

4G 无线路由配置和管理手册	产品版本	页数
	2017-10	共 30 页

4G 无线路由配置和管理手册



北京春笛网络信息技术有限公司

地址：北京市海淀区知春路 23 号 863 软件园量子银座九层
邮编：100191
电话：010-82356575,82356576,82356577
E-mail: service@mailier.com.cn

目录

- 一、 产品外观简介.....3
 - 1 指示灯说明.....3
- 二、 产品概述.....4
 - 1 特点：.....4
- 三、 功能配置指导.....5
 - 1 安装准备.....5
 - 2 登录到配置界面.....6
 - a. 设备概览.....7
 - b. 连接 Internet.....7
 - 3 接口配置.....8
 - a. 移动网络.....8
 - b. WAN 配置.....10
 - c. LAN 配置.....11
 - d. WiFi 配置.....11
 - e. 网桥配置.....12
 - 4 网络应用.....12
 - a. VRRP.....12
 - b. IGMP Proxy.....13
 - c. 端口映射.....13
 - d. 远程服务.....14
 - e. DHCP 配置.....15
 - f. 防火墙配置.....15
 - g. DDNS 配置.....16
 - h. DMZ 配置.....16
 - i. 端口限速.....17
 - 5 WIFI 配置.....17
 - a. 基本设置.....17
 - b. 安全设置.....18
 - 6 VPN 配置.....18
 - a. L2TP.....18
 - b. IPSEC.....19
 - c. 数字证书.....20
 - d. PPTP.....21
 - 7 路由配置.....22
 - a. 路由表.....22
 - b. 添加路由.....23
 - c. 动态路由.....24
 - 8 远程设备配置.....24
 - 9 系统配置.....25
 - a. 系统基本配置.....25
 - b. 恢复出厂配置.....26
 - c. 备份和载入配置文件.....27
 - d. 软件升级.....27
 - e. 重启路由器.....28
 - f. 诊断工具.....29
 - g. 系统日志.....29

一、产品外观简介



实物图

1 指示灯说明



图标	指示灯描述
	电源指示灯，红色 常亮：表示供电正常 常灭：表示供电不正常
	系统指示灯，蓝色 闪烁：表示处理器运行正常 常亮/常灭：表示设备处理器运行不正常
	WiFi 指示灯，蓝色 闪烁：表示 WiFi 开启启动，且运行正常 常灭：表示 WiFi 未开启
	WAN 口 LINK 指示灯，蓝色 常亮：以太网接口连接正常，且无数据收发 常灭：未连接或接口损坏 闪烁：表示以太网接口连接正常，且有数据收发
	LAN1~4 口 LINK 指示灯，蓝色 常亮：以太网接口连接正常，且无数据收发 常灭：未连接或接口损坏 闪烁：表示以太网接口连接正常，且有数据收发

注：SIM 卡插槽，只支持大卡 SIM 卡。

二、产品概述

3G/4G 工业路由器是一种物联网无线通信路由器，利用运营商提供的 3G, 4G 网络为用户提供上网功能。

该产品采用高性能的工业级 32 位通信处理器和工业级无线模块，以嵌入式实时操作系统为软件支撑平台，同时提供 RS232（或 RS485/RS422），以太网接口, WIFI 接口，该产品已广泛应用于物联网产业中，如智能交通、金融、移动 POS 终端、供应链自动化、工业自动化、智能建筑、消防、公共安全、环境保护、气象、数字化医疗、遥感勘测、军事、空间探索、农业、林业、水务、煤矿、石化等领域。

1 特点：

工业级应用设计

采用高性能工业级无线模块
采用高性能工业级 32 位通信处理器
采用金属外壳，特别适合于工控现场的应用
源输入 DC12V/1A
设备尺寸：130mm×31mm×82mm

稳定可靠

硬软双看门狗设计，保证系统稳定
采用完备的防掉线机制，保证数据终端永远在线
SIM/UIM 卡接口内置 15KV ESD 保护
电源接口内置反相保护和过压保护
天线接口防雷保护（可选）

功能强大

支持 VPN（PPTP，L2TP，IPSEC）
支持 APN/VPDN
支持无线视频监控和动态图像传输
支持中国移动，中国联通，中国电信三大运营商的 3G, 4G 网络
支持 DHCP server 及 DHCP client，DDNS，防火墙，NAT，DMZ，端口映射等功能
支持 Telnet、Tftp、Ftp、HTTP 等完善的网络协议
支持设备定时重启

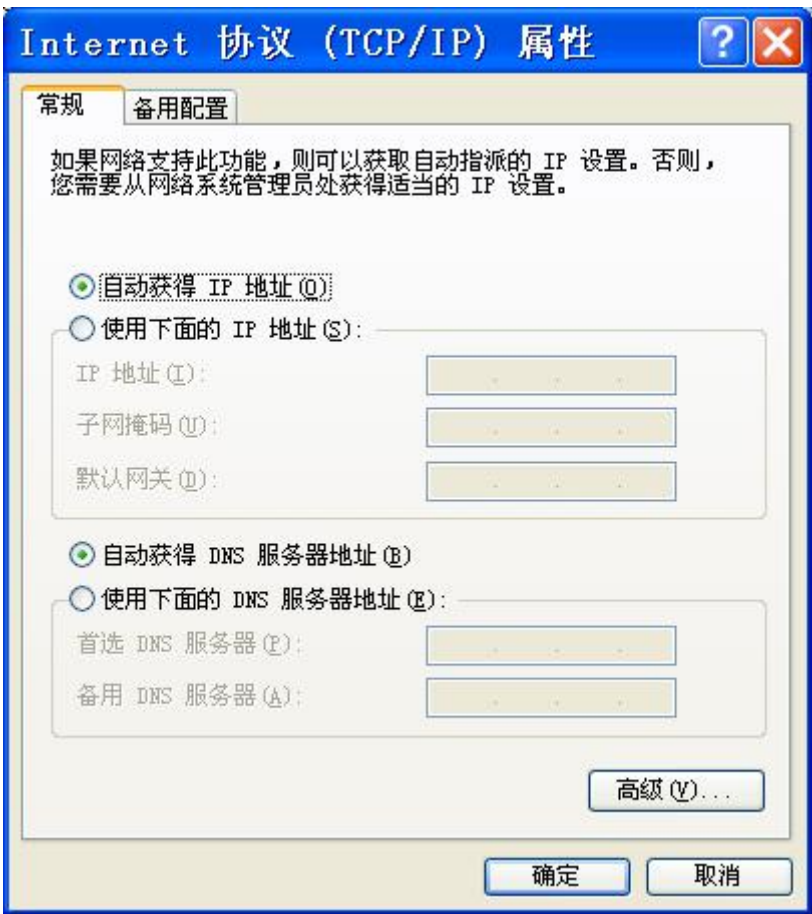
支持 Web 图形界面，命令行，Snmp，TR069 等管理方式

三、功能配置指导

1 安装准备

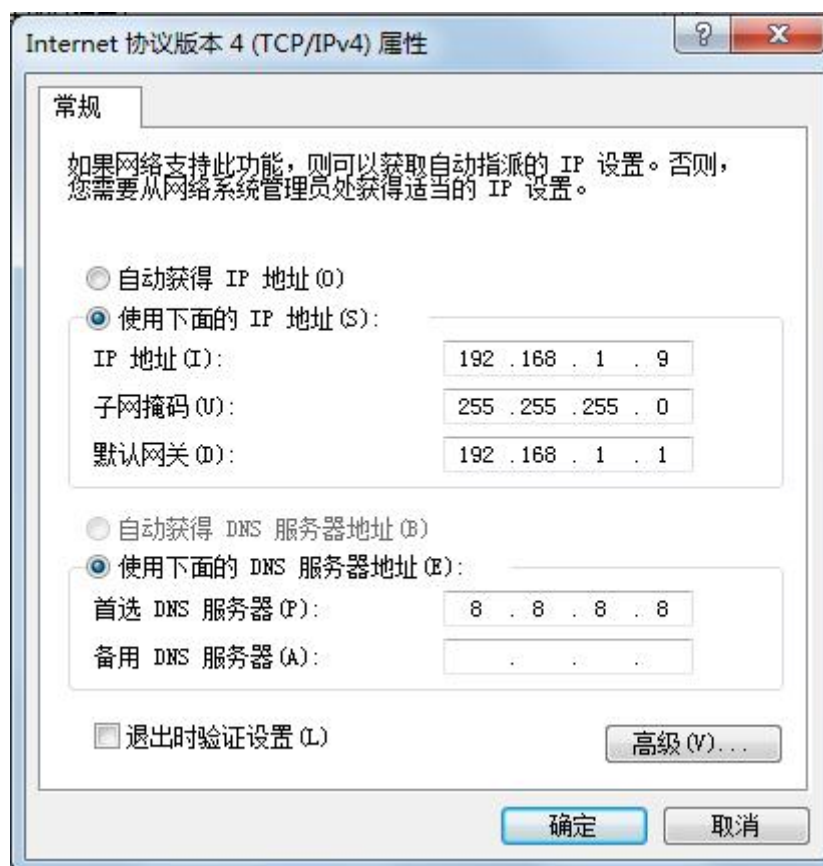
在配置之前，将 PC 的网线接到路由器的 lan 口，PC 机 IP 地址设置（两种方式）

第一种方式：自动获得 IP 地址



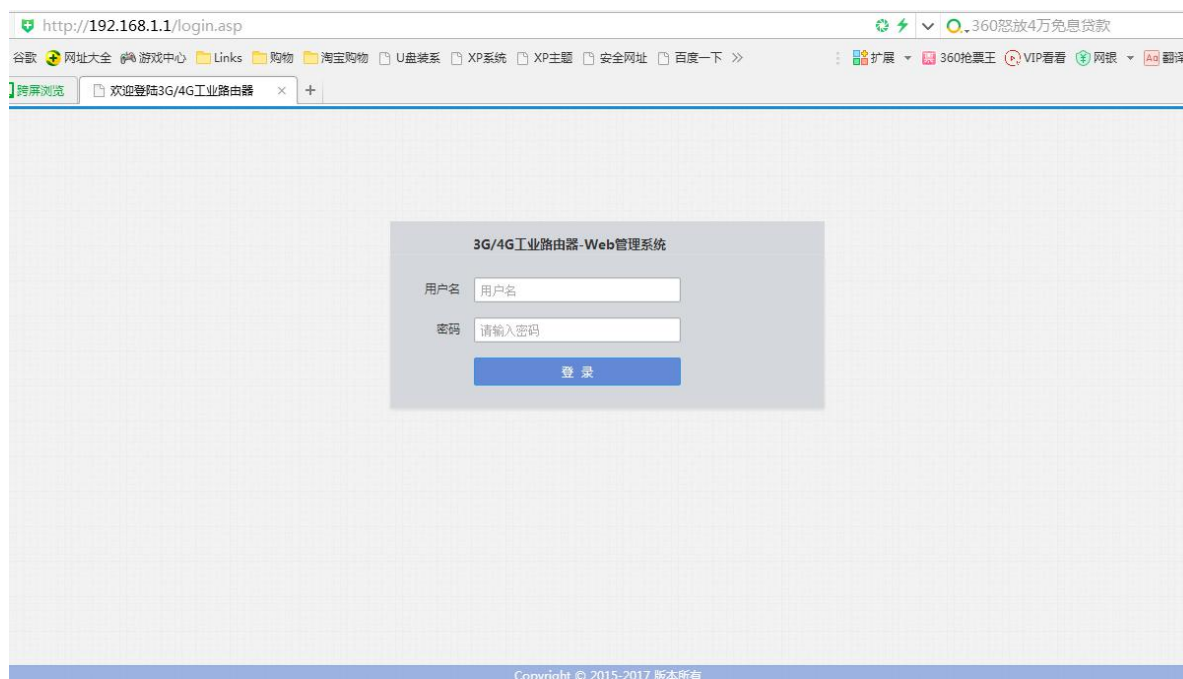
第二种方式：指定 IP 地址

设置 PC 的 IP 地址为 192.168.1.9(或者其他 192.168.1 网段的 IP 地址)，子网掩码设为：255.255.255.0，默认网关设为：192.168.1.1。DNS 设为当地可用的 DNS 服务器。



2 登录到配置界面

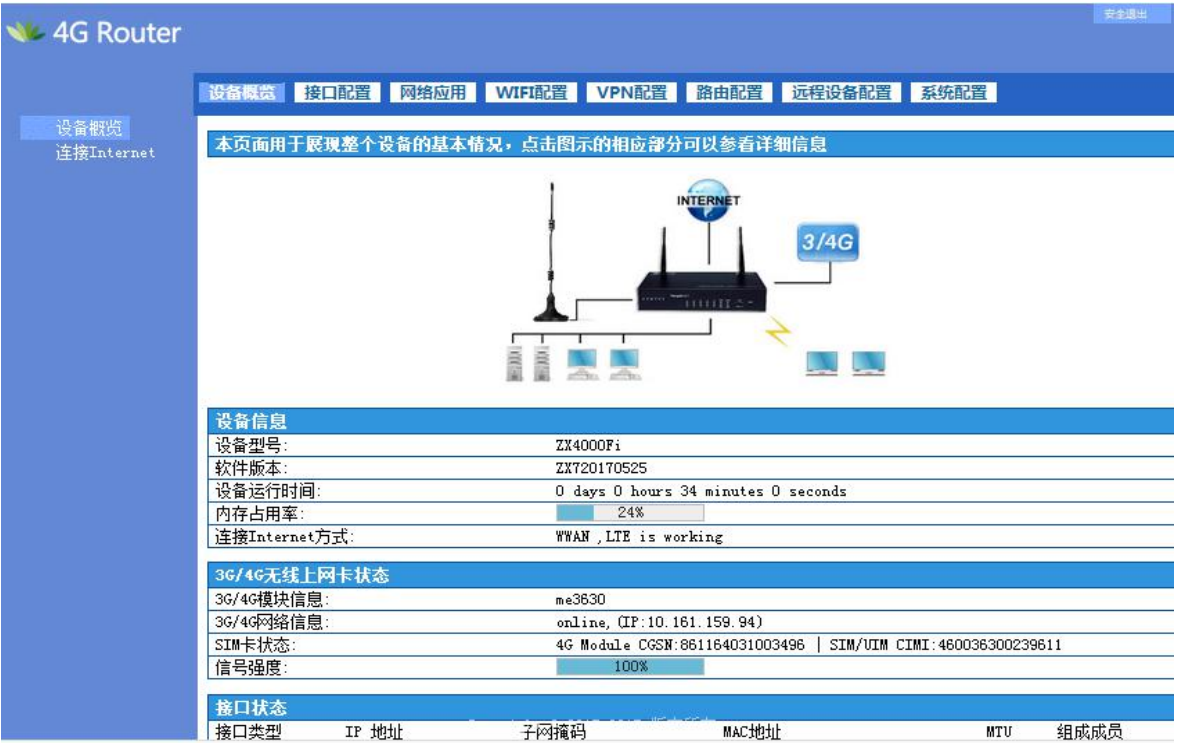
打开浏览器，输入路由器出厂默认的 IP 地址（192.168.1.1）将会出现登陆页面，路由器出厂默认的用户名和密码均为“admin”。



输入用户名和密码，将会进入设备概览界面，该界面的导航栏有两个子页面，设备概览和连接 internet 方式

a. 设备概览

设备概览页面显示了设备的设备基本信息, 3G 或 4G 无线上网卡, 网络接口, vpn 的状态等信息.



b. 连接Internet

目前支持 WWAN(3G/4G) 和 WAN 接入两种模式，默认是 WWAN 接入.

WWAN(3G/4G)： 指通过 3G 或 4G 模块来连接 Internet.

WAN 接入：指通过 WAN 口，手动配置 wan 口 ip 或配置 PPPOE 上网账号来连接 Internet.

注意：在 WAN 接入模式下，wan 口不能加入到网桥中.



3 接口配置

接口配置主要对于移动网络、WAN 口、LAN 口、WIFI 口以及网桥进行相应参数的配置。只有相应的接口配置正确才能保证路由器能够连接到 internet 上。

a. 移动网络

移动网络配置包括 3G, 4G 配置，针对不同的运营商，SIM 卡类型，必须正确填写，否则可能无法连上运营商网络，如下图：

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

移动网络

WANLANWiFi网桥

移动网络

APN:CTLTE

专网卡请根据运营商给的专用APN填写，公网卡移动为：CMNET 联通为：3GNET 电信为：CTLTE

呼叫中心号码:#777

默认移动为：*98*1# 联通为：*99# 电信为：#777 专网卡如有不同请从运营商要求填写

用户名:

专网卡请根据运营商给的用户名填写，没有则不填

密码:

专网卡请根据运营商给的密码填写，没有则不填

mtu:

一般不用填写,默认即可

认证方式:PAP

网络模式:

请根据使用的SIM卡类型填写，4G卡选4G网络，3G卡则要根据不同运营商的3G卡选择相应的3G网络

是否开启网络检测:no

开启心跳检测

检测目标地址:8.8.8.8

填写中心服务器IP地址，如果没有永远在线的中心服务器IP地址，请关闭心跳检测

检测间隔(分钟):1

重置

应用

配置项右边都有相关说明，可对照配置

- APN：运营商的接入点名称 ，公网如下表，专网 APN 请从运营商索要

下表是各运营商的公网上网 APN 对应表：

MCC	MNC	运营商	公网 APN
460	00	中国移动	CMNET/CMWAP
460	02	中国移动	CMNET/CMWAP
460	07	中国移动	CMNET/CMWAP
460	01	中国联通	3GNET/UNINET/UNIWAP
460	03	中国电信	CTNET/CTLTE/CTWAP [推荐 CTLTE]
460	11	中国电信	CTNET/CTLTE/CTWAP [推荐 CTLTE]

- 呼叫中心号码：呼叫到运营商的呼叫号码
- 用户名：公网用户名如下表，专网用户名请从运营商索要
- 密码：公网密码如下表，专网密码请从运营商索要

下表是各运营商的公网默认上网 APN, 呼叫中心号码，用户名，密码对应表：

运营商（ISP）	APN	呼叫中心号码	用户名	密码
中国联通 WCDMA	3GNET	*99#	free	free
中国移动 TD-SCDMA	CMNET	*98*1#	free	free
中国电信 EVDO,CDMA2000	CTLTE	#777	card	card

9

- 是否开启网络检测：如果开启检测，必须正确填写检测目标 IP 地址, 专网客户一般填写对应的数据中心服务器 ip, 公网的话一般填百度等可靠服务器的 ip. 原理就是保证路由器连上网后和对端保持心跳.

b. WAN配置

WAN 口连接类型有两种，第一种静态 IP, 如下图，需要手动填写 wan 口的 ip, 网关，dns 等信息：

4G Router

移动网络
WAN
LAN
WiFi
网桥

设备概览 接口配置 网络应用 WIFI配置 VPN配置 路由配置 远程设备配置 系统配置

WAN设置

WAN口连接类型:	Static	
IP地址:	192.168.2.1	*
子网掩码:	255.255.255.0	*
网关IP地址:		*
数据包MTU (字节):	1500	* (默认是1500，如非必要，请勿修改)
首选DNS服务器:	203.196.0.6	
备用DNS服务器:	220.192.8.58	
开启nat:	yes	
是否加入网桥:	no	

重置 应用

第二种 PPPoE 方式上网 (也就是通常小区 ADSL 拨号上网方式), 如下图，需要填写上网账号，上网密码等.

10

4G Router

安全退出

移动网络
WAN
LAN
WiFi
网桥

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

WAN设置

WAN口连接类型:	PPPoE	
上网帐号:		*
上网密码:		*
连接模式:		
按需拨号间隔(分钟):		*
是否加入网桥:	no	

重置应用

c. LAN配置

LAN 口页面提供了配置 IP, 子网掩码, MTU, 是否开启网卡 NAT, 是否加入网桥等配置项.

4G Router

安全退出

移动网络
WAN
LAN
WiFi
网桥

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

LAN设置

IP地址:	192.168.10.1	*
子网掩码:	255.255.255.0	*
MTU:	1500	*
nat:	yes	
是否加入网桥:	yes	

重置应用

d. WIFI配置

WiFi 口页面提供了配置 IP, 子网掩码, MTU, 是否开启网卡 NAT, 是否加入网桥等配置项.



e. 网桥配置

网桥页面提供了配置 IP, 子网掩码, MTU, 是否开启网卡 NAT 等配置项.



4 网络应用

网络应用部分主要针对一些常用的网络功能的配置，包括 VRRP、IGMP Proxy、链路备份、端口映射、远程服务、DHCP、防火墙、DDNS 以及 DMZ 等功能的配置。

a. VRRP

本页面主要是对热备份（VRRP）的基本设置

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

VRP
IGMP Proxy
端口映射
远程服务
DHCP
防火墙
动态域名
DMZ
端口限速

VRP

开启:	no	
网络接口选择:		
开启虚拟MAC绑定:	no	
虚拟IP:		*
优先级:	100	*
虚拟网络ID (1-255):	255	*
广播时间间隔:	1	*
启用认证:		
认证类型:		
认证密钥:		*

重置应用

b. IGMP Proxy

本页面主要配置 IGMP Proxy 功能，提供上行接口，下行接口选项.

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

VRP
IGMP Proxy
端口映射
远程服务
DHCP
防火墙
动态域名
DMZ
端口限速

IGMP Proxy

开启:	no	
上行接口:	Wan	
下行接口:	Lan	

重置应用

c. 端口映射

端口映射是 NAT 的一种，就是将外网主机的 IP 地址的一个端口映射到内网中一台机器，提供相应的服务。当用户访问该 IP 的这个端口时，服务器自动将请求映射到对应局域网内部的机器上。端口映射有动态和静态之分。本配置是静态的。

本产品的端口映射是关联到具体协议层次，也就是说并不是将内网 ip 端口号和外网 ip 端口号进行映射，而是将内网 ip 和端口映射到外网端口号以及外网接口，同时关注了协议类型。



d. 远程服务

远程服务配置主要对于 telnet 服务、http 服务、syslog 服务以及 ntp 服务的使能配置。

默认 telnet 和 http 都是启动的，telnet 不启动将无法远程登录到设备，http 不启动设备将无法通过 web 进行管理。

网络日志开启可以能够搜集到 log 信息到日志服务器上，便于用户对于感兴趣的 log 信息进行搜集进行分析。

设备支持网络时钟同步机 ntp 的 client，因此可以配置 ntp 使能并将相应的 ntp server 添加进入。



e. DHCP配置

支持 dhcp server 功能。通过该功能可以对内部网络动态分配 ip 地址，可以配置 dhcp 的起始终止 ip、掩码、租约已经 dns 等等。

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

VRP
IGMP Proxy
端口映射
远程服务
DHCP
防火墙
动态域名
DMZ
端口限速

DHCP 设置

是否开启DHCP服务:

yes

网络接口:

Br0

DHCP网络地址:

192.168.1.1

*

DHCP网络掩码:

255.255.255.0

*

DHCP起始IP地址:

192.168.1.100

*

DHCP终止IP地址:

192.168.1.254

*

DHCP缺省网关:

192.168.1.1

*

DHCP地址租期:

30

*(min)

DHCP DNS模式:

static

DHCP主DNS:

203.196.0.6

*

DHCP辅DNS:

220.192.8.58

*

DHCP绑定MAC:

no

绑定MAC地址:

*(XX:XX:XX:XX:XX:XX)

绑定IP地址:

*(X.X.X.X)

重置

应用

f. 防火墙配置

Iptables 规则的配置，主要包含对于源 ip、目的 ip、源 mac、目的 mac、源端口、目的端口、协议等等进行相应的策略配置。

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

VRP
IGMP Proxy
端口映射
远程服务
DHCP
防火墙
动态域名
DMZ
端口限速

防火墙设置

序号	规则	链	协议	源地址	MAC	目的地址	源地址 端口	目的地址 端口	策略
----	----	---	----	-----	-----	------	-----------	------------	----

添加

应用

15

g. DDNS配置

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。 DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

动态域名服务的对象是指 IP 是动态的，是变动的。普通的 DNS 都是基于静态 IP 的，有可能是一对多或多对多，IP 都是固定的一个或多个。但 DDNS 的 IP 是变动的、随机的。随着市场需求的变化，DDNS 需求功能也越来越多，越来越要求方便。

4G Router

安全退出

设备概览

接口配置

网络应用

WIFI配置

VPN配置

路由配置

远程设备配置

系统配置

VRFP

IGMP Proxy

端口映射

远程服务

DHCP

防火墙

动态域名

DMZ

端口限速

DDNS 设置

是否开启动态域名:	no	
动态域名类型:		
动态域名服务器:		*
主机域名:		*
登录用户名:		*
口令:		*

重置

应用

h. DMZ配置

DMZ (Demilitarized Zone)即俗称的非军事区，与军事区和信任区相对应,作用是把 WEB, E-mail, 等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ 可以理解为一个不同于外网或内网的特殊网络区域，DMZ 内通常放置一些不含机密信息的公用服务器，比如 Web、Mail、FTP 等。这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。



i. 端口限速

本页面可以分别设置 Wan 口和 4 个 Lan 口的最大上行速率和最大下行速率



5 WIFI配置

无线路由器产品支持 wifi 功能，对于 wifi 的基本参数以及安全相关信息都可以配置。

a. 基本设置

针对 wifi 的射频、channel、ssid 等等的配置

4G Router

安全退出

基本设置
安全设置

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

无线网络

无线电 开/关	enable ▼	(Status: ON)
无线网络 开/关	enable ▼	(Status: ON)
网络模式	11b/g/n mixed mode ▼	
网络名称 (服务集标识符)	zhongxing	*隐藏 分离
广播网络名称 (服务集标识符)	☒ 启用 ☐ 停用	
AP Isolation	☐ 启用 ☒ 停用	
基本服务集标识符	78:A3:51:2E:EB:9C	
频率 (频道)	2462MHz (Channel 11) ▼	
高吞吐量传送数据流	▼	
高吞吐量接收数据流	▼	

重置应用

b. 安全设置

4G Router

安全退出

基本设置
安全设置

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

"zhongxing"

安全模式	WPA-PSK ▼
Wi-Fi 保护访问 (WPA)	
WPA 算法	☒ TKIP ☐ AES ☐ TKIPAES
通行口令	*****
私钥更新间距	0 seconds
访问策略	
功能	停用 ▼
新增:	

重置应用

6 VPN配置

设备支持 vpn 功能，共支持三种 vpn：L2TP、IPSEC 以及 PPTP。

a. L2TP

L2TP (Layer 2 Tunneling Protocol, 二层隧道协议) 是 VPDN (Virtual Private Dial-up Network, 虚拟私有拨号网) 隧道协议的一种。

VPDN 是指利用公共网络（如 ISDN 或 PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务。即，VPDN 为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

VPDN 采用专用的网络通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

4G Router

L2TP

IPSEC

Certificate

PPTP

设备概览

接口配置

网络应用

WIFI配置

VPN配置

路由配置

远程设备配置

系统配置

L2TP设置

L2TP服务开启:	no	
L2TP服务器IP:		*
L2TP加密口令开启:		
L2TP加密口令:		*
L2TP用户名:		*
L2TP口令:		*
是否指定L2TP IP地址:	no	
L2TP IP地址:		
将L2TP设为缺省路由:	yes	
L2TP内网地址:		
L2TP内网掩码:		
启动NAT服务:	yes	
是否开启L2TP报文监测:	no	
指定L2TP报文监测主机地址:		*
指定L2TP报文监测间隔时间(分钟):		*

重置

应用

b. IPSEC

随着物联网设备不断融入人们的日常生活，物联网设备与互联网的连接就成为不可缺少的条件。那么物联网设备接入互联网时，又如何确保网络通讯的安全呢？而早已演进成熟的 IPsec（Internet Protocol Security，Internet 协议安全性）就成为众多物联网设备确保网络通讯安全的选择。IPsec 有如下两条。

- 1. 保护 IP 数据包的内容。
- 2. 通过数据包筛选及受信任通讯的实施来防御网络攻击。

这两个目标都是通过使用基于加密的保护服务、安全协议与动态密钥管理来实现的。这个基础为专用网络计算机、域、站点、远程站点、Extranet 和拨号用户之间的通信提供了既有力又灵活的保护。它甚至可以用来阻碍特定通讯类型的接收和发送。

其中以接收和发送最为重要。

IPsec 协议工作在 OSI 模型的第三层，使其在单独使用时适于保护基于 TCP 或 UDP 的协议（如安全套接子层（SSL）就不能保护 UDP 层的通信流）。这就意味着，与传输层或更高层的协议相比，IPsec 协议必须处理可靠性和分片的问题，这同时也增加了它的复杂性和处理开销。相对而言，SSL/TLS 依靠更高层的 TCP（OSI 的第四层）来管理可靠性和分片。

4G Router

L2TP

IPSEC

Certifica

PPTP

设备概览

接口配置

网络应用

WiFi配置

VPN配置

路由配置

远程设备配置

系统配置

IPSec 设置

是否开启IPSec:

no

远端IP地址:

安全协议::

模式选择:

序 号

开 启

远端内网地址

远端内网掩码

本地内网地址

本地内网掩码

添加

ISAKMP设置

模式选择:

本地标识类型:

本地标识:

对端标识类型:

对端标识:

加密算法:

哈希算法:

认证方式:

本地证书文件:

本地私钥文件:

对端证书文件:

CA文件名:

Diffie-Hellman组:

启动模式:

生存周期:

SA设置

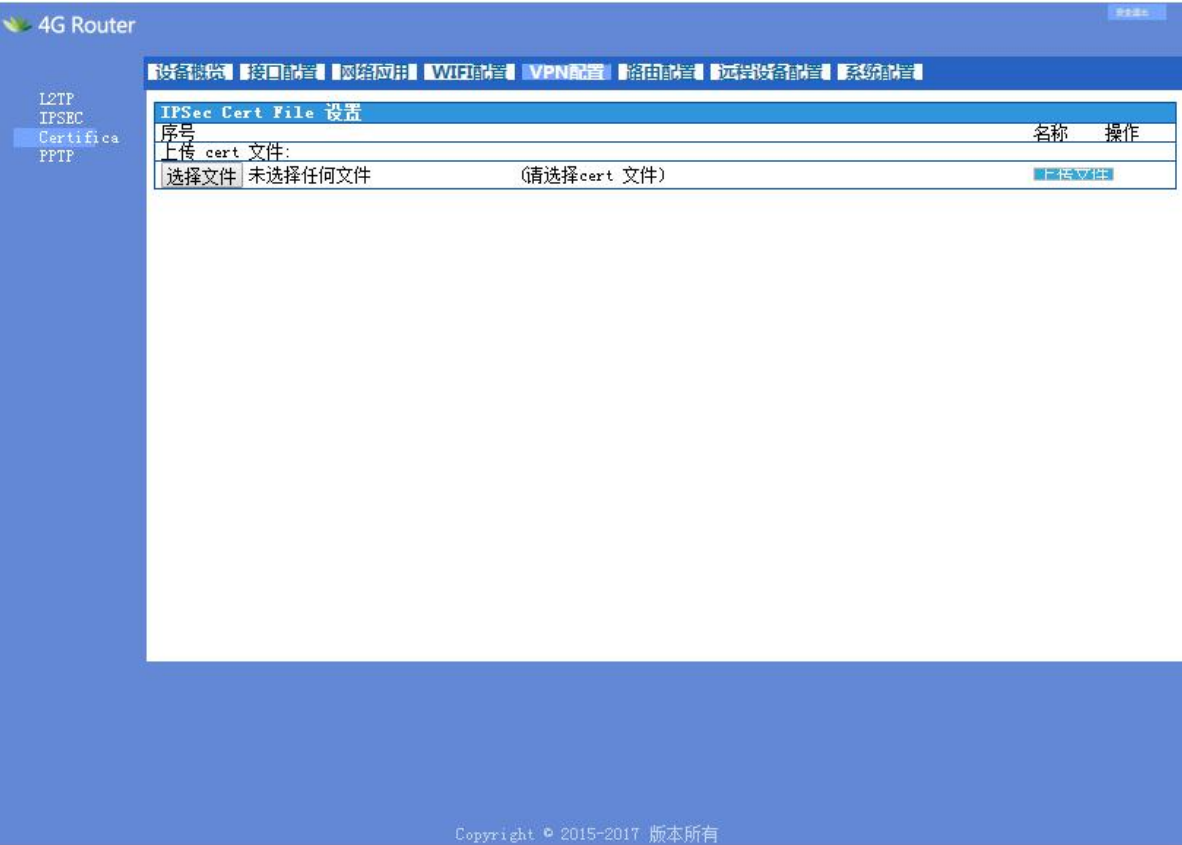
PFS组:

认证算法:

加密算法:

c. 数字证书

可以上传 ipsec 的数字证书用于认证



d. PPTP

PPTP (Point to Point Tunneling Protocol)，即点对点隧道协议。该协议是在 PPP 协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网（VPN），可以通过密码验证协议（PAP）、可扩展认证协议（EAP）等方法增强安全性。可以使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网。

PPTP 主要应用在分公司或者个人用户要连接总部服务器时，通过建立 PPTP 隧道，让用户跟服务器看起来像处于同个局域网内，实现安全通信。

4G Router

L2TP
IPSEC
Certifica
PPTP

设备概览接口配置网络应用WiFi配置VPN配置路由配置远程设备配置系统配置

PPTP设置

PPTP客户端开启:	no
PPTP服务器IP:	
启动NAT服务:	
将PPTP设为缺省路由:	
PPTP内网地址:	
PPTP内网掩码:	
PPTP用户名:	
PPTP口令:	
PPTP IP地址:	
对等PPTP IP地址:	
是否开启PPTP报文监测:	no
指定PPTP报文监测主机地址:	
指定PPTP报文监测间隔时间(分钟):	

重置 应用

Copyright © 2015-2017 版本所有

7 路由配置

路由配置分三个部分：路由表、添加路由以及动态路由。其中路由表是个只读的标项，直接反映了添加路由以及动态路由的配置。

a. 路由表

显示路由表信息.

4G Router

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

路由表
添加路由
动态路由

路由表	目的地址	网关	子网掩码	标志	跳数	参考	状态	接口
	192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2.2
	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
	0.0.0.0	0.0.0.0	0.0.0.0	U	0	0	0	usb0

Copyright © 2015-2017 版本所有

b. 添加路由

添加静态路由

4G Router

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

路由表
添加路由
动态路由

添加路由

序号	规则	目的地址	子网掩码	接口	网关
示例					
X	yes	192.168.0.232	255.255.255.255	WAN	192.168.0.1
添加一条经过WAN到192.168.0.232的路由					
eth2.2:WAN , eth2.1:LAN , br0:BR0 , ra0:WiFi , usb0:LTE					

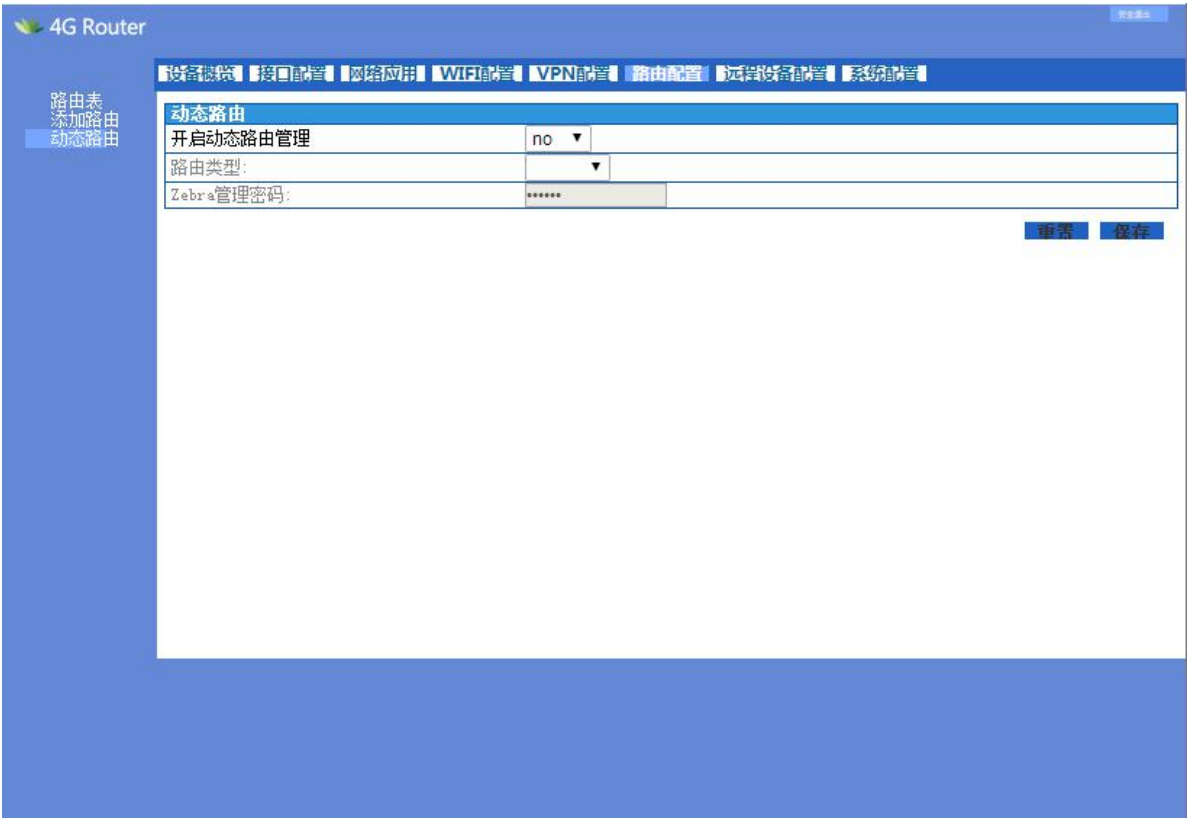
添加保存

Copyright © 2015-2017 版本所有

23

c. 动态路由

支持动态路由协议配置，包括 rip ospf 协议。



8 远程设备配置

该配置是对于 tr069 的配置。

TR-069 是由 DSL 论坛（www.dslforum.org）所开发的技术规范之一，其全称为“CPE 广域网管理协议”。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

现阶段的设备大都提供在 LAN 侧的管理配置接口和界面，因此传统的做法是运营商的维护人员上门进行安装或调试设备，通过 LAN 侧管理接口做一些设备配置或故障诊断的工作。但是，这种一对一的人工服务方式显然运行效率不高而且需要花费大量的人力。随着运营商家庭网络业务的开展，将会有大量的设备需要安置在用户家中，采用过去人工方式对这些设备进行维护和管理将会成为一个巨大的负担。

TR-069 的出现正是为了解决这样一个服务难题，在 TR-069 所定义的框架中，主要包括两类逻辑设备：受管理的用户设备和管理服务器（ACS）。在家庭网络环境下，需要从网络侧进行配置和

管理的设备，一般都是与运营商业务直接相关的设备，比如家庭网关、机顶盒、IP 电话终端等。而所有与用户设备相关的配置、诊断、升级等工作均由统一的管理服务器 ACS 来完成。

4G Router

Tr069配

设备状态

接口配置

网络应用

WiFi配置

VPN配置

路由配置

设备配置

系统配置

TR-069

TR-069开关

EnableDisable

ACS服务器

URL

192.168.1.100/acs

*

用户名

1234

*

密码

*

路由器连接安全配置

外网接口

Wan

用户名

1234

*

密码

*

发送Inform报文

EnableDisable

发送周期

120

Sec* (60-65535, default: 600)

重置

保存

Copyright © 2015-2017 版本所有

9 系统配置

系统配置除了对于路由器基本参数配置外还提供了像软件升级、重启路由器、恢复出厂以及导入导出配置等相应的动作。

a. 系统基本配置

配置路由器的管理员账号密码以及路由器名称，可开启或关闭 WatchDog 功能，WatchDog 功能主要是针对环境恶，设备异常，软件跑飞引起的假死机现象，开启后设备能自动检测到并能及时通过重启修复。

4G Router

安全退出

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

设备名

设备名:Router*

重置提交

修改管理员密码

用户名:admin*

口令:*****

确认口令:*

重置提交

WatchDog

WatchDog:☒ 开启 ☐ 关闭

重置提交

b. 恢复出厂配置

恢复系统默认配置

4G Router

安全退出

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

恢复出厂模式

警告:
恢复出厂设置将会丢失先前的配置，确认恢复出厂设置吗?

恢复出厂

c. 备份和载入配置文件

可以将当前配置以 txt 文本文件形式保存到本地，同时也可以上传配置文件到设备中。



d. 软件升级

提供软件在线升级功能。

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

软件升级

请选择路由器固件升级文件(约2分钟):

选择文件

未选择任何文件

上传

e. 重启路由器

对路由器进行重启, 另外可以设置路由器自动重启功能.

4G Router

安全退出

设备概览接口配置网络应用WIFI配置VPN配置路由配置远程设备配置系统配置

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

重启路由器

警告:

确定要重启路由器吗?

重启路由器

自动重启路由器计划

定时重启

no

每隔

小时设备自动重启

每日

时

分

设备自动重启

保存

28

f. 诊断工具

通过 ping 包进行测试网络连通性以及时延。

4G Router

安全退出

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

设备概览 接口配置 网络应用 WIFI配置 VPN配置 路由配置 远程设备配置

系统配置

诊断工具

IP 地址/域名:		*
Ping 包数目:		*(1-50)
Ping 包大小:		*(4-1472 KB)

路由器已经就绪.....

诊断结果:

重置

保存

g. 系统日志

可以将日志信息记录下来同时可以下载到本地.

系统基本配
恢复出厂设
备份和载入
软件升级
重启路由器
诊断工具
系统日志
存储管理

设备概览 接口配置 网络应用 WIFI配置 VPN配置 路由配置 远程设备配置

系统配置

日志管理

拨号日志 [下载]

Time:Thu Jan 1 08:00:32 1970 Lte Up:10.161.159.94

系统日志 [下载]

```
Jan 1 11:06:06 (none) user.info syslog: usb0 rm log
Jan 1 11:06:06 (none) user.info syslog: usb0 check success
Jan 1 11:07:06 (none) user.info syslog: usb0 rm log
Jan 1 11:07:06 (none) user.info syslog: usb0 check success
Jan 1 11:08:06 (none) user.info syslog: usb0 rm log
Jan 1 11:08:06 (none) user.info syslog: usb0 check success
Jan 1 11:09:06 (none) user.info syslog: usb0 rm log
Jan 1 11:09:06 (none) user.info syslog: usb0 check success
Jan 1 11:10:06 (none) user.info syslog: usb0 rm log
Jan 1 11:10:06 (none) user.info syslog: usb0 check success
Jan 1 11:11:06 (none) user.info syslog: usb0 rm log
Jan 1 11:11:06 (none) user.info syslog: usb0 check success
Jan 1 11:12:06 (none) user.info syslog: usb0 rm log
Jan 1 11:12:06 (none) user.info syslog: usb0 check success
Jan 1 11:13:06 (none) user.info syslog: usb0 rm log
Jan 1 11:13:06 (none) user.info syslog: usb0 check success
Jan 1 11:14:06 (none) user.info syslog: usb0 rm log
Jan 1 11:14:06 (none) user.info syslog: usb0 check success
Jan 1 11:15:06 (none) user.info syslog: usb0 rm log
Jan 1 11:15:06 (none) user.info syslog: usb0 check success
Jan 1 11:16:06 (none) user.info syslog: usb0 rm log
Jan 1 11:16:06 (none) user.info syslog: usb0 check success
Jan 1 11:17:06 (none) user.info syslog: usb0 rm log
Jan 1 11:17:06 (none) user.info syslog: usb0 check success
Jan 1 11:18:07 (none) user.info syslog: usb0 rm log
```