot shows the 'Guest Network' configuration interface. It has two sections for wireless networks: '2.4GHz Wireless' and '5GHz Wireless'. Each section has a checkbox for 'Enable Guest Network' (both are checked), a text input for 'Network Name (SSID)' (both are 'MLGuest-0001'), and a checkbox for 'Hide SSID' (both are unchecked). Below these is a 'Security' section with two radio buttons: 'No Security' (selected) and 'Set Password' (unselected). A red 'Save' button is at the bottom right.

4. Click **Save**. Now your guests can access your guest network using the SSID and password you set!

Tips:

To view guest network information, go to **Advanced** > **Status** and locate the **Guest Network** section.

8.2. Customize Guest Network Options

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced** > **Guest Network**. Locate the **Settings** section.

3. Customize guest network options according to your needs.



Guest Settings

☒ Allow Guests to Access Each Other

☐ Allow Guests to Access My Local Network

☐ Enable QoS for Guest Network

Save

- **Allow Guests to Access Each Other**

Select this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors, Samba, Ping, and FTP.

- **Allow Guests to Access My Local Network**

Select this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors, Samba, Ping, and FTP.

- **Enable QoS for Guest Network**

Select this checkbox if you want to assign the upstream and downstream bandwidths for the guest network. This option is available only when BandwidthControl is enabled on the **Advanced > QoS page**.

4. Click **Save**. Now you can ensure network security, privacy, and fluency!

Chapter 9. NAT Forwarding

Router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external host cannot initiatively communicate with the specified device in the local network.

With forwarding feature the router can penetrate the isolation of NAT and allows the external hosts on the internet to initiatively communicate with the devices in the local network, thus to realize some special functions.

The router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPnP and DMZ.

9. 1. Translate Address and Port by ALG

ALG (Application Layer Gateway) allows customized NAT (Network Address Translation) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols: FTP, TFTP, H323 etc. Enabling ALG is recommended.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > NAT Forwarding > ALG**.

Note: It is recommended to keep the default settings.

ALG	
PPTP Pass-through:	☒ Enable
L2TP Pass-through:	☒ Enable
IPSec Pass-through:	☒ Enable
FTP ALG:	☒ Enable
TFTP ALG:	☒ Enable
H323 ALG:	☒ Enable
SIP ALG:	☒ Enable
RTSP ALG:	☒ Enable

Save

- **PPTP Pass-through:** If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the router.

- **L2TP Pass-through:** If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- **IPSec Pass-through:** If enabled, it allows IPSec (Internet Protocol Security) to be tunneled through an IP network and passed through the router. IPSec uses cryptographic security services to ensure private and secure communications over IP networks.
- **FTP ALG:** If enabled, it allows FTP (File Transfer Protocol) clients and servers to transfer data via NAT.
- **TFTP ALG:** If enabled, it allows TFTP (Trivial File Transfer Protocol) clients and servers to transfer data via NAT.
- **H323 ALG:** If enabled, it allows Microsoft NetMeeting clients to communicate via NAT.
- **SIP ALG:** If enabled, it allows clients communicate with SIP (Session Initiation Protocol) servers via NAT.
- **RTSP ALG:** If enabled, it allows RTSP (Real-Time Stream Protocol) clients and servers to transfer data via NAT.

9.2. Share Local Resources in the Internet by Virtual Server

When you build up a server in the local network and want to share it on the internet, Virtual Server can realize the service and provide it to the internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the internet.

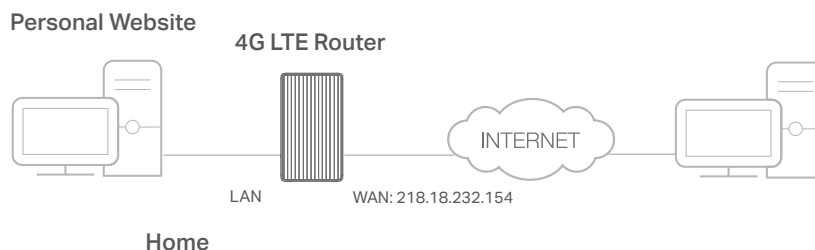
Virtual server can be used for setting up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before the configuration.

I want to:

Share my personal website I've built in local network with my friends through the internet.

For example, the personal website has been built in my home PC (192.168.1.100). I hope that my friends in the internet can visit my website in some way. The PC is connected to

the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit <http://mwlogin.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > Virtual Servers**, click **Add**.

Virtual Servers

ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMF, Virtual Server will not take effect. Service Type: HTTP View Existing Applications External Port: 80 (XX,XX or 300) Internal IP: 192.168.1.100 Internal Port: 80 (XX or Blank, 1-65535) Protocol: TCP ☐ Enable This Entry Cancel Save							

4. Click **View Existing Applications**, and choose **HTTP**. The external port, internal port and protocol will be auto-populated. Enter the PC's IP address 192.168.1.100 in the **Internal IP** field.
5. Click **Save** to save the settings.

Note:

1. It is recommended to keep the default settings of **Internal Port** and **Protocol** if you are not clear about which port and protocol to use.
2. If the service you want to use is not in the **Service Type**, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
3. You can add multiple virtual server rules if you want to provide several services in a router. Please note that the **External Port** cannot be overlapped.

Done!

Users in the internet can enter **http:// WAN IP** (in this example, enter **http:// 218.18.232.154**) to visit your personal website.

Note:

1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN by DDNS, go to **Set Up a Dynamic DNS Service Account** for more information. Then you can use **http://domain name** to visit the website.
2. If you have changed the default **External Port**, you should use **http://WAN IP: External Port** or **http:// domain name: External Port** to visit the website.

9.3. Open Ports Dynamically by Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs and video players. Common applications include MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the port triggering rules:

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced > NAT Forwarding > Port Triggering** and click **Add**.

Port Triggering

Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
MSN Gaming Zone	47024	ALL	2300-2400, 25500-26000	ALL		

View Existing Applications

Application: MSN Gaming Zone

Triggering Port: 47024 (XX, 1-65535)

Triggering Protocol: ALL

External Port: 2300-2400, 25500-26000 (XX or XX-XX, 1-65535, at most 5 ports)

External Protocol: ALL

☒ Enable This Entry

Cancel Save

3. Click **View Existing Applications**, and select the desired application. The triggering port and protocol, the external port and protocol will be auto-populated. Here we take application **MSN Gaming Zone** as an example.
4. Click **Save** to make the settings take effect.

Tips:

1. You can add multiple port triggering rules according to your network need.
2. If the application you need is not listed in the **Existing Applications** list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into **External Port** field according to the format the page displays.

9.4. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, like IP camera and database software, you can set the PC to be a DMZ host.

Note:

DMZ is more applicable in the situation that users are not clear about which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazard. If DMZ is not in use, please disable it in time.

I want to:

Make the home PC join the internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can log in normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ with all ports opened.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit <http://mwlogin.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > DMZ** and select the checkbox to enable DMZ.

4. Enter the IP address 192.168.1.100 in the **DMZ Host IP Address** field.
5. Click **Save** to save the settings.

Done!

The configuration is completed. You've set your PC to a DMZ host and now you can

make a team to game with other players.

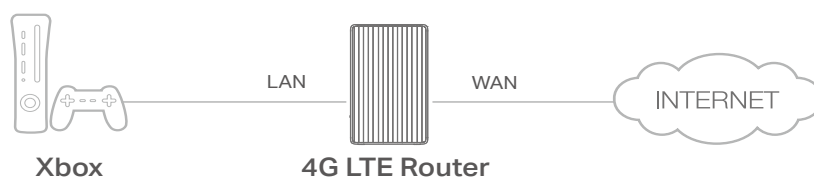
9.5. Make Xbox Online Games Run Smoothly by UPnP

UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other, realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

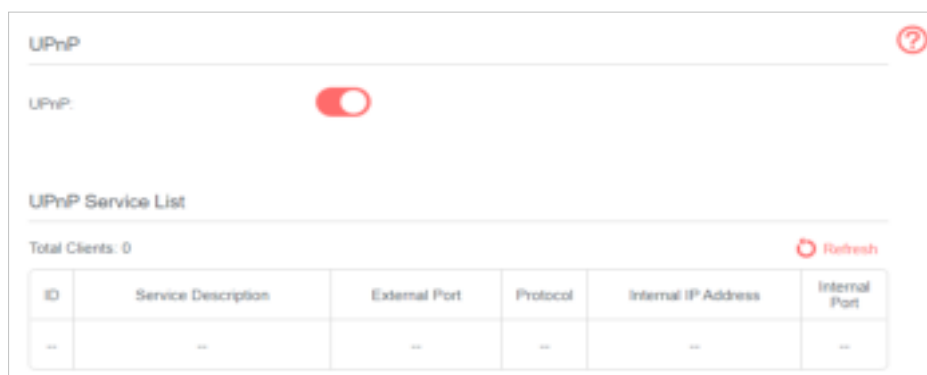
1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send requests to the router to open the corresponding ports, allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router;
2. Go to **Advanced > NAT Forwarding > UPnP** and toggle on or off according to your needs.



Chapter 10. Specify Your Network Settings

10. 1. Create a Connection Profile

If your ISP settings are not detected by the router, you can create an internet connection profile by following the steps below:

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > Internet** page.

WAN Interface

Internet Status: Disconnected

Mobile Data: On

Data Roaming: Off

NAT: On

Network Mode: 4G Preferred

Band: Auto

Dial-up Settings:

Network Search: Auto

Profile Name:

PDP Type: IPv4

APN:

Username:

Password:

Authentication Type: None

[Create Profile](#) Click this button to create a new dial-up profile. Up to 8 profiles can be added.

Delete Save

3. Click **Create Profile**.
4. Specify the **Profile Name**, **Username** and **Password**. Select the **PDP Type**, **APN Type** and **Authentication Type** according to your ISP.



The 'Create Profile' dialog box contains the following fields and options:

- Profile Name:** A text input field.
- PDP Type:** A dropdown menu with 'IPv4' selected.
- APN Type:** A dropdown menu with 'Static' selected.
- APN:** A text input field.
- Username:** A text input field.
- Password:** A text input field with a visibility toggle (eye icon).
- Authentication Type:** A dropdown menu with 'None' selected.

At the bottom right, there are two red buttons: 'Cancel' and 'OK'.

5. Click **OK** to make the settings effective and the new profile will be used to set up a new connection.

Tips:

1. You can view all internet connections or edit connections that are set up manually on this page.
2. You can change the **Network Mode** to **4G Only** or **3G Only** according to your needs.

10.2. Upgrade Your ISP Information

If your ISP information is not detected by the router, you can upgrade ISP information by following the steps below:

6. Download the latest ISP upgrade file from the **Support** page at <https://www.mercusys.com> to your computer.
1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > ISP Upgrade**.



The 'ISP Upgrade' dialog box contains the following elements:

- ISP Upgrade** title bar with a close button (X) on the right.
- Instructional text: "If you fail to log-in Internet access after upgrading to the latest version, please contact us."
- Current ISP Version:** 22062001
- New ISP file:** A text input field for the file path.
- Browse** button: A red button to select a file.
- Upgrade** button: A red button to perform the upgrade.

3. Click **Browse** to locate and select the latest file.
4. Click **Upgrade**.

Note:

3. If you fail to dial-up Internet access after upgrading to the latest version, please contact the technical support.
4. If your ISP settings are still not detected after upgrading, refer to **Create a Connection Profile** to add a new internet connection profile.

10.3. PIN Management

PIN (Personal Identification Number) is used to protect the SIM card from embezzlement. PIN Management allows you to easily change the PIN settings of your SIM card as needed.

Follow the steps below to change your PIN settings.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > PIN Management** page.

The screenshot shows the 'PIN Management' web page. It has a title bar 'PIN Management'. Below it, there are four rows of settings: 'SIM Card Status' with the value 'Ready', 'PIN Lock' with a red toggle switch, 'Auto-unlock PIN' with a red toggle switch, and 'PIN' with a text input field. To the right of the PIN input field is a label 'Remaining Attempts: 3'. At the bottom right of the form is a red button labeled 'Save'.

- **SIM Card Status** - Displays the status of your SIM card.
 - **PIN Lock** - Toggle on to enable PIN Lock. Once it is enabled, every time you start the router with this SIM card inserted, you need to enter the PIN.
 - **Auto-unlock PIN** - When the PIN is required upon router restarting or inserting a SIM card, it will be validated automatically, saving you the trouble to enter the PIN each time you start the router or insert a SIM card. If validation failed, you need to enter the PIN on this page.
 - **PIN** - Enter the PIN to unlock the SIM card. It consists of 4-8 digits.
 - **PUK** - PIN Unlocked Key, also known as Personal Unlock Code (PUC), is used to reset a PIN that has been lost or forgotten. The PUK is a SIM-specific code assigned by the service provider. You need to enter the PUK after 3 incorrect login attempts of PIN. Contact your service provider if you do not know the PUK. It consists of 8 digits.
 - **New PIN** - Enter 4-8 digits to reset the PIN of your SIM card.
 - **Remaining Attempts** - Shows how many attempts are left for you to try entering the PIN or PUK. You have only 3 attempts for entering the PIN and 10 attempts for entering the PUK. If you accidentally fail in 3 attempts, the SIM card will be locked and you will be required to enter the PUK that is written on your SIM card.
3. Click **Save** to save the settings.

10.4. Data Settings

Data Settings is used to monitor the data usage of your router in real-time. You can limit your data usage according to your monthly allowance or total allowance and you will receive a warning if your data usage reaches the specified level.

Follow the steps below to monitor your data usage.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > Data Settings** page.

The screenshot shows the 'Data Settings' page. At the top, there's a 'Monthly Limit' field with '0.000 MB' and a 'Correct' button. Below it, a note says 'You can send messages to your carrier for accurate data usage.' The 'Data Limit' toggle is turned on, with a note: 'The router will automatically disconnect from the network when the data usage limit is reached.' The 'Monthly Allowance' field is empty, with a unit selector set to 'MB'. The 'Usage Alert' field is set to '0%'. The 'SMS Alert for Usage' field has a placeholder 'Please enter phone number' and a 'Send Test Message' button, with a note: 'Note: This function may incur SMS charges.' The 'Monthly Data Statistics' toggle is turned on. The 'Start Date' field has '1' entered. A 'Save' button is at the bottom right.

3. Enable **Data Limit** to set total/monthly data allowance and usage alert to prevent data overuse.
4. Enter the allowed amount of total/monthly data in the **Total/Monthly Allowance** field. When data usage exceeds the allowed level, the router will disconnect from the internet and notify you on the **Basic > Network Map** Page.
5. Enter a percentage in the **Usage Alert** field to prevent data overuse. When data usage reaches the alert level, a warning will be shown on the **Basic > Network Map** Page. If you want to want receive the alert on your phone, enter your mobile phone number in the **SMS Alert for Usage** field.
6. Enable **Monthly Data Statistics** to reset data statistics when the next billing cycle starts.
7. Enter the start date of the billing cycle in the **Start Date** field.
8. Click **Save** to save the settings.

10.5. LAN Settings

10.5.1. Change the LAN IP Address

The router is preset with a default LAN IP 192.168.1.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device on your local network or your network requires a specific IP subnet, you can change it.

Follow the steps below to change your IP address.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > LAN Settings** page.



The screenshot shows the 'DHCP Server' configuration page. It includes the following fields and values:

Field	Value
MAC Address	00-0A-EB-13-00-80
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IGMP Snooping	☐ Enable
Second IP	☐ Enable

3. Type in a new **IP Address** as needed.
4. Select the **Subnet Mask** from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. You can configure the router's **Second IP** and **Subnet Mask** for LAN interface through which you can also access the web management page.
6. Leave the rest of the default settings as they are.
7. Click **Save** to make the settings effective.

10.5.2. Use the 4G LTE Router as a DHCP Server

You can configure the router to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the router, you must configure all computers on the LAN to obtain an IP Address automatically.

Follow the steps below to configure DHCP server.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > LAN Settings** page.

The screenshot shows the 'LAN Settings' page with the 'DHCP' section expanded. The 'DHCP' checkbox is checked. Below it, the 'DHCP Server' is set to 'On'. The 'IP Address Pool' is configured with a start address of 192.168.1.100 and an end address of 192.168.1.199. The 'Address Lease Time' is set to 1440 minutes. Other settings like 'DHCP Relay', 'DHCP Snooping', 'DHCP Guard', and 'DHCP Flood Protection' are all set to 'Default'.

3. Select **DHCP** to enable the DHCP function and select **DHCP Server**.
4. Specify the **IP Address Pool**, the start address and end address must be on the same subnet with LAN IP. The router will assign addresses within this specified range to its clients. It is from 192.168.1.100 to 192.168.1.199 by default.
5. Enter a value for the **Address Lease Time**. The **Address Lease Time** is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
6. Keep the rest of the settings as default and click **Save** to make the settings effective.

Note:

1. The router can be configured to work as a **DHCP Relay**. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using **Condition Pool** feature. For example, you can assign IP addresses within the range (192.168.1.50 to 192.168.1.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your actual situation on **Advanced > Network > LAN Settings** page.

10.5.3. Reserve LAN IP Addresses

You can view and add a reserved address for a client. When you specify an IP address for a device on the LAN, that device will always receive the same IP address each time when it accesses the DHCP server. If there are some devices in the LAN that require permanent IP addresses, please configure Address Reservation on the router for the purpose.

Follow the steps below to reserve an IP address for your device.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > LAN Settings** page.
3. Scroll down to locate the **Address Reservation** table and click **Add** to add an address reservation entry for your device.

The screenshot shows the 'Address Reservation' page. At the top, there are '+ Add' and '- Delete' buttons. Below is a table with the following columns: ☐, MAC Address, Reserved IP Address, Group, Status, and Modify. The table is currently empty. Below the table, there is a form with three input fields: 'MAC Address', 'IP Address', and 'Group' (which has 'Default' selected in a dropdown). To the right of the 'MAC Address' field is a red 'Scan' button. Below the 'IP Address' field is a red 'Enable This Entry' checkbox. At the bottom right of the form are red 'Cancel' and 'Save' buttons.

4. Click **Scan** and select the device for which you want to reserve IP address. Then the **MAC Address** and **IP Address** will be automatically filled in. Or enter the **MAC Address** and **IP Address** manually.
5. Specify the IP address which will be reserved by the router.
6. Check to **Enable this entry** and click **Save** to make the settings effective.

10.6. Wireless Settings

10.6.1. Specify Basic Wireless Settings

The router's wireless network name (SSID) and password, and security options are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Basic > Wireless** page.

The screenshot shows the 'Wireless Settings' page. At the top right is a red question mark icon. The '2.4GHz Wireless Network' section has a checked 'Enable' checkbox. Below this are three input fields: 'Network Name (SSID)' with the value 'Mercusys_0909', 'Password' with the value '12345678', and a 'Hide SSID' checkbox. A red 'Save' button is at the bottom right.

- **To enable or disable the wireless function:**

Enable the **Wireless Network 2.4GHz**. If you don't want to use the wireless function, just uncheck the box. If you disable the wireless function, all the wireless settings won't be effective.

➤ **To change the wireless network name (SSID) and wireless password:**

Enter a new SSID. The default SSID is Mercusys_XXXX and the value is case-sensitive.

Note:

If you use a wireless device to change the wireless settings, you will be disconnected when the settings are effective. Please write down the new SSID and password for future use.

➤ **To hide SSID:**

Select Hide SSID, and your SSID will not broadcast. Your SSID won't display when you scan for local wireless network list on your wireless device and you need to manually join the network.

➤ **To change the mode or channel:**

Go to **Advanced > Wireless > Wireless Settings** page.

- **Mode** - Select the desired mode.
 - **802.11n only** - Select only if all of your wireless clients are 802.11n devices.
 - **802.11g/n mixed** - Select if you are using both 802.11g and 802.11n wireless clients.
 - **802.11b/g/n mixed** - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Note:

When 802.11n only mode is selected, only 802.11n wireless stations can connect to the router. It is strongly recommended that you select 802.11bgn mixed, and all of 802.11b, 802.11g, and 802.11n wireless clients can connect to the router.

- **Channel** - Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width** - Select the channel width from the drop-down list. The default setting is **Auto**, which can adjust the channel width for your clients automatically.
- **Transmit Power** - Select either High, Middle, or Low to specify the data transmit power. The default and recommended setting is **High**.

➤ **To change the security option:**

1. Go to **Advanced > Wireless > Wireless Settings** page.
2. Select an option from the **Security** drop-down list. The router provides four options, None, WPA/WPA2 Personal (Recommended), WPA/WPA2 Enterprise, WEP. WPA2

uses the newest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.

10.6.2. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) feature to add a new wireless device to your existing network quickly.

Method 1 Use the WPS Button

Use this method if your client device has a WPS button.

Note:

The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

1. Press the WPS/RESET button on the back panel of the router for 1 second.

Note:

You can also use the Push button on the web management page. Go to **Advanced > Wireless > WPS** page and click the **Start WPS** button on the screen.



2. Press the WPS button of the client device within two minutes.

Method 2 Enter the client device's PIN on the router

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Wireless > WPS** page.
3. Select **Method Two--PIN** and select **Client's PIN** radio button.

A screenshot of a web-based configuration interface for WPS. At the top, 'Method Two--PIN' is selected with a radio button. Below it, 'Router's PIN' and 'Client's PIN' are listed with radio buttons; 'Client's PIN' is selected and highlighted in red. Under 'Client's PIN', there is a text label 'Enter the client's PIN:' followed by an empty text input field. At the bottom left of the form is a red 'Connect' button.

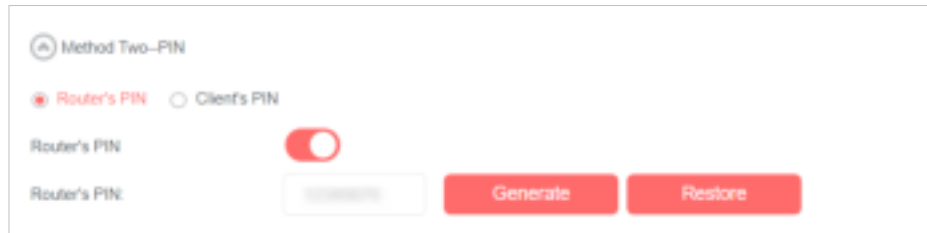
4. Enter the client device's PIN in the field, then click **Connect**.

5. **Connect successfully** will appear on the above screen, which means the client device has successfully connected to the router.

Method 3 Enter the router's PIN on your client device

Use this method if your client device asks for the router's PIN.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Wireless > WPS** page.



3. Take a note of the Current PIN of the router. You can also click the **Generate** button to get a new PIN.
4. On the client device, enter the router's PIN. (The default PIN is also labeled on the bottom of the router.)

10.6.3. Schedule Your Wireless Function

You can automatically turn off your wireless network at time when you do not need the wireless connection.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Wireless > Wireless Schedule** page.
3. Toggle on the button to enable the Wireless Schedule feature.

4. Set the wireless off time. Select **From** and **To** time. You can repeat the schedule every day or just certain days in a week.
5. Click **Save** to make the settings effective.

Note:

1. Please make sure that the time of the router is correct before using this function. For more details, refer to **Set System Time**.
2. The wireless network will be automatically turned on after the time period you set.

10.6.4. View Wireless Information

➤ **To view the detailed wireless network settings:**

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Status** page. You can see the **Wireless** box.

Tips: You can also see the wireless details by clicking the router icon on **Basic > Network Map**.

➤ **To view the detailed information of the connected wireless clients:**

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Wireless > Statistics** page.
3. You can view the detailed information of the wireless clients, including its connected wireless band and security option as well as the packets transmitted.

Tips:

You can also see the wireless details by clicking the wireless clients icon on **Basic > Network Map**.

10.6.5. Advanced Wireless Settings

Advanced wireless settings are for those have a network concept. If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Wireless > Advanced Settings** page.

Setting	Value	Range
Beacon Interval	100	(25-1000)
RTS Threshold	2346	(1-2346)
DTIM Interval	1	(1-255)
Group Key Update Period	0	(0-255)

WMM: ☒ Enable

Short GI: ☒ Enable

AP Isolation: ☐ Enable

Save

- **Beacon Interval** - Enter a value between 25 and 1000 in milliseconds to determine the duration between which beacon packets are broadcasted by the router to synchronize the wireless network. The default is 100 milliseconds.
- **RTS Threshold** - Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.

- **DTIM Interval** - Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as **Beacon Interval**.
- **Group Key Update Period** - Enter the number of seconds (minimum 30) to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- **WMM** - This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode. It is strongly recommended to enable WMM.
- **Short GI** - This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- **AP Isolation** - Select this checkbox to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet. AP isolation is disabled by default.

10.7. Set Up a Dynamic DNS Service Account

DDNS (Dynamic Domain Name System) allows you to assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting the own website, FTP server, or another server behind the router. To begin with, you need to sign up with a Dynamic DNS service provider.

To set up DDNS, please follow the instructions below:

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > Dynamic DNS**.

Dynamic DNS Settings

Service Provider: ☒ Mercusys ☐ Dyndns ☐ NO-IP

DDNS Unavailable

To use our superior Mercusys DDNS service, please [Log in](#) with your Mercusys Cloud account, or choose another service provider.

Current Domain Name:

Domain Name List

	Domain Name	Registered Date	Status	Operation	Modify
☐					

3. Select the DDNS Service Provider (Mercusys, Dyndns or NO-IP).

It is recommended to select Mercusys so that you can enjoy superior DDNS service of Mercusys. To use Mercusys DDNS service, log in with your Mercusys ID and register new domain names.

If you have selected NO-IP or DynDNS, enter the username, password and domain name of your account. If you don't have a DDNS account, register one first.

Tip:

If you want to use a new DDNS account, please log out first, then log in with the new account.

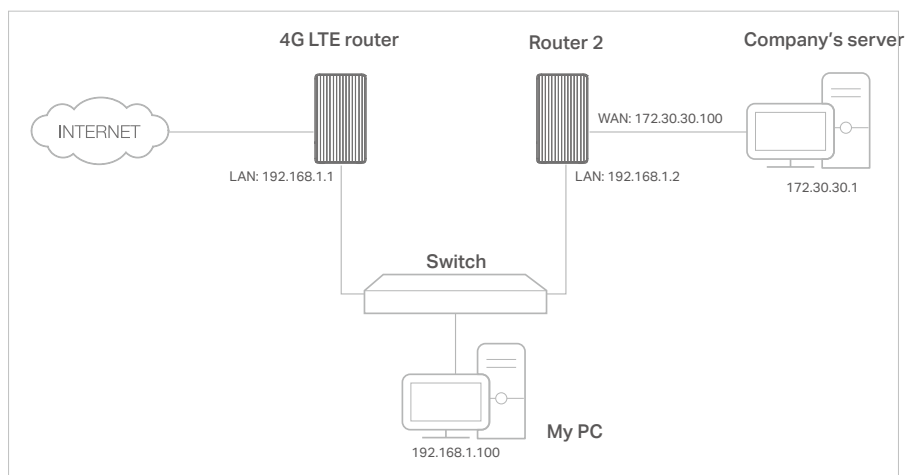
10.8. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured.

I want to:

Visit multiple networks and multiple servers at the same time.

For example, in a small office, my PC can surf the internet, but I also want to visit my company's server. Now I have a switch and another router. I connect the devices as shown in the following figure so that the physical connection between my PC and my company's server is achieved. To surf the internet and visit my company's network at the same time, I need to configure the static routing.



How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable DHCP function of Router 2.
2. Visit <http://mwlogin.net>, and log in with the password you set for the router.

3. Go to **Advanced > Network > Static Routing**.
4. Click **Add** to add a new static routing entry. Finish the settings according to the following explanations:

The screenshot shows a 'Static Route' configuration window. It features a table with the following columns: ID, Network Destination, Subnet Mask, Gateway, Status, and Priority. Below the table, there are input fields for 'Network Destination', 'Subnet Mask', 'Gateway', and 'Interface'. The 'Interface' field is currently set to 'LAN'. At the bottom right of the window, there are 'Cancel' and 'Save' buttons. A red 'Add' button is visible in the top right corner of the window.

- **Network Destination** - The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the router. In the example, the IP address of the company network is the destination IP address, so here enters 172.30.30.1.
- **Subnet Mask** - Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enters 255.255.255.255.
- **Gateway** - The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out the data. In the example, the data packets will be sent to the LAN port of Router 2 and then to the Server, so the gateway should be 192.168.1.2
- **Interface** - Determined by the port that sends out the data packets. In the example, the data is sent to the gateway through the LAN port.

5. Select the checkbox to enable this entry.
6. Click **Save** to save the settings.

Done!

Open a web browser on your PC. Enter the company server's IP address to visit the company network.

10.9. IPv6 Tunnel

IPv6 Tunnel is a transition mechanism that enables IPv6-only hosts to reach IPv4 services or vice versa and allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > IPv6 Tunnel**.
3. Enable **IPv6 Tunnel**.
4. Specify a tunneling mechanism and select a WAN connection.
5. Save the settings.

IPv6 Tunnel

Note: You must reconfigure the IPv6 Tunnel settings every time you reboot the router. Make sure the desired WAN connection is connected before the configuration.

IPv6 Tunnel ☒ Enable

Tunneling Mechanism: 6to4

WAN Connection: No available interface

Save

10.10. USSD

Unstructured Supplementary Service Data (USSD) is a technology that allows you to communicate with your service provider using short codes. It usually consists of a number that starts with * and ends with #. You can query various services on this page.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > USSD**.
3. Enter the USSD request supported by the carrier and click **Send**. You will see the message returned from the carrier in the USSD Result box.

USSD

USSD Request

Send

Cancel

USSD Result

Chapter 11. Administrate Your Network

11.1. Set System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > Time Settings** page.



The screenshot shows the 'System Time' configuration page. It includes a 'Current Time' field displaying '12/12/2022 12:25:22'. Below this is a 'Time Zone' dropdown menu set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'. The 'Date' field shows '12/12/2022' and '(DDMMYY)'. The 'Time' field shows '12:25:22' with hour, minute, and second selectors. There are two 'NTP Server' fields, both set to '0.0.0.0' and marked as '(Optional)'. At the bottom, there are three buttons: 'Get from PC', 'Get from the Internet', and 'Save'.

3. Configure the system time using the following methods :
Manually - Select your time zone and enter your local time.
Get from PC - Click this button if you want to use the current managing PC's time.
Get from the Internet - Click this button if you want to get time from the internet. Make sure your router can access the internet before you select this way to get system time.
4. Click **Save** to make your settings effective.

- After setting the system time, you can set **Daylight Saving** time according to your needs. Tick the checkbox to enable **Daylight Saving**, set the start and end time and then click **Save** to make the settings effective.

11.2. Control LEDs

The router's LEDs indicate router's activities and status. You can turn on or turn off the LEDs either from the web management page.

- Visit <http://mwlogin.net>, and log in with the password you set for the router.
- Go to **Advanced > System Tools > LED Control**.

➤ To turn on/off LEDs

Toggle on or off the LED Status to turn on or off the LEDs.

➤ To set up Night Mode

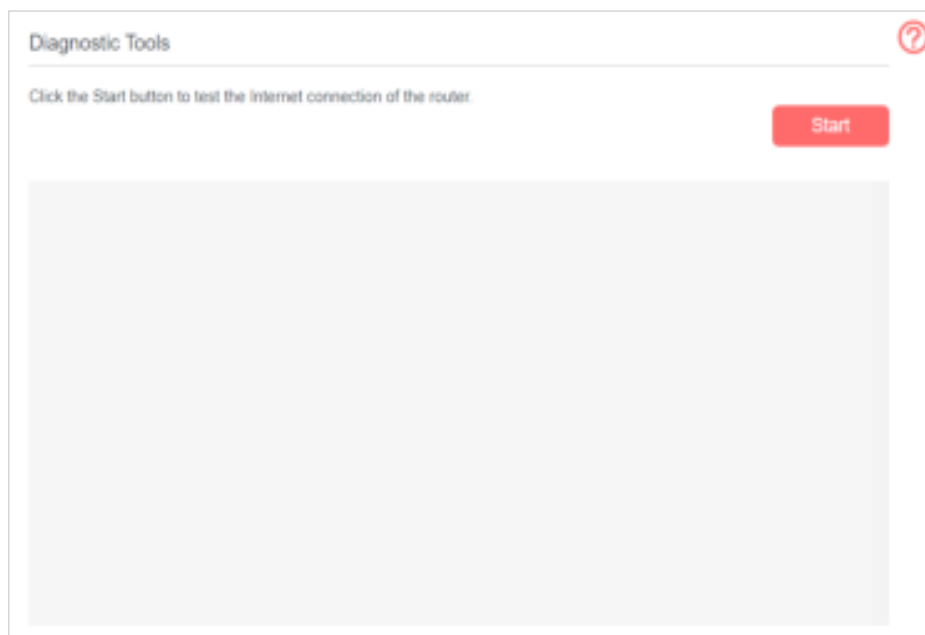
- Enable **Night Mode**.
- Specify a time period in the **Night Mode Period** as needed.

- Click **Save**, and then the LEDs will be off during this period.

11.3. Test Internet Connectivity

After manually set up the internet connection, you need to know the internet connectivity. The router provides a diagnostic tool to help you locate the malfunction.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > Diagnostics** page.



3. Click **Start** to test the internet connectivity and you will see the test result in the gray box.

11.4. Update the Firmware

MERCUSYS is dedicated to improving and enriching the product features, giving you a better network experience.

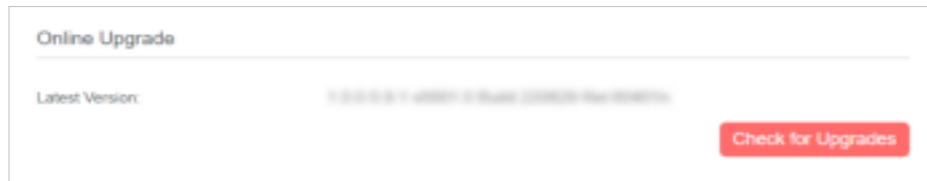
We will inform you through the web management page if there's any update firmware available for your router. Also, the latest firmware will be released at our official website, you can download it from the **Support** page of our website <https://www.mercusys.com> for free.

Note:

1. Make sure that you have a stable connection between the router and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Back up your router configuration before upgrading the firmware.
3. Do NOT turn off the router during the firmware upgrade.

11.4.1. Online Upgrade

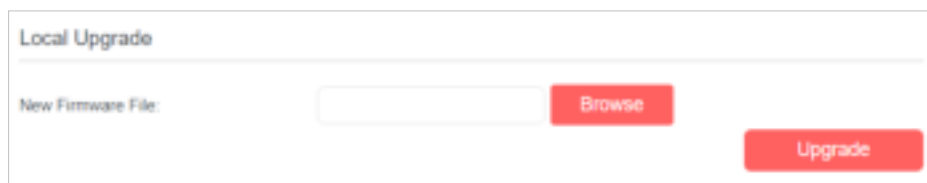
1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > Firmware Upgrade**.
3. Click **Check for Upgrades**.



4. If there's any new firmware, click **Upgrade**. Wait a few moments for the upgrading and rebooting.

11.4.2. Local Upgrade

1. Download the latest firmware file for the router from our website <https://www.mercusys.com>.
2. Visit <http://mwlogin.net>, and log in with the password you set for the router.
3. Go to **Advanced > System Tools > Firmware Upgrade**.
4. Focus on the **Device Information** section. Make sure the downloaded firmware file matches with the **Hardware Version**.
5. Focus on the **Local Upgrade** section. Click **Browse** to locate the downloaded new firmware file, and click **Upgrade**.



6. Wait a few moments for the upgrading and rebooting.

11.5. Back up and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can back up the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the router to the default factory settings.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.

2. Click **Advanced > System Tools > Backup & Restore** page.

The screenshot shows a web interface for Backup & Restore. It is divided into three main sections. The first section, 'Backup', has the instruction 'Save a copy of your current settings.' and a red 'Backup' button. The second section, 'Restore', has the instruction 'Restore previous settings from a saved file', a 'File:' label, a text input field, a red 'Browse' button, and a red 'Restore' button. The third section, 'Factory Default Restore', has the instruction 'Restore all the configuration settings to their default values.' and a red 'Factory Restore' button. A red question mark icon is located in the top right corner of the interface.

- **To back up configuration settings:**
Click **Backup** to save a copy of the current settings to your local computer. A conf. bin file will be stored to your computer.
- **To restore configuration settings:**
 - 1) Click **Browse** to locate the previous backup configuration file, and click **Restore**.
 - 2) Wait for the restoring and then the router will automatically reboot.
- **To reset the router to factory default settings:**
 - 1) Click **Factory Restore** to reset the router.
 - 2) Wait for the resetting and then the router will automatically reboot.

Note:

1. Do not interrupt or turn off the router during the resetting process.
2. We strongly recommend you to back up the current configuration settings before resetting the router.

11.6. Reboot the Router

The Reboot feature cleans the cache to enhance the running performance of the router.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.

2. Go to **Advanced > System Tools > Reboot**.

➤ **To Reboot Manually**

Locate the **Manual Reboot** section and click **Reboot**.

➤ **To Reboot Automatically**

- 1) Locate the **Reboot Schedule** section and check the box to enable **Reboot Schedule**.
- 2) Specify the **Reboot Time** when the router reboots and set **Repeat** to decide how often it reboots.

Note:

Before enabling Reboot Schedule, please make sure your router is connected to the internet, then go to **Advanced > System Tools > Time Settings** and choose Get from the Internet to get the correct network time.

- 3) Click **Save**.

11.7. Change the Administrator Account

Admin account is used to log in to the router's web-based management page. You are required to set the admin account at the first login. You can change it on the web page.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.

2. Go to **Advanced > System Tools> Administration** page. Locate the **Account Management** section.

3. Enter the old password. Enter the new password and enter again to confirm.
4. Click **Save** to make the settings effective.

11.8. Local Management

You can control the local devices' authority to manage the router via the Local Management feature. By default all local connected devices are allowed to manage the router. You can also allow only one device to manage the router.

Follow the steps below to specify the local management.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools> Administration** page. Locate the **Local Management** section.

3. Keep the Port for HTTP as the default settings.
4. Enable **Local Management via HTTPS** to access the router via HTTPS and HTTP, or disable it to access the router only via HTTP.

5. If you only want to allow one specific device to manage the router, enable **Only Allow the Following IP/MAC** and then enter the **IP Address** or **MAC Address** of the device in the IP/MAC Address field.
6. Click **Save** to make the settings effective.

11.9. Remote Management

By default, the remote devices are not allowed to manage the router from the internet. Follow the steps below to allow remote devices to manage the router.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > Administration** page. Locate the **Remote Management** section.

The screenshot shows the 'Remote Management' configuration page. At the top, there's a title bar with a question mark icon. Below it, two toggle switches are visible: 'Remote Management' and 'Remote Management via HTTPS', both currently set to 'Enable'. A note below these toggles states: 'Note: Before using Local/Remote Management via HTTPS, it is recommended to download and install the certificate to your local/remote device first (make sure you install the certificate in the Trusted Root Certification Authorities store). Otherwise, a warning page will appear. In that case, click Trust (or a similar option) to continue.' Below the note, there's a 'Port' field with the value '843'. Underneath that is a label 'Manage This Router via the Address:' followed by an empty text input field. Further down is a section titled 'Client Device Allowed for Remote Management:' with two radio button options: 'Only the Following IP Addresses' (which is selected) and 'All'. Below the 'Only the Following IP Addresses' option is another empty text input field. At the bottom right of the form is a red 'Save' button.

3. Enable **Remote Management**.
4. Enable **Remote Management via HTTPS** to access the router via HTTPS and HTTP, or disable it to access the router only via HTTP.
5. Keep the **Port** as the default setting.
6. If you only want to allow one specific device to manage the router, select **Only the Following IP/MAC Address** and then enter the **IP Address** or **MAC Address**. If you want to allow all remote devices can access the router, select **All**.
7. Click **Save** to make the settings effective.

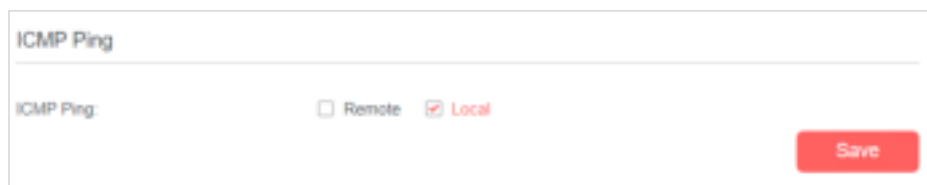
Tips:

1. You can find the WAN IP address of the router on **Basic > Network Map > Internet**.
2. The router's WAN IP is usually a dynamic IP. Please refer to [Set Up a Dynamic DNS Service Account](#) if you want to log in to the router through a domain name.

11. 10. ICMP Ping

ICMP (Internet Control Message Protocol) Ping is used to diagnose the network by sending ICMP echo request packets to the target remote or local host and waiting for an ICMP response.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Click **Advanced** > **System Tools** > **Administration** page. Locate the **ICMP Ping** section.



3. Select **Remote** if you want the computers on a public network to ping the router's WAN IP address. Select **Local** if you want the computers on a private network to ping the router's LAN IP address. Or select both.
4. Click **Save** to make the settings effective.

11. 11. System Log

System Log can help you know what happens to your router, facilitating you to locate the malfunctions. For example when your router does not work properly, you will need to save the system log and send it to the technical support for troubleshooting.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.

2. Click **Advanced** > **System Tools** > **System Log** page.

System Log

Type: ALL

Level: Debug

Refresh Delete All

ID	Time	Type	Level	Log Content
1	2022-12-12 12:30:47	HTTPD	Notice	Clear log.

Log Settings Save Log

➤ **To view the system logs:**

1. Select the log Type.
2. Select the log Level and you will see the logs with the specific or higher levels.
3. Click **Refresh** to refresh the log list.

➤ **To save the system logs:**

You can choose to save the system logs to your local computer or a remote server.

1. Click **Save Log** to save the logs in a txt file to your computer.
2. Click **Log Settings** to set the save path of the logs.

Log Settings

☒ Save Locally

Minimum Level: Information

☒ Save Remotely

Minimum Level: Warning

Server IP: 102.108.1.100

Server Port: 514

Local Facility Name: User

Back Save

- **Save Locally** - Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- **Save Remotely** - Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the

information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

11. 12. CWMP

CWMP (CPE WAN Management Protocol, also called TR-069) allows Auto-Configuration Server (ACS) to perform auto-configuration, provision, connection, and diagnostics to this device. You may configure this function under your ISP's instructions.

1. Visit <http://mwlogin.net>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > CWMP Settings**.
3. Enable **CWMP**.

The screenshot shows the 'CWMP Settings' page. At the top, there's a title 'CWMP Settings' and a help icon. The settings are organized into sections. The 'CWMP' section has a toggle switch that is turned on. The 'Inform' section also has a toggle switch that is turned on. Below 'Inform' is the 'Inform Interval' field with the value '300' and the unit '(seconds)'. The 'ACS URL' field is empty. The 'ACS Username' field contains 'admin'. The 'ACS Password' field is masked with dots. The 'Interface used by TR-069 client' dropdown menu is set to 'Any WAN'. The 'Display SOAP messages on serial console' toggle switch is turned off. Below these is a section titled 'Connection Required Authentication' with a red icon. It contains fields for 'Username' (admin), 'Password' (masked), 'Path' (/root), 'Port' (7547), and 'URL'. There is a 'Get RPC Methods' button and a 'Save' button at the bottom right.

4. If you want to send an Inform message to the ACS (Auto Configuration Server) periodically, enable **Inform** and set the **Inform Interval**.
5. Enter the ACS URL, username and password provided by your ISP.
6. Select the interface used by TR-069 client.
7. Determine whether to display SOAP messages on serial console or not.

8. Select the checkbox **Connection Request Authentication** to enable authentication for the connection request. Enter the username and password for the ACS server to log into the router. Then enter the path, port, and URL that connects to the ACS server.
9. Click **Get RPC Methods** to get the methods that support CWMP.
10. Save the settings.

FAQ

Q1. How do I restore my router to its factory default settings?

With the router powered on, press and hold the WPS/RESET button on the rear panel for more than 5 seconds to reset the router.

Note:

Once the router is reset, the current configuration settings will be lost and you will need to re-configure the router.

Q2. What should I do if I forget my password?

- **Web Management Page Password:**

Restore the router to its factory default settings and then create a new password.

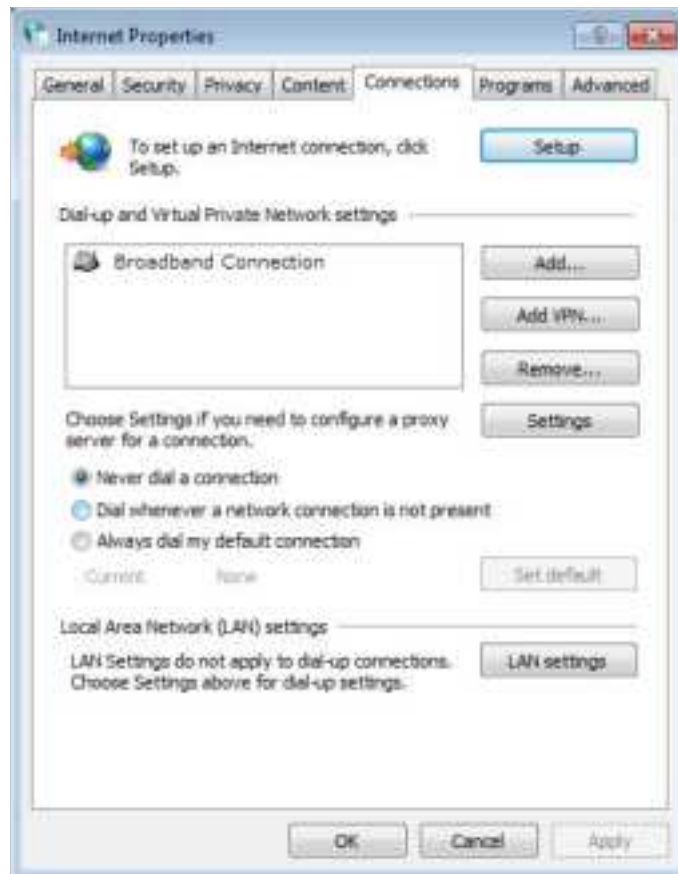
- **Wireless Network Password:**

1. The default Wireless Password/PIN is printed on the product label of the router.
2. If the default wireless password has been changed, connect your computer to the router using an Ethernet cable, log in to the router's web management page, and go to **Basic > Wireless** to retrieve or reset your password.

Q3. What should I do if I cannot access the web management page?

This can happen for a variety of reasons. Please try the methods below to log in again.

- Make sure your computer has connected to the router correctly.
- Make sure the IP address of your computer is configured as **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Make sure you enter the correct IP address to log in: <http://mwlogin.net>.
- Check your computer's settings:
 - 1) Go to **Start > Control Panel > Network and Internet**, and click **View network status and tasks**.
 - 2) Click **Internet Options** on the bottom left.
 - 3) Click **Connections** and select **Never dial a connection**.



4) Click **LAN settings**, deselect the following three options and click **OK**;



5) Go to **Advanced > Restore advanced settings**, click **OK** to save the settings.



- Use another web browser or computer to log in again.
- Reset the router to factory default settings and try again. If the login still fails, please contact the technical support.

Note: You'll need to reconfigure the router to surf the internet once the router is reset.

Q4. What can I do if I cannot access the internet?

1. Verify that your SIM card is an LTE or WCDMA card.
2. Verify that your SIM card is in your ISP's service area.
3. Verify that your SIM card has sufficient credit.
4. Check the LAN connection:
Open a web browser and enter <http://mwlogin.net> or <http://192.168.1.1> in the address bar. If the login page does not appear, refer to Q3 and then try again.
5. Check your ISP parameters:
 - 1) Open a web browser and log in to the web management page.
 - 2) Go to **Advanced > Network > Internet** to verify the parameters (including the APN, Username and Password) provided by your ISP are correctly entered.

If the parameters are incorrect, click **Create Profile** and enter the correct parameters, then select the new profile from the Profile Name list.

6. Check the PIN settings:
 - 1) Open a web browser and log in to the web management page.
 - 2) Go to **Advanced > Network > PIN Management** to verify if PIN is required. If it is, enter the correct PIN provided by your ISP or disable **PIN Lock**, and click **Save**.
7. Check the Data Limit:
 - 1) Open a web browser and log in to the web management page.
 - 2) Go to **Advanced > Network > Data Settings** to verify if the **Total Used** exceeds the **Total Allowance** or if the **Monthly Used** exceeds the **Monthly Allowance**. If it does, click **Correct** and set **Total/Monthly Used** to 0 (zero), or disable **Data Limit**.
8. Check the Mobile Data:
 - 1) Open a web browser and log in to the web management page.
 - 2) Go to **Advanced > Network > Internet** to verify that **Mobile Data** is enabled. If not, toggle it On to access the internet.
9. Check the Data Roaming:
 - 1) Confirm with your ISP if you are in a roaming service area. If you are, open a web browser and log in to the web management page.
 - 2) Go to **Advanced > Network > Internet** to verify that **Data Roaming** is enabled. If not, toggle it On to access the internet.

Q5.What should I do if my internet speed is slow?

1. Make sure you are inside a network coverage area.
2. Relocate your router and your computer to have a better signal reception – you may be in or near a structure that is blocking the signal. Obstacles (for example, walls, ceilings, and furniture) between the router and other wireless devices decrease the signal strength.

Q6.What can I do if I cannot find my wireless network or I cannot connect the wireless network?

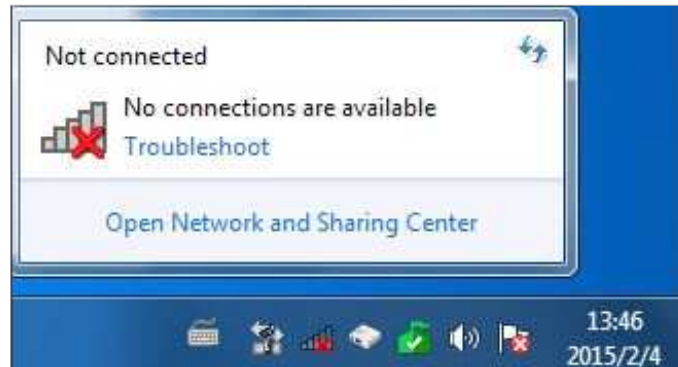
➤ **If you fail to find any wireless network, please follow the steps below:**

1. Make sure the wireless function is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.

2. Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.

On Windows 7

- 1) If you see the message **No connections are available**, it is usually because the wireless function is disabled or blocked somehow;



- 2) Clicking on **Troubleshoot** and windows might be able to fix the problem by itself.

On Windows XP

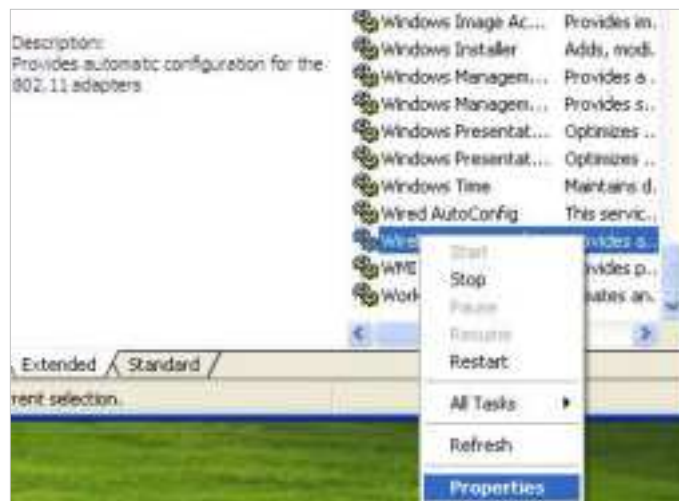
- 1) If you see the message **Windows cannot configure this wireless connection**, this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.



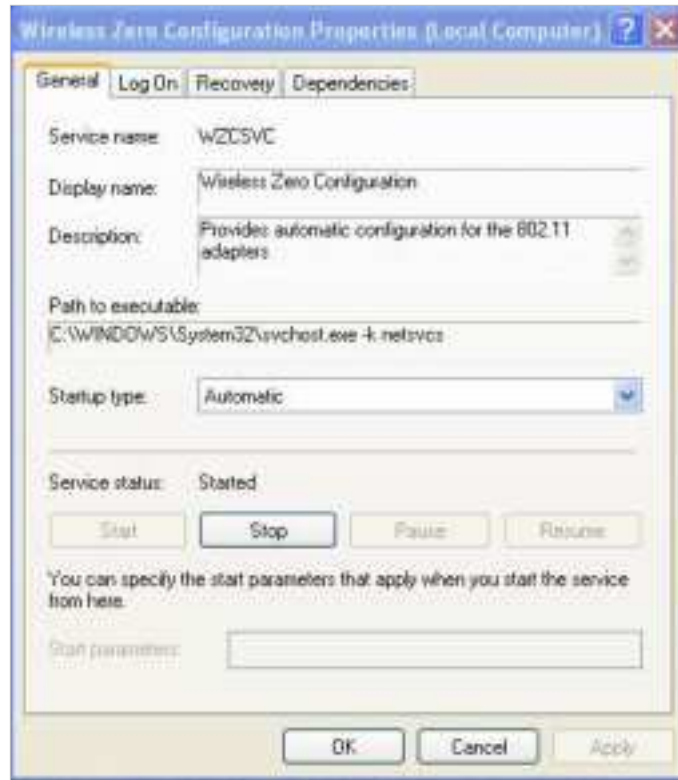
- 2) Exit the wireless configuration tool.
- 3) Select and right click on **My Computer** on desktop, select **Manage** to open Computer Management window.
- 4) Expand **Services and Applications > Services**, find and locate **Wireless Zero Configuration** in the Services list on the right side.



5) Select **Wireless Zero Configuration**, right click it, and then select **Properties**;



6) Change **Startup type** to **Automatic**, click on Start button and make sure the Service status is Started. And then click **OK**.



7) Connect to wireless network.

➤ If you can find other wireless network except your own, please follow the steps below:

1. Make sure your computer/device is still in the range of your router/modem, move closer if it is currently too far away;
2. Go to **Advanced > Wireless > Advanced Settings** page, and check the wireless router settings. Double check your Wireless Network Name, and make sure the SSID is not hidden;
3. Connect to wireless network.

➤ If you can find your wireless network but fail to connect, please follow the steps below:

1. Authenticating problem, password mismatch.
 - 1) Sometimes it will ask you to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the back of your wireless router/modem;



- 2) If you cannot find the PIN or PIN failed, you may choose **Connecting using a security key instead**, and then type in the Network Security Key/Wireless Password;



- 3) If it continues saying network security key mismatch, it is suggested to confirm the wireless password on your wireless router/modem;

■ Note: Wireless password/Network Security Key is case-sensitive.



- 4) Connect to wireless network.
2. Windows was unable to connect to XXXX /Cannot join this network/Taking longer than usual to connect to this network.

- 1) Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again;
- 2) Change the wireless Channel of the router to 1,6,or 11 to reduce interference from other networks;
- 3) Re-install or update the driver for your wireless adapter of the computer;
- 4) Connect to wireless network.