

Bivocom[®]

Industrial Cellular WIFI Router TR321 Series User Guide



Copyright

Copyright © XIAMEN BIVOCOM TECHNOLOGIES CO., LTD. All rights reserved.

Trademark

BIVOCOM logo is a registered trademark of Xiamen Bivocom Technologies Co., Ltd. All other trademarks belong to their respective vendors or manufactures.

Disclaimer

Product specifications and information in this document are subject to change without any notice, and BIVOCOM reserves the right to improve and change this user guide at any time. Users should take full responsibility for their application of products, and Xiamen Bivocom Technologies Co., Ltd. disclaims all warranties and liability for the accurateness, completeness of the information published.

About This Guide

Thank you for choosing Bivocom Industrial Cellular WIFI Router TR321 Series.

Please thoroughly read this user guide before you configure and install the device.

This manual is compatible with below models

| Model | Description |
|----------|-------------------------------|
| TR321-W | Industrial WCDMA ROUTER |
| TR321-LF | Industrial LTE/WCDMA ROUTER |
| TR321-M | Industrial CAT-M NBloT ROUTER |

Table of Contents

| | |
|--|----|
| Copyright | 2 |
| Trademark | 2 |
| Disclaimer..... | 2 |
| About This Guide..... | 3 |
| Table of Contents..... | 4 |
| 1. Introduction | 6 |
| 1.1 Overview | 6 |
| 1.2 Applications..... | 6 |
| 1.3 Dimensions | 7 |
| 1.4 Physical Characteristics..... | 7 |
| 2. Getting Started | 7 |
| 2.1 Package Checklist | 7 |
| 2.2 Installation..... | 8 |
| 2.2.1 SIM/UIM Card | 9 |
| 2.2.2 5-Pin Terminal Block and Console Cable | 9 |
| 2.2.3 Power Supply | 10 |
| 2.2.4 Cellular Antenna | 10 |
| 2.3 LED Indicators..... | 10 |
| 2.4 Reset | 11 |
| 3. Configuration and Management | 11 |
| 3.1 Setup | 11 |
| 3.1.1 WAN | 11 |
| 3.1.2 LAN..... | 13 |
| 3.1.3 Wireless (Option)..... | 15 |
| 3.1.4 Online Detection | 16 |
| 3.1.5 Diagnostics | 18 |
| 3.2 Security | 19 |
| 3.2.1 DMZ Host..... | 19 |
| 3.2.2 Port Forwarding | 20 |
| 3.2.3 Traffic Rules..... | 20 |
| 3.2.4 Custom Settings | 23 |
| 3.3 Management..... | 23 |
| 3.3.1 System | 23 |
| 3.3.2 Password | 24 |
| 3.3.3 Time Setting | 25 |
| 3.3.4 Log Settings | 26 |
| 3.3.5 Backup and Reset | 27 |
| 3.3.6 Firmware Upgrade..... | 27 |
| 3.3.7 Remote Management | 28 |
| 3.3.8 Reboot..... | 30 |

| | |
|--|----|
| 3.4 Advanced | 30 |
| 3.4.1 Dynamic DNS..... | 31 |
| 3.4.2 QoS Settings | 32 |
| 3.4.3 Static Routing..... | 32 |
| 3.4.4 Base Station Location (Option) | 33 |
| 3.4.5 GPS (Option)..... | 33 |
| 3.4.6 Traffic Meter..... | 34 |
| 3.4.7 Serial Application | 34 |
| 3.5 VPN..... | 36 |
| 3.5.1 PPTP | 37 |
| 3.5.2 L2TP | 39 |
| 3.5.3 OpenVPN..... | 41 |
| 3.5.4 IPSec..... | 42 |
| 3.6 View | 43 |
| 3.6.1 System | 43 |
| 3.6.2 Network..... | 44 |
| 3.6.3 Routing Tables | 45 |
| 3.6.4 System Log..... | 46 |
| 3.6.5 VPN Status..... | 46 |

1. Introduction

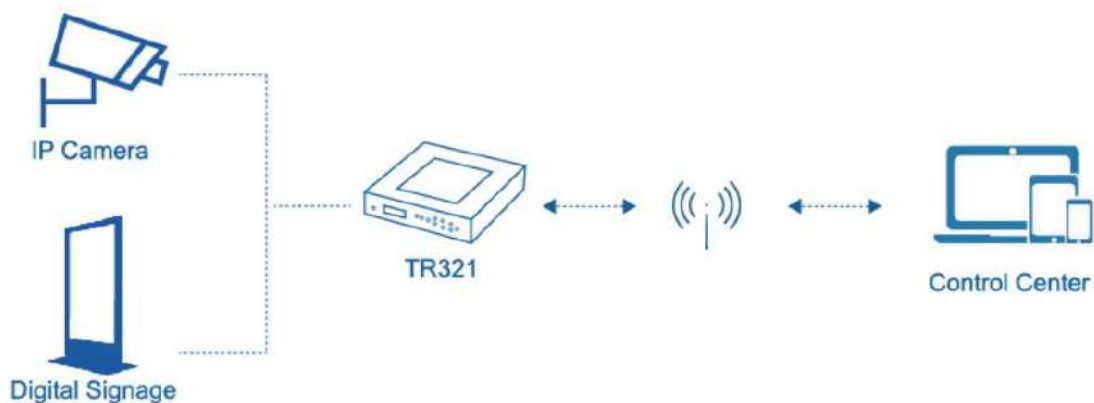
1.1 Overview

TR321 Series Router is a type of compact industrial wireless router, designed to fully meet the needs of industrial standards and industrial users. It adopts high-powered industrial 32-bits CPU, multi-layer software detection and hardware protection mechanism to ensure reliability and stability of the device. It supports worldwide carrier 4G/3G cellular network FDD-LTE, TD-LTE, and WCDMA, EVDO, TD-SCDMA, EDGE, CDMA 1X and GPRS, CAT-M, NB-IoT. With rich VPN protocols(IPSEC、PPTP、L2TP etc.) to ensure the security of data transmission, and rich interfaces, such as RS232 (or RS485/RS422), Ethernet Port, I/O(Optional) and WIFI(Optional), etc.

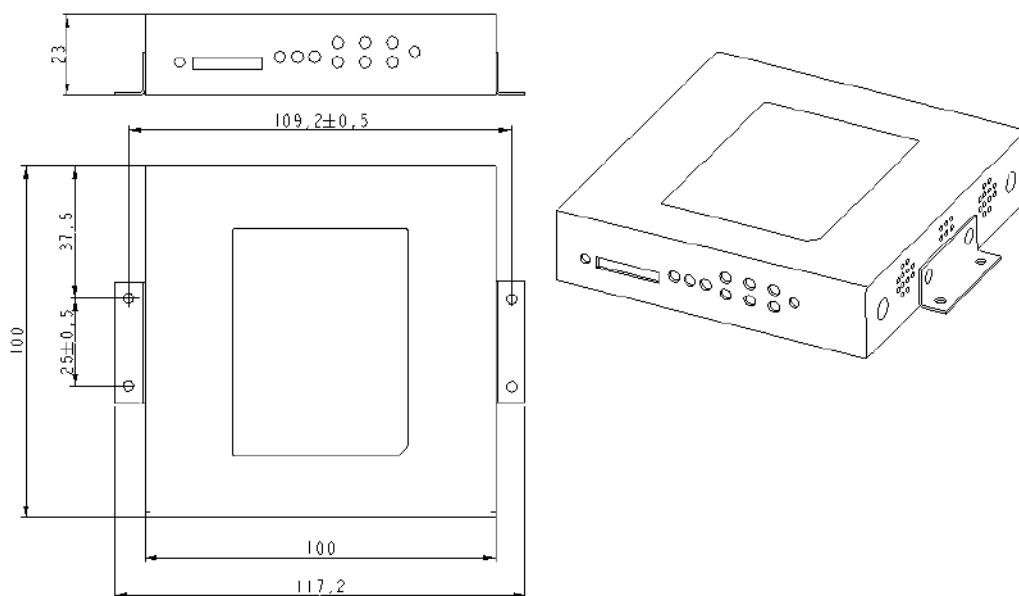
TR321 Series Router enables users to quickly access the Internet, to ensure secure and reliable data transmission. It's ideal for IOT (Internet of Things) and M2M(Machine to Machine) applications, and has been widely used in many applications, such as Intelligent Transportation, Smart Grid, Vending Machine, Agricultural Irrigation, Environmental Protection, Industrial Automation, Energy Saving, Smart Home, etc.

1.2 Applications

TR321 Series Router utilizes cellular network to connect your network devices and serial port devices to your center for remote monitoring and control. Typical application as below.



1.3 Dimensions



1.1
1.22
1.23

1.4 Physical Characteristics

| Physical Characteristics | |
|--------------------------|---|
| Housing | Metal, IP30 |
| Dimensions | 100x100x23mm(3.94x3.94x0.91 inches), Antenna and other accessories not included |
| Weight | 320g(0.71lbs) |

2. Getting Started

2.1 Package Checklist

The following components are included in your TR321 package.

Check the list before installation. If you find anything missing, Please feel free to contact Bivocom.

- TR321 Router Host
- Power Adapter(1.5A/12VDC)
- Cellular Antenna(Male SMA)
- Console Cable(RS232)
- Ethernet Cable(1 meter)

- 5-Pin Terminal Block

Ethernet Cable



RS232 Cable



Power Adapter



TR321 Host

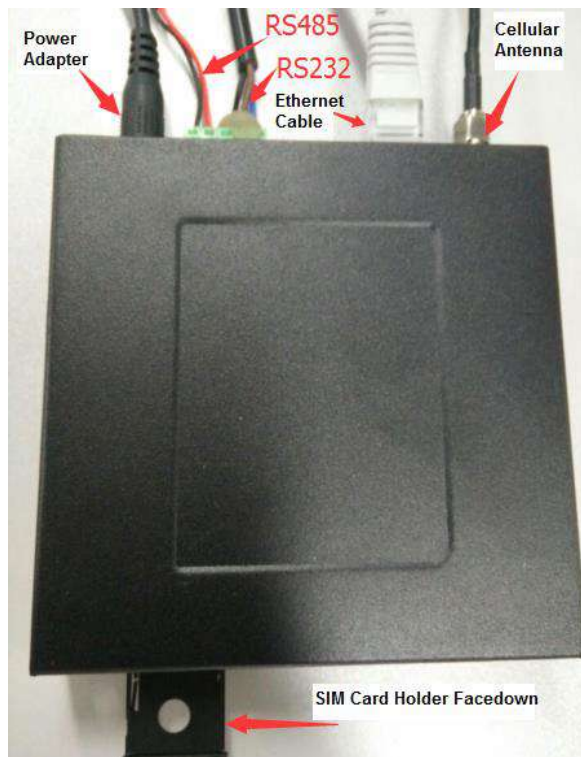


5-Pin Terminal Block



Cellular Antenna

2.2 Installation



2.2.1 SIM/UIM Card

TR321 supports normal SIM/UIM only, so if you're using a Micro SIM or Nano SIM card, you may need to use a Micro SIM or Nano SIM to Normal SIM adapter.

Make sure your router is powered off, then use a needle object(such as a pen) to push the button near the SIM/UIM card holder, it will flick out immediately. Put the SIM/UIM card to card holder with chipset upside, insert it to router and make sure it's tightly matched.

Warning: Never install SIM/UIM card when router is powered on.

2.2.2 5-Pin Terminal Block and Console Cable

TR321 supports RS232 and RS485 serial port, which can be used for firmware upgrade, system log checking, or acts as serial port of a DTU(Please refer to Bivocom TD210 Series DTU).

TR321 designed with industrial terminal block interface, and the cable in this package with ends of female connector and stripping cable, the signal of console cable is defined as below,

RS232 Cable(with DB9 female connector and stripping cable)

| Color of cable | Corresponding DB9-Female Pin No. | Corresponding Pin No. of Router (Pin 1 closes to power jack, Pin 5 closes to ethernet port) |
|----------------|----------------------------------|--|
| Blue | 2 (RX) | 1(TX) |
| Brown | 3 (TX) | 2(RX) |
| Black | 5 (GND) | 3(GND) |

RS485 Cable

| Color of cable | TR321 Router |
|----------------|--------------|
| Red | 4(A) |
| Black | 5(B) |

2.2.3 Power Supply

We suggest you use Bivocom standard power adapter (1.5A/12VDC). If you have to use your own power supply, make sure the power range is 5-35VDC and it is stable enough(Ripple shall be less than 300mV, and Instantaneous voltage shall not larger than 35V), meanwhile, power shall over 4W.

2.2.4 Cellular Antenna

Screw the SMA male antenna to TR321(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators



TR321 Series Router provides 7 LED indicators, as following.

| Indicator | Status | Content |
|-----------------|-------------|--|
| Power | On | Powered On |
| | Off | Powered Off |
| Signal Strength | 1 Lights | Signal weak |
| | 2 Lights | Signal Middium |
| | 3 Lights | Signal Strong |
| System | Blink | System works perfect |
| | Off | System doesn't work |
| Online | On | Router accesses to Internet |
| | Off | Router doesn't access to Internet |
| Alarm | On | <ul style="list-style-type: none">● SIM/UIM Card is not insert corectly or broken● Antenna signal is too weak |
| | 1 Blink Per | Cellular module was not registered to router |

| | | |
|-----|---------------------|---------------------------------|
| | Second | |
| | 2 Blinks Per Second | Router can't access to Internet |
| | Off | Router doesn't have any alarm |
| WAN | On | WAN is connected |
| | Off | WAN is not connected |
| LAN | Blink | LAN works |
| | Off | LAN is not connected |

2.4 Reset

You can click Reset button to reset settings to factory defaults to solve the problem of incorrect configuration that makes you couldn't access to internet, login and management, etc.

Use a needle object(such as pen) to insert into hole of 'Reset', hold until all the LED indicators turn off.

3. Configuration and Management

Use an Ethernet cable to connect the LAN port of TR321 to your laptop, or use your laptop or mobile phone to connect to WIFI hotspot 'Bivocom' of TR321, login with password: admin123, then configure you local IP to 192.168.1.100.

Open browser, enter 192.168.1.1 to enter into to login page, enter username: admin, and password: admin, to go to configuration page.

3.1 Setup

Main menu of this page includes, WAN, LAN, Wireless, Online Detection, Diagnostics.

3.1.1 WAN

WAN supports DHCP/Static IP/PPPoE/3G/LTE connection mode.

Choose the mode you need, then click 'Switch Connection Mode' and configure the related parameters, then you can connect to the internet.

View

Setup

- WAN
- LAN
- Wireless
- Wireless Client
- Online Detection
- Diagnostics

Secure

VPN

Advanced

Administrate

Logout

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Physical Settings

Protocol: LTE

Service Type: AUTO

APN:

PIN:

Username:

Password:

Authentication Type: None PAP CHAP

1) Server Type

Type of network, the default value is AUTO, you can keep it or choose your own preference.

2) APN

Different carrier might have different APN, please ask your carrier if you have no idea of what your APN is.

3) PIN

PIN code of SIM card, please use it carefully, or the SIM card may be locked.

4) PAP/CHAP Username

Only for private network SIM card, if you're using public network SIM card, just keep it as null.

5) PAP/CHAP Password

Only for private network SIM card, if you're using public network SIM card, just keep it as null.

6) Call Center No.

When you're using SIM card, different carrier may have different call center Number, please ask your carrier for this info if you have questions.

7) Authentication Type


If there have username and password, you need to choose authentication type.

- PAP, Plaintext Authentication
- CHAP, Handshake authentication

You need to choose the authentication type according to carrier's network, or you may fail to dial up.

8) WAN Used As LAN

When you use 4G/3G/2G cellular network to access internet, you can change the WAN to act as a LAN port.




WAN Multiplex  Set WAN port as LAN port

3.1.2 LAN

Menu of LAN are mainly for configuring IP address of router, enabling DHCP server, and assign the IP address.

The meaning of the parameters are as follows.

Common Configuration

| | | |
|---------------|----------------------|---|
| General Setup | Advanced Settings | Physical Settings |
| Protocol | Static address |  |
| IPv4 address | <input type="text"/> | |
| IPv4 netmask | 255.255.255.0 |  |
| IPv4 gateway | <input type="text"/> | |
| DNS Servers | <input type="text"/> |  |

1) IPv4 Address

To configure IP address of LAN port.

2) IPv4 Netmask

The netmask of LAN port IP address.

3) IPv4 Gateway

Specify the next-hop routing gateway.

4) DHCP Settings

General Setup

Ignore interface [Disable DHCP for this interface.](#)

Start [Lowest leased address as offset from the network address.](#)

Limit [Maximum number of leased addresses.](#)

Leasetime [Expiry time of leased addresses, minimum is 2 minutes \(2m\).](#)

- **Disable DHCP**

Click to disable DHCP server.

- **Start**

Assign the IP address of DHCP server. For example, 100 means IP address starts from 192.168.1.100.

- **Limit**

Assignable number of IP address, to ensure numbers of IP address of start and limit not exceed 250.

- **Lease time**

Time of assigning the IP address.

3.1.3 Wireless (Option)

Menu of wireless are mainly for configuring the SSID, work mode, password, etc.

WiFi 2.4G Enable Disable

Network Name(SSID)

Channel

Mode

Encryption

Key

Hide SSID

1) WIFI 2.4G

Click 'Enable', to enable the WIFI function.

2) Network Name (SSID)

WIFI network name.

3) Channel

Support 1-13 channels, default value is auto, channel can be changed automatically.

4) Mode

Support 802.11b, 802.11g, 802.11bgn.

802.11b up to 11Mbps, 802.11g up to 54Mbps and 802.11n up to 300Mbps.

5) Encryption

You can only choose below types if the mode is set as 802.11b or 802.11g.



A dropdown menu with a light blue border and a downward arrow icon on the right. The menu is open, showing five options: 'WPA2-PSK-AES' (selected and highlighted in blue), 'No Encryption', 'WPA2-AES-RADIUS', 'WPA2-PSK-AES', and 'WPA-PSK-AES'.

6) Key

Password of sharing the WIFI, user need to enter it to access the internet. The minimum length of password is 8 bytes.

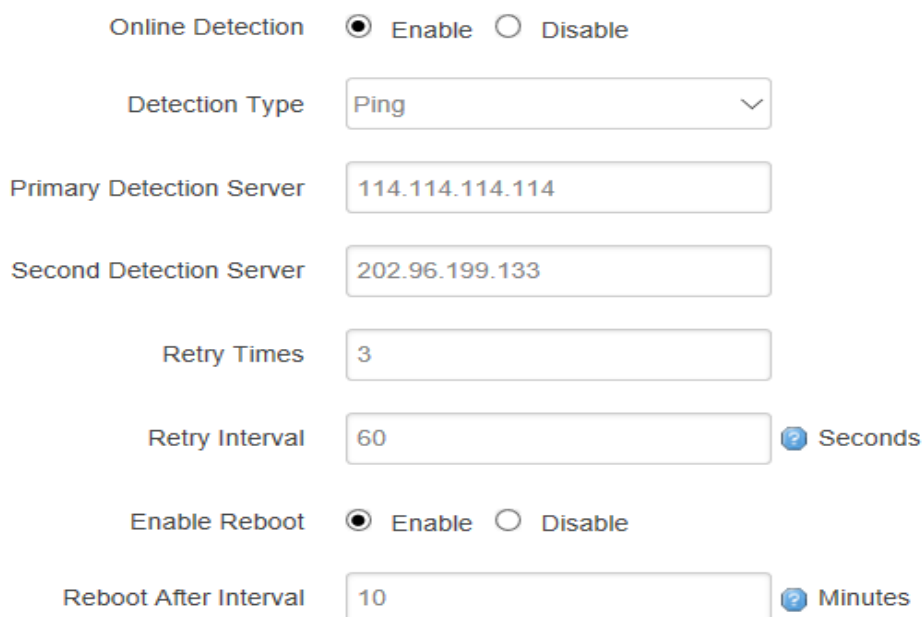
7) Hide SSID

When Hide SSID enabled, SSID is invisible, and user need to enter the SSID to share the WIFI.

3.1.4 Online Detection

Online detection will auto check the internet connection status of the router, if there has issue of connection, router will auto reconnect. If it fails to reconnect after times of trial, router will reboot, to ensure getting online.

The meaning of the parameters are as follows.




Online Detection Enable Disable

Detection Type


Primary Detection Server

Second Detection Server

Retry Times

Retry Interval  Seconds

Enable Reboot Enable Disable

Reboot After Interval  Minutes

1) Detection Type

There are 3 types: ping, traceroute and DNS.

- **Ping**

Router will ping an IP address or DNS, if works, that means router is online.

- **Traceroute**

Traceroute will trace routing path, if achieves the target address, that means router is online.

- **DNS**

DNS will analytic a domain, if it works, that means router is online.

Note: the default setting is Ping, which is highly recommended, as traceroute will cost dataflow of SIM card, while DNS is faster, but as it has cache, it may shows the router is online even it is offline.

2) Primary Detection Server

It can be an IP address or a Domain Name.

3) Second Detection Server

If primary detection server fails, then router will auto switch to second detection server.

4) Retry Times

You can set up retry time in case detection fails.

5) Retry Interval

The interval time between 2 detection.

6) Enable Reboot

Click enable, and router will reboot within the time set if it fails to reconnect.

7) Reboot After Interval

You can specify the time for offline, to reboot the router.

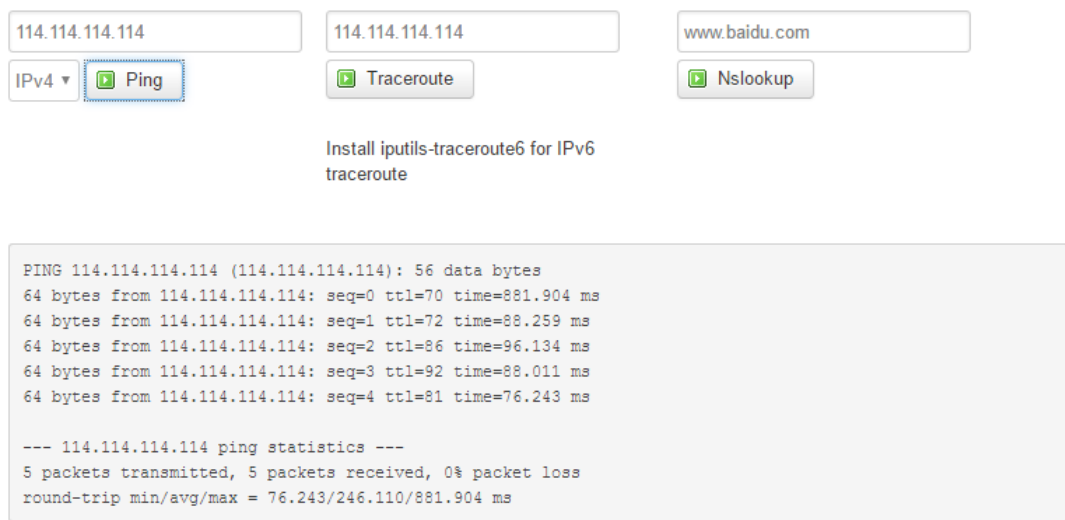
3.1.5 Diagnostics

There are 3 types of diagnostics: ping, traceroute and nslookup

Parameter of ping and traceroute can be a Domain Name or an IP address, used for checking if router is online or not. While nslookup is to analytic domain.

1) Ping

Click ping, then you can check if there is response from an IP address, as bellow.



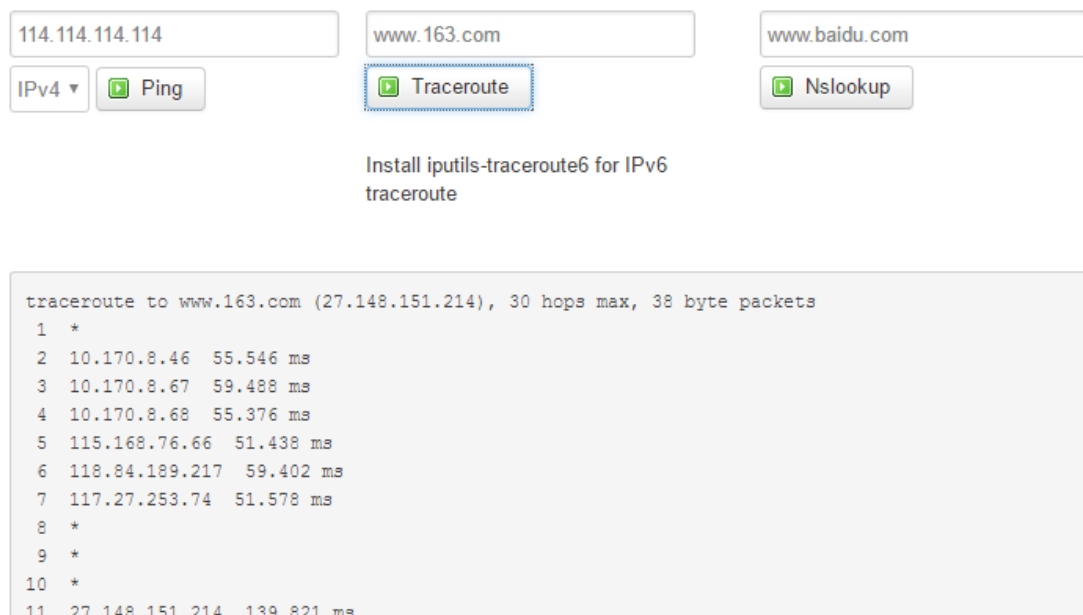
The screenshot shows a web-based diagnostic tool with three input fields: '114.114.114.114', '114.114.114.114', and 'www.baidu.com'. Below each field are buttons for 'IPv4', 'Ping', 'Traceroute', and 'Nslookup'. The 'Ping' button under the first field is highlighted. Below the buttons, there is a message: 'Install iputils-traceroute6 for IPv6 traceroute'. A large text box displays the following output:

```
PING 114.114.114.114 (114.114.114.114): 56 data bytes
64 bytes from 114.114.114.114: seq=0 ttl=70 time=881.904 ms
64 bytes from 114.114.114.114: seq=1 ttl=72 time=88.259 ms
64 bytes from 114.114.114.114: seq=2 ttl=86 time=96.134 ms
64 bytes from 114.114.114.114: seq=3 ttl=92 time=88.011 ms
64 bytes from 114.114.114.114: seq=4 ttl=81 time=76.243 ms

--- 114.114.114.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 76.243/246.110/881.904 ms
```

2) Traceroute

Click traceroute, then you can see similar reponse as below.



The screenshot shows the same web-based diagnostic tool. The 'Traceroute' button under the second input field 'www.163.com' is highlighted. Below the buttons, there is a message: 'Install iputils-traceroute6 for IPv6 traceroute'. A large text box displays the following output:

```
traceroute to www.163.com (27.148.151.214), 30 hops max, 38 byte packets
 1 *
 2 10.170.8.46 55.546 ms
 3 10.170.8.67 59.488 ms
 4 10.170.8.68 55.376 ms
 5 115.168.76.66 51.438 ms
 6 118.84.189.217 59.402 ms
 7 117.27.253.74 51.578 ms
 8 *
 9 *
10 *
11 27.148.151.214 139.821 ms
```

3) Nslookup

Click nslookup, then you can see similar response as below.



The screenshot shows a network utility interface with three columns of input fields and buttons. The first column has the IP address '114.114.114.114', a dropdown menu set to 'IPv4', and a 'Ping' button. The second column has the domain 'www.163.com' and a 'Traceroute' button. The third column has the domain 'www.baidu.com' and an 'Nslookup' button. Below these fields is a text instruction: 'Install iputils-traceroute6 for IPv6 traceroute'. At the bottom, a terminal window displays the following output:

```
Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: www.baidu.com
Address 1: 14.215.177.38
Address 2: 14.215.177.37
```

3.2 Security

Menu of Security are for configuring the firewall, to ensure the security of accessing to internet, and implement the port forwarding, access control, data packet filtering, and other functions.

3.2.1 DMZ Host

DMZ can forward the port of WAN to a host of LAN; all packet from WAN will be forwarded to specified host of LAN.



The screenshot shows the DMZ configuration interface. It includes a label 'DMZ' followed by two radio buttons: 'Enable' (which is selected) and 'Disable'. Below this is a label 'DMZ Host' followed by a text input field containing the IP address '192.168.1.0'.

1) DMZ

You can enable or disable the DMZ.

2) DMZ Host

An IP address of a host of LAN you want to map.

3.2.2 Port Forwarding

Comparing with DMZ, Port Forwarding is for more precise control, user can forward the data packet of a port to a host of LAN, to forward different port to different host.

| New port forward: | | | | | |
|---|-----------------------------------|----------------------------------|----------------------|----------------------|------------------------------------|
| Name | Protocol | External zone | External port | Internal IP address | Internal port |
| <input type="text" value="New port forward"/> | <input type="text" value="TCP+"/> | <input type="text" value="wan"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| | | | | | <input type="button" value="Add"/> |

1) Name

You can name the rule you created.

2) Protocol

You can choose TCP, UDP, or TCP/UDP.

3) External Port

Destination port before port forwarding.

4) Internal IP Address

The Host IP address to forward.

5) Internal Port

The destination port after port forwarding. Normally, external port and internal port are the same, but also can be different.

After configured above-mentioned, click 'Add', then a new rule will be added, and click 'Save & Apply', to have the rule take effect.

3.2.3 Traffic Rules

Traffic rules is used for opening some router ports, such as remote access the configuration page of router, you can open port 80; for remote SSH connection, you can open port 22.

| Open ports on router: | | |
|---|--------------------------------------|------------------------------------|
| Name | Protocol | External port |
| <input type="text" value="New input rule"/> | <input type="text" value="TCP+UDP"/> | <input type="text"/> |
| | | <input type="button" value="Add"/> |

1) Name

You can name the rule yourself.

2) Protocol

Choose the protocol of you want to forward can be TCP, UDP, or TCP/UDP.

3) External Port

Choose the port you want to open.

In addition, traffic rule can be used for creating some access control rules, it can be from LAN to WAN, or WAN to LAN.

| New forward rule: | | | |
|--|----------------------------------|----------------------------------|---|
| Name | Source zone | Destination zone | |
| <input type="text" value="New forward r"/> | <input type="text" value="lan"/> | <input type="text" value="wan"/> | <input type="button" value="Add and ed"/> |

1) Name

You can name the rule yourself.

2) Source Zone

You can choose where to start the data packet.

3) Destination Zone

You can choose where to forward the data packet.

Click 'Add and Edit', then you can get more detailed matching condition.

Rule is enabled

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

Any zone

lan: lan:

wan: wan:

Source MAC address

Source address

Source port

Destination zone

Device (input)

Any zone (forward)

lan: lan:

wan: wan:

Destination address

Destination port

Action

Extra arguments Passes additional arguments to iptables. Use with care!

1) Restrict to Address Family

You can choose IPv4, IPv6, or Pv4/IPv6.

2) Protocol

To choose the protocol you want for access control, it can TCP, UDP or TCP/UDP.

3) Source MAC Address

To choose the source MAC address of data packet.

4) Source Address

To choose the source IP address of data packet.

5) Source Port

To choose the source port of data packet.

6) Destination Address

To choose the destination IP address of data packet.

7) Destination Port

To choose the destination port of data packet.

8) Action

If the above-mentioned conditions matched, then you can choose below actions.

- **Accept**

Allow data packet to go through.

- **Drop**

Drop data packet

- **Reject**

Drop data packet, and return an unachievable data packet.

- **Don't Track**

No action.

3.2.4 Custom Settings

Users can also customize some firewall rules themselves, as those rules consist of iptables, we suggest users that are familiar with iptables command to do this. When you add rules, please add them at the bottom of existing rules, and don't delete them.

3.3 Management

3.3.1 System

| | |
|----------|--|
| Hostname | <input type="text" value="router"/> |
| Timezone | <input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="(GMT+08:00) Beijing, Chongqing"/> |
| Language | <input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="English"/> |

Enable telnet access Enable Disable

Enable SSH access Enable Disable

1) Host Name

The host name of router, default name is router.

2) Time Zone

Set up the time zone of system, default time zone is GMT8.

3) Language

Change the language of configuration interface, default language is English.

4) Enable Telnet Access

To enable the telnet server, the default function is enable.

5) Enable SSH Access

To enable the SSH server, the default function is disable.

3.3.2 Password

To revise the password of router.

| | | |
|-----------------|----------------------|---|
| Origin Password | <input type="text"/> |  |
| Password | <input type="text"/> |  |
| Confirmation | <input type="text"/> |  |

1) Origin Password

You'll be required to enter your origin password before your revise your new password.

2) Password

Type the new password you want to change.

3) Confirmation

Type the new password again to confirm it.

If the new password and confirmation password you type is different, then it fails to revise the password. After password revised, router will return to login page, then you can enter your username and password.

3.3.3 Time Setting

System time type includes RTC (Real Time Clock) and NTP (Network Time Protocol). RTC will save time even router is powered off, while for NTP, router will connect to NTP server which requires internet connection, time won't be saved once powered off. But NTP will be more accurate than RTC, and you may need to adjust the time manual if it is not accurate.

Current system time 2017-03-20 10:10:56

System Time Type ntp rtc

1) Current System Time

Display the time of router.

2) System Time Type

It includes NTP and RTC mentioned above, and different type has different configuration parameters

- **RTC**

You can update data and time yourself.

RTC Date ? eg: 2016-01-01

RTC Time ? eg: 12:00:00


RTC Data

Format must be: 20xx-xx-xx (Year-Month-Day), or you will fail to update it.

RTC Time

Format must be xx: xx: xx (Hour-Min-Second), or you will fail to update it.

- **NTP**

| | | |
|-----------------|---|---|
| NTP Time Server | <input type="text" value="0.openwrt.pool.ntp.org"/> | ▼ |
| Port | <input type="text" value="123"/> | |
| Update Interval | <input type="text" value="600"/> |  seconds |

NTP Time Server

You can select the NTP time server through drop-down menu, or you can customize it yourself.

Port


NTP time server port, default port is 123.

Update Interval

How long to sync the time with NTP server, default time is 600 seconds.

3.3.4 Log Settings

Log settings is for configuring the output parameters of system log.

| | | |
|------------------|--|--|
| Output To Device | <input type="text" value="/var/log/"/> | ▼ |
| Log Size | <input type="text" value="64"/> |  KB |
| Log Server | <input type="text" value="0.0.0.0"/> | |
| Log Server Port | <input type="text" value="514"/> | |
| Output Level | <input type="text" value="Debug"/> | ▼ |

1) Output to Device

You can output the log to serial port, or specified file path, or external storage device, and the default path is:/var/log/

2) Log Size

Set up the size of log, default value is 64KB.

3) Log Server

Set up the IP address of log server.

4) Log Server Port

Set up the port of log server, default value is 514

5) Output Level

There are several levels supported, including 'Debug', 'Info', 'Notice', 'Warning', 'Error', and level increased in sequence, the higher level, the less output log.

3.3.5 Backup and Reset

User can either backup the configuration of router, or reset to factory defaults.

"Perform reset" (only possible with squashfs images).



1) Download Backup

Click to generate a configuration file in format of "backup-router-2016-**-**.tar.gz".

2) Reset to Default

Click 'Perform Reset', and a pop-up confirmation box with 'Really Reset All Changes' will display, then click 'OK' to reset to factory defaults.

3) Restore Backup

To restore configuration files, you can upload a previously generated backup archive here.



After reset to default, you can also upload the saved configuration file to router, to recover the previous configuration. Click 'upload archive', select and upload the backup configuration file, and a pop-up confirmation box with 'Really Restore' will display, then click 'OK', to recover the configuration.

3.3.6 Firmware Upgrade

Before you upgrade the firmware for router, make sure the firmware you're planning to upload is correct. If errors occurs, use serial port and connect the Ethernet cable, upgrade

the firmware through u-boot.

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings:

Image:

1) Keep Settings

Click it, and system configuration will not be changed after firmware upgrade.

2) Choose and Upload Firmware Image

Click 'browse' and select the firmware, then click 'Flash Image', and firmware will be upload to router. Then you'll go to below page.

Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.

Click "Proceed" below to start the flash procedure.

Checksum: `f68983dbe5ec7f0d4bf9258e421ad53d`

Size: 9.00 MB

Configuration files will be kept.

- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

- **Proceed**

Click 'proceed' to start the firmware upgrade, or click 'cancel' to stop the firmware upgrade.

3.3.7 Remote Management

You can configure the IP address and port of remote server, device number and phone number of router, etc., as below.

Remote Manage Enable Disable

Server Address

Server Port

Heart Interval

Device Number

Device Phone Number

Device Type

1) Remote Manage

You can enable or disable this function to choose if you want to remote manage the router or not.

2) Server Address

Type the specified login server address you want to remote manage the router, it can be either an IP address or Domain Name.

3) Server Port

The specified login server port.

4) Heartbeat Interval

The heartbeat time interval (Unit: second)

5) Device Number

Device ID of router.

6) Device Phone Number

The phone number of SIM card insert in router.

7) Device Type

Type of the device, default is router.

You can also remote upgrade the firmware for router, as below.

Remote Upgrade Enable Disable

Server Address

Server Port

Firmware Version

8) Remote Upgrade

Click 'Enable' to enable remote firmware upgrade function.

9) Server Address

Type the server IP address or Domain Name for remote upgrade.

10) Server Port

Type the server port for remote upgrade.

11) Firmware Version

Type the firmware version that you want to upgrade remotely.

3.3.8 Reboot

Reboots the operating system of your device



Click 'Perform Reboot', and a pop-up confirmation box with 'Really Reboot' will display, then click 'OK' to reboot the router.

3.4 Advanced

You can set up some advanced functions here.


3.4.1 Dynamic DNS

If the assigned public IP address of router is dynamic and changes frequently, you can enable DDNS function, while allows you to register a domain to bundle with the IP address, in this case, no matter what the IP address changed, it will direct to your registered domain.

DDNS Enable Disable

Service Type

User Name

User Password 

Host Name

1) Service Type

There are several types of DDNS service supported in router, as below.

- DynDNS.org
- freedns.afraid.org
- ZoneEdit.com**
- No-IP.com
- 3322.org
- easyDNS.com
- TZO.com
- DynSIP.org
- custom
- Oray

2) User Name

The username you register at DDNS service provider.

3) User Password

The password you set up when registering the user name at DDNS service provider.

4) Host Name

The register domain you want to bundle.

3.4.2 QoS Settings

QoS helps you to set up priority for different IP address and port. You can choose 'Priority', 'Express', 'Normal', 'Low'.

You can set up the download and upload speed and click 'Enable' to limit the speed.

WAN

Enable

Classification group

Calculate overhead

Half-duplex

Download speed (kbit/s)

Upload speed (kbit/s)

| Target | Source host | Destination host | Protocol | Ports | Number of bytes | |
|---------------------------------------|----------------------------------|----------------------------------|----------------------------------|------------------------------------|----------------------|---------------------------------------|
| <input type="text" value="priority"/> | <input type="text" value="all"/> | <input type="text" value="all"/> | <input type="text" value="all"/> | <input type="text" value="22,53"/> | <input type="text"/> | <input type="button" value="Delete"/> |

Target: Specify the priority.

Source Host: To match the source IP of data packets.

Destination Host: To match the destination IP of data packets.

Protocol: To match the protocol of data packets.

Ports: If it is TCP/UDP, then the port can be matched.

If above-mentioned are configured, and router will auto implement the related priority level.

3.4.3 Static Routing

Static routing is used to add a routing table entry.

| Interface | Target | IPv4-Netmask | IPv4-Gateway | Metric | |
|----------------------------------|----------------------|--|----------------------|--------------------------------|---------------------------------------|
| | Host-IP or Network | if target is a network | | | |
| <input type="text" value="lan"/> | <input type="text"/> | <input type="text" value="255.255.255.2"/> | <input type="text"/> | <input type="text" value="0"/> | <input type="button" value="Delete"/> |

Interface: To choose which interface you want to add routing.

Target: Can be a host IP, or subnet.

IPv4 Netmask: The netmask of subnet, if the target is host, the netmask shall be

255.255.255.255.

IPv4 Gateway: The address of next-hop gateway address.

Note: this address shall be achievable, or you'll fail to add static routing.

3.4.4 Base Station Location (Option)

Base station location is to locate the TR321 by obtaining the nearest base station number, this function is mainly for rough location of indoor application.

Enter the server IP address and port that you want to report the location of router, then router will auto report its location to server regularly(within the interval time you set).

BS Location Enable Disable

Server Address

Server Port

Report Interval  Seconds

Server Address: The IP address of server that you want the router to report the location, which is based on TCP connection.


Server Port: The port of server.

Report Interval: The interval time for auto report of router location, default value is 60 seconds.

3.4.5 GPS (Option)


GPS location will report GPRMV information regularly, saying longitude and latitude information. And this function is used for accurate location of outdoor open area.

GPS Location Enable Disable

Output Mode 

Server Address

Server Port

Report Interval  Seconds

Server Address: The IP address of server that you want the router to report the location, which is based on TCP connection.

Server Port: The port of server.

Report Interval: The interval time for auto report of router location, default value is 60 seconds.

3.4.6 Traffic Meter

The traffic meter function of TR314 is for traffic statistics from WAN port, meanwhile, it has traffic overflow alarm function. Even if the router is powered off, the traffic statistics will be saved, and when you power on the router, the traffic will be counted based on your last time traffic.

| | |
|---------------------|---|
| Traffic Meter | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Received Bytes | 0.0G |
| Transmitted Bytes | 0.0G |
| Total Bytes | 0.0G |
| Max Volume | <input type="text" value="1024"/> M |
| Inform Phone Number | <input type="text"/> |
| Warning Message | <input type="text" value="reach maximum"/> |

Received Bytes: Current bytes received.

Transmitted Bytes: Current bytes transmitted.

Total Bytes: The total bytes of received bytes and transmitted bytes.

Max Volume: The max volume you set to alarm.

Inform Phone Number: The cell phone number you set for receiving warning message.

Warning Message: The warning message configured phone number will receive once the traffic exceeds the max volume you set, only support English and number input.

3.4.7 Serial Application

The serial port will transfer the data to server, or server will transfer the data to serial port.

| | | |
|--------------|------------|---|
| Baudrate | 115200 | ▼ |
| Databit | 8 | ▼ |
| Stopbit | 1 | ▼ |
| Parity | None | ▼ |
| Flow Control | None | ▼ |
| Protocol | TCP Server | ▼ |
| Listen Port | 5001 | |

1) Baud Rate

There are some baud rate supported below, and default value is 115200.

| |
|--------|
| 115200 |
| 2400 |
| 4800 |
| 9600 |
| 19200 |
| 38400 |
| 57600 |

2) Databit

8 and 7, default value is 8.

3) Stopbit

2 and 1, default value is 1.

4) Parity check

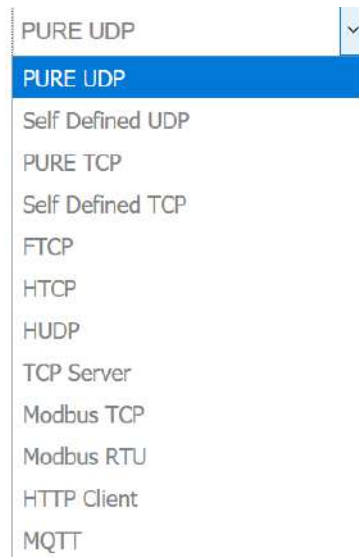
None, Odd Check and Even Check, default value is None.

5) Flow Control

None, Hardware and Firmware, default is None.

6) Protocol

There are some transmission protocols of serial port data, as below.



UDP (DTU): Configured as UDP client, which can be connected to UDP server, specified device number and heartbeat interval is required.

TCP (DTU): Configured as TCP client, which can be connected to TCP server, specified device number and heartbeat interval is required.

PURE UDP: Configured as pure UDP client.

PURE TCP: Configured as pure TCP client.

TCP Server: Configured as TCP server.

Custom TCP: Custom TCP client, it can be format of custom register string, heartbeat string.

If configured as client, a specified address of server is required.

Server Port: Port of server.

Heartbeat Interval: The interval time of heartbeat string sent by client.

Custom Heartbeat String: Hexadecimal format.

Custom Register String: Hexadecimal format.

3.5 VPN

VPN is used to establish a virtual private channel, and all the data in this channel will be encrypted to ensure that data security during transmission.

TR321 support VPN: PPTP, L2TP, OpenVPN and IPSec. PPTP/L2TP are layer 2 VPN, and OpenVPN is VPN based on SSL, while IPSec layer 3 VPN. PPTP/L2TP are more convenient to use, while OpenVPN and IPSec is more complex, as they need complex certification management, meanwhile, they offer more secured encrypted data.

3.5.1 PPTP


You can configure either PPTP client or PPTP server, but not both of them at the same time, as that may cause uncertain issues.

1) PPTP Client

PPTP Client Enable Disable

Server Address

User Name

Password 


Remote Subnet

Remote Subnet Mask

NAT

Enable MPPE Encryption

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

1. PPTP Client

You can enable or disable PPTP client.

2. Server Address

To enter the IP address or Domain Name of PPTP server.

3. User Name and Password

To enter the user name and password provided by server.

4. Remote Subnet

To enter the remote subnet, for example, if LAN of PPTP server is 192.168.2.1, then you can enter remote subnet 192.168.2.0.

5. Remote Subnet Mark

To enter the remote subnet mask, normally it is 255.255.255.0.

6. NAT

If click NAT, all packets come from ppp0, and the source IP of the packets will be replaced as IP of ppp0.

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

Click Default Gateway, then a default route will be established under ppp0, and all the data will go through this route.

2) PPTP Server

PPTP Server Enable Disable

Server Local IP

IP Address Range

Enable MPPE Encryption

DNS1

DNS2

WIN1

WIN2

CHAP Secrets

1. PPTP Server

You can enable or disable PPTP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. DNS1/DNS2

To enter the assigned DNS address.

6. WIN1/WIN2

To enter the WIN address.

7. CHAP Secrets

To create an username and password under CHAP Secrets, format as below,

Username<space>*<space>password<space>*

For example, if you want to create a username: test, password: test, it is as below,

Test * testing *

3.5.2 L2TP


You can also configure either L2TP client or L2TP server, but not both of them at the same time, as that may cause uncertain issues.

1) L2TP Client

L2TP Client Enable Disable

Server Address:

User Name:

Password: 


Remote Subnet:

Remote Subnet Mask:

NAT

Enable MPPE Encryption

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

1. L2TP Client

You can enable or disable L2TP client.

2. Server Address

To enter the IP address or Domain Name of L2TP server.

3. User Name and Password

To enter the user name and password provided by server.

4. Remote Subnet

To enter the remote subnet, for example, if LAN of L2TP server is 192.168.2.1, then you can enter remote subnet 192.168.2.0.

5. Remote Subnet Mask

To enter the remote subnet mask, normally it is 255.255.255.0.

6. NAT

If click NAT, all packets come from ppp0, and the source IP of the packets will be replaced as IP of ppp0.

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

Click Default Gateway, then a default route will be established under ppp0, and all the data will go through this route.

2) L2TP Server

L2TP Server Enable Disable

Server Local IP

IP Address Range eg:10.10.10.100-10.10.10.200

Enable MPPE Encryption

CHAP Secrets

1. L2TP Server

You can enable or disable L2TP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. CHAP Secrets

To create an username and password under CHAP Secrets, format as below,

Username<space>*<space>password<space>*

For example, if you want to create a username: test, password: test, it is as below,

Test * test *

3.5.3 OpenVPN

OpenVPN Enable Disable

Topology

Protocol

Port

Device Type

Peer Address

Authentication Type

Local Tunnel Address

Peer Tunnel Address

Peer Subnet Address

Peer Subnet Mask

Enable NAT

Enable LZO Compress

Cipher Algorithm

MTU

1) OpenVPN

You can enable or disable OpenVPN.

2) Topology

Choose the topology, it can be point to point or subnet

Note: For point to point, a tunnel will be established between 2 devices.

While for subnet, multi devices will be connected to one server.

3) Role

When topology is subnet, you need to choose you want it be a server or client.

4) Protocol

Choose the protocol, it can be UDP or TCP, default is UDP.

5) Port

Enter the port you want to assign to OpenVPN, default port is 1194.

6) Device Type

Choose device type, there are 2 types to choose, TUN and TAP. TUN is layer 3 data encapsulation, while TAP is layer 2 data encapsulation.

7) OpenVPN Server

When you choose server in 角色, you need to enter an IP address or domain name of server.

8) Authentication Type

If topology is subnet, authentication type is certification. If it is point to point, you can choose none, certificate or static secret.

9) TLS Role

When topology is point to point, and authentication type is certification, you need to choose if it is server or client.

3.5.4 IPsec

On IPSEC page, system will display the IPSEC connection and status.

IPSec Enable Disable

| | |
|--------------------------|--|
| Peer Address | <input type="text" value="%any"/> |
| Negotiation Method | <input type="text" value="Main"/> |
| Tunnel Type | <input type="text" value="Site To Site"/> |
| Local Subnet | <input type="text" value="192.168.4.0/24"/> |
| Peer Subnet | <input type="text" value="192.168.5.0/24"/> |
| IKE Encryption Algorithm | <input type="text" value="AES-128"/> |
| IKE Integrity Algorithm | <input type="text" value="SHA-1"/> |
| Diffie-Hellman Group | <input type="text" value="Group14(2048bits)"/> |
| IKE Life Time | <input type="text" value="28800"/> |
| Authentication Type | <input type="text" value="Pre-shared Key"/> |
| Pre-shared Key | <input type="text" value="123456abc"/> |

| | |
|--------------------------|--|
| Local Identifier | <input type="text"/> |
| Peer Identifier | <input type="text"/> |
| ESP Encryption Algorithm | AES-128 <input type="button" value="v"/> |
| ESP Integrity Algorithm | SHA-1 <input type="button" value="v"/> |
| DPD Timeout | <input type="text" value="60"/> <input type="button" value="s"/> seconds |
| DPD Detection Period | <input type="text" value="60"/> <input type="button" value="s"/> seconds |
| DPD Action | Restart <input type="button" value="v"/> |

1) Peer Address

To enter peer IP address or Domain Name, if choose as a server, you don't need to enter it.

2) Negotiation Method

You can choose 'Main' or 'Aggressive'.

3) Tunnel Type

You can choose 'Site to Site', 'Site to Host', 'Host to Host', 'Host to Site'.

4) Local Subnet

Local subnet and mask, like 192.168.10.0/24.

5) Peer Subnet

Peer subnet and mask, like 192.168.20.0/24.

6) IKE Encryption Algorithm

IKE phase encryption method

7) IKE Lifetime

To set up IKE lifetime.

8) Local Identifier

Local identifier of channel, can be an IP address or domain name.

9) Peer Identifier

Peer identifier of channel, can be an IP address or domain name.

10) ESP Encryption Algorithm

The encryption method of ESP.

3.6 View

To check the following system information.

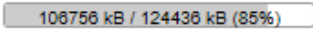
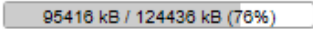

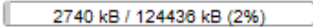
3.6.1 System

Display system information.

System

| | |
|------------------|----------------------------|
| Hostname | router |
| Model | Router |
| SN | 70116229 |
| Firmware Version | 1.0.0.17 |
| Release Time | 2017-03-07 17:36:18 |
| Local Time | 2017-03-20 11:00:34 Monday |
| Uptime | 0h 5m 34s |
| Load Average | 0.11, 0.15, 0.08 |



Memory

| | |
|-----------------|---|
| Total Available |  |
| Free |  |
| Cached |  |
| Buffered |  |

3.6.2 Network

Display network information.

Network

| | |
|-----------------|--|
| IPv4 WAN Status |  Type: lte usb0 Address: 0.0.0.0 Netmask: 255.255.255.255 Gateway: 0.0.0.0 Mac Address: 3a:56:d4:92:c2:a8 Online Status: offline  Signal: 99 dBm Network: - SIM Status: OFF Connect Status: - |
|-----------------|--|

Active Connections 2 / 16384 (0%)

LAN Status

| | |
|-------------|-------------------------------|
| IP Address | 192.168.1.1 |
| Netmask | 255.255.255.0 |
| DHCP Server | Enable |

Wireless Status

| | |
|----------|-------------|
| Wireless | Enable |
| SSID | Router_04fa |

3.6.3 Routing Tables

Display routing tables.

ARP

| IPv4-Address | MAC-Address | Interface |
|---------------|-------------------|-----------|
| 192.168.1.100 | 1c:39:47:3f:28:1d | br-lan |

Active IPv4-Routes

| Network | Target | IPv4-Gateway | Metric |
|---------|----------------|--------------|--------|
| lan | 192.168.1.0/24 | 0.0.0.0 | 0 |

Active IPv6-Routes

| Network | Target | IPv6-Gateway | Metric |
|----------|----------------------|-------------------|----------|
| loopback | 0:0:0:0:0:0:0:0/0 | 0:0:0:0:0:0:0:0/0 | FFFFFFFF |
| loopback | 0:0:0:0:0:0:0:1 | 0:0:0:0:0:0:0:0/0 | 00000000 |
| (eth2) | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0/0 | 00000100 |
| lan | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0/0 | 00000100 |
| (ra0) | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0/0 | 00000100 |
| wan | FF00:0:0:0:0:0:0:0/8 | 0:0:0:0:0:0:0:0/0 | 00000100 |
| loopback | 0:0:0:0:0:0:0:0/0 | 0:0:0:0:0:0:0:0/0 | FFFFFFFF |

3.6.4 System Log

Display system log.



3.6.5 VPN Status

Display VPN status.