

RG2000-V8 系列无线路由器 使用说明书

2018-07

版本信息

RG2000-V8 系列无线路由器

使用说明书

版本： RG2000-V8-V1.00-201807

目 录

第一章 约定说明.....	1
1.1 目的.....	1
1.2 适用范围.....	1
1.3 本书约定.....	1
1.4 专业术语.....	2
第二章 产品介绍.....	4
2.1 产品概述.....	4
2.2 功能特点.....	4
2.3 硬件规格.....	5
2.4 设备面板.....	6
2.5 安装说明.....	8
2.6 串口线缆.....	11
第三章 联机登录.....	13
3.1 环境要求.....	13
3.2 使用准备.....	13
3.3 配置计算机.....	13
3.4 通过 Telnet 登录系统.....	16
3.5 通过 Console 口登录系统.....	16
3.6 通过 WEB 登录系统.....	17
第四章 配置操作.....	19
4.1 设备状态.....	19
4.1.1 设备基本状态.....	19
4.1.2 WAN 接口状态.....	21
4.1.3 路由状态.....	21
4.2 网络配置.....	22
4.2.1 接口管理.....	22
4.2.2 端口管理.....	27
4.2.3 VLAN 管理.....	27
4.2.4 WIFI 配置.....	28
4.2.5 DHCP 配置.....	30
4.2.6 链路探测.....	31
4.3 路由配置.....	32
4.3.1 静态路由.....	32
4.3.2 策略路由配置.....	33
4.3.3 OSPF 配置.....	34
4.3.4 IS-IS 配置.....	35
4.3.5 RIP 配置.....	37
4.4 VPN 配置.....	37
4.4.1 GRE 配置.....	37
4.4.2 IPSec VPN.....	39

4.4.3	L2TP.....	40
4.4.4	PPTP.....	43
4.5	网络安全.....	45
4.6.1	攻击防御.....	45
4.6.2	访问策略配置.....	45
4.6.3	PAT 配置.....	48
4.6.4	DMZ 配置.....	49
4.6.5	SNAT 配置.....	50
4.6.6	UPNP 配置.....	51
4.6.7	QOS 配置.....	52
4.6.8	IP-MAC 绑定.....	55
4.6.9	ALG 配置.....	55
4.6	系统维护.....	56
4.7.1	系统时间.....	56
4.7.2	SNMP 配置.....	56
4.7.3	WEB 管理.....	57
4.7.4	TELNET 设置.....	58
4.7.5	软件升级.....	60
4.7.6	配置管理.....	61
4.7.7	设备重启.....	61
4.7.8	日志管理.....	62
4.7.9	通信检测.....	63
4.7.10	激活参数.....	64
第五章	CLI 命令行介绍.....	65
5.1	CLI 概述.....	65
5.2	CLI 命令常识及使用技巧介绍.....	66
5.2.1	命令帮助.....	66
5.2.2	命令简写.....	67
5.2.3	命令补全.....	67
5.2.4	命令错误提示.....	67
5.2.5	no 命令.....	68
5.2.6	历史命令.....	68
5.3	CLI 命令详细介绍.....	68
5.3.1	基础命令.....	68
5.3.2	接口配置.....	69
5.3.3	端口配置.....	73
5.3.4	DHCP 服务器配置.....	74
5.3.5	VLAN 配置.....	75
5.3.6	DLDP 配置.....	75
5.3.7	BFD 配置.....	76
5.3.8	路由配置.....	76
5.3.9	RIP 路由配置.....	77
5.3.10	OSPF 路由配置.....	78
5.3.11	ISIS 路由配置.....	78

5.3.12 防火墙配置.....	79
5.3.13 访问策略配置.....	80
5.3.14 静态 ARP 配置.....	81
5.3.15 PAT 配置.....	81
5.3.16 DMZ 配置.....	82
5.3.17 ALG 配置.....	82
5.3.18 UPNP 配置.....	83
5.3.19 IPSEC 配置.....	83
5.3.20 GRE 配置.....	84
5.3.21 L2TP 配置.....	85
5.3.22 PPTP 配置.....	89
5.3.23 MPLS 配置.....	90
5.3.24 QOS 参数配置.....	93
5.3.25 GPON 参数配置.....	96
5.3.26 SNMP 参数配置.....	96
5.3.27 NTP 配置.....	97
5.3.28 WEB 配置.....	97
5.3.29 系统信息.....	98
5.3.30 日志信息.....	98
5.3.31 软件升级.....	99
5.3.32 设备参数.....	99
5.3.33 端口镜像命令.....	99
5.3.34 测试工具命令.....	99
5.3.35 主机名及密码修改.....	100
5.3.36 系统时间.....	100
5.3.37 重启设备.....	100

第一章 约定说明

1.1 目的

本说明书用于指导 RG2000-V8 系列 4G 路由器的安装调试、使用及维护。

1.2 适用范围

本说明书适用的对象包括：

- ✓ 具有一定计算机通讯、网络、电子技术等知识的人员；
- ✓ 具有网络设备管理经验的人员。

1.3 本书约定

表 1-1 图形约定表




约定项	释义说明
	说明： 以本标志开始的文本是对正文的补充说明。
	注意： 以本标志开始的文本提醒应注意的事项。
	危险： 以本标志开始的文本提醒危险事项。

表 1-2 文本约定

约定项	释义说明
RG2000-V8	指 RG2000-V8 系列 4G 无线路由器产品。
\	用于隔离多级目录。
<XX-XX>	为 CLI 命令行的表示格式之一，表示输入一个该范围的数字，例如<1-4094>表示输入一个 1 至 4094 范围的数字。
{ XX XX }	为 CLI 命令行的表示格式之一，表示命令行中多选一的命令字，多个命令字在大括号“{}”内用竖线“ ”分隔。
(XX XX)	为 CLI 命令行的表示格式之一，表示多选一，例如 (enable disable)表示 enable 与 disable 二选一。
[XX]	为 CLI 命令行的表示格式之一，表示命令行中的可选命令字。

1.4 专业术语

表 1-3 专业术语

术语	释义说明
APN	接入点名称 Access Point Name
BFD	双向转发检测机制 Bidirectional Forwarding Detection
CDMA	码分多址 Code Division Multiple Access
CLI	命令行界面 Command Line Interface
DHCP	动态主机配置协议 Dynamic Host Configuration Protocol
DLDP	设备连接检测协议 Device Link Detection Protocol
DMZ	隔离区 Demilitarized Zone
DNS	域名系统 Domain Name System
GPRS	通用分组无线业务 General Packet Radio Service
GPS	全球定位系统 Global Positioning System
GRE	通用路由封装 Generic Routing Encapsulation
GSM	全球移动通信系统 Global System for Mobile Communications
IMEI	国际移动设备身份码 International Mobile Equipment Identity
IMSI	国际移动用户识别码 International Mobile Subscriber Identification Number
IP	互联网协议 Internet Protocol
IPv4	IP 协议第 4 版 IP version 4
IPv6	IP 协议第 6 版 IP version 6
IPSEC	IP 安全协议 IP Secure Protocol
L2TP	第二层隧道协议 Layer 2 Tunneling Protocol
LAN	局域网 Local Area Network
LTE	长期演进 Long Term Evolution
MTU	最大传输单元 Maximum Transmission Unit
NAT	网络地址转换 Network Address Translation
NTP	网络时间协议 Network Time Protocol

术语	释义说明
OSPF	开放式最短路径优先 Open Shortest Path First
PAP	密码授权协议 Password Authentication Protocol
PAT	端口地址转换 Port Address Translation
QoS	服务质量 Quality of Service
RIP	路由信息协议 Routing Information Protocol
SIM	用户标识模块 Subscriber Identity Module
SNMP	简单网络管理协议 Simple Network Management Protocol
TCP	传输控制协议 Transmission Control Protocol
TDMA	时分多址 Time Division Multiple Access
UDP	用户数据报协议 User Datagram Protocol
UMTS	通用移动通信系统 Universal Mobile Telecommunication System
VPN	虚拟专用网 Virtual Private Network
WAN	广域网 Wide Area Network

第二章 产品介绍

2.1 产品概述

RG2000-V8 无线路由器是面向全行业推出的新一代网络产品，融合了 4G 接入技术、WIFI 技术、路由技术、交换技术、安全技术等多种网络应用技术，全线兼容 4G/3.5G/3G/2.5G 网络，自带 8 个 10/100/1000M 以太网接口及 2 个 100/1000M SFP 光接口，支持 802.11B/G/N WIFI。旗舰级配置、VPN 链接、工业级设计，可轻松组建高速、稳定的有线、无线传输网络，并支持数据采集，利用公用 4G/3G 网络为用户提供无线长距离数据传输功能。

工业级的设计，严苛的元器件选用，使得设备耐高温、低温，在室外、车载等复杂环境下依然能够稳定工作，为用户提供高可靠、高性价比的无线安全接入组网方案。产品通过国家无线电管理委员会认证 (SRRC 认证)，并获得工信部颁发的进网许可证，可广泛应用于金融，交通，安防，水利，环保，电力，邮政，气象，能源，下一代物联网等行业。

RG2000-V8 无线路由器产品图片如下：



图 2-1 RG2000-V8 产品图片

2.2 功能特点

RG2000-V8 无线路由器功能特点：

- 支持 8 个 10/100/1000M 以太网接口；
- 支持 2 个 100/1000M SFP 光接口；
- 支持多种协议：TCP/IP，UDP，HTTP，TELNET，ICMP，DHCP，PPPOE，DNS 等；

- 支持静态路由、策略路由及 RIP/OSPF/ISIS 动态路由；
- 支持 CLI, WEB 及 SNMP 集中网管；
- 支持 NAT 功能；
- 支持防火墙，包过滤等功能；
- 支持配置 GRE、L2TP VPN、PPTP VPN、IPSec VPN 等 VPN 功能；
- 支持 BFD、DLDP 等链路探测功能，并能够根据探测的结果快速向备份链路切换；
- 支持日志功能。

2.3 硬件规格

RG2000-V8 路由器硬件规格如表 2-1 所示：

表 2-1 硬件规格

序号	名称	说明
1	产品型号	RG2000-V8
2	固定端口	8 个 10/100/1000M 以太接口 2 个 100/1000M SFP 光接口 1 个 SIM 卡插槽 2 个 4G 天线接口 2 个 WIFI 天线接口 1 个 GPS 天线接口 1 个 FUNC 按钮 1 个标准 3 芯电源接口
3	4G/3G/2G 接入	支持全网：TDD-LTE、FDD-LTE、TD-SCDMA、UMTS、EVDO、EDGE、CDMA1x、GPRS
4	WIFI 模块	802.11 b/g/n, 300Mbps 双通道
5	整机尺寸	270mm*154mm*33mm(不含天线、挂件)
6	结构设计	高强度金属外壳
7	整机功耗	≤15W
8	电源输入	DC12V 1.5A
9	工作环境温度	-20~+70° C
10	工作湿度	10~95%RH

序号	名称	说明
11	存储温度	-40~+70° C
12	安装方式	桌面式、壁挂式、导轨式

2.4 设备面板

1. 设备前面板

RG2000-V8 无线路由器设备前面板如下图所示：



图 2-2 设备前面板示意图

前面板描述如表 2-2 所示：

表 2-2 设备前面板

序号	名称	说明
1	V+ V- PGND	标准三芯电源接口, PGND 为电源地。
2	USB	标准 USB2.0 接口。
3	Console	设备串口。
4	SFP0-SFP1	SFP 光接口, 可支持 1000M 或 100M 的光模块, 通常用作设备 WAN 口。
5	GE0-GE7	千兆以太网口, 可任意配置为 WAN 口/LAN 口, 默认均为设备 LAN 口。 (1) 绿灯常亮表示网口已连接, 绿灯闪烁表示有数据传输, 绿灯灭则表示网口未连接。 (2) 黄灯亮表示当前连接速率为 1000Mbps, 黄灯灭表示当前连接速率为 100Mbps 或者 10Mbps。
6	FUNC	功能按键。设备运行过程中, 持续按下 5 秒或以上, 设备将恢复出厂默认参数。设备恢复出厂默认参数后, 需断电重启生效。
7	RSSI	4G 信号强度指示灯, 共 3 个 LED 灯。 (1) 3 个 LED 灯全亮, 表示信号强度非常好; (2) 2 个 LED 灯亮, 表示信号强度良好;

序号	名称	说明
		(3) 1 个 LED 灯亮，表示信号强度较弱； (4) 3 个 LED 灯全灭，表示信号强度非常弱或者无信号。
8	USB	USB 接口连接指示灯，常亮表示 USB 已连接，熄灭表示 USB 未连接。
9	WIFI	WIFI 指示灯，常亮表示 WIFI 模块已启动；闪烁表示 WIFI 模块有数据传输。熄灭表示 WIFI 模块未启动。
10	SIM	SIM 卡指示灯，常亮表示检测到 SIM 卡，熄灭表示未检测到 SIM 卡。
11	RUN	设备运行指示灯，正常运行时闪烁频率为 1 秒亮，1 秒灭。
12	SFP0	SFP0 接口收光指示灯，亮则表示收有光建立；灭则表示收无光。
13	SFP1	SFP1 接口收光指示灯，亮则表示收有光建立；灭则表示收无光。

2. 设备后面板

RG2000-V8 无线路由器设备后面板如下图所示：



图 2-3 设备后面板示意图

后面板描述如表 2-3 所示：

表 2-3 设备后面板

序号	名称	说明
1	WLAN1	WIFI 天线接口 1。
2		设备接地柱。
3	WLAN2	WIFI 天线接口 2。
4	GPS	GPS 天线接口。
5	AUX	4G 天线辅接口。
6	MAIN	4G 天线主接口。
7	SIM	SIM 卡插槽。

 **注意：**

- (1) 设备 5 根天线不能混装，安装时请注意天线标识，确保天线安装正确；
- (2) 设备使用过程中，请确保设备接地柱良好接地。

2.5 安装说明

1. SIM 卡安装

安装 SIM 卡时，需先使用螺丝刀将 SIM 卡挡板卸下，按照面板指示的方向安装 SIM 卡。

安装完成后，需重新安装 SIM 卡挡板。

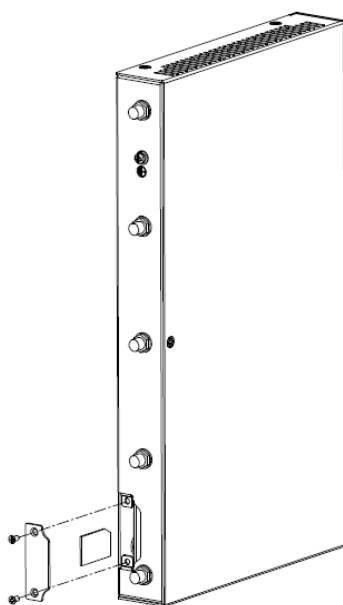


图 2-4 SIM 卡安装示意图



注意： SIM 卡不能带电插拔。需插入或者拔出 SIM 卡时，请先将设备断电后再操作，否则可能导致设备或者 SIM 卡不能正常工作。

2. 电源接线

设备出厂时提供一个 DC12V 1.5A 的电源适配器，电源适配器接线方法如表 2-4 所示：

表 2-4 电源接线表

示意图	说明
	<p>DC12V 1.5A 电源适配器示意图。</p>
 <p>白色条纹线头</p> <p>带字母线头</p>	<p>电源适配器线头，带白色条纹的线头为电源正极，带字母的线头为电源负极。</p>
 <p>白色条纹线头</p> <p>带字母线头</p>	<p>带白色条纹的线头接至电源插头正极，带字母的线头接至电源插头负极（中间孔位）。</p>



注意：

(1) 请按照如上说明将电源适配器接线头与电源插头连接，并将插头的螺丝锁紧，以防线头滑出或接触不良；

(2) 请注意电源适配器接线头与电源插头的连接线序，不要将线序与孔位弄错，否则设备将不能正常工作。

3. 附件安装

设备支持桌面式、壁挂式及导轨式安装方式。出厂时可选配置壁挂安装附件或导轨安装附件。

(1) 壁挂安装

壁挂安装示意图如下：

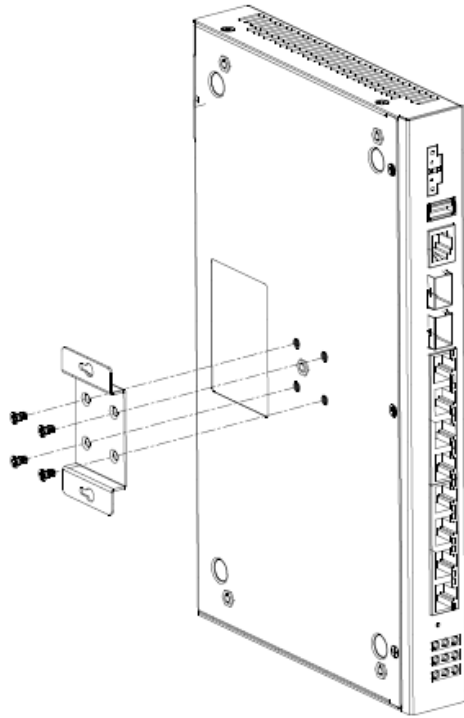


图 2-5 壁挂附件安装示意图

壁挂附件的尺寸如下图所示：

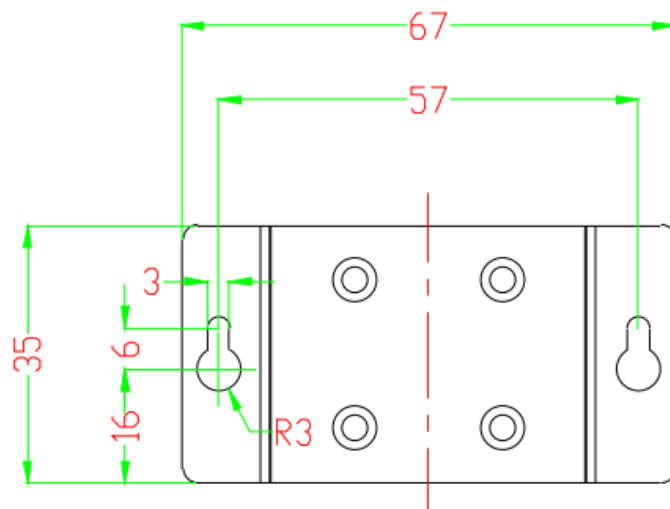


图 2-6 壁挂附件尺寸图

单位：mm。

(2) 导轨安装

设备可支持 DIN 导轨安装，如下图所示：

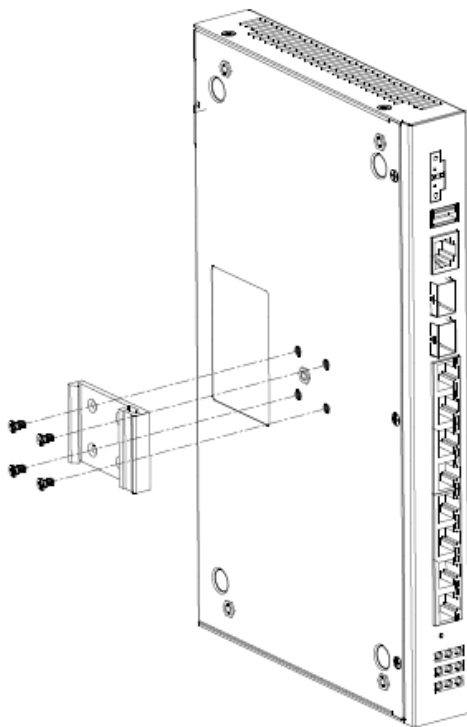


图 2-7 导轨附件安装示意图

导轨附件的尺寸如下图所示：

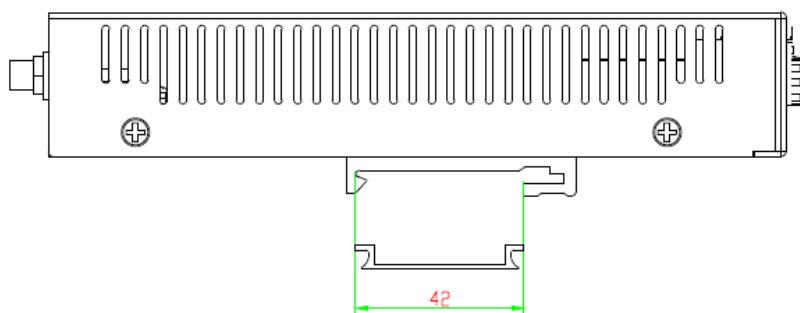


图 2-8 导轨附件尺寸图

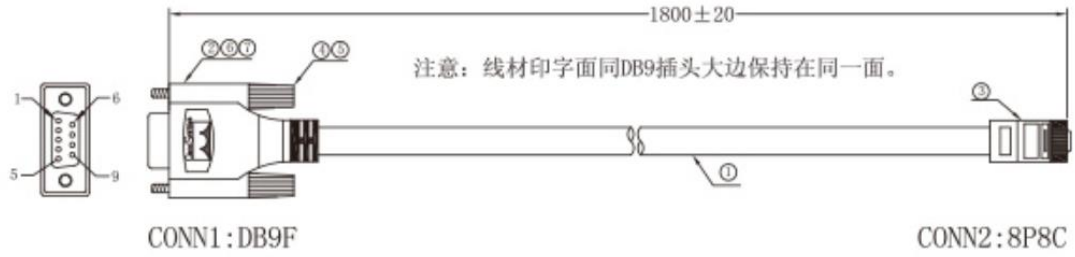
单位：mm。

2.6 串口线缆

通过 Console 口登录设备时，需要使用串口线，8P8C 侧接入设备 Console 口，DB9 侧连接 PC 的 RS232 串口。

注意：如 PC 无 RS232 串口，则需另购标准 USB 转 RS232 串口转接线缆。

串口电缆示意图如下：



DB9孔		RJ45
8 NC	-----	1 NC
6 NC	-----	2 NC
2 RXD	-----	3 RXD
5 GND	-----	4+5 GND
3 TXD	-----	6 TXD
4 NC	-----	7 NC
7 NC	-----	8 NC

图 2-9 串口线缆示意图

第三章 联机登录

3.1 环境要求

RG2000-V8 路由器对使用环境的要求如下：

- 工作环境温度：-20~+70℃
- 储存温度：-40~+85℃
- 工作环境相对湿度：10%~95%
- 存储相对湿度：0~95%

3.2 使用准备

配置使用 RG2000-V8 路由器时，通常，使用准备如下：

(1) 计算机一台

- 配有以太网卡和 TCP/IP 协议的计算机
- IE 6.0 或以上浏览器
- 建议采用 1024x768 或以上分辨率显示

(2) 4G SIM 卡一张

SIM 卡插拔前，需将设备断电，否则，可能导致设备的功能无法正常使用！

(3) 网线连接计算机与设备

通过 Telnet 或 WEB 登录系统时，需使用标准网线把计算机以太网口与 RG2000-V8 路由器的 LAN 口（GE0-GE7）连接起来。

(4) 串口线缆连接计算机与设备

通过 Console 口登录系统时，需使用串口线缆把计算机串口/USB 口与 RG2000-V8 路由器的 Console 口连接起来。

3.3 配置计算机

通过 Telnet 或 WEB 登录系统时，需配置计算机 IP 地址；在 PC 端，有两种方法去配置其 IP 地址，一种是 PC 的网卡开启自动获取 IP 地址，另一种是 PC 的网卡上配置一个与 RG2000-V8 路由器在同一子网的静态 IP 地址。

下面以 WINDOWS 10 系统为例，其它 WINDOWS 系统类似。

- (1) 控制面板->网络和 Internet->网络和共享中心->更改适配器配置，选中需配置的网卡：

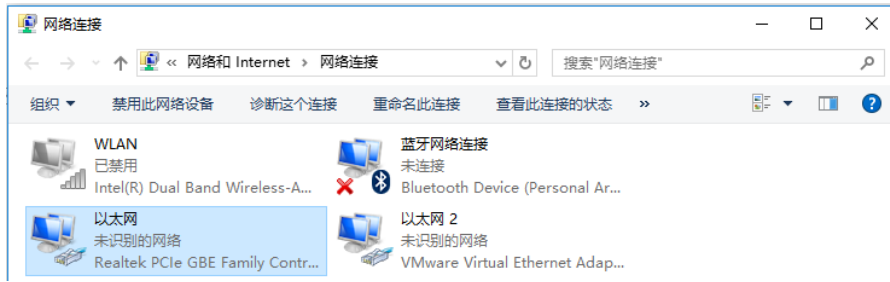


图 3-1 配置网络连接

(2) 点击右键->属性:



图 3-2 配置网卡属性

(3) 双击 Internet 协议版本 4(TCP/IPv4):

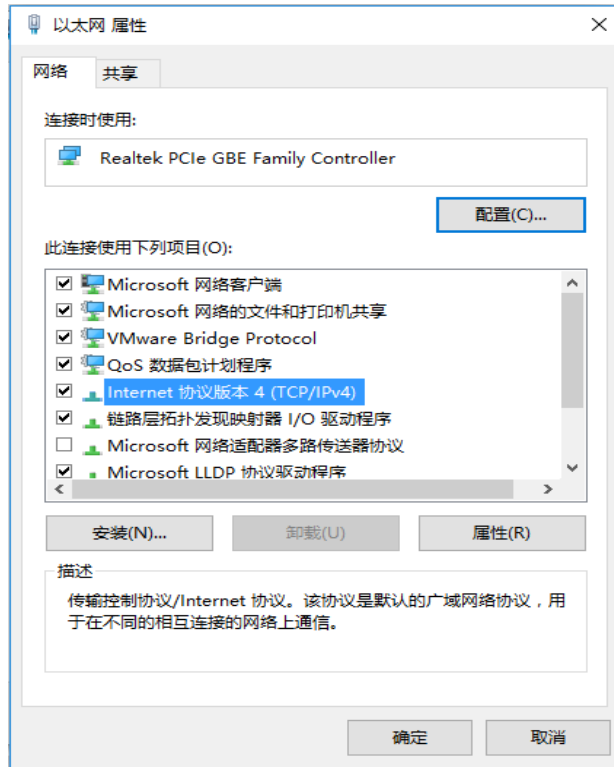


图 3-3 配置网卡 Internet 协议版本

(4) 若使用自动获取 IP 方式，则选择自动，然后点击确定完成配置。



图 3-4 配置网卡 IP 地址

- (5) 若选择配置静态 IP，则指定 IP，然后点击确定完成配置。

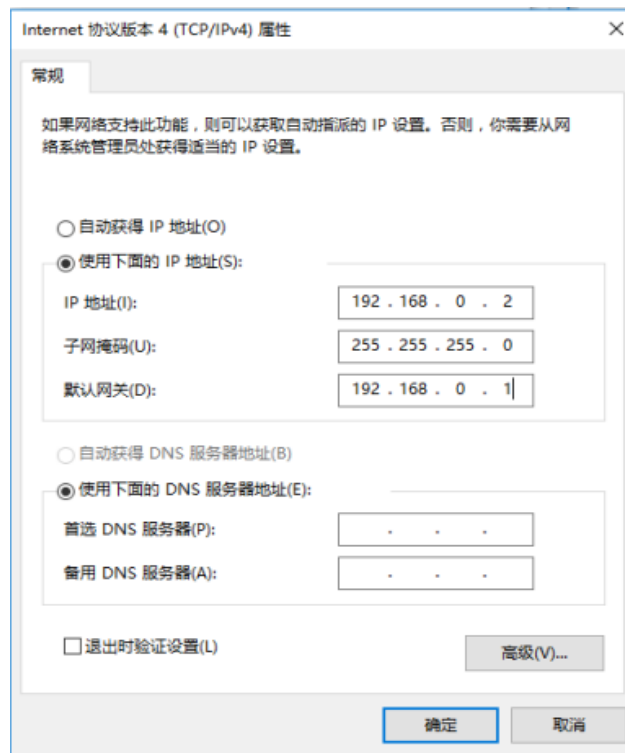


图 3-5 配置网卡 IP 地址

3.4 通过 Telnet 登录系统

在 PC 上运行 Telnet 客户端程序，键入目标设备提供的接口 IP 地址和端口，即可进入 CLI 登录界面；在 CLI 登录窗口输入用户名和口令，验证通过后，出现用户视图的命令行提示符，如<RG2000-V8>，表示用户进入了用户视图配置环境。

CLI 配置命令详见《第五章 CLI 命令行介绍》。

注：RG2000-V8 路由器的 Telnet 服务端口默认为 23，默认的用户名和口令为 admin, admin。

3.5 通过 Console 口登录系统

在通过 Console 口搭建本地配置环境时，用户可以在 PC 上通过 Windows 系统中的“超级终端”与 RG2000-V8 设备建立连接，连接成功后即进入 CLI 配置界面。

具体步骤如下：

- (1) 使用串口线将 PC 的串口与 ATN 设备的 Console 接口连接。
- (2) 在 PC 上启动超级终端。

选择“开始>程序>附件>通讯>超级终端”菜单项，Windows 系统启动超级终端。

(3) 新建连接。

在“名称”栏中输入新建连接的名称并选择“图标”。然后单击“确定”按钮。

(4) 设置连接端口

根据 PC（或配置终端）实际使用的端口在“连接时使用”下拉列表框中进行选择。然后单击“确定”按钮。

(5) 设置通信参数

波特率：115200

数据位：8

停止位：1

奇偶校验：无

数据流控制：无

3.6 通过 WEB 登录系统

RG2000-V8 路由器 LAN 口（GE1-GE4）默认 IP：192.168.0.1，子网掩码：255.255.255.0。

(1) 在 PC 上打开浏览器，在地址栏里输入设备 IP 地址。

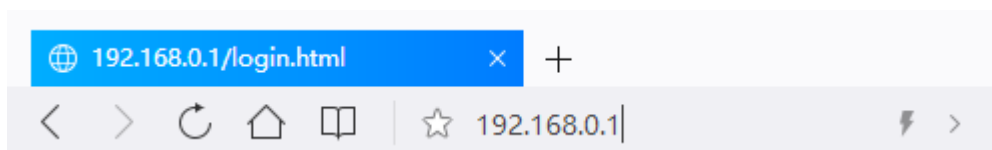


图 3-6 浏览器登录设备

(2) 输入用户名，密码，然后点击登录。

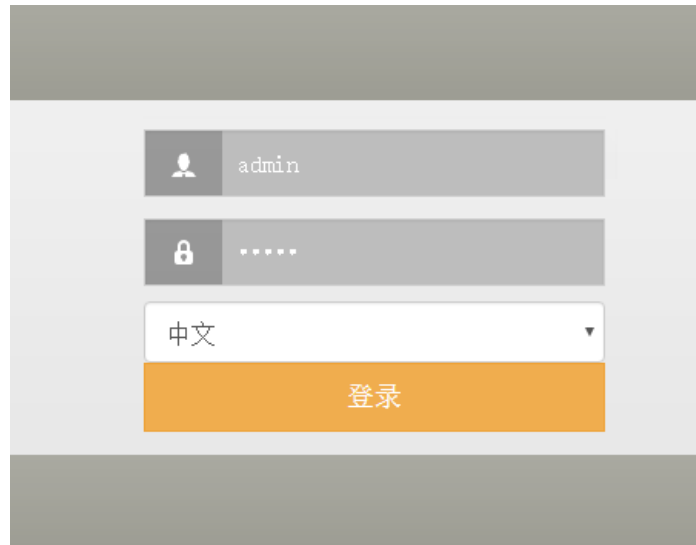



图 3-7 登录界面

正确输入用户名及密码后，点击登录，就能登陆设备 WEB 网管配置界面。

 **说明：** 默认用户名：admin，密码：admin。

第四章 配置操作

4.1 设备状态

设备状态有设备基本状态、WAN 接口状态、路由状态。

4.1.1 设备基本状态

设备基本状态包含基本信息、4G 网络状态、ARP 状态、端口 MAC 列表。

1. 基本信息

基本信息包含设备运行状态，WAN 口状态及以太网口连接状态。

如下图所示：



图 4-1 基本信息

设备运行状态包含：设备名称、序列号、软件版本、硬件版本、CPU 占用率、内存占用率、当前连接数、系统时间、运行时间。

WAN 口状态包含：SFP0/SFP1 的名称、MAC 地址、连接模式、连接状态。

以太网口连接状态包含：SFP0-SFP1、GE0-GE7 的端口 Link 状态、收发包统计数据。

基本信息可点击页面下方的“刷新”按钮进行刷新。

2. 4G 网络状态

4G 网络状态包含：模块状态、SIM 卡状态、SIM 卡注册状态、网络类型、运营商名称、位置信息、IMEI、IMSI、网络状态及 4G 网络地址信息。

如下图所示：



图 4-2 4G 网络状态

4G 网络状态可点击页面下方的“刷新”按钮进行刷新。

3. ARP 状态

ARP 状态包含设备当前的 ARP 表信息。

如下图所示：



图 4-3 ARP 状态

ARP 状态可点击页面下方的“刷新”按钮进行刷新。

4. 端口 MAC 列表

端口 MAC 列表包含交换芯片端口的 MAC 地址信息列表。

如下图所示：



图 4-4 端口 MAC 列表

端口 MAC 列表可点击页面下方的“刷新”按钮进行刷新。

4.1.2 WAN 接口状态

WAN 口状态包含所有 WAN 接口（SFP0、SFP1、创建的 WAN 接口）的状态信息：接口名称、MAC、连接模式、连接状态。

如下图所示：



图 4-5 WAN 接口状态

4.1.3 路由状态

路由状态包含设备当前的主路由表、默认路由表信息。

如下图所示：

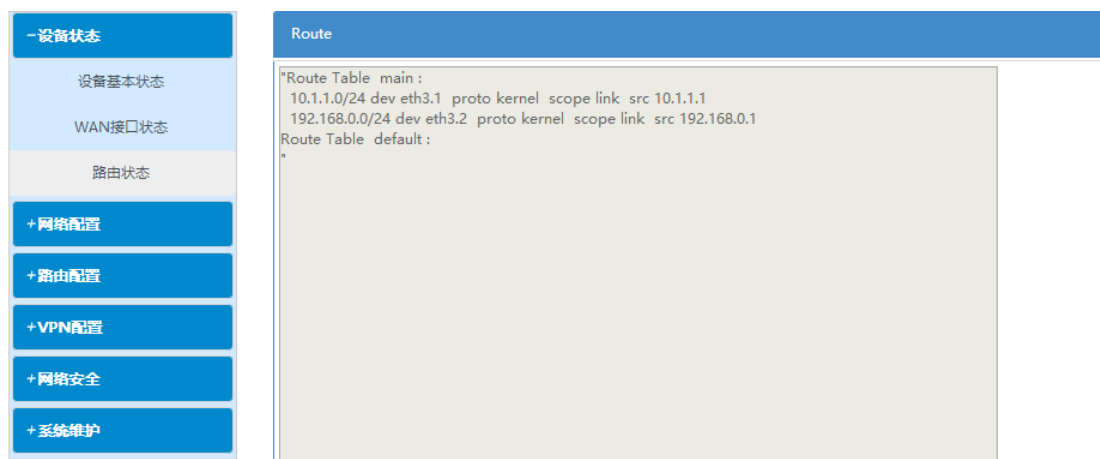


图 4-6 路由状态

4.2 网络配置

4.2.1 接口管理

1. WAN 口配置

路由器 WAN 口用来连接外网，支持配置多个 WAN 口。WAN 口的连接方式支持“静态 IP”、“DHCP”及“PPPOE”。

WAN 口配置界面如下图所示：



图 4-7 WAN 口配置界面

如需创建新的 WAN 接口，请点击“创建”按钮进行创建。

如需编辑 WAN 接口，在 WAN 列表中找到该接口，点击该接口的“编辑”按钮，如下图所示：

编辑	
接口名称:	<input type="text" value="vlan0010"/>
连接方式:	<input type="text" value="静态IP"/>
端口成员:	<input checked="" type="checkbox"/> GE0 <input type="checkbox"/> GE1 <input type="checkbox"/> GE2 <input type="checkbox"/> GE3 <input type="checkbox"/> GE4 <input checked="" type="checkbox"/> SFP
启用VLAN:	<input type="checkbox"/>
主DNS:	<input type="text" value="0.0.0.0"/>
从DNS:	<input type="text" value="0.0.0.0"/>
MTU:	<input type="text" value="1500"/> (512,2048)
IP地址:	<input type="text" value="192.168.60.1"/>
掩码:	<input type="text" value="255.255.255.0"/>
默认网关:	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>
<input type="button" value="保存"/> <input type="button" value="取消"/>	

图 4-8 编辑 WAN 接口

可修改接口名称，连接方式，端口成员，VLAN ID 及优先级，IP 地址，子网掩码，默认网关，DNS 地址，MTU 等配置，修改后点击“保存”按钮进行参数保存。

如需删除一个已有的 WAN 接口，在 WAN 列表中找到对应接口，点击该接口的“删除”按钮进行操作。

 **注意：**前两个 WAN 接口不能被删除。

如选择 DHCP 方式，即启用 DHCP 客户端，如下图所示：

编辑	
接口名称:	<input type="text" value="vlan0010"/>
连接方式:	<input type="text" value="DHCP"/>
端口成员:	<input checked="" type="checkbox"/> GE0 <input type="checkbox"/> GE1 <input type="checkbox"/> GE2 <input type="checkbox"/> GE3 <input type="checkbox"/> GE4 <input checked="" type="checkbox"/> SFP
启用VLAN:	<input type="checkbox"/>
主DNS:	<input type="text" value="0.0.0.0"/>
从DNS:	<input type="text" value="0.0.0.0"/>
MTU:	<input type="text" value="1500"/> (512,2048)
<input type="button" value="保存"/> <input type="button" value="取消"/>	

图 4-9 WAN 接口 DHCP 配置

如需手动指定 DNS 服务器，则需配置主/从 DNS 服务器，否则，将使用 DHCP 获取到的 DNS 服务器。

如选择 PPPOE 方式获取 IP，如下图所示：

编辑	
接口名称:	<input type="text" value="vlan0010"/>
连接方式:	PPPOE ▾
端口成员:	<input checked="" type="checkbox"/> GE0 <input type="checkbox"/> GE1 <input type="checkbox"/> GE2 <input type="checkbox"/> GE3 <input type="checkbox"/> GE4 <input checked="" type="checkbox"/> SFP
启用VLAN:	<input type="checkbox"/>
主DNS:	<input type="text" value="0.0.0.0"/>
从DNS:	<input type="text" value="0.0.0.0"/>
MTU:	<input type="text" value="1500"/> (512,2040)
用户名:	<input type="text" value="test"/> *
密码:	<input type="password" value="****"/> *
服务器名称(AC-Name):	<input type="text"/>
服务名:	<input type="text"/>
LCP间隔:	<input type="text" value="10"/> *[1,3000];default:10
LCP最大失败次数:	<input type="text" value="5"/> *[1,10];default:5
<input type="button" value="保存"/> <input type="button" value="取消"/>	

图 4-10 WAN 接口 PPPOE 配置

可配置用户名，密码，服务器名称，服务名，LCP 间隔及 LCP 最大失败次数。如需手动指定 DNS 服务器，则需配置主/从 DNS 服务器，否则，将使用 PPPOE 获取到的 DNS 服务器。

由于 PPPOE 自身包头长度为 8 个字节，建议 PPPOE 接口的默认 MTU 值设置为 1492。另外，建议 LCP 间隔设置为 10，LCP 最大失败次数设置为 5。

 **说明：** 最多可添加 10 个 WAN 接口。

2. LAN 口配置

路由器 LAN 口用来连接内网，支持配置多个 LAN 口。LAN 口配置如下图所示：

+设备状态		WAN口配置	LAN口配置	4G网络配置	Loopback口配置												
-网络配置		LAN															
接口管理	<table border="1"> <thead> <tr> <th>VlanID</th> <th>接口名称</th> <th>IP地址</th> <th>掩码</th> <th>端口成员</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>LAN0</td> <td>192.168.0.1</td> <td>255.255.255.0</td> <td>GE1,GE2,GE3,GE4,GE5,GE6,GE7,</td> <td>编辑</td> </tr> </tbody> </table>					VlanID	接口名称	IP地址	掩码	端口成员	操作	-	LAN0	192.168.0.1	255.255.255.0	GE1,GE2,GE3,GE4,GE5,GE6,GE7,	编辑
VlanID	接口名称	IP地址	掩码	端口成员	操作												
-	LAN0	192.168.0.1	255.255.255.0	GE1,GE2,GE3,GE4,GE5,GE6,GE7,	编辑												
端口管理	<input type="button" value="创建"/>																
VLAN管理																	

图 4-11 LAN 口配置界面

如需创建新的 LAN 接口，请点击“创建”按钮进行创建。

如需编辑 LAN 接口，在 LAN 列表中找到该接口，点击该接口的“编辑”按钮，如下图所示：

编辑	
接口名称:	<input type="text" value="LAN0"/>
端口成员:	<input type="checkbox"/> GE0 <input checked="" type="checkbox"/> GE1 <input checked="" type="checkbox"/> GE2 <input checked="" type="checkbox"/> GE3 <input checked="" type="checkbox"/> GE4 <input checked="" type="checkbox"/> GE5 <input checked="" type="checkbox"/> GE6 <input checked="" type="checkbox"/> GE7
启用VLAN:	<input type="checkbox"/>
MTU:	<input type="text" value="1500"/> (512,1500)
IP地址:	<input type="text" value="192.168.0.1"/>
掩码:	<input type="text" value="255.255.255.0"/>
启用NAT:	<input checked="" type="checkbox"/>
NAT接口:	<input type="text" value="All"/>
<input type="button" value="保存"/> <input type="button" value="取消"/>	

图 4-12 LAN 口编辑界面

可修改接口名称，端口成员，是否启用 VLAN，VLAN ID 及优先级，IP 地址，子网掩码，MTU，是否启用 NAT 以及 NAT 接口。

其中，NAT 接口：

- 默认为 ALL：即根据设备的具体路由确定 NAT WAN 接口。
- 指定某一个 WAN 接口或者 4G 接口出局：该 LAN 接口的数据固定从指定的 WAN 接口进行 NAT。
- 指定源 IP 地址：类似 ALL，但 NAT 后数据包的源 IP 为指定的 IP 地址。

修改后点击“保存”按钮进行参数保存。

如需删除一个已有的 LAN 接口，在 LAN 列表中找到对应接口，点击该接口的“删除”按钮进行操作。第一个 LAN 接口不能被删除。

 **说明：**最多可添加 8 个 LAN 接口。

 **注意：**WAN 接口及 LAN 接口的 VLAN ID 值不能有冲突。

3. 4G 网络配置

4G 网络配置如下图所示：



图 4-13 4G 网络配置界面

启用 4G 网络：可配置开关 4G 网络功能。

网络供应商类型：可选自定义或自动。默认为自动，无需配置。

特殊网络类型或特殊应用可以选择自定义。自定义类型下需要输入接入点、用户名、密码等参数。

连接模式有自动拨号和备份链路两种。

- 自动拨号模式：在设备启动过程，会自动进行 4G 网络拨号。
- 备份链路模式：当设备检测到有线网络断开时，4G 才会进行 4G 网络拨号；当设备检测到有线网络恢复时，会自动断开 4G 网络。

当配置备份链路模式时，主链路方式可配置为路由或交换模式，这里主链路指有线链路。

- 路由：WAN 口与 LAN 口为路由模式。
- 交换：WAN 口与 LAN 口为交换模式。

4. Loopback 接口配置

Loopback 接口配置如下图所示：



图 4-14 Loopback 接口配置

可配置是否启用 LOOPBACK 接口，可配置 LOOPBACK 口 IP 地址，子网掩码。

4.2.2 端口管理

RG2000-V8 路由器可通过 WEB 配置以太网端口协商方式，如下图所示：



图 4-15 端口管理

其中 GE0~GE7 端口的配置支持如下模式：

- 10M 半双工
- 10M 全双工
- 100M 半双工
- 100M 全双工
- 1000M 全双工
- 自适应

4.2.3 VLAN 管理

RG2000-V8 路由器除了支持逻辑 VLAN 接口用于划分 WAN 接口及 LAN 接口，还支持基于物理端口的 VLAN 划分。配置如下图所示：

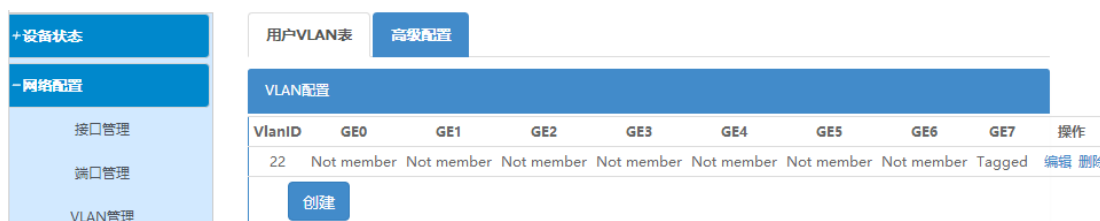


图 4-16 VLAN 管理

如要增加一条 VLAN，点击创建按钮，如下图所示：

配置	
VlanID	<input type="text" value=""/> (2,4094)
GE0:	Not member ▾
GE1:	Not member ▾
GE2:	Not member ▾
GE3:	Not member ▾
GE4:	Not member ▾
GE5:	Not member ▾
GE6:	Not member ▾
GE7:	Not member ▾
VLAN优先级	<input type="text" value="0"/> (0,7)
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-17 创建 VLAN

需配置 VLAN ID, VLAN 成员端口以及 VLAN 优先级。成员端口可包含 GE0-GE7。每个端口的配置支持如下模式：

- Not member: 该端口不属于该 VLAN。
- Tagged: 数据包从该端口出局时加标签。
- Untagged: 数据包从该端口出局时去标签。
- Unmodified: 数据包从该端口出局时，不对标签进行操作。

 **说明：** 最多可添加 50 条 VLAN 规则。

 **注意：** 这里 VLAN ID 与 WAN、LAN 接口的 VLAN ID 值不能有冲突。

4.2.4 WIFI 配置

1. WIFI 基本参数配置

WIFI 基本配置参数如下图所示：

设备状态	Wifi参数	安全	高级配置	客户端列表
网络配置	Wifi参数设置			
接口管理	启用Wifi: <input checked="" type="checkbox"/>			
VLAN管理	SSID: <input type="text" value="rg-wifi-00013C"/>			
WIFI配置	SSID隐藏: <input type="checkbox"/>			
DHCP配置	通道: <input type="text" value="6"/>			
链路探测	无线模式: <input type="text" value="g/n"/>			
路由配置	带宽: <input type="text" value="20/40MHz"/>			
	<input type="button" value="保存"/> <input type="button" value="刷新"/>			

图 4-18 WIFI 基本参数配置

- 启用 WiFi: WiFi 功能开关;
- SSID: 接入点 (AP) 名称;
- SSID 隐藏: 是否隐藏 SSID。如果开启, 客户端将扫描不到 AP;
- 通道: 工作通道配置;
- 无线模式: 支持 11b、11g、11n、11b/g、11g/n、11b/g/n, 请根据实际场景进行配置;
- 带宽: 无线通道带宽, 支持 20MHz、40MHz 及 20/40MHz 自动选择, 仅 11n、11g/n、11b/g/n 模式下有效。

2. 安全参数配置

WiFi 安全参数配置如下图所示:

The screenshot shows the '安全' (Security) configuration page for WiFi. The left sidebar includes '设备状态' (Device Status) and '网络配置' (Network Configuration) with sub-items like '接口管理' (Interface Management), 'VLAN管理' (VLAN Management), 'WiFi配置' (WiFi Configuration), and 'DHCP配置' (DHCP Configuration). The main content area has tabs for 'Wifi参数' (WiFi Parameters), '安全' (Security), '高级配置' (Advanced Configuration), and '客户端列表' (Client List). Under the '安全' tab, the following settings are visible:

- 认证模式 (Authentication Mode): WPA-PSK/WPA2-PSK
- 加密算法 (Encryption Algorithm): TKIP/CCMP
- PSK密码 (PSK Password): [Redacted] (8-63个字符)
- 密钥更新周期 (Key Update Period): 3600 (1-4194303)s

 There are '保存' (Save) and '刷新' (Refresh) buttons at the bottom.

图 4-19 WiFi 安全参数配置

该页面配置 WiFi 认证模式、加密算法、密钥及密钥更新周期。

由于 WEP 加密方式存在被破解的风险, 为安全起见, 建议使用 WPA2 加密模式。

⚠️ 注意: 如果启用 WEP 加密模式, 11N 将不能正常工作。

3. WiFi 高级参数配置

WiFi 高级参数配置如下图所示:

The screenshot shows the '高级' (Advanced) configuration page for WiFi. The left sidebar is the same as in the previous figure. The main content area has tabs for 'Wifi参数' (WiFi Parameters), '安全' (Security), '高级配置' (Advanced Configuration), and '客户端列表' (Client List). Under the '高级配置' tab, the following settings are visible:

- 客户端隔离 (Client Isolation):
- 传输功率 (Transmission Power): 12 (8-19dBm)
- 信标间隔 (Beacon Interval): 100 (20-1000)ms
- 国家地区 (Country): China

 There are '保存' (Save) and '刷新' (Refresh) buttons at the bottom.

图 4-20 WiFi 高级参数配置


- 客户端隔离: 开启此功能则此 AP 下的客户端之间无法通信。默认关闭;
- 传输功率: 一般使用默认值 12dBm;

- 信标间隔：SSID 广播时间间隔，建议使用默认值 100ms；
 - 国家地区：选择设备所在的国家地区。
4. WIFI 连接的客户端列表



图 4-21 WIFI 客户端列表

显示已连接的客户端的 MAC 及 IP 信息。

 **说明：**WIFI 默认与 LAN 接口列表中第一个 LAN 接口桥接。

4.2.5 DHCP 配置

1. DHCP 服务器配置

DHCP 服务器配置如下图所示：



图 4-22 DHCP 服务器配置

可配置 DHCP 服务器动态分配地址池及静态绑定地址池列表。

如需创建一个动态地址池，点击创建按钮进行创建，如下图所示：

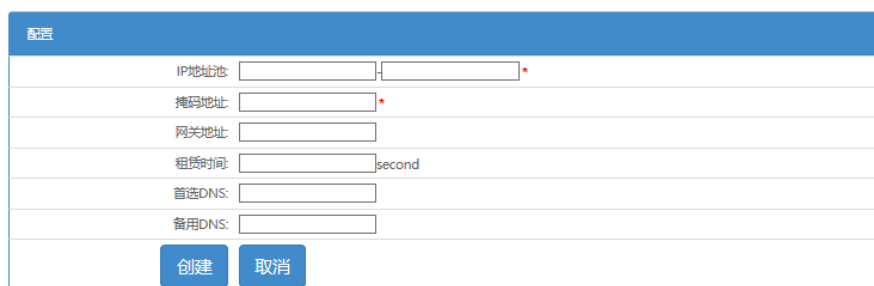


图 4-23 创建动态分配地址池

如需修改某个地址池，则在列表中找到该地址池，点击后面的编辑按钮进行修改。

如需删除某个地址池，则在列表中找到该地址池，点击后面的删除按钮进行删除。

如需静态给客户端分配 IP 地址，需启用静态绑定地址池列表，如下图所示：

创建	
描述:	1
客户端MAC:	f4:8e:38:96:10:3f (xxxxxxxxxxxx)
绑定IP地址:	192.168.0.108
绑定掩码:	255.255.255.0
<input type="button" value="保存"/> <input type="button" value="取消"/>	

图 4-24 创建 DHCP 静态分配地址池

添加需静态绑定的客户端 MAC 地址及需绑定 IP 地址/子网掩码。

注意：创建地址池的网段应该在 LAN 口列表中实际存在。

2. DHCP 服务器客户端列表

可在 WEB 网管中查看 DHCP 服务器动态地址分配情况，如下图所示：

设备状态		DHCP服务	
-网络配置		客户端列表	
客户端地址分配列表			
索引	已分配IP	MAC	客户端主机名
1	192.168.0.108	f4:8e:38:96:10:3f	DELL-PC

图 4-25 DHCP 客户端列表

可查看客户端的 IP 地址、MAC 及客户端主机名。

4.2.6 链路探测

链路探测配置如下图所示：

+设备状态		链路探测配置	
-网络配置		探测模式选择: NONE	
接口管理		<input type="button" value="保存"/> <input type="button" value="刷新"/>	

图 4-26 链路探测配置界面

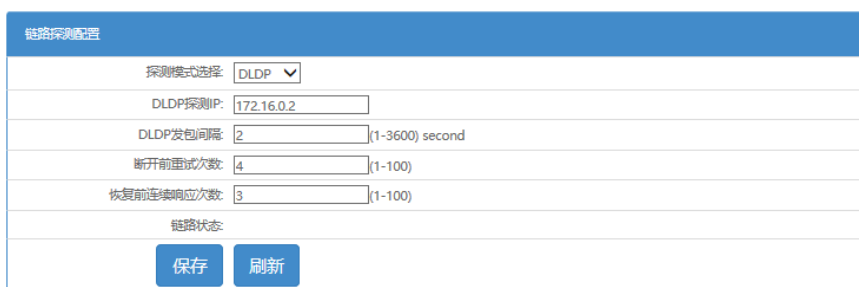
链路探测支持：NONE，DLDP 方式及 BFD 方式。

1. NONE 方式

即关闭链路探测功能。

2. DLDP 方式

DLDP 方式利用 ICMP 报文进行探测，配置如下图所示：

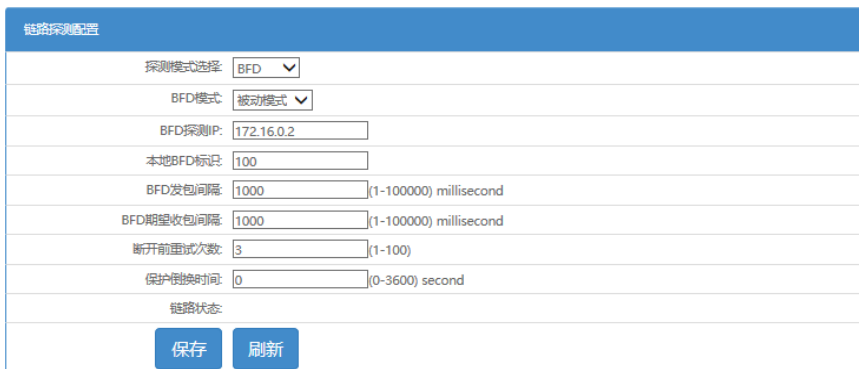


The screenshot shows the '链路探测配置' (Link Detection Configuration) interface. The '探测模式选择' (Detection Mode Selection) is set to 'DLDP'. The 'DLDP探测IP' (DLDP Detection IP) is '172.16.0.2'. The 'DLDP发包间隔' (DLDP Packet Interval) is '2' seconds. The '断开前重试次数' (Retries before disconnection) is '4'. The '恢复前连续响应次数' (Consecutive responses before recovery) is '3'. There are '保存' (Save) and '刷新' (Refresh) buttons at the bottom.

图 4-27 DLDP 配置界面

3. BFD 方式

BFD 方式为双向联动探测行为，两端都要启用，使用协议自身探测报文。配置如下图所示：



The screenshot shows the '链路探测配置' (Link Detection Configuration) interface. The '探测模式选择' (Detection Mode Selection) is set to 'BFD'. The 'BFD模式' (BFD Mode) is set to '被动模式' (Passive Mode). The 'BFD探测IP' (BFD Detection IP) is '172.16.0.2'. The '本地BFD标识' (Local BFD Identifier) is '100'. The 'BFD发包间隔' (BFD Packet Interval) is '1000' milliseconds. The 'BFD期望收包间隔' (BFD Expected Packet Interval) is '1000' milliseconds. The '断开前重试次数' (Retries before disconnection) is '3'. The '保护切换时间' (Protection Switching Time) is '0' seconds. There are '保存' (Save) and '刷新' (Refresh) buttons at the bottom.

图 4-28 BFD 配置界面

BFD 模式可支持被动模式与主动模式。

4.3 路由配置

4.3.1 静态路由

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。

静态路由配置如下图所示：



The screenshot shows the '静态路由配置' (Static Route Configuration) interface. On the left, there are navigation buttons: '+设备状态', '+网络配置', '-路由配置', and '静态路由'. The main area shows a table with the following data:

描述	目的地址	目的掩码	下一跳类型	接口	下一跳地址	操作
10net	10.0.0.1	255.255.255.0	接口	WAN0	0.0.0.0	编辑 删除

There is a '创建' (Create) button below the table.

图 4-29 静态路由配置界面

如需创建一条静态路由，则点击创建按钮，如下图所示：

配置	
描述:	<input type="text" value="10net"/>
目的地址:	<input type="text" value="10.0.0.1"/>
目的掩码:	<input type="text" value="255.255.255.0"/>
下一跳类型:	<input type="text" value="接口"/>
接口:	<input type="text" value="WAN0"/>
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-30 创建静态路由

- 描述：静态路由描述信息；
- 目的地址：设置静态路由的目标地址，如 10.0.0.1；
- 目的掩码：设置目的地址子网掩码；
- 下一跳类型：设置下一跳类型，可选“接口”或者“IP 地址”；
- 接口：指定静态路由下一跳接口；
- 下一跳地址：设置下一跳 IP 地址。

如需修改一条静态路由，则在列表中找到该路由，点击后面的编辑按钮进行修改。

如需删除某条静态路由，则在列表中找到该路由，点击后面的删除按钮进行删除。

4.3.2 策略路由配置

策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。策略路由可以根据 IP 报文源地址、目的地址、端口、协议等内容灵活地进行路由选择。

策略路由配置如下图所示：

+设备状态		策略路由配置						
+网络配置		描述	源地址	目的地址	协议类型	目的端口范围	下一跳	操作
-路由配置		policy1	192.168.10.100/24	10.1.1.1/24	ALL		WAN0	编辑 删除
静态路由		<input type="button" value="创建"/>						
策略路由配置								

图 4-31 策略路由配置

如需创建一条策略路由，则点击创建按钮，如下图所示：

配置	
描述:	<input type="text" value="policy1"/>
下一跳类型:	<input type="text" value="接口"/>
下一跳接口:	<input type="text" value="WAN0"/>
源地址:	<input type="text" value="192.168.10.100"/> / <input type="text" value="255.255.255.0"/>
目的地址:	<input type="text" value="10.1.1.1"/> / <input type="text" value="255.255.255.0"/>
协议类型:	<input type="text" value="ALL"/>
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-32 创建策略路由

- 描述：该条策略路由描述信息；
- 下一跳类型：设置下一跳类型，可选“接口”或者“IP 地址”；
- 下一跳接口：设置下一跳接口，接口指路由器的网络逻辑接口；
- 下一跳地址：设置下一跳 IP 地址；
- 源地址：设置源 IP 地址及子网掩码，可设置为一个网段；
- 目的地址：设置目的 IP 地址及子网掩码，可设置为一个网段；
- 协议类型：可选择 UDP、TCP 及 ALL。

如需修改一条策略路由，则在列表中找到该路由，点击后面的编辑按钮进行修改。

如需删除某条策略路由，则在列表中找到该路由，点击后面的删除按钮进行删除。

4.3.3 OSPF 配置

OSPF (Open Shortest Path First 开放式最短路径优先) 为 IETF OSPF 工作组开发的一种基于链路状态的内部网关路由协议，用于在单一自治系统 (autonomous system, AS) 内决策路由。OSPF 是专为 IP 开发的路由协议，直接运行在 IP 层上面，协议号为 89，采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5 (全部 OSPF 设备) 和 224.0.0.6 (指定设备)。

OSPF 协议配置如下图所示：



图 4-33 OSPF 配置界面

- Router ID: 运行 OSPF 协议的设备，必须存在 Router ID，用于在一个 OSPF 自治系统内唯一的标识一台设备。需要保证自治系统内 Router ID 的唯一性，否则会影响邻居建立和路由学习。可指定 Router ID，若没有指定 Router ID(0.0.0.0)，则根据以下规则进行选举：
 - (1) 首先从 Loopback 接口的 IP 地址中选择最大的作为 Router ID；
 - (2) 若没有配置 IP 地址的 Loopback 接口，则从其它接口的 IP 地址中选择最大的作为 Router ID；
 - (3) 只有接口处于 UP 状态时，该接口地址才可能被选作 Router ID。
- 接口列表: 左边列表框为待选接口，右边列表框为已选接口。已选接口的路由将会添加到 OSPF 进程中；
- 接口区域编号: 可将 OSPF 自治系统划分多个区域，以 0.0.0.0~255.255.255.255 范围的 IP 地址表示。区域 0.0.0.0 表示 OSPF 骨干区域，其它非 0 区域为非骨干区域。所有的区域间路由信息都需要通过骨干区域进行转发，非骨干区域之间不能直接交换路由信息。

4.3.4 IS-IS 配置

IS-IS (Intermediate system to intermediate system, 意为“中间系统到中间系统”)是一种内部网关协议，是电信运营商普遍采用的内部网关协议之一。

ISIS 是一个分级的链接状态路由协议，基于 DECnet PhaseV 路由算法，实

实际上与 OSPF 非常相似，它也使用 Hello 协议寻找毗邻节点，使用一个传播协议发送链接信息。ISIS 可以在不同的子网上操作，包括广播型的 LAN、WAN 和点到点链路。

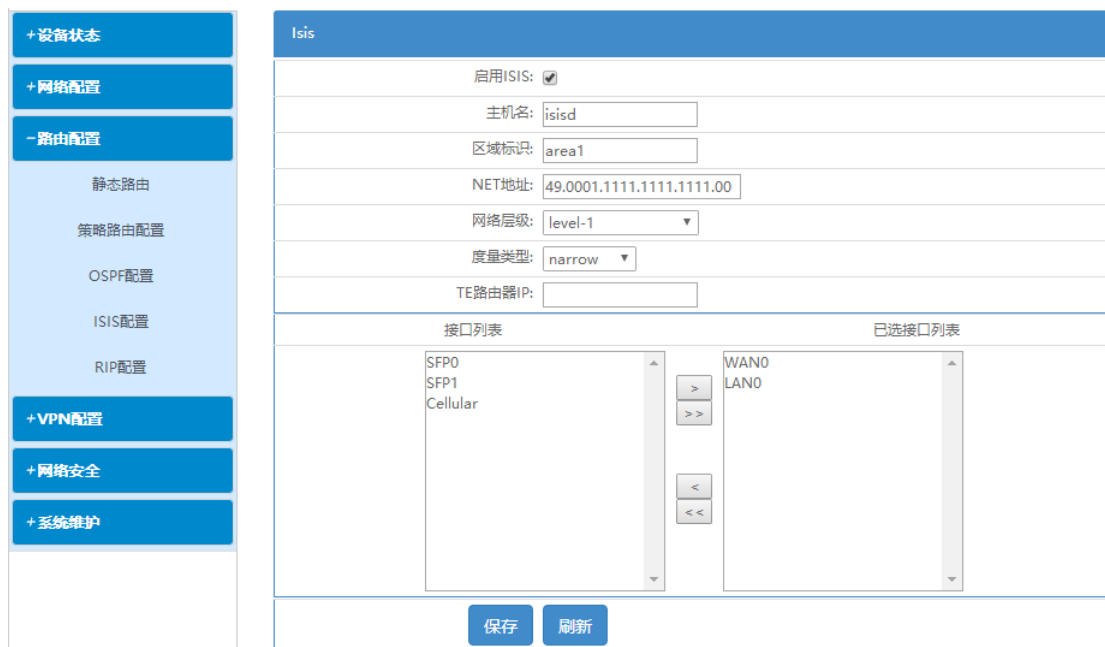


图 4-34 IS-IS 配置界面

- 主机名：IS-IS 路由节点的主机名称，将携带在路由报文中；
- 区域标识：用于标识路由区域，主要用于设备归属多个路由区域的情况，目前只支持一个区域，可输入任意字符串；
- NET 地址：Network Entity Title（网络实体标记），长度范围为 8-20bytes；
- 网络层级：IS-IS 分层，IS-IS 仅支持 2 种分层：Level-1 为普通区域，Level-2 为骨干区域；
- 度量类型：度量值用于衡量接口处方向的开销，度量类型决定接受的 TLV 度量值范围，wide 表示使用新的宽度量，narrow 表示使用旧的窄度量，transition 表示同时支持两种度量类型；
- TE 路由器 IP：用于 MPLS-TE 功能，标记当前路由器；
- 接口列表：左边列表框为待选接口，右边列表框为已选接口。已选接口的路由将会添加到 OSPF 进程中；

4.3.5 RIP 配置

RIP(Routing Information Protocol)路由协议是一种基于距离矢量的路由协议，以路由跳数作为计数单位的路由协议，适合用于比较小型的网络环境。

RIP 使用 UDP 报文交换路由信息，UDP 端口号为 520。通常情况下 RIPv1 报文为广播报文；而 RIPv2 报文为组播报文，组播地址为 224.0.0.9。



图 4-35 RIP 配置界面

- 接口列表：左边列表框为待选接口，右边列表框为已选接口。已选接口的路由将会添加到 RIP 进程中；
- 接口允许通告报文：配置是否在此接口上发送通告报文进行交换路由信息。

4.4 VPN 配置

4.4.1 GRE 配置

GRE (Generic Routing Encapsulation, 通用路由封装) 协议是对某些网络层协议 (如 IP 和 IPX) 的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议 (如 IP) 中传输。GRE 采用了 Tunnel (隧道) 技术，是 VPN (Virtual Private Network) 的第三层隧道协议。Tunnel 是一个虚拟的点对点的连接，提供了一条通路使封装的数据报文能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。



图 4-36 GRE 配置界面


如需创建一条配置，点击创建按钮，如下图所示：

图 4-37 创建 GRE 配置

- 描述：该条 GRE 规则的描述信息。
- 源接口：选择 GRE 的源端接口，源接口生效的 IP 将成为 GRE 的源端 IP 地址；
- 目的地址：配置 GRE 的目的端地址；
- 隧道地址：配置 GRE 隧道接口的地址。
- 隧道对端地址：配置 GRE 隧道接口远端的地址。
- 启用 EOIP：可以配置启用 EOIP VPN 功能，当开启 EOIP，可配置 VPN 绑定的本地 LAN 口。

如需修改某条配置，则在列表中找到该配置，点击后面的编辑按钮进行修改。

如需删除某条配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

 **说明：** EoIP (Ethernet over IP) 隧道是一个建立在两个路由器的 IP 传输层之间的以太网隧道协议，是 MikroTik RouterOS 的自由协议。EoIP 接口表现的类似以太网传输，当路由器的桥接功能被启用后，所有的以太网数据流量（所有的以太网协议）将被桥接就如同在两个路由器（启用了桥接功能）之间有物理交换机接口和光纤收发器一样。

4.4.2 IPsec VPN

IPsec (IP Security) 是一种由 IETF 设计的端到端的确保 IP 层通信安全的机制, 包含了一组 IP 安全协议集。IPsec 协议可以为 IP 网络通信提供透明的安全服务, 保护 TCP/IP 通信免遭窃听和篡改, 保证数据的完整性和机密性, 有效抵御网络攻击。



图 4-38 IPSEC 配置

创建一条 IPSEC 如下图所示:

图 4-39 IPSEC 创建

- 描述: 该条 IPSEC 规则的描述信息;
- 加密接口: 通过选择 IPSEC 加密的源接口方式配置 IPSEC 加密策略中的本地地址, 源接口生效的 IP 将成为 IPSEC 的本地地址;

- 对端 IP: 配置 IPSEC 加密策略中的对端地址。0.0.0.0 表示任意对端 IP。配置为任意对端 IP 时，IKE 协商模式需配置为野蛮模式，且指定对端身份标识；
- IKE 加密提议: 配置 IKE 协商过程中使用的加密算法、散列算法、DH 组；
- 启用 NAT-T: 配置是否开启 IPSEC VPN NAT 穿越功能；
- IKE 协商模式: 配置 IKE 第一阶段协商模式；
- 共享密码: 配置预共享密钥；注意：不要使用全数字密码！
- IPSEC 加密提议: 配置 IPsec 提议是本端接受的安全协议（AH 或 ESP）和算法（加密算法和认证算法）的组合；
- 本地身份, 对端身份: 配置本地和对端身份标识。默认不指定身份标识，不指定身份标识，将使用 IP 地址作为标识；
- SA 时效配置 ipsec sa 的生存周期，SA PF GROUP 配置指定 pf_group
- 组网方式: 配置 IPSEC 安全策略对应的数据流是点到点还是子网到子网；
- 子网配置: 配置安全策略中子网到子网的数据流信息。0.0.0.0/0.0.0.0 表示任意子网。

4.4.3 L2TP

L2TP (Layer Two Tunneling Protocol) 第二层通道协议，是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。L2TP 面向数据包的点对点连接，提供包头压缩、隧道验证等功能。

RG2000-V8 路由器支持 L2TP 客户端及 L2TP 服务端功能。

1. L2TP 客户端配置

L2TP 客户端配置如下图所示：



图 4-40 L2TP 客户端配置界面

如需创建一条配置，点击创建按钮，如下图所示：

配置	
描述:	<input type="text" value="l2tpc-01"/>
用户名:	<input type="text" value="admin"/>
密码:	<input type="password" value="....."/> (不能全为数字)
接口:	<input type="text" value="WAN0"/>
服务器地址:	<input type="text" value="10.1.1.2"/>
启用隧道认证:	<input type="checkbox"/>
启用L2tp over ipsec:	<input type="checkbox"/>
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-41 创建一条 L2TP 配置

- 描述：该条 L2TP 规则的描述信息；
- 用户名，密码：配置 PPP 认证用户名和密码；
- 接口：选择 L2TP 拨号的源接口；
- 服务器地址：L2TP 拨号的服务器地址；
- 启用隧道认证：可配置启用 L2TP 隧道认证，并配置认证密码；
- 启用 L2TP OVER IPSEC：可配置 IPSEC 加密 L2TP 隧道。具体加密参数可参考 IPSEC 配置。

2. L2TP 服务端配置

L2TP 服务端配置如下图所示：

+设备状态	L2TP客户端	L2TP服务器	L2TP服务器认证账号
	+网络配置	L2TP服务器配置	
+路由配置	启用L2TP服务器: <input type="checkbox"/>		
-VPN配置	<input type="button" value="保存"/> <input type="button" value="刷新"/>		
GRE配置			
IPSec VPN			
L2TP			

图 4-42 L2TP 服务端配置界面

启用 L2TP 服务器配置如下图所示：

图 4-43 L2TP 服务端配置

- 启用 L2TP 服务器：配置是否开启 L2TP 服务器功能；
- IP 地址池：L2TP 服务器的地址池；
- 启用隧道认证：可配置启用 L2TP 隧道认证，并配置认证密码；
- 启用 L2TP OVER IPSEC：可配置 IPSEC 加密 L2TP 隧道。具体加密参数可参考 IPSEC 配置。

3. L2TP 服务器认证账号

L2TP 服务器认证账号配置如下图所示：

PPP认证用户名	启用指定分配IP	指定分配IP	操作
admin	YES	11.1.1.1	编辑 删除

图 4-44 L2TP 服务器认证账号配置界面

如需创建一条认证账号，点击创建按钮，如下图所示：

图 4-45 创建 L2TP 服务器认证账号

- PPP 认证用户名，密码：配置用于认证 L2TP 客户端的 PPP 认证用户名和密码；
- 启用指定分配 IP：配置启用 PPP 认证账号与 L2TP 客户端 IP 地址绑定；
- 指定分配 IP：配置当前 PPP 认证账号归属的 L2TP 客户端 IP 地址；

4.4.4 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。

RG2000-V8 路由器支持 PPTP 客户端及 PPTP 服务端功能。

4. PPTP 客户端配置

PPTP 客户端配置如下图所示：



图 4-46 PPTP 客户端配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-47 创建一条 PPTP 配置

- 描述：该条 PPTP 规则的描述信息；
- 用户名，密码：配置 PPP 认证用户名和密码；

- 接口：选择 PPTP 拨号的源接口；
- 服务器地址：PPTP 拨号的服务器地址；

5. PPTP 服务端配置

启用 PPTP 服务器配置如下图所示：

图 4-48 PPTP 服务器配置

- 启用 PPTP 服务器：配置是否开启 PPTP 服务器功能；
 - IP 地址池：PPTP 服务器的地址池；
- ## 6. PPTP 服务器认证账号

PPTP 服务器认证账号配置如下图所示：

PPP认证用户名	启用指定分配IP	指定分配IP	操作
admin	NO	----	编辑 删除

图 4-49 PPTP 服务器认证账号配置界面

如需创建一条认证账号，点击创建按钮，如下图所示：

图 4-50 创建 PPTP 服务器认证账号

- PPP 认证用户名，密码：配置用于认证 PPTP 客户端的 PPP 认证用户名和密码；
- 启用指定分配 IP：配置启用 PPP 认证账号与 PPTP 客户端 IP 地址绑定；
- 指定分配 IP：配置当前 PPP 认证账号归属的 PPTP 客户端 IP 地址；

4.5 网络安全

4.6.1 攻击防御

防火墙基本配置用来设置当前路由器防火墙的行为,包括防火墙默认处理策略,是否禁止 Ping 包,是否防止 Dos 攻击,是否启用防 SYN 泛洪。

基本防火墙配置	
外网禁PING:	<input type="checkbox"/>
防SYN泛洪:	<input checked="" type="checkbox"/> 40 (1-10000)
防DOS攻击:	<input checked="" type="checkbox"/>
TCPMSS:	<input type="checkbox"/> 1460 (128-1500)
最大连接数:	20000 (1000-50000)
<input type="button" value="保存"/> <input type="button" value="刷新"/>	

图 4-51 基本防火墙配置

- 外网禁 PING：开启时，过滤来自外网的 PING 报文。默认未开启。
- 防 SYN 泛洪：开启时，防止来自外网的 SYN 泛洪攻击，默认为每秒接收 40 个 TCP SYN 连接。默认开启。
- 防 DOS 攻击：开启时，设备将开启防 DOS 攻击功能。默认开启。
- TCPMSS：开启时，将限制 TCP 传输最大报文大小，默认未开启。
- 最大连接数：限制系统最大的链接数量。

4.6.2 访问策略配置

访问策略功能包括黑名单和白名单，提供主要的防火墙访问过滤功能。

黑名单：对与规则匹配的访问报文进行过滤拦截，丢弃报文。

白名单：对与规则匹配的访问报文无条件接收、放行。

其中，白名单策略优先级高于黑名单策略。

1. 白名单

白名单功能配置界面如下图所示：



图 4-52 白名单配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-53 创建白名单

- 描述：访问策略的规则描述。
- 匹配源地址类型：
 - ANY：匹配任意源地址；
 - IP Addr：匹配源 IP 地址，选择此类型时，将需要输入一个源 IP 地址；
 - IP Segm：匹配源 IP 地址范围，选择此类型时，将需要配置一个 IP 地址段，包括源 IP 地址、源 IP 掩码；
 - MAC：匹配源 MAC 地址，选择此类型时，将需要配置一个源 MAC 地址；
- 匹配目的地址类型：
 - ANY：匹配任意目的地址；
 - IP Addr：匹配目的 IP 地址，选择此类型时，将需要输入一个目的 IP 地址；
 - IP Segm：匹配目的 IP 地址范围，选择此类型时，将需要配置一个 IP

地址段，包括目的 IP 地址、目的 IP 掩码；

URL：匹配访问 URL，选择此类型时，将需要配置一个 URL 地址；

➤ L4 协议：

IGNORE：不匹配协议字段；

ICMP：匹配 ICMP 协议的数据包；

UDP：匹配 UDP 协议的数据包，选择此协议时，可以选择是否匹配源端口或范围，或者目的端口或范围；

TCP：匹配 TCP 协议的数据包，选择此协议时，可以选择是否匹配源端口或范围，或者目的端口或范围；

如需修改某条白名单配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑、修改。

如需删除某条白名单配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

2. 黑名单

黑名单功能配置界面如下图所示：



图 4-54 黑名单配置界面

如需创建一条配置，点击创建按钮，如下图所示：



图 4-55 创建黑名单

- 描述：黑名单访问策略的规则描述。
- 匹配源地址类型：参考白名单。
- 匹配目的地址类型：参考白名单。
- L4 协议：参考白名单。

如需修改某条黑名单配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑、修改。

如需删除某条黑名单配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

4.6.3 PAT 配置

PAT (Port Address Translation, 端口地址转换) 是 NAT (Network Address Translation, 网络地址转换) 最常用的一种实现方式。NAT 通过将企业内部的私有 IP 地址转换为全球唯一的公网 IP 地址，使内部网络可以连接外网，而 PAT 可以在上述转换过程中，实现企业内网的多个私有 IP 对一个或是多个 IP 复用，从而实现 IP 地址的节约。

PAT 功能配置界面如下图所示：



图 4-56 PAT 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-57 创建一条 PAT 配置

- 描述：该条 PAT 配置的描述；
- 协议：可选择 TCP 或者 UDP；
- 外网接口：配置数据包从设备进入的 WAN 接口。外部设备访问该 WAN 逻辑接口对应的外网端口时，数据包将被送至所配置的内网 IP 及内网端口。另，外网接口可配置为 CUSTOM，此时需要配置一个外网 IP。外部数据包访问该外网 IP 及外网端口时，数据包将被送至所配置的内网 IP 及内网端口；
- 内网 IP：内部网络设备的 IP 地址；
- 内网端口：内部网络设备的端口号。

如需修改某条 PAT 配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑、修改。

如需删除某条 PAT 配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

4.6.4 DMZ 配置

DMZ (Demilitarized Zone, 隔离区)，是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

PAT 功能配置界面如下图所示：



图 4-58 DMZ 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

配置	
描述:	<input type="text" value="1"/>
外网接口:	<input type="text" value="CUSTOM"/>
外网IP:	<input type="text" value="202.16.0.18"/>
内网IP:	<input type="text" value="192.168.0.100"/>
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-59 创建一条 DMZ 配置

- 描述：该条 DMZ 配置的描述；
- 外网接口：配置数据包从设备进入的 WAN 接口。外部设备访问该 WAN 接口时，数据包将被送至所配置的内网 IP 地址。另，外网接口可配置为 CUSTOM，此时需要配置一个外网 IP。外部数据包访问该外网 IP 时，数据包将被送至所配置的内网 IP 地址；
- 内网 IP：内部网络设备的 IP 地址。

如需修改某条 DMZ 配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑修改。

如需删除某条 DMZ 配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

4.6.5 SNAT 配置

SNAT，是源地址转换，其作用是将 IP 数据包的源地址转换成另外一个地址。

SNAT 功能配置界面如下图所示：

+设备状态	
+网络配置	
+路由配置	
+VPN配置	
-网络安全	
攻击防御	
访问策略配置	
PAT配置	
DMZ配置	
SNAT配置	

SNAT配置				
描述	匹配源地址	SNAT出接口	SNAT地址	操作
snat-01	192.168.0.100/255.255.255.0	WAN0	10.1.1.2	编辑 删除
<input type="button" value="创建"/>				

图 4-60 SNAT 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

配置	
描述:	<input type="text"/>
匹配源地址:	<input type="text" value="192.168.0.100"/> <input type="text" value="255.255.255.0"/>
SNAT出接口:	<input type="text" value="WAN0"/>
SNAT地址:	<input type="text" value="10.1.1.2"/>
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-61 创建一条 SNAT 配置

- 描述：该条 SNAT 配置的描述；
- 匹配源地址：配置将被执行 SNAT 的源 IP 地址和源码；
- SNAT 出接口：配置当前 SNAT 规则的出 WAN 接口；
- SNAT 地址：配置源地址将转换成的 IP 地址。

如需修改某条 SNAT 配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑修改。

如需删除某条 SNAT 配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

4.6.6 UPNP 配置

UPNP 功能配置界面如下图所示：

+ 设备状态	
+ 网络配置	
+ 路由配置	
+ VPN配置	
- 网络安全	
攻击防御	
访问策略配置	
PAT配置	
DMZ配置	
SNAT配置	
UPNP配置	

Upnp	
启用Upnp:	<input type="checkbox"/>
上行口:	<input type="text" value="SFPO"/>
下行口:	<input type="text" value="LAN0"/>
<input type="button" value="保存"/> <input type="button" value="刷新"/>	

图 4-62 UPNP 配置界面

- 启用 Upnp：是否启用 UPNP 功能；
- 上行口：选择上行 WAN 接口；
- 下行口：选择下行 LAN 接口；

4.6.7 QoS 配置

QoS 功能主要实现流量整形、ACL 过滤规则等功能。

1. 全局配置

QoS 功能全局配置界面如下图所示：



图 4-63 QoS 全局配置界面

- 启用流控：是否启用流量控制功能；
- 启用 QoS：是否启用 QoS 功能；
- 调度模式：启用 QoS 功能后，可选择调度模式；

2. 端口限速

端口限速功能实现 GE0-GE7 以太网端口的出口流量整形，限制出口最大带宽。

端口限速功能全局配置界面如下图所示：



图 4-64 端口限速配置界面

- 接口：GE0-GE7，物理以太网接口；
- 启用限速：端口是否启用限速的开关；
- 出口带宽：端口出口流量整形的最大带宽，以 kbps 为单位，计算时注意，1M=1024k。

3. ACL 规则

ACL 规则配置界面如下图示：



图 4-65 ACL 规则配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-66 添加 L2 ACL 规则

- 描述：ACL 规则的描述；
- 接口：ACL 规则使能的接口；
- 流类型：L2 表示匹配二层字段，L3/L4 表示匹配三层字段；
- 匹配源 MAC：是否匹配报文的源 MAC，启用后需配置源 MAC 地址，流类型为 L2 时可配；
- 匹配目的 MAC：是否匹配报文的目的 MAC，启用后需配置目的 MAC 地址，流类型为 L2 时可配；
- 匹配以太网类型：是否匹配报文的以太网类型字段，启用后需配置以太网类型，流类型为 L2 时可配；
- 匹配 VLAN：是否匹配报文的 VLAN 字段，启用后需配置 VLAN ID，流类型为 L2 时可配；

如果流类型选择 L3/L4 时，配置界面如下图所示：

配置	
描述:	<input type="text"/>
接口:	<input checked="" type="checkbox"/> GE0 <input checked="" type="checkbox"/> GE1 <input checked="" type="checkbox"/> GE2 <input checked="" type="checkbox"/> GE3 <input checked="" type="checkbox"/> GE4 <input checked="" type="checkbox"/> SFP
流类型:	<input type="radio"/> L2 <input checked="" type="radio"/> L3/L4
匹配源 IP:	<input type="checkbox"/> <input type="text"/> / <input type="text"/>
匹配目的 IP:	<input type="checkbox"/> <input type="text"/> / <input type="text"/>
匹配 L4 协议:	<input type="text" value="IGNORE"/> ▼
丢弃:	<input type="checkbox"/>
修改 VLAN:	<input type="checkbox"/> <input type="text"/>
修改 802.1p:	<input type="checkbox"/> <input type="text"/>
优先级:	<input type="checkbox"/> <input type="text"/>
限速:	<input type="checkbox"/> <input type="text"/> (kbps)
<input type="button" value="创建"/> <input type="button" value="取消"/>	

图 4-67 添加 L3/L4 ACL 规则

- 匹配源 IP: 是否匹配报文的源 IP 地址, 启用后需配置源 IP 地址、掩码;
- 匹配目的 IP: 是否匹配报文的目的 IP 地址, 启用后需配置目的 IP 地址、掩码;
- 匹配 L4 协议: 匹配报文的协议类型字段;
 - IGNORE: 不匹配报文的协议类型字段;
 - ICMP: 匹配 ICMP 协议的数据包;
 - UDP: 匹配 UDP 协议的数据包, 选择此协议时, 可以选择是否匹配源端口或范围, 或者目的端口或范围;
 - TCP: 匹配 TCP 协议的数据包, 选择此协议时, 可以选择是否匹配源端口或范围, 或者目的端口或范围;
 - CUSTOM: 匹配自定义的协议类型;

ACL 处理策略:

- 丢弃: 是否丢弃与规则匹配的报文;
- 修改 VLAN: 是否修改与规则匹配的报文 VLAN ID 字段;
- 修改 802.1P: 是否修改与规则匹配的报文 802.1P 字段;
- 优先级: 是否修改与规则匹配的报文优先级字段;
- 限速: 是否对与规则匹配的流进行限速;

如需修改某条 ACL 规则, 则在列表中找到该规则, 点击后面的编辑按钮进行编辑修改。

如需删除某条 ACL 规则, 则在列表中找到该规则, 点击后面的删除按钮进行

删除。

4.6.8 IP-MAC 绑定

IP-MAC 绑定实现 IP 与 MAC 的一一对应，只有在 IP 地址和 MAC 地址对应时才允许访问设备。

IP-MAC 功能配置界面如下图所示：



图 4-68 IP-MAC 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-69 创建一条 IP-MA 绑定配置

- 绑定 IP 地址：IP-MAC 绑定规则的 IP 地址；
- 绑定 MAC：IP-MAC 绑定规则的 MAC 地址；

如需修改某条 IP-MAC 绑定配置，则在列表中找到该配置，点击后面的编辑按钮进行编辑、修改。

如需删除某条 IP-MAC 绑定配置，则在列表中找到该配置，点击后面的删除按钮进行删除。

4.6.9 ALG 配置

ALG 应用级网关，也叫做应用层网关（Application Layer Gateway）。

ALG 主要完成了对应用层报文的处理，通常情况下 NAT 只对报头中的 IP、PORT 信息进行转换，不对应用层数据载荷中的字段进行分析，如果启用了 ALG，那么在识别了相应报文之后便会对 IP 报头以外的载荷信息进行解析，然后进行地址转换，重新计算校验和。

ALG 功能配置界面如下图所示：



图 4-70 ALG 配置界面

- 启用 SIP ALG：是否启用 SIP 协议 ALG 功能；
- 启用 RSTP ALG：是否启用 RSTP 协议 ALG 功能；
- 启用 FTP ALG：是否启用 FTP 协议 ALG 功能；
- 启用 TFTP ALG：是否启用 TFTP 协议 ALG 功能；
- 启用 PPTP ALG：是否启用 PPTP 协议 ALG 功能；
- 启用 GRE ALG：是否启用 GRE 协议 ALG 功能；

4.6 系统维护

4.7.1 系统时间

系统时间配置路由器的本地时间，其配置界面如下图所示：



图 4-71 系统时间配置

可选择开启和关闭 NTP（Network Time Protocol，网络时间协议）。时区请根据实际所需进行设置。设备默认开启 NTP。

4.7.2 SNMP 配置

RG2000-V8 支持 SNMP 网管，其配置界面如下：



图 4-72 SNMP 配置

- SNMP 开关：是否开启 SNMP；
- 本地端口：设备 SNMP 协议本地端口号；
- 团体名：设置 SNMP 的团体名；
- Trap 开关：是否开启设备 TRAP 包功能；
- Trap 服务器地址：Trap 服务器地址；
- Trap 服务器端口：Trap 服务器端口号；
- Private trap 开关：是否开启私有 trap 包功能；
- Trap 周期：Trap 包发送周期；
- 区域标识：设置区域标识；
- SNMP 注册状态：设备 SNMP 网管注册状态。

4.7.3 WEB 管理

WEB 管理用于配置设备 WEB 网管协议、端口及用户密码、访问权限控制，配置如下图所示：



图 4-73 WEB 配置

1. WEB 配置

- 启用 Guest 用户：是否允许通过 Guest 账户登录 WEB；
- 启用 WEB SSL：是否启用 HTTPS 登录。当开启时，用户需通过 HTTPS 方式访问设备 WEB 网管。默认未启用；
- WEB HTTP 端口：配置 HTTP 登录端口号，默认为 80；
- WEB HTTPS 端口：配置 HTTPS 登录端口号，默认为 443。开启 WEB SSL 时有效。
- 是否允许外网访问：是否允许通过外网登录 WEB 界面；
- 是否允许内网访问：是否允许通过内网登录 WEB 界面；

2. 修改 WEB 登录密码

修改当前用户登录 WEB 网管的密码，如下图所示：

图 4-74 WEB 密码修改

修改密码时，需两次输入相同的密码方可修改成功。

4.7.4 TELNET 设置

TELNET 设置用于配置 telnet 端口、访问控制、修改 telnet 相关密码。

登录 RG2000-V8 路由器 telnet 网管时，首先需输入登录密码。如要取得 telnet 网管的配置权限，需进入 telnet 网管的 enable 模式。在 WEB 网管中，可修改设备 telnet 网管的登录密码及 enable 模式密码。

Telnet 访问控制配置如下图示：



图 4-75 Telnet 访问配置

- TELNET 端口：配置通过 TELNET 访问设备的端口号，默认为 23；
- 是否允许外网访问：是否允许通过外网登录 telnet 界面；
- 是否允许内网访问：是否允许通过内网登录 telnet 界面；

登录密码修改如下图所示：



图 4-76 Telnet 登录密码修改

修改 enable 模式密码如下图所示：



图 4-77 Telnet enable 模式密码修改

4.7.5 软件升级

RG2000-V8 路由器可通过 WEB 网管进行升级，在升级之前请确认已获得系统更新的目标文件。点击菜单栏中的软件升级，界面如下：



图 4-78 软件升级界面

点击“选择文件”按钮，选择升级目标文件，点击“提交”按钮后，会弹出一个确认对话框，点击“确定”开始软件升级，如下图所示：



图 4-79 软件升级界面

升级开始后，界面中会给出一个升级进度条，提示目前的升级进度。升级完成后，会弹出一个对话框，提示升级结果。点击确定，页面自动跳转到“设备状态”页面。

软件升级成功后，需重启设备方能运行升级后的程序。软件版本号在“设备状态”页面中查看。



注意：软件升级过程中，请勿将设备断电，否则，会导致设备无法启动。

4.7.6 配置管理

用户可通过 WEB 网管导出及导入设备的参数文件，也可以将设备恢复出厂默认参数。如下图所示：



图 4-80 配置管理界面

1. 导入文件

用于导入设备的参数文件，点击“选择文件”按钮，选择目标参数文件，点击“提交”按钮后，会弹出一个确认对话框，点击“确定”开始导入参数文件。成功后会弹出一个对话框，提示文件导入结果。点击确定，页面自动跳转到“设备状态”页面。升级文件导入成功后，需重启设备方能运行导入的参数。

2. 恢复出厂默认参数

点击“恢复默认”按钮，会弹出一个确认对话框，点击“确定”开始恢复出厂默认参数。成功后会弹出一个对话框，提示操作结果。恢复出厂默认参数后，需重启设备生效。

3. 导出参数

点击“导出配置文件”按钮，可查看设备当前的参数文件。

4.7.7 设备重启

点击菜单栏“系统维护”->“设备重启”，弹出如下界面：



图 4-81 设备重启界面

点击“立即重启设备”按钮，会弹出一个确认对话框，点击“确定”开始重启设备。

4.7.8 日志管理

RG2000-V8 路由器支持本地日志信息及 SYSLOG 日志信息，点击菜单栏“系统维护”->“日志管理”，可配置和查看设备日志信息。



图 4-82 日志管理界面

1. 日志配置

- 启用日志：是否启用设备日志功能。默认启用。
- 日志文件等级：本地日志文件记录等级，可支持八个等级，分别是致命级 (EMERG), 警戒级 (ALERT), 临界级 (CRIT), 错误级 (ERR), 告警级 (WARN), 注意级 (NOTICE), 通知级 (INFO), 调试级 (DEBUG), 日志等级依次降低。当等级设定后，系统只记录该等级及较该等级更高等级的日志信息。例如，设置为通知级 (INFO) 后，则调试级 (DEBUG) 的日志信息将不被记录。另外，选择 DISABLE 即关闭本地日志记录功能。
- SYSLOG 等级：同日志文件等级。选择 DISABLE 即关闭 SYSLOG 日志功能。
- SYSLOG 服务器 IP：设置 SYSLOG 服务器 IP 地址。
- SYSLOG 服务器端口：设置 SYSLOG 服务器端口号。

2. 日志导出

点击“Export Log File”按钮，可导出日志进行查看。

4.7.9 通信检测

RG2000-V8 路由器支持 PING 检测及 TRACEROUTE 检测功能。

1. PING 检测

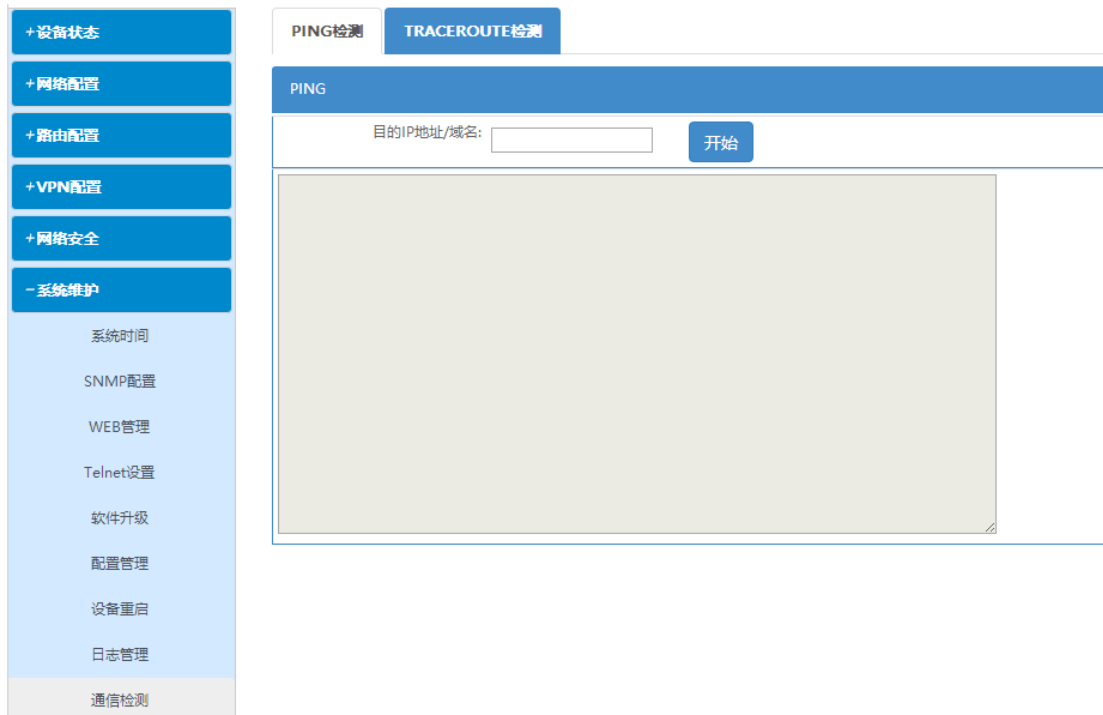


图 4-83 PING 检测

在“目的 IP 地址/域名”文本框中输入要检测的 IP 地址或者域名，点击“开始”按钮后开始检测，下面文本框中给出检测结果。

2. TRACEROUTE 检测

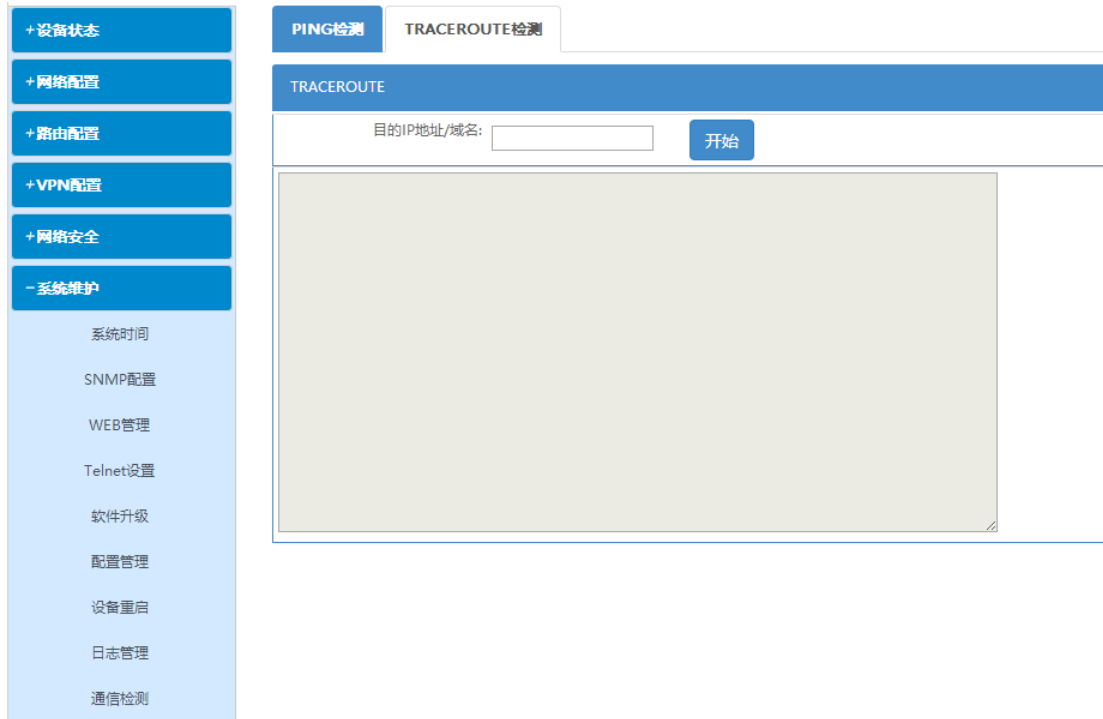


图 4-84 TRACEROUTE 检测

在“目的 IP 地址/域名”文本框中输入要检测的 IP 地址或者域名，点击“开始”按钮后开始检测，下面文本框中给出检测结果。

4.7.10 激活参数

参数配置完成后，可根据页面右上角红色提示进行操作，将当前配置的参数激活生效。

如果提示“激活参数”，则点击“激活参数”即可使参数生效。



如果提示“重启”，则点击“重启”通过重启设备使参数生效。



第五章 CLI 命令行介绍

5.1 CLI 概述

RG2000-V8 无线路由器可通过 CLI 命令行界面对设备参数进行查看和配置。CLI 命令行界面分成若干不同模式，用户当前所处的命令模式决定了可以使用的命令。各命令模式间切换如图 5-1 所示：

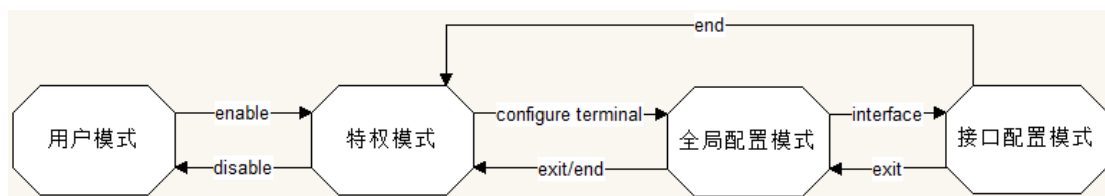


图 5-1 CLI 命令模式切换示意图

当用户和设备 CLI 管理界面建立一个新的会话连接时，用户首先需输入登录密码，登录成功后处于用户模式，可使用用户模式的命令。用户模式的提示符为“>”。在用户模式下，只可以使用少量命令，并且命令的功能也受到一些限制，例如可以使用 ping 命令等。用户模式的命令的操作结果不会被保存。

要使用所有的命令，需先进入特权模式。使用 enable 命令进入特权模式，且需输入特权模式的口令。在特权模式下，用户可以使用所有的特权命令，并且能够由此进入全局配置模式。特权模式的提示符为“#”。

在特权模式下，使用 configure terminal 命令进入全局配置模式。使用配置模式（全局配置模式、接口配置模式等）的命令，会对当前运行的配置参数产生影响。如果用户执行了保存命令，这些修改的参数将会被保存下来，在系统重新启动时，软件模块将会以这些保存的参数启动运行。

从全局配置模式出发，可以进入接口配置模式等各种配置子模式。全局模式的提示符为“(config)#”。

 **说明：**

- (1) RG2000-V8 无线路由器的缺省主机名为“RG2000-V8”；
- (2) CLI 命令行界面不支持中文字符及中文符号；
- (3) CLI 命令行界面中输入问号“?”不回显。

5.2 CLI 命令常识及使用技巧介绍

5.2.1 命令帮助

1. 获得命令列表

在命令提示符下直接输入问号“?”可获取该模式下可用的命令列表。例如：
在特权模式下直接输入问号“?”，可获取该模式下的命令列表：

```
RG2000-V8#?  
configure Configuration from vty interface  
disable Turn off privileged mode command  
end End current mode and change to enable mode  
exit Exit current mode and down to previous mode  
list Print command list  
no Negate a command or set its defaults  
ping Send echo messages  
quit Exit current mode and down to previous mode  
show Negate a command or set its defaults  
start-shell Start UNIX shell  
telnet Open a telnet connection  
terminal Set terminal line parameters  
traceroute Trace route to destination
```



说明：实际使用时，问号“?”不会回显，这里为了表述问号“?”功能特标注出来，同以下章节。

2. 获得相同开头的命令关键字字符串

命令中，有多个相同关键字开头的命令时，可用“关键字+?”进行查看，例如：

```
RG2000-V8(config)# show port?  
port Port  
port-mirroring Port mirror control  
port-vlan Port-based vlan
```

列出以“port”开头的命令列表。

3. 列出该关键字关联的下一个变量

输入命令时，可在命令后使用“空格+?”列出命令行的下一个变量，例如：

```

RG2000-V8(config)# show port-mirroring ?
<cr>
RG2000-V8(config)# show port ?
config          Configuration
negotiation-1000m negotiation-1000m
statistic       Port statistic info
status          Status

```

<cr>表示该命令已经输入完成，后面再无关键字。

5.2.2 命令简写

如果想简写命令，只需要输入命令关键字的一部分字符，只要这部分字符足够识别唯一的命令关键字即可。例如：“show logging”命令可简写为“sh log”。

5.2.3 命令补全

用户可使用 TAB 键使命令的关键字自动补充完整。

当输入命令部分关键字时，如果该部分关键字关联的命令字已无歧义，则直接补全该关键字，否则会列出以该部分关键字开头的所有命令关键字。

例如：

```

RG2000-V8(config)# show port-[TAB 键]
port-mirroring    port-statistic  port-vlan
RG2000-V8(config)# show port-m[TAB 键]
RG2000-V8(config)# show port-mirroring

```



说明：实际使用时，TAB 键不会回显，这里为了表述方便将 TAB 键标注出来。

5.2.4 命令错误提示

命令错误提示及含义如表 5-1 所示：

表 5-1 命令错误提示

序号	提示	含义
1	% Ambiguous command.	用户没有输入足够的字符，设备无法识别唯一的命令。
2	% Command incomplete.	用户没有输入该命令的必需的关键字或者变量参数。
3	% Unknown command.	用户输入未知命令。

5.2.5 no 命令

部分命令有 no 选项。通常，使用 no 选项来禁止某个特性或功能，或者执行与命令本身相反的操作。例如命令 no port-mirroring 执行关闭端口镜像功能。

5.2.6 历史命令

系统提供了用户输入命令的记录。该特性在重新输入长而且复杂的命令时将十分有用。如表 5-2 所描述：

表 5-2 历史命令使用

序号	提示	含义
1	Ctrl-P 或 ↑ 上方向键	在历史命令表中浏览前一条命令。从最近的一条记录开始，重复使用该操作可以查询更早的记录。
2	Ctrl-N 或 ↓ 下方向键	在使用了 Ctrl-P 或上方向键操作之后，使用该操作在历史命令表中回到更近的一条命令。重复使用该操作可以查询更近的记录。

5.3 CLI 命令详细介绍

5.3.1 基础命令

功能	命令	说明
退出当前视图，返回上一级视图	exit	任意视图都有
同 exit	quit	任意视图都有

显示所有命令关键字列表	list	任意视图都有
显示所有命令详细列表	show commandtree	任意视图都有
结束当前视图，并切换到特权视图	end	除用户视图、特权视图外的任意视图都有
进入特权视图，需验证密码	enable	仅用户视图
退出特权视图	disable	仅特权视图
进入系统 shell	start-shell	

5.3.2 接口配置

1. WAN 接口配置命令

功能	命令	说明
进入配置视图	configure terminal	-
进入 WAN 接口配置模式	interface wan NAME	如接口不存在则创建并进入，否则直接进入编辑
删除一个 WAN 接口	no interface wan NAME	
查看一个 WAN 接口配置	show interface wan NAME	
查看所有 WAN 接口配置	show interface wan	
查看路由器所有接口配置	show interface	

WAN 接口配置模式：

功能	命令	说明
增加物理端口成员	port-map port-name	
删除物理端口成员	no port-map port-name	
启用 VLAN，并设置 vlan id 和优先级	vlan id vlanid priority vlan-pri	
禁用 vlan	no vlan	
设置 DNS 服务器地址	dns server primary-dns [secondary-dns]	
禁用 DNS 服务器地址	no dns server	

设置连接类型	link-type <i>dhcp/pppoe/static</i>	
配置接口 IP 和掩码，可行网关	ip address <i>ip mask mask [gateway A.B.C.D]</i>	
配置以太网接口的 IPV4 MTU	mtu <i>mtu</i>	
设置默认网关	gateway <i>A.B.C.D</i>	
禁用默认网关	no gateway	
设置 pppoe 用户名、密码	pppoe username <i>username password</i> <i>password</i>	
设置 pppoe AC NAME	pppoe ac-name <i>ac-name</i>	
设置 pppoe 服务名	pppoe service-name <i>service-name</i>	
设置 pppoe LCP 间隔	pppoe lcp-interval <i>interval</i>	
设置 pppoe LCP 最大失败次数	pppoe lcp-max-fail <i>numbers</i>	
在 RIP 上发布此接口的网段，是否允许通告报文	ip router rip [broadcast]	
取消在 RIP 上发布此接口的网段	no ip router rip	
在 OSPF 上发布此接口的网段	ip router ospf area <i>A.B.C.D</i>	
取消在 OSPF 上发布此接口的网段	no ip router ospf	
在接口上使能 ISIS	ip router isis <i>area-id</i>	
在接口上关闭指定区域的 ISIS	no ip router isis <i>area-id</i>	
在接口上关闭所有相关的 ISIS	no ip router isis	
使能接口的 MPLS LDP 能力	mpls ldp	
关闭接口的 MPLS LDP 能力	no mpls ldp	
最大带宽	mpls te bandwidth max-bandwidth <i>bandwidth</i>	
最大可预留带宽	mpls te bandwidth	

	max-reservable-bandwidth <i>bandwidth</i>	
接口 metric	mpls te metric <i>metric</i>	
删除接口 TE 配置	no mpls te	
查看当前视图的配置	show	
退出当前视图，返回上一视图	exit	

2. LAN 接口基本配置

功能	命令	说明
进入配置视图	configure terminal	-
进入 LAN 接口配置模式	interface lan <i>NAME</i>	如接口不存在则创建并进入，否则直接进入编辑
删除一个 LAN 接口	no interface lan <i>NAME</i>	
查看一个 LAN 接口配置	show interface lan <i>NAME</i>	
查看所有 LAN 接口配置	show interface lan	
查看路由器所有接口配置	show interface	

LAN 接口配置模式：

功能	命令	说明
增加物理端口成员	port-map <i>port-name</i>	
删除物理端口成员	no port-map <i>port-name</i>	
启用 VLAN，并设置 vlan id 和优先级	vlan id <i>vlanid</i> priority <i>vlan-pri</i>	
禁用 vlan	no vlan	
配置接口 IP 和掩码，可行网关	ip address <i>ip</i> mask <i>mask</i> [gateway <i>A.B.C.D</i>]	
配置以太网接口的 IPV4 MTU	mtu <i>mtu</i>	
nat 目的接口	nat interface <i>interface-name</i>	
指定 nat IP	nat ip <i>A.B.C.D</i>	
取消 NAT	no nat	
在 RIP 上发布此接口的网段，	ip router rip [broadcast]	

是否允许通告报文		
取消在 RIP 上发布此接口的网段	no ip router rip	
在 OSPF 上发布此接口的网段	ip router ospf area A.B.C.D	
取消在 OSPF 上发布此接口的网段	no ip router ospf	
在接口上使能 ISIS	ip router isis area-id	
在接口上关闭指定区域的 ISIS	no ip router isis area-id	
在接口上关闭所有相关的 ISIS	no ip router isis	
使能接口的 MPLS LDP 能力	mpls ldp	
关闭接口的 MPLS LDP 能力	no mpls ldp	
最大带宽	mpls te bandwidth max-bandwidth bandwidth	
最大可预留带宽	mpls te bandwidth max-reservable-bandwidth bandwidth	
接口 metric	mpls te metric metric	
删除接口 TE 配置	no mpls te	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

3. 4G 接口

功能	命令	说明
进入配置视图	configure terminal	-
进入 4G 接口配置模式	interface cellular	-
关闭 4G 接口	no interface cellular	
查看 4G 接口配置	show interface cellular	
查看 GPS 状态	show gps	

查看 PLMN 网络类型	show plmn net-type	
--------------	------------------------------------	--

4G 接口配置模式：

功能	命令	说明
开 gps	gps enable	
关 gps	no gps	
gps mode	gps mode <1-7>	
网络类型	plmn net-type type	
设置 PIN 码	pin-code code	
关闭 PIN 码	no pin-code code	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

4. Loopback 接口

功能	命令	说明
进入配置视图	configure terminal	-
进入 Loopback 接口配置模式	interface loopback	-
关闭 Loopback 接口	no interface loopback	
查看 Loopback 接口配置	show interface loopback	

Loopback 接口配置模式：

功能	命令	说明
配置接口 IP 和掩码	ip address ip mask mask	
配置接口 IP 和掩码	ip address ip/digit	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.3 端口配置

功能	命令	说明
进入配置视图	configure terminal	-
查看端口状态	show port status	

查看端口统计信息	show port statistic [port port]	
端口流量统计开关	port statistic enable	
端口流量统计开关	no port statistic enable	
端口流量统计清 0	clear port statistic	
设置以太网端口协商模式	port port-name speed speed duplex duplex	

5.3.4 DHCP 服务器配置

功能	命令	说明
进入配置视图	configure terminal	-
启用 dhcp 服务	ip dhcp service	
关闭 dhcp 服务	no ip dhcp service	
创建 dhcp 服务地址池，并进入 DHCP 地址池配置视图	ip dhcp pool pool-name	-
删除 dhcp 服务地址池	no ip dhcp pool pool-name	
创建 dhcp 静态绑定列表	ip dhcp mac-binding name ip ip-address mask netmask mac mac-address	
删除 dhcp 静态绑定列表	no ip dhcp mac-binding name	
查看 DHCP 服务的客户端列表	show ip dhcp binding	
查看 DHCP 服务配置	show ip dhcp config	

DHCP 服务器配置模式：

功能	命令	说明
添加一个 IP 段到地址池，必须保证有同网段的接口！	network ip mask	
添加一个 IP 范围到地址池，必须保证有同网段的接口！	ip-pool start-ip end-ip [mask]	
设置默认网关地址	gateway gateway-ip	
设置租赁时间	lease time	

设置 dns 地址	dns-server <i>dns1 [dns2]</i>	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.5 VLAN 配置

功能	命令	说明
进入配置视图	configure terminal	-
停用 QinQ 功能	no qinq	
启用并配置 QinQ 外层 TPID，16 进制格式，如 88a8	qinq protocol <i>ethertype</i>	
创建 VLAN，并进入 VLAN 视图	vlan <i>vlan-id</i>	-
删除 VLAN	no vlan <i>vlan-id</i>	
查看 VLAN 配置	show vlan	

VLAN 配置模式：

功能	命令	说明
配置 VLAN 优先级	priority <i>priority</i>	
添加一个或多个端口到 VLAN， action-type 取值范围为 tagged/untagged/unmodified	port <i>port-number action-type</i>	
将一个或多个端口从 VLAN 中 删除	no port <i>port-number</i>	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.6 DLDP 配置

功能	命令	说明
进入配置视图	configure terminal	-

功能	命令	说明
启用并配置 DLDP	dldp ip A.B.C.D interval <1-3600> retry <1-100> resume <1-100>	
关闭 DLDP	no dldp	
查看 DLDP 配置信息	show dldp config	

5.3.7 BFD 配置

功能	命令	说明
进入配置视图	configure terminal	-
启用并配置 BFD	bfd peer-ip A.B.C.D local-id <1-100000> interval <50-10000> min_rx <50-10000> multiplier <3-50> mode (active passive) resume <0-3600>	
关闭 BFD	no bfd	
查看 BFD 配置信息	show bfd config	
查看 BFD session 信息	show bfd sessions	

5.3.8 路由配置

1. 静态路由配置

功能	命令	说明
进入配置视图	configure terminal	-
添加静态路由	ip route-static WORD destination A.B.C.D/M nexthop A.B.C.D	
添加静态路由	ip route-static WORD destination A.B.C.D/M interface interface	
删除静态路由	no ip route-static WORD	
查看静态路由表配置	show ip route-static	

2. 策略路由配置

功能	命令	说明
进入配置视图	configure terminal	-

功能	命令	说明
创建策略路由：网关 IP	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M nexthop A.B.C.D	
创建策略路由：网关 IP+协议	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M nexthop A.B.C.D protocol (all udp tcp)	
创建策略路由：网关 IP+协议+ 端口/端口范围	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M nexthop A.B.C.D protocol (udp tcp) port WORD	
创建策略路由：出接口	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M interface WORD	
创建策略路由：出接口+协议	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M interface WORD protocol (all udp tcp)	
创建策略路由：出接口+协议+ 端口/端口范围	ip route-policy WORD source A.B.C.D/M destination A.B.C.D/M interface WORD protocol (udp tcp) port WORD	
删除策略路由	no ip route-policy route-policy-name	
查看策略路由表配置	show ip route-policy	

3. 路由状态查看

功能	命令	说明
查看 ip 路由表	show ip route	

5.3.9 RIP 路由配置

功能	命令	说明
进入配置视图	configure terminal	-
RIP 总开关，并进入 RIP 配置 视图	router rip	
关闭 RIP 功能	no router rip	

查看 RIP 配置信息	show rip config	
-------------	---------------------------------	--

5.3.10 OSPF 路由配置

功能	命令	说明
进入配置视图	configure terminal	-
OSPF 总开关, 并进入 OSPF 配置视图	router ospf	
关闭 OSPF 功能	no router ospf	
查看 OSPF 配置信息	show ospf config	

OSPF 路由配置模式:

功能	命令	说明
配置 OSPF router id	router-id <i>A.B.C.D</i>	
OSPF MPLS TE 开关	mpls-te on	
关闭 OSPF MPLS TE	no mpls-te	
查看当前视图的配置	show	
退出当前视图, 返回上级视图	exit	

5.3.11 ISIS 路由配置

功能	命令	说明
进入配置视图	configure terminal	-
创建 ISIS 区域, 并进入 ISIS 区域配置视图	router isis area-tag	
删除 ISIS 区域	no router isis area-tag	
查看 ISIS 配置信息	show isis config	

ISIS 路由配置模式:

功能	命令	说明
设置 ISIS hostname	hostname <i>host</i>	
设置 ISIS 等级	is-type <i>level</i>	
配置 NET 地址	net <i>net-addr</i>	

配置度量类型: wide	metric-style style	
ISIS MPLS TE 开关	mpls-te on	
关闭 ISIS MPLS TE	no mpls-te	
MPLS TE 路由器 IP	mpls-te router-address ip-address	
查看当前视图的配置	show	
退出当前视图, 返回上级视图	exit	

5.3.12 防火墙配置

功能	命令	说明
进入配置视图	configure terminal	-
查看防火墙相关配置	show firewall config	
进入防火墙配置视图	firewall configuration	

防火墙配置模式:

功能	命令	说明
公网禁 ping	defend extranet-ping	
关闭公网禁 ping	no defend extranet-ping	
防 syn 泛洪, 不指定 limit 时取默认值	defend syn-flood [limit]	
关闭防 syn 泛洪	no defend syn-flood	
防 dos 攻击	defend dos-attack	
关闭防 dos 攻击	no defend dos-attack	
开启并设置 tcp mss, 默认 1460	tcp-mss [value]	
关闭 tcp mss	no tcp-mss	
设置 tcp 最大连接数, 默认 20000	tcp-contrack-max <1000-50000>	
恢复 tcp 最大连接数到默认	no tcp-contrack-max	

值:20000		
允许 web 外网访问	web-manage internet	
禁止 web 外网访问	no web-manage internet	
允许 web 内网访问	web-manage intranet	
禁止 web 内网访问	no web-manage intranet	
允许 telnet 外网访问	telnet-manage internet	
禁止 telnet 外网访问	no telnet-manage internet	
允许 telnet 内网访问	telnet-manage intranet	
禁止 telnet 内网访问	no telnet-manage intranet	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.13 访问策略配置

功能	命令	说明
进入配置视图	configure terminal	-
创建并进入 ACL 配置视图	ip acl <i>acl-name</i>	
删除 ACL 配置	no ip acl <i>acl-name</i>	
查看 IP ACL 信息	show ip acl [<i>acl-name</i>]	

访问策略配置模式：

功能	命令	说明
设置规则处理策略	policy (deny permit)	
设置匹配协议	protocol (icmp tcp udp)	
设置不匹配协议	no protocol	
设置匹配源地址为 IP	source address ip <i>A.B.C.D</i>	
设置匹配源地址为 IP 段	source address network <i>A.B.C.D A.B.C.D</i>	
设置匹配源地址为 MAC 地址	source address mac <i>address</i>	
设置匹配源地址为 ANY	no source address	

设置匹配目的地址为 IP	destination address ip A.B.C.D	
设置匹配目的地址为 IP 段	destination address network A.B.C.D A.B.C.D	
设置匹配目的地址为 URL	destination address url url	
设置匹配目的地址为 ANY	no destination address	
设置匹配源端口/端口范围	source port start-port [end-port]	
设置不匹配源端口	no source port	
设置匹配目的端口/端口范围	destination port start-port [end-port]	
设置不匹配目的端口	no destination port	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.14 静态 ARP 配置

功能	命令	说明
进入配置视图	configure terminal	-
添加静态 ARP，即 IP 与 MAC 绑定	arp static ip MAC	
删除静态 ARP，即 IP 与 MAC 绑定	no arp static ip MAC	
查看静态 ARP 配置信息	show arp static	

5.3.15 PAT 配置

功能	命令	说明
进入配置视图	configure terminal	-
进入防火墙配置视图	firewall configuration	
创建 PAT	ip pat WORD protocol (tcp/udp) pat-from interface WORD port <1-65535> pat-to A.B.C.D port <1-65535>	

功能	命令	说明
创建 PAT	ip pat <i>WORD</i> protocol (<i>tcp/udp</i>) pat-from interface <i>WORD</i> port-range <1-65535> <1-65535> pat-to <i>A.B.C.D</i>	
创建 PAT	ip pat <i>WORD</i> protocol (<i>tcp/udp</i>) pat-from ip <i>A.B.C.D</i> port <1-65535> pat-to <i>A.B.C.D</i> port <1-65535>	
创建 PAT	ip pat <i>WORD</i> protocol (<i>tcp/udp</i>) pat-from ip <i>A.B.C.D</i> port-range <1-65535> <1-65535> pat-to <i>A.B.C.D</i>	
删除 PAT 配置	no ip pat <i>pat-name</i>	
退出当前视图，返回上级视图	exit	
查看 PAT 配置	show ip pat	

5.3.16 DMZ 配置

功能	命令	说明
进入配置视图	<u>configure terminal</u>	-
进入防火墙配置视图	<u>firewall configuration</u>	
创建 DMZ 配置	ip dmz <i>WORD</i> dmz-from interface <i>WORD</i> dmz-to <i>A.B.C.D</i>	
创建 DMZ 配置	ip dmz <i>WORD</i> dmz-from ip <i>A.B.C.D</i> dmz-to <i>A.B.C.D</i>	
删除 DMZ 配置	no ip dmz <i>dmz-name</i>	
退出当前视图，返回上级视图	exit	
查看 DMZ 配置	show ip dmz	

5.3.17 ALG 配置

功能	命令	说明
进入配置视图	<u>configure terminal</u>	-

ALG 开关	alg (sip rtsp ftp tftp pptp gre all) enable	
关闭 ALG	no alg (sip rtsp ftp tftp pptp gre all) enable	
查看 ALG 配置	show alg	

5.3.18 UPNP 配置

功能	命令	说明
进入配置视图	configure terminal	-
启用 UPNP	upnp up-interface WORD down-interface WORD	
关闭 UPNP	no upnp	
查看 upnp 配置信息	show upnp	

5.3.19 IPSEC 配置

功能	命令	说明
进入配置视图	configure terminal	-
创建 IPSEC，并进入 IPSEC 配置视图	ipsec proposal proposal-name	
删除 IPSEC 配置	no ipsec proposal proposal-name	
清除 IPSEC 信息	clear ipsec sa	
查看 ipsec setkey	show ipsec sa	
查看 ipsec 隧道信息	show ipsec proposal [tunnel-name]	

IPSEC 配置模式：

功能	命令	说明
对端 IP 地址	peer gateway A.B.C.D	
加密接口	encrypt interface interface-name	
IKE 协商模式	ike negotiation mode (aggressive/main)	
共享密码	ike authentication preshared psk-key WORD	
	ike authentication rsa-sig	

IKE 加密提议	ike-proposal encryption-algorithm (3des des aes) integrity-algorithm (md5 sha1 sha256 sha384 sha512) group (group1 group2 group5 group14 group15)	
ipsec 加密提议	ipsec-proposal (esp ah esp_ah) encryption-algorithm (3des des aes) integrity-algorithm (md5 sha1 sha256 sha384 sha512)	
设置安全协议对 IP 报文的封装模式	encapsulation-mode { transport tunnel }	
添加 tunnel 时的本地子网与对端子网	tunnel local-subnet ip/mask remote-subnet ip/mask	
添加 tunnel 时的本地子网/对端子网	tunnel {local-subnet remote-subnet} ip/mask	
删除 tunnel 时的本地子网/对端子网	no tunnel {local-subnet remote-subnet} ip/mask	
启用并配置本地身份	local-id local-id	
关闭本地身份	no local-id	
启用并配置对端身份	peer-id peer-id	
关闭对端身份	no peer-id	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.20 GRE 配置

功能	命令	说明
进入配置视图	configure terminal	-
快捷创建 GRE 隧道	gre tunnel gre-name interface interface	

	destination <i>ipaddress</i> local-tunnel-address <i>ipaddress</i> remote-tunnel-address <i>ipaddress</i>	
快捷创建 GRE 隧道	gre tunnel <i>gre-name</i> interface <i>interface</i> destination <i>ipaddress</i> local-tunnel-address <i>ipaddress</i> remote-tunnel-address <i>ipaddress</i> eoip-interface <i>interface</i>	
创建 GRE 隧道，并进入 GRE 隧道配置视图	gre tunnel <i>gre-name</i>	
删除 GRE 隧道	no gre tunnel <i>gre-name</i>	
查看 GRE 隧道信息	show gre [<i>tunnel-name</i>]	

GRE 配置模式：

功能	命令	说明
源接口	interface <i>interface-name</i>	
目的地址	destination address <i>ip</i>	
隧道地址	tunnel local-address <i>ip</i>	
隧道对端地址	tunnel remote-address <i>ip</i>	
启用 EOIP	eoip interface <i>interface-name</i>	
关闭 EOIP	no eoip	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.21 L2TP 配置

1. L2TP 服务器配置

功能	命令	说明
进入配置视图	configure terminal	-
查看 L2TP 服务器配置	show l2tp server show vpdn l2tp	
查看 VPDN 配置信息(包括 L2TP 和 PPTP 服务器配置)	show vpdn	
查看 /proc/net/ppp0l2tp	show vpdn-l2tp status	

启用 L2TP 服务器	vpdn l2tp	
停用 L2TP 服务器	no vpdn l2tp	
进入 VPDN 配置视图，用于配置 L2TP/PPTP 服务器	vpdn-group WORD	

L2TP 服务器配置模式：

功能	命令	说明
配置 L2TP 服务器地址池	ip-pool start-ip end-ip	-
增加认证用户-密码	authentication username WORD password WORD	
增加绑定 IP 的认证用户-密码	authentication username WORD password WORD bind-ip A.B.C.D	
删除匹配的认证用户-密码	no authentication username WORD password WORD	
开启 L2TP 隧道认证	l2tp tunnel authentication	
L2TP 隧道认证密码	l2tp tunnel password WORD	
关闭 L2TP 隧道认证	no l2tp tunnel authentication	
开启 L2TP 服务器 L2TP OVER IPSEC，并进入配置视图	l2tpipsec	
关闭 L2TP 服务器 L2TP OVER IPSEC	no l2tpipsec	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

L2TP 服务器 IPSEC 配置模式：

功能	命令	说明
配置 IKE 加密提议	ike-proposal encryption-algorithm (3des des aes) integrity-algorithm (md5 sha1) group (group1 group2 group5)	-
配置 IKE 协商模式	ike negotiation mode (aggressive main)	

共享密码	ike authentication preshared psk-key <i>WORD</i>	
ipsec 加密提议	ipsec-proposal (<i>esp/ah/esp_ah</i>) encryption-algorithm (<i>3des/des/aes</i>) integrity-algorithm (<i>md5/sha1</i>)	
启用并配置对端身份	peer-id <i>peer-id</i>	
启用并配置本地身份	local-id <i>local-id</i>	
关闭本地身份	no local-id	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

2. L2TP 客户端配置

功能	命令	说明
进入配置视图	configure terminal	-
查看所有 L2TP 客户端配置	show interface virtual-ppp	
查看指定名称 L2TP 客户端配置	show interface virtual-ppp <i>WORD</i>	
创建并进入虚拟 PPP 接口配置视图，（L2TP/PPTP 客户端）	interface <i>virtual-ppp</i> <i>WORD</i>	
关闭虚拟 PPP 接口（L2TP/PPTP 客户端）	no interface <i>virtual-ppp</i> <i>WORD</i>	

L2TP 客户端配置模式：

功能	命令	说明
配置隧道目的 IP	initiate-to ip <i>A.B.C.D</i>	-
配置隧道出接口	out-interface <i>WORD</i>	
配置隧道认证用户名、密码	ppp pap sent-username <i>WORD</i> password <i>WORD</i>	
开启 L2TP 隧道认证	l2tp tunnel authentication	
L2TP 隧道认证密码	l2tp tunnel password <i>WORD</i>	
关闭 L2TP 隧道认证	no l2tp tunnel authentication	

启用 L2TP 客户端的 l2tp over ipsec 功能，并进入 IPSEC 配置子视图	l2tpoipsec	
关闭 L2TP 客户端的 l2tp over ipsec 功能	no l2tpoipsec	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

L2TP 客户端 IPSEC 配置模式：

功能	命令	说明
配置 IKE 加密提议	ike-proposal encryption-algorithm <i>(3des des aes)</i> integrity-algorithm <i>(md5 sha1)</i> group <i>(group1 group2 group5)</i>	-
配置 IKE 协商模式	ike negotiation mode <i>(aggressive main)</i>	
共享密码	ike authentication preshared psk-key <i>WORD</i>	
ipsec 加密提议	ipsec-proposal <i>(esp ah esp_ah)</i> encryption-algorithm <i>(3des des aes)</i> integrity-algorithm <i>(md5 sha1)</i>	
启用并配置对端身份 hostname	peer-id <i>peer-id</i>	
关闭对端身份 hostname	no peer-id	
启用并配置本地身份 hostname	local-id <i>local-id</i>	
关闭本地身份 hostname	no local-id	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.22 PPTP 配置

1. PPTP 服务器配置

功能	命令	说明
进入配置视图	configure terminal	-
查看 PPTP 服务器配置	show pptp server show vpdn pptp	
查看 VPDN 配置信息(包括 L2TP 和 PPTP 服务器配置)	show vpdn	
启用 PPTP 服务器	vpdn pptp	
停用 PPTP 服务器	no vpdn pptp	
进入 VPDN 配置视图, 用于配置 L2TP/PPTP 服务器	vpdn-group WORD	

PPTP 服务器配置模式:

功能	命令	说明
配置 L2TP 服务器地址池	ip-pool start-ip end-ip	-
增加认证用户-密码	authentication username WORD password WORD	
增加绑定 IP 的认证用户-密码	authentication username WORD password WORD bind-ip A.B.C.D	
删除匹配的认证用户-密码	no authentication username WORD [password WORD]	
查看当前视图的配置	show	
退出当前视图, 返回上级视图	exit	

2. PPTP 客户端配置

功能	命令	说明
进入配置视图	configure terminal	-
查看所有 PPTP 客户端配置	show interface virtual-ppp	
查看指定名称 PPTP 客户端配置	show interface virtual-ppp WORD	
创建并进入虚拟 PPP 接口配置	interface virtual-ppp WORD	

视图, (L2TP/PPTP 客户端)		
关闭虚拟 PPP 接口(L2TP/PPTP 客户端)	<u>no interface</u> virtual-ppp WORD	

PPTP 客户端配置模式:

功能	命令	说明
配置隧道目的 IP	<u>initiate-to</u> ip A.B.C.D	-
配置隧道出接口	<u>out-interface</u> WORD	
配置隧道认证用户名、密码	<u>ppp pap sent-username</u> WORD password WORD	
查看当前视图的配置	<u>show</u>	
退出当前视图, 返回上级视图	<u>exit</u>	

5.3.23 MPLS 配置

功能	命令	说明
进入配置视图	<u>configure terminal</u>	-
查看 MPLS 所有配置	<u>show</u> mpls	
使能 mpls, 并进入 MPLS 配置视图	<u>mpls</u>	
关闭 mpls	<u>no mpls</u>	

1. 静态 LSP 配置

功能	命令	说明
进入配置视图	<u>configure terminal</u>	-
查看 MPLS 静态 LSP	<u>show</u> mpls static-lsp	
配置静态出 LSP	<u>static-lsp</u> egress lsp-name fec ip-address mask nexthop next-hop-address out-label out-label	
删除静态出 LSP	<u>no static-lsp</u> egress lsp-name	
配置静态入 LSP	<u>static-lsp</u> ingress lsp-name in-label in-label	
删除静态入 LSP	<u>no static-lsp</u> ingress lsp-name	

配置静态交换 LSP	static-lsp forward lsp-name in-label in-label nexthop next-hop-address out-label out-label	
删除静态交换 LSP	no static-lsp forward lsp-name	

2. 静态 PW 配置

功能	命令	说明
进入配置视图	configure terminal	-
查看静态 PW 信息	show mpls static-l2vc	
快捷创建静态 PW	static-l2vc WORD ac-interface WORD destination A.B.C.D in-label <16-1048575> out-label <16-1048575> (vlan ethernet) (cw no_cw)	
快捷创建备份静态 PW	static-l2vc WORD ac-interface WORD destination A.B.C.D in-label <16-1048575> out-label <16-1048575> (vlan ethernet) (cw no_cw) secondary	
启用，并配置静态 PW BFD	bfd l2vc WORD interval <50-10000> min_rx <50-10000> multiplier <3-50> mode (active passive) resume <0-3600>	
关闭静态 PW BFD	no bfd l2vc WORD	
开启静态 PW loopback	static-l2vc WORD loopback (enable disable)	

3. 静态 VPLS 配置

功能	命令	说明
进入配置视图	configure terminal	-
查看静态 VPLS 信息	show mpls static-vpls	
快捷创建静态 VPLS	static-vpls WORD ac-interface WORD destination A.B.C.D in-label	

	<16-1048575> out-label <16-1048575> (vlan ethernet) (cw no_cw)	
启用，并配置静态 VPLS BFD	bfd vpls WORD interval <50-10000> min_rx <50-10000> multiplier <3-50> mode (active passive) resume <0-3600>	
关闭静态 VPLS BFD	no bfd vpls WORD	

4. LDP 配置

功能	命令	说明
进入配置视图	configure terminal	-
查看 MPLS LDP 配置	show mpls ldp	
使能 LDP，并进入 LDP 配置视图	mpls ldp	
关闭 MPLS LDP	no mpls ldp	
配置 LDP 实例的 LSR ID	router-id router-id	

5. BGP 配置

功能	命令	说明
进入配置视图	configure terminal	-

6. MPLS TE 配置

功能	命令	说明
进入配置视图	configure terminal	-
MPLS TE 总开关，并进入 MPLS TE 配置视图	mpls te	

MPLS TE 总开关	no mpls te	
添加 RSVP TE 隧道	rsvp-te tunnel destination ip tunnel-id tunnel-id bandwidth bandwidth	
删除 RSVP TE 隧道	no rsvp-te tunnel destination ip tunnel-id tunnel-id bandwidth bandwidth	
查看 MPLS TE 配置	show mpls te	
查看 MPLS TEDB 信息	show mpls tedb	
查看获取的 MPLS TE 路由器列表	show mpls te routers	
查看获取的 RSVP TE 隧道状态	show rsvp te tunnel	
查看 RSVP 会话信息	show rsvp session	
根据 TE 信息，计算到目的地的 CSPF 路径	show cspf-path destination A.B.C.D. bandwidth <1-1000000>	

7. MPLS 转发表查看

功能	命令	说明
进入配置视图	configure terminal	-
查看 MPLS 标签转发信息库	show mpls lfib	

5.3.24 QOS 参数配置

功能	命令	说明
进入配置视图	configure terminal	-
查看 QOS 配置	show qos	
开启 QOS 总开关，并进入 QOS 视图	qos	
关闭 QOS 总开关	no qos	

QOS 配置视图：

功能	命令	说明
QOS 调度模式 PQ	dispatch-mode pq	
QOS 调度模式 WRR，及权重	dispatch-mode wrr weight <0-100> <0-100>	

	<code><0-100> <0-100> <0-100> <0-100> <0-100></code> <code><0-100></code>	
QOS 调度模式 PQ1+WRR7, 及权重	<code>dispatch-mode pq1+wrr7 weight <0-100></code> <code><0-100> <0-100> <0-100> <0-100> <0-100></code> <code><0-100></code>	
QOS 调度模式 PQ2+WRR6, 及权重	<code>dispatch-mode pq2+wrr6 weight <0-100></code> <code><0-100> <0-100> <0-100> <0-100> <0-100></code>	
QOS 调度模式 PQ3+WRR5, 及权重	<code>dispatch-mode pq3+wrr5 weight <0-100></code> <code><0-100> <0-100> <0-100> <0-100></code>	
QOS 调度模式 PQ4+WRR4, 及权重	<code>dispatch-mode pq4+wrr4 weight <0-100></code> <code><0-100> <0-100> <0-100></code>	
QOS 调度模式 PQ5+WRR3, 及权重	<code>dispatch-mode pq5+wrr3 weight <0-100></code> <code><0-100> <0-100></code>	
QOS 调度模式 PQ6+WRR2, 及权重	<code>dispatch-mode pq6+wrr2 weight <0-100></code> <code><0-100></code>	
流控开关	<code>flow-control</code>	
关闭流控开关	<code>no flow-control</code>	
端口限速设置	<code>port port-name rate-limit [ingress ingress-value] egress egress-value</code>	
清除端口限速设置	<code>no port port-name rate-limit</code>	
创建并进入交换芯片 ACL 配置视图	<code>acl acl-name</code>	
删除交换芯片 ACL 配置	<code>no acl acl-name</code>	
查看当前视图的配置	<code>show</code>	
退出当前视图, 返回上级视图	<code>exit</code>	

ACL 配置视图:

功能	命令	说明
添加一个或多个端口到 ACL 规则	<code>port-map port-name</code>	

从 ACL 规则删除一个或多个端口	no port-map <i>port-name</i>	
流类型	flow-type <i>type</i>	
匹配源 MAC	match source-mac <i>mac-address</i>	
关闭匹配源 MAC	no match source-mac	
匹配目的 MAC	match destination-mac <i>mac-address</i>	
关闭匹配目的 MAC	no match destination-mac	
匹配以太网类型	match ethernet-type <i>ethernet-type</i>	
关闭匹配以太网类型	no match ethernet-type <i>ethernet-type</i>	
匹配 VLAN	match vlan <i>vlan-id</i>	
关闭匹配 VLAN	no match vlan <i>vlan-id</i>	
匹配源 IP	match source-address <i>A.B.C.D A.B.C.D</i>	
关闭匹配源 IP	no match source-address	
匹配目的 IP	match destination-address <i>A.B.C.D A.B.C.D</i>	
关闭匹配目的 IP	no match destination-address	
匹配协议	match protocol (<i>icmp/tcp/udp/<0-255></i>)	
关闭匹配协议	no match protocol	
匹配源端口	match source-port <i><1-65535> <1-65535></i>	
关闭匹配源端口	no match source-port	
匹配目的端口	match destination-port <i><1-65535> <1-65535></i>	
关闭匹配目的端口	no match destination-port	
ACL 策略	policy <i>drop/accept</i>	
修改 VLAN	remark vlan <i>vlan-id</i>	
关闭修改 VLAN	no remark vlan	
修改 802.1p	remark 802.1p <i>value</i>	
关闭修改 802.1p	no remark 802.1p	
优先级	remark priority <i>priority</i>	

关闭优先级	no remark priority	
限速	rate-limit rate	
关闭限速	no rate-limit	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.25 GPON 参数配置

功能	命令	说明
进入配置视图	configure terminal	-
查看 GPON 配置	show gpon config	
查看 GPON 状态	show gpon status	
开启 GPON 探测	gpon detect ip ipaddress interface interface	
关闭 GPON 探测	no gpon detect	
设置 GPON OMCI 用户名、密码	omci loid WORD password WORD	

5.3.26 SNMP 参数配置

功能	命令	说明
进入配置视图	configure terminal	-
SNMP 总开关，并进入 SNMP 视图	snmp-agent	
关闭 SNMP 总开关	no snmp-agent	
查看 SNMP 配置	show snmp-agent	

SNMP 配置模式：

功能	命令	说明
SNMP 本地端口	udp-port port	
SNMP 团体名	community community	
SNMP trap 开关	trap enable version 1 2	
关闭 SNMP trap 开关	no trap enable [version 1 2]	

SNMP 服务器 IP 和端口	server-address ip [port port]	
SNMP private trap 开关	private-trap enable	
SNMP private trap 开关	no private-trap enable	
SNMP private trap 周期	private-trap interval interval	
SNMP 区域标识	location location	
查看当前视图的配置	show	
退出当前视图，返回上级视图	exit	

5.3.27 NTP 配置

功能	命令	说明
进入配置视图	configure terminal	-
启用 NTP，并配置 NTP 服务器地址	ntp server server1 [server2]	
设置 NTP 时区	ntp timezone WORD	
关闭 NTP 总开关	no ntp	
查看 NTP 配置	show ntp	

5.3.28 WEB 配置

功能	命令	说明
进入配置视图	configure terminal	
web admin 用户名、码	web admin-user username password	
web guest 用户名、码	web guest-user username password	
开启 web guest 用户	web guest-user enable	
关闭 web guest 用户	no web guest-user	
开启 web ssl	web ssl enable	
关闭 web ssl	no web ssl	
web http 端口	web port port	
web https 端口	web ssl port port	
查看 web 配置	show web config	

--	--	--

5.3.29 系统信息

功能	命令	说明
查看 arp 表	show arp	
查看版本信息	show version	
查看设备信息	show device-info	
查看路由器的时间	show clock/time	
查看 ip 路由表	show ip route	
查看当前目标用户	show target	

5.3.30 日志信息

功能	命令	说明
进入配置视图	configure terminal	-
设置日志输出目的对应的输出等级	log destination priority	<i>destination</i> : 输出目的，如 console/file/syslog/telnet <i>priority</i> : 调试信息输出等级，可行项有： alert/critical/ debug/emergency/error/info/ notice/warning
关闭日志输出到指定目的	no log destination	
配置 syslog 服务器 IP 地址	syslog server A.B.C.D port	
禁用 syslog	no syslog server	
开启日志输出	log on	
关闭日志输出	no log on	

导出日志文件	tftp export log A.B.C.D	
查看 log 配置	show logging	

5.3.31 软件升级

功能	命令	说明
进入配置视图	configure terminal	
系统升级	tftp import sys A.B.C.D firmware	
http 下载	http-download (sys/cfg) file-url	

5.3.32 设备参数

功能	命令	说明
进入配置视图	configure terminal	-
导入参数文件	tftp import cfg A.B.C.D file-name	
导出参数文件	tftp export cfg A.B.C.D file-name	
http 下载	http-download (sys/cfg) file-url	
保存参数	write/save	
清除配置，恢复默认参数	restore default-configuration	
查看当前运行的配置参数	show running-config	

5.3.33 端口镜像命令

功能	命令	说明
端口镜像设置	port-mirroring destination destination - port source source-port direction direction	-
关闭端口镜像	no port-mirroring	
显示端口镜像配置信息	show port-mirroring	

5.3.34 测试工具命令

功能	命令	说明
Ping 测试	ping ip/host	-

traceroute 测试	traceroute ip/host	
telnet 登陆其他设备	telnet ip [port]	

5.3.35 主机名及密码修改

功能	命令	说明
进入配置视图	configure terminal	-
更改路由主机名字	hostname hostname	
同 hostname hostname	rg-hostname hostname	
修改登录密码（进入用户视图）	password password	
修改特权视图的 password 密码	enable password password	
删除特权视图的 password 密码	no enable password	
同 password password	rg-password password	
同 enable password password	rg-enable-password password	
同 no enable password	no rg-enable-password	

5.3.36 系统时间

功能	命令	说明
进入配置视图	configure terminal	-
修改路由器 RTC 的时间	clock set date WORD time WORD	
查看路由器的时间	show clock/time	

5.3.37 重启设备

功能	命令	说明
进入配置视图	configure terminal	-
重启设备	reload	