



# 4G Router

## User's Manual








# Foreword

## General

This manual introduces the functions and operations of the 4G Router device (hereinafter referred to as "the Router").

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.1	Update images in 1.3, 2.3.2 and 3.1.	March 2020
V1.0.0	First release.	Janurary 2020

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please

contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

## Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

## Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

# Table of Contents

<b>Foreword .....</b>	<b>I</b>
<b>Important Safeguards and Warnings .....</b>	<b>III</b>
<b>1 Introduction.....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Features .....	1
1.3 Typical Application.....	2
<b>2 Installation.....</b>	<b>3</b>
2.1 Out-of-Box Checking.....	3
2.2 Dimensions .....	3
2.3 Installation and Cable Connection .....	4
2.3.1 Antenna Installation .....	4
2.3.2 SIM/UIM Card Installation.....	4
2.3.3 Power Supply.....	5
2.3.4 Indicator .....	5
2.3.5 Reset.....	6
<b>3 Configuration and Management .....</b>	<b>7</b>
3.1 Device Connection .....	7
3.2 Login.....	7
3.3 Setup .....	8
3.3.1 Basic Setup.....	8
3.3.2 Dynamic DNS .....	17
3.3.3 MAC Address Clone .....	19
3.3.4 Advanced Router .....	19
3.3.5 VLANS .....	21
3.3.6 Networking.....	22
3.4 Wireless.....	25
3.4.1 Basic Settings .....	25
3.4.2 Wireless Security .....	27
3.5 Services .....	29
3.5.1 DHCP Server .....	29
3.5.2 DNSMasq.....	29
3.5.3 SNMP.....	30
3.5.4 System Log.....	31
3.5.5 Telnet .....	32
3.5.6 WAN Traffic Counter .....	32
3.6 VPN .....	32
3.6.1 PPTP.....	32
3.6.2 L2TP .....	35
3.6.3 OPENVPN .....	37
3.6.4 IPSEC .....	41
3.6.5 GRE .....	45
3.7 Security .....	46

---

3.7.1 Firewall.....	46
3.7.2 Log Management.....	48
3.8 Access Restrictions.....	49
3.8.1 WAN Access .....	49
3.8.2 URL Filter.....	50
3.8.3 MAC Filter.....	50
3.8.4 Packet Filter.....	51
3.9 NAT .....	53
3.9.1 Port Forwarding .....	53
3.9.2 Port Range Forwarding .....	53
3.9.3 DMZ .....	54
3.9.4 Virtual IP Mapping .....	55
3.10 QoS Setting.....	55
3.10.1 Basic .....	55
3.10.2 Classify .....	56
3.11 Serial Applications.....	58
3.12 Administration.....	60
3.12.1 Router Management.....	60
3.12.2 Keep Alive.....	64
3.12.3 Commands .....	64
3.12.4 Factory Defaults.....	65
3.12.5 Firmware Upgrade.....	66
3.12.6 Backup and Restore .....	66
3.13 Status .....	67
3.13.1 Router .....	67
3.13.2 WAN.....	68
3.13.3 LAN.....	70
3.13.4 Wireless .....	72
3.13.5 Device Management.....	74
3.13.6 Bandwidth .....	75
3.13.7 System Information.....	76
<b>Appendix 1 Cybersecurity Recommendations .....</b>	<b>79</b>

# 1 Introduction

## 1.1 Overview

DH-WM4700-O 4G Router (hereinafter referred to as "the Router") is a kind of cellular terminal device that provides data transmission by public cellular network.

It adopts high-powered industrial 32-bit CPU and is embedded real time operating system. It provides one RS232 (or RS485/RS422), four Ethernet LAN, one Ethernet WAN and one Wi-Fi port for serial, Ethernet and Wi-Fi devices to achieve data transmission and routing.

The Router has been widely used on M2M fields, such as self-service terminal industry, intelligent transportation, smart grid, smart home, industrial automation, intelligent building, public security, fire protection, environment protection, telemetry, finance, POS, water supply, meteorology, remote sensing, digital medical, military, space exploration, agriculture, forestry and petrochemical.

## 1.2 Features

### Design for Industrial Application

- High-performance industrial cellular module
- High-performance industrial 32-bit CPU
- Adopt metal shell with IP30 protection. Suitable for industrial control field applications
- Power supply: 12V DC

### Stability and Reliability

- Support hardware and software WDT
- Support auto recovery mechanism to make the Router always online
- Ethernet port: 1.5kV magnetic isolation protection
- RS232/RS485/RS422 port: 15kV ESD protection
- SIM/UIM port: 15kV ESD protection
- Power port: reverse-voltage and overvoltage protection
- Antenna port: lightning protection(optional)
- Standard and Convenience
- Support standard RS232(or RS485/RS422), Ethernet and WIFI port that can connect to serial, Ethernet and WIFI devices directly
- Support standard WAN port and PPPOE protocol that can connect to ADSL directly
- Support intellectual mode, enter into communication state automatically when powered
- Provide management software for remote management
- Support several work modes
- Convenient configuration and maintenance interface (WEB or CLI)

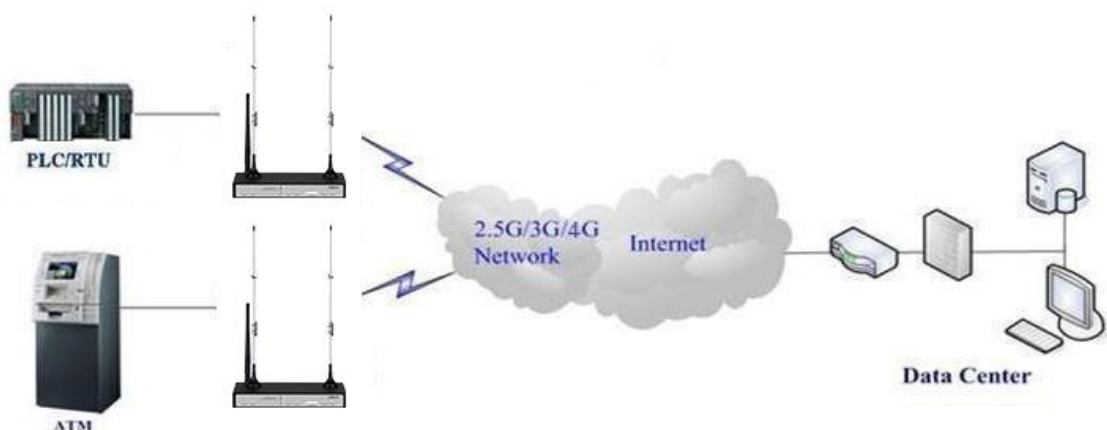
## High-performance

- Multiple WAN access methods, including static IP, DHCP, L2TP, PPTP, PPPOE and 2.5G/3G/4G
- Double link backup between cellular and WAN(PPPOE, ADSL) (optional)
- VPN client (PPTP, L2TP, OPENVPN, IPSEC and GRE)
- VPN server (PPTP, L2TP, OPENVPN, IPSEC and GRE)
- Remote management, such as SYSLOG, SNMP, TELNET, SSHD, HTTPS
- Local and remote firmware upgrade, import and export configure file
- NTP, RTC embedded
- Multiple DDNS provider service
- VLANs, MAC Address clone, PPPoE Server
- WIFI supports 802.11b/g/n, supports AP, client, Repeater, Repeater Bridge and WDS(optional) mode
- WIFI supports WEP,WPA,WPA2 encryption, supports RADIUS authentication and MAC address filter
- Multiple online trigger ways, including SMS, ring and data. Support link disconnection when timeout
- APN/VPDN
- Multi-channel DHCP server and client, DHCP bundled with MAC address, DDNS, firewall, NAT, DMZ host, QoS, traffic statistics, real-time display of data transmission rate
- Full protocol support , such as TCP/IP, UDP, FTP (optional), HTTP
- SPI firewall, VPN traversal, access control, URL filtering
- Schedule Reboot, Schedule Online and Offline

## 1.3 Typical Application

The typical application of the Router is shown in Figure 1-1.

Figure 1-1 Typical application





## 2 Installation

The Router must be installed correctly to make it work properly. Install the Router under the guidance of qualified engineers.



Forbid to install the Router when powered.

### 2.1 Out-of-Box Checking

- Check if there is obvious damage to the appearance of the Router.
- Make sure that the components are complete against the packing list. See Table 2-1 for details.

Table 2-1 Product list

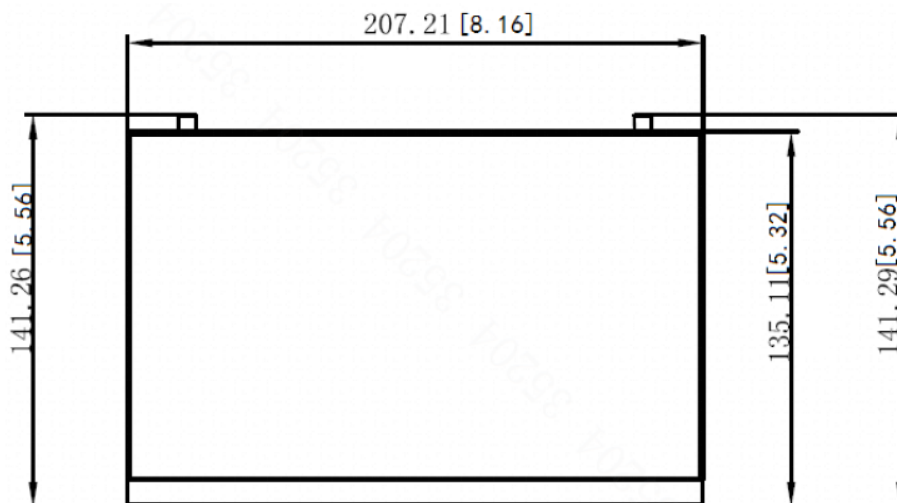
Name	Quantity
Router host	1
Cellular antenna (Male SMA)	2
WIFI antenna (Female SMA)	1
Power adapter	1
Network cable	1
RS232 console cable (optional)	1
Quick Guide Start	1
Certification card	1

### 2.2 Dimensions

Figure 2-1 Front panel (unit: mm [inch])



Figure 2-2 Top panel (unit: mm [inch])



## 2.3 Installation and Cable Connection

### 2.3.1 Antenna Installation



- The cellular antenna and the WIFI antenna cannot be connected reversely, otherwise the Router cannot work.
- Make sure that the antennas are tightened, or the signal quality will be affected.

Step 1 Screw the SMA male pin of the cellular antenna to the female SMA interface of the Router with sign "ANT-M" and "ANT-A".

Step 2 Screw the SMA female pin of the WIFI antenna to the male SMA interface of the Router with sign "WIFI".

### 2.3.2 SIM/UIM Card Installation

Step 1 Power off the Router, and press the out button of the SIM/UIM card outlet with a needle object. And the SIM/UIM card sheath ejects.

Step 2 Put the metal side of SIM/UIM card into the card sheath.

Step 3 Insert the card sheath back to the SIM/UIM card outlet.

Figure 2-3 SIM/UIM card installation



### 2.3.3 Power Supply

The power supply range of the Router is 5V–36V DC. The standard power supply is 12V/1.5A DC.

When you use external power supply, make sure that the power supply is stable (that is, the ripple is less than 300mV, and the instantaneous voltage is not more than 36V) and the power is above 8W.



Standard power supply: 12V/1.5A DC is recommended.

### 2.3.4 Indicator

For details of the indicators of the Router, see Table 2-2.

Table 2-2 Indicator description

Indicator	Status	Description
Power	On	The Router is powered on.
	Off	The Router is powered off or during shutdown by timing switch.
System	Flash	The system is running normally.
	Off	The system is abnormal.
Online	On	The Router is connected to the network.
	Off	The Router is disconnected to the network.
SIM	On	SIM/UIM card is identified.
	Off	SIM/UIM card is not identified.

Indicator	Status	Description
Local Network	On/Flash	<ul style="list-style-type: none"><li>• On: Network port is connected.</li><li>• Flash: Data transmission is in progress.</li></ul>
	Off	Network port is disconnected.
WAN	On/Flash	<ul style="list-style-type: none"><li>• On: WAN port is connected.</li><li>• Flash: Data transmission is in progress.</li></ul>
	Off	WAN port is disconnected.
WIFI	On	Wi-Fi is enabled.
	Off	Wi-Fi is not enabled.
Signal Strength	One light on	Weak signal strength (less than -90 dbm).
	Two lights on	Medium signal strength (-70 dbm to -90 dbm).
	Three lights on	Strong signal strength (more than -70 dbm).

### 2.3.5 Reset

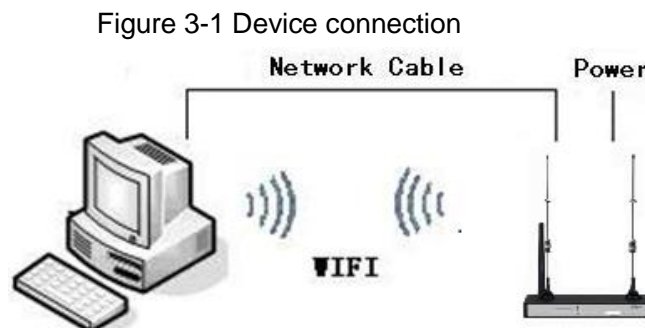
The Router has a Reset button to restore it to the factory default settings. When you press the Reset button for up to 15 s, the Router will restore to the factory default settings and restart automatically.

## 3 Configuration and Management

### 3.1 Device Connection

Before configuration, connect the Router and the PC with the network cable or Wi-Fi. See Figure 3-1.

- Connect with network cable:  
Connect one end of the network cable to the Local Network (LAN) port of the Router, and another end of the network cable to the Ethernet port of the PC.
- Connect with Wi-Fi:  
The default SSID of the Router is "Dahua Wireless", and password is not required.



### 3.2 Login

Before you configure the Router, make sure that:

- The Router is connected to the PC.
- The network of the PC is set to automatic access mode.

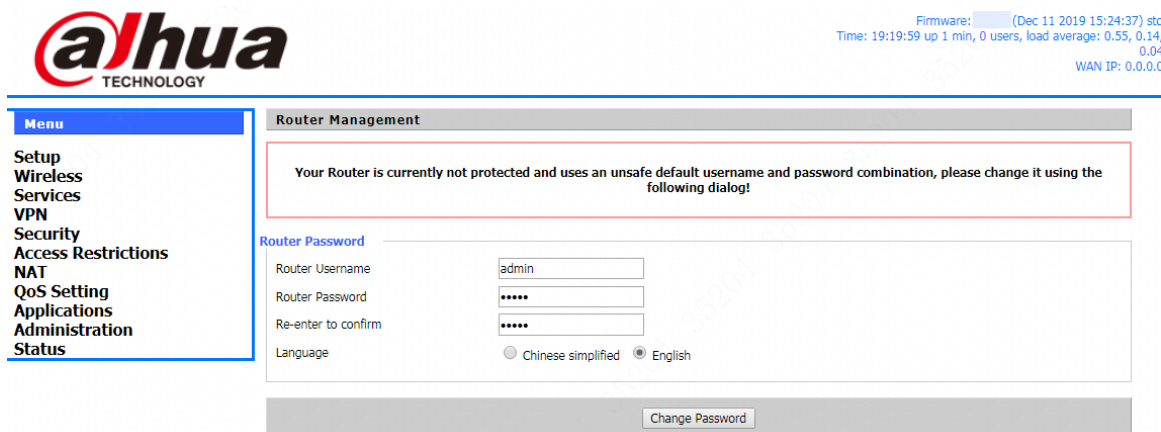
Step 1 Open the browser, enter IP address of the Router (the default IP is 192.168.1.110) and then press Enter key.

Step 2 Enter the login account and password.



- The account is admin and password is admin by default.
- It is recommended to change the user name and password after first login.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
- You can also reset password in **Administratio > Management** , refer to 3.12.1.1 Router Password.

Figure 3-2 Initial interface



## 3.3 Setup

### 3.3.1 Basic Setup

You can configure WAN and network.

#### 3.3.1.1 WAN Setup

You can connect the Router to Internet by WAN setup.

#### WAN Connection Type

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Setup > Basic Setup**.

Step 3 In **WAN Connection Type** section, select **Connection Type**.

6 options are available:

- Disabled: WAN connection is disabled.
- Static IP: Suitable for commercial optical fiber and other special line access.
- Automatic Configuration-DHCP: Wire connection, obtain IP address of WAN port automatically through DHCP.
- dhcp-4G: Obtain IP address of WAN port automatically through DHCP-4G. This option is recommended.
- PPPOE: Wire connection, suitable for China Telecom, China Unicom ADSL broadband service and other broadband service providers.
- 3G/UNMTS/4G/LTE: Network types are selectable.

Step 4 Configure the corresponding parameters.

Figure 3-3 Set WAN connection type

**WAN Connection Type**

Connection Type:

User Name:

Password:   Unmask

APN:

Fixed WAN IP:  Enable  Disable

Allow these authentication:  PAP  CHAP

Connection type:

PIN:   Unmask

Keep Online Detection:

Detection Interval:  Sec.

Primary Detection Server IP:

Backup Detection Server IP:

Enable Dial Failure to Restart:  Enable  Disable (Default: 10 minutes)

Wan Nat:  Enable  Disable

STP:  Enable  Disable

Table 3-1 Parameters to be configured when Static IP as the WAN connection type

Parameter	Description
WAN IP Address	Set IP address by your own or ISP assigns.
Subnet Mask	Set subnet mask by your own or ISP assigns.
Gateway	Set gateway by your own or ISP assigns.
Static DNS 1/DNS 2/DNS 3	Set static DNS by your own or ISP assigns.
Keep Online Detection	Select online detection mode to detect whether the Internet connection is active. The following detection mode are available: None (disable this function), Ping, Route and TCP.
Detection Interval	Set time interval between two detections, expressed by seconds.
Primary Detection Server IP	Enter the IP address of the server which is used to response the Router's detection packet.
Backup Detection Server IP	
Enable Dial Failure to Restart	Whether to enable the restart of the Router when dial-up fails.

Table 3-2 Parameters when Automatic Configuration-DHCP as the WAN connection type

Parameter	Description
Keep Online Detection	Select online detection mode to detect whether the Internet connection is active. The following detection modes are available: <b>None</b> (disable this function), <b>Ping</b> , <b>Route</b> and <b>TCP</b> .
Detection Interval	Set time interval between two detections, expressed by seconds.
Primary Detection Server IP	Enter the IP address of the server which is used to response the Router's detection packet.
Backup Detection Server IP	
Enable Dial Failure to Restart	Whether to enable the restart of the Router when dial-up fails.

Table 3-3 Parameters to be configured when dhcp-4G as the WAN connection type

Parameter	Description
User Name	Enter the user name for login to the Internet.
Password	Enter the password for login to the Internet.
APN	Enter the access point name of your ISP.
Fixed WAN IP	Set whether to enable fixed WAN IP. If enabled, enter the WAN IP address.
Allow these authentication	Supports PAP and CHAP.
Connection type	Supports the following options are available: Auto, Force 3G, Force 2G, Prefer 3G, Prefer 2G and Force 4G.
PIN	Enter PIN code of the SIM card.
Keep Online Detection	Select online detection mode to detect whether the Internet connection is active. The following detection modes are available: <b>None</b> (disable this function), <b>Ping</b> , <b>Route</b> and <b>TCP</b> .
Detection Interval	Set time interval between two detections, expressed by seconds.
Primary Detection Server IP	Enter the IP address of the server which is used to response the Router's detection packet.
Backup Detection Server IP	
Enable Dial Failure to Restart	Whether to enable the restart of the Router when dial-up fails.



Table 3-4 Parameters to be configured when PPPoE as the WAN connection type



Parameter	Description
User Name	Enter the user name for login to the Internet.
Password	Enter the password for login to the Internet.
Keep Online Detection	Select online detection mode to detect whether the Internet connection is active. The following detection modes are available: <b>None</b> (disable this function), <b>Ping</b> , <b>Route</b> , <b>PPP</b> and <b>TCP</b> .
Detection Interval	Set time interval between two detections, expressed by seconds.
Primary Detection Server IP	Enter the IP address of the server which is used to response the Router's detection packet.
Backup Detection Server IP	 <p>When you choose <b>Route</b> or <b>Ping</b> as the detection mode, make sure that <b>Primary Detection Server IP</b> and <b>Backup Detection Server IP</b> are valid and stable, because they have to response the detection packet frequently.</p>
Fixed WAN IP	Set whether to enable fixed WAN IP. If enabled, enter the WAN IP address.
Fixed WAN GW Address	Set whether to enable fixed WAN gateway address. If enabled, enter the WAN gateway address.
Enable Dial Failure to Restart	Whether to enable the restart of the Router when dial-up fails.
Force reconnect	Whether to enable mandatory reconnection.
Time	This parameter is valid only when <b>Force reconnect</b> is enabled. Set when to reconnect.

Table 3-5 Parameters to be configured when 3G/UNMTS/4G/LTE as the WAN connection type

Parameter	Description
User Name	Enter the user name provided by the Internet Service Provider (ISP) for login to the Internet.
Password	Enter the password provided by the ISP for login to the Internet.
Dial String	Select the dial-up number of your ISP.
APN	Enter access point name of your ISP.
PIN	Enter PIN code of your SIM card.
Connection type	Select a connection type as your need.
Allow these authentication	The following authentications are supported: PAP, CHAP, MS-CHAP and MS-CHAPv2.

Parameter	Description
Keep Online Detection	Select online detection mode to detect whether the Internet connection is active. The following detection modes are available: <b>None</b> (disable this function), <b>Ping</b> , <b>Route</b> , <b>PPP</b> and <b>TCP</b> .
Detection Interval	Set time interval between two detections, expressed by seconds.
Primary Detection Server IP	Enter the IP address of the server which is used to response the Router's detection packet.
Backup Detection Server IP	 <p>When you choose <b>Route</b> or <b>Ping</b> as the detection mode, make sure that <b>Primary Detection Server IP</b> and <b>Backup Detection Server IP</b> are valid and stable, because they have to response the detection packet frequently.</p>
Fixed WAN IP	Whether to enable fixed WAN IP address.
Fixed WAN GW Address	Whether to enable fixed WAN gateway address.
Enable Dial Failure to Restart	Whether to enable the restart of the Router when dial-up fails.
Ppp Asyncmap	Whether to enable PPP asyncmap.
Force reconnect	Whether to enable mandatory reconnection.
Time	This parameter is valid only when <b>Force reconnect</b> is enabled. Set when to reconnect.

Step 5 Set WAN NAT and STP.



STP (Spanning Tree Protocol) can be applied to the loop network to achieve path redundancy through certain algorithms. At the same time, the loop network is trimmed to a tree network without loop to avoid the proliferation and infinite loop of packets in the loop network.

Step 6 Click **Save** to save the configuration.

Step 7 Click **Apply Settings** to apply the configuration.

Step 8 (Optional) Click **Cancel Changes** to cancel the configuration.

## Optional Settings

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Setup > Basic Setup**.


Step 3 In **Optional Settings** section, set parameters as needed.

Figure 3-4 Optional settings

**Optional Settings**

Router Name	<input type="text" value="Dahua"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
MTU	Auto ▼ <input type="text" value="1500"/>
Force Net Card Mode	Auto ▼

Table 3-6 Parameter description of optional settings

Parameter	Description
Router Name	Set router name. The name length can be up to 39 characters.
Host Name	Enter host name and domain name which are provided by your ISP.
Domain Name	Generally you can leave them blank.
MTU	<p>MTU (Maximum Transmission Unit) specifies the maximum packet value allowed in Internet transmission.</p> <ul style="list-style-type: none"> <li>● <b>Auto</b>: 1500 by default.</li> <li>● <b>Manual</b>: 576–1492 in PPPoE mode, 576–16320 in other modes. Value among 1200–1500 is recommended.</li> </ul> <p></p> <ul style="list-style-type: none"> <li>● 1492 is recommended.</li> <li>● If the Router is required to select the best MTU for the Internet, select <b>Auto mode</b>.</li> </ul>
Force Net Card Mode	Supports the following modes: <b>Auto</b> , <b>100M</b> and <b>10M</b> .

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.1.2 Network Setup

You can configure router IP, WAN port, DHCP, time settings and adjust time.

#### Router IP

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Basic Setup**.

**Step 3** In **Router IP** section, configure router IP.

Figure 3-5 Router IP

**Router IP**

Local IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Gateway	<input type="text"/>
Local DNS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Table 3-7 Parameter description of router IP

Parameter	Description
Local IP Address	Set local IP address of the Router.
Subnet Mask	Set the subnet mask of the Router.
Gateway	Set the internal gateway of the Router, the default internal gateway is the address of the Router.
Local DNS	DNS server is automatically assigned by the operator's access server. If there is a more stable and reliable DNS server, you can set it. Otherwise, keep the default setting.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## WAN Port



You can set WAN port only when the WAN connection type is disabled.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Basic Setup**.

**Step 3** In **WAN Port** section, enable **Assign WAN Port to Switch** as needed.

Figure 3-6 WAN port

**WAN Port**

Assign WAN Port to Switch

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## Network Address Server Settings (DHCP)

The Router can serve as a DHCP server. And DHCP server automatically assigns an IP address for each computer in the network.

If the DHCP server function of the Router is enabled, you can set all the computers on the LAN to automatically obtain an IP address and DNS.



Make sure that there is no other DHCP server in the network.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Basic Setup**.

**Step 3** In **Network Address Server Settings (DHCP)** section, set parameters.


Figure 3-7 DHCP setting

**Network Address Server Settings (DHCP)**

DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	172.12.70. 100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	0. 0. 0. 0
Static DNS 2	0. 0. 0. 0
Static DNS 3	0. 0. 0. 0
WINS	0. 0. 0. 0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

Table 3-8 Description of DHCP parameters

Parameter	Description
DHCP Type	DHCP Server and DHCP Forwarder. If <b>DHCP Type</b> is set to <b>DHCP Forwarder</b> , you only need to set <b>DHCP Server</b> .
DHCP Server	Enabled by default. <ul style="list-style-type: none"> <li>If there is already a DHCP server on network or you do not want a DHCP server, select <b>Disable</b>.</li> <li>If <b>DHCP Type</b> is set to <b>DHCP Forwarder</b>, you only need to set the IP address of the DHCP Server.</li> </ul>
Start IP Address	Enter a numerical value for the DHCP server to start with when assigning IP addresses. <ul style="list-style-type: none"> <li>The value range is 1–254.</li> <li>The default value is 100.</li> <li>Do not start with 192.168.1.1 (default IP address of the Router).</li> </ul>
Maximum DHCP Users	Enter the maximum number of PCs that the DHCP server can assign IP addresses to.  The absolute maximum is 253 if 192.168.1.2 is your start IP address.

Parameter	Description
Client Lease Time	Specifies the lease period of the dynamic IP address occupied by a network user. After the dynamic IP address expires, a new dynamic IP address will be automatically assigned to the user.  The value range is 0–99999, and the default value is 1440 minutes (1 day).
Static DNS 1/DNS 2/DNS 3	The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS server IP address. If you want to use another DNS server, enter the IP address of the DNS server in one of these fields. So that the Router can quickly access to the operating DNS servers. You can enter up to 3 DNS server IP addresses.
WINS	The Windows Internet Naming Service (WINS) manages every PC that interacts with the Internet. If you want to use a WINS server, enter the IP address of the WINS server. Otherwise, leave it blank.
Use DNSMasq for DHCP	Set as needed.
Use DNSMasq for DNS	Add the domain name to the local search domain to increase the extension of host option. <ul style="list-style-type: none"> <li>• If it is enabled, IP address and DNS will be assigned for the subnet.</li> <li>• If it is disabled, dhcpd service is used to assign IP address and DNS for the subnet.</li> </ul>
DHCP-Authoritative	Set as needed.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## Time Settings

You can set the time zone as needed.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Basic Setup**.

**Step 3** In **Time Settings** section, enable NTP Client.

Figure 3-8 Enable NTP client

**Time Settings**

NTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone	UTC+08:00 ▼
Summer Time (DST)	none ▼
Server IP/Name	<input type="text"/>

**Step 4** Set parameters.

Table 3-9 Parameter description of time settings

Parameter	Description
NTP Client	Whether to get the system time from NTP server or not.
Time Zone	Set time zone.
Summer Time (DST)	Set as needed.
Server IP/Name	Enter IP address of NTP server, up to 32 characters. If blank, the system will find a server by default.

Step 5 Click **Save** to save the configuration.

Step 6 Click **Apply Settings** to apply the configuration.

Step 7 (Optional) Click **Cancel Changes** to cancel the configuration.

## Adjust Time

You can adjust the system time.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Setup > Basic Setup**.

Step 3 In **Adjust Time** section, adjust the system time by **Auto** or **Manual**, and then click **Set**.



If the NTP service is unavailable, you can adjust time manually.

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.2 Dynamic DNS

Dynamic DNS (DDNS) allows you to access your network by using domain names instead of IP addresses. The DDNS service manages changing IP addresses and updates your domain information dynamically.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Setup > DDNS**.

Step 3 Select a DDNS service.

The following options are available: Disable, DynDNS.org, freedns.afraid.org, ZonEdit.com, No-IP.com, 3322.org, easyDNS.com, TZO.com, DynSIP.org and Custom.



The actual interfaces are different when you select different DDNS services. Take **3322.org** as an example.

Figure 3-9 3322.org as DDNS service

**DDNS**

DDNS Service:

User Name:

Password:   Unmask

Host Name:

Type:

Wildcard:

Do not use external ip check:  Yes  No

---

**Options**

Force Update Interval:  (Default: 10 Days, Range: 1 - 60)

---

**DDNS Status**

Connecting to server

---

**Step 4** Set DDNS parameters.

Table 3-10 Description of DDNS parameters

Parameter	Description
User Name	Enter the user name that is registered with the DDNS server. The maximum length is 64 characters.
Password	Enter the password for the user name that is registered with the DDNS server. The maximum length is 32 characters.
Host Name	Enter the host name that is registered in DDNS server.
Type	The types might vary according to different DDNS services, and the actual interface shall prevail.
Wildcard	Set whether to support wildcard or not. The default is OFF. ON means "*.host.3322.org" is equal to "host.3322.org".
Do not use external ip check	Set whether to use external IP check or not.

- Step 5** In **Options** section, set **Force Update Interval**.  
Dynamic DNS will be mandatorily updated to the server in the set interval.
- Step 6** Click **Save** to save the configuration.
- Step 7** Click **Apply Settings** to apply the configuration.
- Step 8** (Optional) Click **Cancel Changes** to cancel the configuration.
- Step 9** (Optional) In **DDNS Status** section, you can view DDNS status.  
DDNS status shows connection log information.



### 3.3.3 MAC Address Clone

Some ISPs might require you to register your MAC address. If you do not want to re-register your MAC address, you can clone the MAC address of the Router to your MAC address registered with ISP.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > MAC Address Clone**.

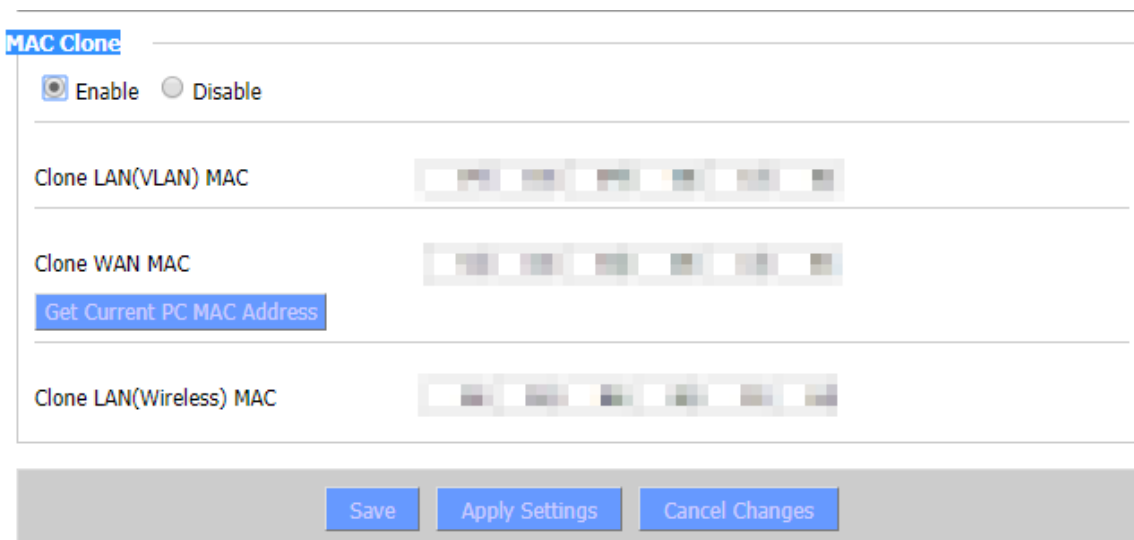
**Step 3** In **MAC Clone** section, select **Enable**.

MAC Clone can clone three parts: LAN MAC Clone, WAN MAC Clone, and Wireless MAC Clone.



- The MAC address is 48-bit and cannot be set as a multicast address, that is, the first byte should be even.
- The MAC address of bridge br0 is determined by the smaller value of wireless MAC address and LAN MAC address.

Figure 3-10 Enable MAC Clone



**Step 4** (Optional) Click **Get Current PC MAC Address** to get your current PC MAC address.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.4 Advanced Router

You can set the operating mode and static routing.

#### Operating Mode

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Advanced Routing**.

**Step 3** In **Operating Mode** section, select an operating mode.

The following operating modes are available: Gateway, BGP, RIP2 Router, OSPF Router and Router.

The default operating mode is Gateway. And Gateway mode is also recommended for most users.



The parameters might vary according to the different operating modes. Take Gateway as an example.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## Static Routing

A static routing is a pre-determined path for transmission of network information to a specific host or network.

To set up a static route between the router and another network:

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Advanced Routing**.

**Step 3** In **Static Routing** section, set parameters.

Figure 3-11 Static routing

Table 3-11 Description of static routing parameters

Parameter	Description
Select set number	Select a number from the dropdown list.  To delete a static routing entry, you can select a number that you want to delete, and then click <b>Delete</b> .
Route Name	Set routing name. The name length can be up to 25 characters.
Metric	The unit of measure for the routing from the source address to the destination address. The range is 0–9999.

Parameter	Description
Destination LAN NET	Enter the address of the network or host to which you want to assign a static routing.
Subnet Mask	The subnet mask determines which portion of an IP address is the network portion, and which portion is the host portion.
Gateway	Enter the IP address of the gateway device that is between the router and the destination network or host.
Interface	Select <b>LAN&amp;WLAN</b> , <b>WAN</b> , <b>ANY</b> , <b>3G</b> and <b>IPSEC</b> according to the destination IP address.



Click **Show Routing Table**, you can view the routing details of the current router.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.5 VLANS

You can divide different VLAN ports as needed.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > VLANS**.

**Step 3** Set VLAN, Port and Assigned To Bridge.

15 VLAN ports (VLAN1–VLAN15) are supported. But there are only 5 time ports (1 WAN port and 4 LAN ports), which are divided according to your needs. Meanwhile LAN port and WAN port cannot be divided into the same VLAN port.

Figure 3-12 VLAN

VLAN

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN ▼
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None ▼

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.3.6 Networking

You can create bridges, assign ports to bridges, view the current bridging list, configure ports and manage DHCPD servers.

### 3.3.6.1 Bridging

#### Create Bridge

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Networking**.

**Step 3** In **Create Bridge** section, click **Add**.

**Step 4** Enter bridge name, set other bridge parameters, and then click **Save**.

- STP: Whether to enable Spanning Tree Protocol.
- Prio: Indicates the priority level of STP. The smaller the number, the higher the priority.
- MTU: Maximum Transmission Unit, the default value is 1500.

Figure 3-13 Create bridge

**Create Bridge**

Bridge 0	<input type="text" value="br0"/>	STP <input type="button" value="Off"/>	Prio <input type="text" value="32768"/>	MTU <input type="text" value="1500"/>	<input type="button" value="Delete"/>
Bridge 1	<input type="text" value="br1"/>	STP <input type="button" value="On"/>	Prio <input type="text" value="32768"/>	MTU <input type="text" value="1500"/>	<input type="button" value="Delete"/>
IP Address	<input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0"/>				
Subnet Mask	<input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0"/>				
<input type="button" value="Add"/>					



- The smaller the number after the bridge, the higher the priority. For example, the priority of Bridge 0 is higher than that of Bridge 1.
- Click **Delete**, you can delete the corresponding bridge.

**Step 5** Enter IP address and subnet mask of the bridge.

**Step 6** Click **Apply Settings** to add a bridge.

**Step 7** (Optional) Click **Cancel Changes** to cancel the adding.

## Assign to Bridge

You can assign any valid interface to a network bridge. For example, assign ra0 interface (wireless interface) to br1 bridge.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Networking**.

**Step 3** In **Assign to Bridge** section, click **Add**.

**Step 4** Select bridge, interface and set priority.

Prio means priority level, works if multiple ports are within the same bridge. The smaller the number, the higher the priority.



This bridge assignment is only used for LAN ports, WAN ports are not supported.

Figure 3-14 Assign to bridge

**Assign to Bridge**

Assignment 0	<input type="button" value="br0"/>	Interface <input type="button" value="eth2"/>	Prio <input type="text" value="63"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>				
<input type="button" value="none"/> <input type="button" value="br0"/>				

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.



In **Current Bridging Table** section, you can view the bridge list and binding relationships between bridges and LAN ports after successful assignment.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.6.2 Port Setup

You can set the properties of each port. Take ra0 port as an example.

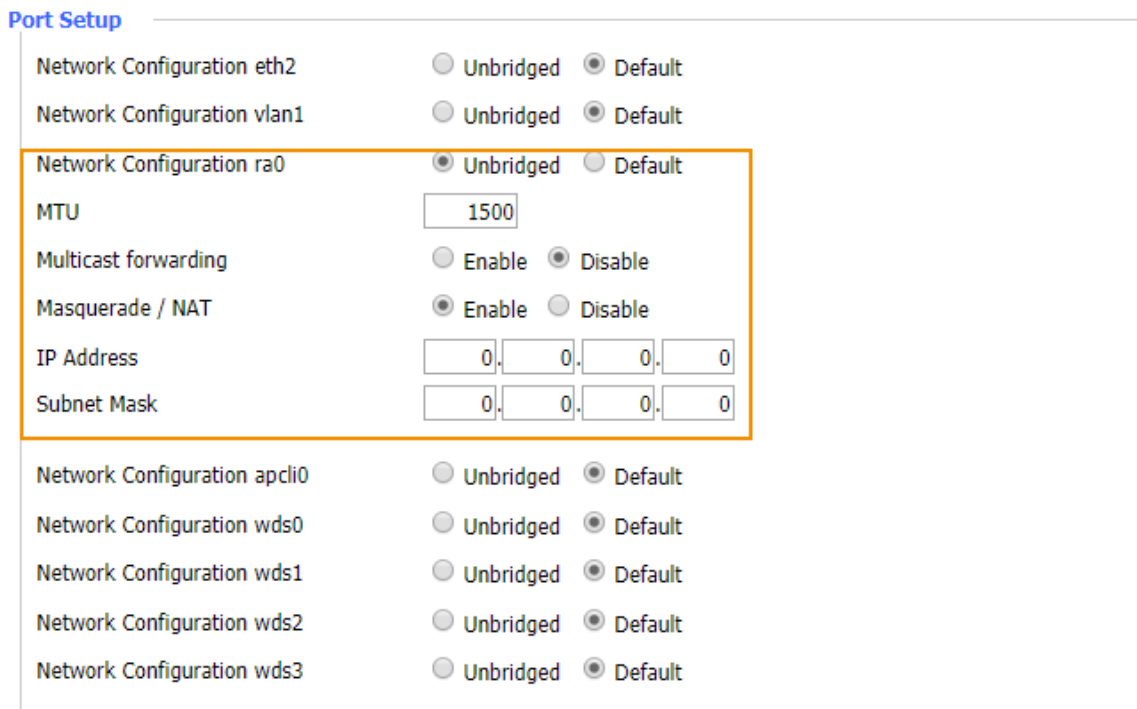
**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Networking**.

**Step 3** In **Port Setup** section, select **Unbridged** next to **Network Configuration ra0**.

**Step 4** Set properties of the selected port.

Figure 3-15 Port setup



**Port Setup**

Network Configuration eth2  Unbridged  Default

Network Configuration vlan1  Unbridged  Default

Network Configuration ra0  Unbridged  Default

MTU

Multicast forwarding  Enable  Disable

Masquerade / NAT  Enable  Disable

IP Address ...

Subnet Mask ...

Network Configuration apcli0  Unbridged  Default

Network Configuration wds0  Unbridged  Default

Network Configuration wds1  Unbridged  Default

Network Configuration wds2  Unbridged  Default

Network Configuration wds3  Unbridged  Default

Table 3-12 Parameter description of port setup

Parameter	Description
MTU	Maximum transmission unit, 1500 bytes by default.
Multicast forwarding	Set whether to enable multicast forwarding.
Masquerade/NAT	Set whether to enable Masquerade/NAT.
IP Address	Set IP address of selected port. It cannot conflict with other ports or bridges.
Subnet Mask	Set subnet mask of the selected port.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.3.6.3 DHCPD

You can use multiple DHCP service.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Setup > Networking**.

**Step 3** In **DHCPD** section, click **Add**.

**Step 4** Configure DHCP.

- Select a port or a bridge in the first dropdown list.
- Set whether to enable DHCP in the second dropdown list.
- Start: Specify the start address.
- Max: Means the maximum assigned DHCP clients.
- Leasetime: Indicates the lease time of the DHCP clients, expressed by minutes.

Figure 3-16 Add DHCP

The screenshot shows the DHCPD configuration page. At the top, there is a header 'DHCPD'. Below it, a section titled 'Multiple DHCP Server' contains a table with one entry. The entry is labeled 'DHCP 0' and has the following configuration: 'eth2' (selected in a dropdown), 'On' (selected in a dropdown), 'Start' (100), 'Max' (50), and 'Leasetime' (3600). Below the table, there are 'Delete' and 'Add' buttons.

**Step 5** Click **Save** to save the configuration.



You can add another DHCP after saving the current one. You cannot configure multiple DHCP servers at the same time.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.4 Wireless

### 3.4.1 Basic Settings

#### 3.4.1.1 Physical Interface

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Wireless > Basic Settings**.

**Step 3** Enable **Wireless Network**, and configure wireless parameters.

Figure 3-17 Configure wireless physical interface

**Wireless Physical Interface w10 [2.4 GHz]**

Wireless Network  Enable  Disable

**Physical Interface ra0 - SSID [Dahua Wireless] HWAddr [XXXXXXXXXX]**

Wireless Mode

Wireless Network Mode

802.11n Transmission Mode

Wireless Network Name (SSID)

Wireless Channel

Channel Width

Wireless SSID Broadcast  Enable  Disable

Network Configuration  Unbridged  Bridged

Table 3-13 Parameter description of physical interface

Parameter	Description
Wireless Mode	The following wireless modes are available: AP, Client, Repeater, Repeater Bridge.
Wireless Network Mode	The following wireless network modes are available: <ul style="list-style-type: none"> <li>● Disabled: Disable wireless network.</li> <li>● Mixed: Supports 802.11b, 802.11g, and 802.11n wireless devices.</li> <li>● BG-Mixed: Supports 802.11b and 802.11g wireless devices.</li> <li>● B-Only: Only supports the 802.11b standard wireless devices.</li> <li>● G-Only: Only supports the 802.11g standard wireless devices.</li> <li>● NG-Mixed: Supports 802.11g and 802.11n wireless devices.</li> <li>● N-Only: Only supports the 802.11n standard wireless devices.</li> </ul>
802.11n Transmission Mode	This parameter is valid only when the Wireless Network Mode is selected under N-Only. <ul style="list-style-type: none"> <li>● Greenfield: When there are no other 802.11a/b/g devices use the same channel, using this mode can increase throughput. If other 802.11a/b/g devices use the same channel, the transmission information may generate errors and retransmission.</li> <li>● Mixed: This mode is contrary to the green mode, but it will reduce the throughput.</li> </ul>
Wireless Network Name (SSID)	The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.
Wireless Channel	13 channels are available. In multiple wireless device environments, try to avoid using the same channel as other devices.
Channel Width	The following options are available: Auto, 20MHZ and 40MHZ.
Wireless SSID Broadcast	<ul style="list-style-type: none"> <li>● Enable: Broadcast SSID.</li> <li>● Disable: Hidden SSID.</li> </ul>



Parameter	Description
Network Configuration	<ul style="list-style-type: none"> <li>• Bridged: Bridge to the Router, normally select this option.</li> <li>• Unbridged: No bridge to the Router, you need to manually configure IP address and subnet mask.</li> </ul>

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

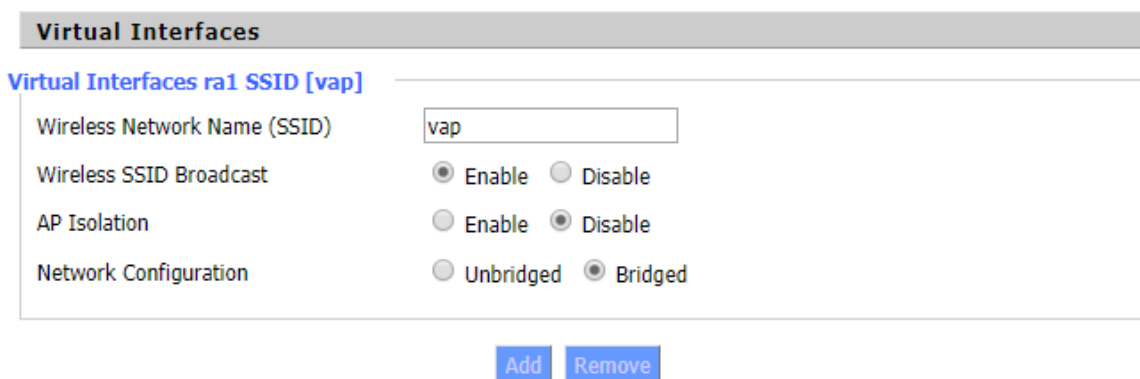
### 3.4.1.2 Virtual Interfaces

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Wireless > Basic Settings**.

Step 3 In **Virtual Interfaces** section, click **Add**.

Figure 3-18 Add virtual interface



Step 4 Set parameters. For details, see Table 3-13.

**AP Isolation:** Isolate all wireless client devices so that they can only access fixed network connected by AP.

Step 5 (Optional) Click **Remove** to delete the virtual interface.

Step 6 Click **Save** to save the configuration.

Step 7 Click **Apply Settings** to apply the configuration.

### 3.4.2 Wireless Security

You can configure the security of your wireless network. There are 7 wireless security modes are available. And the security mode is disabled by default.

To configure the security of the physical interface and the created virtual interfaces:

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Wireless > Wireless Security**.

Step 3 In **Physical Interface** and **Virtual Interfaces** section, select a security mode, and then configure security parameters.

Figure 3-19 WPA2 Personal

**Physical Interface ra0 SSID [Dahua Wireless] HWAddr [redacted]**

Security Mode:

WPA Algorithms:

WPA Shared Key:   Unmask

Key Renewal Interval (in seconds):  (Default: 3600, Range: 1 - 99999)

---


**Virtual Interfaces ra1 SSID [vap]**

Security Mode:



- Security modes vary according to the **Wireless Network Modes** set in **Wireless > Basic Settings**.
- WPA algorithms vary according to different security modes.

Table 3-14 Parameter description of security mode

Parameter	Description
<b>WEP</b>	
Authentication Type	Select <b>Open</b> or <b>Shared Key</b> .
Default Transmit Key	Select the key for transmission encryption form Key 1 to Key 4.
Encryption	<ul style="list-style-type: none"> <li>• 64 bit 10 hex digits/5 ASCII: Each key consists of 10 hexadecimal characters or 5 ASCII characters.</li> <li>• 128 bit 26 hex digits/13 ASCII: Each key consists of 26 decimal characters or 13 ASCII characters.</li> </ul>
ASCII/HEX	<ul style="list-style-type: none"> <li>• ASCII: the key is 5-bit ASCII characters or 13-bit ASCII characters.</li> <li>• HEX: the key is 10-bit or 26-bit hexadecimal digits.</li> </ul>
Passphrase	Enter combination of letters and numbers to generate keys.
Key 1/Key 2/Key 3/Key 4	Automatically generated according to Passphrase or set manually.
<b>WPA Personal, WPA2 Personal, WPA2 Person Mixed</b>	
WPA Algorithms	AES/TKIP/TPIP+AES.  <ul style="list-style-type: none"> <li>• TKIP/AES/TKIP+AES adopt dynamic encryption key, in which TKIP+AES is applicable to TKIP or AES.</li> <li>• WPA Person Mixed allows WPA Personal and WPA2 Personal clients to mix.</li> </ul>
WPA Shared Key	8 to 63 charaters consisting of letters and numbers.
Key Renewal Interval (in seconds)	The range is 1–99999, and the default value is 3600.
<b>WPA Enterprise, WPA2 Enterprise, WPA2 Enterprise Mixed</b>	
WPA Algorithms	AES/TKIP/TPIP+AES.

Parameter	Description
Radius Auth Sever Address	The IP address of the RADIUS server that is connected to the Router.
Radius Auth Server Port	The RADIUS port (1812 by default).
Radius Auth Shared Secret	The shared key between the RADIUS server and the Router.
Key Renewal Interva(in seconds)	The range is 1–99999, and the default value is 3600.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

## 3.5 Services

### 3.5.1 DHCP Server

DHCP server assigns IP addresses to local devices. You can configure DHCP as needed.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, click **Services**.

**Step 3** In **DHCP Server** section, click **Add**.

Figure 3-20 Add service

**DHCP Server**

Additional DHCPd Options

Static Leases

MAC Address	Host Name	IP Address	Client Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> minutes

Add Remove

**Step 4** Set MAC address, host name, IP address and client lease time.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration. Click **Remove** to delete the selected service.

### 3.5.2 DNSMasq

DNSmasq is a local DNS server. It will resolve all host names known to the Router from DHCP (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers. Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, click **Services**.

**Step 3** In **DNSMasq** section, enable **DNSMasq**, and then set parameters.

Figure 3-21 DNSMasq

The screenshot shows the DNSMasq configuration interface. It includes three rows of radio button controls:
 

- DNSMasq**:  Enable  Disable
- Local DNS**:  Enable  Disable
- No DNS Rebind**:  Enable  Disable

 Below these controls is a text input field labeled "Additional DNSMasq Options".

Table 3-15 Description of DNSMasq parameters

Parameter	Description
Local DNS	Enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.
No DNS Rebind	When enabled, it can prevent an external attacker from accessing the Router's internal Web interface. It is a security measure.
Additional DNSMasq Options	You can set some extra options, such as static allocation and max lease number. For example: static allocation: dhcp-host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h max lease number: dhcp-lease-max=2 DHCP server IP range: dhcp-range=192.168.0.110,192.168.0.111,12h

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.5.3 SNMP

SNMP (Simple Network Management Protocol) is a widely used network management protocol. Data is transmitted by the SNMP agent. SNMP agent refers to the hardware or software process, which reports the activities of each network device (such as hubs, routers and bridges) to the workstation to monitor the network. The SNMP agent returns the information contained in the MIB (Management Information Base). A MIB is a data structure that defines the options that are available from the device and can be controlled (such as on or off).

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, click **Services**.

**Step 3** In **SNMP** section, enable **SNMP**, and set parameters.

Figure 3-22 Enable SNMP

SNMP

SNMP  Enable  Disable

Location

Contact

Name

RO Community

RW Community

Table 3-16 Description of SNMP parameters

Parameter	Description
Location	Set the location identification of the device.
Contact	The contact information and name of SNMP.
Name	
RO Community	SNMP RO community name, the default is public, Only with read permission.
RW Community	SNMP RW community name, the default is private, with read and write permissions.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.5.4 System Log

You can enable system log to capture system messages. By default the system log will be collected in the local file `/var/log/messages`.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, click **Services**.

**Step 3** In **SNMP** section, enable **Syslogd**, and then select **Syslog Out Mode**.

The following system output modes are available:

- Console: Outputs the log information to console port.
- Web: Outputs the log information to Web.



**Net** is not supported currently.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.5.5 Telnet

Telnet is a terminal emulation protocol that is commonly used on the Internet and TCP/IP-based networks. It allows end users or computers to log in to remote devices and run programs.

You can enable a telnet server to connect to the Router with telnet. The username is admin and the password is the Router's password.



If you use the Router in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSH and disable telnet.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, click **Services**.

Step 3 In **Telnet** section, enable or disable Telnet.

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.5.6 WAN Traffic Counter

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, click **Services**.

Step 3 In **WAN Traffic Counter** section, enable or disable traffic counter.

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.6 VPN

### 3.6.1 PPTP

#### 3.6.1.1 PPTP Server

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **VPN > PPTP**.

Step 3 In **PPTP Server** section, enable **PPTP Server**, and set parameters.

Figure 3-23 Enable PPTP server

**PPTP Server**

PPTP Server  Enable  Disable

Broadcast support  Enable  Disable

Force MPPE Encryption  Enable  Disable

DNS1

DNS2

WINS1


WINS2

Server IP

Client IP(s)

CHAP-Secrets

Table 3-17 Description of PPTP server parameters

Parameter	Description
Broadcast support	Set whether to enable broadcast or not.
Force MPPE Encryption	Set whether to mandatorily enable MPPE (Microsoft Point-to-Point Encryption) encryption of PPTP data.
DNS1	Set as needed.
DNS2	
WINS1	
WINS2	
Server IP	Enter IP address of the Router as PPTP server, which should be different from the LAN address.
Client IP(s)	Enter IP addresses that are assigned to the clients. The format is xxx.xxx.xxx.xxx-xxx.
CHAP-Secrets	User name and password of the client when using PPTP service.  <ul style="list-style-type: none"> <li>• Client IP must be different with IP assigned by Router DHCP.</li> <li>• The format of CHAP Secrets: "user * password *".</li> </ul>

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.6.1.2 PPTP Client

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > PPTP**.

**Step 3** In **PPTP Client** section, enable **PPTP Client**, and set parameters.

Figure 3-24 Enable PPTP client

**PPTP Client**

**PPTP Client**

PPTP Client Options  Enable  Disable

Server IP or DNS Name

Remote Subnet ...

Remote Subnet Mask ...

MPPE Encryption

MTU  (Default: 1450)

MRU  (Default: 1450)

NAT  Enable  Disable

Fixed IP  Enable  Disable

User Name

Password   Unmask

Table 3-18 Description of PPTP client parameters

Parameter	Description
Server IP or DNS Name	Enter IP address or DNS name of PPTP server.
Remote Subnet	Enter the internal network of the remote PPTP server.
Remote Subnet Mask	Enter subnet mask of the remote PPTP server.
MPPE Encryption	Set whether to enable MPPE encryption.
MTU	Maximum Transmission Unit. The range is 0–1500.
MRU	Maximum Receive Unit. The range is 0–1500.
NAT	Network Address Translation. Set whether to enable NAT.
Fixed IP	Set whether to enable fixed IP. It is disabled by default.
User Name	Enter user name to log in to PPTP server.
Password	Enter password to log in to PPTP server.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.



## 3.6.2 L2TP

### 3.6.2.1 L2TP Server

L2TP (Layer 2 Tunneling Protocol) is an industrial standard Internet tunneling protocol. It is similar to the PPTP protocol, and it can encrypt network data streams. The difference is that L2TP requires data-oriented and point-to-point connections, uses multiple tunnels and provides header compression, tunnel authentication.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > L2TP**.

**Step 3** In **L2TP Server** section, enable **L2TP Server**, and set parameters.

Figure 3-25 Enable L2TP server

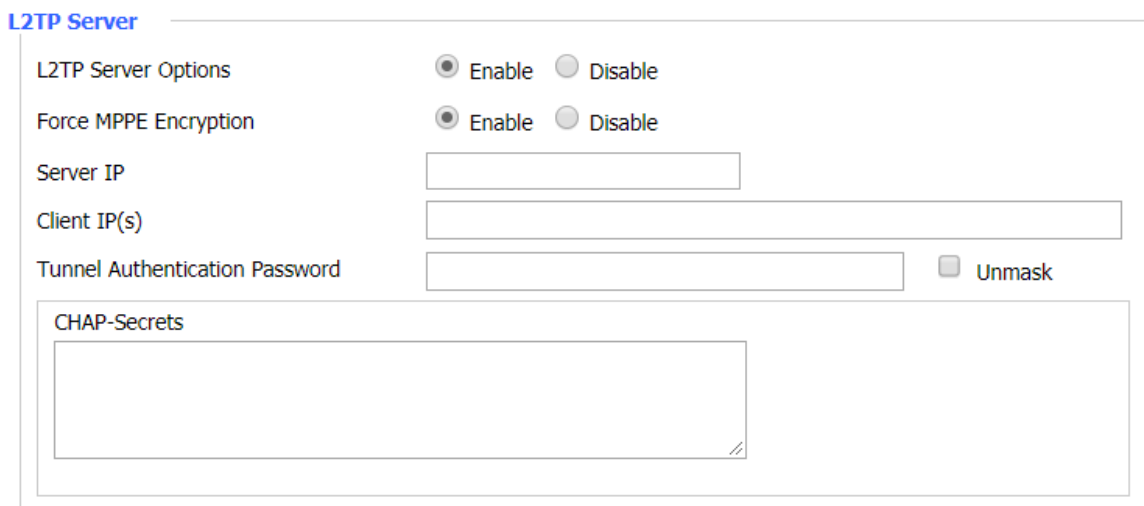



Table 3-19 Description of L2TP server parameters

Parameter	Description
Force MPPE Encryption	Set whether to mandatorily enable MPPE (Microsoft Point-to-Point Encryption) encryption of L2TP data.
Server IP	Enter IP address of the Router as L2TP server, which should be different from the LAN address.
Client IP(s)	Enter IP addresses that are assigned to the clients. The format is xxx.xxx.xxx.xxx-xxx.
Tunnel Authentication Password	Set as needed, not recommended.
CHAP-Secrets	User name and password of the client when using L2TP service.  <ul style="list-style-type: none"> <li>Client IP must be different with IP assigned by Router DHCP.</li> <li>The format of CHAP Secrets: "user * password *".</li> </ul>

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.6.2.2 L2TP Client

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > L2TP**.

**Step 3** In **L2TP Client** section, enable **L2TP Client**, and set parameters.

Figure 3-26 Enable L2TP client

**L2TP Client**

**L2TP Client**

L2TP Client Options  Enable  Disable

Tunnel name

User Name

Password   Unmask

Tunnel Authentication Password   Unmask

Gateway (L2TP Server)

Remote Subnet

Remote Subnet Mask

MPPE Encryption

MTU  (Default: 1450)

MRU  (Default: 1450)

NAT  Enable  Disable

Fixed IP  Enable  Disable

Require CHAP  Yes  No

Refuse PAP  Yes  No

Require Authentication  Yes  No

Table 3-20 Description of L2TP client parameters

Parameter	Description
Tunnel name	Set tunnel name.
User Name	Enter user name to log in to L2TP server.
Password	Enter password to log in to L2TP server.
Tunnel Authentication Password	Set tunnel authentication password as needed, not recommended.
Gateway (L2TP Server)	Enter IP address or DNS name of L2TP server.
Remote Subnet	Enter the internal network of the remote L2TP server.
Remote Subnet Mask	Enter the internal subnet mask of the remote L2TP server.
MPPE Encryption	Set whether to enable MPPE encryption.
MTU	Maximum Transmission Unit. The range is 0–1500.
MRU	Maximum Receive Unit. The range is 0–1500.

Parameter	Description
NAT	Network Address Translation. Set whether to enable NAT.
Fixed IP	Set whether to enable fixed IP. It is disabled by default.
Require CHAP	Set whether to support CHAP.
Refuse PAP	Set whether to support PAP.
Require Authentication	Set whether to support authentication.

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.6.3 OPENVPN

### 3.6.3.1 OPENVPN Server

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **VPN > OPENVPN**.

Step 3 In **OpenVPN Server/Daemon** section, enable **Start OpenVPN Server**, and set parameters.

Figure 3-27 Enable OPENVPN server

**OpenVPN Server/Daemon**

**OpenVPN Server/Daemon**

[Start OpenVPN Server](#)

Enable     Disable

Start Type                       WAN Up     System

Config via                         Server     Daemon

CA Cert

Public Server Cert

Private Server Key

DH PEM

Additional Config

TLS Auth Key

Certificate Revoke List

Table 3-21 Description of OPENVPN server parameters

Parameter	Description
Start Type	<ul style="list-style-type: none"> <li>● WAN Up: Start after online.</li> <li>● System: Start when bootup.</li> </ul>
Config via	Support the following configuration modes: Server or Daemon.
CA Cert	Enter the public CA certification of server and client.
Public Server Cert	Enter public server certification.
Private Server Key	Set private server key.
DH PEM	Enter DH PEM.
Additional Config	Enter additional configuration.
TLS Auth Key	Enter authentication key of TLS.
Certificate Revoke List	Enter certification list that you want to revoke.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.6.3.2 OpenVPN Client

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > OPENVPN**.

**Step 3** In **OpenVPN Client** section, enable **Start OpenVPN Client**, and set parameters.

Figure 3-28 Enable OpenVPN client

**OpenVPN Client**

**OpenVPN Client**

Start OpenVPN Client  Enable  Disable

Server IP/Name

Port  (Default: 1194)

Tunnel Device

Tunnel Protocol

Encryption Cipher

Hash Algorithm

User Pass Authentication  Enable  Disable

Advanced Options  Enable  Disable

CA Cert

Public Client Cert

Private Client Key

Table 3-22 Description of OPENVPN client parameters

Parameter	Description
Server IP/Name	Enter the IP address or DNS name of the OPENVPN server.
Port	Enter the listening port of the OPENVPN server.
Tunnel Device	<ul style="list-style-type: none"> <li>● TUN: Router mode.</li> <li>● TAP: Bridge mode.</li> </ul>
Tunnel Protocol	Supports UDP and TCP.
Encryption Cipher	The following encryption cipher modes are available: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC and None.
Hash Algorithm	Hash algorithm provides a fast way to access data, including SHA1, SHA256, SHA512, MD5, MD4 and None.
User Pass Authentication	Set whether to enable user authentication. If it is enabled, user name and password are required.
Advanced Options	Set whether to enable advanced options. For details, refer to Table 3-23.
CA Cert	Enter the public CA certification of the server and client.

Parameter	Description
Public Client Cert	Enter the public client certification.
Private Client Key	Enter the private client key.

Figure 3-29 Advanced options

Advanced Options  Enable  Disable

TLS Cipher

Use LZO Compression

NAT  Enable  Disable

Bridge TAP to br0  Enable  Disable

IP Address

Subnet Mask

TUN MTU Setting  (Default: 1500)

Tunnel UDP Fragment  (Default: Disable)

MSS-Fix/Fragment across the tunnel  Enable  Disable

nsCertType verification

TLS Auth Key

Additional Config

Policy based Routing

PKCS12 Key

Static Key

Table 3-23 Description of advanced options

Parameter	Description
TLS Cipher	Select TLS encryption standard. None by default.
Use LZO Compression	Set whether to enable LZO compression during data transmission.
NAT	Network Address Translation. Set whether to enable NAT.
Bridge TAP to br0	Set whether to bridge TAP to br0.
IP Address	Enter IP address of the local OPENVPN client.
Subnet Mask	Enter subnet mask of the local OPENVPN client.
TUN MTU Setting	Set the MTU for the tunnel.
Tunnel UDP Fragment	Set UDP fragment for the tunnel.
TCP MSS	Set the maximum segment size of TCP data.
nsCertType verification	Set whether to support ns certification type.
TLS Auth Key	Set authentication key of TLS.
Additional Config	Set additional configuration of the OPENVPN server.

Parameter	Description
Policy based Routing	Customize the routing policy.
PKCS12 Key	Private key format, set as needed.
Static Key	Set as needed.

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.6.4 IPSEC

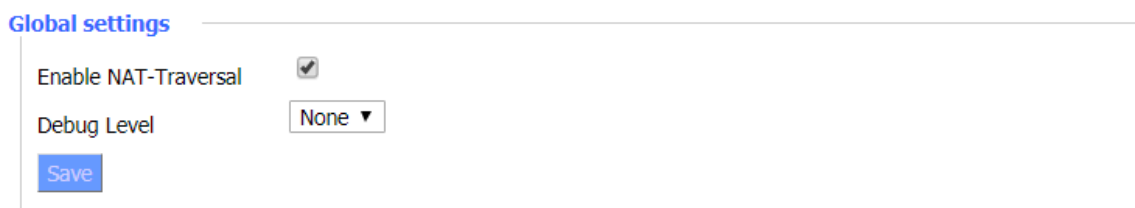
### 3.6.4.1 Global Settings

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **VPN > IPSEC**.

Step 3 In **Global settings** section, select **Enable NAT-Traversal** and **Debug Level**.

Figure 3-30 Global settings



Step 4 Click **Save** to save the configuration.

### 3.6.4.2 Connection Status and Control

You can view IPSEC connection and status of the Router on IPSEC page.

Step 1 Log in to the web interface of the Router.

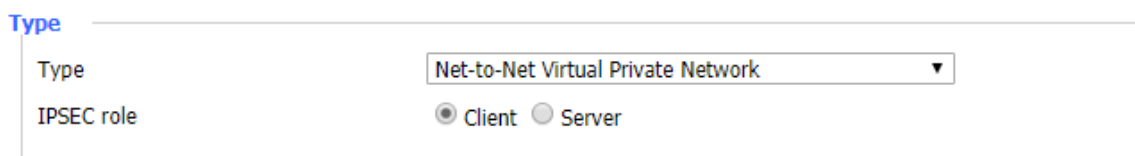
Step 2 In the left navigation menu, select **VPN > IPSEC**.

Step 3 In **Connection status and control** section, click **Add**.

Step 4 Configure IPSEC type.

- Type: Supports Net-to-Net Virtual Private Network and Host-to-Host Virtual Private Network (RoadWarrior).
- IPSEC role: Supports Client and Server.

Figure 3-31 Connection type



Step 5 Configure basic address information of the tunnel.

Figure 3-32 Connection type

**Connection**

Name	<input type="text"/>	Enabled	<input checked="" type="checkbox"/>
Local WAN Interface	WAN ▼	Peer WAN address	<input type="text"/>
Local Id	<input type="text"/>	Peer ID	<input type="text"/>

- Name: Indicates the connection name, must be unique.
- Enabled: If enabled, the connection will send tunnel connection request when it is reboot or re-connection.
- Local WAN Interface: Local address of the tunnel.
- Peer WAN address: Peer IP or domain name. If the server function of tunnel mode is used, leave this option blank.
- Local ID: The local identification of the channel, which can be IP or domain name.
- Peer ID: Peer identification of the channel, which can be IP and domain name.

**Step 6** Configure DPD detection.

- 1) Enable DPD detection.
- 2) Set time interval, timeout and action.

**Step 7** Enable advanced settings, including IKE and ESP.



After the advanced settings are enabled, you can configure parameters of Phase 1 and Phase 2, otherwise, it will be automatically negotiated with the peer.

Table 3-24 Parameter description of advanced settings

Parameter	Description
<b>Phase 1</b>	
IKE Encryption	The following IKE encryption modes are available: AES (256 bit), AES (192 bit), AES (128 bit), 3DES and DES.
IKE Integrity	The following IKE integrity solutions are available: MD5, SHA1, SHA2 (256) and SHA2 (512).
IKE Grouptype	DH exchange algorithm.
IKE Lifetime	Set IKE lifetime, expressed by hour, and the default value is 0.
<b>Phase 2</b>	
ESP Encryption	The following ESP encryption modes are available: SHA2 (512), SHA2 (256), SHA1, MD5 and MD5-96.
ESP Integrity	The following ESP integrity solutions are available: MD5, SHA1, SHA2 (256) and SHA2 (512).
ESP Grouptype	Select ESP Grouptype.
ESP Keylife	Set ESP keylife, expressed by hour, and the default value is 0.
IKE aggressive mode allowed	Select to adopt aggressive mode, otherwise, adopt main mode.
Perfect Forward Secrecy (PFS)	Set whether to enable PFS.

**Step 8** Select an authentication method. Use a pre-shared key or generate and use the X.509 certificate. Currently only a pre-shared key is supported.



**Step 9** Click **Apply Settings** to save the configuration.

Figure 3-33 Connection Status

Connection status and control

Num	Name	Type	Common Name	status	Action
1	conn	Transport		CLOSED	<input checked="" type="checkbox"/>

[Add](#)

Table 3-25 Parameter description of connection status

Parameter	Description
Num	Connection number.
Name	The name of the IPSEC connection.
Type	Types and functions of the current IPSEC connection.
Common Name	Displays addresses and subnets of the local and peer.
Status	The state of the connection, including: <ul style="list-style-type: none"> <li>● Closed: The connection did not initiate a connection request to the peer.</li> <li>● Negotiating: The connection has initiated a request to the peer and is still in the negotiation process, but the connection has not been established.</li> <li>● Establish: The connection has been established and the channel can be used.</li> </ul>
Action	You can perform operations on the connection, including: <ul style="list-style-type: none"> <li>● : Delete the connection. If the IPSEC channel is established, it will also be removed.</li> <li>● : Edit the connection. After the modification, you need to reload the connection to make the configuration take effect.</li> <li>● : Reconnect. This operation will remove the current channel and request a channel establishment.</li> <li>● <input checked="" type="checkbox"/>: Enabled: When the connection is enabled, the system will initiate a channel establishment request when the system restarts or reconnects; otherwise, the connection will not initiate a request.</li> </ul>

### 3.6.4.3 Certificate Management

You can add, view, download and delete certificates.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > IPSEC**.

**Step 3** In **Certificate Management** section, click **Add**.

**Step 4** Select a certificate adding method.

- Import a certificate

- 1) Select **Import A Cert** in **ADD Method**.

Figure 3-34 Import a certificate

**ADD Method**

ADD Method

Include Private Key

---

**Info Incorporated**

**Import CA**

Name Of CA

Public CA Cert

- 2) Set whether to include private key.
  - 3) Enter the name of the imported certificate and public CA certificate.
    - Generate a certificate
- 1) Select **Generate A Cert** in **ADD Method**.

Figure 3-35 Generate a certificate

**ADD Method**

ADD Method

Signed Method  Signed Self  Signed By Another

---

**Info Incorporated**

**RDNs**

Name Of CA

length of private Key

Country Name(2 letter code)[AU]

State or Province Name(full name)

Locality Name(eg,city)

Organization Name(eg,company)

Organizational Unit Name(eg,section)

Common Name(eg,YOUR name)

Email Address

Effective number of days

- 2) Select a **Signed Method**.
- 3) Configure parameters as needed for generating a certificate.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

Figure 3-36 Certificate management

Certificate Management			
Name	Ref Count	Action	
catest	0		
<a href="#">Add</a>			

- Click to delete the certificate.
- Click to view the certificate details.
- Click to download the certificate.

### 3.6.5 GRE

The GRE (Generic Routing Encapsulation) protocol encapsulates data packets of certain network layer protocols (such as IP and IPX) so that these encapsulated data packets can be transmitted in another network layer protocol (such as IP).

GRE uses tunnel technology, which is a Layer 3 tunneling protocol for VPN (Virtual Private Network).

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **VPN > GRE**.

**Step 3** In **GRE Tunnel** section, enable GRE tunnel, and then set parameters.

Figure 3-37 Enable GRE tunnel

GRE Tunnel	
GRE Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Number	1 () <a href="#">Delete</a>
Status	Disable ▾
Name	<input type="text"/>
Through	WAN(Static IP) ▾
Peer Wan IP Addr	<input type="text"/>
Peer Subnet	<input type="text"/> (eg:192.168.1.0/24)
Peer Tunnel IP	<input type="text"/>
Local Tunnel IP	<input type="text"/>
Local Netmask	<input type="text"/>
Keepalive	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Retry times	<input type="text"/>
Interval	60
Fail Action	Hold ▾
<a href="#">View GRE Tunnels</a>	

Table 3-26 Description of GRE tunnel parameters

Parameter	Description
Number	Selectable tunnels. Up to 12 GRE tunnels can be set.
Status	Select Enable to enable the current GRE tunnel; select Disable to disable the current GRE tunnel.
Name	GRE tunnel name, the length can up to 30 characters.
Through	The GRE transceiver interface: PPP, LAN and WAN (Static IP).
Peer Wan IP Addr	Enter the WAN IP address of the peer GRE.
Peer Subnet	Enter the subnet IP address of the peer GRE. For example, 192.168.1.0/24.
Peer Tunnel IP	Enter the IP address of the peer GRE tunnel.
Local Tunnel IP	Enter the IP address of the local GRE tunnel.
Local Netmask	Enter the local subnet mask.
Keepalive	Enable or disable GRE keepalive.
Retry times	Set the retry times of GRE keepalive.
Interval	Set the sending interval of GRE keepalive packet.
Fail Action	Select the keepalive failure action.

Step 4 (Optional) Click **View GRE Tunnels** to view the tunnel details.

Step 5 Click **Save** to save the configuration.

Step 6 Click **Apply Settings** to apply the configuration.

Step 7 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.7 Security

### 3.7.1 Firewall

You can enhance network security by filtering specific Internet data types and blocking anonymous Internet requests.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Security > Firewall**.

Step 3 In **Security** section, enable **SPI Firewall**.



- Firewall enhances network security and checks the packets entering the network by using SPI. To use firewall protection, select **Enable**, otherwise select **Disable**.
- Additional Filters, Block WAN Requests and Impede WAN DoS/Bruteforce are valid only when SPI firewall is enabled.

Figure 3-38 Security

**Security**

**Firewall Protection**

SPI Firewall  Enable  Disable

**Additional Filters**

Filter Proxy

Filter Cookies

Filter Java Applets

Filter ActiveX

**Block WAN Requests**

Block Anonymous WAN Requests (ping)

Filter IDENT (Port 113)

Block WAN SNMP access

**Impede WAN DoS/Bruteforce**

Limit SSH Access

Limit Telnet Access

Limit PPTP Server Access

Limit L2TP Server Access

**Step 4** Configure **Additional Filters**.

- Filter Proxy: Using WAN proxy server may reduce the security of the gateway. Select the checkbox to deny any access to any WAN proxy server or deselect to disable the function.
- Filter Cookies: Cookies are data stored on your computer by Web sites. They are used when you interact with Internet sites. Select the checkbox to enable cookies filtering or deselect to disable the function.
- Filter Java Applets: If you reject Java, you may not be able to open web pages programmed with Java tools. Select this check box to enable Java applet filtering or deselect to disable this function.
- Filter ActiveX: If you reject ActiveX, you may not be able to open web pages programmed with ActiveX tools. Select the check box to enable ActiveX filtering or deselect to disable the function.

**Step 5** Configure Block WAN Requests.

- Block Anonymous WAN Requests (ping): Enabled to prevent your network from being pinged or probed by other Internet users, which makes it more difficult for external users to penetrate your network.
- Filter IDENT (Port 113): Enabled to prevent port 113 from being scanned by devices outside your local network.
- Block WAN SNMP access: Enabled to block SNMP connection requests from the WAN.

**Step 6** Configure Impede WAN DoS/Bruteforce.

- Limit SSH Access: This function limits SSH access requests from the WAN. For the same IP, up to 2 SSH connection requests are accepted per minute.
- Limit Telnet Access: This function restricts Telnet access requests from the WAN. For the same IP, up to 2 Telnet connection requests are accepted per minute.
- Limit PPTP Server Access: When a PPTP server is created for the device, this function limits PPTP access requests from the WAN. For the same IP, up to 2 PPTP connection requests are accepted per minute.
- Limit L2TP Server Access: When a L2TP server is created for the device, this function limits L2TP access requests from the WAN. For the same IP, up to 2 L2TP connection requests are accepted per minute.

**Step 7** Click **Save** to save the configuration.

**Step 8** Click **Apply Settings** to apply the configuration.

**Step 9** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.7.2 Log Management

The Router can keep logs of all incoming or outgoing traffic for your Internet connection.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Security > Firewall**.

**Step 3** In **Log Management** section, enable **Log**, and set parameters.

- Log: To keep activity logs, select **Enable**. To stop logging, select **Disable**.
- Log Level: The higher the log level, the more the logs.
- Options: When select **Enable**, the corresponding connection will be recorded in logs; otherwise logs will not be recorded.

Figure 3-39 Enable log

**Log Management**

**Log**

Log  Enable  Disable

Log Level Low ▼

**Options**

Dropped Disable ▼

Rejected Disable ▼

Accepted Disable ▼

Incoming Log Outgoing Log

**Step 4** (Optional) Click **Incoming Log** to view the latest temporary incoming logs of the Router.

**Step 5** (Optional) Click **Outgoing Log** to view the latest temporary outgoing logs of the Router.

**Step 6** Click **Save** to save the configuration.

**Step 7** Click **Apply Settings** to apply the configuration.

**Step 8** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.8 Access Restrictions

You can block or allow specific types of Internet applications, and set Internet access policies for specific PCs.

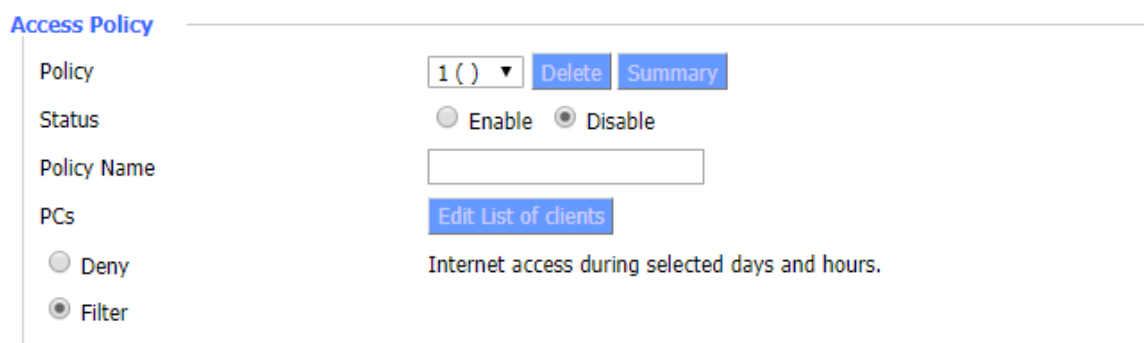
### 3.8.1 WAN Access

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Access Restrictions > WAN Access**.

**Step 3** Configure access policy.

Figure 3-40 Access policy



- Policy: Select a policy, you can customize up to 10 access policies.
  - ◇ Click **Delete** to delete the selected policy.
  - ◇ Click **Summary** to view the policy details.
- Status: Set whether to enable to the selected policy.
- Policy Name: Enter the policy name.
- PCs: Click **Edit List of clients** to add PC clients to the policy. You can add clients by MAC addresses, IP addresses and IP ranges.
- Deny: If you select **Deny**, the specific PCs will be denied to access any Internet service during specific time periods.
- Filter: If you select **Filter**, the specific PCs will be prevented from accessing the specific websites during specific time periods. You can set up 10 Internet access policies to filter Internet services accessed by the specific PCs during specific time periods.

**Step 4** Configure when the policy takes effect.

- 1) In **Days** section, select the date on which the policy will be applied.
- 2) In **Times** section, set the time when the policy will be applied.

**Step 5** Set the blocking websites by URL addresses.

You can block access to websites by entering the URL addresses.

**Step 6** Set the blocking websites by keywords.

You can block access to websites by the keywords contained in the web pages.

**Step 7** Click **Save** to save the configuration.

**Step 8** Click **Apply Settings** to apply the configuration.

**Step 9** (Optional) Click **Cancel Changes** to cancel the configuration.



The Router does not have a battery to keep the clock running. Turning off the Router power or rebooting the Router will cause the temporary failure of the Router clock. After the failure, if the NTP time server cannot be synchronized automatically, you need to recalibrate the time to ensure that the relevant functions controlled by time period perform correctly.

## 3.8.2 URL Filter

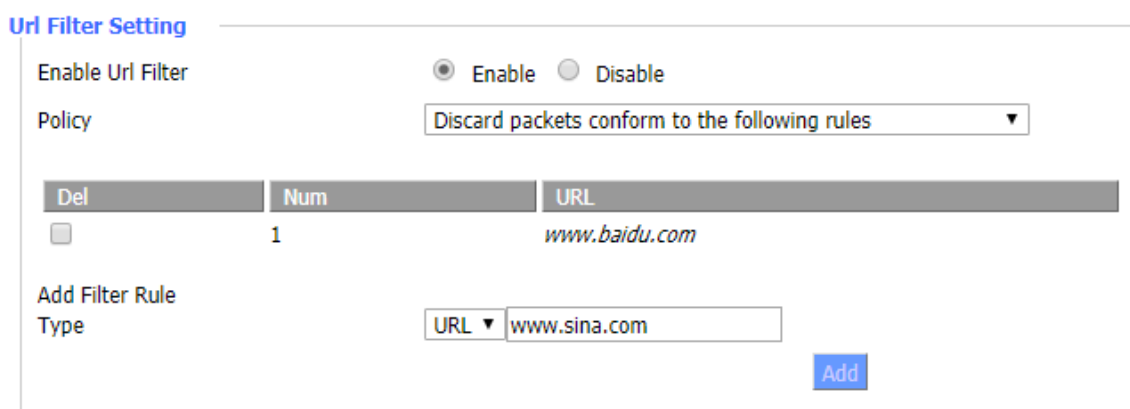
With URL filter, you can prevent certain clients from accessing to specific network domain name, such as www.sina.com.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Access Restrictions > URL Filter**.

**Step 3** Enable URL filter.

Figure 3-41 URL filter



**Url Filter Setting**

Enable Url Filter  Enable  Disable

Policy Discard packets conform to the following rules ▼

Del	Num	URL
<input type="checkbox"/>	1	www.baidu.com

Add Filter Rule

Type URL ▼  Add

**Step 4** Select a policy.

- **Discard packets conform to the following rules:** Only discard the matching URL addresses in the list.
- **Accept only the data packets conform to the following rules:** Only accept the matching URL addresses in the list, discard all other URL addresses.

**Step 5** Enter URL address in **Add Filter Rule** box, and then click **Add**.

**Step 6** Click **Save** to save the configuration.

**Step 7** Click **Apply Settings** to apply the configuration.

**Step 8** (Optional) Click **Cancel Changes** to cancel the configuration.

**Step 9** (Optional) Select the target URL in **Del** column, and then click **Save** to delete the selected URL.

## 3.8.3 MAC Filter

With MAC filter, your clients can be allowed or denied to only access to the specific MAC addresses.

**Step 1** Log in to the web interface of the Router.



**Step 2** In the left navigation menu, select **Access Restrictions > MAC Filter**.

**Step 3** Enable MAC filter.

Figure 3-42 MAC filter

**Mac Filter Setting**

Enable Mac Filter  Enable  Disable

Policy

Del	Num	MAC
- None -		

Add Filter Rule

MAC

**Step 4** Select a policy.

- **Discard packets conform to the following rules:** Only discard the matching MAC addresses in the list.
- **Accept only the data packets conform to the following rules:** Only accept the matching MAC addresses in the list.

**Step 5** Enter MAC address in **Add Filter Rule MAC** box, and then click **Add**.

**Step 6** Click **Save** to save the configuration.

**Step 7** Click **Apply Settings** to apply the configuration.

**Step 8** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.8.4 Packet Filter

With packet filter, you can prevent certain packets from entering to the Internet through the Router or prevent certain Internet packets from getting into the local network.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Access Restrictions > Packet Filter**.

**Step 3** Enable packet filter.

Figure 3-43 Packet filter

**Packet Filter Setting**

Enable Packet Filter  Enable  Disable

Policy

Del	Num	Source IP	SPorts	Destination IP	DPorts	Pro	Interface	Dir
Add Filter Rule								
Dir		<input type="text" value="INPUT"/>						
Pro		<input type="text" value="TCP/UDP"/>						
SPorts		<input type="text" value="1"/> - <input type="text" value="65535"/>						
DPorts		<input type="text" value="1"/> - <input type="text" value="65535"/>						
Source IP		<input type="text" value="IP Address"/> <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> / <input type="text" value="0"/>						
Destination IP		<input type="text" value="IP Address"/> <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> / <input type="text" value="0"/>						
<input type="button" value="Add"/>								

**Step 4** Select a policy.

- **Discard packets conform to the following rules:** Only discard the matching packets in the list.
- **Accept only the data packets conform to the following rules:** Only accept the matching packets in the list.

**Step 5** Configure filtering rules, and then click **Add**.

- Add Filter Rule Dir: Select a filtering rule direction.
  - ◇ INPUT: Packet from WAN to LAN.
  - ◇ OUTPUT: Packet from LAN to WAN.
- Pro: Select a protocol type of the packet.
- SPorts: Set source port of the packet.
- DPorts: Set destination port of the packet.
- Source IP: Set source IP address of the packet.
- Destination IP: Set destination IP address of the packet.



SPorts, DPorts, Source IP and Destination IP could not be all empty, you have to input at least one of these four parameters.

**Step 6** Click **Save** to save the configuration.

**Step 7** Click **Apply Settings** to apply the configuration.

**Step 8** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.9 NAT

### 3.9.1 Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions, such as video conferencing or online gaming. When users send this type of request to your network through the Internet, the Router will forward those requests to the appropriate PC. If you want to forward a whole range of ports, see 3.9.2 Port Range Forwarding.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **NAT > Port Forwarding**.

**Step 3** Click **Add**, and then set parameters.

Figure 3-44 Add port forwarding

Delete	Num	Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
<input type="checkbox"/>	1	<input type="text"/>	Both ▼	<input type="text"/>	0	0.0.0.0	0	<input type="checkbox"/>

Table 3-27 Description of port forwarding parameters

Parameter	Description
Application	Enter the name of the application.
Protocol	Select a protocol for the application: TCP,UDP or Both.
Source Net	Enter the IP address of the Internet user.
Port from	Enter the external port number used by the application.
IP Address	Enter the intranet IP address of the server accessed by Internet users.
Port to	Enter the internal port number used by the application.
Enable	Set whether to enable the application.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

**Step 7** (Optional) Select the target application in **Delete** column, and then click **Save** to delete the selected application.

### 3.9.2 Port Range Forwarding

Some applications may require a specific port range to be forwarded for normal operation. When a request is made for a certain port range from the Internet, the router will send this data

to the specified computer. For security reasons, you may want to restrict port forwarding to only those ports that are in use. If you no longer use the port forwarding, it is recommended to cancel selection in the **Enable** checkbox to temporarily disable the port forwarding.

If you only want to forward a single port, see "3.9.1 3.9.1Port Forwarding".

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **NAT > Port Range Forwarding**.

**Step 3** Click **Add**, and then set parameters.

Figure 3-45 Add port range forwarding

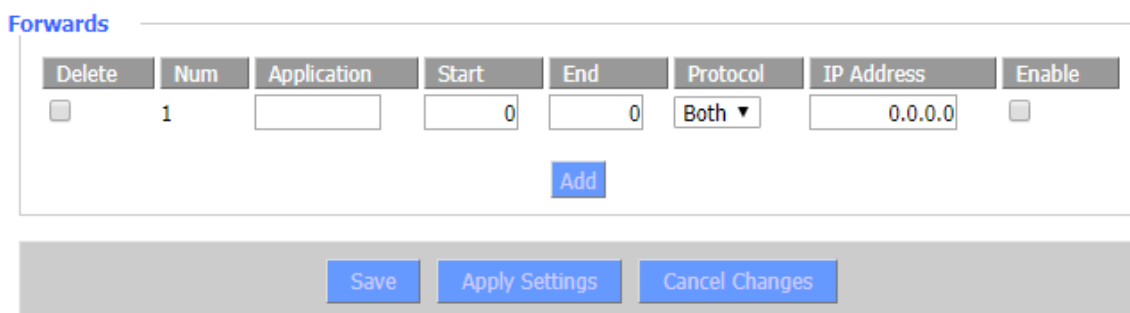


Table 3-28 Description of port range forwarding parameters

Parameter	Description
Application	Enter the name of the application.
Start	Enter the starting port number of the port forwarding range.
End	Enter the end port number of the port forwarding range.
Protocol	Select a protocol for the application: TCP,UDP or Both.
IP Address	Enter the intranet IP address of the server accessed by Internet users.
Enable	Set whether to enable the application.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

**Step 7** (Optional) Select the target application in **Delete** column, and then click **Save** to delete the selected application.

### 3.9.3 DMZ

The DMZ (Demilitarized Zone) function allows a network user to be exposed to the Internet for special services, such as Internet gaming or videoconferencing. The DMZ host forwards all ports to a computer at the same time.

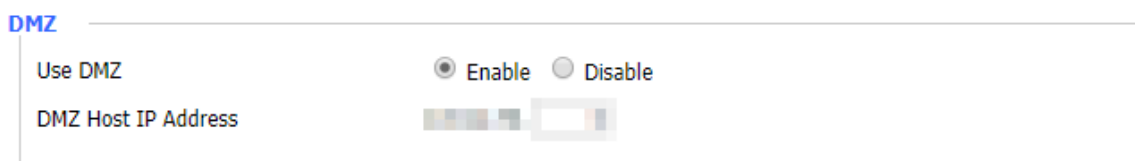
The Port Forwarding function is more secure because it only opens ports that you want to open, while the DMZ host opens all ports of a computer, and exposes the computer to the Internet.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **NAT > DMZ**.

**Step 3** In **Use DMZ**, select **Enable**.

Figure 3-46 DMZ



- Step 4 Enter the IP Address of DMZ Host.
- Step 5 Click **Save** to save the configuration.
- Step 6 Click **Apply Settings** to apply the configuration.
- Step 7 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.9.4 Virtual IP Mapping

- Step 1 Log in to the web interface of the Router.
- Step 2 In the left navigation menu, select **NAT > Virtual IP Mapping**.
- Step 3 Click **Add**.

Figure 3-47 Add virtual IP mapping



Delete	Num	Virtual IP	Real IP	Objective IP	Device	Enable
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>	<input type="text"/>	lo ▼	<input type="checkbox"/>

[Add](#)

- Step 4 Set virtual IP, real IP, objective IP and device.
- Step 5 Select **Enable** check box to enable the virtual IP mapping. Cancel selection to disable the virtual IP mapping.
- Step 6 Click **Save** to save the configuration.
- Step 7 Click **Apply Settings** to apply the configuration.
- Step 8 (Optional) Click **Cancel Changes** to cancel the configuration.
- Step 9 (Optional) Select the target application in **Delete** column, and then click **Save** to delete the selected application.

## 3.10 QoS Setting

### 3.10.1 Basic

QoS allows you to limit the traffic of upload and download separately, and assign priorities to specific IPs or MACs.

- Step 1 Log in to the web interface of the Router.
- Step 2 In the left navigation menu, select **QoS Setting > Basic**.

**Step 3** Configure QoS settings.

Figure 3-48 QoS settings

**QoS Settings**

Start QoS  Enable  Disable

Port

Packet Scheduler

Uplink (kbps)

Downlink (kbps)

- Start QoS: Set whether to enable QoS.
- Port: Select port.
- Packet Scheduler: Select packet scheduler.
- Uplink (kbps): Set bandwidth for upload. It is generally 80% to 90% of your maximum bandwidth.
- Downlink (kbps): Set bandwidth for download. It is generally 80% to 90% of your maximum bandwidth.

**Step 4** Set HTB uplink/downlink bandwidth according to HTB priorities.

Figure 3-49 HTB setting

**HTB Setting**

**HTB Prio Setting Uplink**

Priority	Band range	Band value
Premium	<input type="text" value="75"/> % - <input type="text" value="75"/> %	WAN : 0 -- 0 kbps
Express	<input type="text" value="15"/> % - <input type="text" value="15"/> %	WAN : 0 -- 0 kbps
Standard	<input type="text" value="10"/> % - <input type="text" value="10"/> %	WAN : 0 -- 0 kbps
Bulk	<input type="text" value="1"/> % - <input type="text" value="1"/> %	WAN : 0 -- 0 kbps

**HTB Prio Setting Downlink**

Priority	Band range	Band value
Premium	<input type="text" value="75"/> % - <input type="text" value="75"/> %	WAN : 0 -- 0 kbps
Express	<input type="text" value="15"/> % - <input type="text" value="15"/> %	WAN : 0 -- 0 kbps
Standard	<input type="text" value="10"/> % - <input type="text" value="10"/> %	WAN : 0 -- 0 kbps
Bulk	<input type="text" value="1"/> % - <input type="text" value="1"/> %	WAN : 0 -- 0 kbps

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.10.2 Classify

You can specify priority for all traffic of a given IP address or IP range, and you can also set the netmask and MAC priority.

- Step 1** Log in to the web interface of the Router.
- Step 2** In the left navigation menu, select **QoS Setting > Classify**.
- Step 3** Add netmasks and set netmask priorities.
- Step 4** Add MACs and set MAC priorities.

Figure 3-50 Classify

**Setting of Classify Based on HTB**

**Netmask Priority**

Delete	Net	Protocol	src Port Range	dst Port Range	Priority
<input type="checkbox"/>	[blurred]	<i>both</i>	<i>1-- 65535</i>	<i>1-- 65535</i>	Standard ▾
<input type="button" value="Add"/>	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> / <input type="text" value="0"/>	<input type="button" value="TCP/UDP"/> ▾	<input type="text" value="1"/> -- <input type="text" value="65535"/>	<input type="text" value="1"/> -- <input type="text" value="65535"/>	

**MAC Priority**

Delete	Num	MAC Address	Priority
<input type="checkbox"/>	1	[blurred]	Standard ▾
<input type="button" value="Add"/>		<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/>	

- **Exempt**

This priority is independent of the other four priorities. The data flow is unrestricted, and the bandwidth is limited only by the hardware.

The relationship between Exempt and the other four priorities is as follows:

Suppose the total upload bandwidth is Max\_Up, the total download bandwidth is Max\_Down, the upload limit is Uplink, the download limit is Downlink, and the unrestricted data flow rate is Exempt\_Rate\_Up and Exempt\_Rate\_Do.

  - ◇ The total upload bandwidth of other priorities is  $\min(\text{Max\_Up} - \text{Exempt\_Rate\_Up}, \text{Uplink})$ .
  - ◇ The total download bandwidth of other priorities is  $\min(\text{Max\_Downlink} - \text{Exempt\_Rate\_Do}, \text{Downlink})$ .
- **Other four priorities**

After the unrestricted data stream is sent, the remaining bandwidth is allocated by the remaining data streams with four priorities according to a certain ratio. Assume that the remaining upload and download bandwidth are 1000 kbps respectively. There are four data streams with different priorities, and the upload and download bandwidth of each data stream is as follows:

  - ◇ Premium:  $(75/100) * \text{Uplink}$ ;  $(75/100) * \text{Downlink}$ .
  - ◇ Express:  $(15/100) * \text{Uplink}$ ;  $(15/100) * \text{Downlink}$ .
  - ◇ Standard:  $(10/100) * \text{Uplink}$ ;  $(10/100) * \text{Downlink}$ .
  - ◇ Bulk: 1000 bit (almost 0); 1000 bit (almost 0).



- For Bulk priority, the upload and download rates are both 1000 bit. The data streams with Bulk priority starts to be sent after the data streams with other priorities are sent.
- When there is only one level of data stream, the bandwidth of the data stream is limited only by the upload and download restrictions in QoS Settings.
- When a connection meets the control conditions in both MAC priority and netmask priority, the rule added first shall prevail.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

**Step 7** (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.11 Serial Applications

The console port of the Router is usually used as a console, but you can configure it to an ordinary serial port by the built-in serial port to TCP/IP application of the Router. After configuration, the console port of the Router can be used as a serial protocol conversion device, or it can be equivalent to a DTU device.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Applications > Serial Applications**.

**Step 3** In **Serial Applications**, select **Enable**, and then set parameters.

Figure 3-51 Enable serial applications

**Serial Applications**

Serial Applications  Enable  Disable

Baudrate

Databit

Stopbit

Parity

Flow Control

Protocol

Server Address

Server Port

Device Number

Device Id   escape data

Heartbeat Interval



Table 3-29 Description of serial application parameters

Parameter	Description
Baudrate	Indicates the number of bytes per second transmitted by the Router, commonly used baud rate is 115200, 57600, 38400, 19200.
Databit	The number of data bit can be 4, 5, 6, 7, 8, and usually in ASCII code. The transmission starts from the lowest bit and is located by the clock.
Stopbit	Indicates the end of a character data. It can be a high level of 1-bit, 1.5-bit and 2-bit.
Parity	Indicates the data error checking method used by a set of data: Odd or Even.
Flow Control	Includes hardware and software.
Protocol	<p>The following protocols are available:</p> <ul style="list-style-type: none"> <li>• UDP (DTU): Serial port to UDP connection, including custom application layer protocol, which is equivalent to the function of a IP modem</li> <li>• Pure UDP: Standard serial port to UDP connection.</li> <li>• TCP (DTU): Serial port to TCP connection, including custom application layer protocol, which is equivalent to the function of an IP modem.</li> <li>• Pure TCP: Standard serial port to TCP connection.</li> <li>• TCP server: Standard TCP server connection.</li> <li>• TCST: Custom TCP connection.</li> <li>• Modbus TCP: Modbus protocol based on Ethernet TCP/IP.</li> <li>• DCUDP: UDP connection in CUDP mode.</li> <li>• DCTCP: TCP connection in CTCP mode.</li> </ul>
Server Address	The IP address or domain name of the data service center.
Server Port	The listening port of the data service center.
Listen Port	This parameter is valid only when <b>Protocol</b> is <b>TCP Server</b> or <b>Modbus TCP</b> .
Device Number	<p>This parameter is valid only when <b>Protocol</b> is among <b>UDP(DTU)</b>, <b>TCP(DTU)</b>, <b>DCUDP</b> and <b>DCTCP</b>.</p> <p>The ID of the Router, an 11-byte data string.</p>
Device ID	<p>This parameter is valid only when <b>Protocol</b> is <b>TCP(DTU)</b> or <b>DCTCP</b>.</p> <p>It is an 8-byte data string.</p>
Heartbeat Interval	<p>This parameter is valid only when <b>Protocol</b> is among <b>UDP(DTU)</b>, <b>TCP(DTU)</b>, <b>TCST</b>, <b>DCUDP</b> and <b>DCTCP</b>.</p> <p>The time interval to send heart beat packet.</p>
Custom Heartbeat Packet	<p>This parameter is valid when <b>Protocol</b> is <b>TCST</b>.</p> <p>Set the heartbeat packet.</p>
Custom Registration Packet	<p>This parameter is valid when <b>Protocol</b> is <b>TCST</b>.</p> <p>Set the registration packet.</p>
ASCII/HEX	<p>This parameter is valid when <b>Protocol</b> is <b>TCST</b>.</p> <p>Set whether to enable ASCII/HEX.</p>

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.12 Administration

The network administrator can manage specific router functions to ensure access and security.

### 3.12.1 Router Management

#### 3.12.1.1 Router Password

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Management**.

Step 3 In **Router Password** section, set username and password.

The user name is admin by default.



- The new password must not exceed 32 characters and must not contain any blank spaces.
- We strongly recommend that you change the default password and update it regularly for security.

Figure 3-52 Router password

**Router Password**

Router Username	<input type="password" value="....."/>	
Router Password	<input type="password" value="....."/>	Please update password regularly
Re-enter to confirm	<input type="password" value="....."/>	

Step 4 Click **Save** to save the configuration.

Step 5 Click **Apply Settings** to apply the configuration.

Step 6 (Optional) Click **Cancel Changes** to cancel the configuration.

#### 3.12.1.2 Adding User

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Management**.

Step 3 In **Client Password** section, set name and password for the new user.

Figure 3-53 Add user

**Client Password**

Client Username	<input type="password"/>	
Client Password	<input type="password"/>	Please update password regularly
Client Password	<input type="password"/>	

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.3 Web Access

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Web Access** section, set parameters.

- Auto-Refresh (in seconds): Set the refresh interval of the web interface. "0" means to disable the auto-refresh.
- Enable Info Site: Set whether to display the system information webpage before login.
- Info Site Password Protection: Set whether to enable password protection for system information webpage.

Figure 3-54 Web access

**Web Access**

Auto-Refresh (in seconds)	<input type="text" value="3"/>
Enable Info Site	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Info Site Password Protection	<input type="checkbox"/> Enabled

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.4 Remote Access

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Remote Access** section, set parameters.

- Web GUI Management: Set whether to enable remote management of the Router.
- Use HTTPS: Set whether to use HTTPS. If HTTPS is used, you need to specify the URL as https://xxx.xxx.xxx.xxx (not all firmwares support SSL reconstruction).
- Telnet Management: Set whether to enable telnet management.
- Telnet Remote Port: Set telnet remote port. The range is 1–65535, and the default value is 23.

Figure 3-55 Remote access

**Remote Access**

Web GUI Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use HTTPS	<input checked="" type="checkbox"/>
Telnet Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Telnet Remote Port	<input type="text" value="23"/> (Default: 23, Range: 1 - 65535)

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.5 Cron

The Cron subsystem schedules execution of Linux commands. You will need to use the command line or startup scripts to use this function.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Cron** section, enable Cron and add additional Cron jobs.

Figure 3-56 Cron

**Cron**

Cron	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Additional Cron Jobs	<input type="text"/>

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.6 Language Selection

You can set the language of the web interface of the Router.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Language Selection** section, select a language.

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.7 Remote Management

You can monitor, manage and configure the Router remotely through the custom remote management server.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Remote Management** section, enable remote management, and then set parameters as needed.

Figure 3-57 Remote management

**Remote Management**

Remote Management  Enable  Disable

Protocol  V1.0  V2.0

Remote Login Server IP

Remote Login Server Port  (Default: 44008, Range: 1 - 65535)

Remote Server IP

Remote Server Listen Port  (Default: 40001, Range: 1 - 65535)

Heart Interval  (Default: 60Sec.Range: 1 - 999)

Flow Upload Interval  (Default: 300Sec.Range: 1 - 86400)

Device Code

Device ID

Device Type Description

Customized Local Domian

**Step 4** Click **Save** to save the configuration.

**Step 5** Click **Apply Settings** to apply the configuration.

**Step 6** (Optional) Click **Cancel Changes** to cancel the configuration.

### 3.12.1.8 Firmware Upgrade

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Administration > Management**.

**Step 3** In **Firmware Upgrade** section, enable firmware upgrade.

Figure 3-58 Enable firmware upgrade

**Firmware Upgrade**

Firmware Upgrade  Enable  Disable

Upgrade Server IP

Upgrade Server Port  (Default: 882, Range: 1 - 65535)

**Step 4** Set server IP address and port for firmware upgrade.

**Step 5** Click **Save** to save the configuration.

**Step 6** Click **Apply Settings** to apply the configuration.

Step 7 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.12.2 Keep Alive

You can schedule to turn on/off and reboot of the Router.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Keep Alive**.

Step 3 In **Schedule Boot&Shutdown** section, enable **Schedule Boot&Shutdown**.

Figure 3-59 Enable schedule boot and shutdown

**Schedule Boot&Shutdown**

Schedule Boot&Shutdown  Enable  Disable

Match  Day  Weekday  Days  Weekdays

Shutdown Time 00 : 00

Shutdown Date \* - 01 Sunday - Sunday

Boot Time 00 : 00

Boot Date \* - 01 Sunday - Sunday

Step 4 Set period, shutdown time, shutdown date, boot time and boot date.

Step 5 In **Schedule Reboot** section, enable **Schedule Reboot**.

Figure 3-60 Enable schedule reboot

**Schedule Reboot**

Schedule Reboot  Enable  Disable

Interval (in seconds)  3600

At a set Time  00 : 00 Sunday

Step 6 Set interval or set to reboot at a specified time.

- Interval (in seconds): Reboot after the interval.
- At a set Time: Reboot at a specified time.



Before enabling schedule reboot, you must enable the Cron function.

Step 7 Click **Save** to save the configuration.

Step 8 Click **Apply Settings** to apply the configuration.

Step 9 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.12.3 Commands

You can run command lines directly through the web interface of the Router.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Commands**.

Figure 3-61 Run commands

- **Run Commands:** You can run command lines through the web interface. In **Commands** text box, enter command and then click **Run Commands**.
- **Save Startup:** You can set command lines that are executed when the Router starts up. In **Commands** text box, enter command (only one command line) and then click **Save Startup**.
- **Save Shutdown:** You can set command lines that are executed when the Router shuts down. In **Commands** text box, enter command (only one command line) and then click **Save Shutdown**.
- **Save Firewall:** You can set command lines that are executed when the firewall is enabled. In **Commands** text box, enter command (only one command line) and then click **Save Firewall**.
- **Save Custom Script:** Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. In **Commands** text box, enter command (only one command line) and then click **Save Custom Script**.

### 3.12.4 Factory Defaults

If the Router is not working and you do not know how to fix it, you can restore to factory defaults.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Factory Defaults**.

Step 3 In **Restore Factory Defaults**, select **Yes**.

Figure 3-62 Factory defaults

Step 4 Click **Apply Settings** to apply the configuration.

After resetting, all configuration is restored to factory defaults.

Step 5 (Optional) Click **Cancel Changes** to cancel the configuration.

## 3.12.5 Firmware Upgrade

You can get the upgrading file from technical support, and upgrade the Router to a new firmware version.



- Export the configuration file for backup before upgrade, and then import it after the upgrade is completed. For details, refer to "3.12.6 Backup."
- Do not disconnect the power or network, or reboot or shutdown the Router during upgrade.



Upgrading with the wrong version might cause unavailability of the Router and data loss.

Please operate carefully.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Firmware Upgrade**.

Step 3 Click **Browse** to select the upgrading file.

Step 4 Click **Upgrade** and wait until the upgrade is finished.

Firmware upgrading may take a few minutes.

## 3.12.6 Backup and Restore

You can back up the current configuration of the Router in case you need to upgrade the firmware or reset the Router to the factory defaults.

You can also restore the configuration of the Router by using the backup configuration file.



You can only restore configurations with files that are backed up through the same firmware and the same model of routers.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Administration > Backup**.

Step 3 Click **Backup** to download the configuration file.

Step 4 In **Restore Configuration** section, click **Browse** to select the backup configuration file.

Step 5 Click **Restore** to restore the configuration.



## 3.13 Status

### 3.13.1 Router

You can view system information, serial application status, memory and network of the Router. All information is read-only.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Status > Router**.

Figure 3-63 Router information

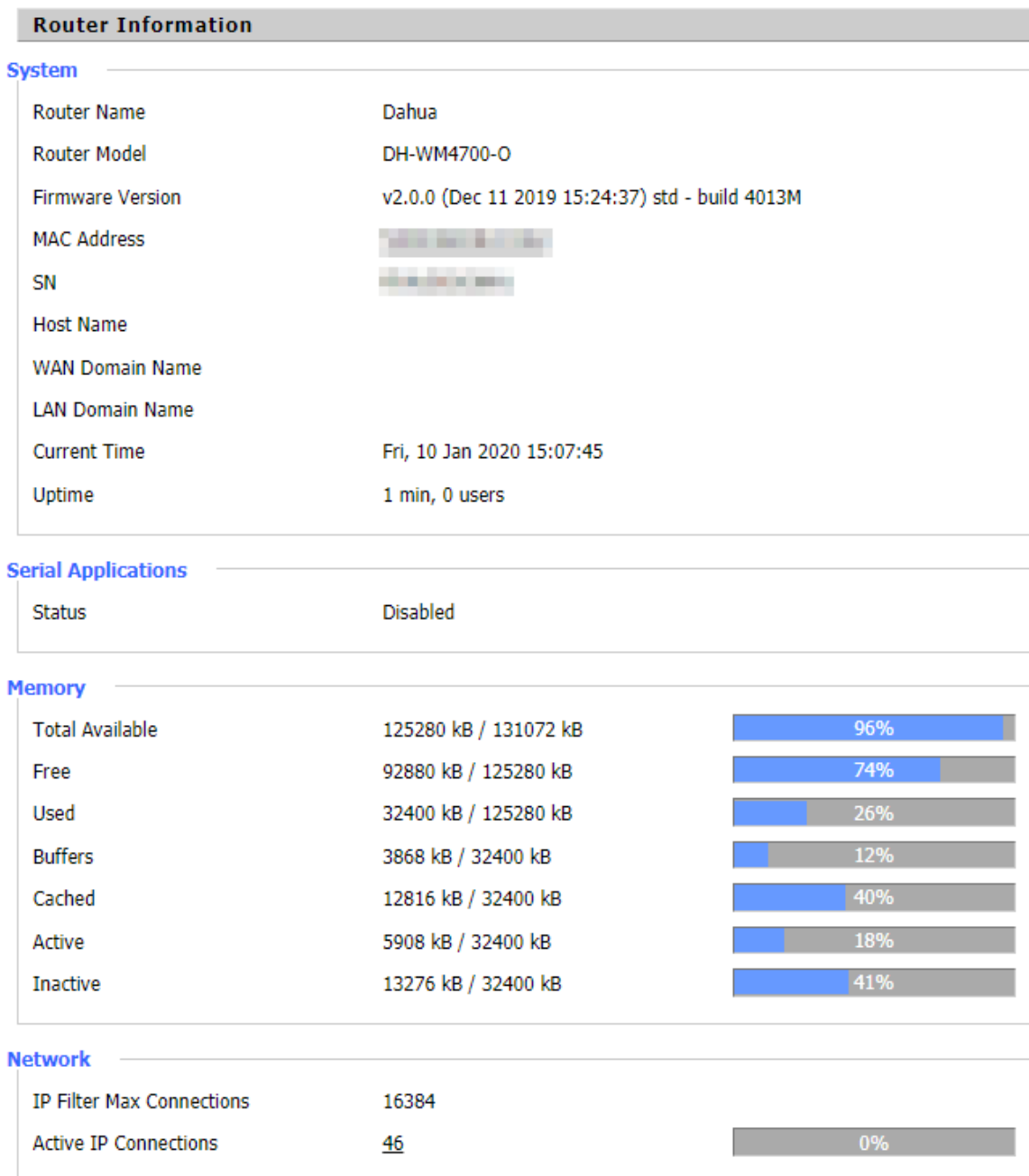


Table 3-30 Description of router information

Parameter	Description
<b>System</b>	
Router Name	The name of the Router, you can modify it in <b>Setup &gt; Basic Setup</b> . For details, refer to "3.3.1 Basic Setup."
Router Model	The model of the Router.
Firmware Version	The firmware version of the Router.
MAC Address	The MAC address of WAN, you can modify it in <b>Setup &gt; MAC Address Clone</b> . For details, refer to "3.3.3 MAC Address Clone."
SN	The serial number of the Router.
Host Name	The host name of the Router, you can modify it in <b>Setup &gt; Basic Setup</b> . For details, refer to "3.3.1 Basic Setup."
WAN Domain Name	The domain name of WAN, you can modify it in <b>Setup &gt; Basic Setup</b> . For details, refer to "3.3.1 Basic Setup."
LAN Domain Name	The domain name of LAN, it cannot be modified.
Current Time	The current time of the system.
Uptime	The duration of system power on.
<b>Serial Applications</b>	
Status	The status of the serial application.
<b>Memory</b>	
Total Available	The total available memory of RAM (that is physical memory minus the reserved bits and the kernel's binary code size).
Free	The free memory of the system. The Router will reboot if the memory is less than 500 KB.
Used	The used memory of the system (that is the total available memory minus the free memory).
Buffers	The used memory by the buffer (that is the total available memory minus the used memory).
Cached	The memory used by high-speed cache memory.
Active	The size of the active buffer or high-speed cache memory.
Inactive	The size of the inactive buffer or high-speed cache memory.
<b>Network</b>	
IP Filter Max Connections	The default value is 16384, and it cannot be modified.
Active IP Connections	The active IP connections in real time. Click the number to view details of the active IP connections, including protocol, timeout, source address, remote address, service name and state.

### 3.13.2 WAN

You can view the WAN connection type, and manage the traffic if the WAN connection is enabled.

**Step 1** Log in to the web interface of the Router.

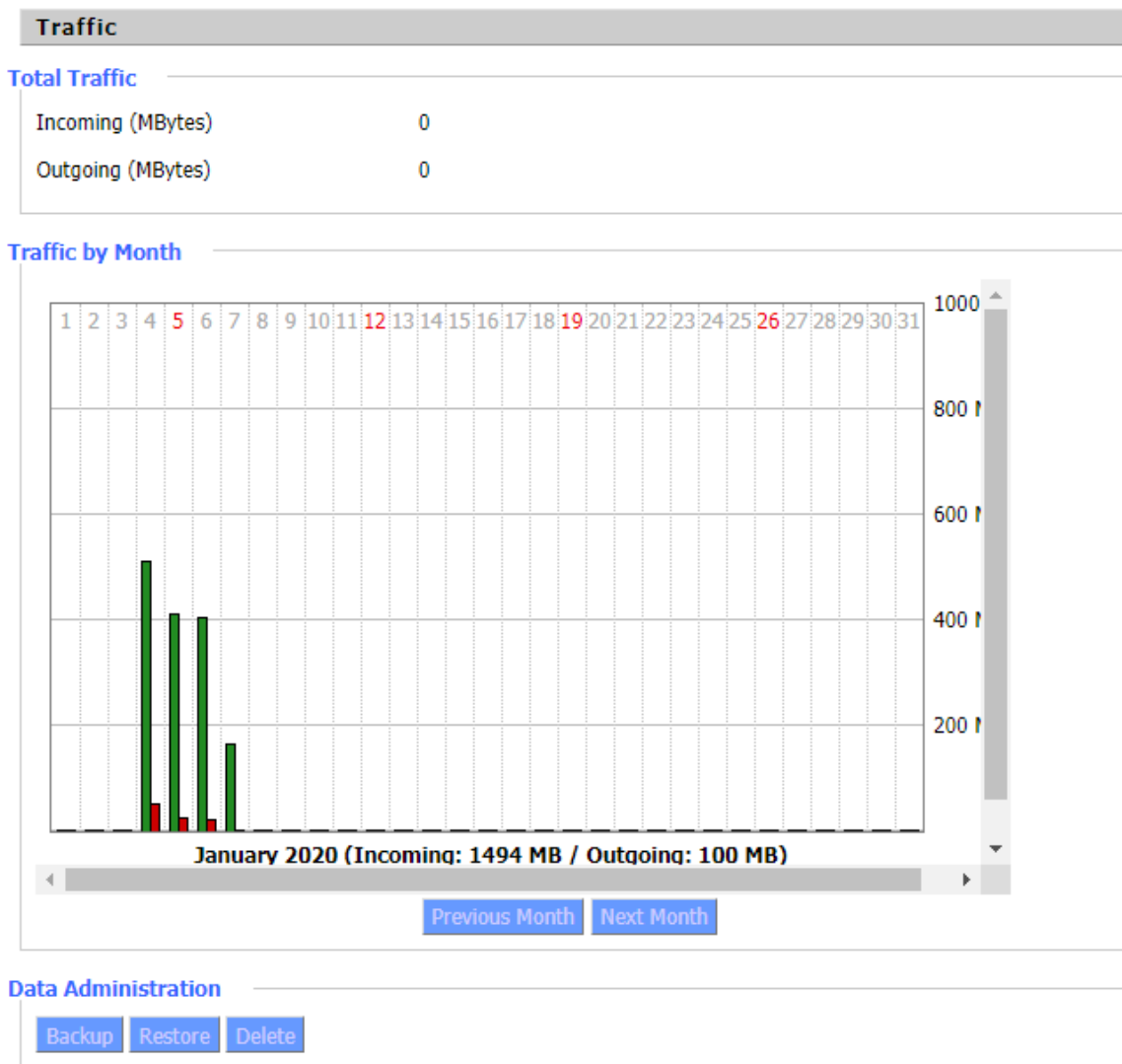
**Step 2** In the left navigation menu, select **Status > WAN**.

- Configuration Type: Display the information required by your ISP for connection to the Internet. You can modify the information in **Setup > Basic Setup**. For details, refer to "3.3.1 Basic Setup."
- Total Traffic: Display the Internet traffic of the Router since the latest reboot.
- Traffic by Month: Display the Internet traffic of the Router by month. Drag the mouse over the graph to see daily data.
- Data Administration: You can backup, restore or delete the traffic data.

Figure 3-64 WAN connection type

WAN	
<b>Configuration Type</b>	
Connection Type	Static
Connection Uptime	Not available
IP Address	
Subnet Mask	
Gateway	
DNS 1	
DNS 2	
DNS 3	

Figure 3-65 Traffic



### 3.13.3 LAN

You can view the LAN status, active clients, DHCP status and DHCP clients.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Status > LAN**.

Figure 3-66 LAN

**Local Network**

**LAN Status**

MAC Address	
IP Address	
Subnet Mask	
Gateway	
Local DNS	

**Active Clients**

Host Name	IP Address	MAC Address	Conn. Count	Ratio [16384]
*			0	0%

**Dynamic Host Configuration Protocol**

**DHCP Status**

DHCP Server	Enabled
DHCP Daemon	DNsmasq
Start IP Address	
End IP Address	
Client Lease Time	1440 minutes

**DHCP Clients**

Host Name	IP Address	MAC Address	Client Lease Time	Delete
- None -				

Table 3-31 Description of LAN parameters

Parameter	Description
<b>LAN Status</b>	
MAC Address	MAC address of LAN.
IP Address	IP address of LAN.
Subnet Mask	Subnet mask of LAN.
Gateway	Gateway of LAN.
Local DNS	DNS of LAN.
<b>Active Clients</b>	
Host Name	Host name of LAN client.
IP Address	IP address of the client.
MAC Address	MAC address of the client.
Conn. Count	Connections of the client.
Ratio	The ratio of 4096 connection
<b>DHCP Status</b>	
DHCP Server	Status of the DHCP server, enabled or disabled.
DHCP Daemon	When DNsmasq is enabled, the value is DNsmasq.

Parameter	Description
	When DNSMasq is disabled, the value is uDHCPd.
Start IP Address	Starting IP address of the DHCP server to start with when assigning IP addresses.
End IP Address	Ending IP address of the DHCP server to end with when assigning IP addresses.
Client Lease Time	Lease time of the DHCP client.
<b>DHCP Clients</b>	
Host Name	Host name of LAN client.
IP Address	IP address of the DHCP client.
MAC Address	MAC address of the DHCP client.
Client Lease Time	Lease time of the DHCP client.
Delete	Click to delete the selected DHCP client.

### 3.13.4 Wireless

You can view wireless status, wireless packet information and wireless node information.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Status > Wireless**.

Figure 3-67 Wireless

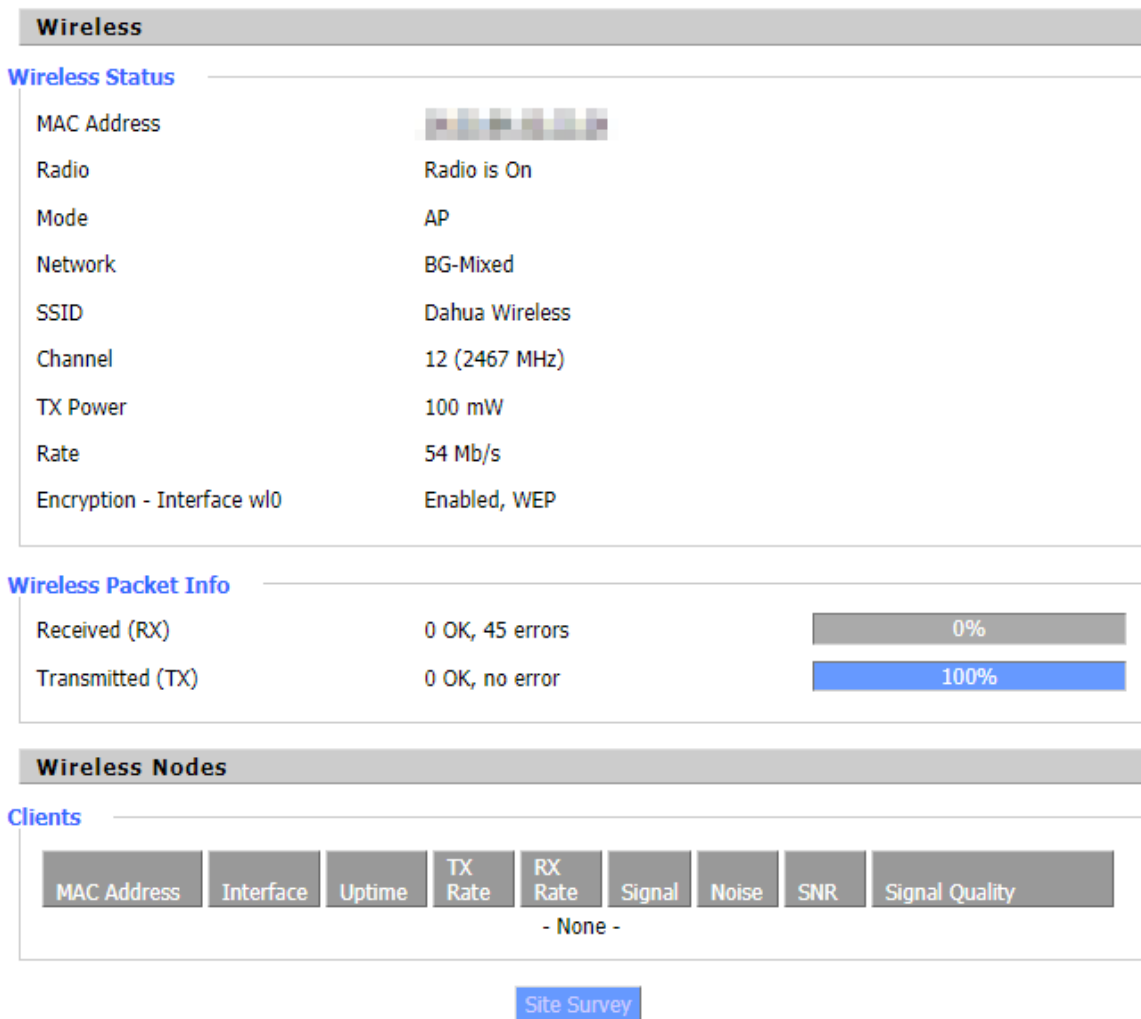


Table 3-32 Description of wireless parameters

Parameter	Description
<b>Wireless Status</b>	
MAC Address	MAC address of the wireless client.
Radio	Display whether radio is on or not.
Mode	Wireless mode.
Network	Wireless network mode.
SSID	Wireless network name.
Channel	Wireless network channel.
TX Power	Transmission power of wireless network.
Rate	Transmission rate of wireless network.
Encryption-Interface w10	Display whether the w10 interface is encrypted or not.
<b>Wireless Packet Info</b>	
Received (RX)	Received data packet.
Transmitted (TX)	Transmitted data packet.
<b>Wireless Nodes</b>	
MAC Address	MAC address of wireless client.

Parameter	Description
Interface	Interface of wireless client.
Uptime	Connection duration of wireless client.
TX Rate	Transmission rate of wireless client.
RX Rate	Receiving rate of wireless client.
Signal	Signal of wireless client.
Noise	Noise of wireless client.
SNR	Signal to noise ratio of wireless client.
Signal Quality	Signal quality of wireless client.



Click **Site Survey** to view all wireless networks that are reachable by the Router in the neighborhood.

### 3.13.5 Device Management

You can view connection status, upgrade status and Rsync update status in **Device Management**.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Status > Device Management**.

Figure 3-68 Device management

**Device Management**

**Connection Status**

Status	Disabled
Server Ip And Port	
Connection status	Ready...
Active Time	

**Firmware Upgrade**

Status	no update, waiting...
Server Ip And Port	
update version	
upgrade progress	

**rsync update local ad file**

Status	no update, waiting...
update info	
update progress	



## 3.13.6 Bandwidth

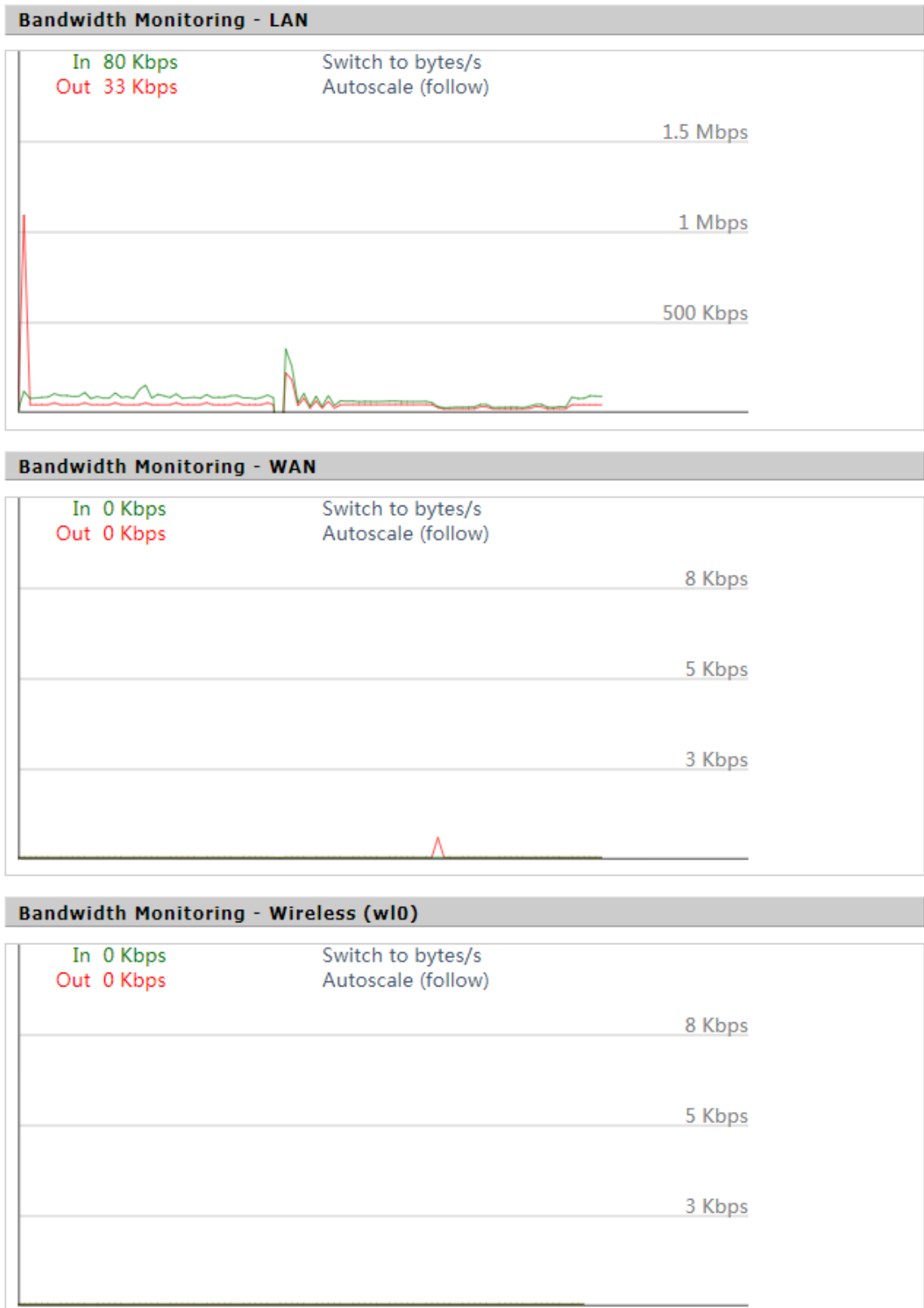
You can view the bandwidth of LAN, WAN and wireless network.

Step 1 Log in to the web interface of the Router.

Step 2 In the left navigation menu, select **Status > Bandwidth**.

- The abscissa axis of the graph indicates time.
- The vertical axis of the graph indicates speed rate.
- Switch to: Click the label to switch unit (bytes/s or bits/s).
- Autoscale: Click the label to choose graph scale type.

Figure 3-69 Bandwidth



### 3.13.7 System Information

You can view system information including the Router, wireless network, wireless packet, wireless clients, DHCP clients, services and memory.

**Step 1** Log in to the web interface of the Router.

**Step 2** In the left navigation menu, select **Status > Sys-Info**.

Figure 3-70 System information

**System Information**

**Router**

Router Name	Dahua
Router Model	DH-WM4700-0
LAN MAC	██████████
WAN MAC	██████████
Wireless MAC	██████████
WAN IP	0.0.0.0
LAN IP	172.12.70.172

**Services**

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Enabled

**Wireless**

Radio	Radio is On
Mode	AP
Network	BG-Mixed
SSID	Dahua Wireless
Channel	12 (2467 MHz)
TX Power	100 mW
Rate	54 Mb/s

**Memory**

Total Available	122.3 MB / 128.0 MB
Free	90.0 MB / 122.3 MB
Used	32.3 MB / 122.3 MB
Buffers	3.8 MB / 32.3 MB
Cached	12.7 MB / 32.3 MB
Active	6.2 MB / 32.3 MB
Inactive	12.9 MB / 32.3 MB

**Wireless Packet Info**

Received (RX)	0 OK, no error
Transmitted (TX)	0 OK, no error

**Wireless**

**Clients**

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

**DHCP**

**DHCP Clients**

Host Name	IP Address	MAC Address	Client Lease Time
- None -			

Table 3-33 Description of system information parameters

Parameter	Description
<b>Router</b>	
Router Name	Name of the Router.
Router Model	Model of the Router.
LAN MAC	MAC address of LAN port.
WAN MAC	MAC address of WAN port.
Wireless MAC	MAC address of wireless client.
WAN IP	IP address of WAN port.
LAN IP	IP address of LAN port.
<b>Wireless</b>	
Radio	Display whether wireless network is enabled.
Mode	Mode of wireless.
Network	Mode of wireless network.

Parameter	Description
SSID	Name of wireless network.
Channel	Channel of wireless network.
TX Power	Transmission power of wireless network.
Rate	Transmission rate of wireless network.
<b>Wireless Packet Info</b>	
Received (RX)	Received data packet.
Transmitted (TX)	Transmitted data packet.
Wireless client	
MAC Address	MAC address of wireless client.
Interface	Interface of wireless client.
Uptime	Connection duration of wireless client.
TX Rate	Transmission rate of wireless client.
RX Rate	Receiving rate of wireless client.
Signal	Signal of wireless client.
Noise	Noise of wireless client.
SNR	Signal to noise ratio of wireless client.
Signal Quality	Signal quality of wireless client.
<b>DHCP</b>	
Host Name	Host name of LAN client.
IP Address	IP address of the DHCP client.
MAC Address	MAC address of the DHCP client.
Client Lease Time	Lease time of the DHCP client.
Services	
DHCP Server	Display whether DHCP server is enabled.
ff-radauth	Display whether radauth service is enabled.
USB Support	Display whether USB is supported.
<b>Memory</b>	
Total Available	The total available memory of RAM (that is physical memory minus some reserved bits and the kernel's binary code size).
Free	The free memory of the system. The Router will reboot if the memory is less than 500 KB.
Used	The used memory of the system (that is the total available memory minus the free memory).
Buffers	The used memory by the buffer (that is the total available memory minus the used memory).
Cached	The memory used by high-speed cache memory.
Active	The size of the active buffer or high-speed cache memory.
Inactive	The size of the inactive buffer or high-speed cache memory.

# Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

## 5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

## 6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

## 7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

## 8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

## 9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

## 10. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

## 11. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

## 12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

## 13. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

## 14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

1