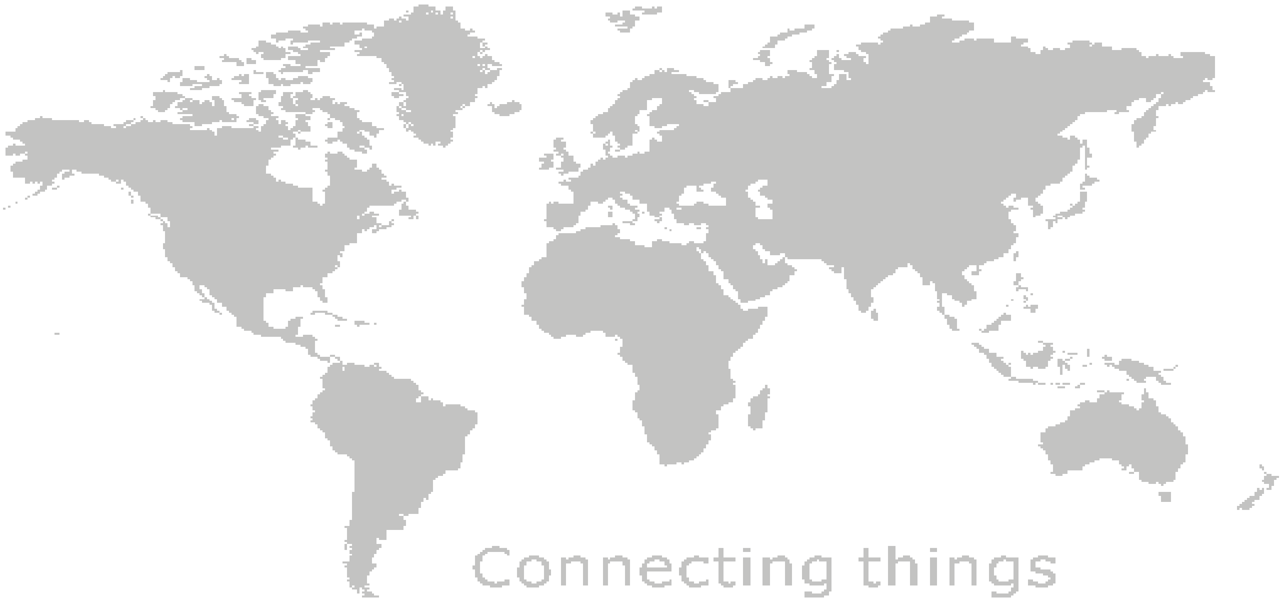
User Manual

MRR8860 Industrial Intelligent Gateway

Connecting things
Hongdian



Shenzhen Hongdian Technology Co., Ltd. will provide customers with all-round technical supinterface, users can directly contact the company's headquarters.

Shenzhen Hongdian Technology Co., Ltd.

Address:	F14 - F16, Tower A, Building 14, Headquarters Center, Hisense Science and Technology Park, the middle section of Bulan Road，Longgang District, Shenzhen
Website:	http://www.hongdian.com
Technical line:	Call 400-00-64288 and then transfer 2
Complaint hotline:	Call 400-00-64288 and then transfer 3
Fax:	0755-83644677
Postal code:	518112

Brand Statement

宏电 Hongdian、DTU is the trademark of Shenzhen Hongdian Technology Co., Ltd. The other trademarks mentioned in this specification are owned by the organization that owns the trademarks, and Hongdian does not have the right to own other trademarks.

Attention

The contents of this document are updated from time to time due to product version upgrades or other reasons. Unless otherwise agreed, this document is for use only and all representations, information and recommendations in this document do not constitute any warranty, express or implied.

Foreword

FCC Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

Note: The Grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. such modifications could void the user's authority to operate the equipment.

The device has been evaluated to meet general RF exposure requirement.

To maintain compliance with FCC's RF exposure guidelines, the distance must be at least 20 cm between the radiator and your body, and fully supported by the operating and installation.

Overview

The MRR8860 Industrial Intelligent Gateway is a new generation VPN router with edge computing capability, which is based on industry-wide hardware platform, has powerful data processing and computing capability, supports data local storage and analysis decision, open system design, supports secondary development and third-party SDK.

With wireless network and a variety of bandwidth services, the device provides stable and reliable Internet access everywhere, with its excellent product quality and comprehensive security, realizing tens of thousands of equipment networking, for the real sense of equipment information, manufacturing intelligence, industrial Internet solutions.

The main functions of this document are to help readers understand the features and typical applications of the product, to be familiar with the installation, deployment and configuration of the product, and to master common troubleshooting during use.

Reader object

This document applies to the following people:

- R & D Engineer
- Technical Support Engineer
- Customer

In the case of first-time exposure and use of the Hongdian Industrial Routing and Industrial Gateway product, it is recommended that you read the entire contents of this document, starting with Chapter 1, for the appropriate product understanding and correct use.

If you have known or used the Hongdian Industrial Routing and Industrial Gateway products, it is recommended that you selectively read the sections you want to know through the document structure navigation.

Convention

Symbolic convention

The following symbols that appear in the text represent the following meanings.

Symbol	Description
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you address a problem or save your time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Common format convention

Format	Explain
Song style	The text is in the form of a song.
Black body	The first, second and third headings are in bold type.
Regular script	Warnings, reminders and other contents are all in italics, and before and after the addition of lines and text isolation.
TerminalDisplay format	The Terminal Display format represents screen output information. In addition, the user input from the terminal that is included in the screen output information is indicated in bold font.

Graphical interface element reference convention

Format	Significance
“ ”	The format with double quotation marks " " represents various interface control names and data tables, such as clicking OK.
>	Multi-level menus are separated by ">". If you select File>New>Folder, you select the Folder menu item under the new

Format	Significance
	submenu under the File menu.

Keyboard operating convention

Format	Significance
Characters with ' '	Represents the key name. Such as " Enter ", " Tab ", " Backspace ", " A ", and so on, respectively represent the car back, tab, backspace, lowercase letter A.
Key 1 + Key 2	Indicates that several keys are pressed simultaneously on the keyboard. Such as " Ctrl+Alt+A " means that the three keys " Ctrl ", " Alt ", " A " are pressed simultaneously.
Key 1, Key 2	Means press the first key, release, and then press the second key. For example, " Alt, F " means press the " Alt " key first, release it, and then press the " F " key.

Mouse operation convention

Format	Significance
Click	Quickly press and release a mouse button.
Double click	Quickly press and release a mouse button twice in a row.
Drag	Hold down a mouse button, move the mouse.

Modifying a record

The revision records accumulate notes for each document update. The latest version of the document contains updates for all previous document versions.

Document version	Revision Time	Reviser	Revision notes
V1.0.0.1	2019-03-08	Liu Linfeng	First draft
V1.0.0.2	2019-03-14	Liu Linfeng	Modify Section Description Error

Contents

Table contents

Figure contents

1 Product introduction

1.1 Overview

The MRR8860 Industrial Intelligent Gateway is a new generation wireless VPN router with edge computing capability, which is based on industry-wide hardware platform, has powerful data processing and computing capability, supports data local storage and analysis decision, open system design, supports secondary development and third-party SDK.

With wireless network and a variety of bandwidth services, the device provides stable and reliable Internet access everywhere, with its excellent product quality and comprehensive security, realizing tens of thousands of equipment networking, for the real sense of equipment information, manufacturing intelligence, industrial Internet solutions.

The device also supports the development of M2M wireless remote integrated network management platform. The M2M platform can realize the statistics of the information and state of the wireless network and the remote upgrade and configuration management of the MRR8860 industrial intelligent gateway.

1.2 Product positioning

The MRR8860 Industrial Intelligent Gateway is mainly industrial oriented, with powerful data collection, storage, analysis and processing capabilities, providing customers with integrated solutions for device networking, edge computing and intelligent operation of the Industrial Internet.

Intelligent plant equipment wireless networking

The intelligent factory is a new stage of the development of factory informatization, and the equipment networking is the first step toward the intelligent factory. In view of the bad environment of the electronic manufacturing workshop on the spot, the MRR8860 industrial intelligent gateway adopts the all-industry hardware platform, wide temperature and wide pressure, dustproof and damp-proof, anti-seismic, anti-electromagnetic interference, through the compatibility of the mainstream industrial protocol, the industrial data is efficiently transferred to the background management system for analysis and processing.

Numerical control machine tool remote intelligent monitoring

With the increasing demands of modern manufacturing processes for complexity, precision, large scale and automation equipment, CNC machine tools have been widely used. Macropower MRR8860 Industrial Intelligent Gateway provides base station location, helps equipment manufacturers implement asset tracking and management, collects and analyzes equipment operation status and performance indicators, realizes equipment predictive maintenance, and provides better service to customers.

1.3 Features

Basic function

- Support WAN, WLANand other multi-network simultaneous on-line and multi-network backup switching
- Supports WLAN AP/Station client functionality for up to 1200 Mbps wireless LAN transmission rate
- Support 8 Gigabit LAN, 1 Gigabit WAN port
- Support WAN port PPPoE dialing
- Support VPDN, APN private network access
- Supports IPSec, GRE (Generic Routing Encapsulation), IPIP, PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and OpenVPN supports CA digital certificates
- Support for DHCP Server features
- Support for local or remote firmware or patch upgrades
- Supports Web, CLI, and platform parameter management modes
- Support M2M platform management, real-time statistics of device traffic, monitoring device network status
- Supports parameter backup and import, supports the use of private key import export parameter configuration
- Support for DNS and DDNS features
- Support NTP network timing function
- Supports RTC real-time clock functionality
- Supports SNMP network management functions
- Provide system local log and remote log sending for real-time network monitoring
- QoS (Quality of Service) support for intelligent QoS bandwidth management for business, protocol, IP network segments
- Supports static routing, RIPv2 (Routing Information Protocol) and OSPF (Open Shortest Path First, Open Shortest Path First) dynamic routing, supports source address policy routing
- Support timing management, support timing offline or data idle offline
- Support LCP (Link Control Protocol) detection, ICMP (Internet Control Message Protocol) detection, heartbeat packet detection and other link detection functions to ensure the wireless network stability and reliability
- LED status monitoring (status of display system, ignal strength, etc.)

1.4 Technical indicators and specifications

Serial MRR8860 type:

Interface

- Antenna connector: Reverse Thread SMA, two WIF-2.4 and two WiFi-5.8 antenna connectors

- Ethernet connector: Four RJ45 Switches, 10000000/ 100 M/ 1000 MBase-T Adaptive
- WAN interface: One RJ45 Switch 10000000/ 100 M/ 1000 MBase-T Adaptive
- Reset button: One-key recovery factory key
- DC power outlet: Supply voltage
- Ground stud: ground wire

Power supply

- Voltage: +9V~+48 VDC
- Idle average power consumption approximately 500 mA@ 12V DC
- Average operating power consumption: Approx. 650 Ma @ 12V DC

Additional parameters

- Weight: Approx. 610 g
- Operating environment temperature: C-30~+ 75 º C
- Storage temperature: C-40~+ 85 º C
- Relative humidity: ≤ 95% (no condensation)

MRR8860 gateway edition:

Interface

- Antenna connector: Reverse Thread SMA,two WIF-2.4 and two WiFi-5.8 antenna connectors
- Ethernet connector: Eight 10000000/ 100 M/ 1000 MBase-T adaptive LAN port
- WAN interface: One RJ45 Switch 10000000/ 100 M/ 1000 MBase-T Adaptive
- Reset button: One-key recovery factory key
- DC power outlet: Supply voltage
- Ground stud: ground wire

Power supply

- Voltage: +9V~+48 VDC
- Average idle power consumption: 500 MA @ 12V DC
- Average operating power consumption: 650 MA @ 12V DC

Additional parameters

- Weight: Approx. 610 g
- Operating environment temperature: C-30~+ 75 º C
- Storage temperature: C-40~+ 85 º C
- Relative humidity: ≤ 95% (no condensation)

2 Product structure

About this chapter

Chapter	Content brief
错误!未找到引用源。 Hardware structure	This section provides an overview of the hardware structure of the MRR8860 Industrial Intelligent Gateway.
错误!未找到引用源。 Function structure	This section provides an overview of the functional structure of the MRR8860 Industrial Intelligent Gateway product.

2.1 Hardware structure

2.1.1 Equipment appearance and dimensions

Appearance diagram

The physical image of the appearance of the Industrial Intelligent Gateway for Macropower MRR8860 is shown in Figure 2-1.

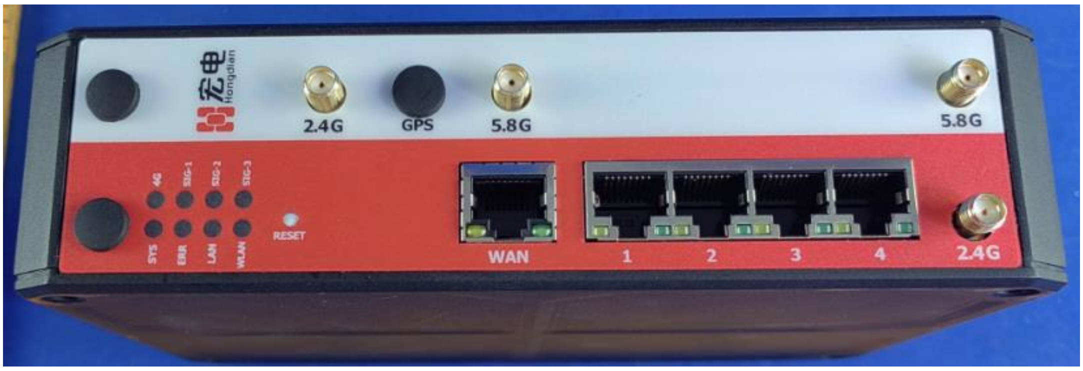


Figure2-1 Physical drawing of the appearance of the MRR8860 industrial intelligent gateway

Size

Device name	Length × width × height (mm)	Socket description
MRR8860 serial port version	180×125×48	• One WAN port: for wired Internet connection • Four LAN ports: for connecting the lower machine
MRR8860 gateway version	180 × 125 × 48	• One WAN port: for wired Internet connection • Eight LAN ports: for connecting the lower machine

Figure2-1MRR8860 Industrial Intelligent Gateway Device Size Specification

The dimensions of the appearance structure of the MRR8860 Industrial Intelligent Gateway are shown in Figure 2-2.

NOTE

In the following figures, the units corresponding to the physical dimensions of the equipment are millimeters, which are not described below.

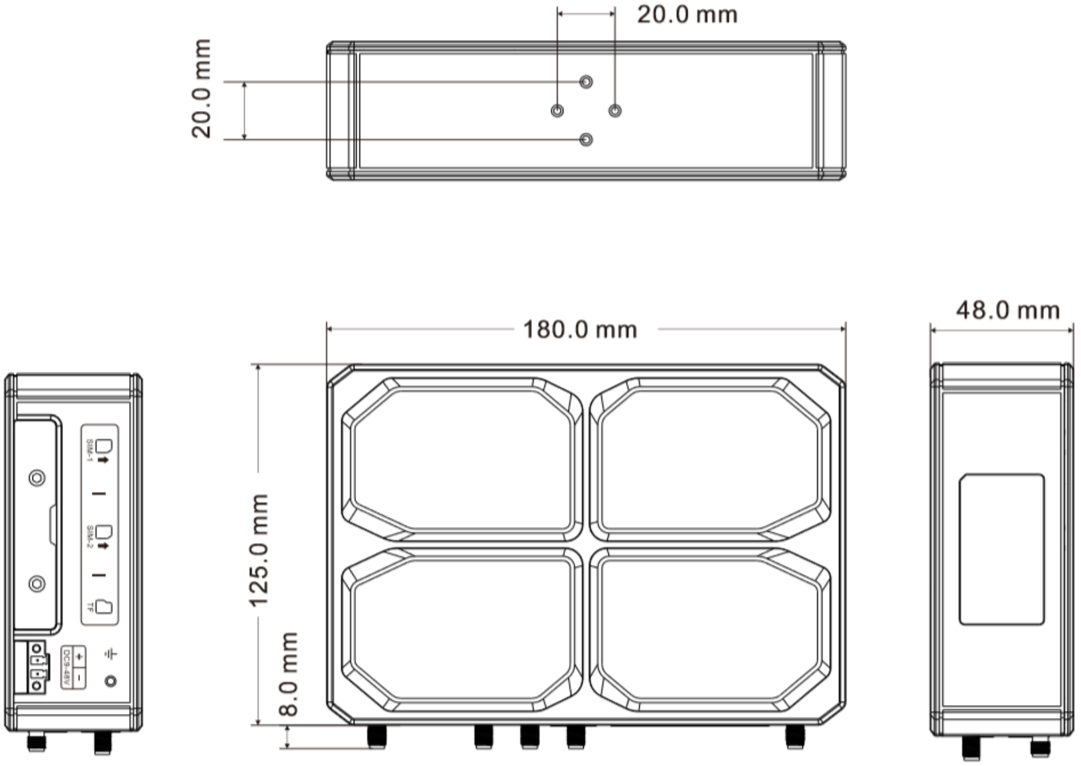


Figure2-2 MRR8860 industrial intelligent gateway structure size chart

2.1.2 Equipment configuration and accessories

Accessories Description

The MRR8860 Industrial Intelligent Gateway contains accessories as shown in Table 2-3.

Gadget Name	Quantity	Remark
Standard assignment		
MRR8860 Industrial Intelligent Gateway Host	One	Packing according to customer order
Wifi antenna	Four	Two for 2.4 g, two for 5.8 g
RJ45	One	None
Mounting fixture	One pair	None
Certificate and warranty card	One	None
Plug connection terminal of 1MRR8860 PIN (female)	One	None

Table2-2 List of MRR8860 Industrial Intelligent Gateway Fittings

Model description

The MRR8860 industrial intelligent gateway is a non-line route transmission product based on wireless communication technology (which supports wired transmission at the same time), supports secondary development, has high performance dual-frequency WiFi function, adopts full-industry design, electromagnetic compatibility design, modularization design, and is suitable for different industry application requirements and network environment of operators.

2.2 Functional structure

The MRR8860 industrial intelligent gateway is divided into single mode plus WLAN.

Master controller module

The module is primarily responsible for the following functions:

- Controlling a router's wired connection to the Internet
- Forwarding IP packets
- Run advanced functions such as routing protocol, firewall protocol, VPN protocol
- Maintain proper operation of equipment

LAN

The gateway data processing module of the router communicates with the lower computer through RJ45 network line, and provides the IP packet forwarding function for the lower computer.

WAN

This module is mainly used to enable the MRR8860 Industry Smart Gateway to connect to the Internet by wire.

WLAN

This module is mainly used for WLAN terminal to connect MRR8860 industrial intelligent gateway WiFi hot spot, so it is convenient for WLAN terminal to connect external network. The module supports dual-frequency 2.4 G and 5.8 GWiFi, with powerful performance. It also supports two functional modes, bridging and client, through which you can connect to other AP and Internet access.

3 Installing the MRR8860 Industrial Intelligent Gateway

3.1 Unpacking

After the equipment arrives at the site, it is necessary to open the box and check whether the fittings are complete. Under normal circumstances, the kit should contain accessories as shown in Table 2-2. Take care of the packing materials after opening the box for use in the secondary transfer process.

3.2 Installation and wiring

3.2.1 Ethernet wire connection

The MRR8860 Industrial Intelligent Gateway configuration is simple to use, and normal configuration management and data communication is possible through Ethernet cabling. Ethernet connections can be divided into single-device direct connection mode and multi-device LAN connection mode.

Single device direct connection mode

The Ethernet cable using the RJ-45 type connector connects the configuration computer directly to either of the two switches of the MRR8860 Industrial Intelligent Gateway.

3.2.2 Connections for Ethernet cables

The MRR8860 Industrial Intelligent Gateway supports 4 (gateway version 8) LAN and 1 WAN LAN/WAN connections, one end of the network cable can be plugged into the router's LAN connector using an RJ45 network cable, and the other end can be connected to other devices.

3.3 Power supply

The MRR8860 Industrial Intelligent Gateway product uses +9V~+48V DC power.

3.4 Installation check

Before installing and preparing to power on, check the see if it is plugged in. After the power is plugged in, check the working state LED of the gateway. All the lights will be on in the instant when the power is plugged in. Next, the SYS light will be on. After a period of time, the LAN light connected to the PC will be on, indicating that the system has been started and connected to the PC.

CAUTION

Be sure to connect the antenna before power up, so as to avoid the radio frequency part impedance mismatch, resulting in poor signal and unable to dial up the line.

4 Installing before configuring

4.1 LED status

Industrial IntelligencTable 4-1 LED Description Table

Indicating filament print	LED name	Status description
SYS	System status LED (green)	Normal light: indicates that the system is normal Flashing: Indicates initialization is in progress
LAN	LAN LED (green)	Normal light: any LAN port connection is normal ; Flashing: Data passing through any LAN port ; Off: No LAN port connection
WiFi	Wireless LED (green)	Normal light: indicating normal wireless ; Flashing: Indicates data transfer

Tre are eight LED indicators on the front panel of the gateway that indicate the operational and network status of the MRR8860 Industrial Intelligent Gateway. The LED status descriptions are shown in Table 4-1.

4.2 Local connection configuration

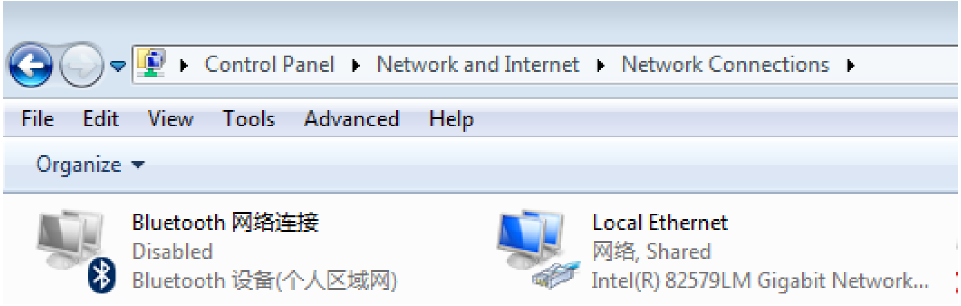
Prerequisite condition

- Power has been supplied to the MRR8860 Industrial Intelligent Gateway.
- The MRR8860 Industrial Intelligent Gateway gateway gateway gateway has been connected over the Ethernet cable.

For details on Ethernet connections, see 3.2.2 Ethernet wire connections. The local connection configuration of the MRR8860 Industrial Intelligence Network includes the specified IP mode and DHCP automatic access IP mode, which are described in detail below.

Specify IP Mode

Step 1 Click Start>Control Panel>Network and Internet>Network Sharing Center> Local Area Connection, as shown in Figure 4-1.

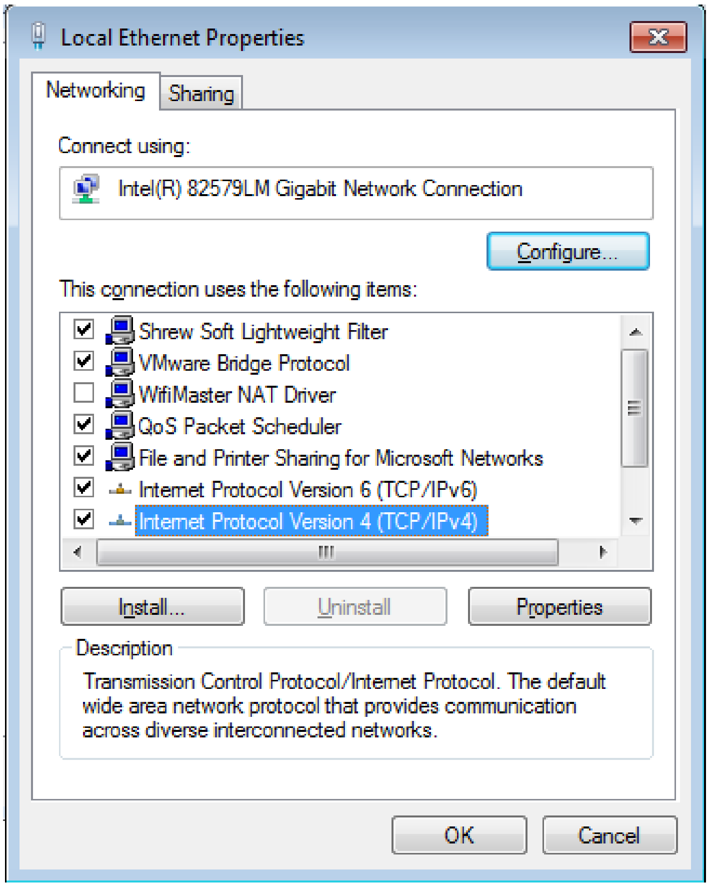

Control Panel ▸ Network and Internet ▸ Network Connections ▸
File Edit View Tools Advanced Help
Organize ▾

Bluetooth 网络连接
Disabled
Bluetooth 设备(个人区域网)

Local Ethernet
网络, Shared
Intel(R) 82579LM Gigabit Network...

Figure 4-1 Network connection window

Step 2 Click Local Connection to open the Local Connection Status window, as shown in Figure 4-2.



Connect using:
Intel(R) 82579LM Gigabit Network Connection

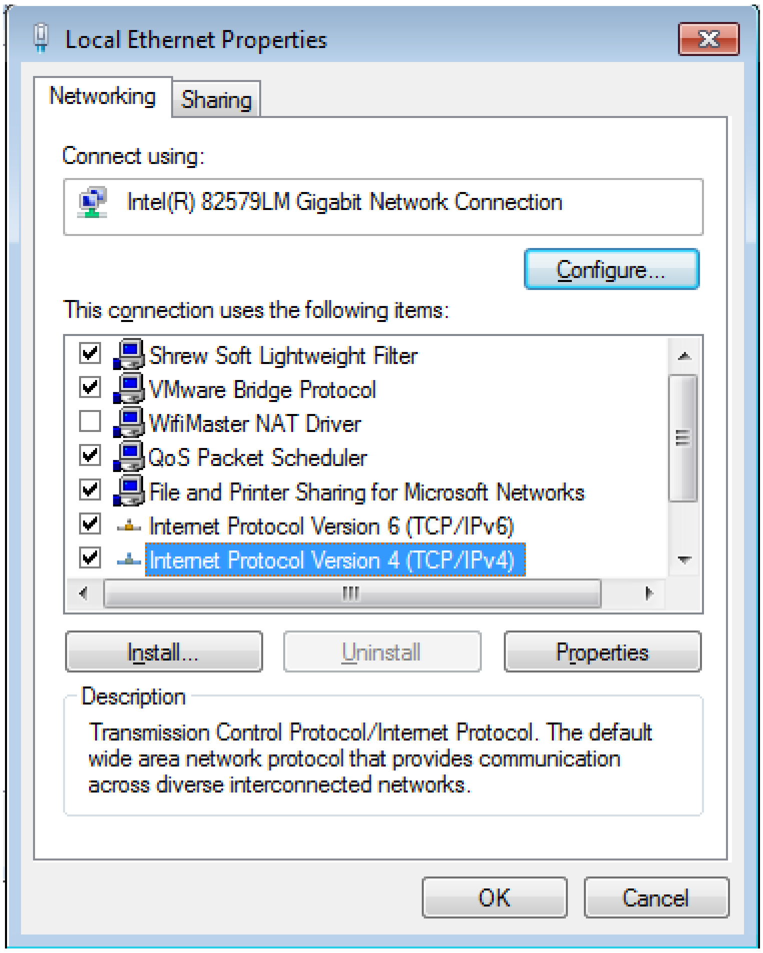
This connection uses the following items:

- ☑ Shrew Soft Lightweight Filter
- ☑ VMware Bridge Protocol
- □ WifiMaster NAT Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 4-2 Local connection status

Step 3 Click Properties in the Local Connection Status window to open the Local Connection Properties window, as shown in Figure 4-3.



Local Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) 82579LM Gigabit Network Connection

Configure...

This connection uses the following items:

- ☑ Shrew Soft Lightweight Filter
- ☑ VMware Bridge Protocol
- ☐ WifiMaster NAT Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Figure 4-3 Internet Protocol (TCP/IPv4)

There are two configuration methods for the latter configuration, general method configuration and advanced configuration.

- General method configuration

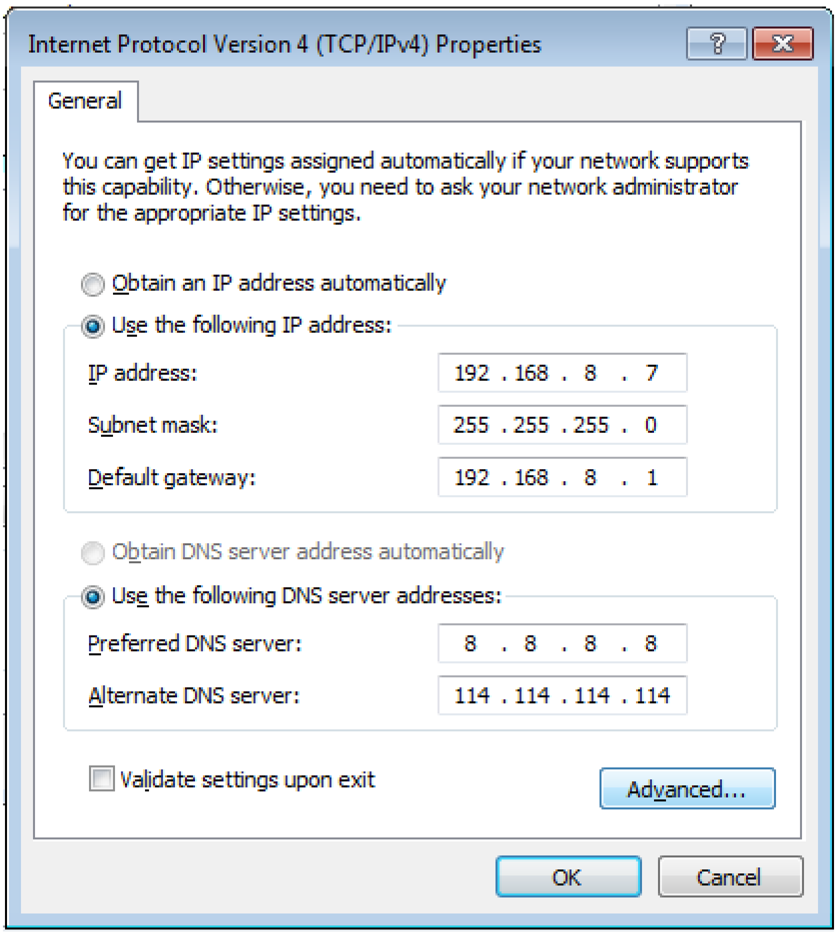
1. In the Local Connection Properties window, double-click Internet Protocol (TCP/IP) to open the Internet Protocol (TCP/IP) Properties window. Modify the general network configuration in the General tab. As shown in Figure 4-4.

CAUTION

Because of the factory default parameters for the MRR8860 Industrial Intelligent Gateway,

- IP address: 192.168.8.1
- Subnet mask: 255.255.255.0

Therefore, in the Internet Protocol (TCP/IP) Properties window, the Default Gateway and Subnet Mask are configured as factory defaults for the MRR8860 Industrial Intelligent Gateway.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 8 . 7
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 8 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 114 . 114 . 114 . 114

□ Validate settings upon exit

Figure 4-4 Internet Protocol (TCP/IPv4) Properties Window 3

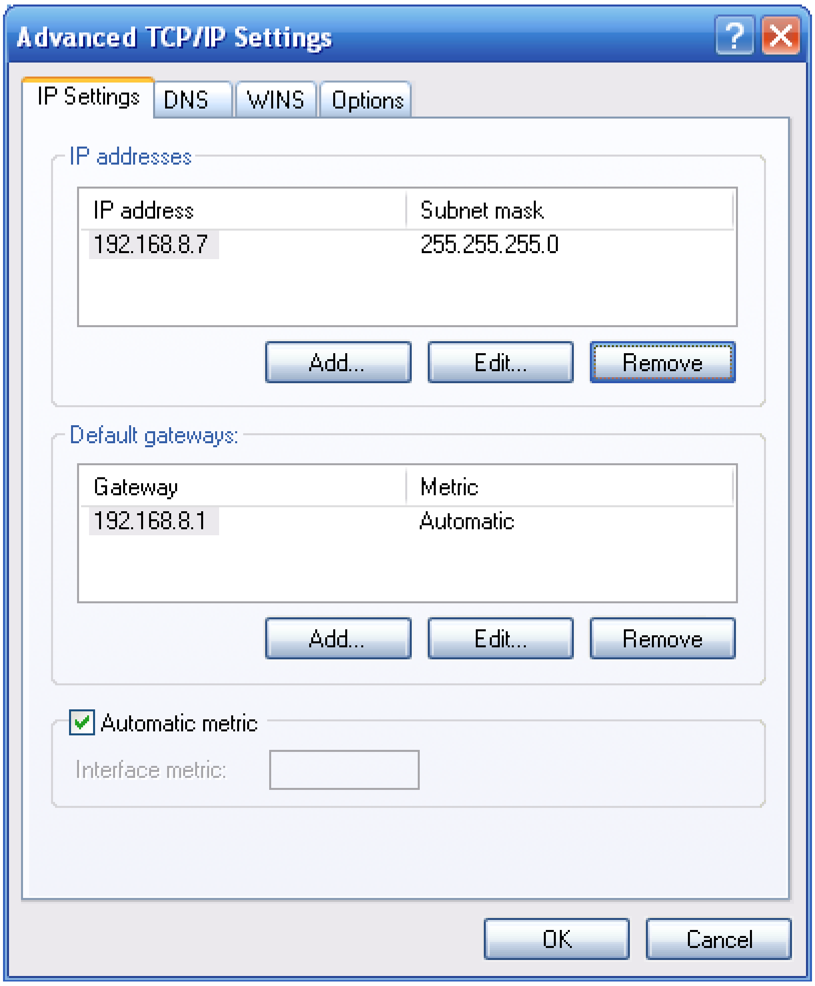
Note: The IP address can be 192.168.8. * (where * represents any integer between 2 and 254).

2. Click OK to complete the configuration.

- Advanced configuration

This method, when you do not want to interrupt the local PC to continue LAN communication under the original network environment configuration (steps 1-3), and you can configure the MRR8860 industrial intelligent gateway, you can consider adding an advanced configuration.

1. Click Advanced to open Advanced TCP/IP Settings, as shown in Figure 4-5.



IP addresses

IP address	Subnet mask
192.168.8.7	255.255.255.0

Default gateways:

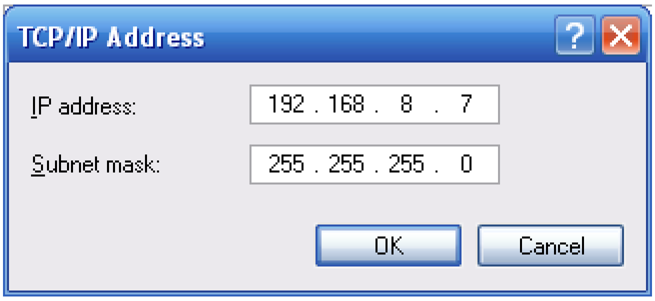
Gateway	Metric
192.168.8.1	Automatic

☑ Automatic metric

Interface metric:

Figure 4-5 Advanced TCP/IP Settings

2. Click Add in IP Address (R) to complete the IP address that you need to configure, as shown in Figure 4-6.



IP address: 192 . 168 . 8 . 7

Subnet mask: 255 . 255 . 255 . 0

Figure 4-6 TCP/IP address

3. Click Add to complete the configuration.

---End

DHCP Auto Get IP Mode

The MRR8860 Industrial Intelligent Gateway built-in DHCP (Dynamic Host Configuration Protocol) server automatically assigns IP (Internet Protocol) addresses to terminals (or PCs, etc.) connected to it by preset parameters.

NOTE

The DHCP service built into the MRR8860 Industry Smart Gateway is factory turned on, and the DHCP service is turned on until this feature is configured.

Step 1 Click Start>Control Panel>Network and Internet>Network Connections, as shown in Figure 4-7.

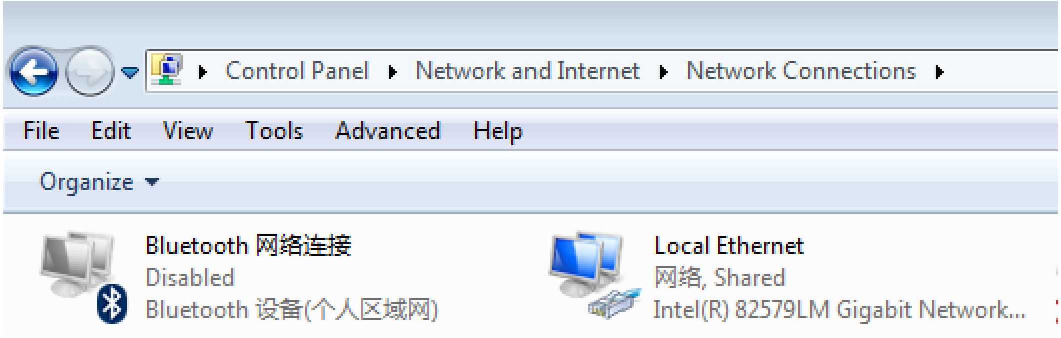
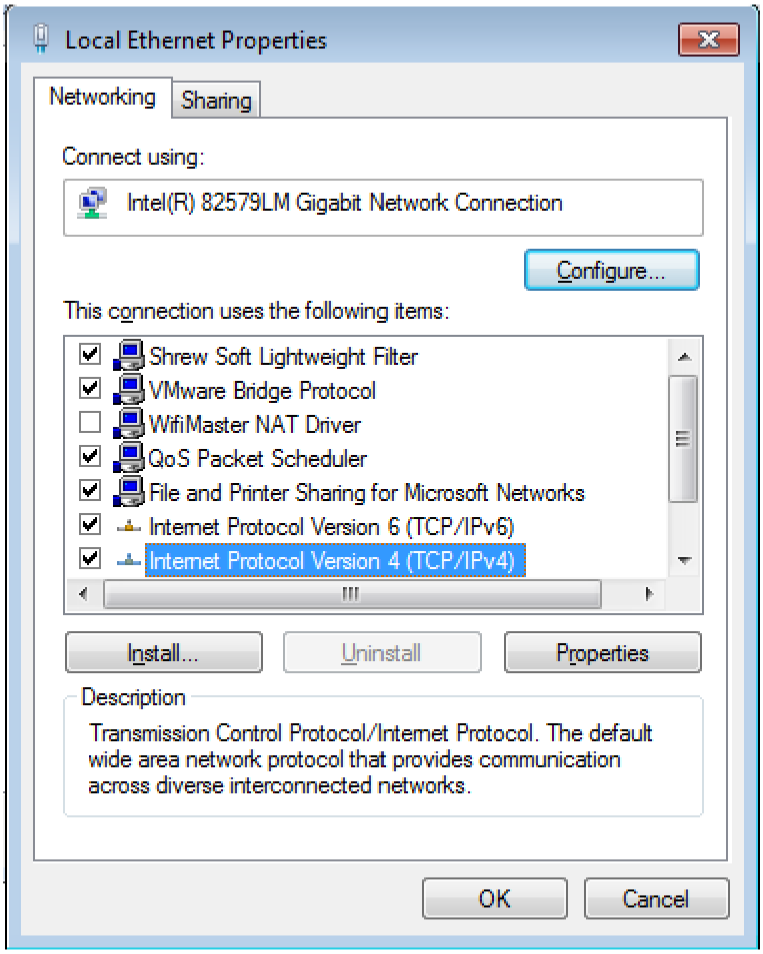

Control Panel ▸ Network and Internet ▸ Network Connections ▸
File Edit View Tools Advanced Help
Organize ▾
Bluetooth 网络连接
Disabled
Bluetooth 设备(个人区域网)
Local Ethernet
网络, Shared
Intel(R) 82579LM Gigabit Network...

Figure 4-7 Network connection window

Step 2 Right-click local Connection and click Properties in the pop-up menu to open the Local Connection window, as shown in Figure 4-8.



Local Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) 82579LM Gigabit Network Connection

This connection uses the following items:

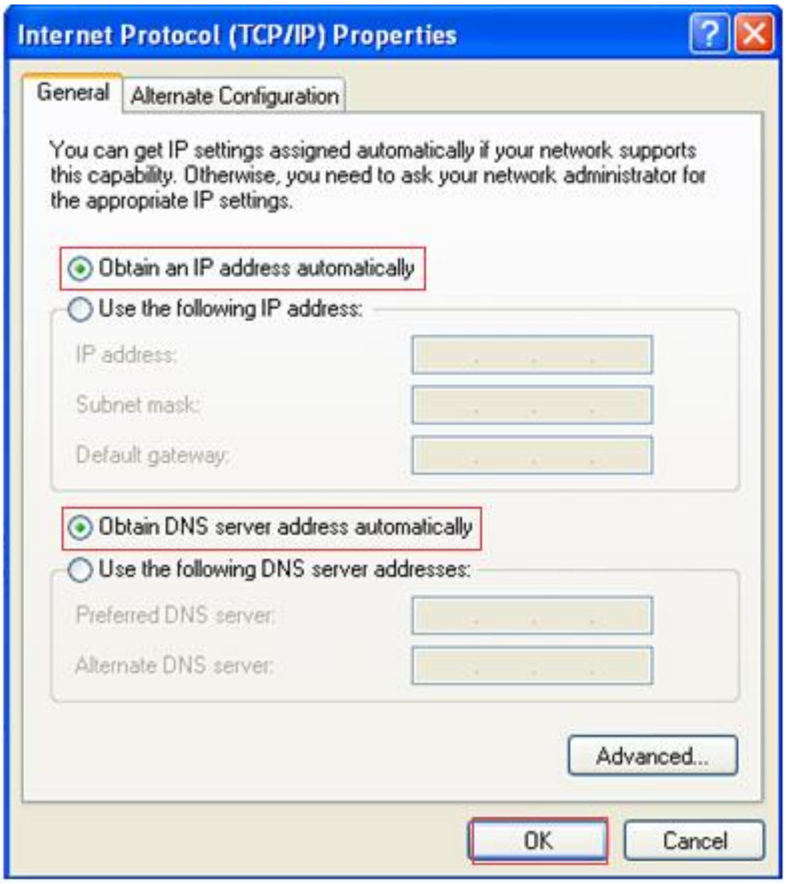
- ☑ Shrew Soft Lightweight Filter
- ☑ VMware Bridge Protocol
- □ WifiMaster NAT Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 4-8 Local connection properties

Step 3 In " This connection uses the following items (0): ", select Internet Protocol Version 4 (TCP/IPv4) and double-click the Internet Protocol Version 4 (TCP/IPv4) Properties window, as shown in Figure 4-9.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Figure 4-9 Internet Protocol Version 4 (TCP/IP) properties

Step 4 If the Internet Protocol Version 4 (TCP/IPv4) properties are shown in Figure 4-9, no changes are required ; If the Internet Protocol Version 4 (TCP/IPv4) property is not shown in Figure 4-9, select Automatically get IP address in General.

Step 5 Click OK to complete the configuration.

---End

Configuration check

Step 1 IP configuration check

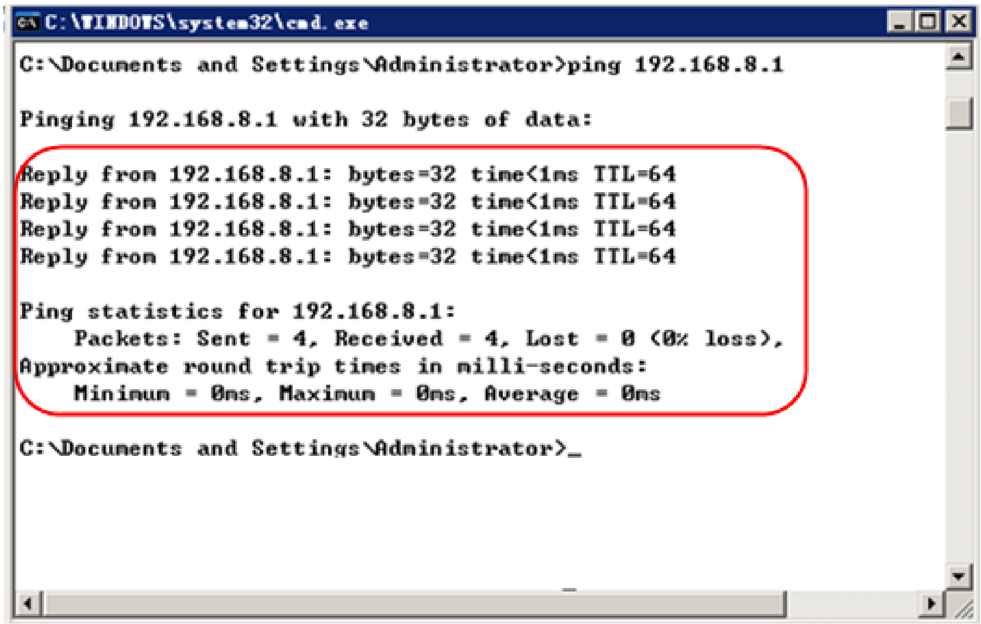
Use the command of ipconfig to check whether the IP address is correctly set or added. You can enter DOS mode and key-in command: ipconfig, for instance:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter local connection:


        Connection-specific DNS Suffix.:

        Auto configuration IP Address . . .: 192.168.8.7

        Subnet Mask . . . . . . . . . . .: 255.255.255.0

        Default Gateway . . . . . . . . .: 192.168.8.1
```

Step 2 Connectivity check

After the configuration is completed, you can check the connectivity between it and Galaxy MRR8860 by ping command. Key-in ping command in system command line:

Connectivity check



```
C:\Documents and Settings\Administrator>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:

Reply from 192.168.8.1: bytes=32 time<1ms TTL=64
Reply from 192.168.8.1: bytes=32 time<1ms TTL=64
Reply from 192.168.8.1: bytes=32 time<1ms TTL=64
Reply from 192.168.8.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

By now, it means that the configuration computer has been connected to the router. You can carry out configuration operation on it.

---End

5 Product Configuration

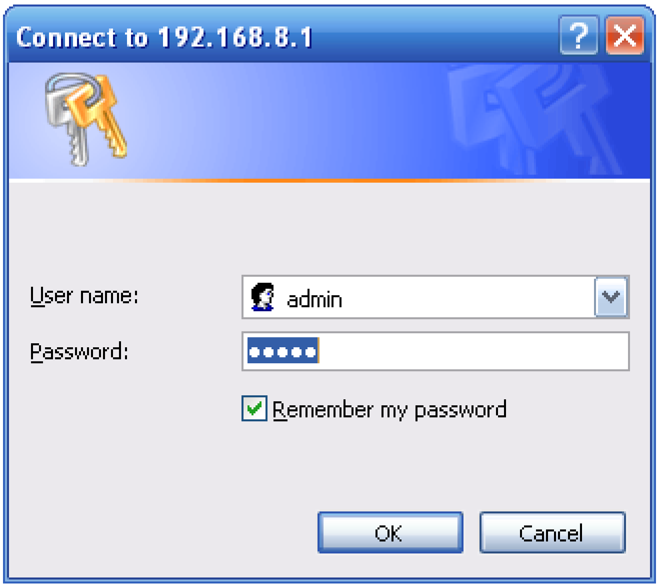
5.1 Overview

The MRR8860 industrial intelligent gateway can be configured in Web mode, which is easy to operate and intuitive. After you complete the local connection configuration for your PC and the MRR8860 Industry Smart Gateway by following Local Connection Configuration, you can start Internet Explorer or other browsers on your PC and log in to the MRR8860 Industry Smart Gateway for configuration.

- Support for IE 8 and above browsers
- Support for Google Chrome browsers
- Firefox browser support
- Edge browser support
- Support Safari browser

5.2 Login Configuration

Open the Configuration Computer IE browser and enter " http:// 192.168.8.1 /" in the address bar. Enter the MRR8860 Industry Smart Gateway device login interface, as shown in Figure 5-1, enter the user name and password, and enter the Web configuration page, as shown in Figure 5-2.



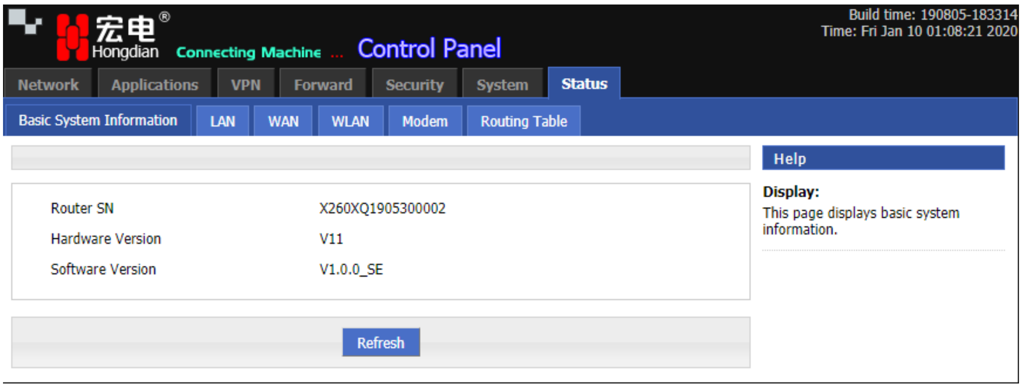
Connect to 192.168.8.1

User name: admin

Password: •••••

☑ Remember my password

Figure 5-1 MRR8860 Industry Intelligent Gateway Device Login Interface



Build time: 190805-183314
Time: Fri Jan 10 01:08:21 2020

Router SN	X260XQ1905300002
Hardware Version	V11
Software Version	V1.0.0_SE

Help

Display:
This page displays basic system information.

Figure 5-2 MRR8860 Industry Intelligent Gateway Device Web Configuration Interface

NOTE

The default user name and password are required when the user first logs on to the system. The default user name is " admin " and the password is " admin ". To modify the password, see 5.7.5 User Management.

---End

5.2.1 Network Settings

Network setup mainly completes LAN, WAN, WLAN, mobile network, parameter switching and network connection, link backup, DHCP server configuration. The configuration is complete to meet basic network communication requirements.

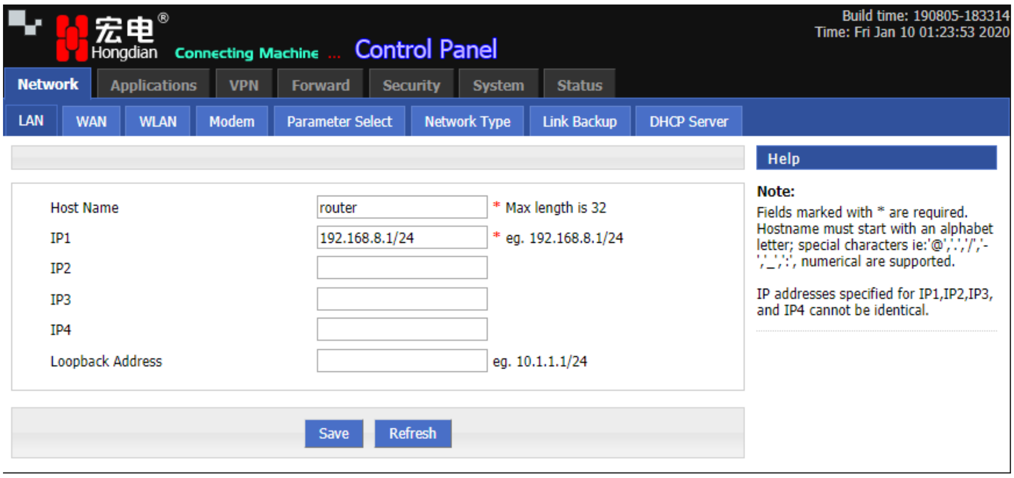
LAN

The LAN port configuration is mainly used to connect the router to the slave computer, so that the slave computer can access the external network through the router, and ensure the normal communication between the network segments connected to the router.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2 Click Network Settings>LAN.

Open the LAN tab, as shown in Figure 5-3.



Build time: 190805-183314
Time: Fri Jan 10 01:23:53 2020

Host Name router * Max length is 32
IP1 192.168.8.1/24 * eg. 192.168.8.1/24
IP2
IP3
IP4
Loopback Address eg. 10.1.1.1/24

Note:
Fields marked with * are required.
Hostname must start with an alphabet letter; special characters ie:'@','.','/','-','_',':', numerical are supported.

IP addresses specified for IP1,IP2,IP3, and IP4 cannot be identical.

Figure 5-3 LAN tab

Step 3 Configure the LAN port connection parameters, as shown in Table 5-1.

Table 5-2 LAN port connection type parameter descriptions

Parameter name	Meaning	How to Configure
Host name	The name of the router.	Manually enter a generic Word type string with a maximum length of 32 bits, for input specifications see the Parameter Specification Table.
IP1～4	Used to delimit molecular networks, which can communicate with each other, IP1-4 represents four subnets.	Enter manually. Format: A . B . C . D/M connector, input specification refer to Parameter Specification Table The IP1 default value is 192.168.8.1 /24, IP2-4 entered in the above format, but the contents between the two cannot be the same.
Loopback address	The virtual interface address of the router, which will not disappear after the LAN interface is configured.	Enter manually. Format: A . B . C . D/M connector, input specification see Parameter Specification Table.

Step 4 Click Save to complete the configuration of the LAN port connection type.

NOTE

When a user modifies an IP1 address, if the page does not automatically tab, make sure that the user's computer has an address on the same network segment as the modified LAN address, or set the computer to automatically acquire the IP, and then enter the new IP1 address in the browser.

---End

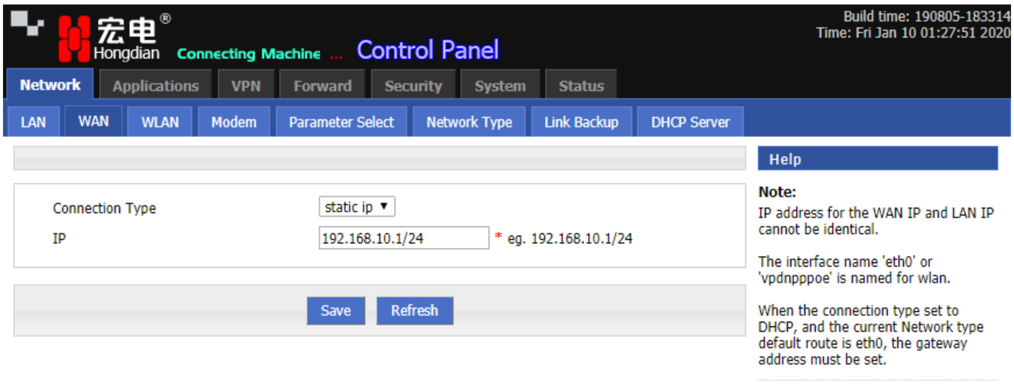
WAN

WAN is mainly used to connect to the Internet over Ethernet, with static IP, DHCP and PPPoE.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Network Settings>WAN.

Open the WAN tab, as shown in Figure 5-4.



Build time: 190805-183314
Time: Fri Jan 10 01:27:51 2020

Connection Type: static ip ▾

IP: 192.168.10.1/24 * eg. 192.168.10.1/24

Note:
IP address for the WAN IP and LAN IP cannot be identical.

The interface name 'eth0' or 'vpdnpppoe' is named for wlan.

When the connection type set to DHCP, and the current Network type default route is eth0, the gateway address must be set.

Figure 5-4 Wan tab

Step 3 Configure the WAN port connection type.

The parameter descriptions are shown in Table 5-2.

table 5-2 WAN port connection type parameter descriptions

Parameter name	Meaning	How to Configure
Connection Type	The connection type of the WAN.	Drop-down box selection, including: • Static IP: Manually configure the interface IP, and if you need to access the network over a WAN, you need to supplement the configuration of the gateway, DNS, default route, and so on in the network connection type. • DHCP: The DHCP client automatically

Parameter name	Meaning	How to Configure
		obtains the IP mode, and if you need WAN access, you need to supplement the default routing configuration in the network connection type. ● Pppoe: pppoe dials for IP mode (usually an external ADSL cat for ADSL dial access), and if you need WAN access, you need to supplement the default routing configuration in the network type type.
IP: Display when Connection Type selects Static IP		
IP	Configuration is required when Connection Type selects Static IP.	Mouth type A.B.C.D/M , Input specification See Parameter Specification Table For example: 192.168.10.1 / 24
Basic Settings: Display when Connection Type selects PPPoE		
Interface name	The unique identifier name of the interface that is used when other functions call or associate this interface, such as configuring the routing of the interface, controlling the disabling and enablement of the rule interface.	PPPoE Unconfigurable item. The PPPoE interface name for the Web page configuration is specified by the system and its interface name is: PPPoE
Service name	Configure the PPPoE service name, which is typically used for identification and judgment between the client and the server, typically provided by the server and provided by an ISP when ADSL is dialed.	General Word type, maximum 64 bytes, cannot be empty, input specification see Parameter Specification Table.
Username/Password	User name/password used for PPPoE dialing, usually provided on the server side, and provided by ISP when ADSL dialing.	General Word type/Code type, each with a maximum length of 64 bytes, is not empty, see the Parameter Specification Table for input specifications.
Advanced Settings	Advanced parameters are used in special cases and are not generally recommended for configuration, as described in the " Advanced Settings " parameter descriptions, see the relevant parameters in Table 5-3.	Click Show to display the advanced settings parameters.

Step 4 Click Save to complete the WAN port connection type configuration.

---End

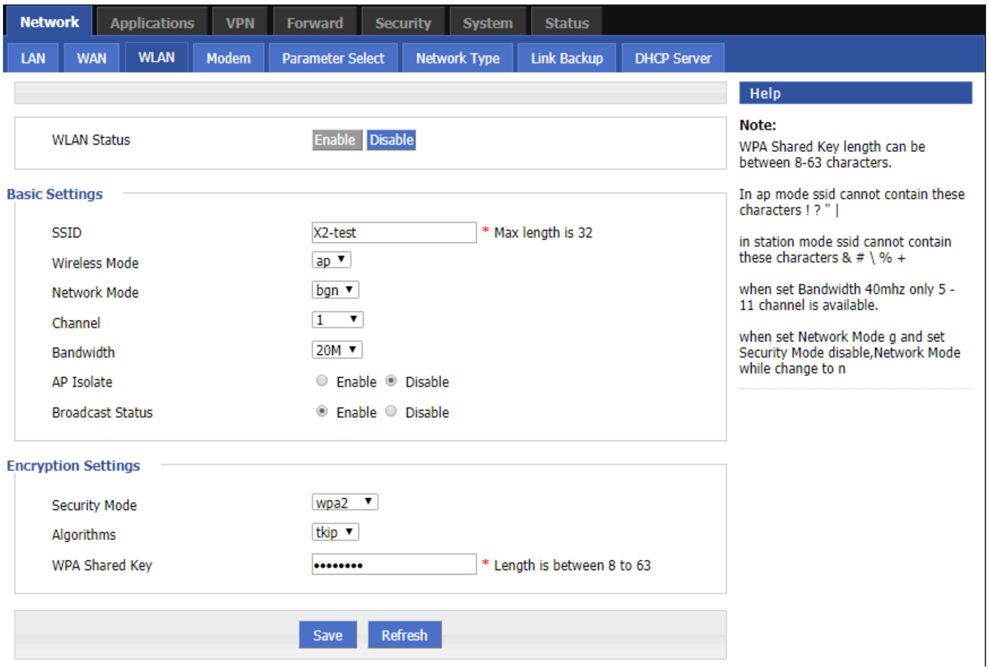
WLAN

The MRR8860 industrial intelligent gateway provides WLAN AP and Station client, through AP function, MRR8860 industrial intelligent gateway can provide wireless LAN hot spot ; The Station client function allows the MRR8860 Industry Smart Gateway to connect to other AP devices so that the subordinate machines of the MRR8860 Industry Smart Gateway can access the external network through the connected AP devices.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2 Click Network Settings>WLAN.

Open the WLAN Configuration tab and when you select a different WLAN working mode (AP, Station), the display pages are shown in Figure 5-10 and Figure 5-11. When the WLAN mode of operation selects Station, the surrounding AP needs to be scanned to select an AP access, as shown in Figure 5-12.



WLAN Status: Enable [✓ Disable]

Basic Settings

SSID: X2-test * Max length is 32

Wireless Mode: ap

Network Mode: bgn

Channel: 1

Bandwidth: 20M

AP Isolate: ○ Enable ● Disable

Broadcast Status: ● Enable ○ Disable

Encryption Settings

Security Mode: wpa2

Algorithms: tkip

WPA Shared Key: •••••••• * Length is between 8 to 63

Note:

WPA Shared Key length can be between 8-63 characters.

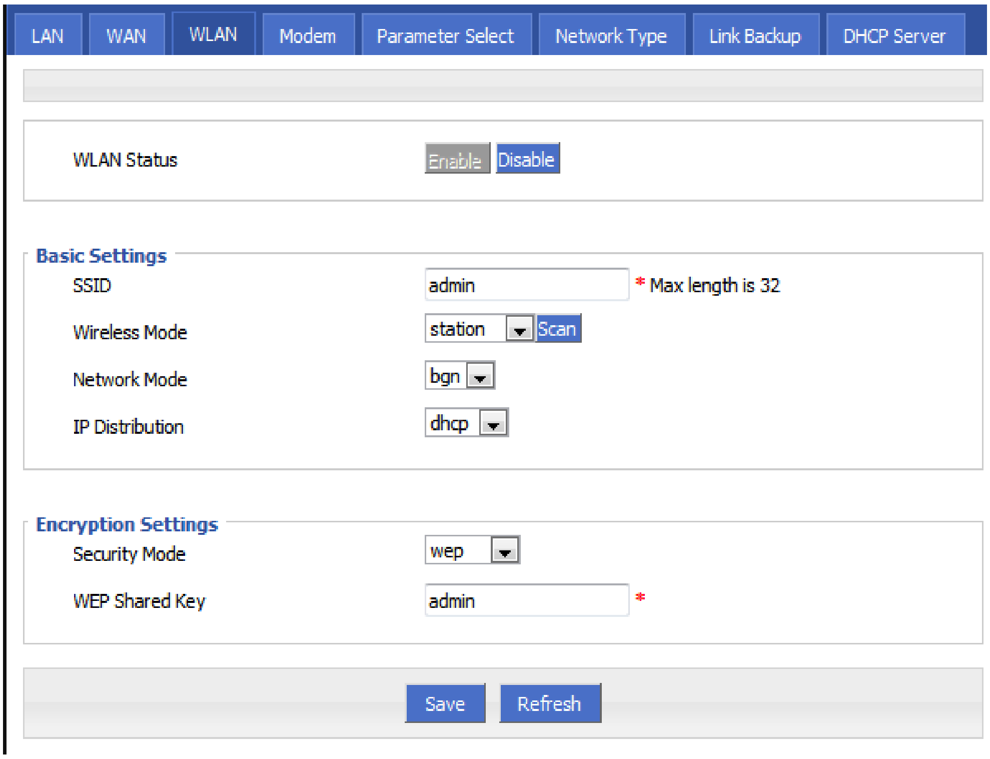
In ap mode ssid cannot contain these characters ! ? " |

in station mode ssid cannot contain these characters & # \ % +

when set Bandwidth 40mhz only 5 - 11 channel is available.

when set Network Mode g and set Security Mode disable,Network Mode while change to n

Figure 5-10 AP mode configuration tab



WLAN Status: Enable Disable

Basic Settings

SSID: admin * Max length is 32

Wireless Mode: station Scan

Network Mode: bgn

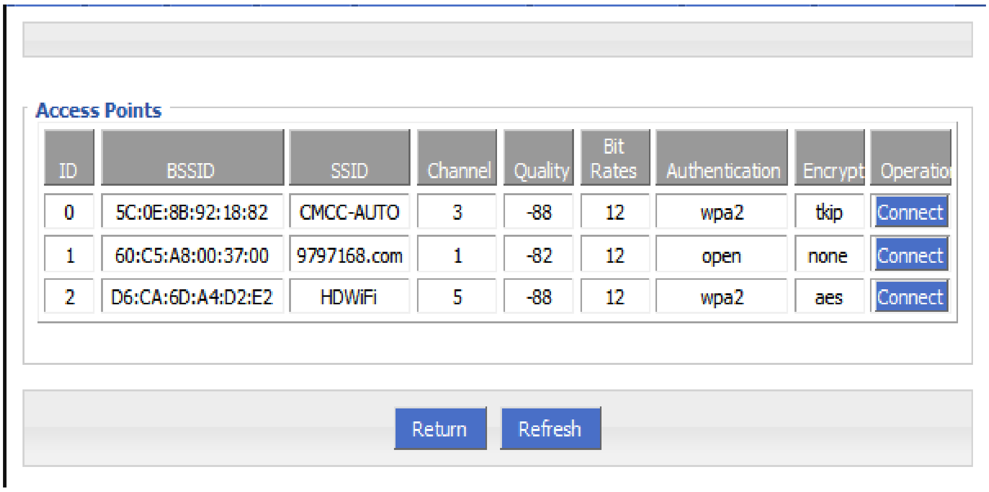
IP Distribution: dhcp

Encryption Settings

Security Mode: wep

WEP Shared Key: admin *

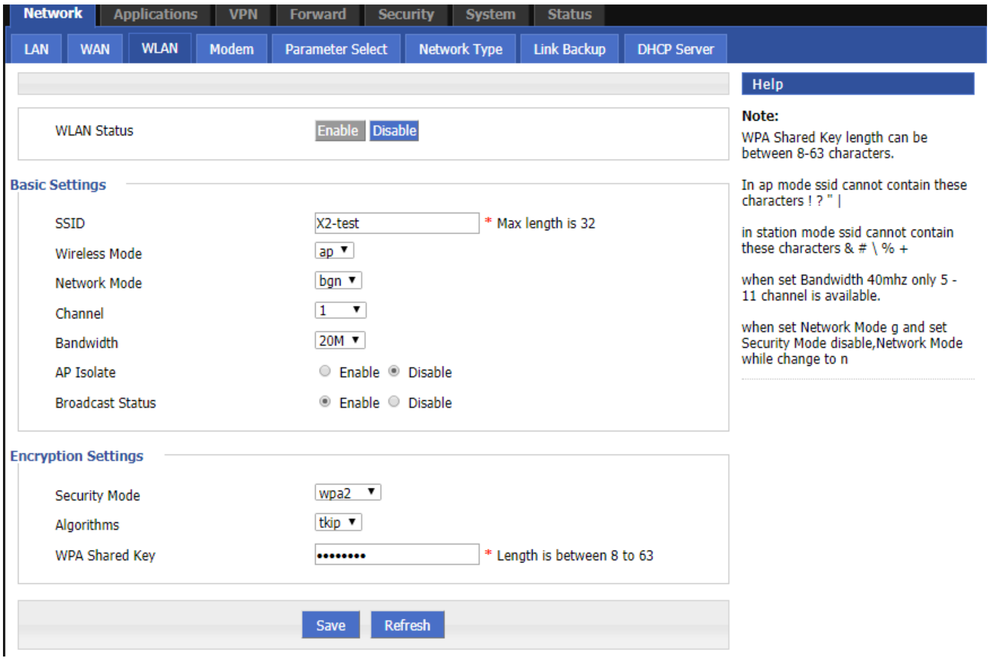
Figure 5-11 Station mode configuration tab


Access Points

ID	BSSID	SSID	Channel	Quality	Bit Rates	Authentication	Encrypt	Operatio
0	5C:0E:8B:92:18:82	CMCC-AUTO	3	-88	12	wpa2	tkip	Connect
1	60:C5:A8:00:37:00	9797168.com	1	-82	12	open	none	Connect
2	D6:CA:6D:A4:D2:E2	HDWiFi	5	-88	12	wpa2	aes	Connect

Figure 5-12 Scan tab when selecting Station

Step 3 Click Network Settings>WLAN_5G. WLAN_5G has only AP mode configuration tabs as shown in Figure 5-13.



WLAN Status Enable Disable

Basic Settings

SSID	X2-test * Max length is 32
Wireless Mode	ap
Network Mode	bgn
Channel	1
Bandwidth	20M
AP Isolate	○ Enable ● Disable
Broadcast Status	● Enable ○ Disable

Encryption Settings

Security Mode	wpa2
Algorithms	tkip
WPA Shared Key	•••••••• * Length is between 8 to 63

Help

Note:

WPA Shared Key length can be between 8-63 characters.

In ap mode ssid cannot contain these characters ! ? " |

in station mode ssid cannot contain these characters & # \ % +

when set Bandwidth 40mhz only 5 - 11 channel is available.

when set Network Mode g and set Security Mode disable,Network Mode while change to n

Figure 5-13 WLAN_5G configuration tab

Step 4 Configure WLAN related parameters.

The parameter descriptions are shown in Table 5-4.

Table 5-4 WLAN Parameter Description

Parameter name	Meaning	How to Configure
WLAN Status	Enable WLAN functionality	Button selection ● Enable ● Disabling
Basic information		
SSID	The WLAN server identity.	General Word type, maximum 32 bytes, input specification see Parameter Specification Table.
Working mode	WLAN working mode, supports AP/Station mode.	Drop-down box option ● ap ● station
Network mode	WLAN network mode, different network mode transmission rates have great differences, the default BGN hybrid mode. When working mode chooses AP, the network mode of AP needs to be set manually. When the working mode selects Station, the network mode is the network mode of the AP selected and cannot be	Drop-down box option ● N indicates that the WLAN rate is 400 Mbps ● bg indicates WLAN speed is 11 Mbps, 54 Mbps adaptive ● bgn indicates a mixed-mode support of 11 Mbps, 54 Mbps, 400 Mbps, adaptive to the WLAN client being accessed

Parameter name	Meaning	How to Configure
	manually modified.	
Working channel	WLAN working channel, according to the specific requirements of the network environment configuration, default AUTO.	Drop-down box option WLAN_2.4G • auto • 1～13 WLAN_5.8G • auto • 149～165 AUTO Presentation Channel Adaptive
Bandwidth	The WLAN works in a bandwidth configuration in 802.11 B/G/N and 802.AC modes.	Drop-down box option WLAN_2.4G • 20MHz • 40MHz High-speed mode with 40 MHz representing 802.11 n WLAN_5G • 20MHz • 40MHz • 80MHz
AP isolation	The WLAN client accessing AP is isolated so that each client cannot access each other.	Radio button selection • Enable • Disabling
Broadcast status	Used to configure whether the WLANSSID is broadcast so that the client can search for the SSID, which is usually disabled if you do not want others to search and use the WLAN function, or disabled to hide the SSID function in a network environment, which the user needs to add manually to connect.	Radio box selection • Enable • Disabling
IP allocation (required when working mode selection station)	The address to communicate with the AP when the MRR8860 Industrial Intelligent Gateway does a Station connection to the AP.	Drop-down box option • dhcp：Obtain an IP address from the DHCP function of the AP • static：Set the IP address manually
IP (required when working mode selects Station)	The address that needs to be configured to communicate with the AP build when IP Assignment selects Static.	Format: Type A.B.C.D, input specification See Parameter Specification Table
WLAN encryption		
Encryption	Configure the encryption mode of	Drop-down box option

Parameter name	Meaning	How to Configure
mode	the WLAN to disable when no encryption validation is required.	● disable ● wpa ● wpa2
WPA/WPA2 (WiFi Protected Access, WiFi Network Secure Access)		
Algorithm	Encryption using algorithm ● tkip ● aes	Drop-down box option selection.
WPA shared secret	The encryption key of the WLAN used to connect to the specified SSID.	Alphanumeric word item, input specification see Parameter Specification Table.

NOTE

When Station is selected for the mode of operation, the MRR8860 industry intelligent gateway automatically matches the corresponding encryption mode and algorithm according to the AP selected (to maintain the same encryption mode as AP) ; The shared key and update interval is filled in with the AP attached key and interval.

---End

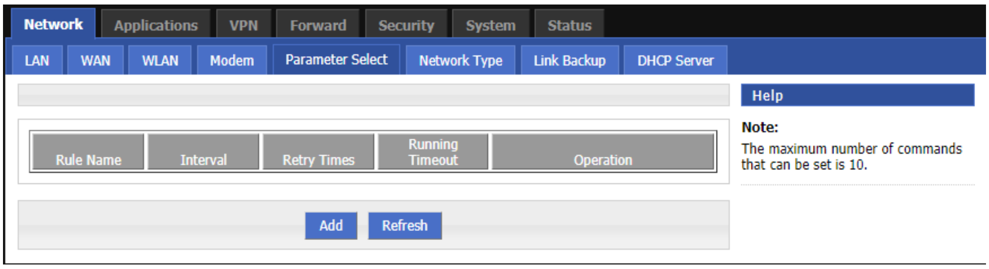
Parameter switching

The MRR8860 industry intelligent gateway parameter switching function is a backup switching function developed by our company. The main application scenarios are: multi-server backup, multi-operator backup (many countries a SIM card supports multiple operators, one operator network exception switches to another operator) and other conflicting networking scenarios that require backup switching between each other.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2 Click Network Settings>Parameter Switching.

Open the Parameter Switch tab, as shown in Figure 5-14.



Note:
The maximum number of commands that can be set is 10.

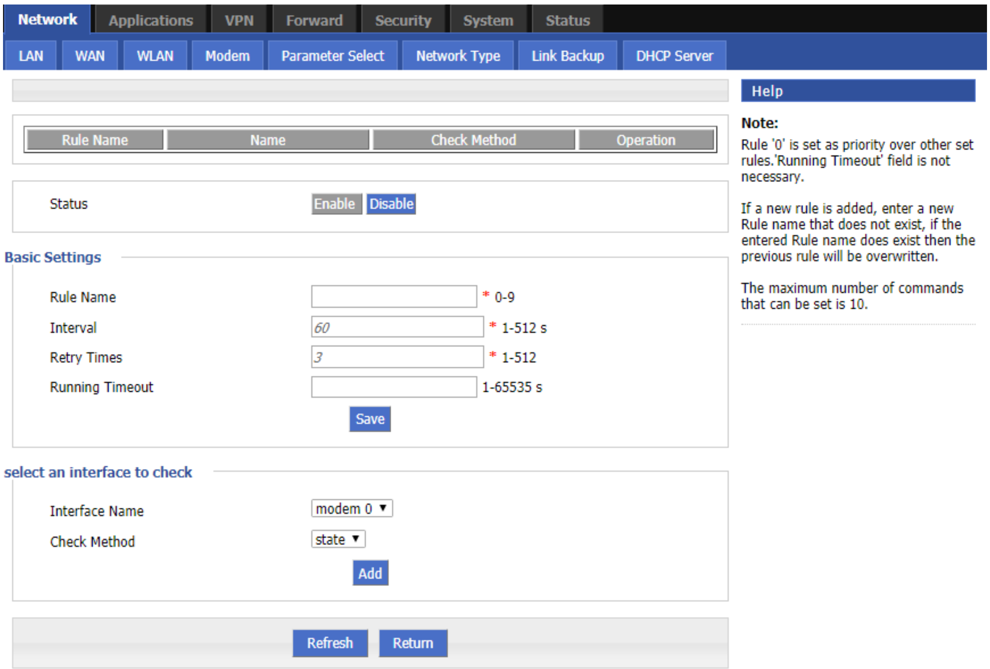
Figure 5-14 Parameter switching tab

Step 5 Configure the Parameter Switch related parameters.

You can add, edit, delete, enable, delete corresponding Parameter Rules.

- Add

1. Click Add to display the Parameter Switch Configuration page, as shown in Figure 5-15.



Status

Basic Settings

Rule Name * 0-9

Interval 60 * 1-512 s

Retry Times 3 * 1-512

Running Timeout 1-65535 s

select an interface to check

Interface Name modem 0

Check Method state

Help

Note:

Rule '0' is set as priority over other set rules.'Running Timeout' field is not necessary.

If a new rule is added, enter a new Rule name that does not exist, if the entered Rule name does exist then the previous rule will be overwritten.

The maximum number of commands that can be set is 10.

Figure 5-15 Parameter switch configuration page

2. Add a Parameter Backup rule.

The parameter descriptions are shown in Table 5-5.

Table 5-7 Parameter switching parameter specification

Parameter name	Meaning	How to Configure
Status	Enables the current rule. Only one rule is running for all enabled rules, and the associated interface in all disabled rules is disabled. For example: MODEM0, IPS1, VPDN2 are selected in Rule 0, MODEM0, IPS1, VPDN2 are disabled if Rule 0 is disabled.	Button selection • Enable • Disabling
Basic information		
Rule Name	Parameter toggles the rule name identifier to distinguish between different rules.	Range of values: [0, 9]
Interval Time/Retry Count	The time interval and maximum number of failures detected. If the number of failures reaches the configured number, switch to the next rule to work.	Range of values: 1-512 Unit: Seconds/Times Default: 60 / 3

Parameter name	Meaning	How to Configure
Timeout time	Used to qualify the maximum working time of the current rule, which is not valid in Rule 0, configured in other rules and switched to Rule 0 after the maximum working time has been reached, and not configured to switch in the order of Rule. Configuration is generally not recommended without strict master and slave requirements.	Range of values: 1-65535 Unit: Seconds
Add Interface Detection Rule		
Interface name	The rule association parameter interface name, such as MODEM interface name: 0 MODEM.	Drop-down box option, automatically generated depending on the current number of system configuration interface names.
Detection method	Detection methods are divided into interface state detection and ICMP detection, which determine whether switching to the next rule is required by checking the status or link (after the maximum number of failures is reached).	Drop-down box option ● state ● icmp
Destination IP	Configuration is required to select the ICMP detection method to configure the ICMP detection destination address.	For input specifications, please refer to the Parameter Specification Table. For example: 192.168.8.2

3. Click Add to finish adding the rule.

- Delete

  Click Delete to delete the selected Parameter Switch Rule.

- Enable

  Click Enable to start and apply the Parameter Switch Rule.

- Disabling

  Click Disable to disable the Parameter Switch Rule.

- Refresh

  Click Refresh to refresh the current page.

NOTE

When using both parameter switching and link backup functions, ensure that the two functions use different interface categories. If you need to use, please contact our technical support staff.

---End

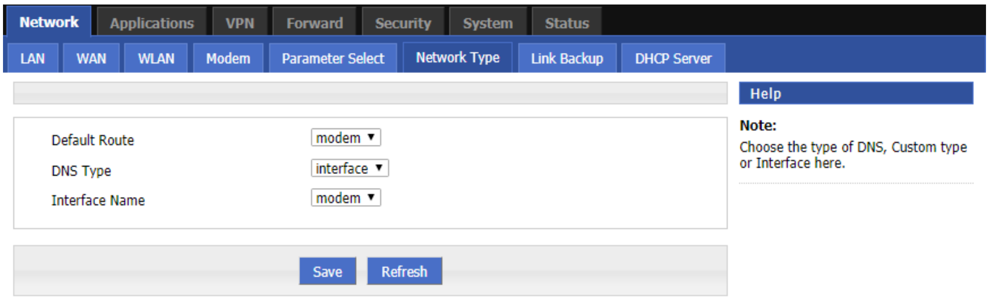
Network connection

Provides users with a default routing configuration page.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2 Click Network Settings>Network Connections.

Open the Network Connections tab, as shown in Figure 5-16.



Default Route modem ▾
DNS Type interface ▾
Interface Name modem ▾

Note:
Choose the type of DNS, Custom type or Interface here.

Figure 5-16 Network connection tab

Step 3 Configure the Network Connection related parameters.

The parameter descriptions are shown in Table 5-6.

Table 5-8 Network Connection Parameter Description

Parameter name	Meaning	How to Configure
Default route	The default forwarding path for router packets. Configure the default route according to your specific needs, and when you need a multi-network switch, see Link Backup.	Drop-down box option Configure as needed.
Gateway	When the WAN port is selected by default and the WAN is a static IP, you need to configure the next hop gateway address for the WAN port address and, if you need to access the domain name, customize the configuration DNS.	For input specifications, please refer to the Parameter Specification Table. For example: 192.168.10.254
DNS type	Configure the DNS type of router, use interface dialing when selecting the interface to automatically get DNS, if you want to set DNS manually for WAN static IP.	Drop-down box option ● interface ● custom
DNS1/DNS2	DNS type is configured when Custom is selected, DNS addresses are manually configured, up to two can be configured.	Connector type A.B.C.D For example: 8.8.8.8
Interface name	The DNS type is configured when selecting an interface, and the router is configured to use the DNS associated interface to obtain the DNS, so special attention needs to be paid to whether the interface can obtain	Drop-down box option ● modem ● eth0 ● wlan0

Parameter name	Meaning	How to Configure
	DNS.	Eth0 indicates DNS obtained by the associated WAN port pppoe dial or DHCP, paying special attention to the invalid selection of eth0 when WAN static IP, the invalid selection of MODEM when PPP dial configuration disables peer DNS, and the WLAN 0 indicates the DNS obtained by WLAN.

Step 4 Click Save to complete the configuration of the network connection.

NOTE

When " Default Routing " selects the " eth0 " interface and the WAN port is switched from DHCP or static IP to PPPoE, the router's default route needs to click " Save " on the Network Connections page to display and take effect.

---End

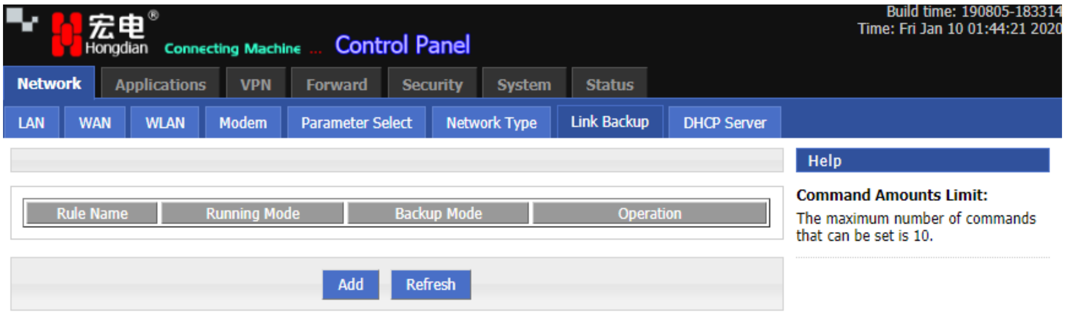
Link backup

The MRR8860 industrial intelligent gateway can realize the backup function of multi-network link according to the actual needs of customers, can realize the alternate switch between wireless and wireless, wireless and wired link, can quickly switch to backup link in case of a link failure, and guarantee the connectivity and stability of the communication link of the lower computer, thus guarantee the user data service is not affected. The MRR8860 Industrial Intelligent Gateway supports two main backup modes: cold and hot . The advantage of hot backup is that it can communicate directly after the link is switched.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2 Click Network Settings>Link Backup.

Open the Link Backup tab, as shown in Figure 5-17.



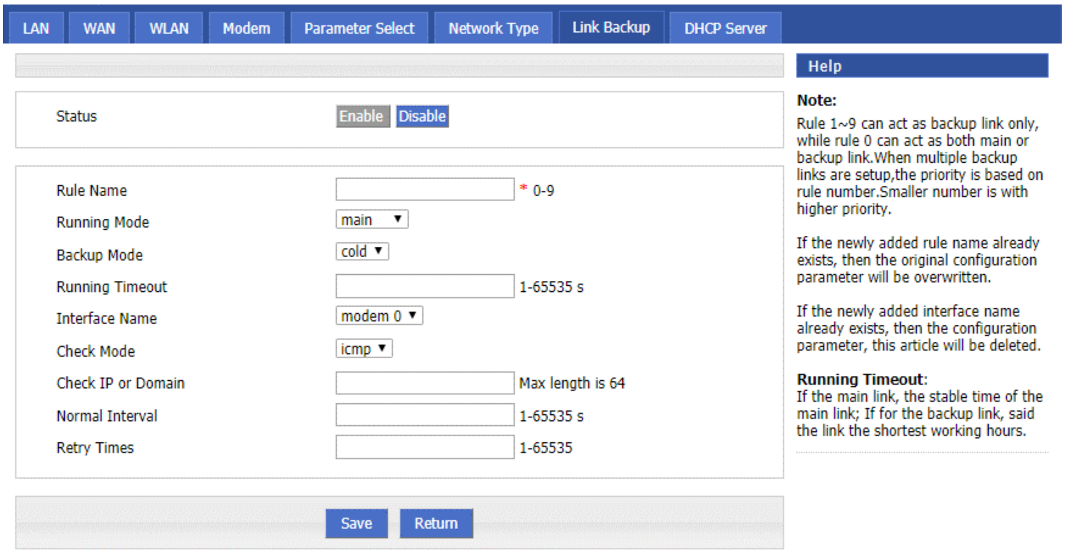
Rule Name	Running Mode	Backup Mode	Operation

Command Amounts Limit:

The maximum number of commands that can be set is 10.

Figure 5-17 Link backup tab

Step 3 Click Add to open the Add Link Backup rule page, as shown in Figure 5-17.



Status Enable Disable

Rule Name * 0-9

Running Mode main

Backup Mode cold

Running Timeout 1-65535 s

Interface Name modem 0

Check Mode icmp

Check IP or Domain Max length is 64

Normal Interval 1-65535 s

Retry Times 1-65535

Note:
Rule 1~9 can act as backup link only, while rule 0 can act as both main or backup link.When multiple backup links are setup,the priority is based on rule number.Smaller number is with higher priority.

If the newly added rule name already exists, then the original configuration parameter will be overwritten.

If the newly added interface name already exists, then the configuration parameter, this article will be deleted.

Running Timeout:
If the main link, the stable time of the main link; If for the backup link, said the link the shortest working hours.

Figure 5-18 Link Backup Rule Add Page

Step 4 Configure the Link Backup related parameters.

The parameter descriptions are shown in Table 5-7.

Table 5-7 Link backup parameter descriptions

Parameter name	Meaning	How to Configure
Status	Enables link backup functionality.	Button ● Enable ● Disabling
Rule Name	Link Backup Rule Name ID Explain Can be a primary link or a backup link ; Only 1-9 can be a backup link ; The backup link 1-9 determines the priority based on the number size, the smaller the number, the higher the priority.	Range of values: 0-9
Link operation mode	Backup mode, including: ● main：Link mode is the primary link. ● backup：The link mode is a backup link.	Drop-down box selection.

Parameter name	Meaning	How to Configure
Backup mode	Backup mode with cold and hot backups. Hot backup refers to the corresponding link processing enabled state, the advantages of hot backup is fast switching, the disadvantage is that when the link is online will increase network overhead and tariff costs. A cold backup is when only the interface of the current work link is enabled. Other interfaces that are not working are offline.	Drop-down box option • cold • hot
Timeout time	• If the current link is the primary link, indicates the primary link stability time. • If the current link is a backup link, it indicates the minimum working time for the link. Explain Timeout applies only to primary and secondary switches.	Range of values: 1-65535 Unit: Seconds
Interface name	Interface for link switching.	The following options are available: • modem 0 • wlan0 • eth0
Detect IP or domain name	Ping packet mode detects IP address or domain name, ping does not determine detection failure.	Word type, maximum 64 bytes, input specification see Parameter Specification Table.
Detection interval/retransmission times	Link normal detection interval and maximum number of failures. The link is switched when the maximum number of failures is reached.	Range of values: 1-65535 Unit: Seconds/Times

Step 5 Click Save to complete the link backup configuration.

NOTE

When the link backup function is enabled, the default route of the router is the default route of the link backup rule ;
When the link backup is the main standby switch, as long as the main link detection is successful, immediately switch to the main link ;

---End

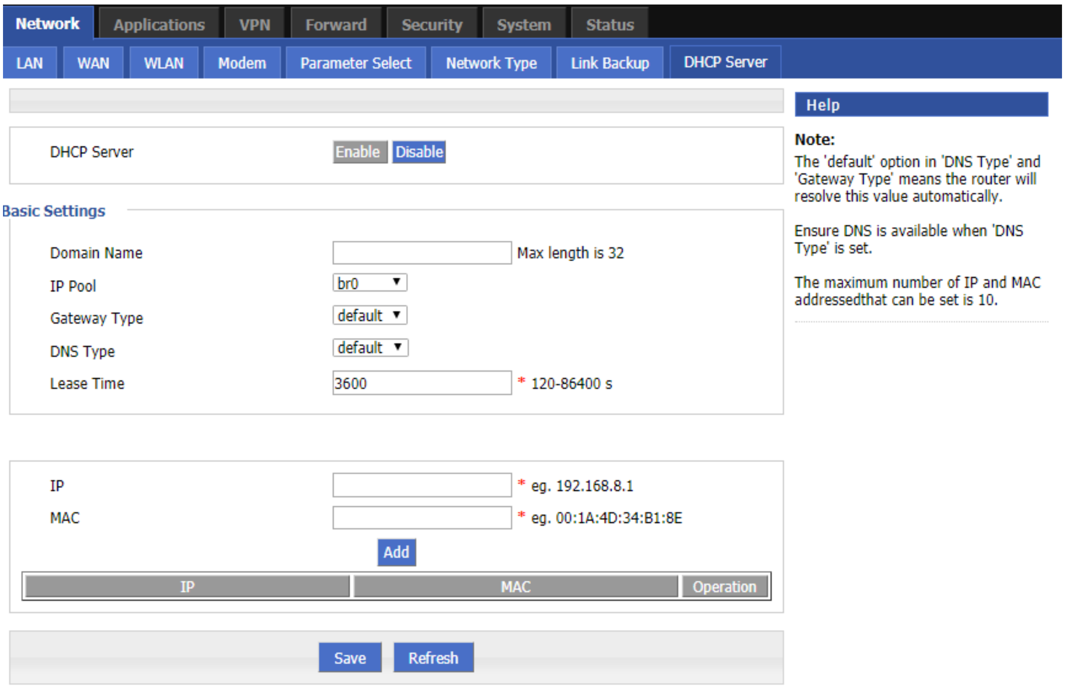
DHCP service

The Dynamic Host Configuration Protocol (DHCP) is a network protocol for a LAN. When DHCP is enabled, the next function automatically obtains the dynamic IP.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Network Settings>DHCP Service.

Open the DHCP Service tab, as shown in Figure 5-19.



Help

Note:
The 'default' option in 'DNS Type' and 'Gateway Type' means the router will resolve this value automatically.

Ensure DNS is available when 'DNS Type' is set.

The maximum number of IP and MAC addressedthat can be set is 10.

DHCP Server: Enable | Disable

Basic Settings

Domain Name: Max length is 32

IP Pool: br0

Gateway Type: default

DNS Type: default

Lease Time: 3600 * 120-86400 s

IP: * eg. 192.168.8.1

MAC: * eg. 00:1A:4D:34:B1:8E

Figure 5-19 DHCP service tab

Step 3 Configure DHCP Server Settings.

The DHCP server settings parameters are shown in Table 5-8.

Table 5-8 DHCP Server Setup Parameter Description

Parameter name	Meaning	How to Configure
DHCP service	DHCP service enable button to enable/disable DHCP service.	Button Select Settings. • Enable • Disabling
Basic settings (DHCP is not recommended without special networking requirements)		
Address pool	DHCP client gets the range of IP addresses. When you select an interface, represents the network segment of the associated interface. This option is typically configured when you need to specify a range of addresses that the subordinate machine can assign, for	Drop-down box option • br0 • custom

Parameter name	Meaning	How to Configure
	example, you want to automatically acquire IP for up to four machines.	
Start IP	The address pool is configured when Custom is selected and the starting IP address of the DHCP address pool is configured.	For input specifications, please refer to the Parameter Specification Table. For example: 192.168.8.2
End IP	The address pool is configured when Custom is selected and the end IP address of the DHCP address pool is configured.	For input specifications, please refer to the Parameter Specification Table. For example: 192.168.8.254
Gateway type	The gateway IP source obtained by the DHCP client is divided into DEFAULT, BR0, ETH0, CUSTOM, and when the interface is associated, the IP of the interface is assigned to the DHCP client as the gateway.	Drop-down box option Default: default
Gateway	The gateway type is configured when you select Custom, which is typically used when specifying the next machine gateway IP.	For input specifications, please refer to the Parameter Specification Table. For example: 192.168.8.1
DNS type	The source of the DNS IP obtained by the DHCP client is DEFAULT, MODEM, ETH0, BR0, CUSTOM, etc. This configuration is not generally recommended, especially in dual-mode application scenarios.	Drop-down box option • default • modem • eth0 • br0 • custom Configured as default is assigned based on the DNS address of the router itself.
DNS1/DNS2	Configured when DNS Type Select Custom, configure the DHCP client to obtain the IP address of the DNS.	For input specifications, please refer to the Parameter Specification Table. For example: 8.8.8.8
Lease Time	After the DHCP client obtains the IP, the IP rental time is usually renegotiated by the client at the middle of the lease time to obtain the IP address. Lease time is primarily used to free up idle IP and avoid IP address resources after a DHCP client shutdown.	Range of values: 120-86400 Unit: Seconds The default value is 3600
An IP, MAC binding that is used to assign a fixed IP address to a machine in a specified range		
IP	Paired with the specified MAC, when a DHCP request is made by the DHCP	For input specifications, please refer to the Parameter

Parameter name	Meaning	How to Configure
	client of the bound MAC, the IP address that is bound to the MAC address is assigned to it. The IP address assignment is not assigned to another MAC address even if it is not occupied.	Specification Table. For example: 192.168.8.2
MAC	Configure the MAC address of the DHCP client that requires DHCP to obtain IP.	WORD type MAC format For example: 00: 1A: 4D: 34: B1: 8E

---End

5.3 Application Configuration

The MRR8860 industrial intelligent gateway has developed many functions for wireless network products, including ICMP link detection, M2M terminal management, task management, etc.

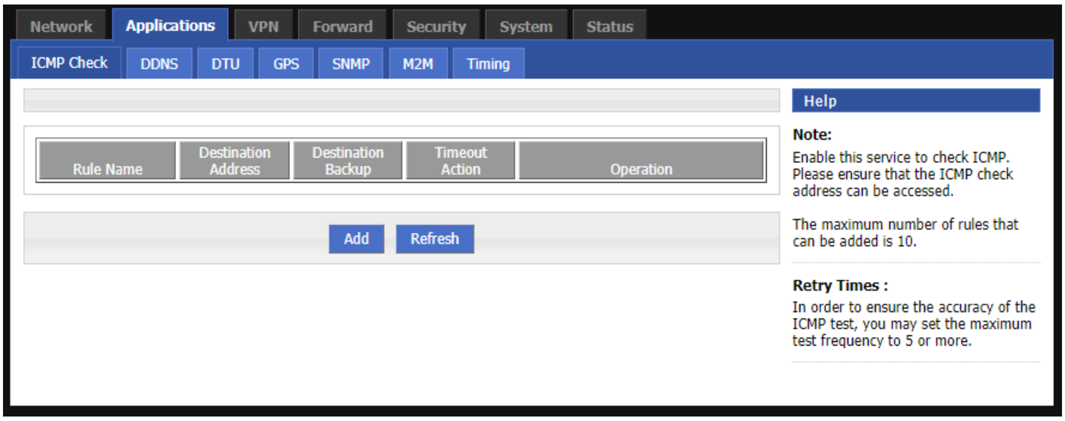
5.3.1 ICMP Detection

There are anomalies in the wireless network such as false links (dial for IP, but no link), which are usually maintained by means such as LCP, and the MRR8860 Industrial Intelligent Gateway provides more reliable ICMP link detection in addition to this detection. ICMP detection mainly detects the communication link through ping packet detection, performs the user set action when detecting the link exception, realizes the link and the system fast recovery. ICMP link detection is mainly used to detect wireless links at the beginning of design . The MRR8860 Industrial Intelligent Gateway supports detection of tunnel links such as VPN, multi-rules simultaneous detection and up to 10 ICMP detection rules.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Application Settings>ICMP Detection.

Open the ICMP Detection tab, as shown in Figure 5-20.



Note:
Enable this service to check ICMP. Please ensure that the ICMP check address can be accessed.

The maximum number of rules that can be added is 10.

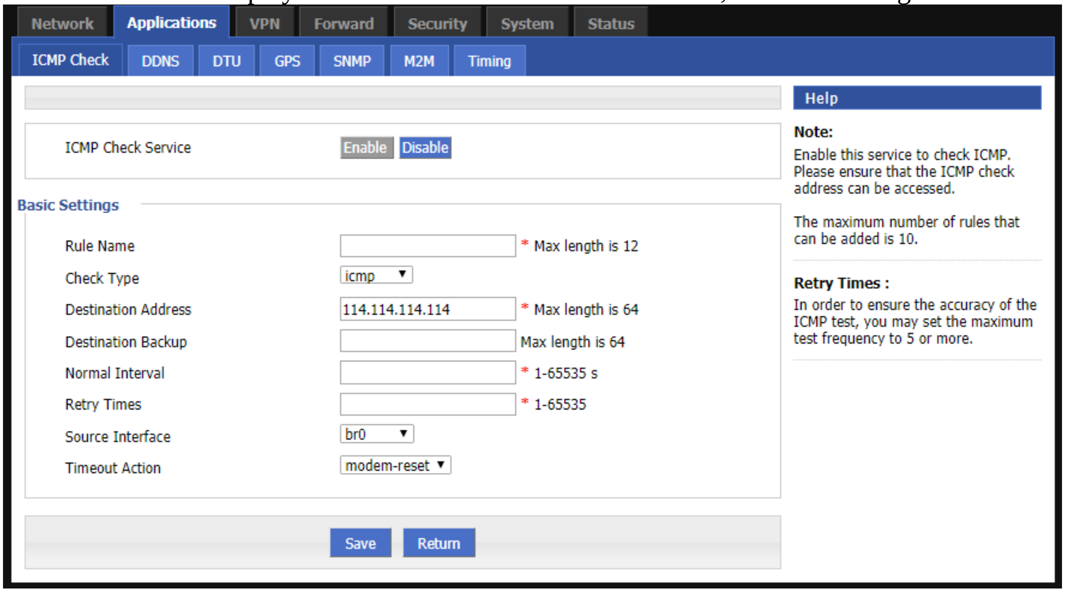
Retry Times :
In order to ensure the accuracy of the ICMP test, you may set the maximum test frequency to 5 or more.

Figure 5- 20 ICMP detection page

Step 3 Add, edit, delete, enable, and disable ICMP Detection.

- Add

1. Click Add to display the add interface for ICMP Detection, as shown in Figure 5-21.



ICMP Check Service [Enable] [Disable]

Basic Settings

Rule Name		* Max length is 12
Check Type	icmp	
Destination Address	114.114.114.114	* Max length is 64
Destination Backup		Max length is 64
Normal Interval		* 1-65535 s
Retry Times		* 1-65535
Source Interface	br0	
Timeout Action	modem-reset	

Note:
Enable this service to check ICMP. Please ensure that the ICMP check address can be accessed.

The maximum number of rules that can be added is 10.

Retry Times :
In order to ensure the accuracy of the ICMP test, you may set the maximum test frequency to 5 or more.

Figure 5-21 ICMP Add Page

2. Configure ICMP detection service parameters.

The parameter descriptions are shown in Table 5-9.

Table 5-9 ICMP Detection Rule Parameter Description

Parameter name	Meaning	How to Configure
Detection service	Enables ICMP detection rules. Multiple rules can run simultaneously or a rule can be disabled.	Button ● Enable ● Disabling
Basic Settings		
Rule Name	The ICMP detection rule name identifier, which has no specific meaning, is used only to distinguish between different rules.	Word type, maximum 12 bytes, input specification see Parameter Specification Table.
Destination address	ICMP detects the destination address, either IP or domain name, and is set to the domain name to ensure that the router is configured with the correct DNS.	Word type, maximum 64 bytes, input specification see Parameter Specification Table.
Backup address	ICMP detects the backup destination address and detects the backup address when the primary address fails	Word type, maximum 64 bytes, input specification see Parameter

Parameter name	Meaning	How to Configure
	detection.	Specification Table.
Detection interval/retransmission times	The detection interval and maximum number of failures when the link is normal. The maximum number of failures arrives to perform action tasks corresponding to ICMP rules, such as modem redial, and so on.	Range of values: 1-65535 Unit: Seconds/Times
Source interface	The source address where the router sends an ICMP sense packet	Drop-down box option • br0 • modem
Timeout action	When the detection failure reaches the maximum number of failed actions, mainly re-dial, custom actions.	Drop-down box options. • modem-reset：modem modem redial • custom：Custom actions
Execute command	Configured when the timeout action selects Custom, the command is a background action command, which is generally not recommended. Please contact our technical staff if necessary.	Word type, maximum 64 bytes, input specification see Parameter Specification Table.

3. Click Save to complete the addition of an ICMP detection rule.

NOTE

ICMP is normally sent at ICMP detection intervals, and if an exception occurs, ICMP packets are sent continuously according to abnormal ICMP detection immediately . If the detection destination address is not valid, the backup address is detected. If the number of times a backup address cannot be detected also reaches the number of retransmissions, the router performs a timeout action.

- Edit

  As shown in Figure 5-20, you can edit a parameter configuration record by clicking Edit. The parameter descriptions are shown in Table 5-9.

- Delete

  As shown in Figure 5-20, you can delete a parameter configuration record by clicking Delete.

- Enable

  As shown in Figure 5-20 to determine a parameter configuration record, click Enable to enable the parameter configuration.

- Disabling

  As Figure 5-20 identifies a parameter configuration record, click Disable to disable the parameter configuration to take effect.

- Refresh

Click Refresh to refresh the current page.

---End

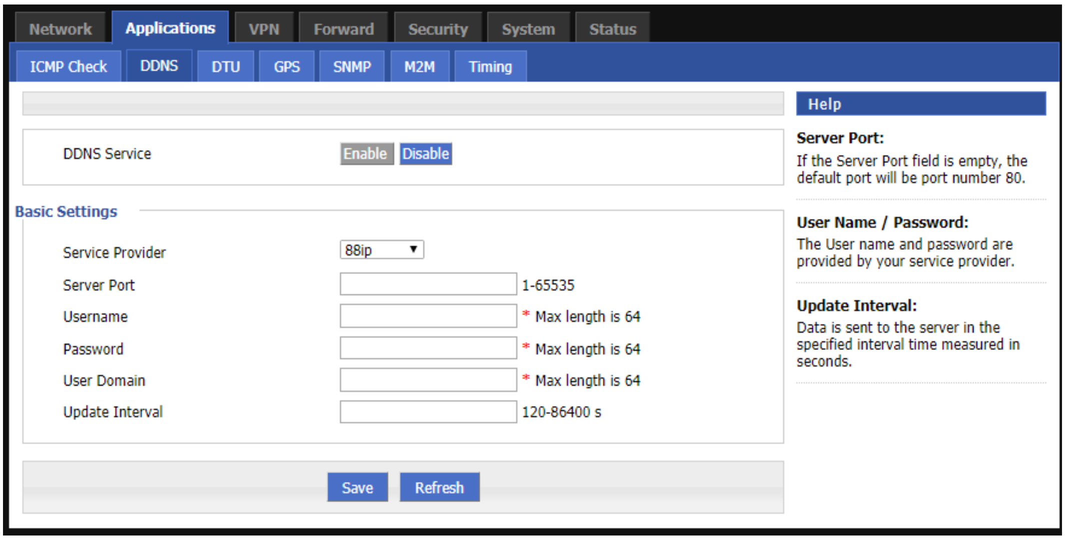
5.3.2 DDNS settings

DDNS is the abbreviation of the dynamic domain name system, the DDNS protocol provides the corresponding query function between the dynamic IP and the domain name. DDNS allows users to access the router's pages through the domain name on any PC that can connect to the public network. Of course, the network corresponding to the SIM card used by the router must be a public network accessible address, so that the input domain name can access the router.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Application Settings>DDNS Settings.

Open the DDNS Settings tab, as shown in Figure 5-22.



DDNS Service

Basic Settings

Service Provider 88ip

Server Port 1-65535

Username * Max length is 64

Password * Max length is 64

User Domain * Max length is 64

Update Interval 120-86400 s

Server Port:
If the Server Port field is empty, the default port will be port number 80.

User Name / Password:
The User name and password are provided by your service provider.

Update Interval:
Data is sent to the server in the specified interval time measured in seconds.

Figure 5-22 Dns settings tab

Step 3 Configure the DDNS service parameters.

The parameter descriptions are shown in Table 5-10.

Table 5-13 DDNS service parameter descriptions

Parameter name	Meaning	How to Configure
DDNS service	Enables the DDNS service.	Button • Enable • Disabling
Basic Settings		
Service provider	The domain name of the application corresponds to the domain name provider option, we currently do not support the list of domain name providers DDNS service.	Drop-down box option • 3322 • 88ip • Dnsexit • Dyndns

Parameter name	Meaning	How to Configure
		• Zoneedit • changeip • custom
Service Address	The service provider configures when Custom is selected, when the DDNS server is built, the custom defaults to the standard DDNS protocol, and if configured, contact our technician to customize the protocol.	General Word type, maximum 64 bytes, input specification see Parameter Specification Table.
Service port	The DDNS server port number of the domain name service provider, which is typically 80 by default, is typically not 80 when customizing the DDNS service.	Range of values: 1-65535 Unconfigured indicates port 80 .
Username/Password	The user name and password when registering the DDNS service provider domain name.	General Word type/Code type, up to 64 bytes.
User domain name	The domain name provided by the DDNS service provider that corresponds to the IP of the router, typically by accessing the domain name to access the router's IP.	Generic Word type, up to 64 bytes.
Update Interval	When the router updates the IP address to the DDNS domain name service provider, if this parameter is set, the router reports the IP address according to the Update Interval ; If not set, the IP address is escalated to the domain name provider when the IP address changes.	Range of values: 120-86400 Unit: Seconds

Step 4 Click Save to complete the DDNS service configuration.

NOTE

- Domestic DDNS service providers: 88 IP (www.88ip.net), 3322 (www.3322.org)
- CHANGEIP(www.changeip.com)、DYNDNS(www.members.dyndns.org)
- DDNS service providers abroad: DNSExit （wwwwwwww．dnsexit．com），ZoneEdit （wwwww．Zoneedti．com），ChangeIP （wwwww．changeip．com），DynDNS （wwwwwww．members．dyndns．org）
- The IP address obtained from the SIM/UIM card service provider changes each time the router restarts. If the user is using the requested DDNS domain name when logging on to the router remotely, the user can log on to the router page no matter how the router MODEMIP address changes.

---End

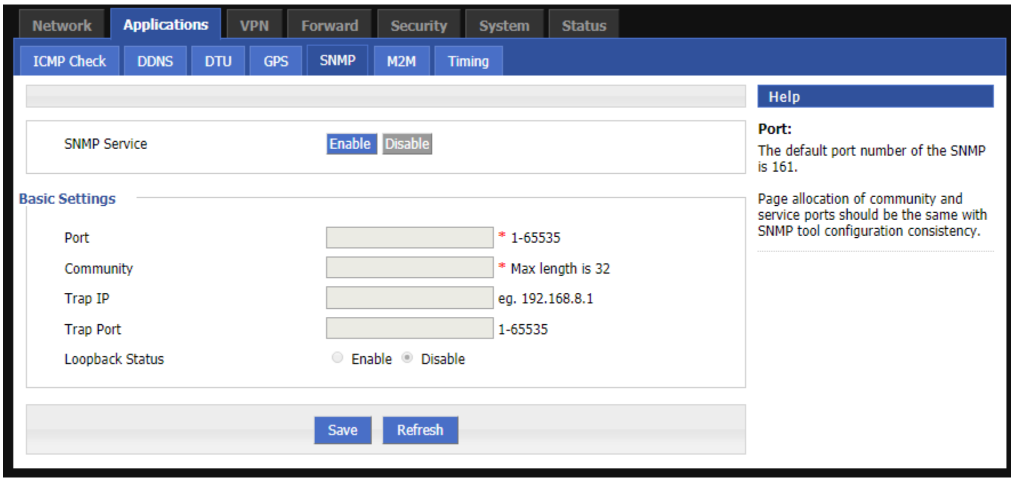
5.3.3 SNMP Configuration

SNMP (Simple Network Management Protocol) Simple Network Management Protocol (Simple Network Management Protocol) is a simple network management protocol that, when enabled, enables remote monitoring of devices using the SNMP management tool to view the operational status of devices (state viewing such as VPN support requires importing into our MIB library).

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Application Settings>SNMP Configuration.

Open the SNMP Configuration tab, as shown in Figure 5-23.



SNMP Service: Enable Disable

Basic Settings

Port		* 1-65535
Community		* Max length is 32
Trap IP		eg. 192.168.8.1
Trap Port		1-65535
Loopback Status	○ Enable ● Disable	

Port:
The default port number of the SNMP is 161.

Page allocation of community and service ports should be the same with SNMP tool configuration consistency.

Figure 5-23 SNMP Configuration tab

Step 3 Configure SNMP parameters.

The parameter descriptions are shown in Table 5-11.

Table 5-11 SNMP parameter descriptions

Parameter name	Meaning	How to Configure
SNMP service	Enables the SNMP service.	Radio button selection. • Enable • Disabling
Basic Settings		
Service port	The SNMP service listens on port, which is recommended to be configured as its default port 161 .	Range of values: 1-65535 Default: 161
Community	The community password for the SNMP client connection router SNMP service for identity recognition.	Word type, up to 16 bytes, input specification see Parameter Specification Table.
Trap IP	The server address to which the router link status is escalated.	Format: A . B . C . D connector, input specification refer to the

Parameter name	Meaning	How to Configure
		Parameter Specification Table.
Trap port	The server port for which the router link status is escalated.	Range of values: 1-65535 Default: 162
Loopback identification status	Corresponds to the loopback address on the LAN page: Enabled in the loopback ID status, and if the loopback address is successfully configured, the IP packet source address reported by the router TRAP is the loopback address ; If the loopback ID status is Disabled, the IP packet source address reported by the router TRAP is the LAN port address.	Radio button selection • Enable • Disabling

Step 4 Click Save to complete the SNMP configuration.

NOTE

Trap: One of the five data types of the SNMP protocol, which refers to a trap message that is reported by the managed device, indicating a notification that the device has failed or changed. The types and contents of the TRAP reported by the MRR8860 Industrial Intelligent Gateway include: the connection status of the MODEM, which interface, which SIM card to dial, the connection and disconnection of the VPDN/tunnel/IPsec interface, and so on.

The MIB library corresponding to SNMP can be downloaded on our website . If necessary, please contact our technician.

---End

5.3.4 M 2 M Configuration

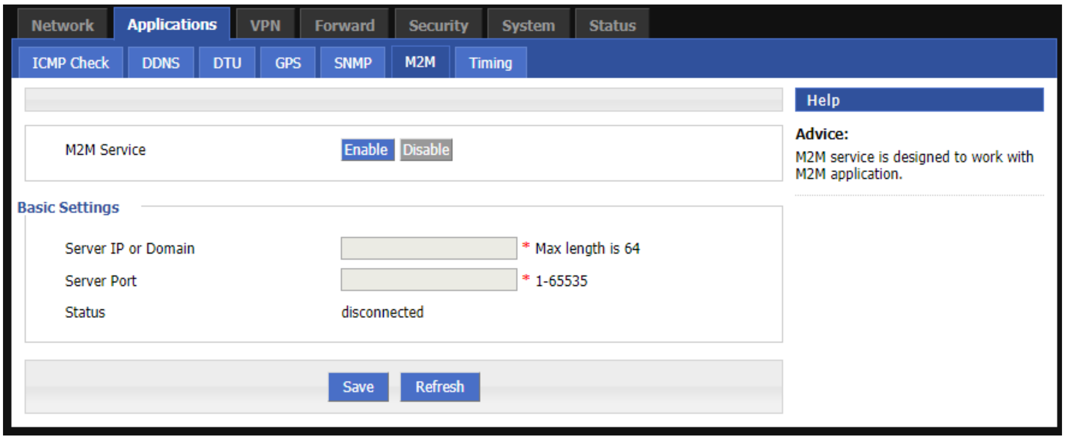
The MRR8860 Industrial Intelligent Gateway communicates with the M2M (Machine-to-Machine) platform through the Wireless Machine-to-Machine Protocol, which enables remote maintenance management of the device and monitoring of the network status on site, such as viewing device information, upgrading patches, upgrading firmware, configuration parameters, etc. The specific settings are described below.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Application Settings>M2M Configuration.

Open the M2M Configuration tab, as shown in Figure 5-24.

Figure 5-24 M 2 M Configuration Tab



M2M Service Enable Disable

Advice:
M2M service is designed to work with M2M application.

Basic Settings

Server IP or Domain		* Max length is 64
Server Port		* 1-65535
Status	disconnected	

Step 3 Configure the M2M parameter.

The parameter descriptions are shown in Table 5-12.

Table 5-15 M 2 M Parameter Description

Parameter name	Meaning	How to Configure
M 2 M Service	To enable M2M service, this function needs to be used with our M2M terminal management platform.	Button ● Enable ● Disabling
Basic Settings		
Service IP or domain name	The IP address or domain name of the appliance cloud platform server.	Word type, up to 64 bytes, input specification see Parameter Specification Table.
Service port	The port number used by the device cloud platform server WMMMP service to match the server.	Range of values: 1-65535
Number of Logins	The maximum number of retries for the router login device cloud platform, and if the maximum number is reached, restart the M2M function to reinitialize and log in again.	Range of values: 1-5 Unit: Secondary
Heartbeat interval	In addition to the time between the heartbeat packets sent by the router and the device cloud platform to maintain the connection, the heartbeat packet also includes the network state data of the router to update the real-time network state data of the device cloud platform.	Range of values: 1-65535 Unit: Seconds

Parameter name	Meaning	How to Configure
Retransmission times	All data packet interactions between the router and the device cloud platform have retransmission mechanism . When the number of retransmissions arrives, the interaction is judged to have failed.	Range of values: 1-5 Unit: Secondary
Timeout time	The retransmit judgment time of all data packet interactions between router and device cloud platform, and the data interaction time out and data retransmit when there is no reply.	Range of values: 1-65535 Unit: Seconds

Step 4 Click Save to complete the M2M configuration.

---End

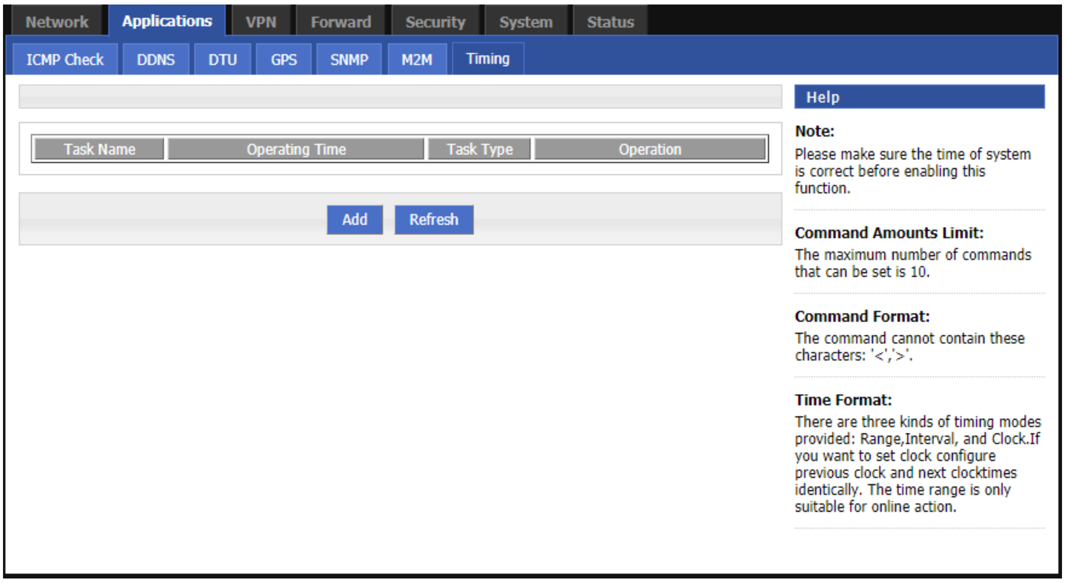
5.3.5 Task Management Settings

MRR8860 industrial intelligent gateway task management can provide users with router online time, timing task execution and other functions. Customers can configure multiple online time periods (such as hours of a day), set up task execution at a certain point in time, and so on, as required (such as redialing at midnight every day or restarting the system). Supports up to 10 task rules.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Application Settings>Task Management.

Open the Task Management tab, as shown in Figure 5-25.



Note:
Please make sure the time of system is correct before enabling this function.

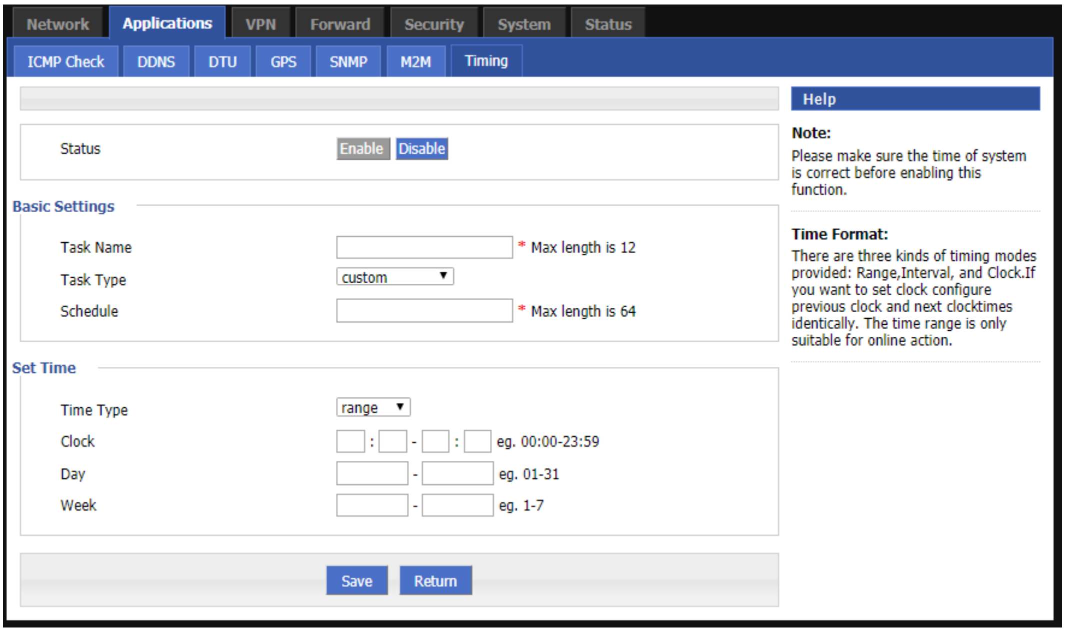
Command Amounts Limit:
The maximum number of commands that can be set is 10.

Command Format:
The command cannot contain these characters: '<','>'.

Time Format:
There are three kinds of timing modes provided: Range,Interval, and Clock.If you want to set clock configure previous clock and next clocktimes identically. The time range is only suitable for online action.

Figure 5-25 Time period management settings tab

Step 3 : To add a new task management rule, click Add to enter the task management rule settings interface, as shown in Figure 5-29.



Status Enable Disable

Basic Settings

Task Name * Max length is 12

Task Type custom

Schedule * Max length is 64

Set Time

Time Type range

Clock : - : eg. 00:00-23:59

Day - eg. 01-31

Week - eg. 1-7

Note:
Please make sure the time of system is correct before enabling this function.

Time Format:
There are three kinds of timing modes provided: Range,Interval, and Clock.If you want to set clock configure previous clock and next clocktimes identically. The time range is only suitable for online action.

Figure 5-26 Task management configuration interface

Step 4 Configure task management rule parameters.

The parameter descriptions are shown in Table 5-13.

Table 5-13 Task Management Rule Parameter Description

Parameter name	Meaning	How to Configure
Status	Enables timing rules. Multiple rules can run simultaneously or a rule can be disabled. In addition to interval type action tasks, other tasks need to be used with NTP services, otherwise it is difficult to achieve reasonable time task control.	Radio box selection. • Enable • Disabling
Basic Settings		
Task name	Task management rule name identifier, used only to distinguish between different rules.	The maximum length is 12 bits and the input specification is shown in the Parameter Specification Table.

Parameter name	Meaning	How to Configure
Task Type	Tasks are mainly action class tasks and status class tasks, action class tasks are configured as a time point or interval, status class tasks are configured as a time period, status class tasks are only online, it indicates that the configured time zone MODEM is online (automatic re-dial off), other time zones remain offline (not dial).	Drop-down box option ● modem-online ● reboot ● custom ● Select Custom to display the Command parameter, which requires a user to enter a command (either a command such as DIAUP or some other command). ● The maximum length is a 64 bit string, for input specifications see the Parameter Specification Table.
Commands	Command for background operation commands, usually not recommended, if necessary, please contact our technical staff.	Word type, up to 64 bytes, input specification see Parameter Specification Table.
Set Time		
Time Type	It is divided into time range and time interval, which correspond to state task and action task.	Drop-down box option ● range ● interval
When Time Type selects Range		
Clock	Configure hours, minutes, and points for action class tasks when intervals are consistent.	Range of values: [00: 00, 23: 59] Format: hh: mm-hh: mm
Days	The number of days a task is executed, representing the time period or point in the month at which the task is executed.	Value Range: [01, 31] Format: xx-xx
Week	Week setting for action execution. Perform a task on behalf of a time period or point in time on a day of the week. Both days and weeks are configured to perform tasks when both time conditions are met.	Range of values: [1, 7] Format: x-x One for Monday
When Time Type selects Interval		
Time interval	Action class tasks can be configured to execute every once in a while, in addition to configuring the point-in-time execution.	Range of values: 1-65535 Unit: Minutes

Step 5 Click Save to complete the task management service configuration.

When the task management time type is " range ", you must first turn on System Time, which is NTP service (manual timing is not supported for task management for the time being) ; If the time type is " Interval ", you do not need to turn on System Time. To use System Time, see 5.7.4 System Time.

Due to the stability of MODEM, the router has several functions on the operation of MODEM, such as task management, parameter switching, link backup, ICMP detection, trigger setting, and so on . The task management is to change the state of the MODEM, while the other functions are to change the state of the MODEM, so please take into account other functions when using the task management . If necessary, please contact our technician.

---End

5.4 Secure configuration

5.4.1 Overview

Security settings refer to the firewall functionality of the router. The MRR8860 Industrial Intelligent Gateway supports three security settings, such as IP filtering, domain name filtering, and MAC address filtering. The user compares the IP address/port, MAC address, domain name of the incoming router packet with the firewall rules added by the user, and performs receive or discard actions on packets that match the firewall rules for purposes such as allowing/disallowing certain segments of the network to access the external network, allowing/disallowing other users to access the router.

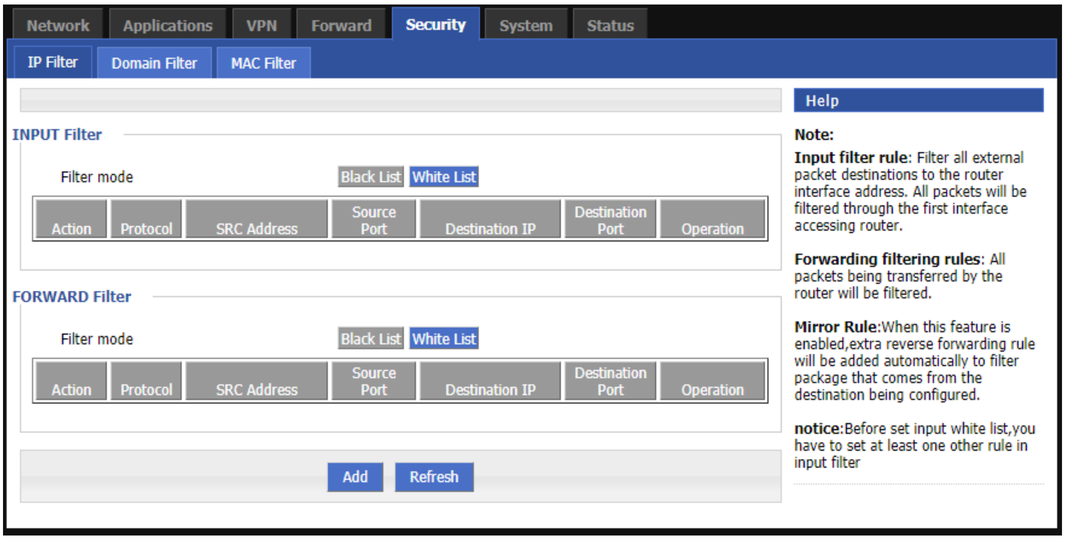
5.4.2 Configuring actions

IP filtering

IP filtering is the process by which a router filters IP address rules to determine whether external devices are allowed to access the router and whether packets are allowed to pass through the router.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Security Settings>IP Filtering to open the IP Filtering tab, as shown in Figure 5-27.



INPUT Filter

Filter mode Black List White List

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation

FORWARD Filter

Filter mode Black List White List

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation

Help

Note:

Input filter rule: Filter all external packet destinations to the router interface address. All packets will be filtered through the first interface accessing router.

Forwarding filtering rules: All packets being transferred by the router will be filtered.

Mirror Rule:When this feature is enabled,extra reverse forwarding rule will be added automatically to filter package that comes from the destination being configured.

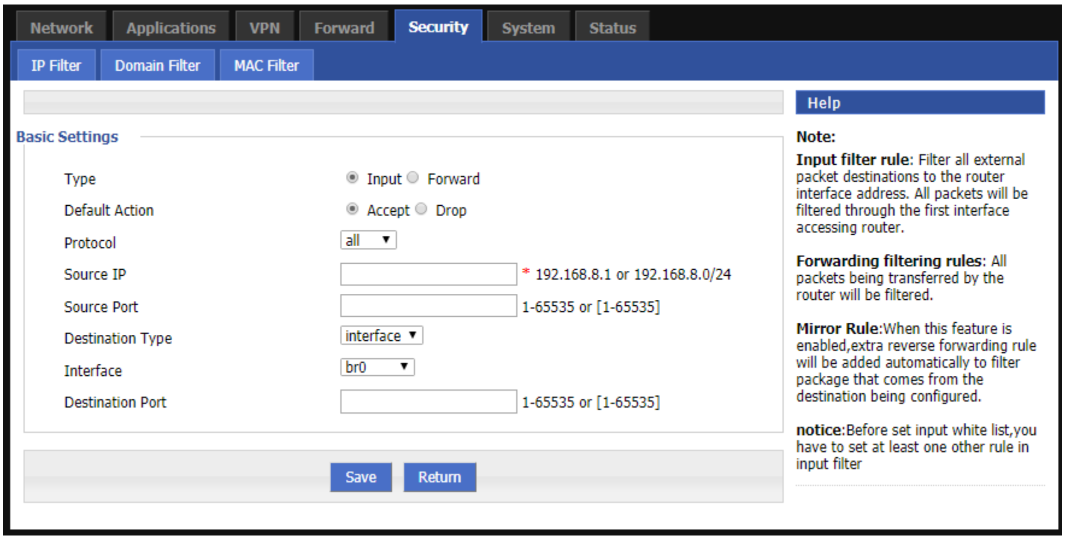
notice:Before set input white list,you have to set at least one other rule in input filter

Figure 5-27 IP filter tab

In the input/forward filter rule ,

- Blacklist: Allows packet forwarding by default, and packets that meet the " drop " rule in the list cannot be forwarded by the router.
- Whitelist: Default to reject packet forwarding, the list of " accept " rules of packets can be forwarded through the router.

Step 3 ： Click Add to add a new IP filtering rule to configure IP filtering parameters. There are two types of filtering for IP filtering: Input and Forward, and the rules configuration page is shown in Figure 5-28 and Figure 5-29.



Basic Settings

Type	● Input ○ Forward
Default Action	● Accept ○ Drop
Protocol	all
Source IP	* 192.168.8.1 or 192.168.8.0/24
Source Port	1-65535 or [1-65535]
Destination Type	interface
Interface	br0
Destination Port	1-65535 or [1-65535]

Help

Note:

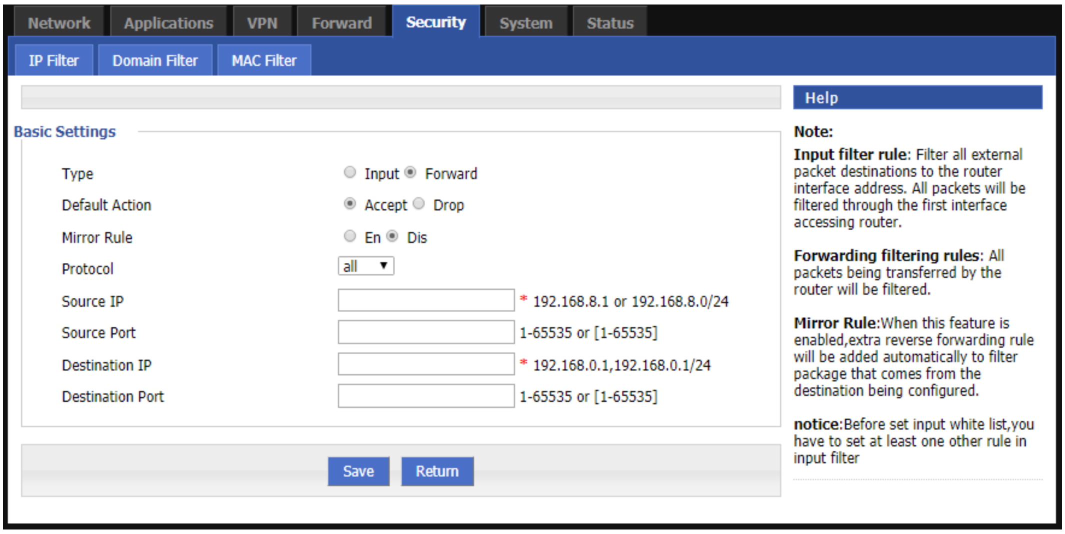
Input filter rule: Filter all external packet destinations to the router interface address. All packets will be filtered through the first interface accessing router.

Forwarding filtering rules: All packets being transferred by the router will be filtered.

Mirror Rule:When this feature is enabled,extra reverse forwarding rule will be added automatically to filter package that comes from the destination being configured.

notice:Before set input white list,you have to set at least one other rule in input filter

Figure 5-28 Enter filter rules page



Basic Settings

Type	○ Input ● Forward
Default Action	● Accept ○ Drop
Mirror Rule	○ En ● Dis
Protocol	all
Source IP	* 192.168.8.1 or 192.168.8.0/24
Source Port	1-65535 or [1-65535]
Destination IP	* 192.168.0.1,192.168.0.1/24
Destination Port	1-65535 or [1-65535]

Note:

Input filter rule: Filter all external packet destinations to the router interface address. All packets will be filtered through the first interface accessing router.

Forwarding filtering rules: All packets being transferred by the router will be filtered.

Mirror Rule:When this feature is enabled,extra reverse forwarding rule will be added automatically to filter package that comes from the destination being configured.

notice:Before set input white list,you have to set at least one other rule in input filter

Figure 5-29 Forward filter rules page

The parameter descriptions are shown in Table 5-14.

Table 5-14 IP Filter Parameter Description

Parameter name	Meaning	How to Configure
Filter Type	Select a filter type to select Input or Forward based on your requirements. • Enter whether to allow access to the router. • Forwarding: Whether forwarding through the router is allowed.	Radio button selection.
Filtering action	The default action for this rule. You can select Accept or Discard. • Accepted: The firewall accepts the packet, which is ready to go through. • Discard: This packet is directly discarded by the firewall.	Radio button selection. Choose Accept or Discard based on your needs.
Mirror rule	Configuration is required when Filter Type Select Forward • Enable: Add an additional rule based on the configured rule that reverses the source address/port from the destination address/port ; • Disabled: No processing.	Radio button selection.
Protocol	Protocol used by IP packets	Drop-down list selection. • all • tcp • udp • icmp

Parameter name	Meaning	How to Configure
Source Address	The source address of the IP packet.	Format: Type A.B.C.D, input specification see Parameter Specification Table. For example: 192.168.8.1 or 192.168.8.1 / 24
Source Port	The source port of the IP packet, which does not need to be configured when the protocol selects " ICMP ".	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.
When Filter Type Select Input		
Destination address type	Specifies the router interface for IP packet access.	Drop-down list selection. • interface • any
Interface	The destination address type selection ' interface ' needs to be configured to represent the router port accessed by the IP packet (or all interfaces of the router if the destination address type selects ' any ').	Drop-down list selection. • br0 • modem • eth0 • wlan0
Destination port	Router port for IP packet access (does not need to be configured when protocol selects " ICMP ")	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.
When Filter Type Select Forward		
Destination address	The destination address in the IP packet.	Format: Type A.B.C.D, input specification see Parameter Specification Table.
Destination port	Destination port in IP packet	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.

Step 4 Click Save to complete the IP filter rule configuration.

NOTE

An IP input rule indicates whether other devices are allowed to access the router, and the destination address in the rule can only select the router's interface ; An IP forwarding rule indicates whether IP packets are allowed to be forwarded through the router, and the destination address in the rule can be all IP addresses except the router interface address.

When the port is configured in the rule, select the " ALL " protocol to select both TCP and UDP protocols ; When the port is not configured in the rule, selecting the " All " protocol means selecting both TCP, UDP, and ICMP protocols.

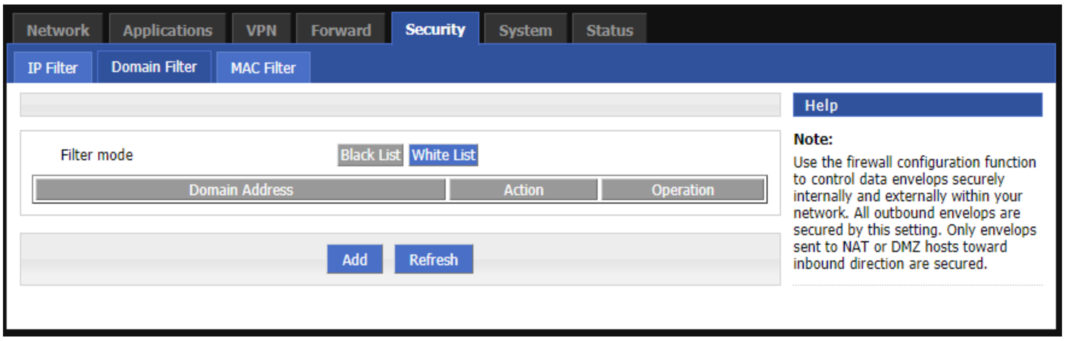
--End

Domain name filtering

Domain name filtering supports black and white lists, primarily to prevent local area network hosts from accessing certain domain names or only to allow access to specified domain names.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Security Settings>Domain Name Filter to open the Domain Name Filter tab, as shown in Figure 5-30.



Filter mode

Domain Address	Action	Operation

Note:

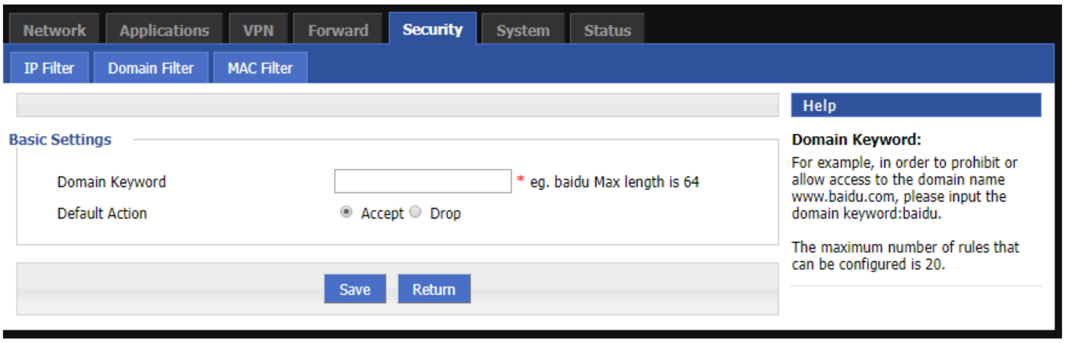
Use the firewall configuration function to control data envelops securely internally and externally within your network. All outbound envelops are secured by this setting. Only envelops sent to NAT or DMZ hosts toward inbound direction are secured.

Figure 5-30 Domain name filter tab

- ● Blacklist: Allows access to any domain name by default, and packets that conform to the " drop " rule in the list are discarded.
- ● Whitelist: Access to any domain name is denied by default, and packets that conform to the " Accept " rule in the list are accepted and forwarded.

Step 2

Click the Add button to add a new domain name filter rule to configure the domain name filter parameters. The rule configuration page is shown in Figure 5-31.



Basic Settings

Domain Keyword * eg. baidu Max length is 64

Default Action ● Accept ○ Drop

Domain Keyword:

For example, in order to prohibit or allow access to the domain name www.baidu.com, please input the domain keyword:baidu.

The maximum number of rules that can be configured is 20.

Figure 5-31 Domain name filter rule configuration page

The parameter descriptions are shown in Table 5-15.

Table 5-15 Domain name filter rule configuration parameter descriptions

Parameter name	Meaning	How to Configure
Domain name keyword	The keyword for the domain name needs to be filtered.	Type Word, maximum length is 64 bits, input specification see Parameter Specification Table. For example, the domain name keyword for wwwwwwwww.baidu . com is " baidu ".
Filtering action	The action performed on the domain name keyword.	Click the button Select. • Accept: The action for packets whose domain name keyword is an input string is Accept and Forward • Discard: The action for packets with an input string for the domain name keyword is Discard

Step 3 Click Save to complete the domain name filter rule configuration.

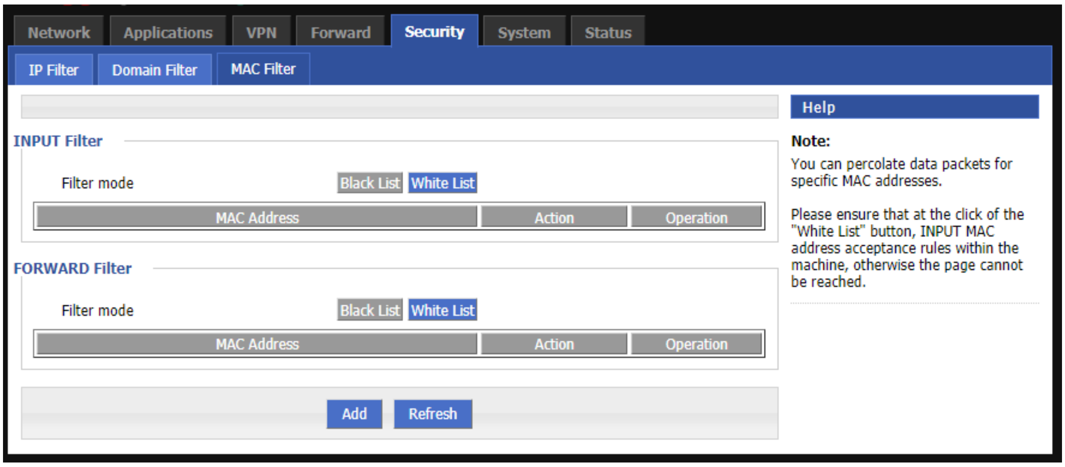
---End

Mac filtering

MAC filtering also supports black and white lists, which are often used to control host access to routers. In addition to this functionality, the MRR8860 Industrial Intelligent Gateway can restrict external network access for a specific MAC host or allow only hosts with a specific MAC address to access the external network.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Security Settings>MAC Filter to open the MAC Filter tab, as shown in Figure 5-32.



Note:

You can percolate data packets for specific MAC addresses.

Please ensure that at the click of the "White List" button, INPUT MAC address acceptance rules within the machine, otherwise the page cannot be reached.

Figure 5-32 Mac filter tab

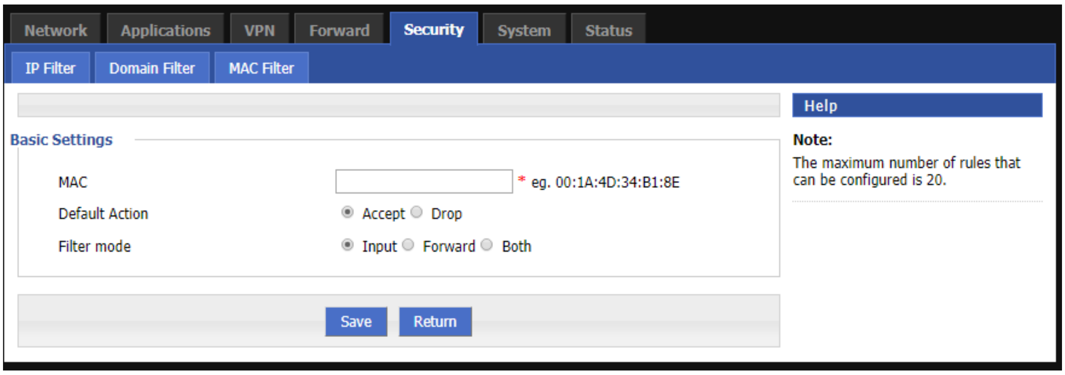
The parameter descriptions are shown in Table 5-16.

Table 5-16 MAC Filter Tab Description

Parameter name	Meaning	How to Configure
MAC Input Filter Rule Configuration		
Action	Enable MAC Input Filter Blacklist/Whitelist.	Radio button selection. • Blacklist: Allows access to the router by default, and packets of devices that meet the " drop " rule in the list accessing the router are discarded. • Whitelist: Access to routers is denied by default, and packets from devices that meet the " Accept " rule in the list are accepted. At the same time, only one list of blacklists and white lists is valid.
MAC Forwarding Filter Rule Configuration		
Action	Enable MAC forwarding to filter blacklists/whitelists.	Radio button selection. • Blacklist: Forwarding of packets is accepted by default, and packets that meet the " drop " rule in the list are discarded. • Whitelist: Default to reject the forwarding of packets, which meet the " accept " rule in the list will be accepted and forwarded. • At the same time, only one list of blacklists and white lists is valid.

Step 3

Click Add to add a new MAC filter rule to configure the MAC filter parameters. The rule configuration page is shown in Figure 5-33.



Basic Settings

MAC * eg. 00:1A:4D:34:B1:8E

Default Action ● Accept ○ Drop

Filter mode ● Input ○ Forward ○ Both

Note:
The maximum number of rules that can be configured is 20.

Figure 5-33 MAC Filter Rule Configuration page

The parameter descriptions are shown in Table 5-17.

Table 5-17 MAC Filter Rule Configuration Parameter Description

Parameter name	Meaning	How to Configure
Basic Settings		

Parameter name	Meaning	How to Configure
MAC	MAC address to filter.	Word type MAC format: xx: xx: xx: xx: xx: xx
Filtering action	The default action for this rule can be Accept or Discard. • Accept: All packets issued from this MAC address are accepted. • Discard: Discard all packets sent from this MAC address.	Radio button selection. Choose Accept or Discard based on your needs.
Filter mode	The filter mode for this rule, which can be Input, Forward, or Input and Forward. • Input: All packets that access the router. • Forward: All packets forwarded by the router. • Input and forward: All packets that access the router and all packets that are forwarded by the router.	Radio button selection. Select Input, Forward, or Input or Forward based on your requirements.

Step 4

Click Save to complete the MAC filter rule configuration.

---End

5.5 Forwarding configuration

5.5.1 Overview

The MRR8860 industry intelligent gateway forwarding functions include NAT, static routing, dynamic routing (RIP, OSPF), and QoS.

5.5.2 NAT

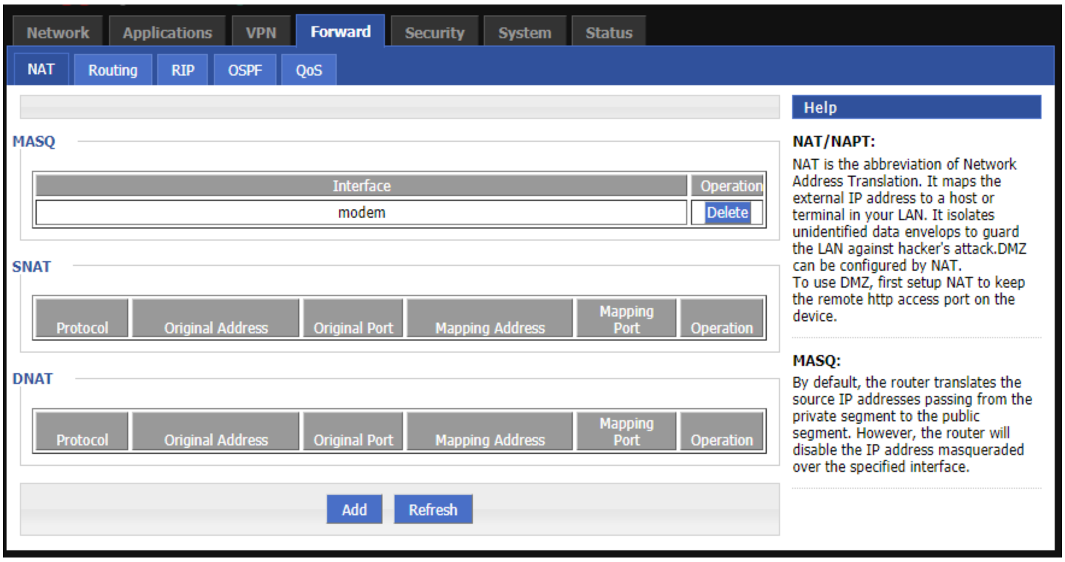
NAT (NetWord Address Translation), network address translation, is generally used to replace private network (LAN) IP addresses with public network IP addresses.

DNAT Rule Configuration

DNAT is a destination address replacement that replaces destination addresses inside the external network access router with user-set addresses.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Forward Settings>NAT to open the NAT tab, as shown in Figure 5-34.



MASQ

Interface	Operation
modem	Delete

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

DNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

Help

NAT/NAPT:

NAT is the abbreviation of Network Address Translation. It maps the external IP address to a host or terminal in your LAN. It isolates unidentified data envelops to guard the LAN against hacker's attack.DMZ can be configured by NAT.
To use DMZ, first setup NAT to keep the remote http access port on the device.

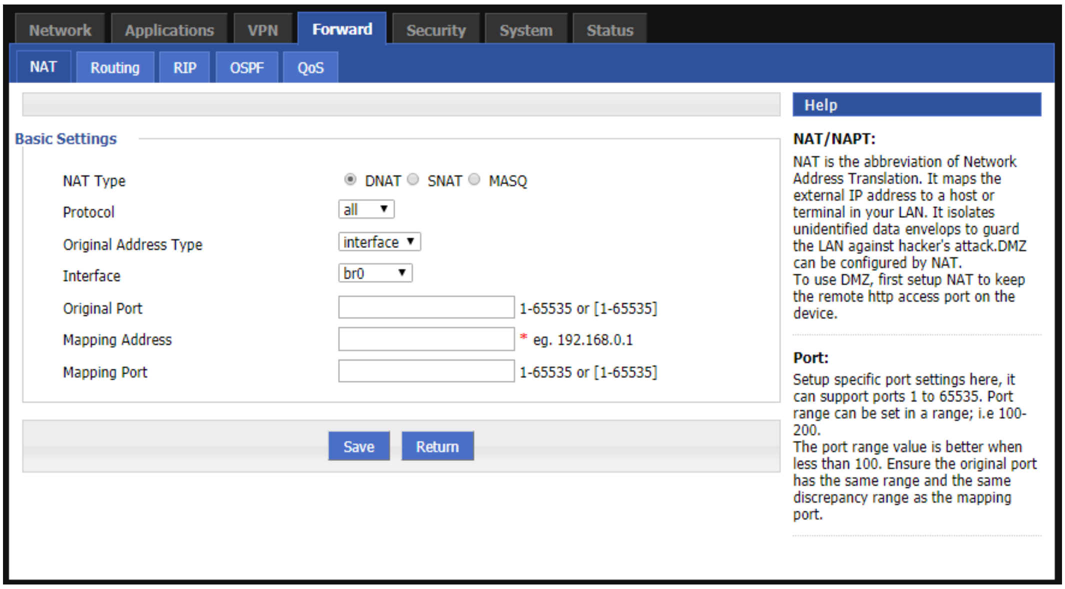
MASQ:

By default, the router translates the source IP addresses passing from the private segment to the public segment. However, the router will disable the IP address masqueraded over the specified interface.

Figure 5-34 NAT tab

Step 3

Click the Add button to select a new DNAT rule with a translation type of DNAT, as shown in Figure 5-35.



Basic Settings

NAT Type	● DNAT ○ SNAT ○ MASQ
Protocol	all
Original Address Type	interface
Interface	br0
Original Port	1-65535 or [1-65535]
Mapping Address	* eg. 192.168.0.1
Mapping Port	1-65535 or [1-65535]

Help

NAT/NAPT:

NAT is the abbreviation of Network Address Translation. It maps the external IP address to a host or terminal in your LAN. It isolates unidentified data envelops to guard the LAN against hacker's attack.DMZ can be configured by NAT.
To use DMZ, first setup NAT to keep the remote http access port on the device.

Port:

Setup specific port settings here, it can support ports 1 to 65535. Port range can be set in a range; i.e 100-200.
The port range value is better when less than 100. Ensure the original port has the same range and the same discrepancy range as the mapping port.

Figure 5-35 NAT rules configuration page

Step 4 Configure the DNAT rule parameters. The parameter descriptions are shown in Table 5-18.

Table 5-18 DNAT parameter specification

Parameter name	Meaning	How to Configure
Basic Settings		

Parameter name	Meaning	How to Configure
Protocol	Destination address translation for which protocol packet.	Drop-down list Selection: • all • tcp • udp • icmp
Initial address type	The destination address type of the IP packet that needs to be converted.	Drop down list box selection: • interface Interface • static Static
Interface (required when initial address type selection interface)	Indicates that the destination address of the IP packet is an interface of the router.	Drop down list box selection: • br0 • modem • eth0 • wlan0
Initial address (required when initial address type static is selected)	Indicates the destination address of the IP packet entering the router, which needs to be converted.	A . B . C . D . connector or A . B . C . D/M ; Please refer to " Parameter Specification Table " for input specification
Initial port	The port used by the destination address in the IP packet.	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.
Map Address	The address after the original destination address is replaced.	A . B . C . D joint die, input specification see Parameter Specification Table
Mapping port	The port after the initial port is replaced.	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.

Step 5 Click Save to complete the configuration of this DNAT rule.

NOTE

When the port is configured in the DNAT rule, the protocol selection of " ALL " means the choice of " TCP " and " UDP " protocols ; When no port is configured in the DNAT rule, the protocol selection of " ALL " means that the three protocols " TCP ", " UDP ", " ICMP " are selected.

---End

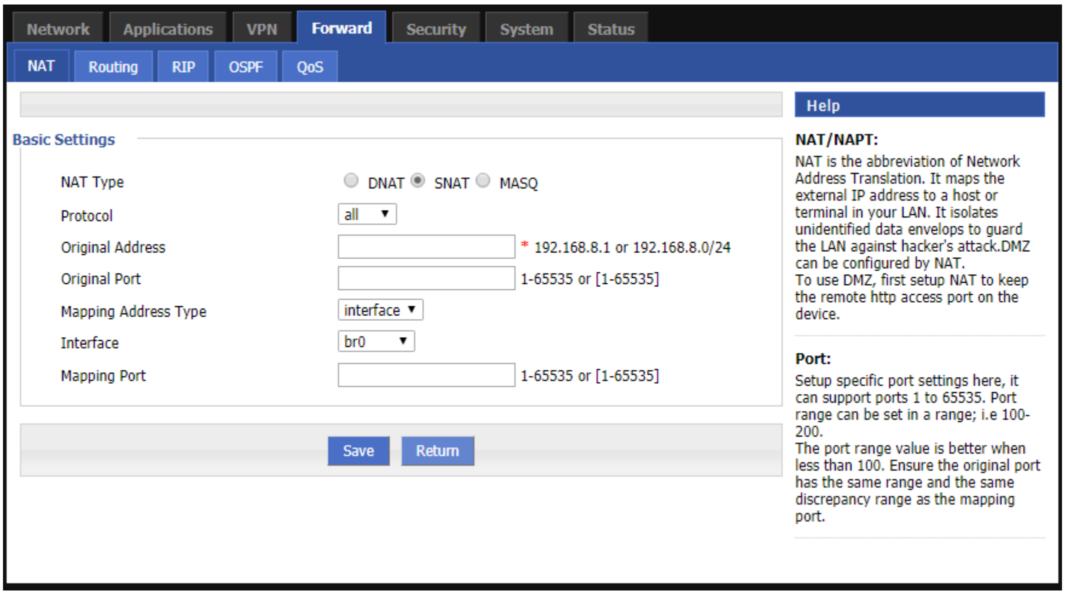
SNAT Rule Configuration

SNAT is a source address translation that converts the source address of an IP packet to another address.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Forward Settings>NAT to open the NAT tab, as shown in Figure 5-34.

Step 3 When you select Convert Type to SNAT, the configuration interface is shown in Figure 5-36.



Basic Settings

NAT Type ○ DNAT ● SNAT ○ MASQ

Protocol: all

Original Address: * 192.168.8.1 or 192.168.8.0/24

Original Port: 1-65535 or [1-65535]

Mapping Address Type: interface

Interface: br0

Mapping Port: 1-65535 or [1-65535]

Help

NAT/NAPT:

NAT is the abbreviation of Network Address Translation. It maps the external IP address to a host or terminal in your LAN. It isolates unidentified data envelops to guard the LAN against hacker's attack.DMZ can be configured by NAT.
To use DMZ, first setup NAT to keep the remote http access port on the device.

Port:

Setup specific port settings here, it can support ports 1 to 65535. Port range can be set in a range; i.e 100-200.
The port range value is better when less than 100. Ensure the original port has the same range and the same discrepancy range as the mapping port.

Figure 5-36 SNAT Rule Configuration Interface

Step 4 Configure the SNAT rule parameters. The parameter descriptions are shown in Table 5-20.

Table 5-19 SNAT Rule Parameter Description

Parameter name	Meaning	How to Configure
Protocol	Destination address translation for which protocol packet.	Drop-down list Selection: • all • tcp • udp • icmp
Initial address	Source Address to Replace	A . B . C . D . connector or A . B . C . D/M ; For the input specification, refer to the Parameter Specification Table.
Initial port	Source Address Port to Replace	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.
Map Address Type	New Source Address Type After Source Address Replacement	Drop-down list Selection: • interface

Parameter name	Meaning	How to Configure
		• static
Interface (required when mapping address type selection interface)	Select an interface of the router as the replacement source address	Drop-down list Selection: • br0 • modem • eth0 • wlan0
Map Address	New source address after source address replacement	A . B . C . D joint die, input specification see Parameter Specification Table
Mapping port	Source address port after replacement	Range of values: 1-65535 or [1-65535] ; Can be a range or a single port.

Step 5 Click Save to complete the routing pattern rule configuration.

NOTE

When a port is configured in the SNAT rule, the protocol selection of " ALL " means the selection of " TCP " and " UDP " protocols ; When the port is not configured in the SNAT rule, the protocol selection of " ALL " indicates the selection of " TCP ", " UDP ", " ICMP " three protocols.

---End

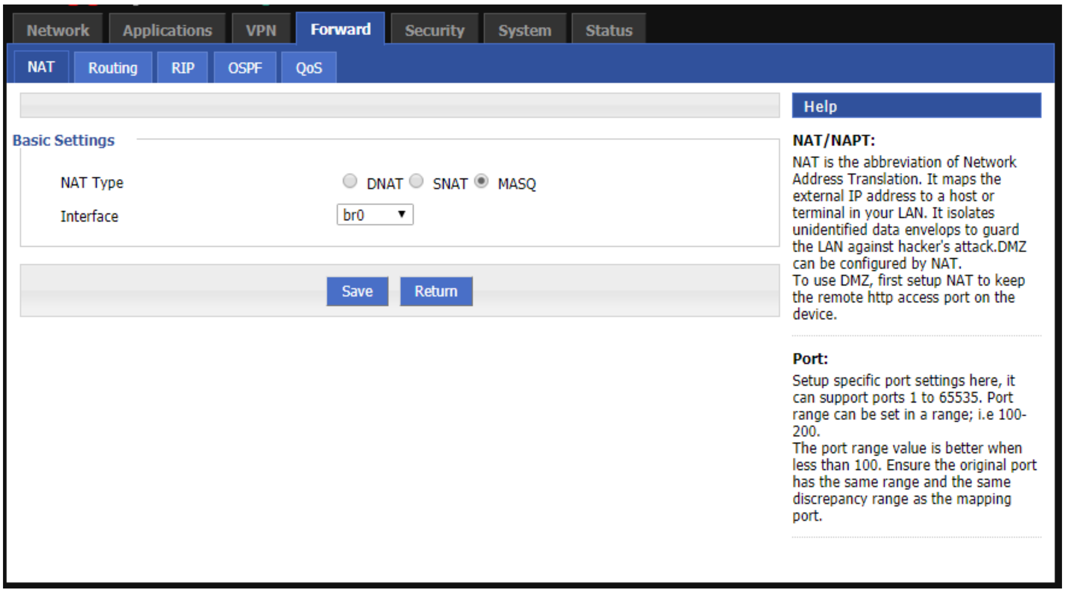
MASQ Rule Configuration

MASQ, or MASQUREADE, addresses spoofing, converts the source IP address of all packets forwarded by the router to the user-set IP address. The MRR8860 Industrial Intelligent Gateway supports the conversion of the source IP of a packet to one of the router's interface addresses.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2

Click Forward Settings>NAT to open the NAT tab and select Convert Type to MASQ, as shown in Figure 5-37.



Basic Settings

NAT Type ○ DNAT ○ SNAT ● MASQ

Interface br0

NAT/NAPT:

NAT is the abbreviation of Network Address Translation. It maps the external IP address to a host or terminal in your LAN. It isolates unidentified data envelops to guard the LAN against hacker's attack.DMZ can be configured by NAT.
To use DMZ, first setup NAT to keep the remote http access port on the device.

Port:

Setup specific port settings here, it can support ports 1 to 65535. Port range can be set in a range; i.e 100-200.
The port range value is better when less than 100. Ensure the original port has the same range and the same discrepancy range as the mapping port.

Figure 5-37 MASQ Rule Configuration Interface

Step 3 Configure the MASQ rule parameters. The parameter descriptions are shown in Table 5-20.

Table 5-20 MASQ Rule Parameter Description

Parameter name	Meaning	How to Configure
Interface	Interface contains: • BR0: Use BR0 port address as router and LAN and external communication address • MODEM: Modem port address as router and LAN and external communication address • Eth0: WAN address as router and LAN and external communication address • WLAN 0: WLAN address as router and LAN and external communication address	Drop-down list selection. It is recommended that you select the desired interface from the drop-down list according to your needs.

Step 4

Click Save to complete the routing pattern rule configuration.

NOTE

MASQ rule: Change the source address of all packets sent from the local area network to the IP address of the specified interface of the router so that the packets can be sent out from the PC on the local area network side ; If you delete the MASQ rule from the Router page, the PC on the LAN side of the router cannot communicate with the external.

---End

5.5.3 Static routing configuration

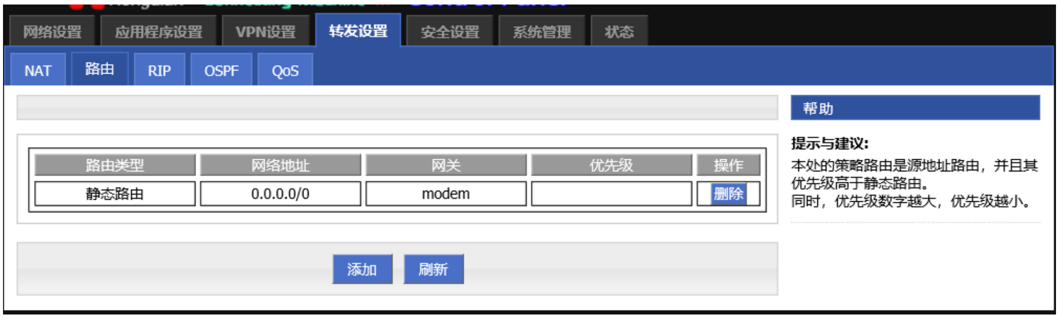
Static routing is to provide a specific forwarding path for the router to forward packets, which must be manually configured by the user. Static routing is divided into static routing and policy routing . Static routing is based on destination address. Policy routing is the routing based on the source address (the router detects the source address of the received forwarding packet and then selects the corresponding policy routing forwarding based on the source address), and the policy routing priority is divided by 3-252 digits, the smaller the number, the higher the priority. There is also a priority between static routing and policy routing: policy routing takes precedence over static routing.

Step 1

Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2

Click Forward Settings>Routing. Open the Routing tab, as shown in Figure 5-38.



路由类型	网络地址	网关	优先级	操作
静态路由	0.0.0.0/0	modem		删除

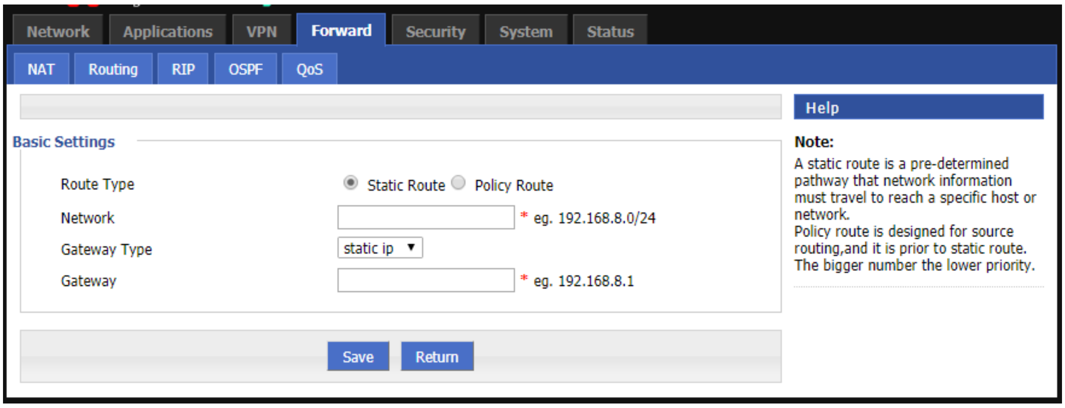
提示与建议:

本处的策略路由是源地址路由，并且其优先级高于静态路由。
同时，优先级数字越大，优先级越小。

Figure 5-38 Static route tab

Step 3

Click the Add button to create a new static routing rule. The configuration interface is shown in Figure 5-39 and Figure 5-40.



Basic Settings

Route Type ● Static Route ○ Policy Route

Network * eg. 192.168.8.0/24

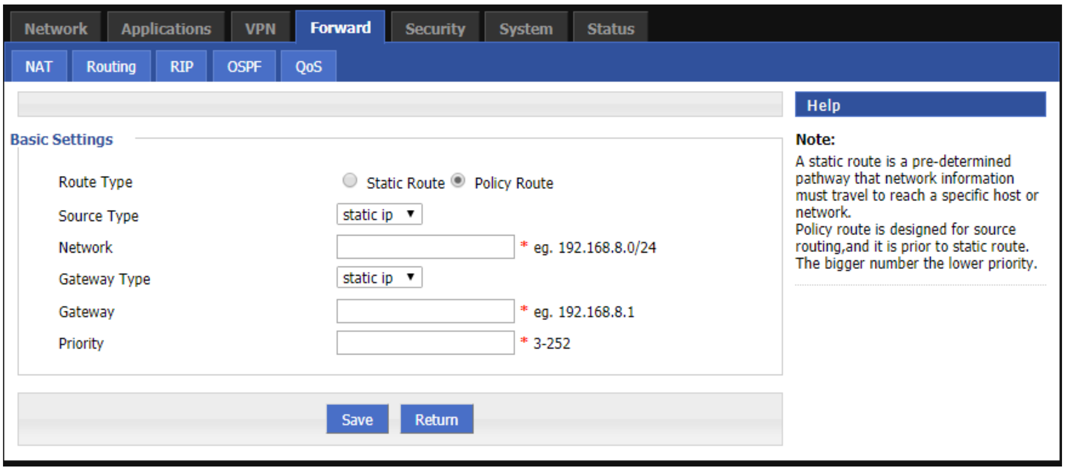
Gateway Type static ip ▼

Gateway * eg. 192.168.8.1

Note:

A static route is a pre-determined pathway that network information must travel to reach a specific host or network.
Policy route is designed for source routing,and it is prior to static route.
The bigger number the lower priority.

Figure 5-39 Static routing configuration page



Basic Settings

Route Type	○ Static Route ● Policy Route	
Source Type	static ip ▾	
Network		* eg. 192.168.8.0/24
Gateway Type	static ip ▾	
Gateway		* eg. 192.168.8.1
Priority		* 3-252

Help

Note:
A static route is a pre-determined pathway that network information must travel to reach a specific host or network.
Policy route is designed for source routing,and it is prior to static route.
The bigger number the lower priority.

Figure 5-40 Policy Routing Configuration page

The parameter descriptions are shown in Table 5-21.

Table 5-21 Static route parameter specification

Parameter name	Meaning	How to Configure
Basic Settings		
Routing type	Select whether to static route or policy route.	Drop-down box option
When Routing Type selects Static Routing		
Network address	Sets the destination address and subnet mask bits for the static route.	Fill in the destination address and subnet mask digits. Format: A.B.C.D/M, input specification see Parameter Specification Table.
Gateway type	Specifies the type of gateway that the static route acts on. Include: • Interface • Static IP	Drop-down list selection. You can select the required interface IDs from the drop-down list, which are static IP and interface.
Gateway	Sets the next hop IP address for the static route, which is the port address of the adjacent router.	Drop-down list Selection • If the gateway type chooses static IP, the gateway needs to be input manually, in the form a.b.c.d • If the gateway type selects an interface, the gateway requires a drop-down list selection.

Parameter name	Meaning	How to Configure
When Routing Type selects Policy Routing		
Source Type	Sets the source address type of the policy route. ● Static IP ● Interface	Drop-down box options.
Network address	You need to configure when the source type selects Static IP and add the network address manually.	Fill in the destination address and subnet mask digits. Format: A.B.C.D/M, input specification see Parameter Specification Table.
Source interface	Configuration is required when Source Address Select Interface, select the source address for the policy route. ● modem	Drop-down box options. When the router creates other interfaces such as VPDN, IPSec, the interface name is also displayed in the Source Interfaces list.
Gateway type	Sets the next address for the policy route. ● Static IP ● Interface	Drop-down box options.
Gateway	The IP address needs to be filled in when the gateway type selects Static IP, and the appropriate interface needs to be selected as the gateway when the gateway type selects Interface.	Format: A.B.C.D/M, input specification see Parameter Specification Table.
Priority	Sets the priority of the policy route, and the lower the priority number, the higher the priority.	Range of values: [3252]

Step 4 Click Save to complete the static routing configuration.

NOTE

Static routing means that the router selects a route based on the destination address of the forwarded packet received and then forwards the packet out . If the router receives a packet with a source address of 1.1.1.1 /destination address of 2.2.2.2 , the router selects a route in the routing table that meets the destination address of 2.2.2.2 and sends the packet to the next hop.
Policy routing means that the router routes the forwarding packet according to the destination address of the received forwarding packet . If the router receives a packet with a source address of 1.1.1.1 /destination address of 2.2.2.2 , the router selects a route in the routing table that conforms to the source address of 1.1.1.1 and forwards the packet to the next hop.
Policy routing takes precedence over static routing, regardless of the priority of policy routing.

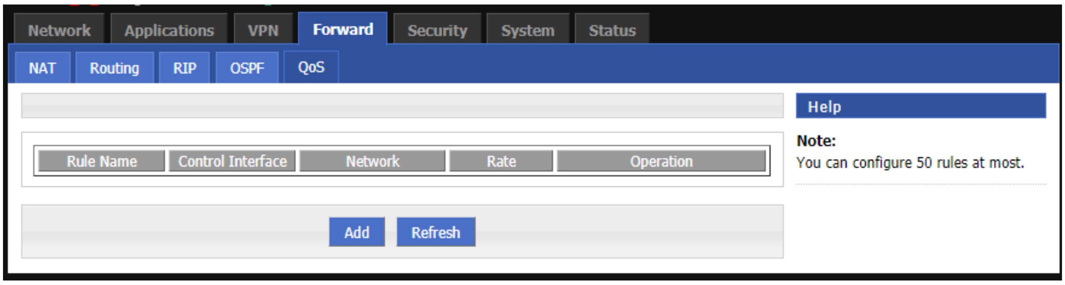
---End

5.5.4 QoS

QoS (Quality of Service) quality of service is a security mechanism of network and a technology to solve the problems of network bandwidth allocation and network priority. When the network is overloaded or congested, QoS ensures that important traffic is not delayed or discarded, while ensuring efficient operation of the network.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

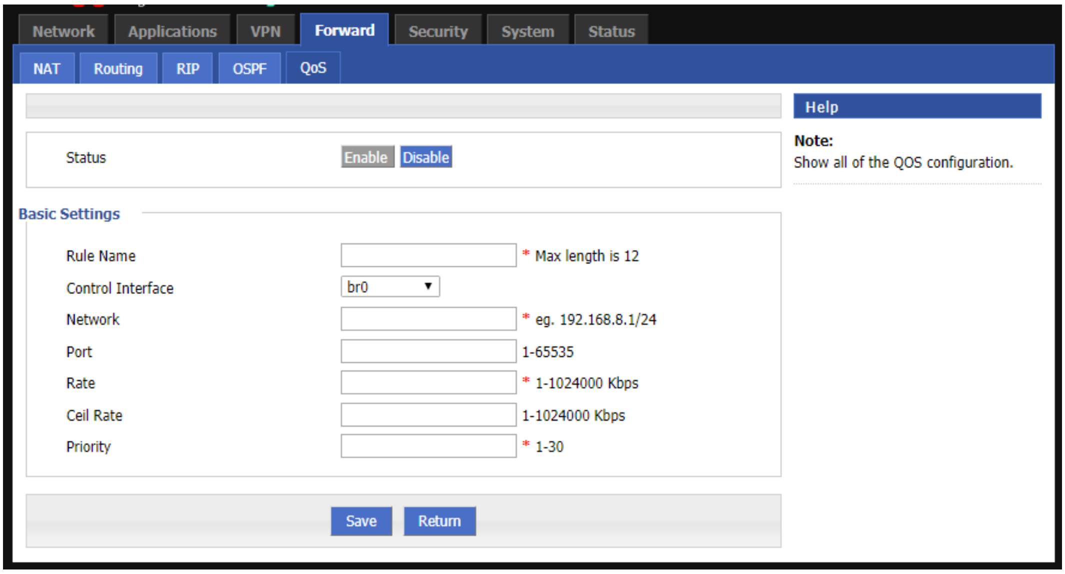
Step 2 Click Forward Settings>QoS to open the QoS tab, as shown in Figure 5-41.



Note:
You can configure 50 rules at most.

Figure 5-41 QoS tab

Step 3 Click Add to create a new QoS rule. The configuration interface is shown in Figure 5-42



Note:
Show all of the QOS configuration.

Status Enable Disable

Basic Settings

Rule Name * Max length is 12
Control Interface br0
Network * eg. 192.168.8.1/24
Port 1-65535
Rate * 1-1024000 Kbps
Ceil Rate 1-1024000 Kbps
Priority * 1-30

Figure 5-42 QoS configuration interface

Step 4 Configure the QoS parameters. The parameters for QoS are explained in Table 5-22.

Table 5-22 QoS parameter specification

Parameter name	Meaning	How to Configure
Status	Enable/disable QoS functionality.	Click the Enable/Disable button

Parameter name	Meaning	How to Configure
		selection.
Basic Settings		
Rule Name	The rule name for QoS.	A maximum of 12 characters is allowed. Can only be set when a new rule is added, and cannot be modified later. The rule name cannot be repeated, otherwise the rule that is added later overrides the rule that was added earlier.
Flow control interface	The type of interface for flow control, including: ● br0：The interface for the flow control is a LAN port ● eth0： The interface of the flow control is a WAN port ● vpdnpppoe:The interface for flow control is VPDNPPPoE ● modem：The interface for the flow control is MODEM	Drop down options: ● br0 ● eth0 ● modem ● vpdnpppoe
Network address	In and out of the flow control interface network address, speed limit objects.	Fill in the destination address and subnet mask digits. Format: A.B.C.D/M, input specification see Parameter Specification Table.
Port	A network port that requires flow control.	Range of values: 1-65535 The port can be unconfigured and, if not, all ports.
Rate	The rate at which the network address is set.	Range of values: 1-1024000 Unit: Kbps
Redundant bandwidth	The maximum bandwidth available for this network address communication is guaranteed at the base rate and the bandwidth is free.	Range of values: 1-1024000 Unit: Kbps
Priority	Set the priority of the rule.	Range of values: [1, 30]

Step 5 Click Save to complete the parameter configuration.

NOTE

QoS is mainly used for the router to distribute the average route to the Internet users or to give priority to one of the Internet users to use bandwidth. If the router has two subnets: 192.168.8.1 /24 and 192.168.9.1 /24, the router can control the speed of these two subnets through QoS. If the bandwidth of the router is relatively abundant, the router can satisfy the high priority redundancy bandwidth according to the priority and redundancy bandwidth of the two subnets, and then satisfy the redundant bandwidth of the lower priority subnets.

---End

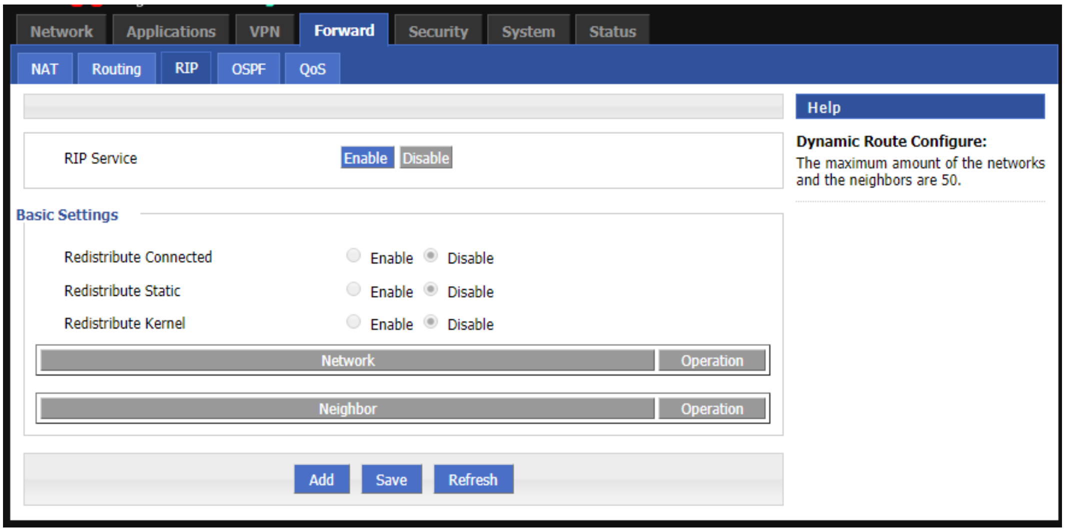
5.5.5 Dynamic routing configuration

RIPConfiguration

The RIP (Route Information Protocol) protocol is one of the most widely used IGP (Internal Gateway Protocol) and is designed for small networks using the same technology, so it is suitable for most campus networks and regional networks where the rate change is not a large continuous line. For more complex environments, the RIP protocol is generally not used. RIP services can be configured according to user needs when the MRR8860 Industrial Intelligent Gateway is shipped from the factory.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Forward Settings>RIP to open the RIP tab, as shown in Figure 5-43.



RIP Service Enable Disable

Dynamic Route Configure:
The maximum amount of the networks and the neighbors are 50.

Basic Settings

Redistribute Connected ○ Enable ● Disable
Redistribute Static ○ Enable ● Disable
Redistribute Kernel ○ Enable ● Disable

Figure 5-43 RIP tab

The parameter descriptions are shown in Table 5-23.

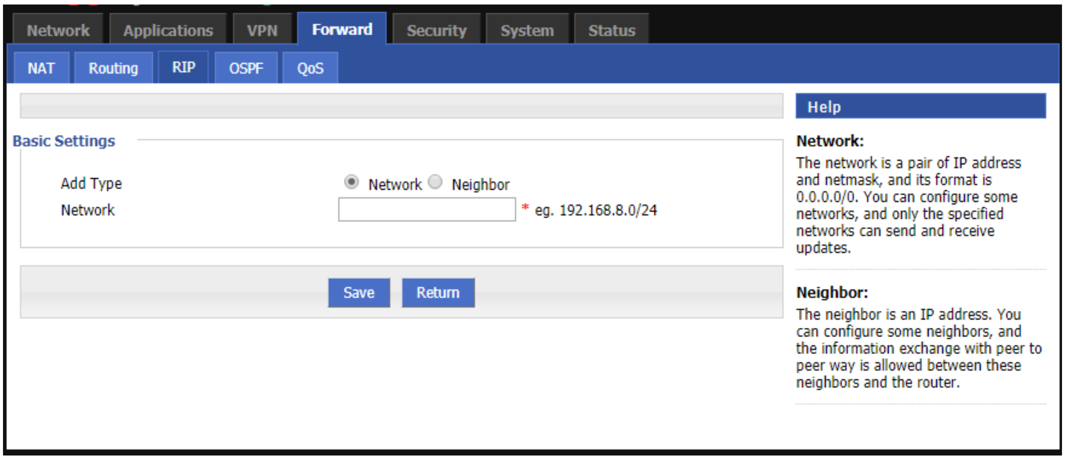
Table 5-23 RIP Parameter Description I

Parameter name	Meaning	How to Configure
RIP service	Enable/Disable RIP Service	Radio button selection.
Publish Connection Routing	Whether to allow publish connection routing	Radio button selection. Choose whether to allow publish connection routing based on your requirements.

Publish static route	Whether to allow publishing static routes	Radio button selection. Choose whether to allow publish static routes based on your requirements.
Publish kernel route	Whether to allow kernel routing to be published	Radio button selection. Choose whether to allow publish kernel routing based on your requirements.

Step 3

Click the Add button to create a new RIP rule. The configuration interface is shown in Figure 5-44. A.



Basic Settings

Add Type ● Network ○ Neighbor

Network * eg. 192.168.8.0/24

Help

Network:
The network is a pair of IP address and netmask, and its format is 0.0.0.0/0. You can configure some networks, and only the specified networks can send and receive updates.

Neighbor:
The neighbor is an IP address. You can configure some neighbors, and the information exchange with peer to peer way is allowed between these neighbors and the router.

Figure 5-44 RIP Rule Configuration page

Step 4

Configure the routing pattern rule parameters. The parameter descriptions are shown in Table 5-24.

Table 5-24 RIP Parameter Description II

Parameter name	Meaning	How to Configure
Basic Settings		
Notification type	Add the type of RIP route.	Radio button selection. Select the type you want. • When you select Network, you need to configure the destination network address (typically a network directly connected to the router). • When you select Neighborhood, you configure the IP address of the neighbor (the IP address of the router to which the router is connected).

Parameter name	Meaning	How to Configure
Network (networks directly connected to the router can be added)	Add the destination network for RIP routing.	Fill in the destination network address where RIP routing needs to be added. Format: a.b.c.d/m, input specification see " Parameter specification table ".
Neighbor (router directly connected to the router)	Add the IP address of the neighbor of the RIP route.	Fill in the IP address of the neighbor that needs to add RIP routing. Format: a.b.c.d/m, input specification see " Parameter specification table ".

Step 5

Click Save to complete the RIP rule configuration.

NOTE

Routing Information Protocol (RIP) is a standard for exchanging routing information between gateways and hosts. RIP is an internal gateway protocol. In national networks, such as the current Internet, there are many routing protocols for the entire network.

- Exchange information only with neighboring routers. If communication between two routers does not pass through another router, the two routers are adjacent. RIP protocol, not adjacent routers do not exchange information.
- The information exchanged by the router is all the information known by the router. That is, its own routing table.
- The routing information is exchanged at a fixed time, such as every 30 seconds, and the router updates the routing table based on the received routing information.

The " distance " of the RIP protocol is also known as the " hop count ", because every time a router passes, the number of hops is increased by 1. RIP believes that good routing is the number of routers it passes through, that is, " short distance . " RIP allows a path to contain up to 15 routers. Therefore, when " distance " equals 16, it is equivalent to unreachable. Visible RIP only applies to small Internet.

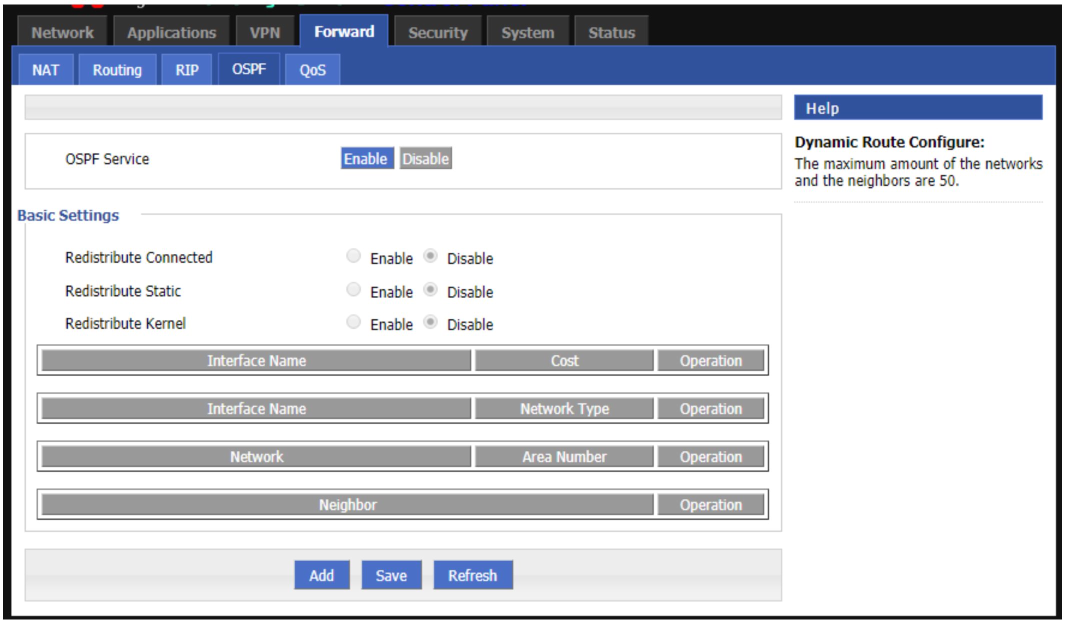
---End

OSPF configuration

The OSPF (Open Shortest Path First) protocol is one of the most widely used IGP (Internal Gateway Protocol) protocols for decision routing within a single autonomous system (AS) for large networks. Ospf services can be configured according to user needs when the MRR8860 Industrial Intelligent Gateway is shipped from the factory

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click Forward Settings>OSPF to open the OSPF tab, as shown in Figure 5-45.



OSPF Service [✓ Enable] Disable

Help

Dynamic Route Configure:
The maximum amount of the networks and the neighbors are 50.

Basic Settings

Redistribute Connected ○ Enable ● Disable

Redistribute Static ○ Enable ● Disable

Redistribute Kernel ○ Enable ● Disable

Interface Name	Cost	Operation

Interface Name	Network Type	Operation

Network	Area Number	Operation

Neighbor	Operation

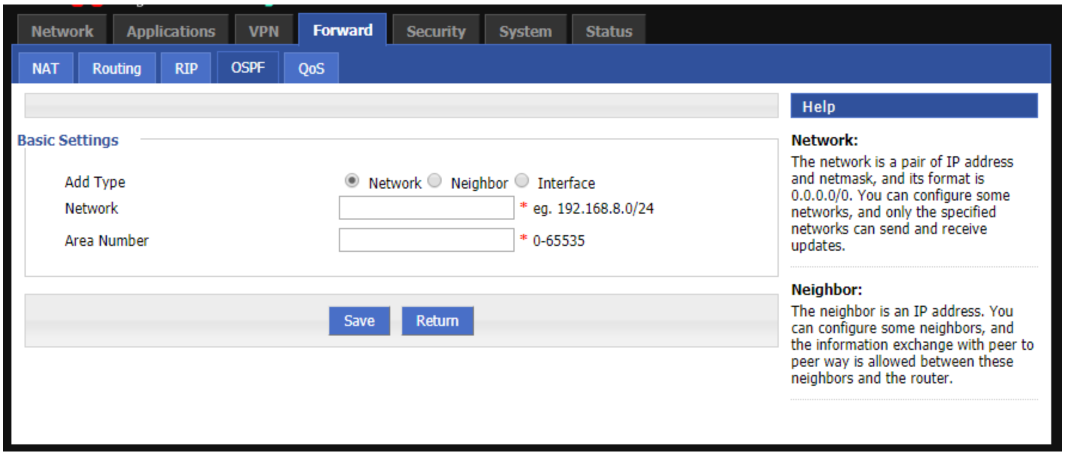
Figure 5-45 Ospf tab

The parameter descriptions are shown in Table 5-25.

Table 5-25 OSPF Parameter Description I

Parameter name	Meaning	How to Configure
OSPF service	Enable/Disable OSPF Service	Radio button selection.
Publish Connection Routing	Whether to allow publish connection routing	Radio button selection. Choose whether to allow publish connection routing based on your requirements.
Publish static route	Whether to allow publishing static routes	Radio button selection. Choose whether to allow publish static routes based on your requirements.
Publish kernel route	Whether to allow kernel routing to be published	Radio button selection. Choose whether to allow publish kernel routing based on your requirements.

Step 3 Click Add to create a new OSPF rule. The configuration interface is shown in Figure 5-46.



Basic Settings

Add Type ● Network ○ Neighbor ○ Interface

Network * eg. 192.168.8.0/24

Area Number * 0-65535

Help

Network:
The network is a pair of IP address and netmask, and its format is 0.0.0.0/0. You can configure some networks, and only the specified networks can send and receive updates.

Neighbor:
The neighbor is an IP address. You can configure some neighbors, and the information exchange with peer to peer way is allowed between these neighbors and the router.

Figure 5-46 Ospf rule configuration page

Step 4

Configure the routing pattern rule parameters. The parameter descriptions are shown in Table 5-26.

Table 5-26 OSPF Rule Parameter Description II

Parameter name	Meaning	How to Configure
Notification type	Add an OSPF routing type.	Radio button selection. Select the type you want. ● Network ● Neighborhood ● Interface
When Notify Type selects Network		
Network	Set a network segment as the router OSPF send address.	Format: A . B . C . D/M connector, input specification see Parameter Specification Table.
Domain address	Used to identify the network (OSPF protocol is used to exchange routing information only between routers with the same domain address).	Manual input, range of values: [0, 65535]
When Notify Type selects Neighborhood		
Neighborhood	The address of the device to which the router can hop.	Manual input, format: A . B . C . D/M connector, input specification refer to " Parameter Specification Table . "
When Notification Type selects Interface		

Parameter name	Meaning	How to Configure
Interface name	One of the router's interfaces	Drop-down list Selection: • br0 • modem • wlan0 • eth0
Interface properties	Configure the properties of the router interface, including both the overhead and network properties	Click Button Selection • Overhead • Network
Overhead	Configure the overhead of the router interface for OSPF routing table learning	Manual input, value range: 1-65535
Network type (configured when interface properties select Network)	Configure the network type of the router interface.	Drop-down list Selection: • broadcast • non-broadcast • point-to-multipoint • point-to-point

Step 5 Click Save to complete the OSPF rule configuration.

NOTE

OSPF routing protocol is a typical link-state routing protocol, which is generally used in the same routing domain. In this case, a routing domain is an autonomous system, which refers to a set of networks that exchange routing information with each other through a unified routing policy or routing protocol. In this AS, all OSPF routers maintain the same database describing the AS structure, which holds the status information of the corresponding links in the routing domain through which OSPF routers calculate their OSPF routing tables.

As a routing protocol for link state, OSPF transmits link state broadcast data LSA (Link State Advertisement) to all routers in a region, unlike the distance vector routing protocol. The distance vector routing protocol is to pass some or all of the routing tables to its neighboring router.

---End

5.6 VPN feature configuration

5.6.1 Overview

VPN (Virtual Private Network), a virtual private network, is a secure LAN based on the Internet . At present, the MRR8860 Industrial Intelligent Gateway supports not only the separate use of L2TP/PPTP/GRE/IPIP/IP/IPsec five VPN protocols, but also VPN over VPN, such as GRE over IPSec, IPTP/L2TP/GRE/IPIP and so on. Multi-layer VPN can be set up to better number off the user's communication data security.

5.6.2 VPDN configuration

VPDN (Virtual Private Dial-Up Networks), also known as Virtual Private Dial-Up Networks (VPDN), is a kind of VPN service, which is based on the virtual private dial network of dial-up users. That is, access to the Internet by dialing is a secure virtual private network built by combining the carrying function of IP network with the corresponding authentication and authorization mechanism, and is a technology developed rapidly with the development of Internet in recent years.

VPDN supports both L2TP and PPTP protocols.

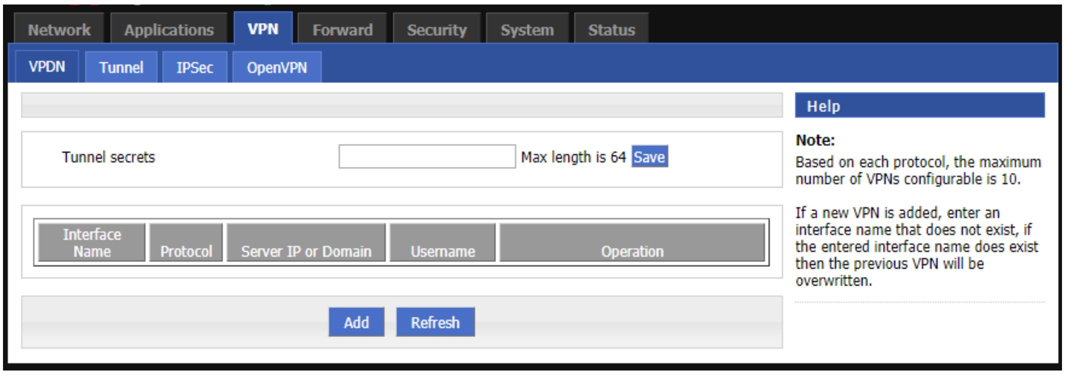
The PPTP (Point to Point Tunneling Protocol) peer-to-peer tunneling protocol is a network technology that supports multi-protocol virtual private networks and is also the second layer protocol. This protocol allows remote users to securely access the corporate network through the Windows mainstream operating system and other systems with point-to-point protocols, and to dial in local ISPs and securely connect to the corporate network over the Internet.

An abbreviation for the L2TP (Layer Two Tunneling Protocol) Layer 2 channel protocol, a VPDN (Virtual Private Dialing Network) technology designed for channel transfer of Layer 2 data. The L2TP provides a means of remote access control . A typical application scenario is where a company employee uses PPP to dial into the company's local network access server (NAS) to access the company's internal network, obtain an IP address, and access network resources with appropriate permissions. The employee is as secure and convenient as the company's local area network.

Step 1 Log in to the Web configuration interface for the MRR8860 Industry Smart Gateway.

Step 2

Click VPN Settings>VPDN Configuration to open the VPDN Configuration tab, as shown in Figure 5-47.



Tunnel secrets ____ Max length is 64 Save

Interface Name	Protocol	Server IP or Domain	Username	Operation

Add Refresh

Note:

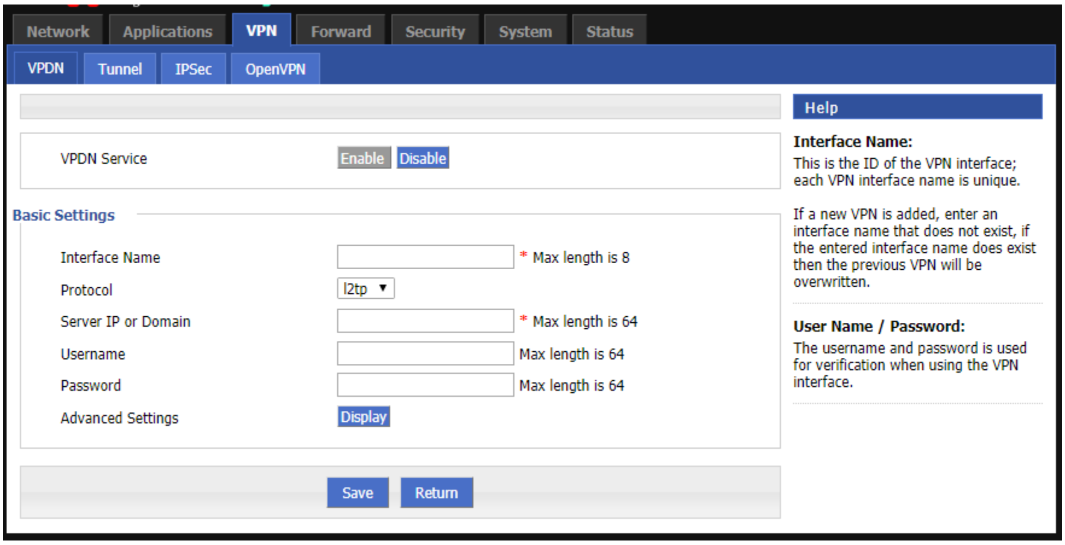
Based on each protocol, the maximum number of VPNs configurable is 10.

If a new VPN is added, enter an interface name that does not exist, if the entered interface name does exist then the previous VPN will be overwritten.

Figure 5-47 VPDN configuration tab

Step 3

Click Add to add a new VPDN rule. As shown in Figure 5-48.



VPDN Service

Basic Settings

Interface Name * Max length is 8

Protocol l2tp

Server IP or Domain * Max length is 64

Username Max length is 64

Password Max length is 64

Advanced Settings

Help

Interface Name:

This is the ID of the VPN interface; each VPN interface name is unique.

If a new VPN is added, enter an interface name that does not exist, if the entered interface name does exist then the previous VPN will be overwritten.

User Name / Password:

The username and password is used for verification when using the VPN interface.

Figure 5-48 VPDN configuration page

Step 4 Configure the VPDN rule parameters. The parameter descriptions are shown in Table 5-27.

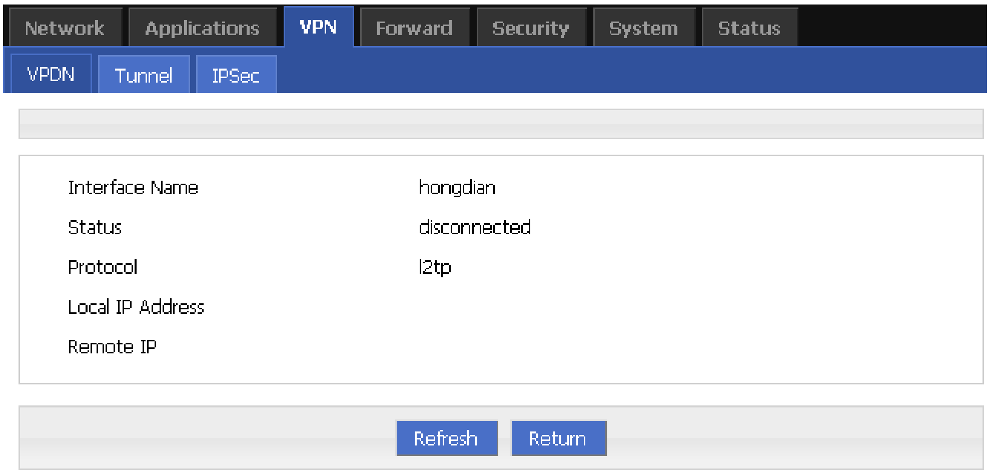
Table 5-27 VPDN Rule Parameter Description

Parameter name	Meaning	How to Configure
VPDN Service	Enable/disable this VPDN rule.	Click Enable to enable the rule.
Basic Settings		
Interface name	The name of this VPDN rule.	An easily identifiable name is recommended. Such as city-city, specific events (travel), and so on. Modification is not allowed after saving.
Protocol	Protocols used by VPDN, including: ● L2TP ● PPTP	Drop-down list selection. Depending on the actual setting, modification is not allowed after setting.
Service Address	The server IP address or domain name for access.	Fill in the server IP address or domain name for access.
User name	The legitimate access user authorized by the access server.	Fill in the legal access user name that the access server has authorized.
Password	The legal access user password that the access server has authorized.	Fill in the legal access user password that the access server has authorized.

Parameter name	Meaning	How to Configure
Advanced configuration	The PPP link negotiates advanced parameter settings, refer to the Mobile Network advanced parameter configuration for details.	Click and expand.

Step 5 Click Save to complete the VPDN rule configuration.

After completing a VPDN rule configuration, the router will automatically contact the service address and establish VPN communication. When the service address is connected, the router will be automatically added to the router on the terminal network instead of manually adding static routes, much less adding MASQ, which greatly reduces the user's operation. To view the status of a VPDN tunnel, click the View button for the tunnel, as shown in Figure 5-49.



Interface Name	hongdian
Status	disconnected
Protocol	l2tp
Local IP Address	
Remote IP	

Figure 5-49 L2TP Tunnel Status page

---End

5.6.3 Tunnel configuration

Tunnel technology is a way of transmitting data between networks through Internet infrastructure. The logical path through which the encapsulated packets pass over the public network is called a tunnel.

Tunnel configuration supports both GRE and IPIP modes.

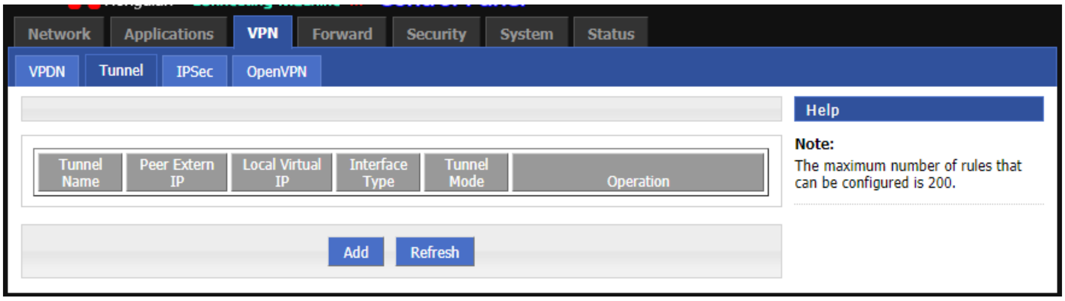
The GRE (Generic Routing Encapsulation) specifies how one network protocol can be used to encapsulate another. There are two main uses of the GRE protocol: Enterprise Internal Protocol Packaging and Private Address Packaging.

IPIP Tunneling is a simple protocol for encapsulating IP packets between two routers . IPIP Tunneling interfaces appear in the interface list like a physical interface . Many routers, including Cisco, basically support the protocol. This protocol enables multiple network distributions.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click VPN Settings>Tunnel Configuration to open the Tunnel Configuration tab, as shown in Figure 5-50.



Note:
The maximum number of rules that can be configured is 200.

Figure 5-50 Tunnel configuration page

Step 3 Click Add to add a new tunnel rule. The parameter descriptions are shown in Table 5-28.

Table 5-28 Tunnel Rule Parameter Description

Parameter name	Meaning	How to Configure
Tunnel service	Enable/disable the IP Tunneling service.	Click Enable to enable the tunnel rule.
Basic Settings		
Tunnel name	The name of the tunnel cannot be modified after saving.	Fill in the tunnel name that you want to set, and it is recommended that you use a name that is easy to recognize. Modification is not allowed after saving.
Tunnel mode	Tunnel operation mode, divided into: ● gre ● ipip	Drop-down list selection. Depending on the actual requirements settings, you cannot modify them after saving.
Interface virtual IP	The virtual IP address of the local tunnel.	Fill in the virtual IP address of the local GRE tunnel. Format: A . B . C . D/M, input specification see Parameter Specification Table.
Peer interface virtual IP	Virtual IP address of the peer tunnel	Fill in the virtual IP address of the opposite GRE tunnel. Format: Type A . B . C . D/M, input specification refer to Parameter Specification Table
Interface type	External interface type, select Interface or Static IP.	Drop-down list selection. Select Interface or Static IP depending on your requirements.
Local interface	The drop down box option that appears after the Interface Type selects Interface allows you to select any interface that you have built up	Drop-down list selection. Select External Interfaces for the Tunnel Local Network from the drop-down list.

Parameter name	Meaning	How to Configure
	as a local external interface (interface and modem built in VPDN settings).	
Local address	The drop-down box option that appears after the Interface ID selects Static IP. Set the local to external IP address.	Fill in the external interface IP of the local network of the tunnel. Format: A . B . C . D connector, input specification refer to the Parameter Specification Table.
Peer address	The external interface IP of the tunnel-to-end network is usually the public network IP (Internet) address, but also can be the enterprise different intranet IP.	Fill in the external interface IP of the tunnel-to-end network. Format: A . B . C . D connector, input specification refer to the Parameter Specification Table.

Step 4 Click Save to complete the tunnel rule configuration.

---End

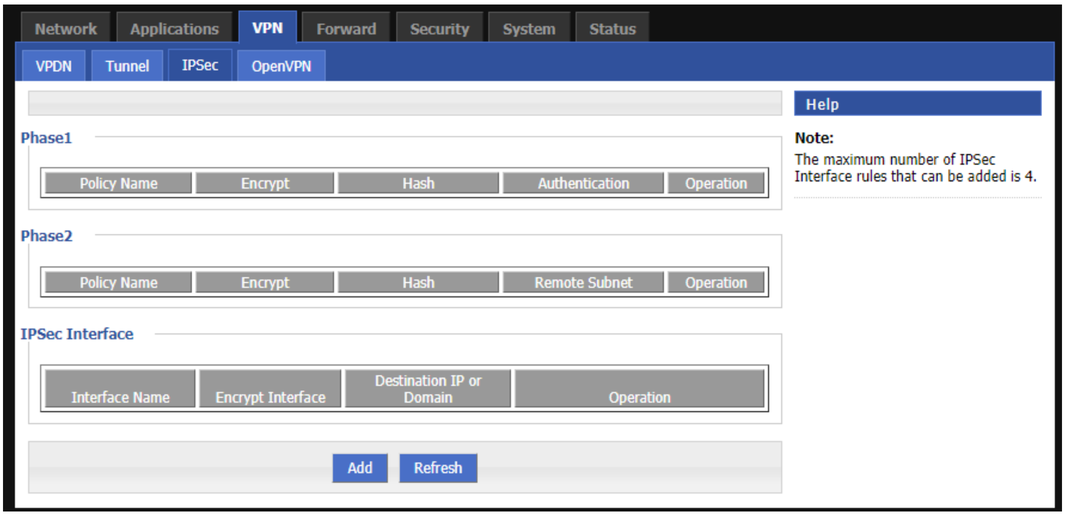
5.6.4 IPSec settings

IPSec (IP_Security) is a protocol built on top of the Internet Protocol (IP) layer. It allows two or more hosts to communicate in a secure manner. IPSec is the long-term direction of secure networking. It provides proactive protection against attacks on private networks and the Internet through end-to-end security. IPsec in the MRR8860 Industrial Intelligent Gateway uses a common Phase 1, which allows connection negotiation with most IPSec servers, while the MRR8860 Industrial Intelligent Gateway also supports IPSec pulling through other interfaces, such as through MODEM, eliminating manual user operation. IPSec has two modes: tunnel mode and transport mode.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click VPN Settings>IPSec Configuration to open the IPSec Configuration tab, as shown in Figure 5-51.



Phase1

Policy Name	Encrypt	Hash	Authentication	Operation

Phase2

Policy Name	Encrypt	Hash	Remote Subnet	Operation

IPSec Interface

Interface Name	Encrypt Interface	Destination IP or Domain	Operation

Note:
The maximum number of IPSec Interface rules that can be added is 4.

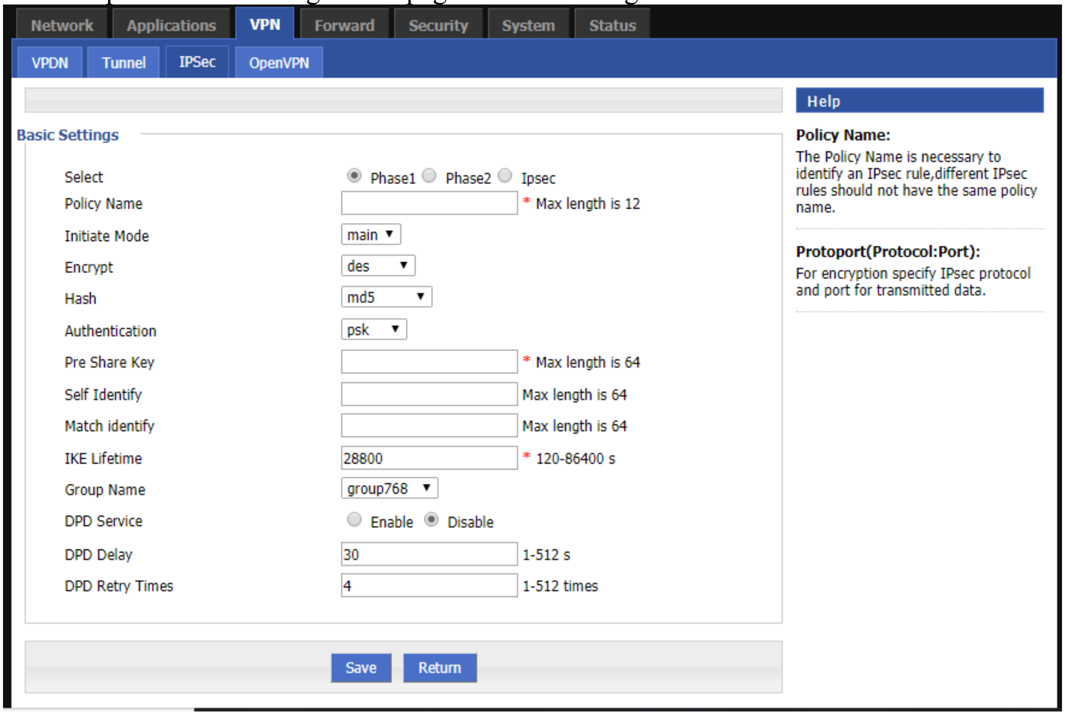
Figure 5-51 IPSec configuration tab

Step 3

Click Add to add a new IPSec rule. This IPSec page is divided into three phases of configuration, as follows:

1. First stage parameter configuration.

The first phase of the configuration page is shown in Figure 5-52.



Basic Settings

Select	● Phase1 ○ Phase2 ○ Ipsec	
Policy Name		* Max length is 12
Initiate Mode	main ▾	
Encrypt	des ▾	
Hash	md5 ▾	
Authentication	psk ▾	
Pre Share Key		* Max length is 64
Self Identify		Max length is 64
Match identify		Max length is 64
IKE Lifetime	28800	* 120-86400 s
Group Name	group768 ▾	
DPD Service	○ Enable ● Disable	
DPD Delay	30	1-512 s
DPD Retry Times	4	1-512 times

Help

Policy Name:
The Policy Name is necessary to identify an IPsec rule,different IPsec rules should not have the same policy name.

Protoport(Protocol:Port):
For encryption specify IPsec protocol and port for transmitted data.

Figure 5-52 IPsec Stage 1 configuration page

The IPsec rules Stage 1 parameters are described in Table 5-29.

Table 5-29 IPsec Rule Stage 1 Parameter Description

Parameter name	Meaning	How to Configure
Basic Settings		
Select	Sets the stage type for IPSec, including the first, second, and third stages.	Radio button selection. The first phase rule is added here, so select Phase 1.
Policy name	The name of the stage, primarily for the third stage match.	Fill in the name of the stage. Cannot modify after saving.

Parameter name	Meaning	How to Configure
Negotiation mode	The negotiation mode for the first phase of IPSec, including " main " and " aggr " (brutish mode).	Drop-down list selection. Select the startup mode that you want to set from the drop-down list, usually with NAT at both ends and USERID in the recommended " barbaric mode ".
Encryption mode	Supports DES, 3 DES, and AES encryption modes.	Drop-down list selection. Select the encryption mode to set from the drop-down list.
Hash algorithm	Supports both MD5 and SHA1 encryption algorithms.	Drop-down list selection. Select the encryption algorithm to set from the drop-down list.
Authentication mode	Pre-shared key mode authentication is supported.	Drop-down list selection. ● psk ● rsasig
Pre-shared key	Set the pre-shared key.	Fill in the preshared key that is preset by the IPSec peer server. An alphanumeric string with a maximum length of 64 bits . For input specifications, see the Parameter Specification Table.
Native identifier	Configure the IPSec native identifier to identify the local identity, and if not, the IP identifier.	Fill in the ipsec native ID, which is consistent with the ipsec peer server is preset peer ID. General Word type, input specification see " parameter specification table " ; In addition, the native presentation supports space input.
Peer ID	Configure an IPSec peer ID to identify the peer, or an IP if not configured.	Just fill in the IPSec peer ID, which is consistent with the native ID preset by the IPSec peer server. General Word type, input specification see " parameter specification table " ; In addition, the native presentation supports space input.
IKE Lifetime	IKE key lifetime.	Fill in the appropriate key lifecycle. Range of values: 120-86400 Unit: Seconds

Parameter name	Meaning	How to Configure
DH Group	Configured here as the key length for Phase 1 IKE negotiation.	Drop-down list selection. Select the appropriate group name from the drop-down list.
DPD detection	Enabling DPD detection, which requires peer server support for DPD peer detection, detects whether the IKE environment is normal or not, and immediately renegotiates the IKE environment to ensure the security of the IPSec environment and the stability and connectivity of the connection.	Click the button Select. Click Enable to enable the peer detection service.
Detection interval	Sets the DPD detection interval time.	Manual input Range of values: 1-512 Unit: Seconds
Retry Count	Maximum number of consecutive DPD detection failures.	Manual input Range of values: 1-512 Unit: Secondary

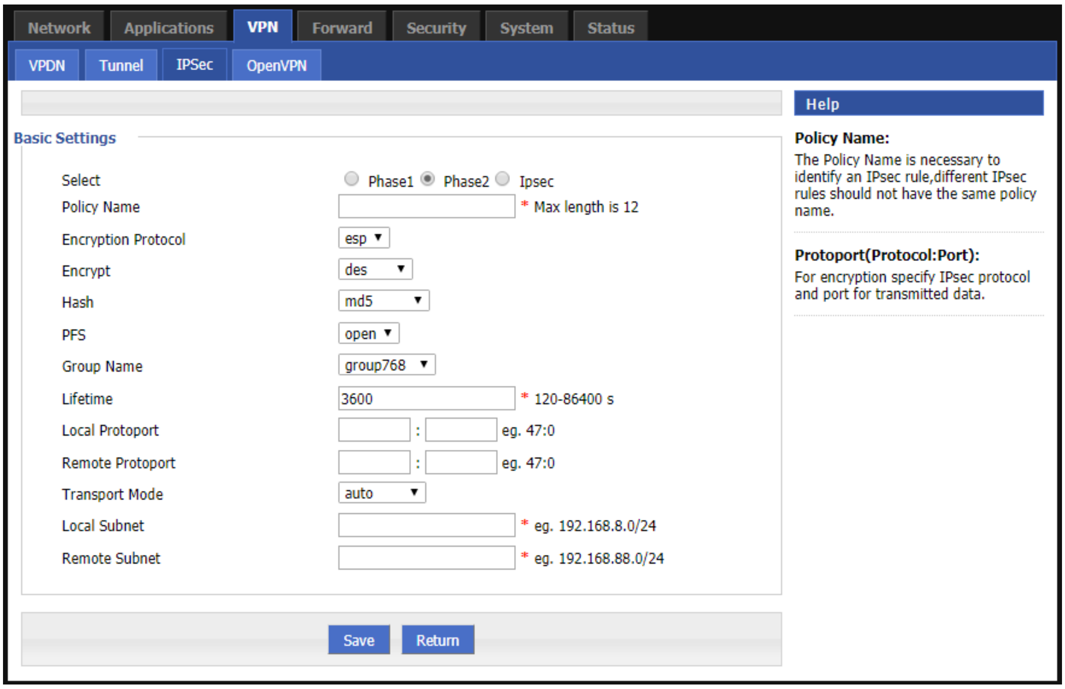
Click Save to complete the IPsec Stage 1 rule configuration.

2. Second stage parameter configuration.

The second stage parameter configuration page is shown in Figure 5-53.

CAUTION

In the above parameters, negotiation mode, encryption mode, hash algorithm, authentication mode, pre-shared key, IKE lifetime, DH group should be consistent with IPSec server settings. The native and peer IDs are to be consistent with the peer IDs in the IPSec server and the native IDs.



Basic Settings

Select ○ Phase1 ● Phase2 ○ Ipsec

Policy Name * Max length is 12

Encryption Protocol esp

Encrypt des

Hash md5

PFS open

Group Name group768

Lifetime 3600 * 120-86400 s

Local Protoport : eg. 47:0

Remote Protoport : eg. 47:0

Transport Mode auto

Local Subnet * eg. 192.168.8.0/24

Remote Subnet * eg. 192.168.88.0/24

Help

Policy Name:

The Policy Name is necessary to identify an IPsec rule,different IPsec rules should not have the same policy name.

Protoport(Protocol:Port):

For encryption specify IPsec protocol and port for transmitted data.

Figure 5-53 IPSec Stage 1 configuration page

The IPsec rules Stage 2 parameters are described in Table 5-31.

Table 5-30 IPsec Rule Phase 2 Parameter Description

Parameter name	Meaning	How to Configure
Basic Settings		
Select	Sets the stage type for IPSec, including the first, second, and third stages.	Radio button selection. The second phase rule is added here, so select Phase 2.
Policy name	The name of the stage, primarily for the third stage match.	Fill in the name of the stage. Cannot modify after saving.
Encryption mode	Supports DES, 3 DES, and AES encryption modes.	Drop-down list selection. Select the encryption mode to set from the drop-down list.
Hash algorithm	Supports both MD5 and SHA1 encryption algorithms.	Drop-down list selection. Select the encryption algorithm to set from the drop-down list.
Perfect forward encryption	Enabling or disabling perfect forward encryption increases the system overhead by enabling perfect forward encryption, but increases the	Drop-down list selection. Select Open or Close, depending on the settings for the peer IPSec server.

Parameter name	Meaning	How to Configure
	security of IPSec.	
DH Group	Used when perfect forward encryption is enabled, configured here as the key length negotiated by IPSec Phase 2 SA.	Drop-down list selection. Select the appropriate group name from the drop-down list.
Key survival time	IPSec SA (IPSec security alliance) key lifetime.	Fill in the appropriate key lifecycle. Range of values: 120-86400 Unit: Seconds
Local protocol port	Configuring protocols and ports that require encryption on the local side	Enter manually, enter the protocol code in the front box, and port in the back box.
Remote protocol port	Configuring protocols and ports that require encryption on a peer	Enter manually, enter the protocol code in the front box, and port in the back box.
Transmission mode	Supports tunnel mode, transport mode, or automatic selection.	Drop-down list selection. Select the desired transfer mode from the drop-down list.
Local Subnet	The local subnet configuration.	You do not need to configure subnets in transport mode, and you need to configure in automatic and tunnel mode. Fill in the local subnet address. Format: A.B.C.D/M, input specification see Parameter Specification Table.
Remote terminal network	Remote terminal network configuration.	You do not need to configure subnets in transport mode, and you need to configure in automatic and tunnel mode. Fill in the remote terminal network address. Format: A.B.C.D/M, input specification see Parameter Specification Table.

Click Save to complete the IPSec Phase 2 rule configuration.

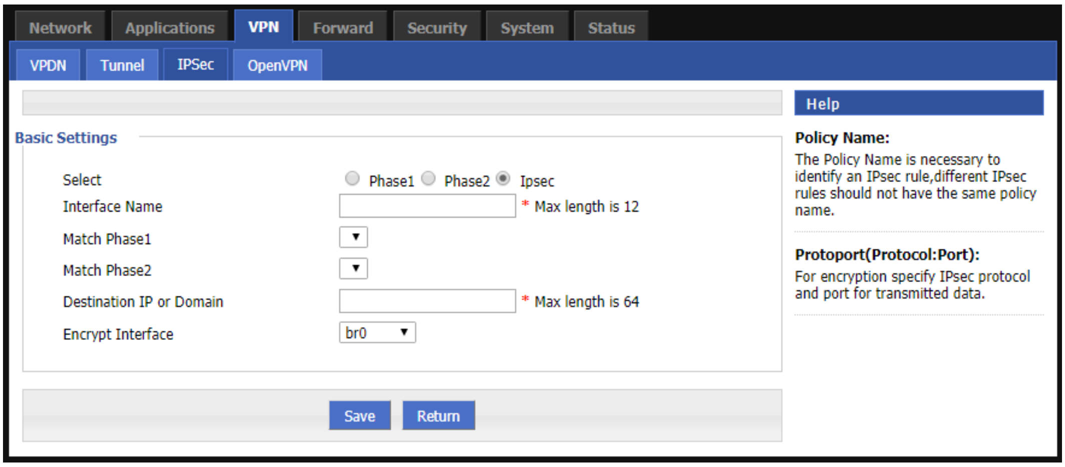
CAUTION

In the above parameters, the transmission protocol, encryption mode, hash algorithm, DH group, perfect forward encryption, key survival time and so on are consistent with the IPSec server configuration ; If the transport mode is set to Automatic or Tunneling mode, the local and remote subnets are aligned with the configuration of the remote and local subnets in the IPSec server.

The protocol code of the local protocol port and the remote protocol port must be consistent, indicating encryption of one protocol ; When the local protocol port and the remote protocol port are configured, IPsec input encrypts the protocol and port, and other communication is not encrypted ; When this parameter is not configured, IPsec encrypts all communications.

2. Matches the stage parameter configuration.

The Match stage configuration page is shown in Figure 5-54.



Basic Settings

Select ○ Phase1 ○ Phase2 ● Ipsec

Interface Name * Max length is 12

Match Phase1

Match Phase2

Destination IP or Domain * Max length is 64

Encrypt Interface br0

Help

Policy Name:

The Policy Name is necessary to identify an IPsec rule,different IPsec rules should not have the same policy name.

Protoport(Protocol:Port):

For encryption specify IPsec protocol and port for transmitted data.

Figure 5-54 IPsec Match Stage Configuration page

Configure the IPSec Rule Match stage parameters and click Save when you are finished configuring.

NOTE

When the encryption interface selects BR0 and the BR0 interface has more than one address, IPsec selects an IP1 address with an address of BR0.

IPsec rule matching stage parameters are explained in Table 5-31.

Table 5-31 IPsec Rule Match Stage Parameter Description

Parameter name	Meaning	How to Configure
Basic Settings		
Select	Sets the stage type for IPSec,	Radio button selection.

Parameter name	Meaning	How to Configure
	including the first, second, and third stages.	The rules for matching stages are added here, so select IPSec.
Interface name	The name of the stage, primarily for the third stage match.	A maximum of 12 bit string is allowed. Fill in the name of the stage. Cannot modify after saving.
Phase1 Match Phase 1	Select the policy name that you want to match for the IPsec Phase 1 configuration.	Drop-down box options. Select the policy name for the first stage configuration.
Phase2 Match Phase 2	Select the policy name that you want to match for the IPSec Phase 2 configuration.	Drop-down box options. Select the policy name for the second stage configuration.
Service Address	IPsec peer server IP or domain name.	Fill in the IPsec peer server IP or domain name. A maximum of 64 bit string is allowed.
Encryption interface	By selecting the binding interface of IPsec and binding the VPDN/MODEM/BR0 interface as the local terminal of IPsec negotiation, network applications such as IPSECOVER VPDN can be implemented . In addition, IPsec rules will change with the changing state of the bound interface, and the connection of IPsec on the dialing interface can be restored as quickly as possible to ensure the connectivity of IPsec.	Drop-down list selection. Select the appropriate interface from the drop-down list.

---End

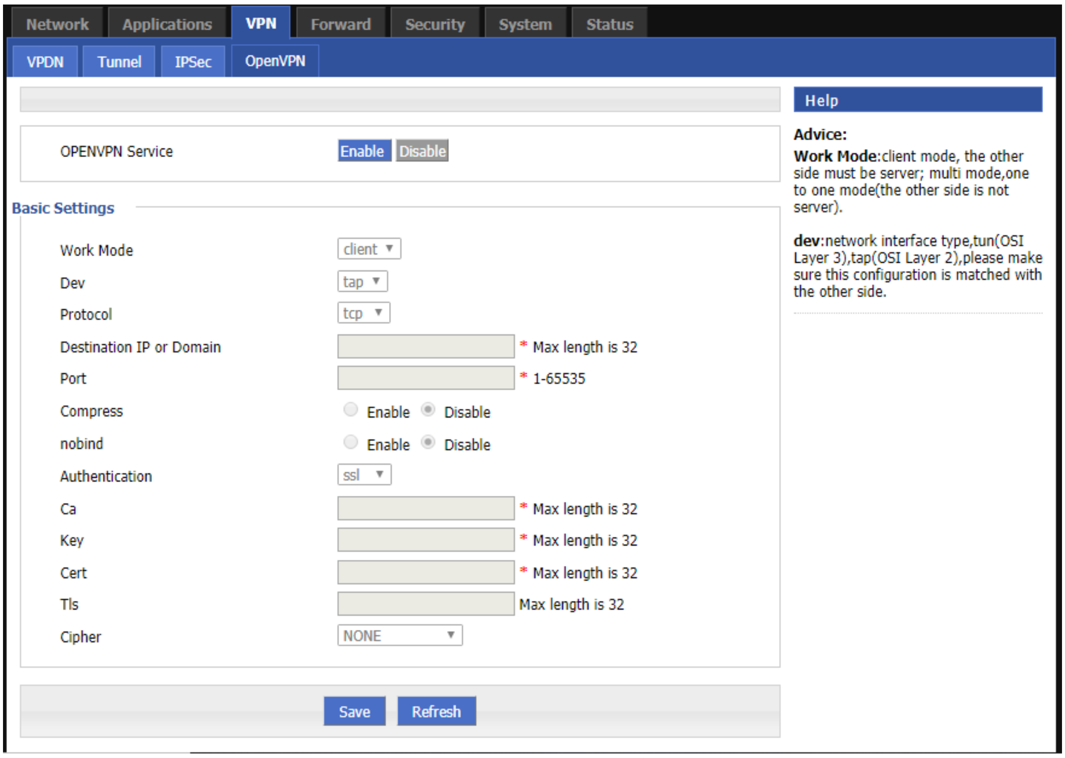
5.6.5 Open VPN Settings

Open VPN is an application layer VPN implementation based on the OpenSSL library. Compared with traditional VPN, its advantage is simple and easy to use. Open VPN All communications are based on a single IP port, with UDP protocol by default and TCP supported. Open VPN connections work well with most proxy servers and in NAT environments. The server has the ability to " push " certain network configuration information to the client, including IP addresses, routing settings, and so on. The Open VPN provides two virtual network interfaces: a generic TUN/TAP driver, through which you can build a three-tier IP tunnel or a virtual two-tier Ethernet that can transmit any type of two-tier Ethernet data. The official port assigned to Open VPN by IANA (Internet Assigned Numbers Authority) is 1194 .

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click VPN Settings>Open VPN Configuration to open the Open VPN Configuration tab, as shown in Figure 5-55.



OPENVPN Service Enable Disable

Basic Settings

Work Mode client

Dev tap

Protocol tcp

Destination IP or Domain * Max length is 32

Port * 1-65535

Compress ○ Enable ● Disable

nobind ○ Enable ● Disable

Authentication ssl

Ca * Max length is 32

Key * Max length is 32

Cert * Max length is 32

Tls Max length is 32

Cipher NONE

Advice:

Work Mode:client mode, the other side must be server; multi mode,one to one mode(the other side is not server).

dev:network interface type,tun(OSI Layer 3),tap(OSI Layer 2),please make sure this configuration is matched with the other side.

Figure 5-55 OpenVPN configuration page

Step 3 Configure the Open VPN parameters as shown in Table 5-32.

Table 5-32 OpenVPN Parameter Description

Parameter name	Meaning	How to Configure
OpenVPN service	Enables the OpenVPN service.	Radio button selection. • Enable • Disabling
Basic Settings		
Working mode	Supports both Client and Multi-mode of operation • Client pattern is client type pattern • Multi mode is one to one mode of operation (opposite end is non-server)	Drop-down list selection. Select the desired working mode from the drop-down list.
Dev	Dev represents the network interface type. Supports both TUN and TAP types • tun（OSI Layer 3）：tun simulates network layer devices and operates Layer 3 packets, such as IP	Drop-down list selection. Select the desired working mode from the drop-down list. Requirements remain

Parameter name	Meaning	How to Configure
	packets. • tap（OSI Layer 2）：tap is the equivalent of an Ethernet device that operates Layer 2 packets, such as Ethernet data frames.	consistent with the other end.
Protocol	Data transfer protocol type settings. • TCP: TCP protocol is a connection-oriented reliable transmission protocol, which is suitable for high reliability requirements and low sensitivity to communication efficiency. • UDP: UDP protocol is a non-connected and unreliable transmission protocol, which is suitable for the situation of high efficiency and low reliability.	Drop-down list selection. Select the desired transport protocol from the drop-down list Requirements remain consistent with the other end.
Destination address or domain name	Specifies the server address of the connection.	Word type, maximum 32 bytes, input specification see Parameter Specification Table. Requirements remain consistent with the other end.
Destination port	Specifies the port to connect to the server.	Range of values: 1-65535 • Default: 1194 Requirements remain consistent with the other end.
Compress	Compression protocol: Configuring whether VPN connection compression is turned on If the server is turned on, the client must be turned on	Radio button selection. • Enable • Disabling
nobind	Configuring whether to bind specific local port numbers	Radio button selection. • Enable • Disabling
Certificate	Configuring how VPN data is transmitted • ssl： Encrypting network connections at the transport layer with high security • text：Transferred as text during transfer with low safety factor	Drop-down list selection. Select the desired data transfer mode from the drop-down list
Ca	Specifies the file path for the client CA certificate	Word type, maximum 32 bytes, input specification see Parameter Specification Table.

Parameter name	Meaning	How to Configure
Key	Specifies the private key path for the current client	Word type, maximum 32 bytes, input specification see Parameter Specification Table.
Cert	Specifies the certificate file path for the current client	Word type, maximum 32 bytes, input specification see Parameter Specification Table.
Tls	Turn on TLS, and if the server is turned on, the client must also be turned on. TLS: Secure Transport Layer Protocol (TLS) is used to provide confidentiality and data integrity between two communication applications. The protocol consists of two layers: TLS Record and TLS Handshake	Word type, maximum 32 bytes, input specification see Parameter Specification Table.
Cipher	SSL encryption algorithm system	Drop-down box option • NONE • BF-CBC • DES-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC

Step 4 Click Save to complete the Open VPN configuration.

---End

5.7 System management configuration

5.7.1 Overview

The MRR8860 industrial intelligent gateway system management function mainly carries on some daily maintenance operation to the system. For example: Log analysis of system performance, user account information management, network testing, system file upgrades, and so on.

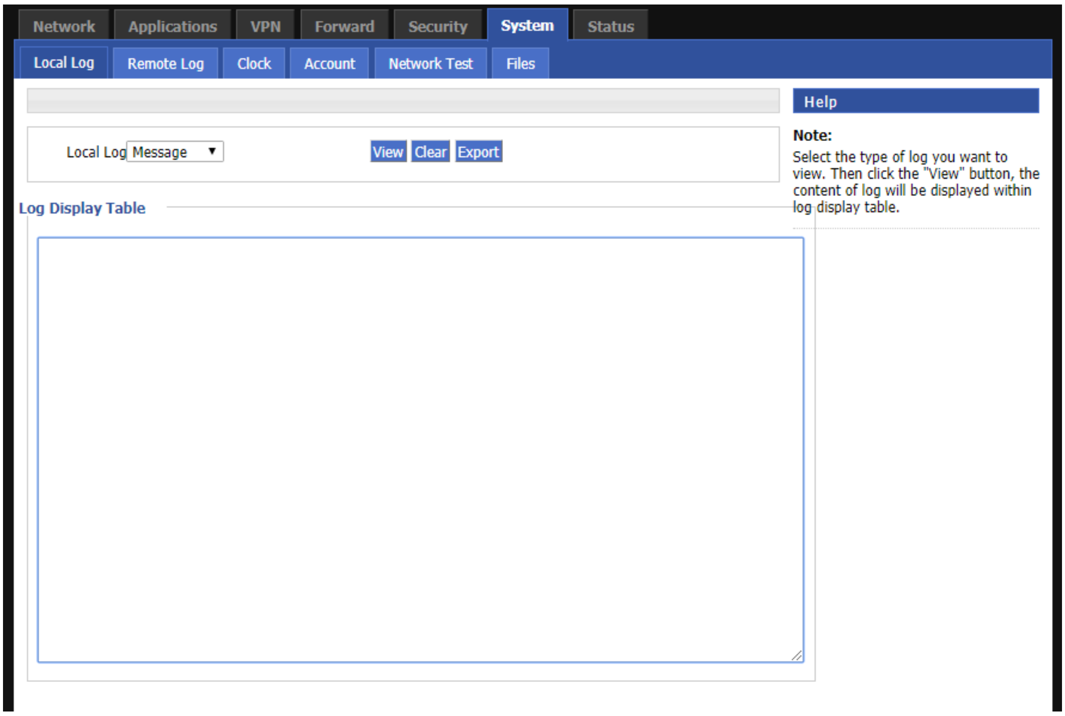
5.7.2 Local log

Local logs refer to information such as system operation, operation configuration, and so on, directly viewed through the MRR8860 Industrial Intelligent Gateway management interface.

This information enables you to find system anomalies and pinpoint problems and take effective precautions or remedies.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click System Administration>Local Log to open the Local Log tab, as shown in Figure 5-56.



Note:
Select the type of log you want to view. Then click the "View" button, the content of log will be displayed within log display table.

Figure 5-56 Local log tab

Step 3

Select the type of log you want to query in the System Log and click View to display the log you are querying in the Log List.

You can also click Clear to clear the log information in the Log List ; Click Export to export log information locally.

There are three types of log classifications:

- Message: The system log, which records the router run log, generally only applies to the system log.
- Application: The application log, which records information such as on or off of the router process.
- Kernel: Program kernel log, print kernel information, usually viewed by developers for reference.

---End

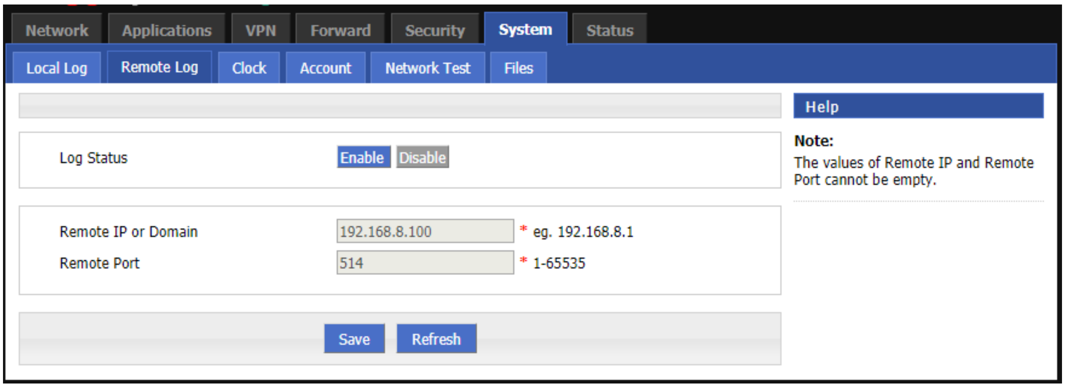
5.7.3 Remote Log

The Remote Log is used primarily to connect to the remote log server, and the router can upload the local log to the remote log server as follows:

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click System Administration>Remote Log to open the Remote Log tab, as shown in Figure 5-57.



Log Status

Remote IP or Domain 192.168.8.100 * eg. 192.168.8.1

Remote Port 514 * 1-65535

Note:
The values of Remote IP and Remote Port cannot be empty.

Figure 5-57 Syslog tab

Step 3 Configure system log parameters. The parameter descriptions are shown in Table 5-33.

Table 5-36 Syslog parameter descriptions

Parameter name	Meaning	How to Configure
Log Status	Enable/disable remote logging.	Click Enable to enable the syslog feature.
Remote log server address	The IP address of the remote log server (either the IP address of the LAN-side PC or the public network address).	Fill in the IP address of the PC that receives the log information.
Remote log server port number	The port number of the remote log server.	Fill in the port number of the remote log server, which defaults to 514 .

Step 4 Click Save to complete the system log parameter configuration.

NOTE

After the router sends the system log to the remote log server address, it receives it using the syslog facility ; The syslog facility allows you to differentiate between logs to different routers and functions, making it easy for users to view logs.
The syslog tool can be downloaded from the Shenzhen Hongdian Technology Ltd. website.

---End

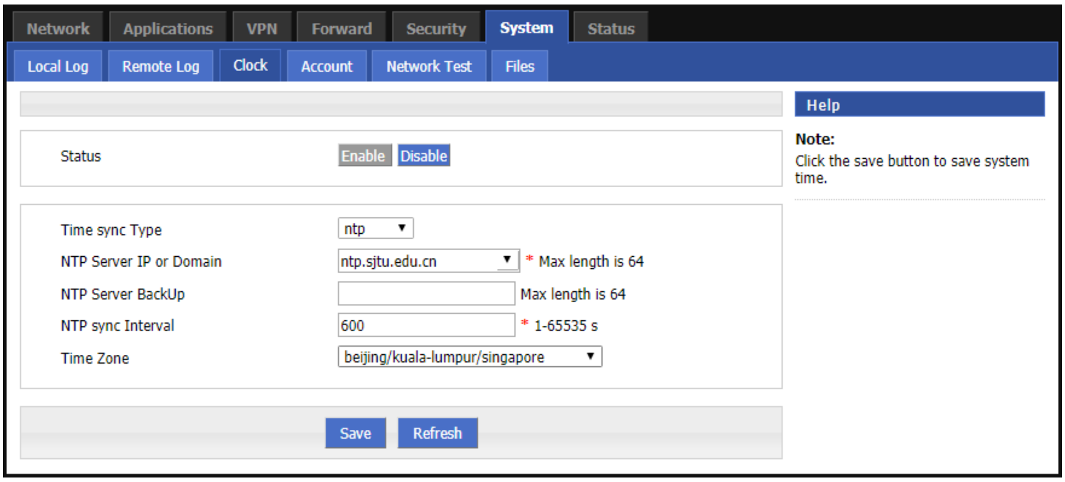
5.7.4 System Time

The MRR8860 Industrial Intelligent Gateway supports NTP (Network Time Protocol) network protocol pairs. NTP network can ensure that the system time of the router corresponds to the actual time, and the task management functions can be performed at the correct time. The steps are as follows.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click System Administration>System Time to open the System Time tab and, depending on the Time Synchronization Type, the displayed pages are shown in Figure 5-58 and Figure 5-59.



Status Enable Disable

Time sync Type ntp

NTP Server IP or Domain ntp.sjtu.edu.cn * Max length is 64

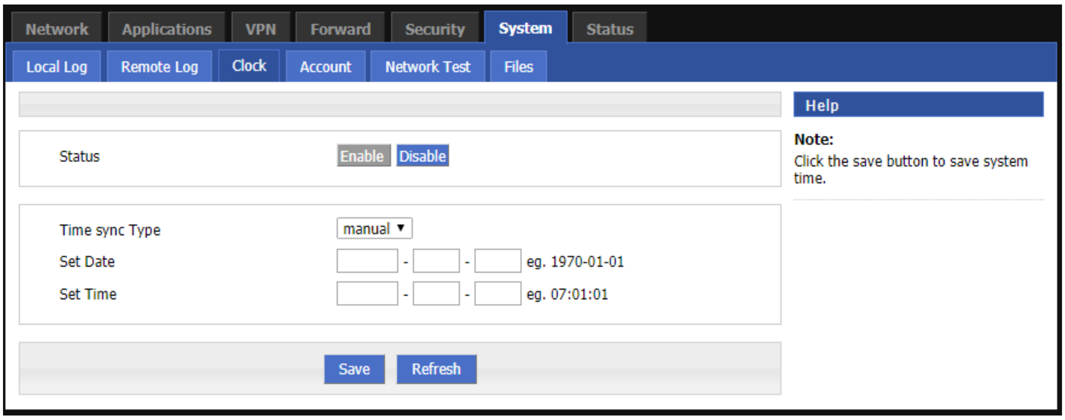
NTP Server BackUp Max length is 64

NTP sync Interval 600 * 1-65535 s

Time Zone beijing/kuala-lumpur/singapore

Note:
Click the save button to save system time.

Figure 5-58 Network time synchronization mode



Status Enable Disable

Time sync Type manual

Set Date - - eg. 1970-01-01

Set Time - - eg. 07:01:01

Note:
Click the save button to save system time.

Figure 5-59 Manual mode synchronization time

Step 3 Configure the system time parameters. The parameter descriptions are shown in Table 5-34.

Table 5-37 System time parameter descriptions

Parameter name	Meaning	How to Configure
Status	Enable or Disable system time synchronization.	● Click Enable to enable the system time synchronization feature.

Parameter name	Meaning	How to Configure
		● Click Disable to disable the system time synchronization feature.
Time synchronization type	The type of time synchronization for system time checking.	Select from the list box below. ● NTP Network Time Proofreading ● Manual proofreading
When Time Sync Type selects Network Time		
Primary server address	NTP clock server domain name.	Select the appropriate NTP clock server domain name from the drop-down list.
Alternate server address	An alternative NTP server domain name or IP address, where the primary server is unavailable or cannot be synchronized to time, is generally not configured.	Manually enter the server domain name or IP address.
Synchronization interval	The frequency at which NTP synchronizes with the server time, such as automatic alignment every 10 minutes (600 seconds).	Range of values: 1-65535 Unit: Seconds Default: 600
Time zone	Geographic time zone.	Select the time zone in which the router is located from the drop-down list.
When Time Synchronization Type selects Manual (This page shows only the configured time, System Real Time is in the upper right corner of the Web page)		
Date	The standard date for the check.	Format is YYYY-MM-DD Such as 1970-01-01
Clock	The standard time for the verification.	Format is hh: mm: mm Such as 07: 01: 01

Step 4 Click Save to complete the system log parameter configuration.

---End

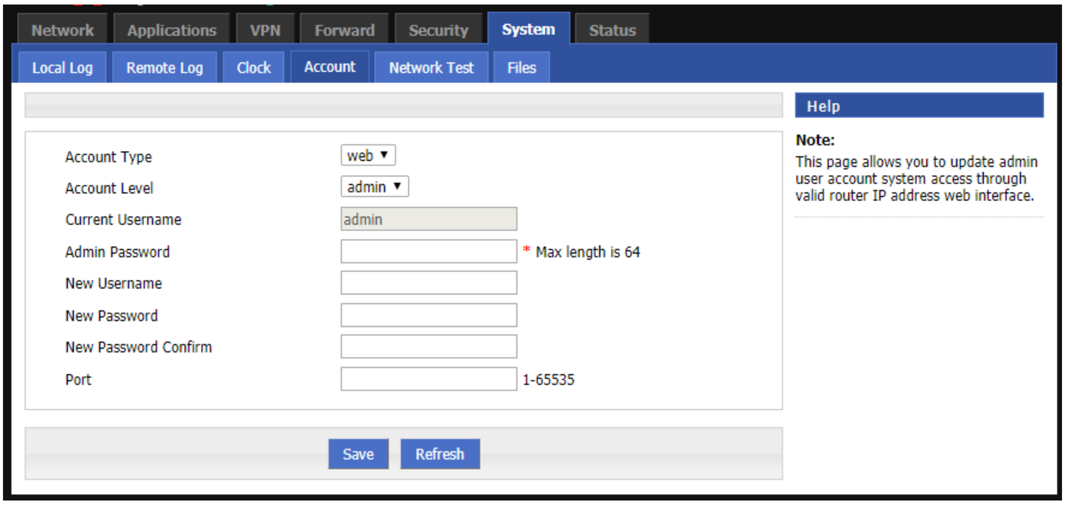
5.7.5 User Management

User Management provides the ability for users to modify user names/passwords. At the same time, user management can modify the router's Web access port to mask other user access routes.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click System Administration>User Management to open the User Management tab, as shown in Figure 5-60 .



Account Type: web

Account Level: admin

Current Username: admin

Admin Password: * Max length is 64

New Username

New Password

New Password Confirm

Port: 1-65535

Note:
This page allows you to update admin user account system access through valid router IP address web interface.

Figure 5-60 User Management Configuration page

Step 3 Configure user management parameters. The parameter descriptions are shown in Table 5-35.

Table 5-35 User management parameter description

Parameter name	Meaning	How to Configure
Account Type	Log in to the router through a web page.	Drop-down list selection.
User level	The user level at which the router is logged in.	Select from the drop-down list. ● admin: Administrator, ability to view and modify parameters ● guest: General users, in addition to viewing the page, can also log everywhere and use network testing capabilities.
Current User Name	The user currently logged on to the router page.	Cannot be configured to display as the currently logged in user.
Enter old password	The login password of the current login user.	Enter the login password for the currently logged in user.
Enter a new user name	User is modified user name.	Manually enter a Word string with a maximum length of 64 bits . For input specifications, see the Parameter Specification Table.
Enter a new password	The user is modified password.	Manually enter a Word string with a maximum length of 64 bits . For input specifications, see the Parameter Specification Table.
Confirm New Password	The user modified the password, the modified confirmation password.	Manually enter a Word string with a maximum length of 64 bits . For input specifications, see the Parameter Specification Table.

Parameter name	Meaning	How to Configure
Port	User login router page port.	Manual input Range of values 1-65535 Default: 80

NOTE

User management only provides user modification, not add, delete, and so on.
If the " port " parameter has not been modified, then directly enter the router IP address can log on to the router page ; If the port is modified to a different number and the modification is successful, you need to enter the router's IP: port to log in to the router page.
The admin user can only modify the admin itself password, but not the guest password and parameters ; Guest itself does not have user management capabilities.

Step 4

Click Save when you have finished modifying. After the save is successful, the page or automatically jumps to the login interface and the user needs to enter the modified user name/password to enter.

---End

5.7.6 Network test

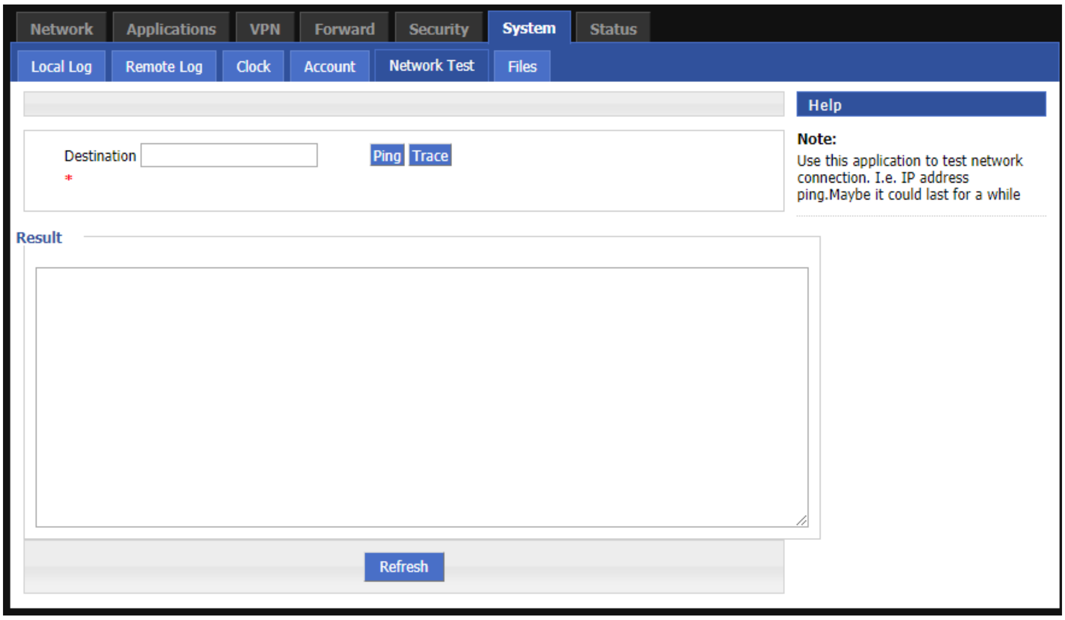
Network test

Network testing, which includes common ping and traceroute functions, uses the following steps:

Step 1 Log in to the MRR8860 router web configuration interface.

Step 2 Click System Administration>Network Testing.

Open the Network Test tab, as shown in Figure 5-61 .



Note:
Use this application to test network connection. I.e. IP address ping.Maybe it could last for a while

Figure 5-61 Network Test Configuration page

Step 3

In the Detect Address box, enter the IP address or domain name that you want to test, click Ping to test the router's connectivity to the destination address.

The parameters and button descriptions are shown in Table 5-36.

Table 5-39 Local log parameter descriptions

Parameter name	Meaning	How to Configure
Destination address	Set the destination IP address or domain name for the test.	Fill in the destination IP address or domain name that you want to use for the test.
PingPing	Use the ping command to test network connectivity.	Click Ping.
Trace	Use the trace command to test the number of hops that the router has reached the destination address.	Click this button to use the trace command.
Inspection results	The results of the network test.	None.

说明

Trace: that is traceroute, through traceroute we can know the information from the computer to the other end of the Internet host is to go what path ; Measure how long it takes to send a small packet to the destination device until it returns. Each device traceroute on a path is measured three times. The output includes the time of each test (ms) and the name of the device, if any, and its IP address.

---End

5.7.7 File upgrade

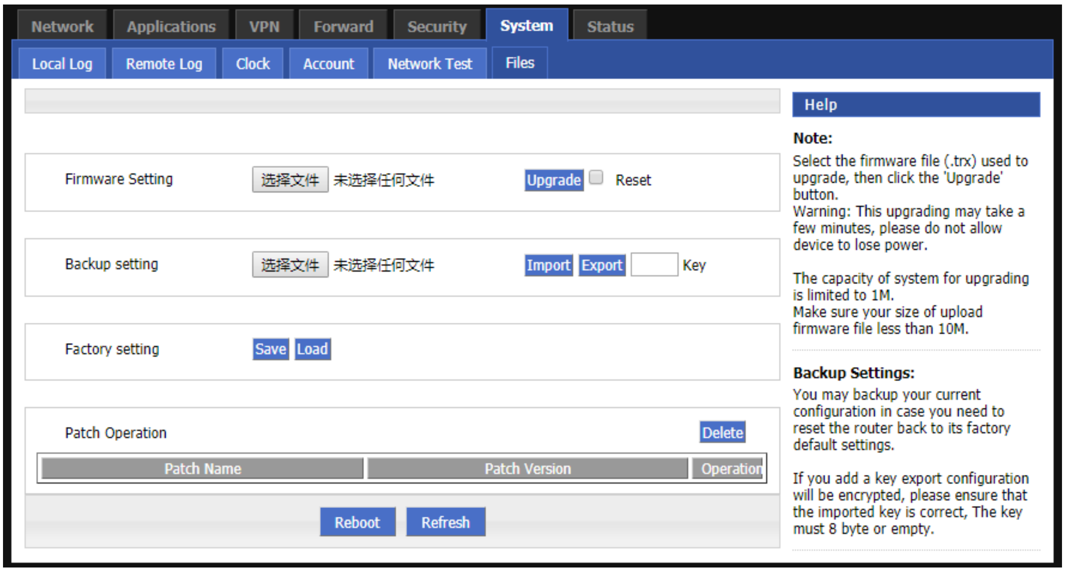
Upgrade Settings

The MRR8860 Industrial Smart Gateway supports local network mode upgrade system files . Before upgrading, make sure that you have the target file for the system update and save the update file on the computer where the LAN is located.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2 Click System Administration>File Upgrade.

The File Upgrade interface is displayed, as shown in Figure 5-62 .



Firmware Setting 选择文件 未选择任何文件 Upgrade □ Reset

Backup setting 选择文件 未选择任何文件 Import Export Key

Factory setting Save Load

Patch Operation Delete

Patch Name	Patch Version	Operation

Reboot Refresh

Note:
Select the firmware file (.trx) used to upgrade, then click the 'Upgrade' button.
Warning: This upgrading may take a few minutes, please do not allow device to lose power.

The capacity of system for upgrading is limited to 1M.
Make sure your size of upload firmware file less than 10M.

Backup Settings:
You may backup your current configuration in case you need to reset the router back to its factory default settings.

If you add a key export configuration will be encrypted, please ensure that the imported key is correct, The key must 8 byte or empty.

Figure 5-62 File upgrade page

Step 3

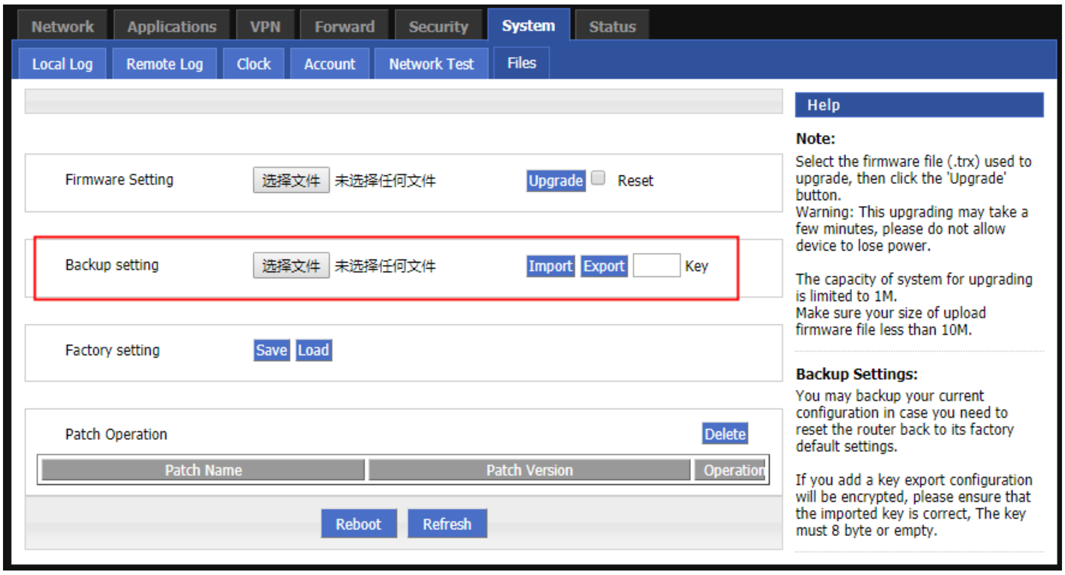
Click Browse, select the upgrade file locally, and click Upgrade to start the upgrade. Select Restore Defaults to restore the router configuration to the factory settings after the patch or program is upgraded ; Unchecked, means that only patches or programs are upgraded and the router's parameter configuration is maintained.

---End

Backup Settings

The MRR8860 Industry Smart Gateway supports backup and restore of configuration files, as shown in Figure 5-63 .

- Click Browse, browse for the local configuration file that you want to import, and click Import to complete the import of the file. If the router parameter is incorrect or the file is missing, you can use the Import function to restore the parameter.
- Click Export to export the configuration file locally for file/parameter backup.



Note:

Select the firmware file (.trx) used to upgrade, then click the 'Upgrade' button.

Warning: This upgrading may take a few minutes, please do not allow device to lose power.

The capacity of system for upgrading is limited to 1M.

Make sure your size of upload firmware file less than 10M.

Backup Settings:

You may backup your current configuration in case you need to reset the router back to its factory default settings.

If you add a key export configuration will be encrypted, please ensure that the imported key is correct, The key must 8 byte or empty.

Figure 5-63 Backup function

NOTE

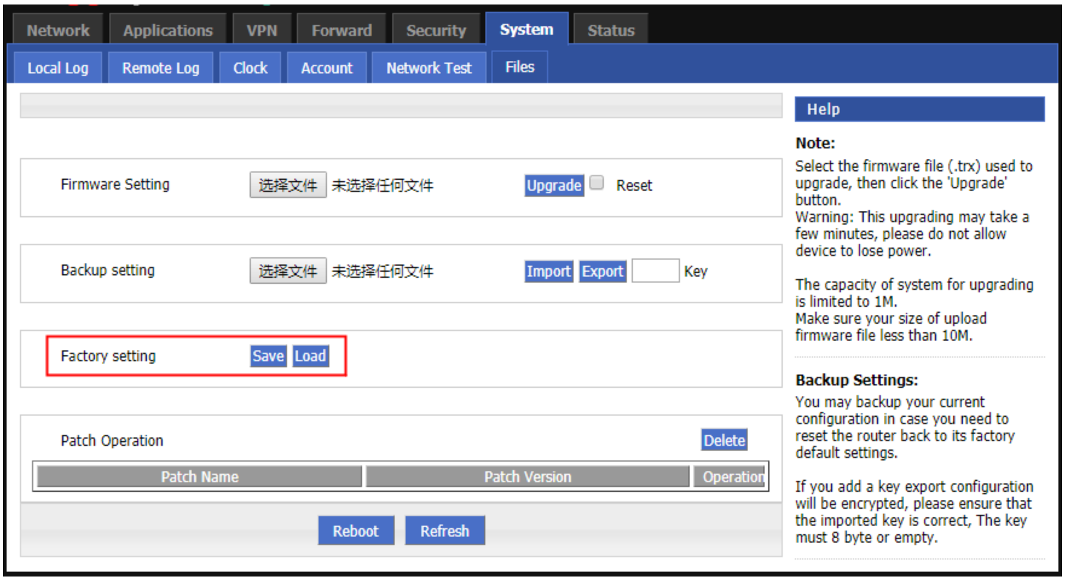
After you import the backup file, the system automatically restarts before it takes effect after you restart the system.

Key: When exporting a file, add the encryption key, which needs to be entered when importing the file, otherwise the router will be corrupted ; The key may not be filled in. If the key is entered incorrectly when you import, you will not be able to enter the router page.

If the key is output, the key must be eight bits.

Factory settings

The MRR8860 Industrial Intelligent Gateway has common factory setup functions and can be restored to the factory setup state as needed. You can also make the existing configuration the default configuration and generate a default configuration file in the router where the user can click Restore Defaults to restore the configuration to the default configuration at any time. If the default profile is deleted or deleted, the router reverts to the original factory settings.



Note:

Select the firmware file (.trx) used to upgrade, then click the 'Upgrade' button.

Warning: This upgrading may take a few minutes, please do not allow device to lose power.

The capacity of system for upgrading is limited to 1M.

Make sure your size of upload firmware file less than 10M.

Backup Settings:

You may backup your current configuration in case you need to reset the router back to its factory default settings.

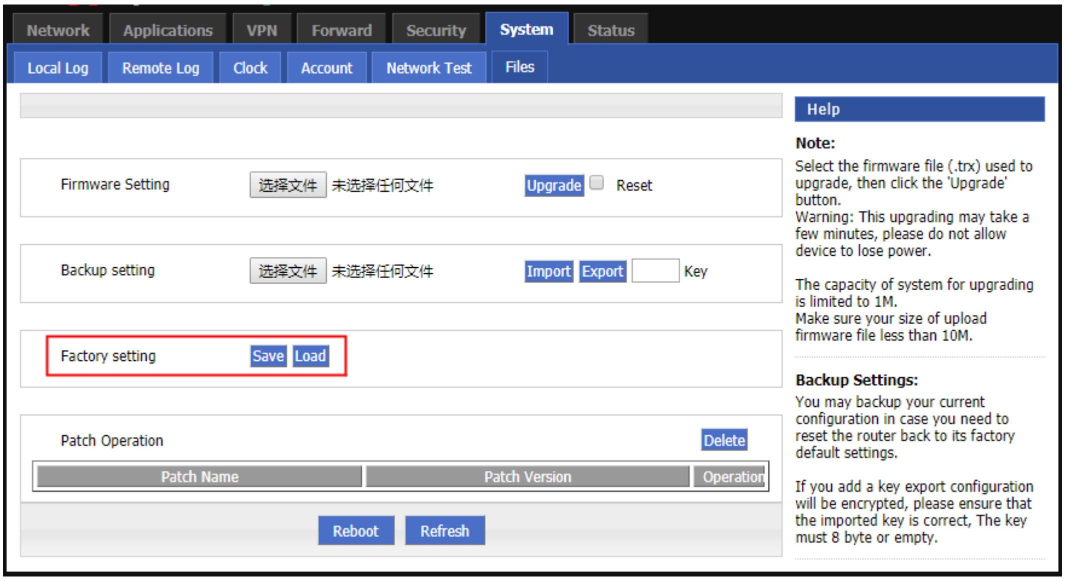
If you add a key export configuration will be encrypted, please ensure that the imported key is correct, The key must 8 byte or empty.

Figure 5-64 Factory Setup Page

- Set to Default: saves the current configuration as the default factory configuration.
- Restore the default: Restore the factory configuration.

Viewing patch information

The MRR8860 Industry Smart Gateway has the ability to view patch information, view patch information under the patch folder, and delete all patch files.



Note:

Select the firmware file (.trx) used to upgrade, then click the 'Upgrade' button.

Warning: This upgrading may take a few minutes, please do not allow device to lose power.

The capacity of system for upgrading is limited to 1M.

Make sure your size of upload firmware file less than 10M.

Backup Settings:

You may backup your current configuration in case you need to reset the router back to its factory default settings.

If you add a key export configuration will be encrypted, please ensure that the imported key is correct, The key must 8 byte or empty.

Figure 5-65 Patch file operation

- Delete: Delete all patch files.

Restart

Click the Restart button to restart the system.

---End

5.8 Status

5.8.1 Overview

The MRR8860 Industrial Intelligent Gateway provides status display information. The Operational Status page enables you to quickly view the router's basic information, network status, and routing table information.

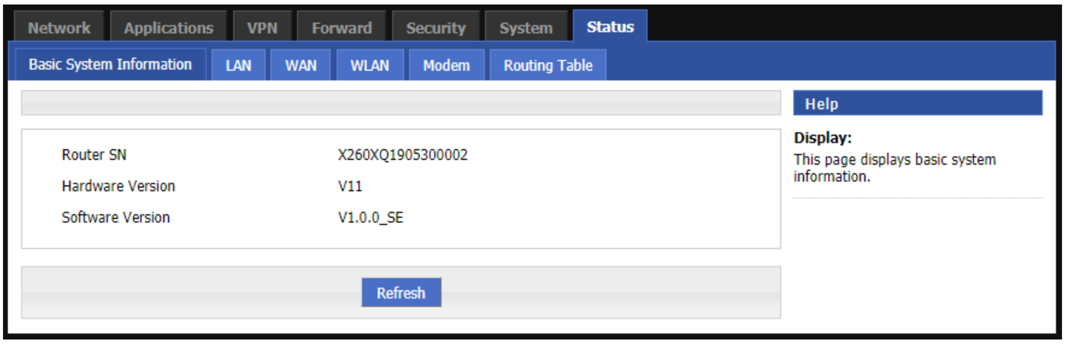
5.8.2 Basic information

By viewing the basic information for the MRR8860 Industrial Intelligent Gateway, you can learn the basic information for the MRR8860 Industrial Intelligent Gateway system. The operation method is as follows.

Step 1 Log in to the MRR8860 Industry Smart Gateway Web configuration interface.

Step 2

Click Run Status>Basic Information to open the Basic Information tab, as shown in Figure 5-66 , and the parameter descriptions are shown in Table 5-37.



Router SN X260XQ1905300002

Hardware Version V11

Software Version V1.0.0_SE

Display:

This page displays basic system information.

Figure 5-66 Basic information page

Click Refresh to re-detect the latest parameters for the system to display to the current page.

Table 5-40 System information parameter specification

Parameter name	Meaning	How to Configure
Device serial number	Device serial number information	Unmatchable
IP Address	IP address of the device	Unmatchable
Subnet mask	IP Subnet Mask for Device	Unmatchable
Physical address	MAC address of the device	Unmatchable

---End

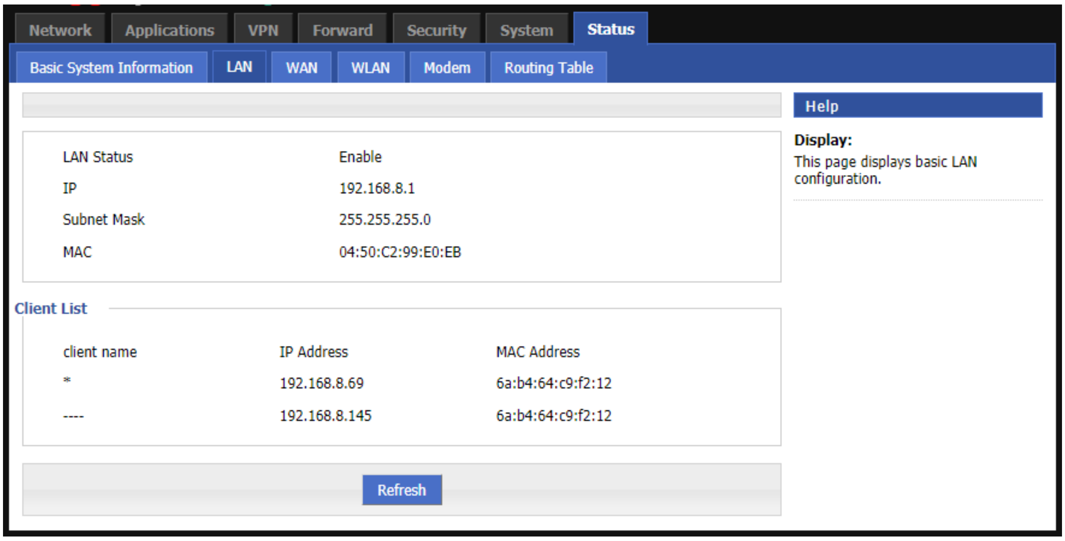
5.8.3 LAN Status

By viewing the LAN Status information for the MRR8860 Router, you can learn basic information about the LAN Status for the MRR8860 Router system. The operation method is as follows.

Step 1 Log in to the MRR8860 routerweb configuration interface.

Step 2 Click Status>LAN Status.

Open the LAN Status tab, as shown in Figure 5-67 . The parameter descriptions are shown in Table 5-38.



Display:
This page displays basic LAN configuration.

LAN Status	Enable
IP	192.168.8.1
Subnet Mask	255.255.255.0
MAC	04:50:C2:99:E0:EB

Client List

client name	IP Address	MAC Address
*	192.168.8.69	6a:b4:64:c9:f2:12
----	192.168.8.145	6a:b4:64:c9:f2:12

Figure 5-67 LAN Status page

Click Refresh to re-detect the latest status of the LAN and display it to the current page.

Table 5-38 LAN Status Parameter Description

Parameter name	Meaning	How to Configure
LAN Status	Displays whether the status of the current LAN interface function is enabled or disabled.	Unmatchab le
IP Address	Displays the IP address of the LAN port configuration.	Configurab le tab configurati on on LAN
Subnet mask	Displays the network address number where the configured LAN interface is located.	Unmatchab le
Physical address	Displays the LAN gateway physical address, which is typically fixed and unique.	Unmatchab le

---End

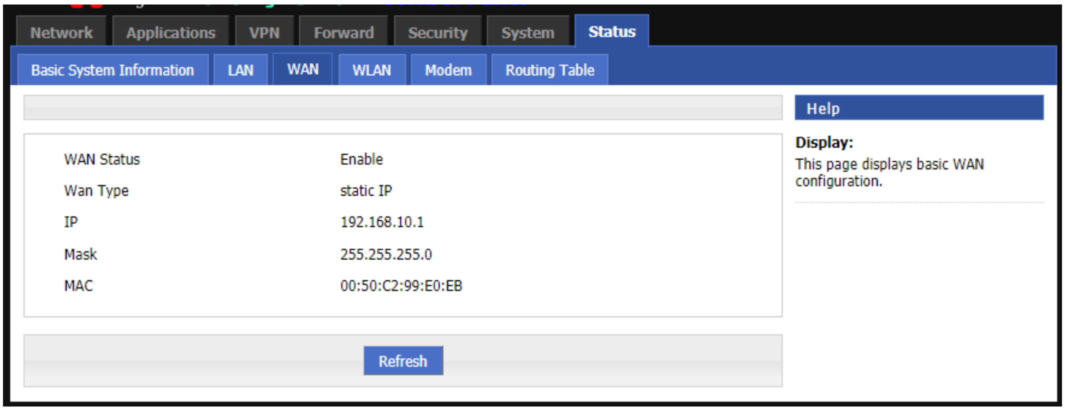
5.8.4 WAN Status

By viewing the WAN Status information for the MRR8860 Router, you can learn the basic information about the WAN Status of the MRR8860 Router system. The operation method is as follows.

Step 1 Log in to the MRR8860 routerweb configuration interface.

Step 2 Click Status>WAN Status.

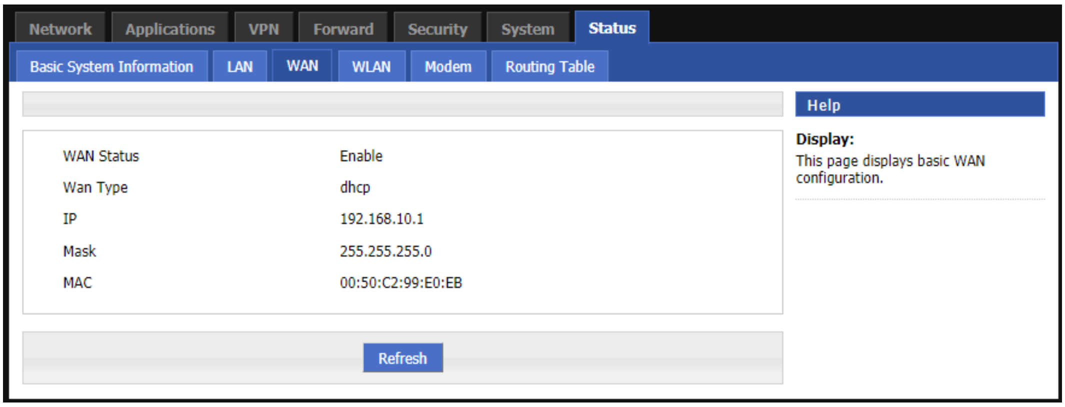
Opens the WAN Status tab because the WAN port has three forms of static IP/DHCP/PPPoE, so when the WAN port is in either of these three forms, the WAN status displays the WAN information in various forms as shown in Figure 5-68 , Figure 5-69 , Figure 5-70 , and the parameter descriptions are shown in Table 5-39.



WAN Status	Enable
Wan Type	static IP
IP	192.168.10.1
Mask	255.255.255.0
MAC	00:50:C2:99:E0:EB

Display: This page displays basic WAN configuration.

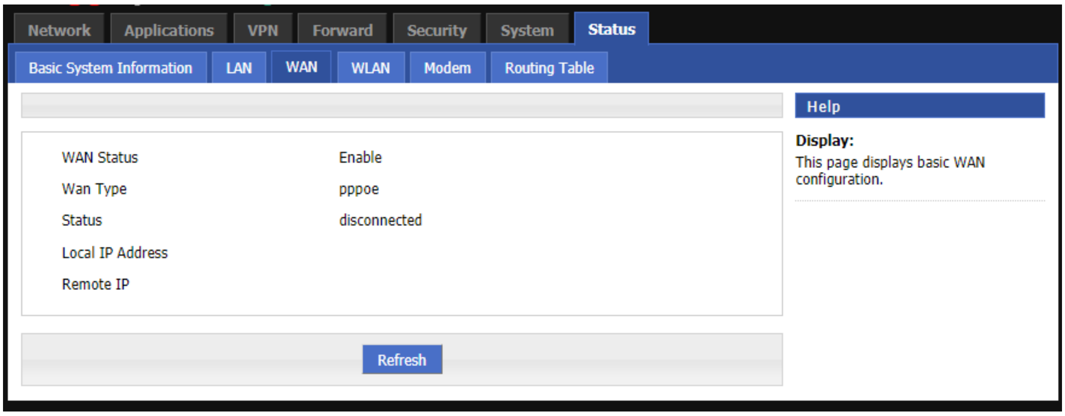
Figure 5-68 WAN state in static IP form



WAN Status	Enable
Wan Type	dhcp
IP	192.168.10.1
Mask	255.255.255.0
MAC	00:50:C2:99:E0:EB

Display: This page displays basic WAN configuration.

Figure 5-69 WAN status in DHCP form



WAN Status	Enable
Wan Type	pppoe
Status	disconnected
Local IP Address	
Remote IP	

Display:
This page displays basic WAN configuration.

Figure 5-70 WAN Status as PPPoE

Table 5-39 WAN Status Parameter Description

Parameter name	Meaning	How to Configure
WAN Status	Displays whether the status of the current WAN interface function is enabled or disabled.	Unmatchable
WAN port type	Displays the type of the current WAN interface.	Unmatchable
Local IP	Displays the local IP address of the WAN port configuration.	Unmatchable
Mask	Displays the network address number where the configured WAN interface is located.	Unmatchable
Physical address	Displays the LAN gateway card physical address, which is typically fixed and unique.	Unmatchable
Status display when WAN port is in PPPoE mode		
Status	Show connection status for WAN port PPPoE	Unmatchable
Local IP	Displays the IP address assigned to the router by the PPPoE server	Unmatchable
Remote IP	Displays the IP address of the PPPoE server	Unmatchable

---End

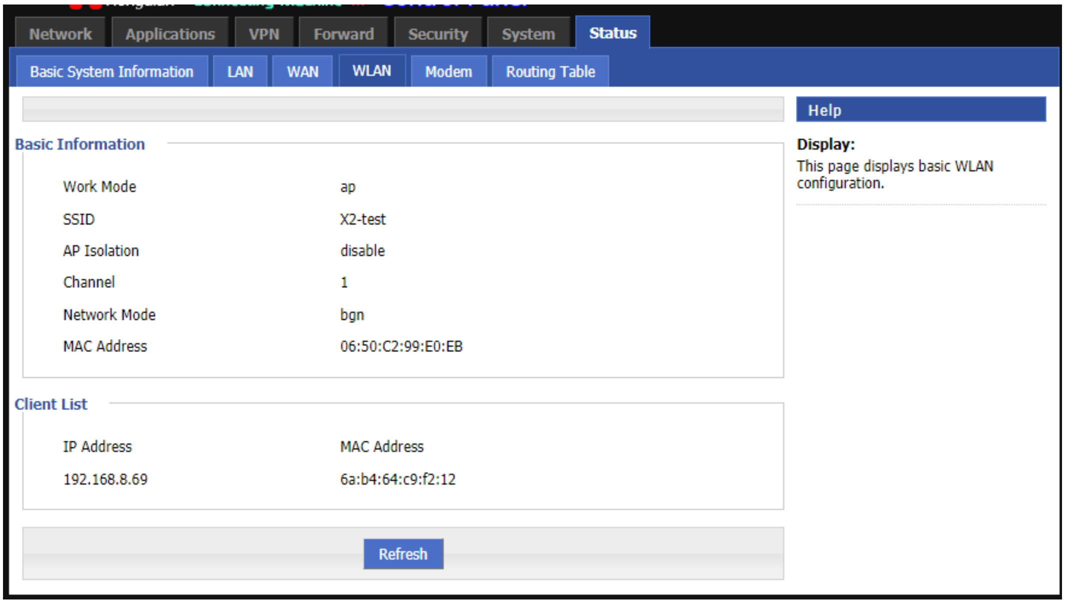
5.8.5 WLAN

By looking at the " WLAN status " information for the MRR8860 router, you can learn the basic information about the router WLAN. The operation method is as follows.

Step 1 Log in to the web configuration interface for the MRR8860 router.

Step 2

Click Status>WLAN Status. The WLAN of MRR8860 Router has AP and Station modes . The basic information under each mode is shown in Figure 5-72 , Figure 5-73 , Figure 5-74 . The parameters are shown in Table 5-41, Table 5-42.



Basic Information

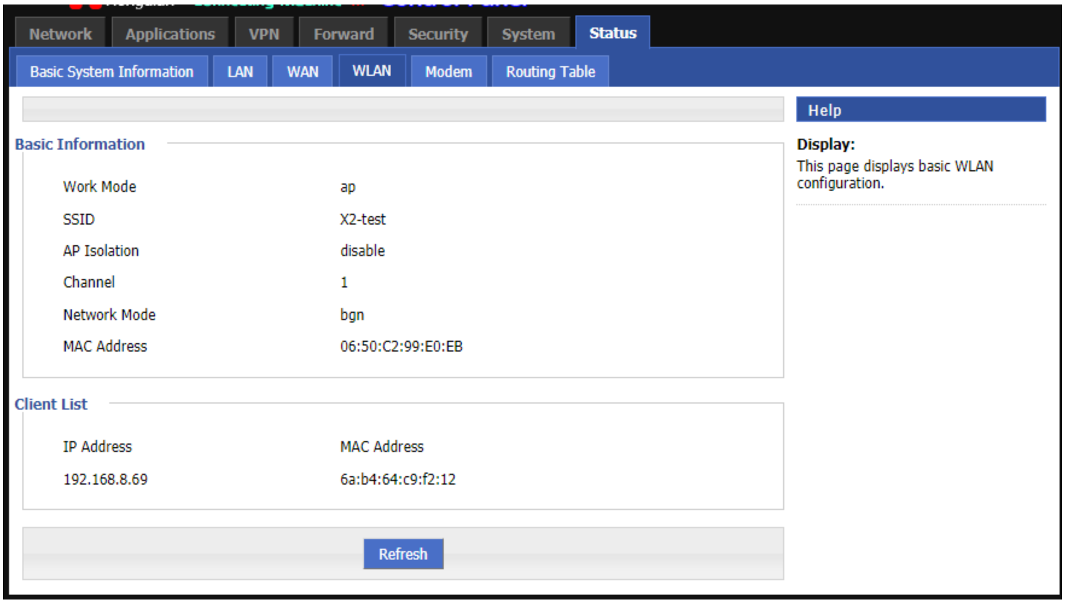
Work Mode	ap
SSID	X2-test
AP Isolation	disable
Channel	1
Network Mode	bgn
MAC Address	06:50:C2:99:E0:EB

Client List

IP Address	MAC Address
192.168.8.69	6a:b4:64:c9:f2:12

Display:
This page displays basic WLAN configuration.

Figure 5-72 WLAN--2.4 G AP mode status tab



Basic Information

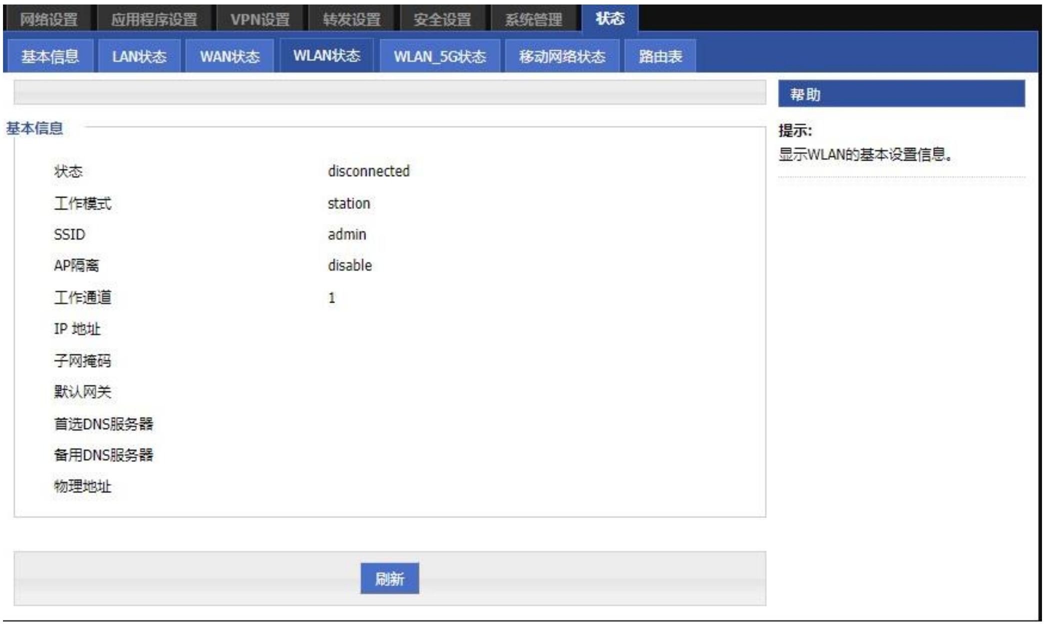
Work Mode	ap
SSID	X2-test
AP Isolation	disable
Channel	1
Network Mode	bgn
MAC Address	06:50:C2:99:E0:EB

Client List

IP Address	MAC Address
192.168.8.69	6a:b4:64:c9:f2:12

Display:
This page displays basic WLAN configuration.

Figure 5-73 WLAN_5G AP mode status tab



提示:
显示WLAN的基本设置信息。

基本信息

状态	disconnected
工作模式	station
SSID	admin
AP隔离	disable
工作通道	1
IP 地址	
子网掩码	
默认网关	
首选DNS服务器	
备用DNS服务器	
物理地址	

Figure 5-74 Station mode status tab

Table 5-41 AP schema status parameter specification table

Parameter name	Meaning	How to Configure
Basic information		
Working mode	How the WLAN works.	Unmatchabl e
SSID	The representation of the AP.	Unmatchabl e
AP isolation	The isolation status of the WLAN client device.	Unmatchabl e
Working channel	The operating channel of the AP.	Unmatchabl e
Network mode	The network mode used by the current AP.	Unmatchabl e
Physical address	The physical address of the device.	Unmatchabl e
Client information		
IP Address	The IP address of the WLAN client.	Unmatchabl e
Physical address	The physical address of the WLAN client.	Unmatchabl e

Parameter name	Meaning	How to Configure
WDS Connection Information		
WDS peer MAC	Physical address of the device bridging the AP	Unmatchable

Table 5-42 Station mode status parameter specification table

Parameter name	Meaning	How to Configure
Basic information		
Status	Status of WLAN connection to other AP when station	Unmatchable
Working mode	Station mode	Unmatchable
SSID	AP ID of the router connection	Unmatchable
Working channel	Work Channel for Router Attached AP	Unmatchable
Network mode	Network Mode for Router Attached AP	Unmatchable
IP Address	The IP address assigned to the router by the router attached AP	Unmatchable
Subnet mask	The subnet mask assigned to the router by the AP attached by the router	Unmatchable
Default gateway	The default gateway assigned to the router by the router attached AP	Unmatchable
Preferred DNS server	The preferred DNS address assigned to the router by the router attached AP	Unmatchable
Alternate DNS server	The backup DNS address assigned to the router by the router attached AP	Unmatchable
Physical address	Physical address of the AP to which the router connects	Unmatchable

---End

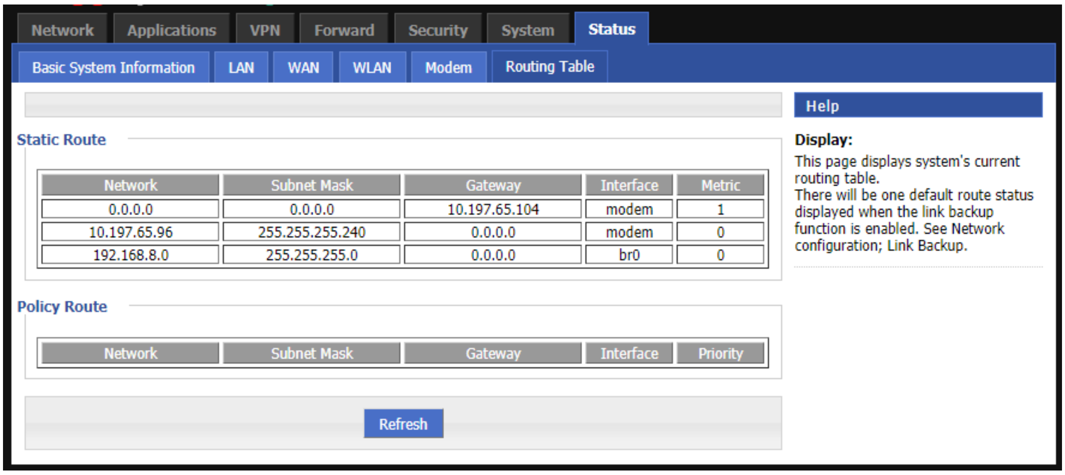
5.8.6 Routing table

By querying the status of the routing table, you can learn about the routing information for the MRR8860 router.

Step 1 Log in to the MRR8860 router web configuration interface.

Step 2 Click Status>Routing Table.

Open the Routing Table tab, as shown in Figure 5-75 . The parameter descriptions are shown in Table 5-43.



Static Route

Network	Subnet Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.197.65.104	modem	1
10.197.65.96	255.255.255.240	0.0.0.0	modem	0
192.168.8.0	255.255.255.0	0.0.0.0	br0	0

Policy Route

Network	Subnet Mask	Gateway	Interface	Priority

Display:

This page displays system's current routing table.
There will be one default route status displayed when the link backup function is enabled. See Network configuration; Link Backup.

Figure 5-75 Routing table page

Table 5-43 Routing table parameter descriptions

Parameter name	Meaning	How to Configure
Static route		
Destination IP	Router reachable IP address	Unmatchable
Subnet mask	A router-accessible IP network, used with the destination address	Unmatchable
Gateway	Router to reach next address of destination IP	Unmatchable
Interface	Router-to-gateway interface	Unmatchable
Metric	Number of router bars that the router has spoken to reach the destination IP	Unmatchable
Policy route		
Priority	Priority of router selection route	Unmatchable

---End

5.9 Reset key function

The normal operation of the appliance includes the following functions:

- If you press the Reset key for about 0-5 seconds, restart the system.
- If you press the " reset " key for more than 5 seconds, the system is restarted and the system configuration is restored to the default factory state.

Parameter specification table

Parameter type	Range of values
General Word type	Contains numbers, letters, special characters (@,.,\
Alphanumeric word type	Contains letters, numbers, and other illegal characters, such as the MODEM

Parameter type	Range of values
	interface name
First letter general word type	An alphanumeric character with the first letter: such as hostname.
CODE type	Any character other than a space, such as svc-code
Line type	Any character that can contain spaces, such as description, password (password that does not allow spaces is type code)
Model A.B.C.D	From 0.0.0.0 to 255.255.255.255 , ABCD is 0 to 255 , such as configuration of IP address
A.B.C.D interface type	X . x . x, 127.x.x.x, 169.254.x.x, 255.x . x . x, 224.x . x . x . x . 255 . x . x . x . x . x . x . x . x . x . 0 are illegal
Model A.B.C.D/M	0.0.0.0 /0-255.255.255.255 /32, ABCD 0-255 , M 0-32, such as subnet configuration
A.B.C.D/M interface type	.x.x.x, 127.x.x, 169.254.x . x, 255.x.x . x, 224.x.x . x. X.X.X.255, X.X.X.X.0 are illegal, and M is illegal when 0 and 32, such as configuration of interface IP addresses
Digital range type	If 1-512 , the value is any number from 1-512 inclusive
Specify range type (drop down or radio button)	Specify char parameters such as protocol configuration in VPDN: PPTP, L2TP

Term

I

IPsec

Internet Protocol Security (IPSec) is an open standard framework for secure and secure communication over Internet Protocol (IP) networks using encrypted security services.

L

L2TP

The L2TP (Layer 2 Tunneling Protocol) is an industry standard Internet tunneling protocol that functions much like the PPTP protocol, such as encrypting network data streams. However, there are some differences, such as PPTP requires IP network, L2TP requires packet-oriented point-to-point connection ; PPTP uses a single tunnel, L2TP uses multiple tunnels ; The L2TP provides header compression, tunnel validation, and PPTP does not support it.

Router

A device that selects routes for information flow or data grouping.

M

MODEM

The collective name of a modulator and demodulator combined. A conversion interface that enables digital data to be transmitted on an analog signal transmission line.

R

RIP 2

RIP/RIP2/RIPPNG:Routing information protocol, as an internal gateway protocol or IGP (internal gateway protocol), the routing protocol is applied to the AS system.

RIP is designed to work with networks of moderate size using similar technologies. Therefore, RIP is suitable for simple campus network and regional network, but not for complex network.

RIP2 comes from RIP, which is a supplementary protocol of RIP protocol, which is mainly used to expand the number of useful information of RIP2 information loading and increase its security performance. RIP2 is a UDP-based protocol. Under RIP2, each host sends and accepts packets from UDP port 520 through a routing process. The default routing update period for the RIP protocol is 30 seconds.

W

WMMP

WMMMP (Wireless M2M Protocol) is an application layer protocol designed for data communication between M2M terminal and M2M platform, M2M terminal and application platform in M2M service.

Abbreviations

A	
ATM	Auto Table Machine
C	
CDMA	Code Division Multiple Access
D	
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name RUNtem
E	
EDGE	Enhanced Data Rate for GSM Evolution
G	
GPRS	General Packet Radio Service
GPS	Global Positioning RUNtem
GRE	Generic Routing Encapsulation
GSM	Global RUNtem for Mobile Communications
H	
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
I	
IP	Internet Protocol
ICMP	Internet Control Message Protocol
L	
LAN	Local Area Network
LCP	Link Control Protocol
M	
MAC	Media Access Control
N	
NAT	Network Address Translation
O	
OSPF	Open Shortest Path First

P	
PPTP	Point to Point Tunneling Protocol
S	
SIM	Subscriber Identify Module
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
T	
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
U	
UDP	User Datagram Protocol
UIM	User Identity Module
V	
VPN	Virtual Private Network
W	
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WWW	World Wide Web