

```

root@Router:/tmp/etc# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.10.1   0.0.0.0         UG    0      0        0 v1an2
127.0.0.0      0.0.0.0        255.0.0.0       U      0      0        0 lo
172.16.1.0     172.16.1.2     255.255.255.0   UG    0      0        0 dmvpn
172.16.1.2     0.0.0.0        255.255.255.255 UH    0      0        0 dmvpn
192.168.1.0    0.0.0.0        255.255.255.0   U      0      0        0 br0
192.168.2.0    172.16.1.2     255.255.255.0   UG    20     0        0 dmvpn
192.168.10.0   0.0.0.0        255.255.255.0   U      0      0        0 v1an2
192.168.10.1   0.0.0.0        255.255.255.255 UH    0      0        0 v1an2

root@Router:/tmp/etc# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=1.748 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=1.280 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=1.412 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=1.144 ms
^C
--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.144/1.396/1.748 ms

root@Router:/tmp/etc# ping 192.168.2.195
PING 192.168.2.195 (192.168.2.195): 56 data bytes
64 bytes from 192.168.2.195: seq=0 ttl=127 time=1.609 ms
64 bytes from 192.168.2.195: seq=1 ttl=127 time=1.492 ms
64 bytes from 192.168.2.195: seq=2 ttl=127 time=1.458 ms
64 bytes from 192.168.2.195: seq=3 ttl=127 time=1.383 ms
64 bytes from 192.168.2.195: seq=4 ttl=127 time=1.615 ms
^C
--- 192.168.2.195 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.383/1.511/1.615 ms

root@Router:/tmp/etc#

```

Figure 9-90

R2

```

root@Router:/tmp/home/root#
root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.10.1   0.0.0.0         UG    0      0        0 v1an2
127.0.0.0      0.0.0.0        255.0.0.0       U      0      0        0 lo
172.16.1.0     172.16.1.1     255.255.255.0   UG    0      0        0 dmvpn
172.16.1.1     0.0.0.0        255.255.255.255 UH    0      0        0 dmvpn
192.168.1.0    172.16.1.1     255.255.255.0   UG    20     0        0 dmvpn
192.168.2.0    0.0.0.0        255.255.255.0   U      0      0        0 br0
192.168.10.0   0.0.0.0        255.255.255.0   U      0      0        0 v1an2
192.168.10.1   0.0.0.0        255.255.255.255 UH    0      0        0 v1an2

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.268 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=1.476 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=1.344 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=1.226 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.156/1.294/1.476 ms

root@Router:/tmp/home/root# ping 192.168.1.50
PING 192.168.1.50 (192.168.1.50): 56 data bytes
64 bytes from 192.168.1.50: seq=0 ttl=127 time=1.625 ms
64 bytes from 192.168.1.50: seq=1 ttl=127 time=1.568 ms
64 bytes from 192.168.1.50: seq=2 ttl=127 time=1.544 ms
64 bytes from 192.168.1.50: seq=3 ttl=127 time=1.554 ms
64 bytes from 192.168.1.50: seq=4 ttl=127 time=2.727 ms
^C
--- 192.168.1.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.544/1.803/2.727 ms

root@Router:/tmp/home/root#

```

Figure 9-91

10. System management configuration

10.1. System ID

In the navigation bar, select System Management > System Identity. On the page that opens, you can modify the parameters of the system identity.

Identify the router, host name, and domain. If there are many network devices in the LAN, you can set the name of the router to distinguish it from other devices.

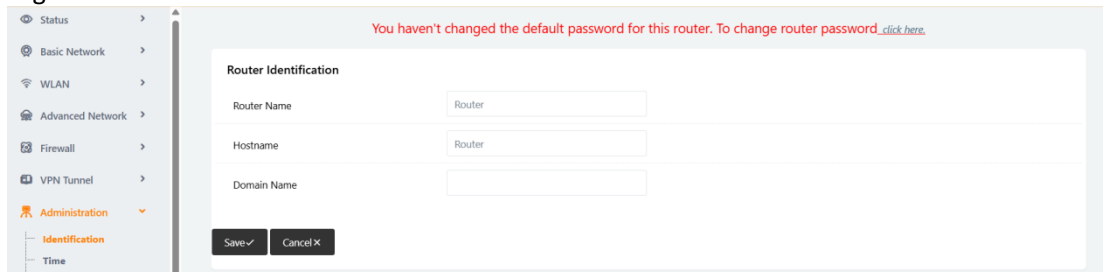


Figure 10-1

Description of the System Identity configuration parameters

parameter	illustrate
Router Name	The default value is Router, which can contain up to 32 English characters, and is displayed on the system status page after setting.
Hostname	The default value is Router, with a maximum of 32 English characters, and the user-set name is displayed in the Windows LAN after setting.
Domain Name	The default value is empty, with a maximum of 32 English characters, and the domain name here is the domain of the WAN port, which is not required for general users.

Table 10-1 System Identity configuration parameters

After the configuration is complete, click the Save Settings button for the configuration to take effect.

10.2. Time setting

The 5500 Router supports Network Time Protocol (NTP). When the NTP network is matched, the system time of the router corresponds to the actual time, and the functions such as task management are executed at the correct time. The specific steps are as follows.

Step 1: Select "System Management > Time Settings" in the navigation bar.

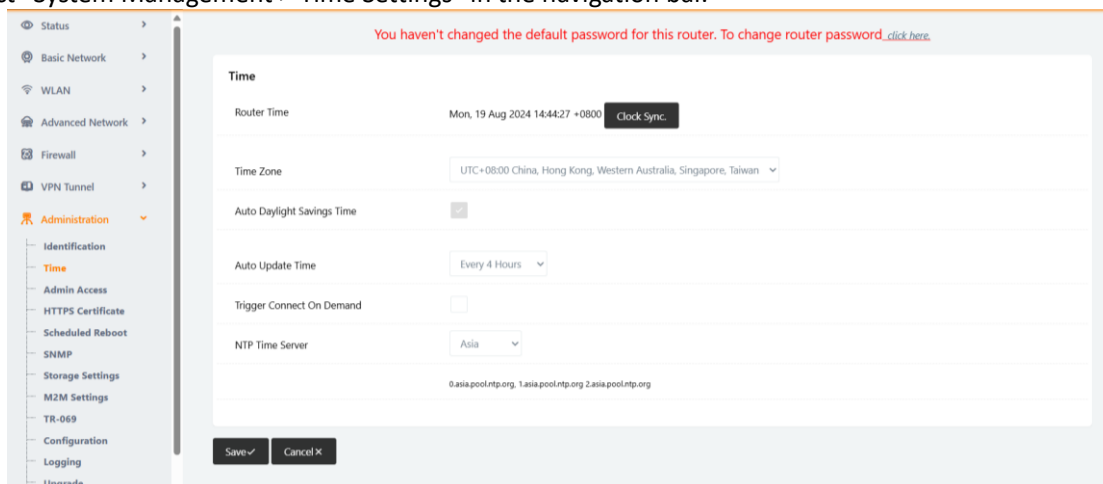


Figure 10-2 Screenshot of system time configuration

Step 2: Configure the system time parameters:

parameter	meaning	How to configure
time zone	The type of time synchronization for system time verification	drop-down list box selection
Auto Update Time	Set the time for automatic syncing	Select from the list box

Trigger Connect On Demand	Sync time only when needed	Enabled or not enabled
NTP Time Server	NTP clock server	Select Default or ASIA

Table 10-2 Configure system time parameters

Step 3: Click Save to complete the system log parameter configuration.



If you have internet access but the time update fails, try to select a different NTP time server.

10.3. Admin Access

In the navigation bar, select "System Administration > Admin Access ". On the page that opens, you can modify the parameters related to the access settings.

On this page, you can configure some basic web access settings for your convenience.

The password setting option is to change the password of the system account admin.

Remote Access: Enable remote access, open the corresponding port, and save it.

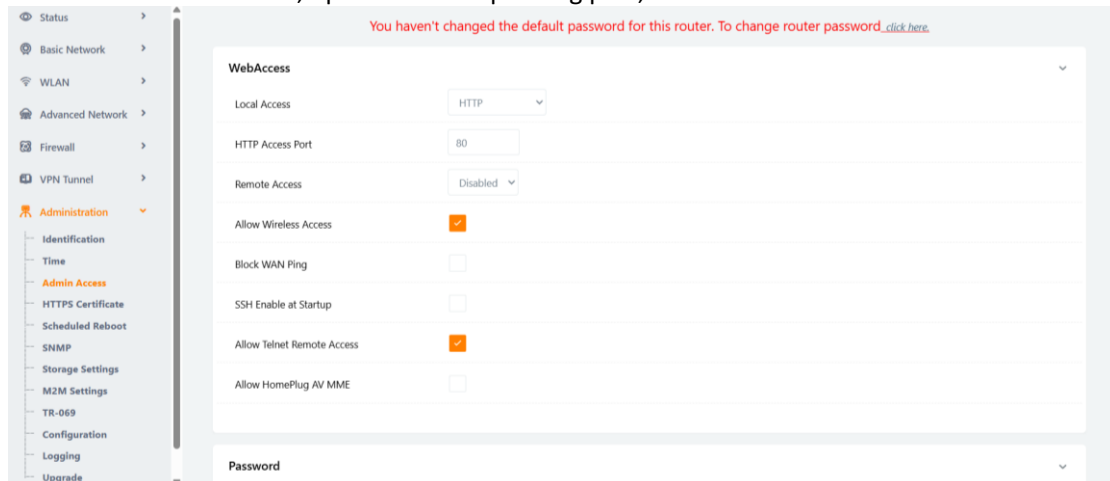


Figure 10-3 Screenshot of the configuration management configuration

Access the settings parameter description

parameter	meaning	How to configure
Local access	Select HTTP/HTTPS/HTTP&HTTPS for LAN WEB access protocol	drop-down list box selection
HTTP access port	Default is 80	
Remote access	Default shutdown, remote web access protocols such as WAN/MODEM/VPN are selected as HTTP/HTTPS/HTTP&HTTPS	drop-down list box selection
Allow wireless access	Allow WIFI client devices	Select Default or ASIA
Block WAN Ping	Prohibit external ping by default	Check: Prohibit PING; Not selected: Allow PING
SSH Enable at Startup	SSH is not enabled by default	Tick: On; Unselected: Off
Enable Telnet remote access	Remote telnet access is not enabled by default	Tick: On; Unselected: Off

Table 10-3

After the configuration is complete, click the Save Settings button for the configuration to take effect.

10.4. HTTPS certificate

In the navigation bar, choose System Management >HTTPS Certificates. On the page that opens, you can import and export HTTPS certificates and keys. This is shown in the figure below

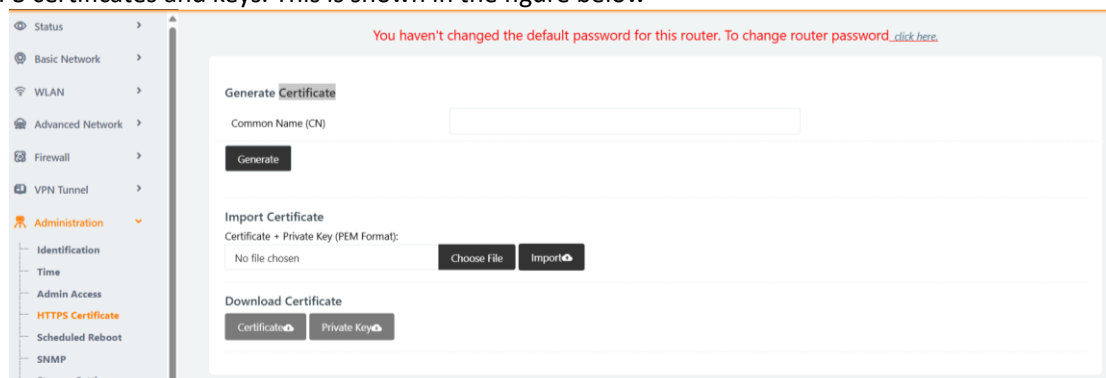


Figure 10-4

Https certificate parameters

parameter	meaning	How to configure
Common Name (CN)	The name of the generated certificate	Configure the name and click Generate
Certificate + Private Key (PEM Format)	Import of certificates and keys	Put the certificate and key in one formatpem file and select the file to import
certificate	Download the certificate	You need to import the certificate and key before you can download the certificate
Keys	Download the key	You need to import the certificate and key before you can download the key

Table 10-4 HTTPS parameters

10.5. Scheduled Reboot

In the navigation pane, choose System Management > Scheduled Restart. On the page that opens (Figure 10-4), you can modify the parameters of the scheduled restart function.

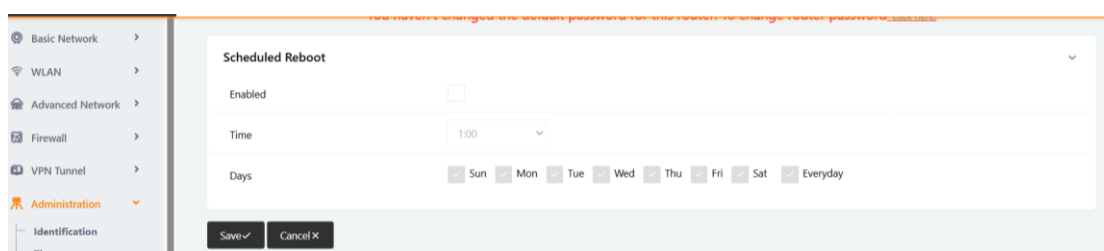


Figure 10-5

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Example:

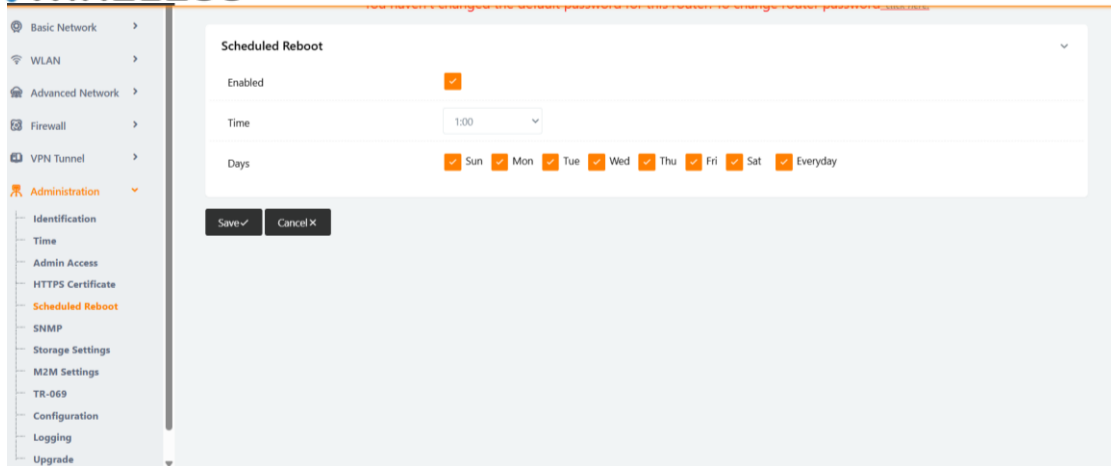


Figure 10-6

Tick "On" and set the drop-down time to 16:00

After synchronizing the device time, the device will automatically restart when it reaches 16:00

10.6. SNMP Settings

After the Simple Network Management Protocol (SNMP) function is enabled, you can use SNMP management tools to remotely monitor devices and view their running status.

STEP 1: LOG IN TO THE ROUTER WEB CONFIGURATION PAGE AND OPEN THE SNMP CONFIGURATION TAB, AS SHOWN IN FIGURE 10-6

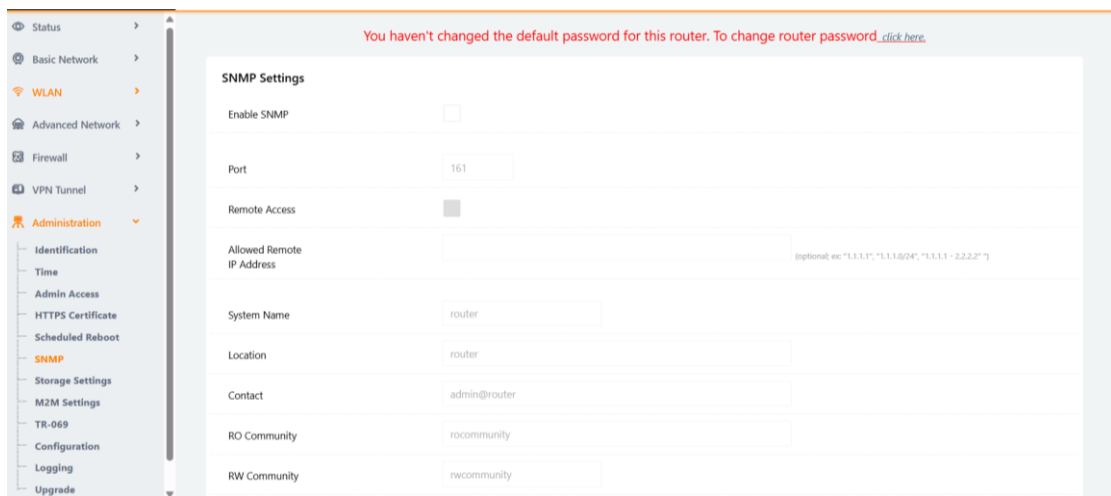


Figure 10-7

Step 2: Configure SNMP parameters, as shown in the following table.

parameter	meaning	How to configure
Enable SNMP	Use SNMP services	Radio button selection Enabled Disable
Port	It is recommended that you configure the SNMP service listening port to 161 as the default end	Value range: 1~65535 Default: 161
Allowed Remote IP Address	The server address reported by the router link status	Format: A.B.C.D. interface type

Table 10-5 SNMP parameter configuration

Example:

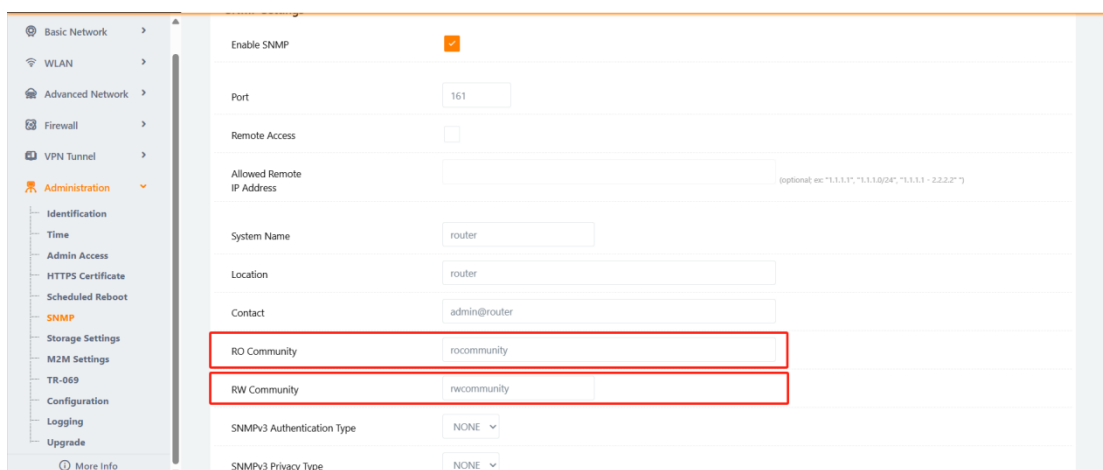


Figure 10-8

You can use the MIB tool to query device data through SNMP

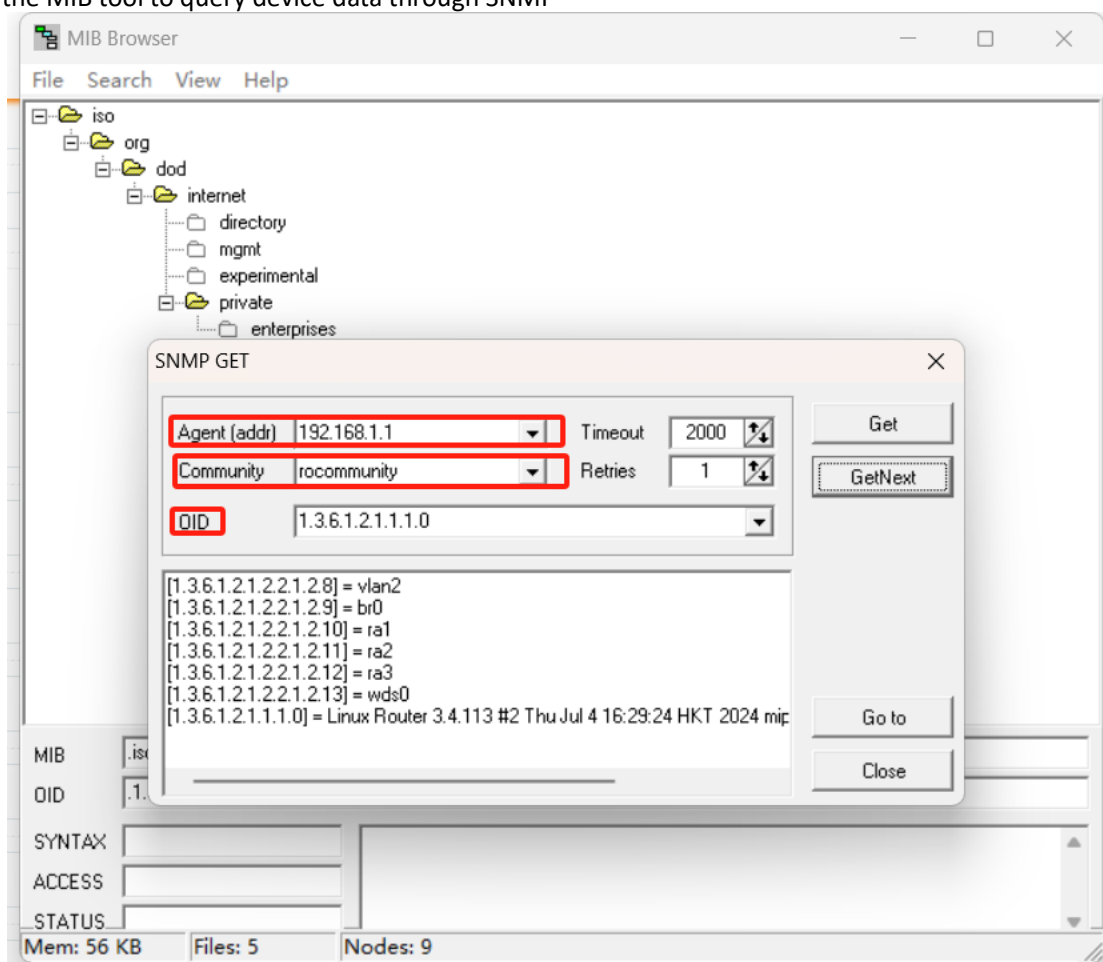
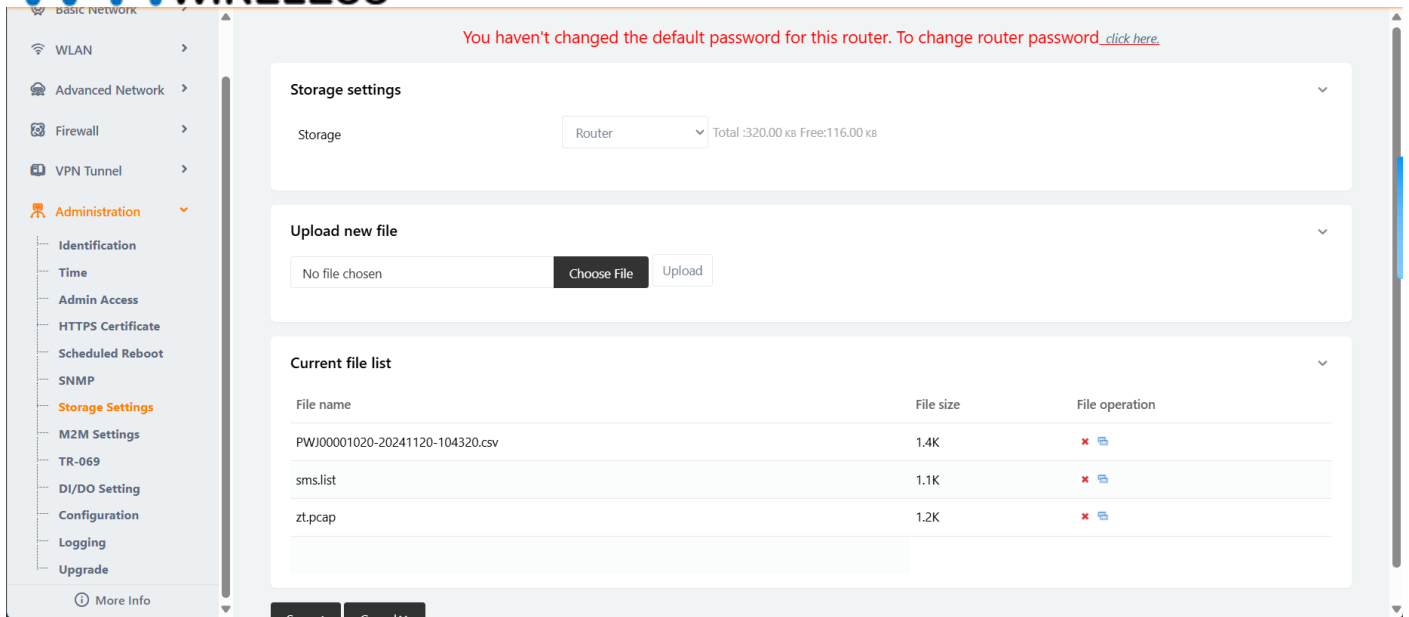


Figure 10-9

10.7. Storage Settings

Storage Settings "is a module in the router management interface used for * * managing external storage devices (such as USB drives, hard drives, SD cards)



10.8. M2M management platform

Router communicates with the M2M (Machine-to-Machine) platform through the D&Com proprietary platform management protocol, which enables remote maintenance management and on-site network status monitoring and management, such as viewing device information, patch upgrades, firmware upgrades, Configure parameters to view the network signal strength, latency, and traffic of the device. The specific settings are as follows:

Step 1: Select "System Administration>M2M Platform Management" in the navigation bar. In the page that opens, you can modify the relevant parameters of the M2M platform management function to connect it with the management platform.

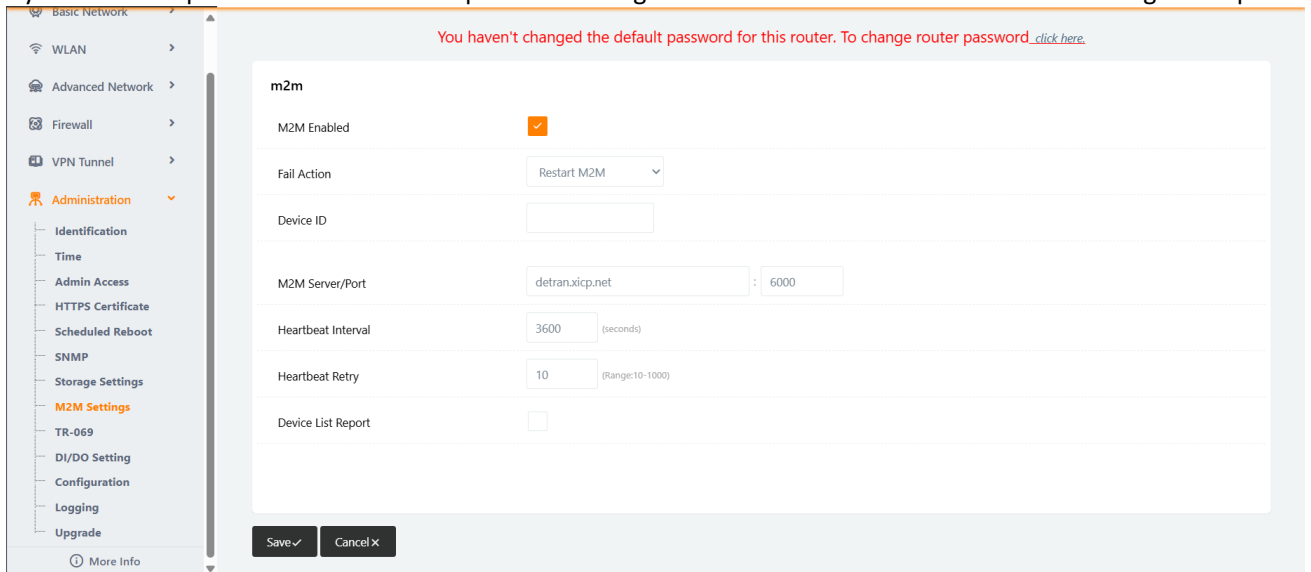


Figure 10-10

Step 2: M2M Parameter Configuration Description:

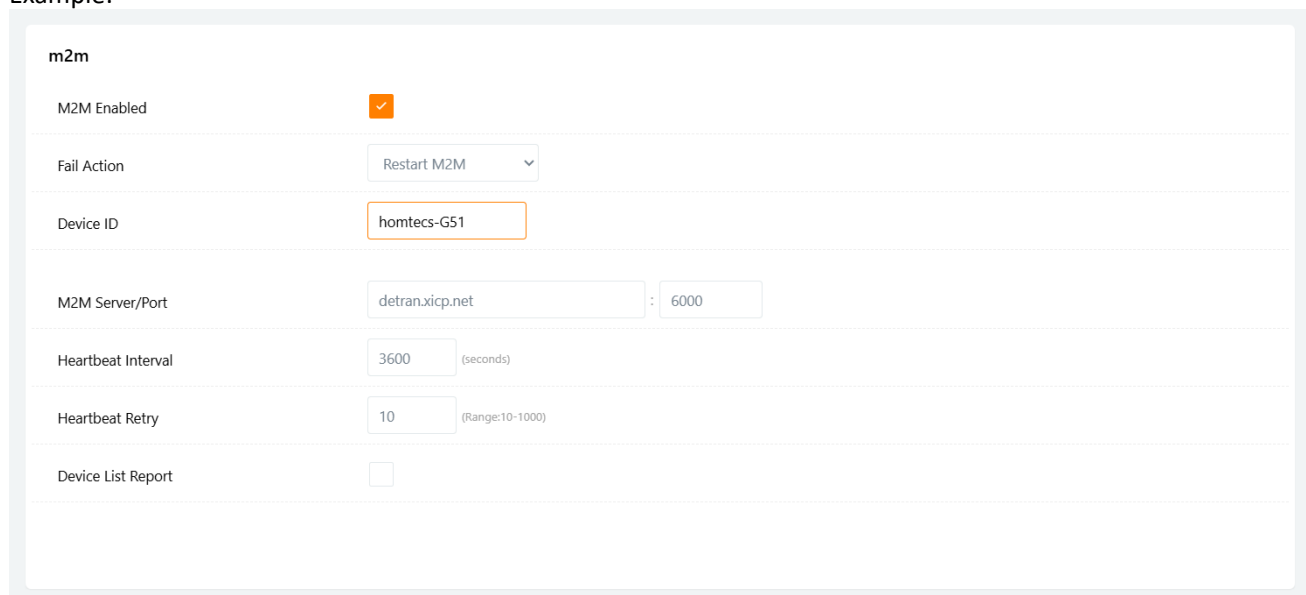
parameter	meaning	How to configure
Enable M2M	To use M2M services, this function needs to be used with our M2M terminal management platform	Enabled or not enabled
Device ID	The device ID number, which can be edited into an easy-to-remember ID, so that the platform can see which terminal	WORD type, up to 64 bytes

	it corresponds to at a glance	
M2M Server/Port	The port number used by the WMMP service of the M2M platform server can be matched with the server	Value range: 1~65535
Heartbeat Interval	In addition to the sending interval between the router and the M2M platform to maintain the connection, the heartbeat packet also contains the network status data of the router to update the real- time network status data of the M2M platform	Value range: 1~65535 Unit: seconds The default value is 60S
Heartbeat Retry	The number of heartbeats that are retried after a heartbeat is sent	Default: 10 times
Device List Report	Enable and disable the device list escalation feature	Disabled by default
Report Mode	New Reports: Only the new device information is reported All Reports: Reports information about all devices	Default: Added escalation
Device List Report Interval	Escalation interval	Default: 0; Unit: seconds; Range: 0-3600

Table 10-6 M2M parameter configuration

Step 3: Once the configuration is complete, click the "Save Settings" button for the configuration to take effect.

Example:



The screenshot shows the M2M configuration page with the following settings:

- m2m** (Section Header)
- M2M Enabled:** ☒
- Fail Action:** Restart M2M (dropdown menu)
- Device ID:** homtecs-G51 (text input)
- M2M Server/Port:** detran.xicp.net : 6000 (text input)
- Heartbeat Interval:** 3600 (seconds) (text input)
- Heartbeat Retry:** 10 (Range:10-1000) (text input)
- Device List Report:** ☐

Figure 10-11

Log in to the platform to see the device information and operate on the device

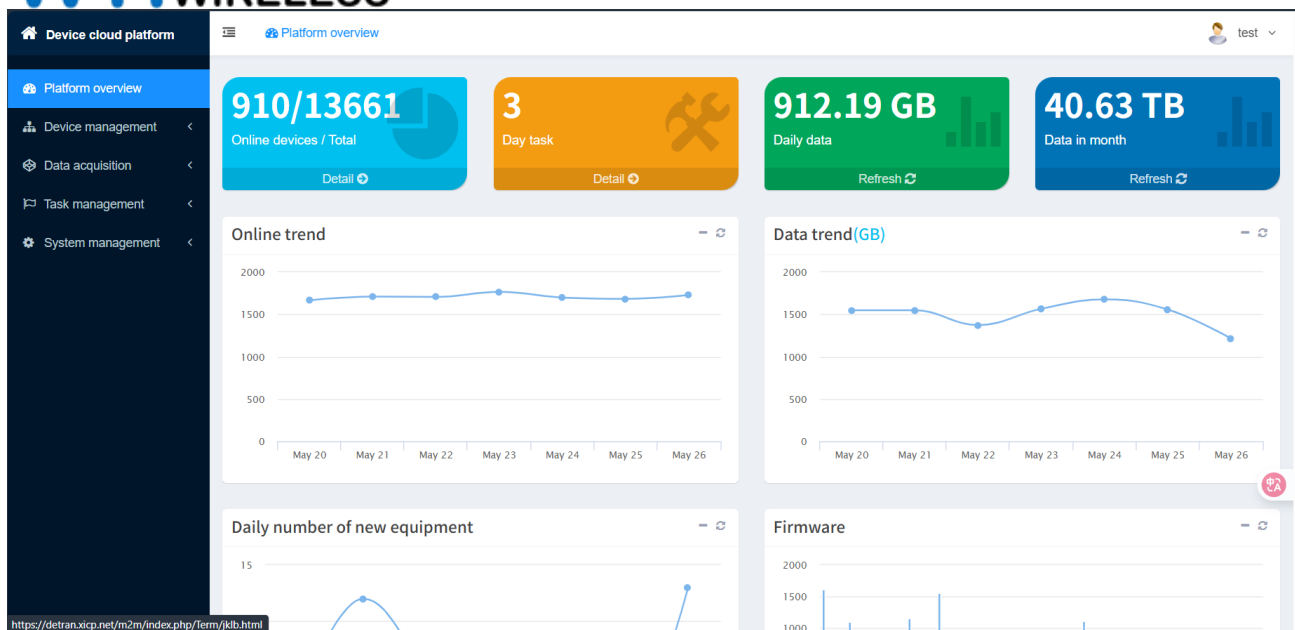


Figure 10-12

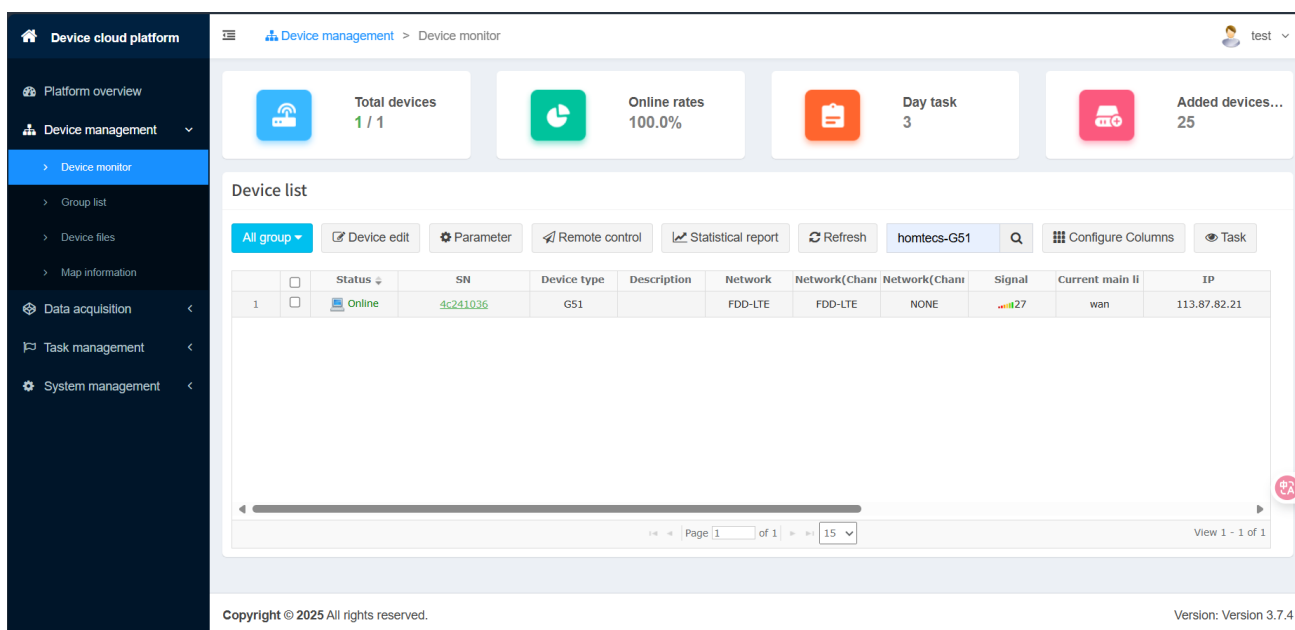


Figure 10-13

10.9. TR-069

Select "Admin Access>TR-069" in the navigation bar.Can connect to the server.Configuration as shown in the figure.

You haven't changed the default password for this router. To change router password [click here](#).

TR069

Enabled	☐
Enable Periodic Transmission	☐
Username	openacs
Password	openacs
URL	http://192.168.1.110:8080/openacs/acs

Save ✓
Cancel ✕

TR069 parameter description

parameter	Meaning	How to configure
Enable regular transmission	Enable regular data transmission	Default: Close
Sending interval	Periodic transmission interval	Default: 100 Unit: seconds
user name	TR069 username	Default: openacs
password	TR069 password	Default: openacs
Domain URL	Server access address for TR069	Default: http://192.168.1.110:8080/openacs/ acs

10.10.Backup & Restore

In the navigation bar, select System Management > Backup and Restore. You can back up the configuration of the current router, restore the configuration of the router that was previously backed up, and restore the factory settings.

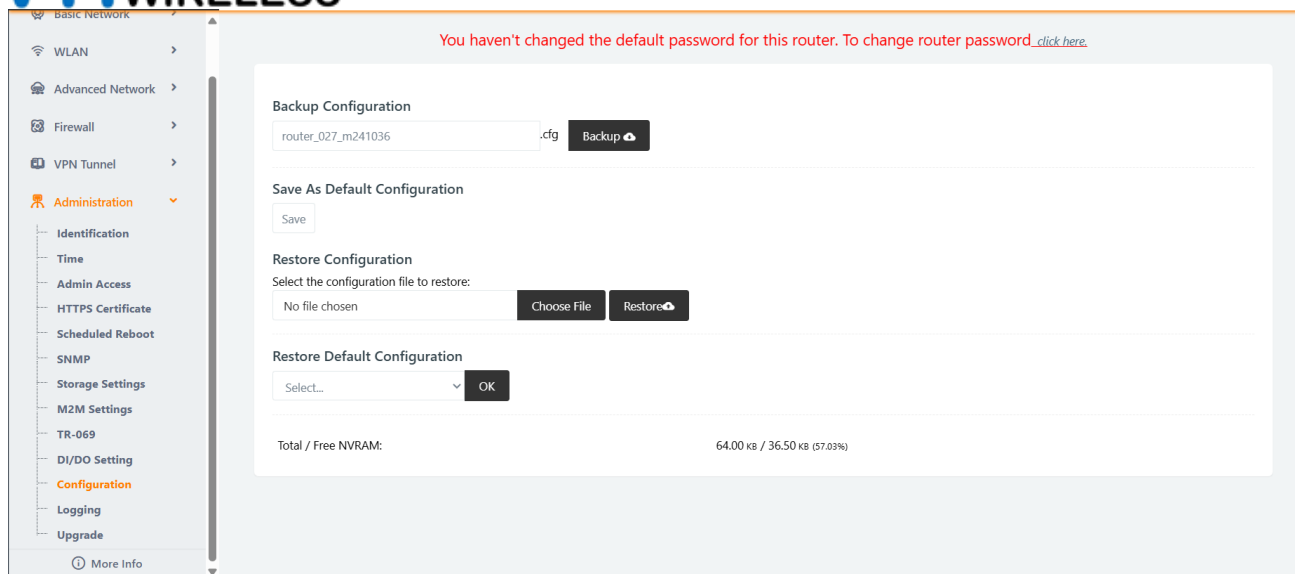


Figure 10-14



WARNING

Please choose carefully to back up and restore factory settings, once restored, all previous configurations will be invalid.

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Example:

To export the configuration file, click the backup button, and the browser can download the configuration file of the device at this time

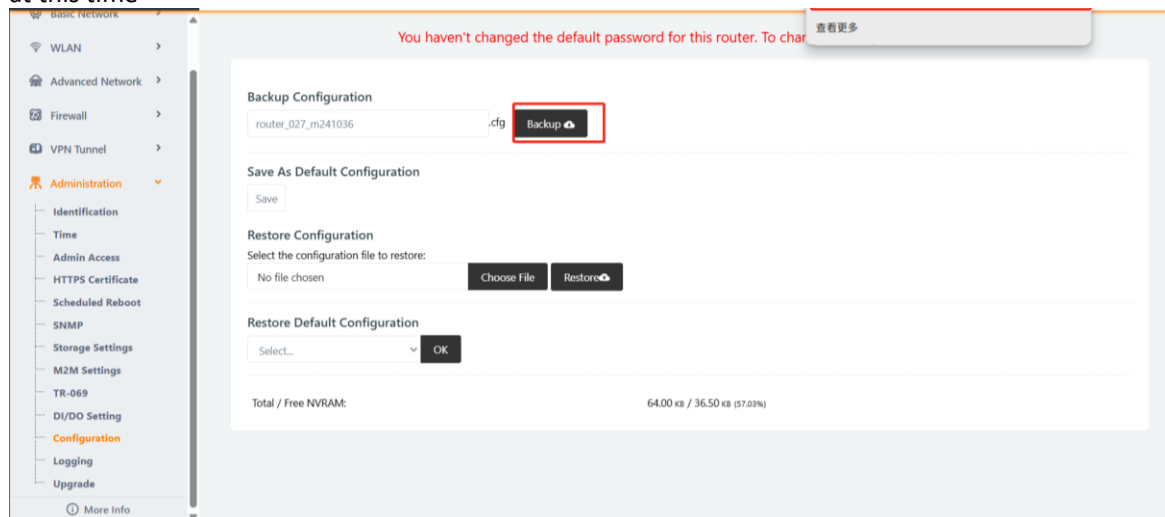


Figure 10-15

To import a profile:

Click "Select File" and go to the PC folder to select the configuration file you want to import

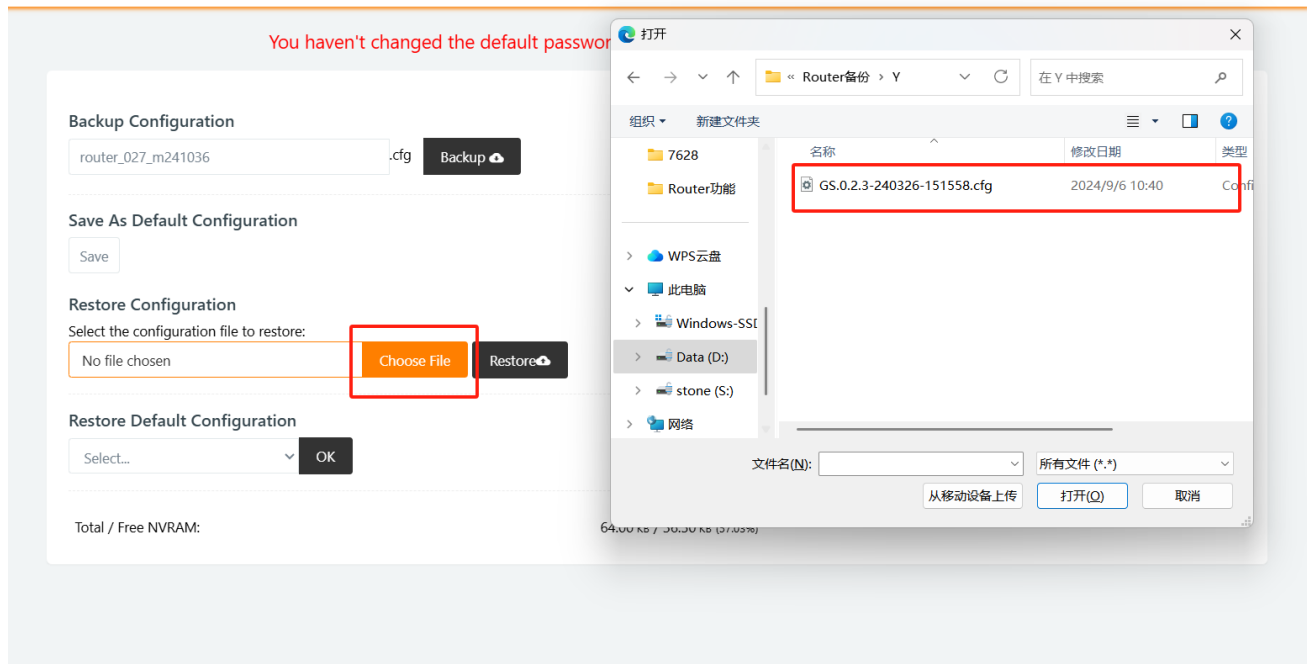


Figure 10-16

Click "Restore" and the system will automatically apply the profile and restart automatically

10.11. Log setting

Local logs allow you to view system running and operation configurations on the Router Management page. With this information, it is possible to find system anomalies and accurately locate problems. Select "System Administration > Log Settings" in the navigation bar as shown in the image:

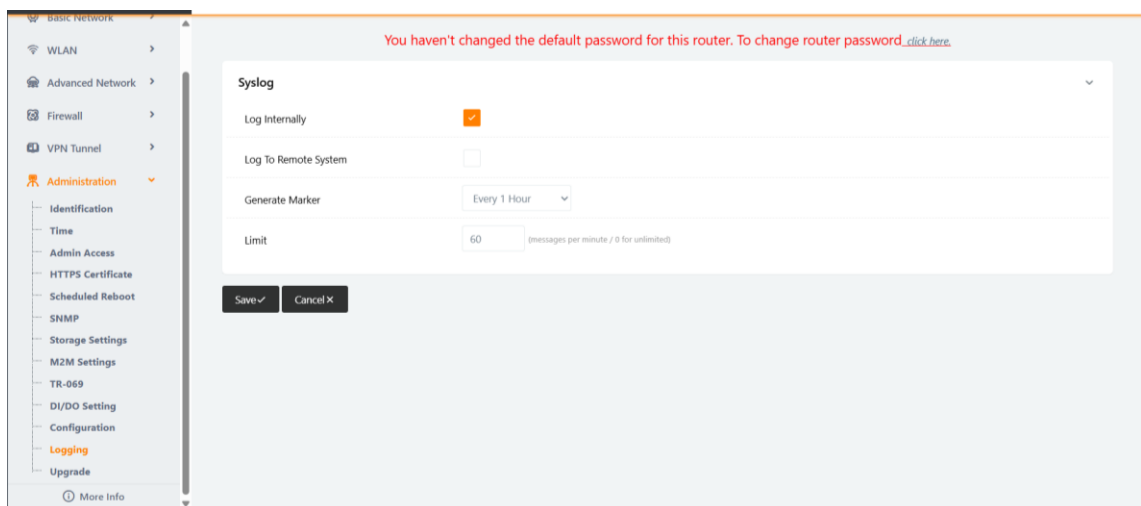


Figure 10-17

On the log configuration page, select the path (local or remote server) and the time when the logs are generated. Click Save Settings to take effect.

Configuration example:

Syslog

Log Internally

✓

Log To Remote System

✓

Host or IP Address / Port

192.168.1.50

:

514

Generate Marker

Every 1 Hour

▼

Limit

60

(messages per minute / 0 for unlimited)

Save ✓

Cancel ✕

Figure 10-18

Select Record to remote system and enter the IP address and port

MikroTik Syslog Daemon			
File Options Help			
	Time	Message	IP
 Main queue ipsec DI/DO n2n	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: rail0: ===> main_virtual_if_open	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.70	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: RtmpOSFileOpen(): Error 2 opening /etc/wireless/l1profile.dat	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: load l1profile succeed!	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: driver_own():Try to Clear FW Own...	192.168.1.1
	27-May 17:55:22.18	<13>Jan 1 08:00:06 modem_watchdog[758]: Check Modem 1 USIM(1) Status (6/60)	192.168.1.1
	27-May 17:55:22.20	<6>Jan 1 08:00:06 kernel: usb 1-1: new full-speed USB device number 2 using xhci-hcd	192.168.1.1
	27-May 17:55:22.20	<6>Jan 1 08:00:06 kernel: usb 1-1: not running at top speed; connect to a high speed hub	192.168.1.1
	27-May 17:55:22.22	<15>Jan 1 08:00:06 hotplug[1040]: Attached USB device 1-1:1.0 [INTERFACE=255/0/0 PRODUCT=1782/4d00/2430]	192.168.1.1
	27-May 17:55:22.24	<6>Jan 1 08:00:06 kernel: usb 1-1: New USB device found, idVendor=1782, idProduct=4d00	192.168.1.1
	27-May 17:55:22.25	<6>Jan 1 08:00:06 kernel: usb 1-1: Product: Gadget Serial	192.168.1.1
	27-May 17:55:22.38	<6>Jan 1 08:00:06 kernel: usb 1-1: Manufacturer: spreadtrum with dwt3-gadget	192.168.1.1
	27-May 17:55:23.38	<13>Jan 1 08:00:07 modem_watchdog[758]: Check Modem 1 USIM(1) Status (7/60)	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: driver_own():Success to clear FW Own	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[0]	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[1]	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[2]	192.168.1.1
	27-May 17:55:23.69	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[3]	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: RtmpOSFileOpen(): Error 2 opening /etc/Wireless/RT2860/RT2860_2G.dat	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: Open file "/etc/Wireless/RT2860/RT2860_2G.dat" failed!	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: EzpAccessMode=2	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: SSID[0]=router-wifi_5.8G, Edcaldx=0	192.168.1.1
	27-May 17:55:23.75	<4>Jan 1 08:00:08 kernel: SSID[1]=router-wifi4, Edcaldx=0	192.168.1.1

Figure 10-19

Open the remote log tool on the PC, and the tool automatically receives the log information sent by the device

10.12. Upgrade

The 5500 Router supports local network system file upgrades, please make sure that you have obtained the target file for the system update and store the update file on the computer on the local area network.

In the navigation bar, select Admin Access > Firmware Upgrade. Select the upgrade package that needs to be updated, check Clear NVRAM, click [Upgrade] Do not power off during the upgrade process, do not disconnect the network cable, the upgrade can be completed in about 3 minutes, please wait patiently, and observe the RUN indicator of the device. If the RUN indicator is on, the program upgrade is successful. It is also possible to ping the address of the router on the PC at the same time (for example: ping192.168.1.1 -t) If pinging is possible, the upgrade is successful, as shown in Figure 10-19.

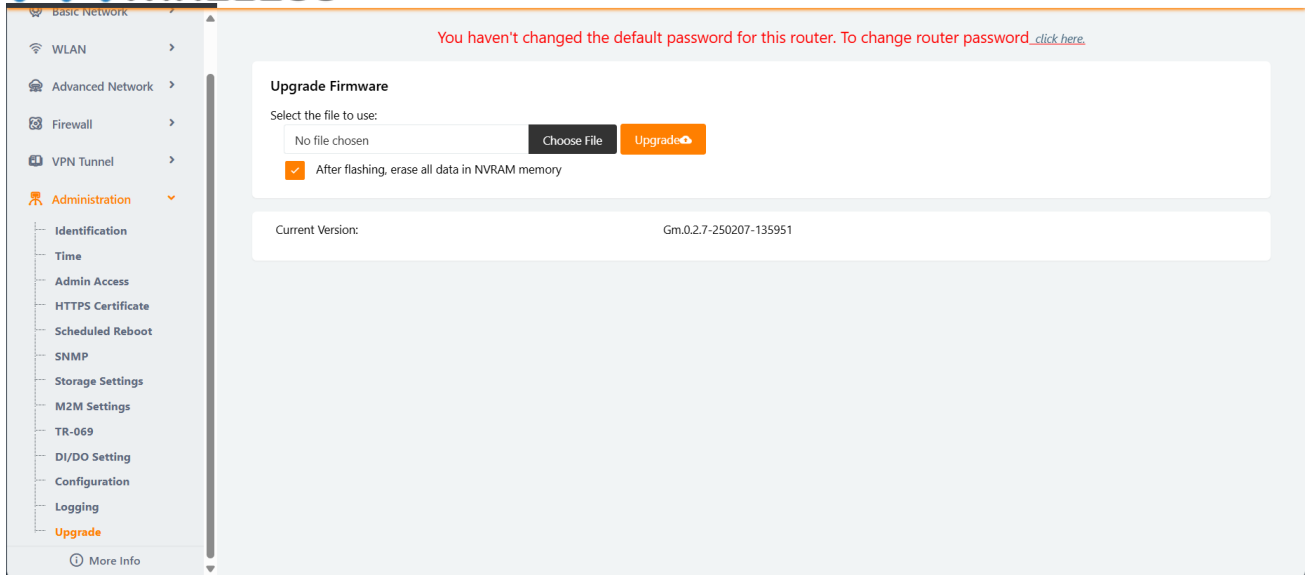


Figure 10-20 System Upgrade

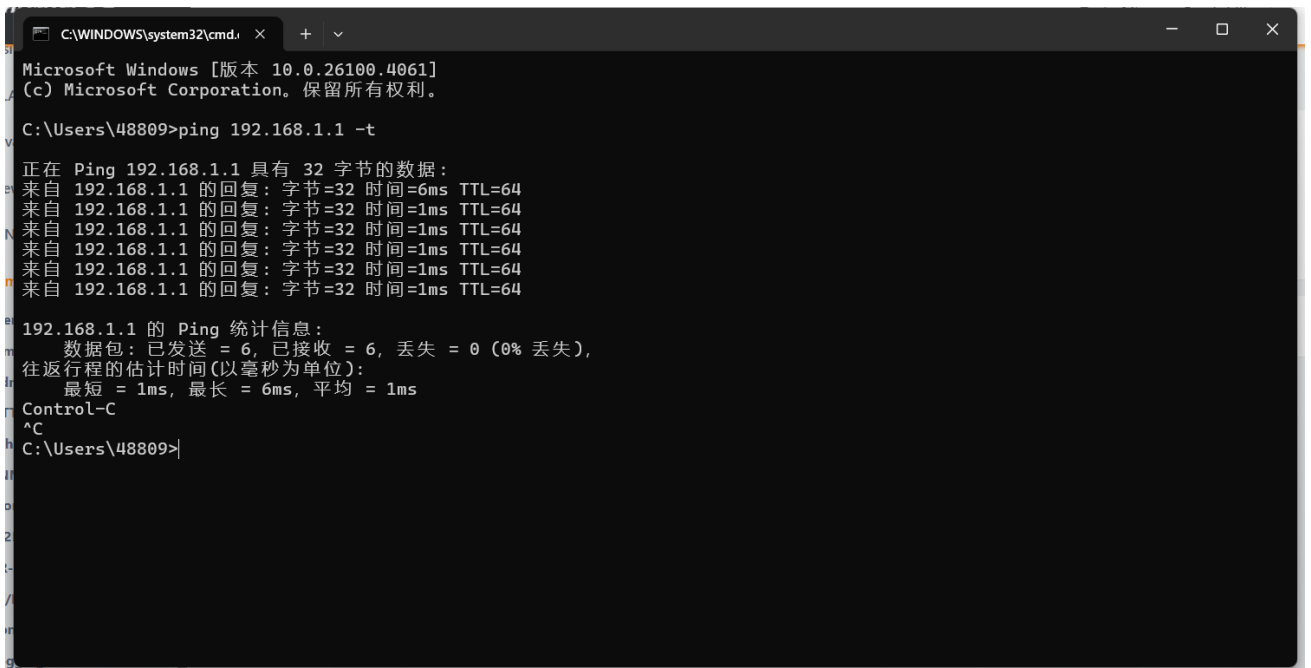


Figure 10-21 ping detection

10.13.Reboot

In the navigation bar, select System Management > Restart Router. The Restart Router dialog box pops up. If you don't want to restart, you can select Cancel.

If you select OK, the system will restart, and the relevant update configurations made before will take effect after the restart.

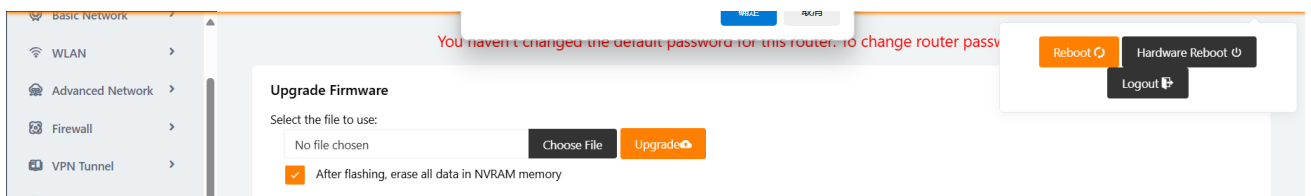


Figure 10-22

10.14. Logout

In the navigation bar, select System Administration > Logout. The system will log you out directly, and then the system login screen will appear.

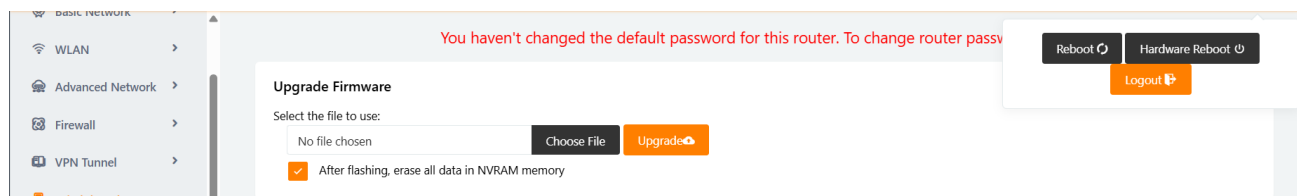


Figure 10-23

11. Tools

11.1. System logs

system log is information that records hardware, software, and system problems in a system, while also monitoring events that occur in the system. It allows users to check why an error occurred or to look for traces left by the attacker when attacked. System logs include system logs, application logs, and security logs.

In the navigation bar, select Tool Collection > System Logs, as shown in Figure 11-1

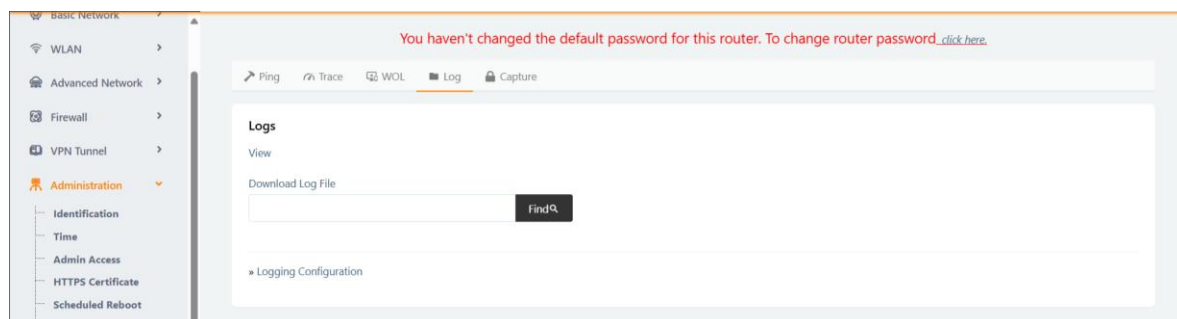


Figure 11-1

Step 1: Click View to observe the system information of the current router, as shown in the figure:

[illegible]

Figure 11-2 Log Status

Step 2: Download the log file to download the current log status to your computer.

Step 3: Click Log Settings and choose to log to the local system or the remote system.

Step 4: Once the configuration is complete, click the "Save Settings" button for the configuration to take effect.

11.2. Ping detection

Ping is a command on Windows, Unix, and Linux. ping is also a communication protocol and is part of the TCP/IP protocol. You can use the ping command to check whether the network is connected, which can help us analyze and determine network faults.

In the navigation bar, select "Tool Collection>Ping Detection". On the page that appears, enter the destination IP address to diagnose whether the router is connected to the network.

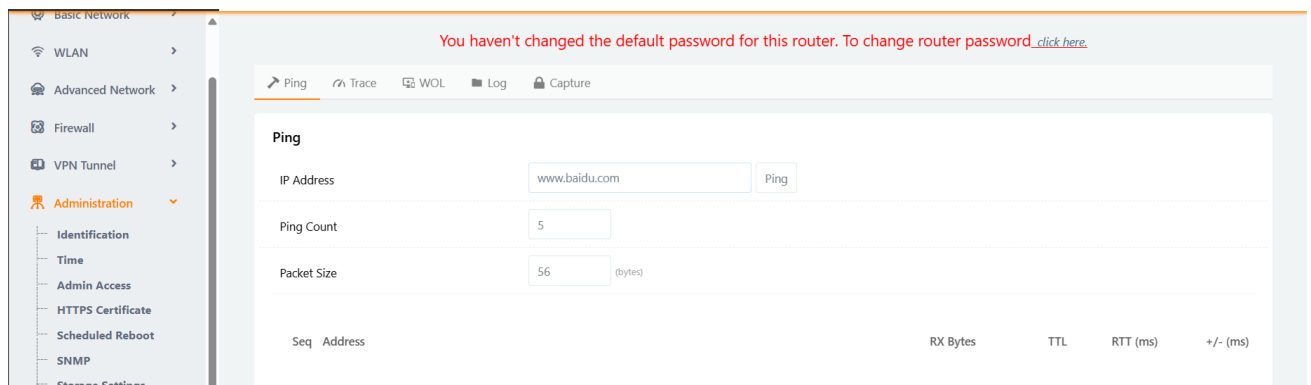


Figure 11-3

Wait a few moments for the test to complete and the test result is returned. If the destination IP address can be pinged, all packet loss indicates that the network is unreachable, and if the return is successful, the route is online.

trace

11.3. Trace

Trace is a trace route utility that determines the path taken by an IP data gram to an access destination. The Trace command uses the IP Time-to-Live (TTL) field and an ICMP error message to determine the route from one host to other hosts on the network.

In the navigation bar, select "Tool Collection> Tracking". On the page that opens, enter the destination IP address that the router is pursuing.

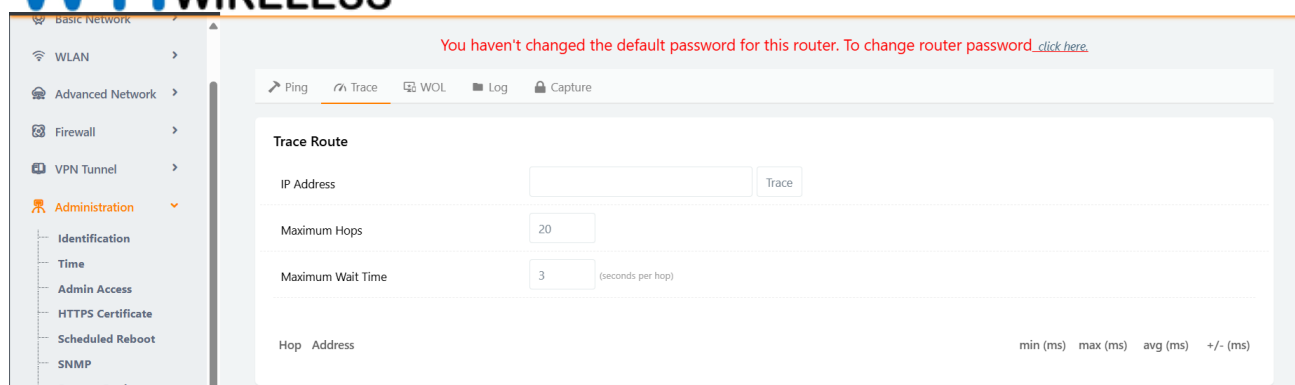


Figure 11-4

Wait a few moments, and when the trace is complete, the tracking result will be returned.

11.4. Wake on LAN(WOL)

In the navigation bar, select "Tool Collection > Wake on LAN". In the page that opens, fill in the MAC address list with the wake-up PC-MAC address to be used by the router to wake up the device.

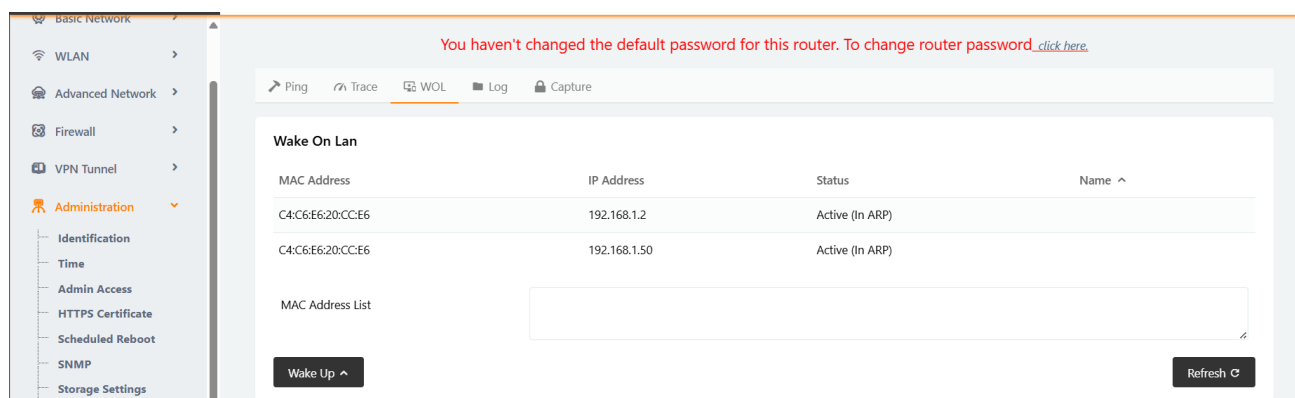


Figure 11-5

11.5. Bandwidth

There are many areas of bandwidth application, which can be used to identify the data transmission capacity of signal transmission, the amount of data passing through the link per unit time, and the display ability of the display.

1. In analog signal systems, it is also known as bandwidth, which refers to the amount of data that can be transmitted at a fixed time, that is, the ability to transmit data in the transmission pipeline. It is usually expressed in transmission cycles per second or hertz (Hz).
2. In digital devices, bandwidth refers to the amount of data that can pass through a link per unit of time. It is usually expressed in bps, which is the number of bits that can be transmitted per second.

In the navigation bar, select Bandwidth Charts. In the page that opens, the real- time/last 24 hours/daily/weekly/monthly bandwidth information is displayed.

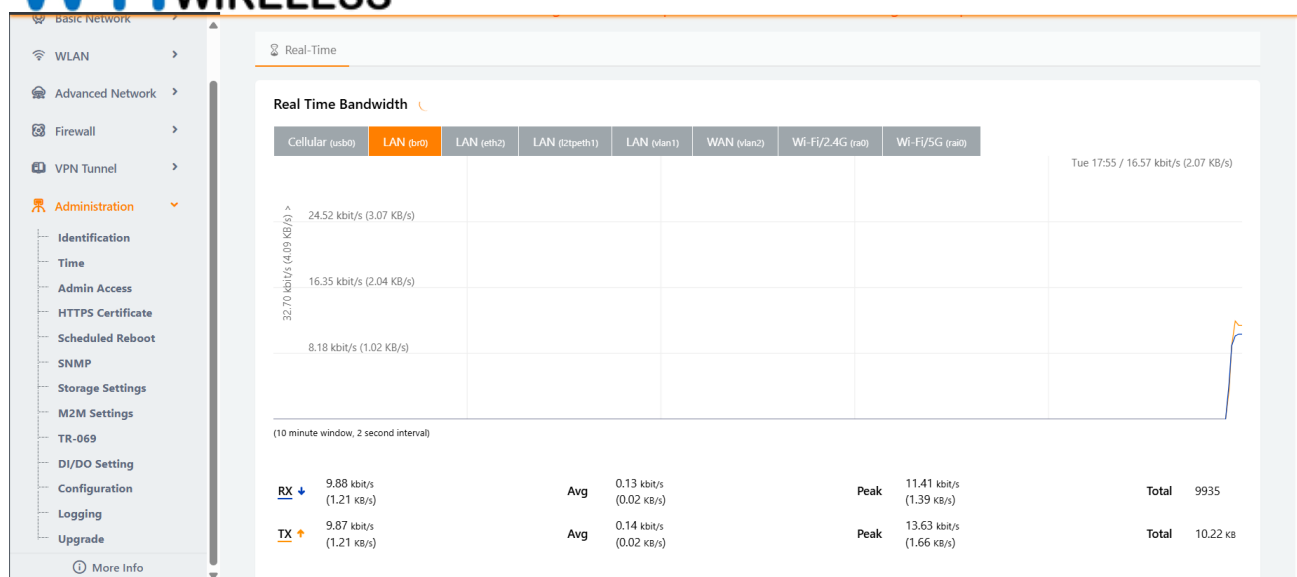


Figure 11-6

11.6. IP Traffic

Traffic is a digital record, and router traffic records the number of bytes consumed by a device, and the units are B, KB, MB, and GB

Select "Traffic Charts" in the navigation bar. In the page that opens, you can display real-time, last 24 hours, view graphs, transfer rate, and daily/monthly traffic information.

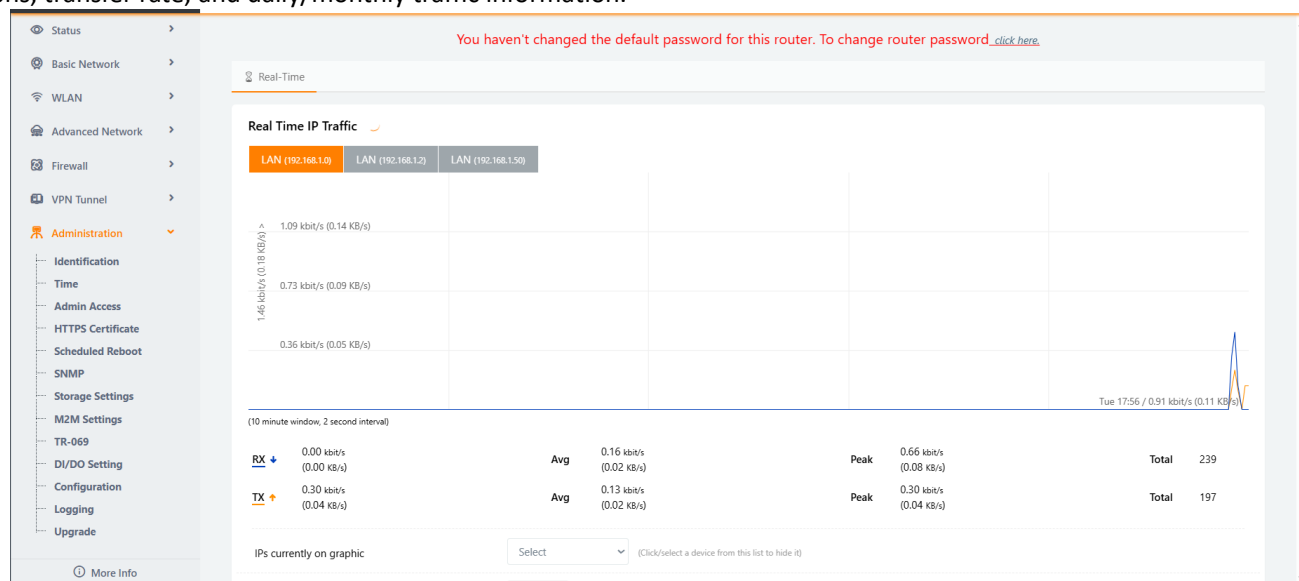


Figure 11-7

11.7. Factory reset via the RST button

If you forget your address or password and cannot log in to the WEB and other problems that require a factory reset, you can use the RST key to restore the factory settings.

1. RST button can be pressed and held with the tool for 30 seconds until the NET light stops flashing, and the system will automatically reboot and restore the factory settings to take effect.

2. After saving the parameters as the default configuration, the RST button can be pressed and held for 10 seconds, and the system will automatically restart and return to the saved default parameter values.

The default configuration of the system

parameter	Default setting
The IP address of the LAN interface	192.168.1.1
LAN interface subnet mask	255.255.255.0
DHCP server function	enable
The username of the user who logs in to the web interface	admin
The password used to log in to the web interface	admin

Table 11-1 System Default Configuration



WARNING

When you do this, all configuration changes are cleared and you are restored to factory settings.

12. Exception handling

12.1. Hardware issues

12.1.1. None of the indicators are on

Problem phenomenon

None of the 5500 Router indicators are on

Cause analysis

The possible causes are as follows:

The power supply does not meet the requirements

The power supply is not connected to the power port of the router

Solution

If the power supply does not meet the requirements, please make sure that the power supply range of the power supply is 5~36V.

If the power port of the router cannot be connected to the power supply, please plug the power cable into the power port.

12.1.2. Problems with the SIM card connectivity

Problem phenomenon

The SIM card holder cannot be inserted properly.

Cause analysis

The possible causes are as follows:



The SIM card holder has been damaged

The SIM card is inserted in the wrong direction

Solution

If the SIM card holder is damaged, please contact our technical support engineer if you need to report for repair.

If the SIM card is inserted in the wrong direction, make sure that the SIM card is inserted into the card slot correctly.

12.1.3. Network port connection issues

Problem phenomenon

The LAN port indicator is not lit and the router page cannot be accessed.

Cause analysis

The possible causes are as follows:

The network cable is not installed correctly

The network cable is damaged

The PC NIC is working abnormally

Solution

If the network cable is installed incorrectly, please reinstall the network cable. If the network cable is damaged, please replace the network cable.

If the network card on the PC side is working abnormally, please replace the network card.

12.1.4. Antenna connection issues

Problem phenomenon

The antenna does not fit properly

Cause analysis

possible causes are as follows:

The antenna does not meet the requirements of the accessories

The antenna connection is incorrect

Solution

If the antenna is installed incorrectly, replace the antenna that meets the requirements.

If the antenna is not connected correctly, please reconnect the antenna.

12.2. Dial-up issues

12.2.1. Dial-up dropped

Problem phenomenon

5500 Router is interrupted during dialing and fails to dial.

possible causes are as follows:

The SIM card network type does not meet the requirements

The SIM card is in arrears

The power supply does not meet the requirements

Modem dialing configuration is incorrect

Solution

If the SIM card network type is incorrect, please replace the corresponding type of SIM card according to the module.

If the SIM card is in arrears, please go to the designated ISP to top up the SIM card.

If the power supply does not meet the requirements, please replace the power supply that meets the requirements.

If the modem dial-up configuration is incorrect, please refer to "Mobile Network" for correct configuration.

12.2.2. No signal display

Problem phenomenon

5500 Router mobile network status page is not displayed.

Cause analysis

possible causes are as follows:

The antenna connection is not normal The modem is not dialed on the line Modem disconnected

Solution

Reconnect the antenna as per the correct operation

If the modem does not dial the number, see "Mobile Network".

If the modem is disconnected, please check whether there is a process in the application of the router that causes the router to go offline

12.2.3. SIM/UIM card could not be found

Problem phenomenon

5500 Router mobile network status page shows that the SIM card could not be found.

Cause analysis

possible causes are as follows:

The SIM card is damaged

The SIM card is loose, the contact is not normal, or the installation is incorrect

Solution

If the SIM card is damaged or invalid, replace the SIM

If the SIM card is loose, has abnormal contact, or is not installed correctly, please reinstall it.

12.2.4. Communication signal is weak

Problem phenomenon

5500 Router Mobile Network Status page shows no or poor signal.

Cause analysis

possible causes are as follows:

The antenna is not installed or damaged

The network coverage and signal strength of the area where the device is located are weak

Solution

Reconnect the antenna as per the correct operation

If the antenna is damaged, replace the antenna

If the network coverage and signal strength in the area where the device is located are weak, contact the network operator for a reasonable solution

12.3. VPN connection issues

12.3.1. VPN can't connect

Problem phenomenon

The status page shows that the VPN could not connect

Cause analysis

The possible causes are as follows:

The interface used by the VPN connection is not working properly

The VPN configuration parameters are incorrect

Solution

If the interface used by the VPN connection is not working properly, reconfigure the interface used correctly. If the modem interface is not working properly, see Mobile Network.

If the VPN interface is not working properly, see VPN Configuration.

If the VPN configuration parameters are incorrect, see VPN Configuration.

If the VPN peer server is not working properly, check the configuration and working status of the VPN peer server.

12.3.2. The VPN can't communicate

Problem phenomenon

The VPN page shows that it is connected, but it is unable to communicate

Cause analysis

possible causes are as follows:

The route information configured in the routing table is incorrect The VPN peer server is incorrectly configured

Solution

If the route is incorrect, add the correct route

If the VPN peer server is incorrectly configured, change the configuration of the VPN peer server.

12.4. WEB configuration operation issues

12.4.1. firmware upgrade failed

Problem phenomenon

The firmware upgrade found that the upgrade was not successful

Cause analysis

possible causes are as follows:

The router restarts due to other functions during the upgrade The power supply does not meet the requirements

The model and format of the upgraded firmware are incorrect

The router loses power during the upgrade

Solution

If the upgrade fails due to the restart due to other functions during the upgrade, please disable the other functions and upgrade again.

If the power supply does not meet the requirements, replace the power supply that meets the requirements.

If the firmware model is incorrect, replace the firmware with the correct format and match the 5500 Router.

If the router is powered off during the upgrade, make sure that the router is powered normally during the upgrade.

12.4.2. Forgot router password

Problem phenomenon

I forgot my password when logging in to the router page

Cause analysis

The user has changed the password on the user management page

Solution

Step 1: The router is powered on

Step 2: Press and hold the RST reset button for about 15 seconds for the system to reboot successfully, otherwise try the operation again.

12.4.3. What is the cause of frequent reboots

Check first:

Whether the module is normal.

Whether the Router is inserted into the SIM card.

Whether the SIM card is enabled for data service and whether it is shut down in arrears.

Whether the dialing parameter account/password is correct. Check if the signal is normal.

Check if the power supply voltage is normal.

12.5. Other issues

12.5.1. After modifying the IP address, I forgot to configure the Router and could not set it

The router is powered on, and the REST settings button can be restored by pressing and holding the REST settings button (until the system restarts).

12.5.2. Why is the network indicator not lit when connected to the PC after powering on?

When the PC and Router are directly connected through a network cable, please check whether the PC and Router are connected with a network crossover cable. Check if the network cable is normal.