

TG451 系列网关说明书	文档编号	产品版本	密级
		V3.0	低
	产品名称: TG451		共 43 页

# TG451 工业网关用户使用说明书

## V3.0

厦门计讯物联科技有限公司

Xiamen Top-Iot Technology Co., Ltd.



## 文档修订记录

日期	版本	说明	作者
2016. 1. 16	V1. 0	第一次发布新版手册	刘伟
2016. 3. 1	V2. 0	修改部分配置文档	刘伟
2016. 4. 15	V2. 1	完善 VPN 配置	刘伟
2017. 5. 15	V2. 2	增加备份版本	林文浩
2018. 7. 7	V2. 3	完善协议	苏振焱
2020. 11. 23	V3. 0	细节完善	卢惠铃

## 目录

<b>第一章 产品简介</b> .....	<b>4</b>
1.1、产品概述 .....	4
1.2、产品外观尺寸图 .....	4
1.3、物理特性 .....	5
<b>第二章 产品安装</b> .....	<b>5</b>
2.1、安装前确认 .....	5
2.2、配件的安装 .....	5
2.3、USB 接口 .....	7
<b>第三章 参数配置</b> .....	<b>9</b>
3.1、设置 .....	10
3.2、安全 .....	19
3.3、管理 .....	23
3.4、高级 .....	28
3.5、VPN .....	34
3.6、查看 .....	40

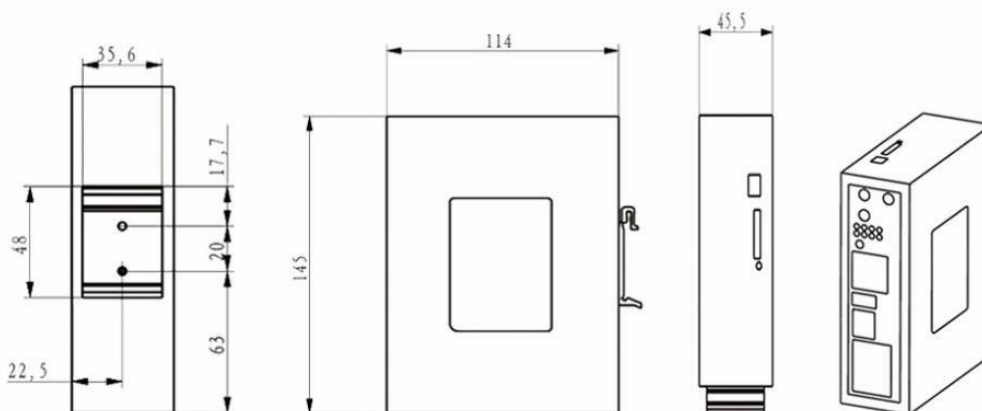
## 第一章 产品简介

### 1.1、产品概述

TG451 系列网关是一款工业级物联网无线网关，设计完全满足工业级标准和工业用户的需求，采用高性能的工业级 32 位通信处理器，软件多级检测和硬件多重保护机制来提高设备稳定性。支持中国电信 4G/3G，中国联通 4G/3G、中国移动 4G/3G 并往下兼容 EDGE、CDMA 1X 及 GPRS 网络，同时支持多种 VPN 协议（OpenVPN、IPSEC、PPTP、L2TP 等）来保证数据传输的安全性。支持 4×LAN、1xWLAN、1xUSB、SIM 卡、2×继电器（可选）、1×RS232（预留 RS485）、1×RS485、2×DI、Wifi 功能、单模双卡（可选）、双模双卡（可选）。



### 1.2、产品外观尺寸图



### 1.3、物理特性

项目	内容
外壳	金属外壳，保护等级 IP30。外壳和系统安全隔离，特别适合工控现场应用
外形尺寸	145*113.7*45.7(不包括天线和安装件)
重量	790g

## 第二章 产品安装

### 2.1、安装前确认

设备的包装包括以下：

- 一台网关主机
- 一个电源
- 一根 4G 天线
- 一根 WiFi 天线
- 一根串口线（选配）
- 一根以太网线
- 两个 6PIN 绿色接线端子
- 一个 2PIN 绿色接线端子

如果有缺失，请联系销售人员

### 2.2、配件的安装

配件接线如下图：



#### ■ SIM 卡安装:

SIM/UIM 卡是无线路由器拨号上网的必要辅件，所以 SIM/UIM 卡必须被正确安装才能达到无线路由器稳定快速上网的效果。

现今运营商办理在 SIM/UIM 卡有多种标准，本路由器使用的是大卡，若办理的是小卡，则需要带着相应卡套方能在本路由器上使用。

安装时先用尖状物插入 SIM/UIM 卡座旁边小黄点，卡槽弹出。SIM/UIM 金属芯片朝外放置于 SIM/UIM 卡槽中，插入抽屉，并确保插到位。

注意：SIM 卡请勿在设备上电的情况下插拔，会导致 SIM 卡损坏

#### ■ 串口连接:

本路由器自带一个 RS232 和和一个 RS485 串口（选配），此串口可用于路由器固件升级、

系统日志查看、串口 DTU 功能等应用。

TG451 串口采用工业级端子接口，标配串口线为一端剥线，一端 DB9 母头，其线序定义定义如下：



#### RS232 线（一端为 DB9 母头）：

线材颜色	对应 DB9 母头管脚	对应网关
蓝色	2 (RX)	(RX)
棕色	3 (TX)	(TX)
黑色	5 (GND)	(GND)

#### RS485 线：

线材颜色	对应网关
红	(A)
黑	(B)

#### USB 接口

接口标准	USB2.0
功能说明	可以接 U 盘存数据或者可以用于升级(支持 32G)

#### 继电器接口 (K0+ K0-、K1+ K1-)

负载能力	2 路继电器输出接口 最大切换电压：30VDC/220VAC 最大切换电流：5A
------	--

功能说明	控制外设供电
------	--------

### DI 接口 (DI0 、 DI1)

输入范围	2 路开关量输入接口（光隔离） 逻辑 0：湿节点 0-3VDC，或干节点导通 逻辑 1：湿节点 5-30VDC，或干节点断开
功能说明	用于检测外设状态

#### ■ 电源安装：

可使用标配 1.5A/12VDC 电源，也可以直接采用 5-35VDC 电源给设备供电，当用户采用外加电源给设备供电时，必须保证电源的稳定性（纹波小于 300mV，并确保瞬间电压不超过 35V）。

#### ■ 天线安装：

天线为路由器增强信号的必要配件，必须正确安装方能达到最优的上网体验。

TG451 天线接口为 SMA 阴头插座。将配套天线的 SMA 阳头旋到 ANT 天线接口上，并确保旋紧，以免影响信号质量。

#### ■ 指示灯说明：

指示灯是路由器运行状态的最直观显示，从指示灯的状态可以方便、快速、较准确地判断路由器的运行状态。

TG451 系列路由器共有 8 种状态指示灯，其状态说明如下：



指示灯	状态	说明
PWR	亮	设备电源正常
	灭	设备未上电
信号强度指示灯	亮一个灯	信号强度较弱
	亮两个灯	信号强度中等
	亮三个灯	信号强度极好
System	闪烁	系统正常运行
	灭	系统不正常



Online	亮	设备已登录网络
	灭	设备未登录网络
Alarm	常亮	SIM/UIM 卡未插到位或损坏
	一秒闪烁一次	路由器读不到模块
	两秒闪烁一次	路由器无法注册网络
	灭	设备无报警
	一秒闪三次	路由器处于固件升级或恢复出厂设置状态
WIFI	灭	WIFI 未启用
	亮	WIFI 已启用
WAN	灭	WAN 网线未连接
	亮	WAN 网线已连接
LAN	LAN1 闪烁	LAN1 口连接正常
	LAN2 闪烁	LAN2 口连接正常
	LAN3 闪烁	LAN3 口连接正常
	LAN4 闪烁	LAN4 口连接正常
	灭	LAN 口未连接

#### ■ 复位按钮说明

Reset 按钮是路由器的复位按钮，其作用是不进入路由器配置页面的条件下直接将路由器的参数配置恢复到出厂默认值。

复位按钮可以直接、有效地解决由于参数配置不当，造成的路由器无法上网、无法登录、无法管理等问题。

TG451 系统无线路由器设有一个 Reset 按钮，位于路由器前面板 LAN 口信号灯附近。在需要将路由器恢复出厂设置时，用尖细硬物插入“Reset”孔位，并轻轻按住，直到所有的指示灯全部熄灭后放开，网关的配置即已恢复为出厂值。

## 第三章 参数配置

用一根网线将路由器的 LAN 口与电脑的网口连接起来；

或使用笔记本电脑或手机等移动终端连接路由器的默认 WIFI 热点 top-iot，默认 WIFI 密码：admin123；

配置你的网卡 IP 为 192.168.1.100；

打开浏览器，输入 192.168.1.1，进入登陆页面；

输入用户名 admin，密码 admin，进入配置页面。

### 3.1、设置

设置主菜单下面包括了需要设置的对象有：WAN， LAN， 无线， 在线探测等子菜单项。主要是用来设置网络相关参数。

#### 3.1.1、WAN 口 [标准版、单模双卡版(选配)]

WAN 口菜单项支持 DHCP/静态 IP/PPPoE/3G/LTE 等连接模式。

选择你需要的模式，点击切换“切换协议”，再配置相关的参数，就可以实现连接。



**服务类型：**指的是网络类型，默认是自动的，如果对网络类型不熟悉，请保持默认值

**APN:**运营商的 apn，不同的运营商有不同的 apn。

中国移动是 cmnet，中国联通是 3gnet，中国电信是 ctnet。

专网卡也会有一个专门的 apn，在办卡时，由运营商提供；具体的 apn 参数可以咨询运营商对于普通的数据卡，这个值可以为空。

通常情况下，保留默认参数即可，路由器将自动启用最合适的 apn。

若运营商有要求特定的 APN 参数，则按照运营商给的 APN 参数配置。

**PIN:** SIM 卡的 PIN 码，请慎重使用，以避免卡被锁住

**PAP/CHAP 用户名：**专网卡时需要输入用户名，其它卡时可以为空

**PAP/CHAP 密码：**专网卡时需要输入密码，其它卡时可以为空

当使用的是非专网卡

**拨号号码：**不同的网络类型对应不同的拨号号码

**认证类型：**如果有用户名，密码，需要指定认证类型。

PAP 是明文认证，CHAP 是握手认证。

要根据运营商的网络来选择认证类型，否则拨号会失败

**WAN 口复用：**当连接模式 3G 或者 LTE 时，可以利用 WAN 口为 LAN 口



### 3.1.2、双卡版（选配）

**双卡功能：**路由器可插入两张 SIM 卡，当卡 1 离线时自动切换卡 2

### 3.1.3、WAN 口 [双备份版（选配）]

路由器 WAN 口接入网线并插入 SIM 卡

物联网通信产品

解决方案提供商

TG451

工业智能网关

---

- > 查看
- > 设置
  - WAN
  - 备份WAN
  - LAN
  - 无线
  - 无线客户端
  - 在线探测
  - 网络诊断
- > 安全
- > VPN
- > 高级
- > 管理
- 退出

### 接口 - WAN

配置网络接口信息。

一般设置

基本设置
高级设置
物理设置

协议

DHCP服务器主机名

保存&应用
保存
复位

物联网通信产品

解决方案提供商

TG451

工业智能网关

---

- > 查看
- > 设置
  - WAN
  - 备份WAN
  - LAN
  - 无线
  - 无线客户端
  - 在线探测
  - 网络诊断
- > 安全
- > VPN
- > 高级
- > 管理
- 退出

### 接口 - SWAN

配置网络接口信息。

一般设置

基本设置
物理设置

协议

服务类型

APN

PIN

用户名

密码

认证类型  无  PAP  CHAP

保存&应用
保存
复位

默认主 WAN 为 DHCP，备份 WAN 为 LTE

注：双备份版只能有线和无线或者无线和有线，如下图所示：

主 WAN	备份 WAN
DHCP 客户端、静态地址、PPPoE 拨号	LTE、3G
LTE、3G	DHCP 客户端、静态地址、PPPoE 拨号

## 网络

IPv4 WAN状态	类型: dhcp eth2.2 地址: 172.17.144.102 子网掩码: 255.255.255.0 网关: 172.17.144.1 MAC地址: 00:52:24:60:7c:02 DNS 1: 172.17.144.1 已连接: 0h 5m 20s
IPv4备份WAN状态	类型: lte usb0 地址: 10.123.164.177 子网掩码: 255.255.255.252 网关: 10.123.164.178 MAC地址: 8e:ed:33:73:77:f9 DNS 1: 218.104.128.106 DNS 2: 58.22.96.66 已连接: 0h 4m 58s 信号: 28 dBm 网络: LTE SIM卡状态: ON IMEI: 357942050465030 连接状态: 已连接

网线和无线拨号同时在线，主 WAN 进行数据传输。

主链路离线自动切换备份链路。

当主链路恢复，自动从备份链路切换回主链路。

### 3.1.4、WAN 口 [双模双卡 (选配)]

路由器插入两张 SIM 卡





- > 查看
- > 设置
  - WAN
  - 备份WAN
  - LAN
  - 无线
  - 无线客户端
  - 在线探测
  - 网络诊断
- > 安全
- > VPN
- > 高级
- > 管理
- 退出

## 接口 - SWAN

配置网络接口信息。

### 一般设置

基本设置

物理设置

协议

服务类型

APN

PIN

用户名

密码

认证类型  无  PAP  CHAP

保存&应用

保存

复位

双模双卡版具有双备份版功能，还支持两张 SIM 进行拨号。

如下图所示：

主 WAN	备份 WAN
LTE、3G	LTE、3G
DHCP 客户端、静态地址、PPPoE 拨号	LTE、3G
LTE、3G	DHCP 客户端、静态地址、PPPoE 拨号

### 网络

IPv4 WAN状态

usb1 类型: lte  
地址: 10.168.158.248  
子网掩码: 255.255.255.240  
网关: 10.168.158.249  
MAC地址: de:27:a5:37:7a:0d  
DNS 1: 218.85.157.99  
DNS 2: 218.85.152.99  
已连接: 0h 0m 15s  
信号: 26 dBm  
网络: LTE  
SIM卡状态: ON  
IMEI: 358433081506975  
连接状态: 已连接

IPv4备份WAN状态

usb1 类型: lte  
地址: 10.97.50.120  
子网掩码: 255.255.255.240  
网关: 10.97.50.121  
MAC地址: de:27:a5:37:7a:0d  
DNS 1: 218.104.128.106  
DNS 2: 58.22.96.66  
已连接: 0h 0m 17s

主卡离线后切换副卡，主卡重新上线后切换回主卡。

两个模块只负责各自的 SIM 卡

### 3.1.5、LAN 口

LAN 口菜单项主要用来配置路由器的 IP，DHCP 服务器的启用，以及分配的 IP 地址的范围。

参数的含义如下：

IPv4 地址：要配置 LAN 口的地址

IPv4 子网掩码：LAN 口地址的掩码

IPv4 网关：指明下一跳路由网关

#### DHCP服务器

关闭 DHCP：点击关闭 DHCP 服务器

开始：分配的 dhcp 服务器的起始地址，比如 100，代表从 192.168.1.100 开始分配

客户数：可分配的 IP 地址数，确保开始数加客户数不能超过 250

租用时间：分配的 IP 的时间长短。

### 3.1.6、LAN 口

无线菜单项主要用来设置无线的 SSID，工作模式，密码等参数，不同的环境可能需要不同的配置参数。



WiFi 2.4G：点击”开启“，启用 WiFi 功能

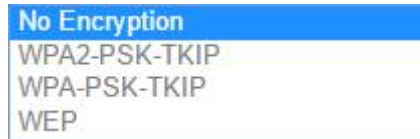
网络名（SSID）：无线网络名

信道：支持 1~13 信道，默认是自动，信道可以自动变化。

模式：目前支持 802.11b，802.11g，802.11bgn。802.11b 速率只能达到 11Mbps，802.11g 可以达到 54Mbps，802.11n 最高，可以达到 300Mbps

加密：当模式为 802.11b 或者 802.11g，只能选择以下几种加密方式：





当模式为 802.11bgn 时，只能选择以下几种加密方式：



密码：预共享密码，用户需要输入这个密码，才能连上。密码最短 8 个字节

隐藏 SSID：当选择隐藏 SSID 则用户看不到这个 SSID，需要手动输入这个 SSID 进行连接

### 3.1.7、在线探测

在一些恶劣的环境，很容易出现网络连接断开的接况。在线探测会定时去检测网络连接状况，如果出现异常，就会重新连接；在尝试了一段时间后，如果还是无法连上，就会重启设备，以达到网络上线的目的。各个参数的含义如下：



**探测类型：**目前支持 ping/traceroute/DNS 三种探测方式。

Ping: ping 会去 ping 一个 IP 或者域名，ping 通否认为在线

Traceroute: traceroute 会去跟踪路由路径，如果可以到达目的地址，则认为在线

DNS: DNS 会解析一个域名, 如果可以解析, 则认为在线

默认使用 ping, 使用 traceroute 相对会比较耗流, DNS 解析较快, 但因为 DNS 有缓存, 导致离线后, 还在线的情况。相对使用 ping 是最合理的。

**主探测服务器:** 优先检测的服务器, 可以是 IP, 也可以是域名

**次探测服务器:** 如果探测主服务器失败, 则可以选择次探测服务器。

**重试次数:** 如果探测失败, 可以指定重试的次数

**重试间隔:** 两次探测之间的时间间隔

**启用重启:** 如果一直不在线, 点击“开启“, 会在指定的时间后重启

**探测失败重启时间:** 指定多长时间不在线, 重启设备

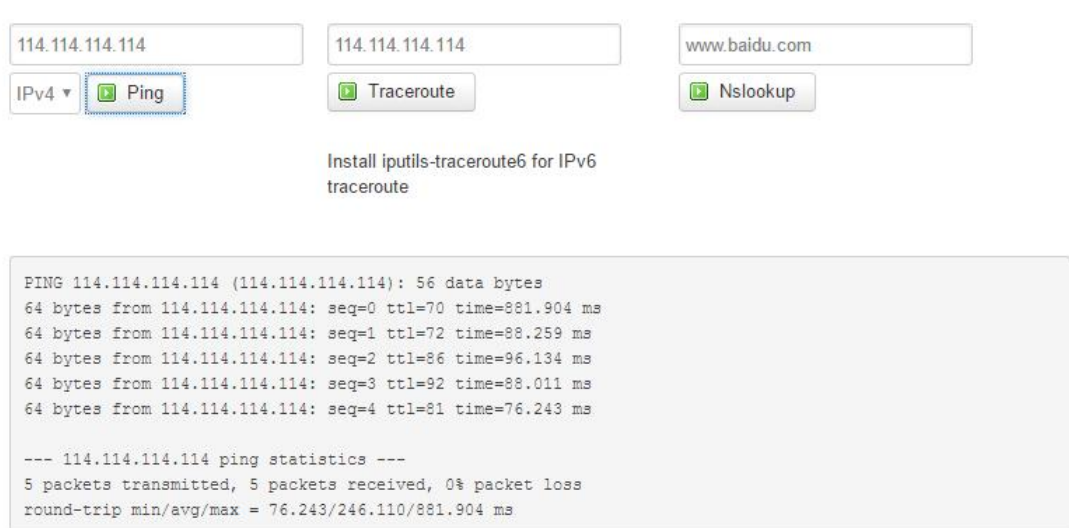
### 3.1.8、网络诊断

支持 ping/traceroute/dnslookup 这三种方式的网络诊断;

ping/traceroute 参数可以是一个域名, 或者是一个 IP, 是用来诊断网络是否在线。

Dnslookup 用来解析一个域名。

点击 ping, 就可以诊断一个地址是否有响应, 如下:



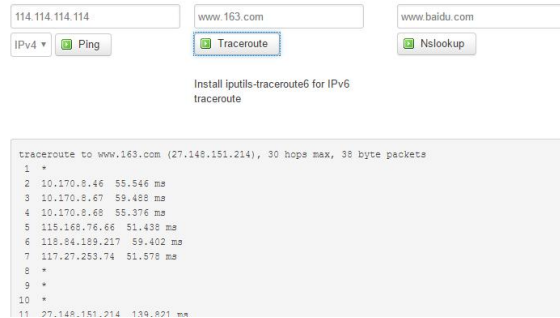
The screenshot shows a web-based diagnostic tool with three input fields: '114.114.114.114', '114.114.114.114', and 'www.baidu.com'. Below the first field, there are buttons for 'IPv4', 'Ping', 'Traceroute', and 'Nslookup'. The 'Ping' button is highlighted. Below the buttons, there is a message: 'Install iputils-traceroute6 for IPv6 traceroute'. The main area displays the output of a ping command:

```

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
    
```

点击 traceroute



点击 nslookup:



## 3.2、安全

安全菜单主要是为了配置防火墙;目前所有从WAN口进来的TCP/UDP连接都会被过滤掉,但是从WAN口出去的包则会放过。如果需要对特定的IP,特定的端口放行的话,则需要配置子菜单项中的某一项。

### 3.2.1、DMZ 主机

DMZ 功能可以把 WAN 口所有端口映射到 LAN 端的某一台主机对应的端口;所有到 WAN 口的访问都会被转到指定的 LAN 端主机。



DMZ: 选择开启的时候, 启用 DMZ 功能

DMZ 主机: 指定要映射的 LAN 端某一台主机的 IP 地址

### 3.2.2、端口转发

相比 DMZ, 端口转发是更精细化控制, 可以把发往某一端口的数据包转发到 LAN 端的某一台主机, 可以实现把不同的端口转到不同的主机。



**名字:** 指定这条规则的名字, 可以起一个有意义的名字

**协议:** 指定要转发的协议, 可以是 TCP, UDP, 或者 TCP/UDP

**外部端口:** 端口转发前的目的端口

**内部 IP 地址:** 要转发的主机 IP 地址

**内部端口:** 端口转发后的目的端口, 一般外部端口与内部端口是一样的, 也可以不一样。

配置完后, 点击“添加”按钮, 新增一条转发规则。点击“保存&应用”按钮, 使规则生效。

### 3.2.3、通信规则

通信规则可以用来打开一些路由器端口，比如需要远程访问路由器的配置页面，可以打开 80 端口，远程 ssh 连接，可以打开 22 端口。



**名字：**指定这条规则的名字，可以起一个有意义的名字

**协议：**指定要转发的协议，可以是 TCP，UDP，或者 TCP/UDP

**外部端口：**指定路由器要打开的端口号。

通信规则还可以用来新建一些访问控制规则，可以从 LAN 到 WAN，也可以从 LAN 到 LAN。



**名字：**指定这条规则的名字，可以起一个有意义的名字

**源区域：**指定数据包从哪里开始

**目标区域：**指定数据包要转到哪里。

点击“添加并编辑”按钮，可以看到更详细的匹配条件。

Rule is enabled  禁用

名字


限制地址


协议

匹配ICMP类型

源区域

任意区域

lan: lan: 

wan: wan: 

源MAC地址


源地址


源端口

目标区域

设备 (输入)

任意区域 (转发)

lan: lan: 

wan: wan: 

目标地址

目标端口

动作

附加参数  传递到iptables的额外参数。小心使用!

**限制地址：**可以指定限制 IPv4, IPv6, 或者 IPv4/IPv6 地址。

**协议：**指定要访问控制的协议，可以是 TCP, UDP, 或者 TCP/UDP

**源 MAC 地址：**指定数据包的源 MAC

**源地址：**指定数据包的源 IP

**源端口：**指定数据包的源端口

**目标地址：**指定数据包的目标 IP

**目标端口：**指定数据包的目标端口

**动作：**如果匹配上面的条件，执行相应的动作。

目前支持的动作有：

接受（允许数据包通过）

丢弃（丢掉数据包）

拒绝（丢掉数据包，并返回一个不可达数据包）

无动作（不做任何处理）

### 3.2.4、自定义

用户可以自定义一些防火墙规则；这些规则是由 iptables 构成，所以需要用户熟悉 iptables 指令才能自定义规则。添加规则时，要加到原有规则的最下面，不要删掉原有的规则。

## 3.3、管理

管理菜单主要是用来管理路由器设备，配置一些与管理相关的参数。

### 3.3.1、系统

系统设置用来系统的主机名，时区，是否允许 telnet，ssh 连接等参数。

主机名	<input type="text" value="router"/>
时区	<input type="text" value="(GMT+08:00)北京,重庆,香港,乌兹"/>
语言	<input type="text" value="中文"/>
开启telnet访问	<input checked="" type="radio"/> 开启 <input type="radio"/> 禁用
开启SSH访问	<input type="radio"/> 开启 <input checked="" type="radio"/> 禁用

主机名：指定路由器的主机名，默认是 GateWay

时区：配置系统的时区，默认是 GMT8

语言：指定配置界面的语言，默认是中文

开启 telnet 访问：点击“开启”，启用 telnet 服务端，默认是开启

开启 SSH 访问：点击“开启”，启用 SSH 服务端，默认是禁用

### 3.3.2、密码

主要用来修改路由器的密码

密码

确认密码

**密码：**指定你要修改的密码

**确认密码：**确认你要修改的密码

如果密码与确认密码不一致，则修改密码会失败。

如果一致，则修改成功，页面会重新跳到登陆页面，让你重新输入用户名与密码

### 3.3.3、时间设置

时间类型包括 RTC, NTP; RTC 掉电后，时间不会丢失; NTP 需要连接到 NTP 服务器，需要有网络连接，断电后，时间不保存。但是 NTP 时间会比 RTC 更精确; RTC 会由于时钟不准，导致时间不准，所以需要手动调节。

当前系统时间 2016-09-18 15:06:49

系统时间类型  ntp  rtc

**当前系统时间：**显示当前路由器的时间

**系统时间类型：**时间类型有 ntp 跟 rtc 两种，选择不同的类型会有不同的配置参数。

当选择 rtc，可以更新 RTC 的时间：

RTC日期  eg: 2016-01-01

RTC时间  eg: 12:00:00

**RTC 日期：**日期的格式一定是：20\*\*-\*\*-\*\*，否则会更新失败

**RTC 时间：**时间的格式一定是： \*\*: \*\*: \*\*, 否则会更新失败。

当选择 ntp 时：

NTP时间服务器

端口

更新间隔  秒



**NTP 时间服务器：**指定 NTP 时间服务器，可以从下拉框中选，也可以自定义

**端口：**NTP 时间服务器端口，默认是 123

**更新间隔：**指定多长时间与服务器同步时间，默认是 600 秒

### 3.3.4、日志设置

日志设置主要用来配置系统的日志输出参数。

输出到设备	<input type="text" value="/var/log/"/>
日志大小	<input type="text" value="64"/> KB
日志服务器	<input type="text" value="0.0.0.0"/>
日志服务器端口	<input type="text" value="514"/>
输出级别	<input type="text" value="调试"/>

**输出到设备：**指定日志要输出到哪里，可以输出到串口，也可以输出到用户指定的文件路径，如果有外接存储设备，还可以存储到外接设备，默认路径：/var/log/。

**日志大小：**指定日志文件的大小，默认是 64KB，最大为 2048KB

**日志服务器：**指定日志服务器的 IP 地址

**日志服务器端口：**指定日志服务器的端口，默认是 514

**输出级别：**目前支持的输出级别有“调试”，“信息”，“注意”，“警告”，“错误”，级别依次递增，级别越高，输出的日志越少

### 3.3.5、备份与恢复

用户可以备份路由器的当前配置，也可以恢复到出厂设置。

备份/恢复当前系统配置文件或重置 OpenWrt(仅squashfs固件有效)。

下载备份:	<input type="button" value="生成备份"/>
恢复到出厂设置:	<input type="button" value="执行复位"/>

**下载备份：**点击“生成备份”，会生成一个“backup-GateWay-2016-\*\*-\*\*.tar.gz”配置文件

**恢复到出厂设置：**点击“执行复位”，会弹出一个“确认放弃所有修改”的确认框，点击“确定”开始恢复出厂设置。

恢复完出厂设置后，也可以把保存的配置导入到路由器，恢复到以前的配置。

上传备份存档以恢复配置。

恢复配置:  未选择任何文件

**恢复配置：**点击“选择文件”，选择你的备份配置文件，点击上传备份。会弹出一个“真的要恢复”的确认框，选择“确定”，开始恢复系统配置。

### 3.3.6、路由器升级

升级路由器之前，务必确认下要升级的固件，是针对你手上的设备。如果升级的固件出错，只能使用电脑接路由器串口，接网线，从 u-boot 升级固件。

#### 刷写新的固件

上传兼容的sysupgrade固件以刷新当前系统。

保留配置:

固件文件:  未选择任何文件

**保留配置：**升级固件后，系统配置不会变

**固件文件：**点击“选择文件”，选择你的固件文件。点击”刷写固件”，会上传固件文件到路由器。

#### 刷新固件 - 验证

固件已上传，请注意核对文件大小和校验值！  
刷新过程切勿断电！

校验值: 19e21582fbee97e020bd7828057b2323  
大小: 9.00 MB  
注意: 配置文件将被删除。

**校验值：**固件的 MD5 检测值

**大小：**固件文件的大小

点击“执行”，开始固件升级

### 3.3.7、远程配置

在这个菜单项中可以指定远程服务器的地址与端口，本设备的设备号等信息。



**远程管理：**选择”开启“，启用远程管理，选择“禁用“，禁用远程管理

**服务器地址：**指定登陆服务器的地址，可以是 IP 地址，也可以是一个域名

**服务器端口：**指定登陆服务器的端口

**心跳包间隔：**指定发送心跳包的时间间隔，单位是秒

**设备号：**指定路由器的设备 ID

### 3.3.8、手动重启

这个菜单项主要用来重启设备。



点击“执行重启”，会弹出一个“真的要重启的确认框”，选择“确定”开始重启

### 3.3.9、定时重启

#### 定时重启

启用定时重启  启用  禁用

定时类型  按周期  按时间

周期间隔  分，最小5分钟

保存&应用 保存 复位

定时重启有两种方式

- 1、周期重启，设置 5 分钟，每 5 分钟就会重启一次。
2. 时间重启：在特定的时间重启，可以设置周一至周天的其中一天，也可以每天。

#### 定时重启

启用定时重启  启用  禁用

定时类型  按周期  按时间

小时

分钟

星期

保存&应用 保存 复位

## 3.4、高级

高级菜单中包含了一些高级功能，一般是不常用的功能。

### 3.4.1、静态路由

静态路由用来添加路由表项

接口	目标	IPv4-子网掩码	IPv4-网关	跃点数	
	主机IP或网络	如果对象是一个网络			
lan	<input type="text"/>	255.255.255.255	<input type="text"/>	0	<input type="button" value="删除"/>

**接口：**指定要在哪一个接口增加路由

**目标：**可以是主机 IP，也可以是子网

**IPv4 子网掩码：**目标的子网掩码，如果目标是主机，子网掩码应该是 255.255.255.255

**IPv4 网关：**下一跳网关地址，注意，这个地址应该是可达的，否则会添加失败

### 3.4.2、串口应用

串口应用会把串口的数据发到服务器，或者服务器把数据发到串口。

波特率	<input type="text" value="115200"/>
数据位	<input type="text" value="8"/>
停止位	<input type="text" value="1"/>
奇偶校验	<input type="text" value="无"/>
协议	<input type="text" value="纯TCP"/>
启用缓存	<input type="checkbox"/> <input checked="" type="checkbox"/> 如果无法连上服务端，缓存数据
服务器地址	<input type="text" value="192.168.1.10"/>
服务器端口	<input type="text" value="9010"/>
连接状态	

**波特率：**目前支持的波特率有：

4800
9600
19200
38400
57600
115200
230400

默认是 115200

**数据位：**数据位有 8 位，7 位两个选择，默认是 8 位

**停止位：**停止位有 2 位，1 位两个选择，默认是 1 位

**奇偶校验：**校验有无校验，奇校验，偶校验，默认是无校验

流控制：流控制有无控制，硬件控制，软件控制三种选择，默认是无控制

帧间隔：串口发送一帧数据时，两个字节的间隔时间

协议：串口数据的传输协议，现在支持以下几种：



纯 UDP：配置为单纯 UDP 客户端，无注册包、无心跳包

纯 TCP：配置为单纯 TCP 客户端，无注册包、无心跳包

自定义 TCP：自定义 TCP 客户端，可以自定义注册包，心跳包的格式

FTCP：配置为 TCP 客户端，有特定格式的注册包和心跳包，需要指定设备号与心跳包间隔

HTCP：配置为 TCP 客户端，数据使用 DCTCP 协议，需要设置 ID 号和 SIM 卡号码等

HUDP：配置为 UDP 客户端，数据使用 DCUDP 协议，需要设置 ID 号和 SIM 卡号码等

TCP 服务端：配置为 TCP 服务端，可以监听某个端口，等待客户的连接

MODBUS TCP：配置为 TCP 服务端，监听某端口，MODBUS TCP 和 MODBUS RTU 做协议转换

MODBUS RTU：配置为 TCP 客户端，监听某端口，MODBUS TCP 和 MODBUS RTU 做协议转换

服务器地址：如果是客户端，需要指定服务端的地址

服务器端口：服务端的端口

心跳包间隔：客户端发送心跳包的时间间隔

自定义心跳包：自定义心跳包的格式，以 16 进制表示

自定义注册包：自定义注册包的格式，以 16 进制表示。

### 3.4.3、花生壳

花生壳这个功能实现了内网 IP 与域名绑定的功能。

服务提供商:	花生壳
状态:	在线
SN:	TOPS4890fc48bc30e8cc
<div style="display: flex; justify-content: space-around;"> <span>登陆管理</span> <span>重置</span> </div>	

点击“登陆管理”，开始配置

点击“重置”会清空以前的配置

### 3.4.4、DI DO

2路继电器接口（预留）：控制外设供电

2路开关量输入接口（光隔离）：用于检测外设状态

## DI DO控制

### DI状态

DI0状态	DI1状态
1	1

DO0设置  高  低

DO1设置  高  低

启用报警  启用  禁用

服务器地址

服务器端口

协议

自定义心跳包

心跳包间隔  0不发送

设备ID  只能一个字节

DI0 状态：

逻辑 0：湿节点 0-3VDC，或干节点导通。逻辑 1：湿节点 5-30VDC，或干节点断开

DO 设置：DO 置高，继电器闭合。DO 置低，继电器断开

启用报警：选择“开启”，启用报警，选择“禁用”，禁用报警

服务器地址：要上报的平台服务器地址

服务器端口：平台服务器的端口

协议：TCP 或 UDP

自定义心跳包：自定义心跳包的格式，以 16 进制表示

心跳包间隔：指定发送心跳包的时间间隔，单位是秒

设备 ID：指定设备的 ID，大小一个字节

### 3.4.5、流量统计

流量统计功能用来统计 WAN 口的流量，并具有流量超阈值告警功能。

断电后，流量也保存。下次开机后会以上次的流量基础上递增。

#### 流量统计

流量统计

已接收字节	已发送字节	总字节
0.0G	0.0G	0.0G

流量统计  启用  禁用

最大量  M

通知电话号码

警告信息

**已接收字节：**从上次清 0 到当前的接收字节数

**已发送字节：**从上次清 0 到当前的发送字节数

**总字节：**已接收与已发送字节的总和

**最大量：**设定达到多少流量报警

**通知电话号码：**指定要报警的电话号码

**警告信息：**要报警的信息，请使用英文，中文会出现乱码

### 3.4.6、基站定位

基站定位是获取最近的基站编号以定位设备的地址，基站定位功能可用于室内环境下的模糊定位。

指定需要上报的服务器的地址与端口，则路由器会定时的上报基站信息。



服务器地址	<input type="text" value="192.168.1.100"/>
服务器端口	<input type="text" value="6004"/>
上报间隔	<input type="text" value="60"/> 秒

**服务器地址：**要上报的平台服务器地址，是基于 TCP 连接

**服务器端口：**平台服务器的端口

**上报间隔：**上报的时间间隔，单位是秒，默认 60 秒

### 3.4.7、GPS 定位

需要 GPS 模块

GPS 定位会定时的上报 GPRMV 信息，即当前经纬度信息。GPS 定位功能可用于户外无遮挡区域的精准定位。

**GPS定位**

GPS定位  启用  禁用

输出模式

服务器地址

服务器端口

上报间隔  秒

设备ID

心跳包间隔  秒

连接状态 -

**输出模式：**可以选择输出到网络或者串口

**服务器地址：**要上报的平台服务器地址，是基于 TCP 连接

**服务器端口：**平台服务器的端口

**上报间隔：**上报的时间间隔，单位是秒，默认 60 秒

**设备 ID：**指定 GPS 的设备 ID

**心跳包间隔：**指定发送心跳包的时间间隔，单位是秒

### 3.4.8、动态 DNS

动态 DNS 用来绑定 WAN 口的公网 IP 跟一个域名。不管 WAN 口的 IP 怎么变，域名总会跟 WAN 口 IP 一一对应。

DDNS  开启  禁用

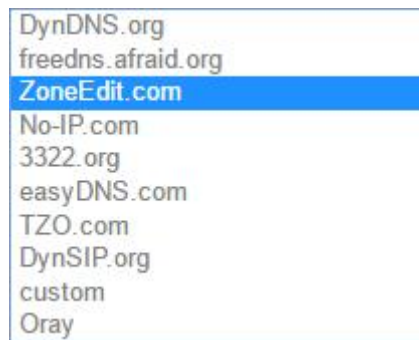
服务类型

用户名

用户密码  

主机名

**服务类型：**目前支持的动态 DNS 有以下几中类型



**用户名：**你在服务提供商注册的用户名

**用户密码：**你在服务提供商注册时设定的密码

**主机名：**要绑定的域名

### 3.5、VPN

VPN 用来创建一条虚拟专用通道，在这条通道上，数据是加密的，以保证数据的安全传输。

可创建 VPN 的软件有 PPTP，L2TP，OpenVPN，IPSec。

PPTP/L2TP 是二层 VPN。OpenVPN 是基于 SSL VPN。IPSec 是三层 VPN。

PPTP/L2TP 使用相对方便，OpenVPN，IPSec 需要复杂的证书管理，所以会比较难用，但是提供更安全的数据加密。

#### 3.5.1、PPTP

PPTP 可配置为客户端或者服务端，注意要么服务端生效，要么客户端生效，否会引起一些不可预测的问题`

PPTP 客户端：点击“开启”，则启用 PPTP 客户端功能

## PPTP设置

设置PPTP

PPTP客户端  启用  禁用

服务器地址

用户名

密码

对端子网  eg: 192.168.10.0

对端子网掩码  eg: 255.255.255.0

NAT

启用MPPE加密

启用静态IP地址

默认网关   所有流量会通过VPN上网

服务器地址：指定 PPTP 服务端的地址，可以是 IP 地址，也可以是域名

用户名：服务器提供的用户名

密码：服务器提供的密码

对端子网：对端的子网，比如 PPTP 服务端的 LAN 端是 192.168.2.1 那么对端子网就是 192.168.2.0

对端子网掩码：子网的掩码，一般是 255.255.255.0

NAT：所以从 ppp0 接口出去的包，包的源 IP 都会替换成 ppp0 的 IP

启用 MPPE 加密：打勾选择 MPPE 加密

启用静态 IP 地址：可以设置 VPN 的静态 IP

默认网关：打勾，则会以 ppp0 创建一条默认路由，所有的数据都会走这条路由

PPTP 服务：点击开启，启用 PPTP 服务端功能

PPTP服务  启用  禁用

服务端本地IP

IP地址范围  eg: 10.10.10.1-10.10.10.254

启用MPPE加密

NAT

DNS1

DNS2

WIN1

WIN2

CHAP密码  eg: test \* test \*

客户端子网  eg: test 192.168.10.0

服务端本地 IP：指定服务端的 IP 地址

IP 地址范围：指定要分配的 IP 地址范围

启用 MPPE 加密：打勾选择 MPPE 加密

DNS1/DNS2：指定要分配的 DNS 地址

WIN1/WIN2：指定 WIN 的地址

CHAP 密码：用来创建客户账号，一条记录对应一个用户。

格式如下：

用户名<空格> \*<空格>密码<空格> \*，

比如增加一个账号：test 密码：test，

则这条记录如：test \* test \*

### 3.5.2、L2TP

L2TP 可配置为客户端或者服务端，注意要么服务端生效，要么客户端生效，否会引起一些不可预测的问题

L2TP 客户端：点击“开启”，则启用 L2TP 客户端功能

#### L2TP设置

设置L2TP

L2TP客户端  启用  禁用

服务器地址

用户名

密码

使用IPsec

预共享密钥

对端ID

对端子网  eg: 192.168.10.0

对端子网掩码  eg: 255.255.255.0

NAT

启用MPPE加密

启用静态IP地址

服务器地址：指定 PPTP 服务端的地址，可以是 IP 地址，也可以是域名

用户名：服务器提供的用户名

密码：服务器提供的密码

使用 Ipsec：勾选使用密匙

预共享密匙：服务器提供的密匙

对端子网：对端的子网，比如 L2TP 服务端的 LAN 端是 192.168.2.1 那么对端子网就是 192.168.2.0

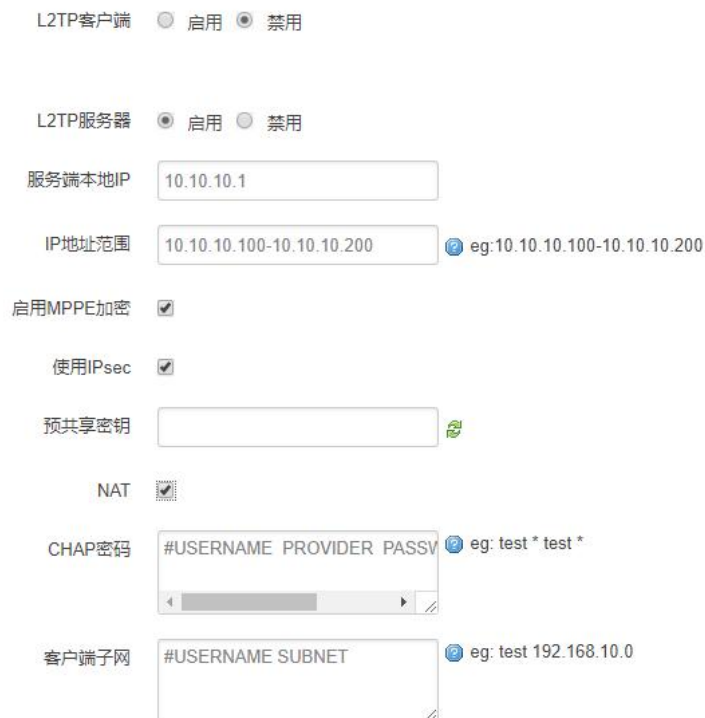
对端子网掩码：子网的掩码，一般是 255.255.255.0

NAT：所以从 ppp0 接口出去的包，包的源 IP 都会替换成 ppp0 的 IP

启用 MPPE 加密：打勾选择 MPPE 加密

默认网关：打勾，则会以 ppp0 创建一条默认路由，所有的数据都会走这条路由

L2TP 服务器：点击开启，启用 L2TP 服务端功能



The screenshot shows a configuration form for L2TP. It includes radio buttons for 'L2TP客户端' (disabled) and 'L2TP服务器' (enabled). There are input fields for '服务端本地IP' (10.10.10.1) and 'IP地址范围' (10.10.10.100-10.10.10.200). Checkboxes are present for '启用MPPE加密', '使用IPsec', and 'NAT'. There is a text input for '预共享密钥' and a dropdown for 'CHAP密码' with a hint '#USERNAME PROVIDER PASSW'. Another text input is for '客户端子网' with a hint '#USERNAME SUBNET'.

服务端本地 IP：指定服务端的 IP 地址

IP 地址范围：指定要分配的 IP 地址范围

启用 MPPE 加密：打勾选择 MPPE 加密

使用 Ipsec：设置密匙

CHAP 密码：用来创建客户账号，一条记录对应一个用户。

格式如下：

用户名<空格> \*<空格>密码<空格> \*，  
 比如增加一个账号：test，密码：test，  
 则这条记录如：test \* test \*

### 3.5.3、OpenVPN

OpenVPN  开启  禁用

拓扑

角色

协议

端口

设备类型

OpenVPN服务端

认证类型

CA  未选择任何文件

公开证书  未选择任何文件

私钥  未选择任何文件

DH  未选择任何文件

对端子网地址

对端子网掩码

启用NAT

启用LZO压缩

加密算法

MTU

OpenVPN：点击“开启”开始 OpenVPN 服务

拓扑：指定 OpenVPN 组网的拓扑结构，可以是点到点，也可以是子网

点对点：两个设备之间建立一条隧道

子网：多个设备连到一个服务器

角色：当拓扑结构是子网的时候，需要指定设备的角色是客户端还是服务端

协议：指定连接是基于 UDP，还是 TCP，默认是 UDP

端口：指定 OpenVPN 使用哪一端口连接，默认端口是 1194

设备类型：设备的类型有 tun, tap, tun 是在三层数据封装，tap 是二层数据封装

OpenVPN 服务端：你角色是客户端的时候，需要指定服务端的地址，可以是 IP，或是域名

认证类型：拓扑结构是子网，认证方式为证书，是点对点，可以无密码，证书或者静态密码

TLS Role：当认证类型是证书认证，需要指定 TLS 的角色是客户端还是服务端

### 3.5.4、IPSec

在 IPSEC 页面，会显示当前设备具有的 IPSEC 连接及其状态。

IPSec	<input checked="" type="radio"/> 开启 <input type="radio"/> 禁用
对端地址	<input type="text" value="%any"/>
协商方法	<input type="text" value="主模式"/>
隧道类型	<input type="text" value="子网到子网"/>
本地子网	<input type="text" value="192.168.4.0/24"/>
对端子网	<input type="text" value="192.168.5.0/24"/>
IKE加密算法	<input type="text" value="AES-128"/>
IKE检验算法	<input type="text" value="SHA-1"/>
Diffie-Hellman组	<input type="text" value="Group14(2048bits)"/>
IKE生存时间	<input type="text" value="28800"/>
认证类型	<input type="text" value="预置密钥"/>
预置密钥	<input type="text" value="123456abc"/>
本地识别码	<input type="text"/>
对端识别码	<input type="text"/>
ESP加密算法	<input type="text" value="AES-128"/>
ESP检验算法	<input type="text" value="SHA-1"/>
DPD超时	<input type="text" value="60s"/>
DPD检测周期	<input type="text" value="150"/>
DPD Action	<input type="text" value="重启"/>

**对端地址：**对端的 IP 地址或域名。如果采用了服务端功能，则该选项不可填；

**协商方法:** 可选择“主模式”和“积极模式”

**隧道类型:** 可选择“子网到子网”、“子网到主机”、“主机到子网”、“主机到主机”等

**本端子网:** 本地子网及子网掩码, 例如: 192.168.10.0/24;

**对端子网:** 对端子网及子网掩码, 例如: 192.168.20.0/24;

**IKE 加密算法:** IKE 阶段的加密方式;

**IKE 生存时间:** 设置 IKE 的生命周期;

**本端识别码:** 通道本端标识, 可以为 IP 及域名;

**对端识别码:** 通道对端标识, 可以为 IP 及域名。

**ESP 加密:** ESP 的加密方式;

## 3.6、查看

查看菜单用来查看系统相关信息

### 3.6.1、系统

显示与系统相关的信息

#### 状态

##### 系统

主机名	router
主机型号	tg451
SN	1806211005
固件版本	1.0.0.31
发布时间	2018-06-25 09:44:31
本地时间	2018-07-25 09:47:26 Wednesday
运行时间	0h 33m 9s
平均负载	0.23, 0.16, 0.17

##### 内存

可用数	104624 kB / 124348 kB (84%)
空闲数	92180 kB / 124348 kB (74%)
已缓存	9652 kB / 124348 kB (7%)
已缓冲	2792 kB / 124348 kB (2%)



### 3.6.2、网络

显示网络信息

#### 网络

IPv4 WAN状态	 类型: lte 地址: 10.73.117.109 子网掩码: 255.255.255.252 网关: 10.73.117.110 MAC地址: 8e:9f:a3:4b:6c:0e DNS 1: 211.136.20.203 DNS 2: 211.136.17.107 已连接: 1h 31m 53s  信号: 28 dBm 网络: LTE SIM卡状态: ON IMEI: 357942050465030 连接状态: 已连接
------------	--

在线状态	在线
活动连接	86 / 16384 (0%)

#### LAN状态

IP地址	192.168.1.1
子网掩码	255.255.255.0
DHCP服务器	启用
MAC地址	00:52:24:60:7c:02

#### 无线状态

无线	启用
SSID	top-iot_7c04
信道	auto
加密	wpa2psk-aes
MAC地址	00:52:24:60:7c:04

#### DHCP分配

主机名	IPv4-地址	MAC-地址	剩余租期
LAPTOP-8S9D298B	192.168.1.212	98:83:89:35:4a:63	10h 26m 32s

### 3.6.3、路由表

显示路由表

#### ARP

IPv4-地址	MAC-地址	接口
192.168.1.100	08-57-00-e5-88-93	br-lan

#### 活动的IPv4-链路

网络	目标	IPv4-网关	跃点数
wan	172.28.120.22	0.0.0.0	0
lan	192.168.1.0/24	0.0.0.0	0
wan	0.0.0.0/0	172.28.120.22	0

#### 活动的IPv6-链路

网络	目标	IPv6-网关	跃点数
loopback	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	00000000
lan	FF02:0:0:0:0:0:1:2	0:0:0:0:0:0:0:0	00000000
(eth2)	FF00:0:0:0:0:0:0:8	0:0:0:0:0:0:0:0	00000100
lan	FF00:0:0:0:0:0:0:8	0:0:0:0:0:0:0:0	00000100
(ra0)	FF00:0:0:0:0:0:0:8	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	FFFFFFFF

### 3.6.4、系统日志

显示系统日志



### 3.6.5、VPN 状态

显示 VPN 的状态



Tel: 0592-6211770

Web: [www.top-iot.com](http://www.top-iot.com)

Mail: [service@top-iot.com](mailto:service@top-iot.com)

总部地址：厦门市软件园三期 F14 栋 27-28 层、C07 栋 14 层

制造中心：厦门市集美区杏滨街道杏前路 189 号 4 楼