RG2000 系列路由器
使用说明书

2017-05

版权声明

免责声明

版本信息

RG2000 系列路由器

使用说明书

版本： RG2000-R-V1.00-201705

深圳市拓普泰尔科技有限公司热情为客户提供全方位的技术支持，用户可与就近办事处联系，也可直接与公司客服部联系。

深圳市拓普泰尔科技有限公司

客服热线：400-920-5674

咨询电话：0755-3326 0850

网址：http://www.sztoptel.com/

目　　录

第一章　约定说明

1.1　目的

本说明书用于指导 RG2000 系列路由器的安装调试、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	指 RG2000 系列路由器产品。
\	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
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
GRE	通用路由封装 Generic Routing Encapsulation
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
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
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
SNMP	简单网络管理协议 Simple Network Management Protocol
TCP	传输控制协议 Transmission Control Protocol
UDP	用户数据报协议 User Datagram Protocol

术语	释义说明
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 路由器是深圳市拓普泰尔科技有限公司面向全行业推出的新一代网络产品，融合了 WIFI 技术、路由技术、交换技术、安全技术等多种网络应用技术，自带 5 个 10/100/1000M 以太网接口及 1 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、稳定的传输网络。

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，能源等行业。

RG2000 路由器产品图片如下：

图 2-1 RG2000 产品图片

2.2　功能特点

RG2000 路由器功能特点：

- 支持 5 个 10/100/1000M 以太网接口；
- 支持 1 个 100/1000M SFP 光接口；
- 支持多种协议：TCP/IP，UDP，HTTP，TELNET，ICMP，DHCP，PPPOE，DNS 等；

- 支持静态路由及 RIP/OSPF 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、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 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
2	固定端口	5 个 10/100/1000M 以太接口 1 个 100/1000M SFP 光接口 2 个 WIFI 天线接口 1 个 FUNC 按钮 1 个标准 3 芯电源接口
3	WIFI 模块	802.11 b/g/n，300Mbps 双通道
4	整机尺寸	176mm*134mm*33mm(不含天线、挂件)
5	结构设计	高强度金属外壳
6	整机功耗	≤15W
7	电源输入	DC12V 1.5A
8	工作环境温度	-40～+85° C
9	工作湿度	10～95%RH
10	存储温度	-40～+85° C
11	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 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	SFP	SFP 光接口，可支持 1000M 或 100M 的光模块，通常用作设备 WAN 口。
3	GE0	千兆以太网口，通常用作设备 WAN 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。
4	GE1-GE4	千兆以太网口，通常用作设备 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。
5	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。
6	SYS	设备运行指示灯，闪烁频率为 1 秒亮，1 秒灭。
7	SFP	SFP 接口收光指示灯，亮则表示收有光建立；灭则表示收无光。

序号	名称	说明
8	WLAN	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。

2. 设备后面板

RG2000 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。

注意：

（1）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. 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
	DC12V 1.5A 电源适配器示意图。
	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。
	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）。

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。

2. 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：

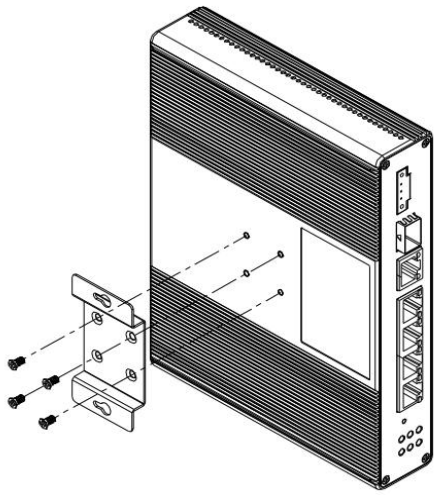

图 2-4 壁挂附件安装示意图

壁挂附件的尺寸如下图所示：

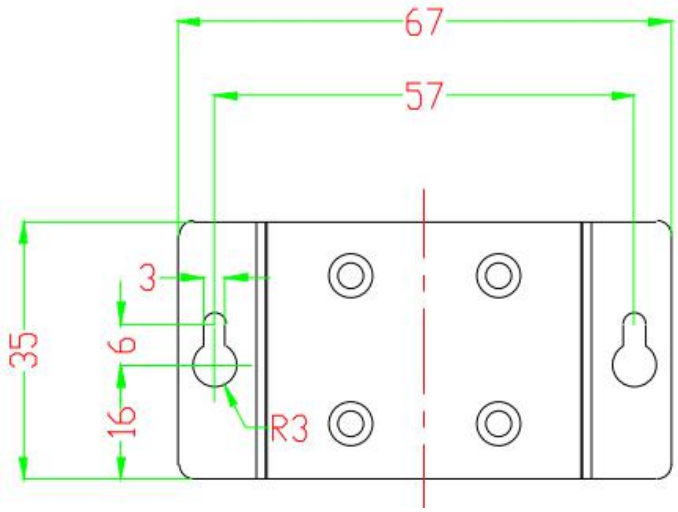

图 2-5 壁挂附件尺寸图

单位：mm。

（2）导轨安装

设备可支持 DIN 导轨安装，如下图所示：

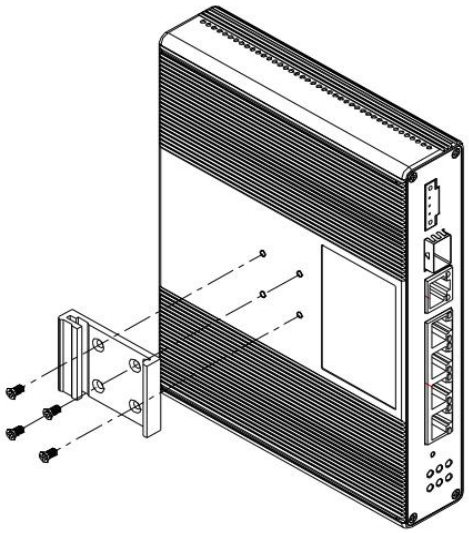

图 2-6 导轨附件安装示意图

导轨附件的尺寸如下图所示：

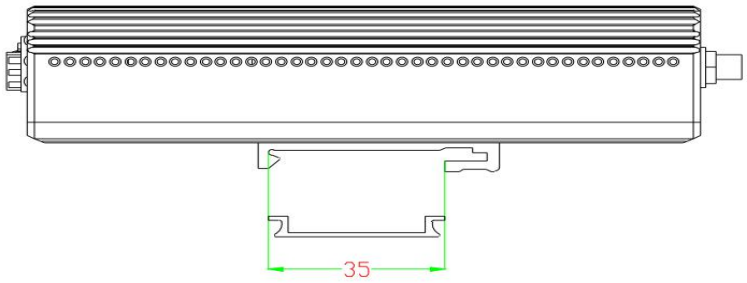

图 2-7 导轨附件尺寸图

单位：mm。

第三章　联机登录

3.1　环境要求

RG2000 路由器对使用环境的要求如下：

- 工作环境温度：-40～+85℃
- 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 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） 网线连接计算机与设备

使用标准网线把计算机以太网口与 RG2000 路由器的 LAN 口（GE1-GE4）连接起来。

3.3　配置计算机

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 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。

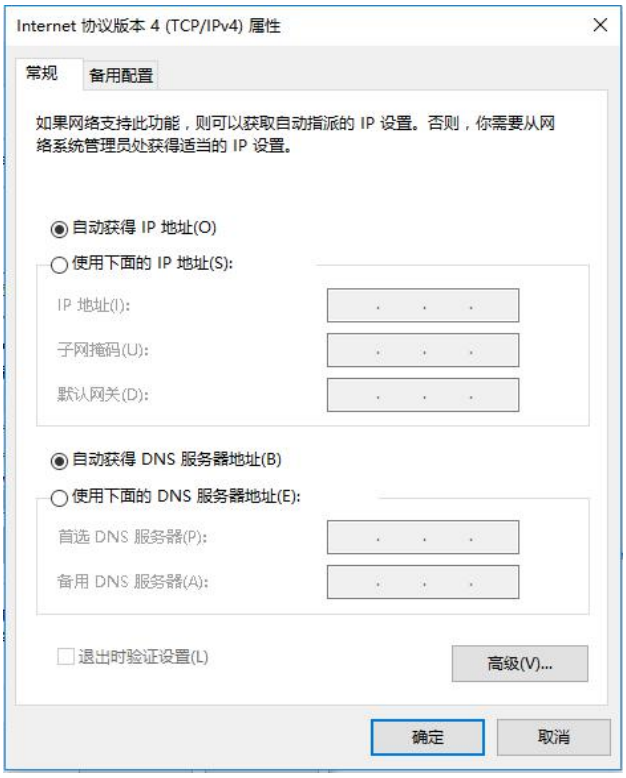

图 3-4 配置网卡 IP 地址

（5） 若选择配置静态 IP，则指定 IP，然后点击确定完成配置。

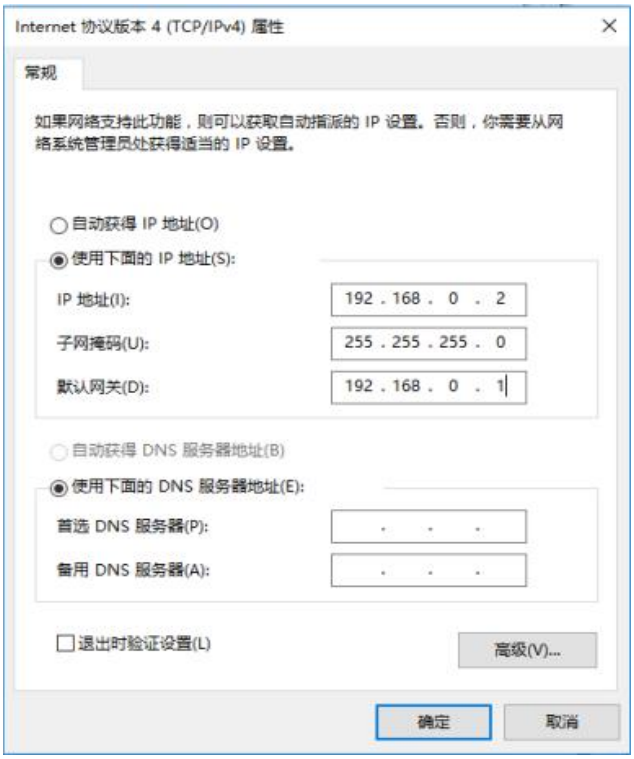

图 3-5 配置网卡 IP 地址

3.4 登录系统

RG2000 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。

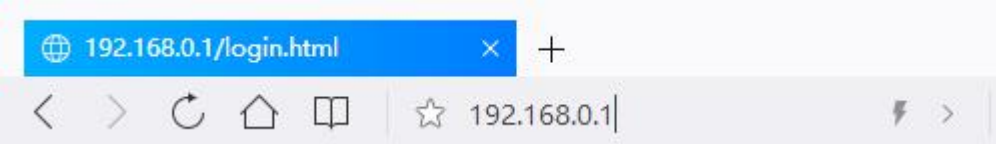

图 3-6 浏览器登录设备

（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

设备状态包含系统信息、WAN 口状态，如下图所示：

图 4-1 设备状态

系统信息包含：设备名称、序列号、软件版本、硬件版本、CPU 占用率、内存占用率、系统时间、运行时间。

WAN 口状态包含：WANO 名称、MAC 地址、连接模式、IP 地址、子网掩码、默认网关、DNS 信息。

设备状态可点击页面下方的“刷新”按钮进行刷新。

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 4-2 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：

图 4-3 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，点击该接口的的“删除”按钮进行操作。

注意：第一个接口不能被删除。

如选择 DHCP 方式，即启用 DHCP 客户端，如下图所示：

图 4-4 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：

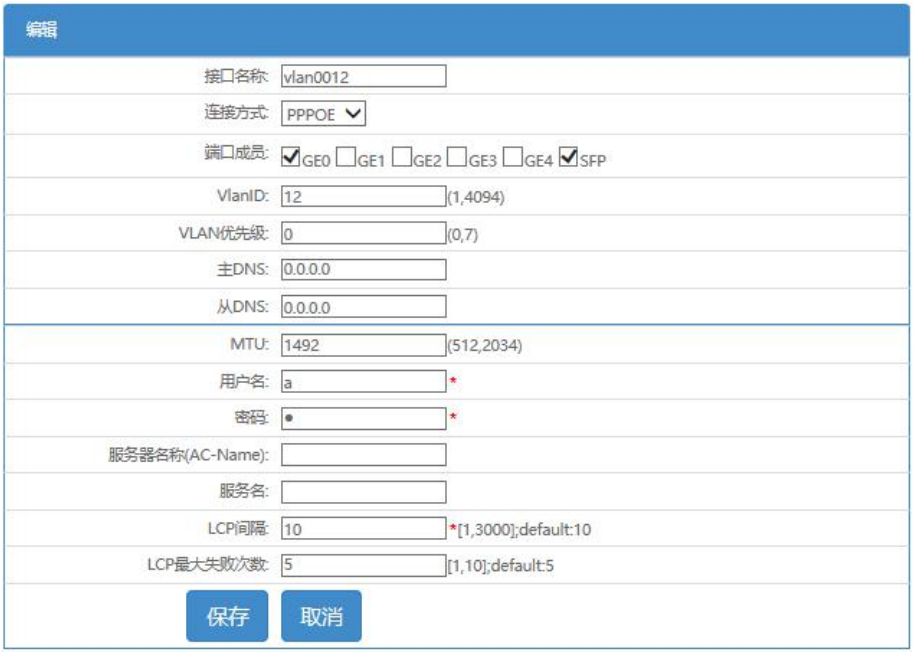

图 4-5 WAN 接口 PPPOE 配置

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 5 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：

图 4-6 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：

图 4-7 LAN 口编辑界面

可修改接口名称，端口成员，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

的“删除”按钮进行操作。第一个接口不能被删除。

说明：最多可添加 5 个 LAN 接口。

注意：WAN 接口及 LAN 接口的 VLAN ID 值不能有冲突。

4.2.2 VLAN 管理

RG2000 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：

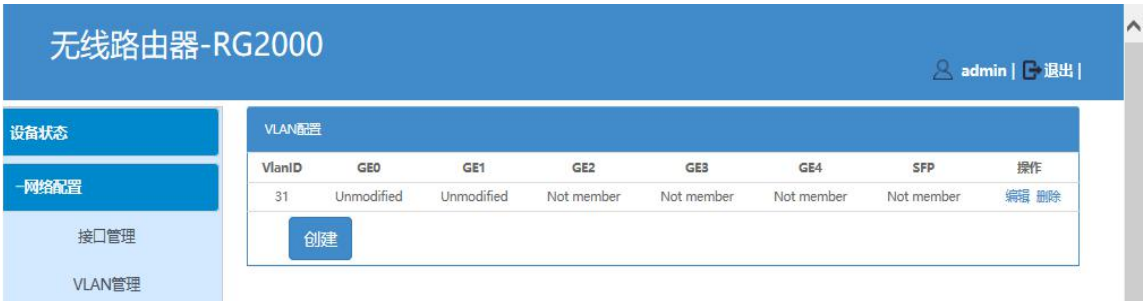

图 4-8 VLAN 管理

如要增加一条 VLAN，点击创建按钮，如下图所示：

图 4-9 VLAN 管理

需配置 VLAN ID，VLAN 成员端口以及 VLAN 优先级。成员端口可包含 GE0-4 以及 SFP 光口。

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 10 条 VLAN 规则。

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

4.2.3 WIFI 配置

1. WIFI 基本参数配置

WIFI 基本配置参数如下图所示：

图 4-10 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：

图 4-11 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：

图 4-12 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；
- 传输功耗：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 4-13 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。

4.2.4 DHCP 配置

1. DHCP 服务器配置

DHCP 服务器配置如下图所示：

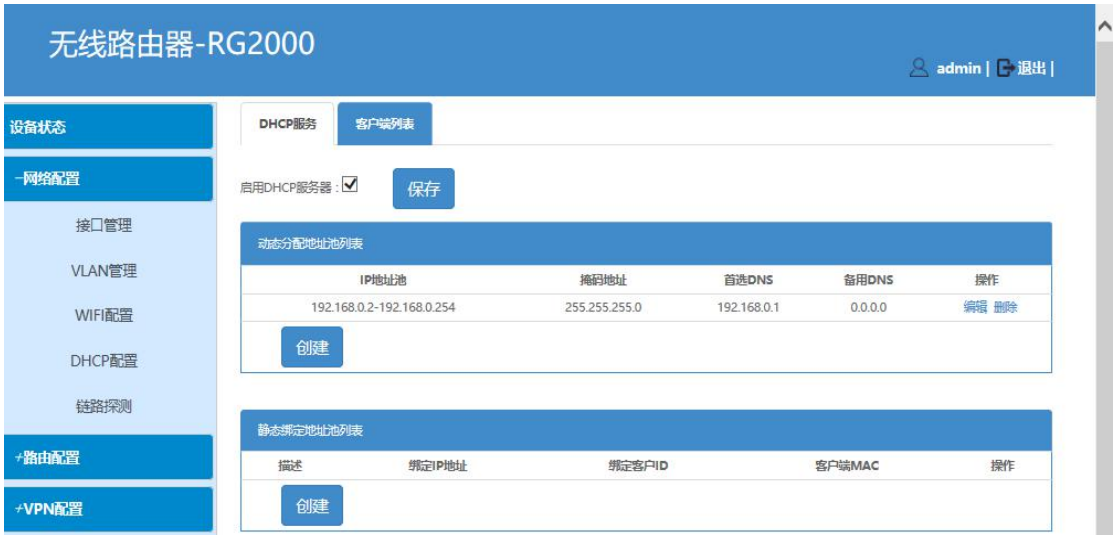

图 4-14 DHCP 服务器配置

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：

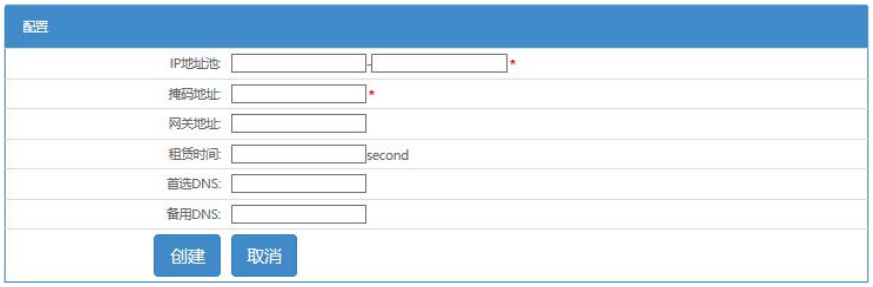

图 4-15 创建动态分配地址池

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：

图 4-16 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：

图 4-17 DHCP 客户端列表

可查看客户端的 IP 地址、MAC 及客户端主机名。

4.2.5 链路探测

链路探测配置如下图所示：

图 4-18 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：

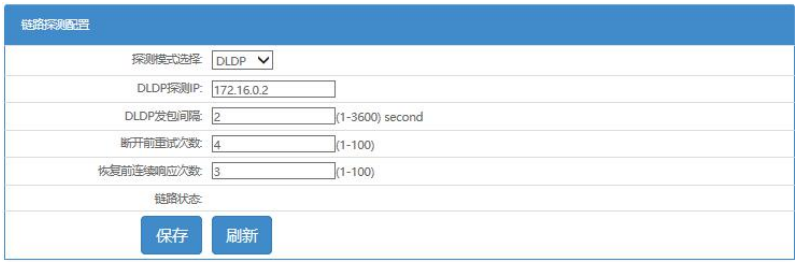

图 4-19 DLDP 配置界面

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：

图 4-20 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：

图 4-21 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：

图 4-22 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：

图 4-23 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：

图 4-24 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 4-25 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 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 4-26 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 4-27 GRE 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

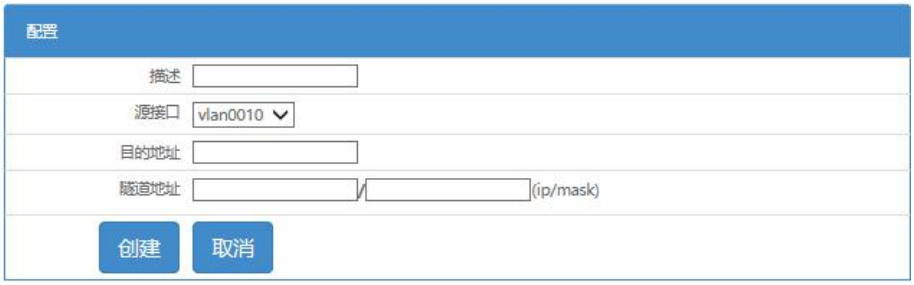

图 4-28 创建 GRE 配置

- 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。

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。

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。

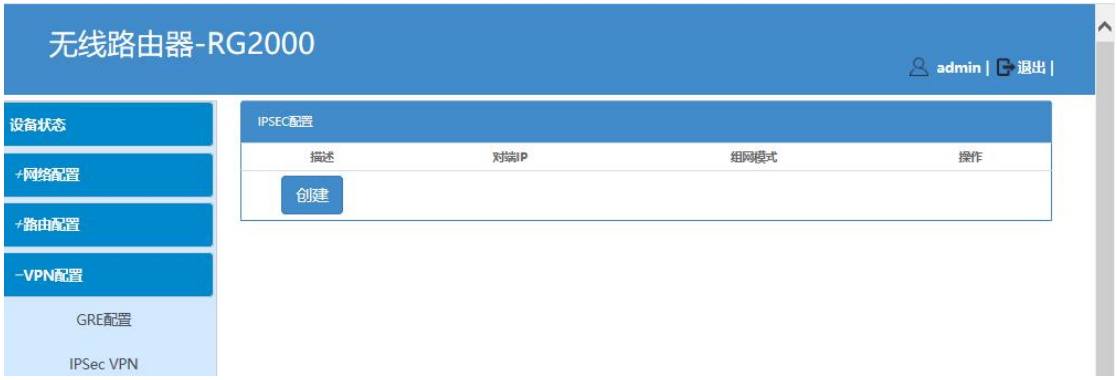

图 4-29 IPSEC 配置

创建一条 IPSEC 如下图所示：

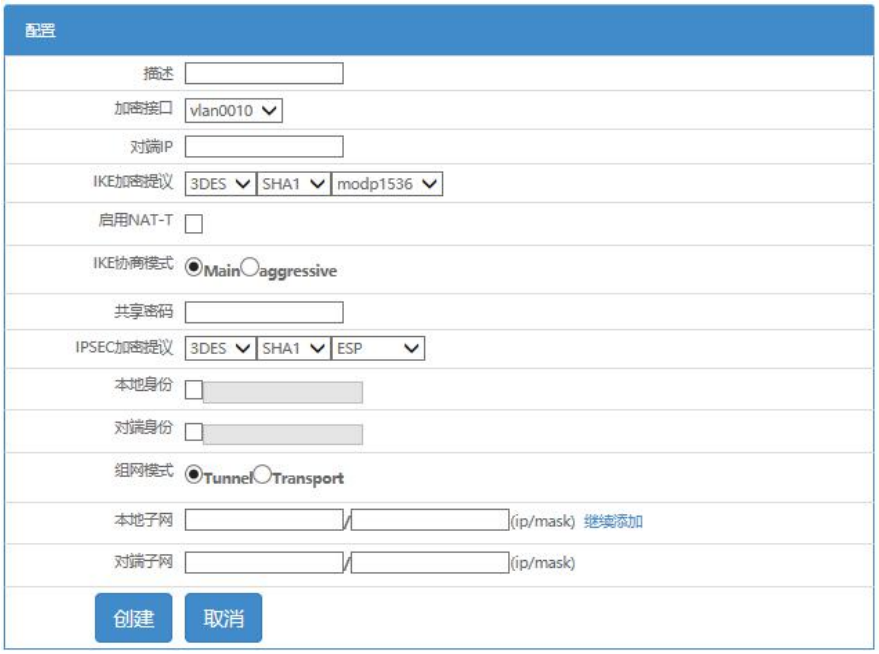

图 4-30 IPSEC 创建

- 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；

- 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；
- 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 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：

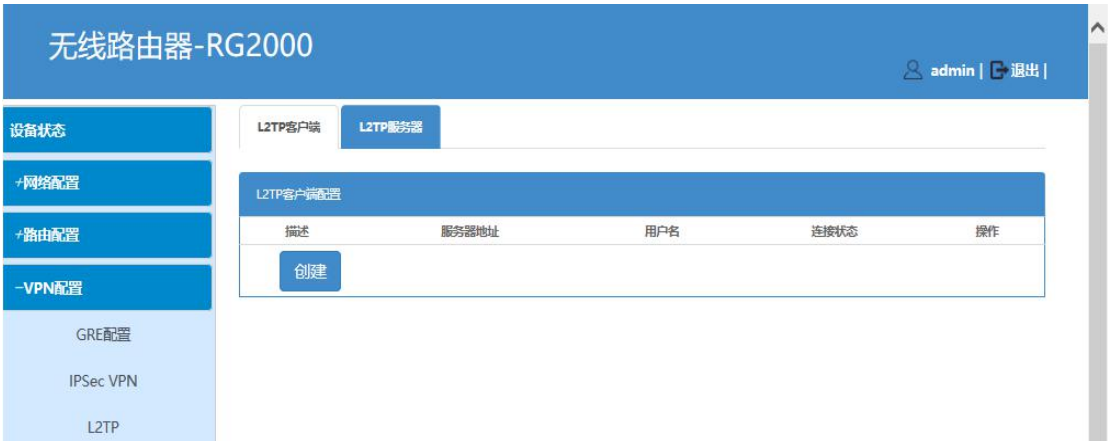

图 4-31 L2TP 客户端配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-32 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 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：

图 4-33 L2TP 服务端配置界面

启用 L2TP 服务器配置如下图所示：

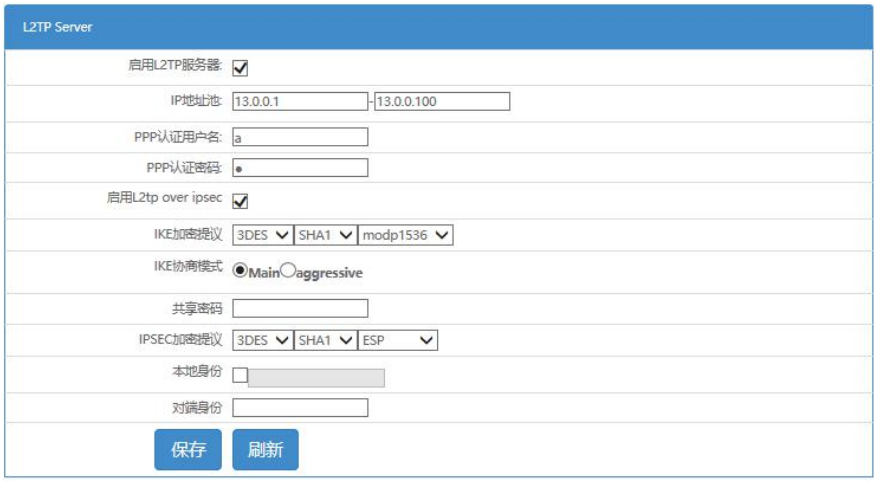

图 4-34 L2TP 服务端配置

- 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；
- 用户名，密码：配置 PPP 认证用户名和密码；
- 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。

4.5 网络安全

4.5.1 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。

图 4-35 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。

4.5.2 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：

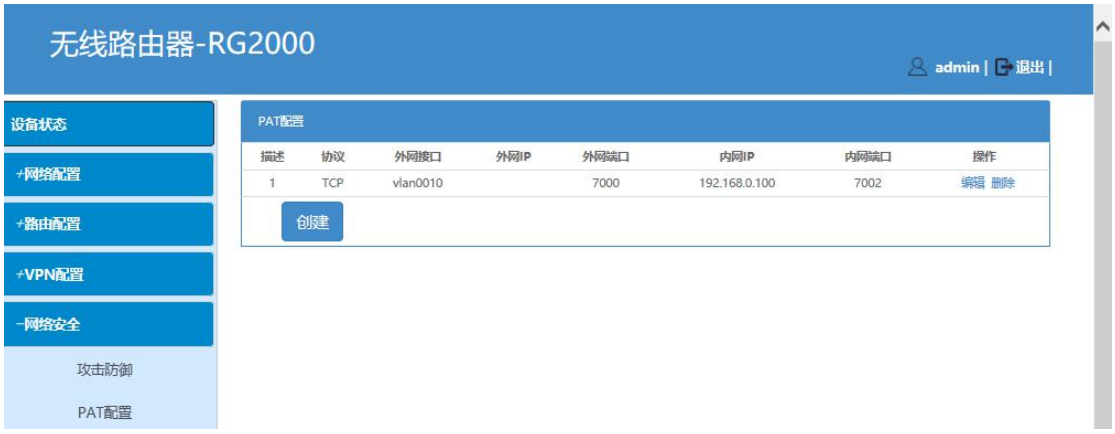

图 4-36 PAT 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-37 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。

4.5.3 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 4-38 DMZ 配置界面

如需创建一条配置，点击创建按钮，如下图所示：

图 4-39 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 系统维护

4.6.1 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 4-40 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。

4.6.2 SNMP 配置

RG2000 支持 SNMP 网管，其配置界面如下：

图 4-41 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。

4.6.3 WEB 管理

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

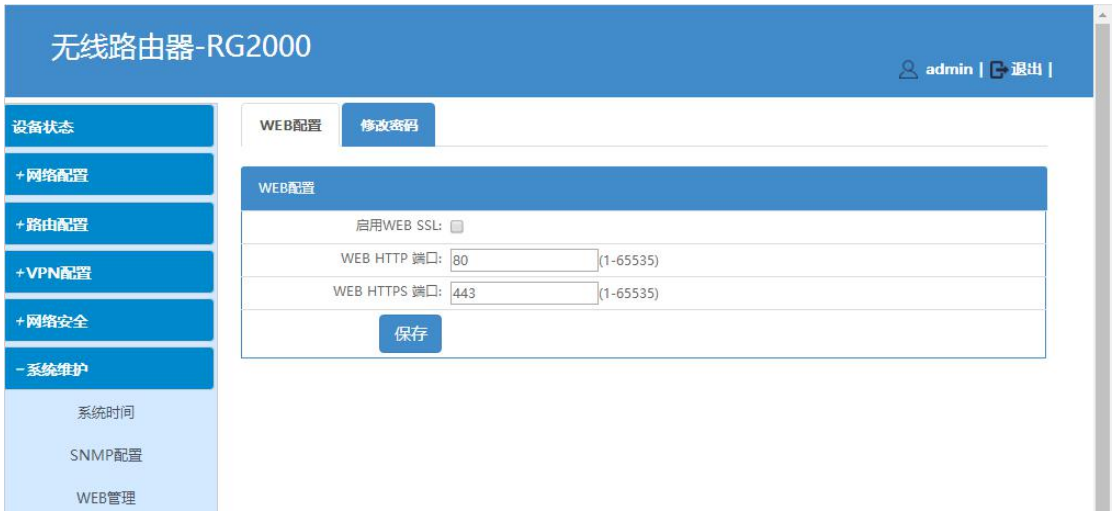

图 4-42 WEB 配置

1. WEB 配置

- 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。

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 4-43 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。

4.6.4 TELNET 设置

登录 RG2000 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。

登录密码修改如下：

图 4-44 Telnet 登录密码修改

修改 enable 模式密码如下：

图 4-45 Telnet enable 模式密码修改

4.6.5 软件升级

RG2000 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 4-46 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 4-47 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。

4.6.6 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 4-48 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。

4.6.7 设备重启

点击菜单栏“系统维护”->“设备重启”，弹出如下界面：

图 4-49 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。

4.6.8 日志管理

RG2000 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。

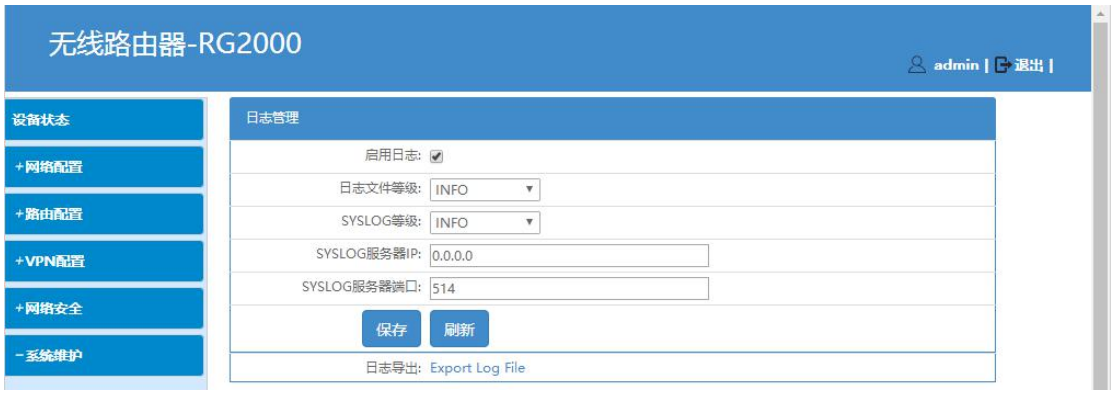

图 4-50 日志管理界面

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。

4.6.9 通信检测

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

1. PING 检测

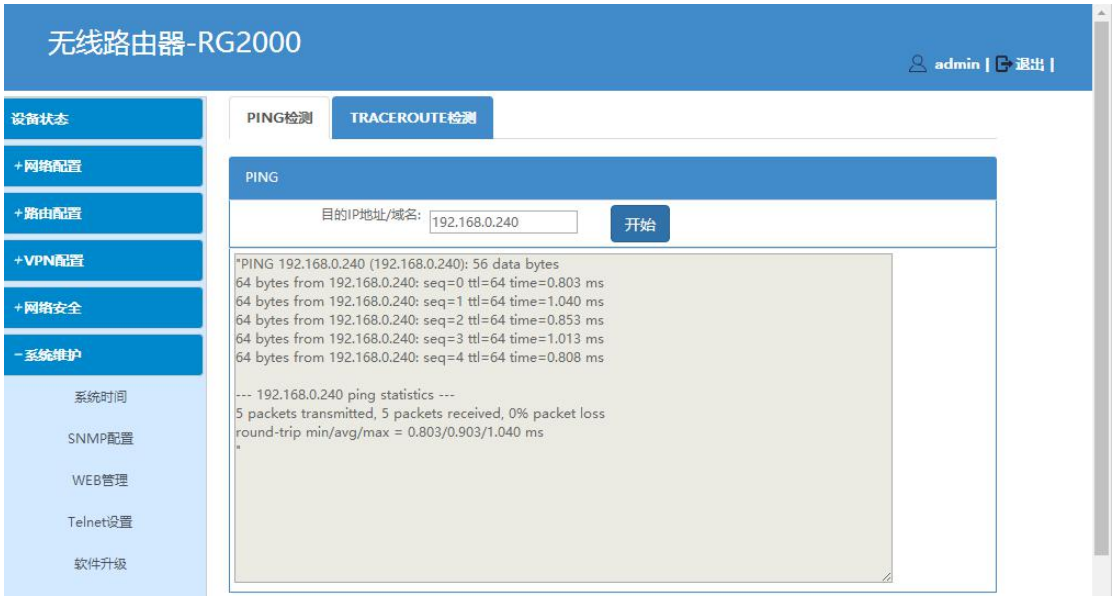

图 4-51 PING 检测

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

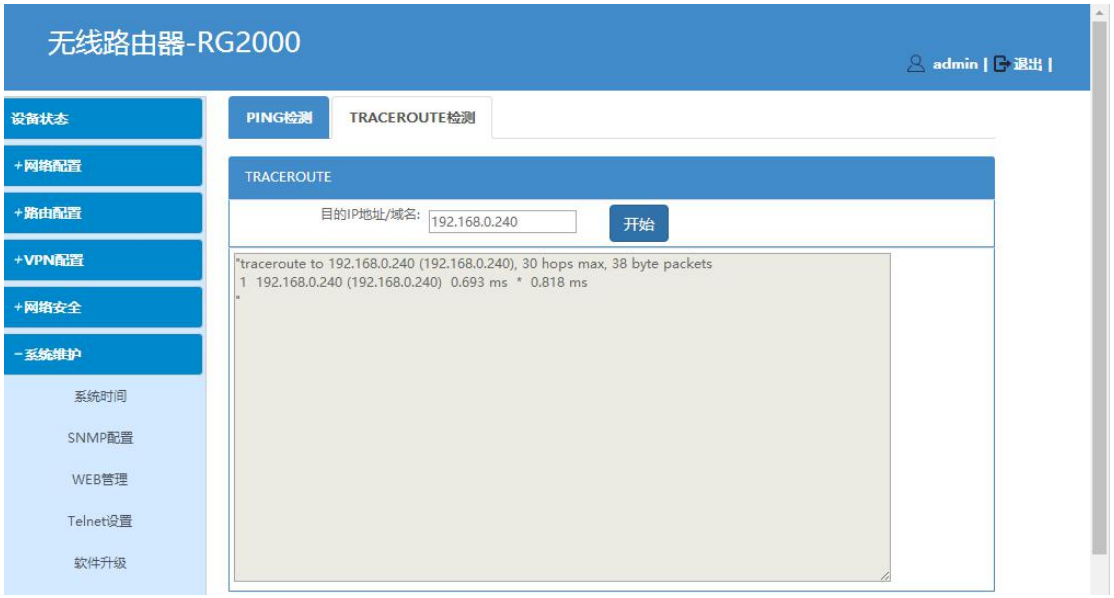

图 4-52 TRACEROUTE 检测

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。

第五章　CLI 命令行介绍

5.1　CLI 概述

RG2000 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：

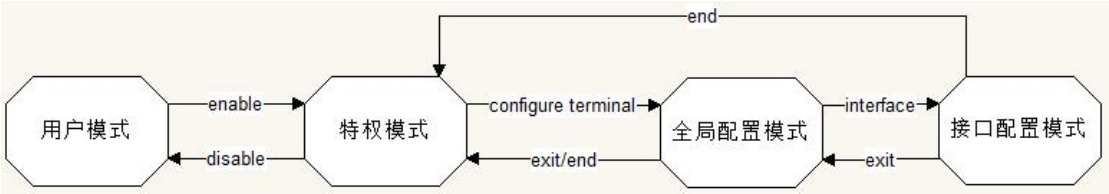

图 5-1 CLI 命令模式切换示意图

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 路由器的缺省主机名为“RG2000”；

（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#?
  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
  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(config)# show port?
  port           Port
  port-mirror    Port mirror control
  port-statistic Port statistics
  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(config)# show port-mirror ?
  <cr>
RG2000(config)# show port-statistic ?
  port  Port name
```

<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(config)# show port-[TAB 键]
port-mirror     port-statistic  port-vlan
RG2000(config)# show port-m[TAB 键]
RG2000(config)# show port-mirror
```

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-statistic 执行关闭端口包统计功能。

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 接口配置

1. WAN 口配置命令

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
进入接口（VLAN 接口）配置模式	**interface vlan** *<1-4094>*	-

步骤	命令	说明
删除接口配置	**no interface vlan** *<1-4094>*	
查看接口配置	**show interface vlan** *<1-4094>*	

2. WAN 接口基本配置

步骤	命令	说明
进入接口（VLAN 接口）配置模式	**interface vlan** *<1-4094>*	必选。 如参数列表中没有指定的接口名称，则创建新的接口；如列表中有指定的接口名称，则进行接口编辑
配置接口类型	**port-type** {**wan**|**lan**}	新创建接口在进入接口配置模式后必须先选择接口类型。 而修改接口时不可修改接口类型。 WAN 口选择 wan。
配置接口端口成员	**port-map** **ge0** (*enable*|*disable*) **ge1** (*enable*|*disable*) **ge2** (*enable*|*disable*) **ge3** (*enable*|*disable*) **ge4** (*enable*|*disable*) **sfp** (*enable*|*disable*)	配置该 VLAN 成员端口。
配置手工指定 DNS 服务器地址	**ip name-server** *ip-address* **second-name-server** *ip-address*	配置 0.0.0.0 表示不使用手工配置的 DNS。
配置 MTU	**mtu** *<512-1500>*	配置 MTU 值。
配置接口的 VLAN 优先级	**vlan pri** *<0-7>*	-
静态 IP 配置	**ip address** *ip-address ip-mask [gateway ip-address]*	配置接口 IP,掩码以及默认网关。
开启 PPPOE 客户端	**pppoe-client enable**	
关闭 PPPOE 客户端	**no pppoe-client enable**	
配置 PPPoe 认证用户名和密码	**ppp sent-username** *username* **password** *password*	
配置 DHCP 客户端	**ip address dhcp**	
关闭 DHCP 客户端	**no ip address dhcp**	
退出接口配置视图	**exit**	

3. LAN 口配置命令

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
进入接口（VLAN 接口）配置模式	**interface vlan** *<1-4094>*	-
删除接口配置	**no interface vlan** *<1-4094>*	
查看接口配置	**show interface vlan** *<1-4094>*	

4. LAN 接口基本配置

步骤	命令	说明
进入接口（VLAN 接口）配置模式	**interface vlan** *<1-4094>*	必选 如参数列表中没有指定的接口名称，则创建新的接口；如列表中有指定的接口名称，则进行接口编辑
配置接口类型	**port-type** {*wan*|*lan*}	新创建接口在进入接口配置模式后必须先选择接口类型。而修改接口时不可修改接口类型。 LAN 口选择 lan
配置接口端口成员	**port-map** **ge0** (*enable*|*disable*) **ge1** (*enable*|*disable*) **ge2** (*enable*|*disable*) **ge3** (*enable*|*disable*) **ge4** (*enable*|*disable*) **sfp** (*enable*|*disable*)	
配置 MTU	**mtu** *<512-2042>*	-
配置接口的 VLAN	**vlan pri** *<0-7>*	-
静态 IP 配置	**ip address** *ip-address ip-mask*	配置接口 IP 及掩码
NAT 配置	**ip nat** (**enable**|**disable**) [**nat-if** *interface-name* | **nat-ip** *ip-address* | **all**]	Nat disable:关闭 NAT nat-if：指定 NAT 接口 nat-ip：指定 NAT IP All：NAT 到所有上行口
退出接口配置视图	**exit**	

5. 端口配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
设置物理端口属性	**port**	auto 表示自协商。速率与双

步骤	命令	说明
	(ge0/ge1/ge2/ge3/ge4) **speed** *(auto/10/100/1000)* **duplex** *(auto/half/full)*	工模式默认皆为自协商。
设置 SFP 接口速率	**port sfp speed** *(100/1000)*	默认为 1000Mbps
查看端口属性	**show port status**	-
开启端口收发包统计功能	**port-statistic** **clear-after-read** *(on/off)*	clear-after-read 设置读完统计信息后统计信息是否清零，on 表示清零，off 不清零
关闭端口收发包统计功能	**no port-statistic**	-
查看端口收发包统计信息	**show port-statistic port** *(gmac0/p0/ge0/ge1/ge2/ge3/ge4/sfp)*	gmac0 表示 CPU GMAC0 端口，p0 表示交换芯片与 CPU GMAC0 连接端口。
查看交换芯片 802.1Q VLAN 配置信息	**show vlan table**	-
查看交换芯片基于端口 VLAN 配置信息	**show port-vlan**	-

5.3.2 DLDP 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
配置 DLDP	**dldp ip** *A.B.C.D* **interval** *<1-3600>* **retry** *<1-100>* **resume** *<1-100>*	配置 DLDP 检测的目的 IP 地址,探测间隔，DOWN 前重传次数，恢复 UP 前连续收到的响应次数
禁用 DLDP	**no dldp**	
查看 DLDP 配置及状态	**show dldp**	

5.3.3 BFD 配置

1. 配置命令

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
配置 BFD	**bfd peer-ip** *A.B.C.D* **mydisc** *<1-100000>* **interval** *<50-10000>* **min_rx** *<50-10000>* **multiplier** *<3-50>* **mode** (active|passive) **resume** *<0-3600>*	配置检测 IP，本地标识,发包间隔，最小收包间隔，检测次数，模式(主动/被动)，保护倒换时间。
禁用 BFD	**no bfd**	
查看 bfd 配置及状态	**show bfd**	

2. 配置示例

配置针对 WAN 0 接口的 BFD，检测对端的设备 IP 是 172.16.0.3。

```
RG2000(config)# bfd peer-ip 172.16.0.3 mydisc 100 interval 1000 min_rx 1000 multiplier 3 mode passive
resume 0
RG2000(config)# show bfd
       BFD : enable
 NeighAddr    TxInter    RxInter DetectMult     Resume       Mode  LocalDisc RemoteDisc Status
172.16.0.3       1000       1000          3          0    passive        100       8192 UP
```

查看配置及状态，状态为 UP，学习到对端的标识为 8192。

5.3.4 路由配置

1. 静态路由配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
添加静态路由[出口选择网关地址]	**static-route** *route_name* **destination** *A.B.C.D/M* **gateway** *A.B.C.D*	出口选择网关地址
添加静态路由[出口选择接口]	**static-route** *route_name* **destination** *A.B.C.D/M* **out-interface** *interface_name*	出口选择接口
删除静态路由	**no static-route** *route_name*	
查看静态路由配置	**show static-route**	

（1）interface_name：选择接口方式时，对应接口名称。当接口名不确定时候，可先输入一个错误的接口名，设备会给出提示，然后从提示中选择一个需配置的接口名，例如：

```
RG2000(config)# static-route 1 destination 10.0.0.1/24 out-interface ww
Can not find any up net interface name "ww"! Please check up net-if name
        wan if name:
                vlan0010
```

WAN 接口名称为“vlan10”。

（2）A.B.C.D/M：A.B.C.D 表示 IP 地址或网段，M 为子网掩码的数字值，例如，子网掩码“255.255.255.0”对应数字 24。

2. 策略路由配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
添加策略路由[出口选择网关地址]	**policy-route route_name src** *A.B.C.D/M* **dst** *A.B.C.D/M* **gw** *A.B.C.D*	出口选择网关地址
添加策略路由[出口选择网关地址]	**policy-route route_name src** *A.B.C.D/M* **dst** *A.B.C.D/M* **protocol** *tcp/udp* **startport** *port* **endport** *port* **gw** *A.B.C.D*	出口选择网关地址，指定协议，端口。
添加策略路由[出口选择接口]	**policy-route route_name src** *A.B.C.D/M* **dst** *A.B.C.D/M* **out-interface** *interface_name*	出口选择接口
添加策略路由[出口选择接口]	**policy-route route_name src** A.B.C.D/M **dst** *A.B.C.D/M* **protocol** *tcp/udp* **startport** *port* **endport** *port* **out-interface** *interface_id*	出口选择接口，指定协议，端口。
删除策略路由	**no policy-route route_name**	
查看策略路由配置	**show policy-route**	

（1）src/dst A.B.C.D/M 配置为 0.0.0.0/0 时表示 any src /any dst。

（2）interface_name：同静态路由配置。

3. 路由状态查看

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
查看路由命令	**show ip route**	

5.3.5 PAT 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
添加或修改 PAT 命令	**ip pat pat-name protocol** (*tcp/udp*) **pated-netif** *up-netif-name* <*1-65535*> **pat-to** *A.B.C.D* <*1-65535*>	指定上行接口
添加或修改 PAT 命令	**ip pat pat-name protocol** (*tcp/udp*) **pated-ip** *A.B.C.D* <*1-65535*> **pat-to** *A.B.C.D* <*1-65535*>	指定上行被 PAT 映射的 IP
删除 PAT 命令	**no ip pat pat-name**	
查看 PAT 命令	**show ip pat**	

（1）pated-netif：指上行被 PAT 映射接口；

（2）pated-ip：指上行被 PAT 映射的 IP；

（3）pat-to：指内网的地址，端口。

5.3.6 DMZ 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
添加或修改 dmz 命令	**ip dmz** *dmz-name* **dmzed-netif** *up-netif-name* **dmz-to** *A.B.C.D*	指定上行接口
添加或修改 dmz 命令	**ip dmz** *dmz-name* **dmzed-ip** *A.B.C.D* **dmz-to** *A.B.C.D*	指定上行被 DMZ 映射的 IP
删除 DMZ 命令	**no ip dmz dmz-name**	
查看 DMZ 命令	**show ip dmz**	

（1）dmzed-netif：指上行被 dmz 映射接口

（2）dmzed-ip：指上行被 dmz 映射的 IP

（3）dmz-to：指内网的地址，端口。

5.3.7 IPSEC 配置

1. 全局命令

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
删除 IPSEC 隧道	**no crypto tunnel tunnel-name**	
查看 IPSEC 隧道配置	**show crypto tunnel** [*tunnel-name*]	不指定 tunnel-name 时，查看所有 IPSEC 隧道的配置
显示 IKE SA 状态	**show crypto ike sa**	
显示 IPSEC SA 状态	**show crypto ipsec sa**	

2. 隧道配置命令

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
进入对应隧道配置模式	**crypto tunnel** *tunnel-name*	当 IPSEC 隧道不存在时，创建隧道
配置加密接口	**set encryp-netif** *netif-name*	netif-name 表示接口的名称
配置对端地址	**set peer** *ip-address*	0.0.0.0 表示 any

步骤	命令	说明
配置 IKE 第一阶段协商模式	**set mode** { *aggressive* | *main* }	
配置 IKE 的认证方式	**set authentication** {*preshared*|*rsa-sig*} [**ike-key** *key-string*]	
配置 IKE 提议参数	**set ike-proposal encryption** { *3des* | *des* | *aes* } **integrity** { *md5* | *sha1*} **group** { *group1* | *group2* | *group5* }	
配置 IPSEC 提议	**set ipsec-proposal** {*esp*|*ah*|*esp_ah*} **encryption** { *3des* | *des* | *aes128* } **integrity** { *md5* | *sha1*}	
配置 IPSEC 安全策略	**set flow mode** {*transport* | *tunnel* } [*source-ip-address mask destination-ip-address mask*]	
配置对端身份标识	**set peer-id** {*enable*|*disable*} [**id** *WORD*]	disable 表示认证方式采用对端 IP 地址作为对端身份，enable 情况需要带后面 id 参数，表示采用指定 id 名称进行认证
配置本地身份标识	**set local-id** {*enable*|*disable*} [**id** *WORD*]	disable 表示认证方式采用本地 IP 地址作为本端身份，enable 情况需要带后面 id 参数，表示采用指定 id 名称进行认证
显示当前隧道的配置	**display**	
退出 IPSEC 隧道配置模式	**exit**	

名称	加密算法	认证算法	Diffie-Hellman组	生命期（秒）
g1-des-sha1	DES	SHA1	1（768 位模数）	86400
g1-des-md5	DES	MD5	1（768 位模数）	86400
g2-3des-sha1	3DES	SHA1	2（1024位模数）	86400
g2-3des-md5	3DES	MD5	2（1024位模数）	86400
g2-aes128-sha1	AES128	SHA1	2（1024位模数）	86400
g2-sm1-sha1	SM1	SHA1	2（1024位模数）	86400
g5-3des-sha256	3DES	SHA2-256	5 (1536位模数)	86400
g5-aes256-sha256	AES256	SHA2-256	5 (1536位模数)	86400

3. 隧道模式配置示例

（1）网络需求

Device1 和 Device2 之间采用隧道模式建立 IPsec 隧道，保护 PC1 和 PC2 所在网络的数据通信。

IPsec 提议安全协议采用 ESP，IKE 提议和 IPsec 提议加密算法采用 3DES，认证算法采用 SHA1。认证采用预共享密钥方式，共享密码“123456”。

（2）网络拓扑

步骤 1：配置各接口的 IP 地址和路由。（略）

步骤 2：配置 IKE、IPsec 提议、预共享密钥、IPsec 隧道、IPsec 安全策略

Device1：

```
RG2000# configure terminal
RG2000(config)# crypto tunnel ipsec1
RG2000(config-tunnel)#set authentication preshared psk-key 123456
```

```
RG2000(config-tunnel)# set ike-proposal encryption 3des integrity sha1 group group5
RG2000(config-tunnel)# set ipsec-proposal esp encryption des integrity sha1
RG2000(config-tunnel)# set mode main
RG2000(config-tunnel)# set encryp-netif vlan0010
RG2000(config-tunnel)# set peer 151.255.24.24
RG2000(config-tunnel)# set flow mode tunnel local 100.0.0.1/24 remote 101.0.0.1/24
RG2000(config-tunnel)# display

                description : ipsec1
                   vpn mode : tunnel
               encrypt netif : vlan0010
                        peer : 151.255.24.24
                local subnet : 100.0.0.1/24
               remote subnet : 101.0.0.1/24
                ike-proposal : 3des-sha1-modp1536
                 negotiation : main
             authentication  : preshared
                   psk key   : 123456
              ipsec-proposal : ESP-des-sha1
```

Device2：

```
RG2000# configure terminal
RG2000(config)# crypto tunnel ipsec1
RG2000(config-tunnel)#set authentication preshared psk-key 123456
RG2000(config-tunnel)# set ike-proposal encryption 3des integrity sha1 group group5
RG2000(config-tunnel)# set ipsec-proposal esp encryption des integrity sha1
RG2000(config-tunnel)# set mode main
RG2000(config-tunnel)# set encryp-netif vlan0010
RG2000(config-tunnel)# set peer 129.255.169.15
RG2000(config-tunnel)# set flow mode tunnel local 101.0.0.1/24 remote 100.0.0.1/24
RG2000(config-tunnel)# display

                description : ipsec1
                   vpn mode : tunnel
               encrypt netif : vlan0010
                        peer : 129.255.169.15
                local subnet : 101.0.0.1/24
               remote subnet : 100.0.0.1/24
                ike-proposal : 3des-sha1-modp1536
                 negotiation : main
             authentication  : preshared
                   psk key   : 123456
              ipsec-proposal : ESP-des-sha1
```

（3）检验结果

PC1 与 PC2 间能经过 Device1 和 Device2 之间的 IPsec 隧道互相 ping 通，报文被 IPsec 隧道保护。

4. 传输模式配置示例

（1）网络需求

Device1 和 Device2 之间采用传输模式建立 IPsec 隧道，保护 Device1、Device2 之间端到端的数据通信。

IPsec 提议采用安全协议 ESP，ESP 加密算法采用 DES，认证算法采用 MD5，IKE 提议加密算法采用 DES，认证算法采用 MD5。认证采用预共享密钥方式，共享密码“123456”。

（2）网络拓扑

步骤 1：配置各接口的 IP 地址和路由。（略）

步骤 2：配置 IKE、IPsec 提议、预共享密钥、IPsec 隧道、IPsec 安全策略。

Device1：

```
RG2000# configure terminal
RG2000(config)# crypto tunnel ipsec1
RG2000(config-tunnel)#set authentication preshared psk-key 123456
RG2000(config-tunnel)# set ike-proposal encryption des integrity md5 group group5
RG2000(config-tunnel)# set ipsec-proposal esp encryption des integrity md5
RG2000(config-tunnel)# set mode main
RG2000(config-tunnel)# set encryp-netif vlan0010
RG2000(config-tunnel)# set peer 151.255.24.24
RG2000(config-tunnel)# set flow mode transport
RG2000(config-tunnel)# display

                description : ipsec1
                   vpn mode : transport
              encrypt netif : vlan0010
                       peer : 151.255.24.24
             ike-proposal : des-md5-modp1536
              negotiation : main
           authentication  : preshared
                 psk key   : 123456
```

```
        ipsec-proposal : ESP-des-md5
```

Device2：

```
RG2000# configure terminal
RG2000(config)# crypto tunnel ipsec1
RG2000(config-tunnel)#set authentication preshared psk-key 123456
RG2000(config-tunnel)# set ike-proposal encryption des integrity md5 group group5
RG2000(config-tunnel)# set ipsec-proposal esp encryption des integrity md5
RG2000(config-tunnel)# set mode main
RG2000(config-tunnel)# set encryp-netif vlan0010
RG2000(config-tunnel)# set peer 129.255.169.15
RG2000(config-tunnel)# set flow mode transport
RG2000(config-tunnel)# display

          description : ipsec1
             vpn mode : transport
        encrypt netif : vlan0010
                 peer : 129.255.169.15
         ike-proposal : des-md5-modp1536
          negotiation : main
       authentication  : preshared
             psk key  : 123456
        ipsec-proposal : ESP-des-md5
```

（3）检验结果

Device1 与 Device2 间能 ping 通，报文被 IPsec 隧道保护。

5.3.8 L2TP 配置

1. 全局配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
删除虚拟 PPP 接口的配置	**no interface virtual-ppp name**	
查看 L2TP 信息	**show vpdn detail**	
查看虚拟 PPP 接口模板配置列表	**show interface virtual-ppp** [*name*]	不指定 name 时，查看所有隧道的配置
查看 LNS 配置	**show vpdn-group lns**	

2. LNS 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-

启用或禁用 L2TP SERVER	**vpdn** {*enable*|*disable*}	
进入 VPDN 组配置视图	**vpdn-group lns**	
进入 L2TP LNS 配置视图	**accept-dialin**	
配置 L2TP 服务器 IP 池	**ippool start** *A.B.C.D* **end** *A.B.C.D*	
配置 PPP 认证用户名密码	**ppp auth_user** *WORD* **auth_password** *WORD*	
配置是否启用 L2TP OVER IPSEC	**l2tpoipsec** {*enable*|*disable*}	
配置 IPSEC 提议	**psec-proposal** {*esp*|*ah*|*esp_ah*} **encryption** {*3des*|*des*|*aes128*} **integrity** { *md5* | *sha1*}	
配置 IKE 第一阶段协商模式	**ike-mode** { *aggressive* | *main* }	
配置 IKE 的认证方式	**ike-authentication** { *preshared* | *rsa-sig*} [**ike-key** *key-string*]	
配置 IKE 提议参数	**ike-proposal encryption** { *3des*| *des* | *aes* } **integrity** { *md5*|*sha1*} **group** { *group1* | *group2* | *group5* }	
配置对端身份标识，	**peer-id enable id** *WORD*	表示采用指定 id 名称进行认证，peer-id 可使用 IP 地址字符串方式
配置本地身份标识	**local-id** {*enable*|*disable*} [**id** *WORD*]	disable 表示认证方式采用本地 IP 地址作为本端身份，enable 情况需要带后面 id 参数，表示采用指定 id 名称进行认证
退出 LNS 配置视图	**exit**	

3. LAC 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
进入 PPP 配置视图	**interface virtual-ppp** *name*	PPP 接口已存在则进入特定 PPP 接口的 PPP 配置视图，不存在则创建虚拟 PPP 接口
配置 PPP 为 L2TP 连接，并且对端服务器的 IP 地址	**pseudowire** *ip-address* **pw-class l2tp out-interface** *netif-name*	
配置 PPP 认证用户名和密码	**ppp pap sent-username** *username* **password**	

步骤	命令	说明
	password	
配置是否启用 L2TP OVER IPSEC	**l2tpoipsec** {*enable*|*disable*}	
配置 IPSEC 提议	**psec-proposal** {*esp*|*ah*|*esp_ah*} **encryption** { *3des* | *des* | *aes128* } **integrity** { *md5* | *sha1*}	
配置 IKE 第一阶段协商模式	**ike-mode** { *aggressive* | *main* }	
配置 IKE 的认证方式	**ike-authentication** { *preshared* | *rsa-sig*} [**ike-key** *key-string*]	
配置 IKE 提议参数	**ike-proposal encryption** { *3des* | *des* | *aes* } **integrity** { *md5* | *sha1*} **group** { *group1* | *group2* | *group5* }	
配置对端身份标识，	**peer-id** {*enable*|*disable*} [**id** *WORD*]	disable 表示认证方式采用对端 IP 地址作为对端身份，enable 情况需要带后面 id 参数，表示采用指定 id 名称进行认证
配置本地身份标识	**local-id** {*enable*|*disable*} [**id** *WORD*]	disable 表示认证方式采用本地 IP 地址作为本端身份，enable 情况需要带后面 id 参数，表示采用指定 id 名称进行认证
退出 PPP 接口配置视图	**exit**	

4. L2TP over ipsec 配置示例

（1）网络需求

Device1 作为 LAC,Device2 作为 LNS,Netwok-Center 作为数据中心。Device1 通过公网地址与 Device2 之间建立 IPsec，之后再建立 L2TP 连接，以 IPsec 的传输模式保护 device1 与 Device2 之间的 L2TP 数据通信。

Device1 与设备 Device2 建立 L2TP 隧道，针对 Device1 下的 PC1 添加路由，针对 Device2 下的 PC2（数据中心）添加路由，PC1 能与 PC2（数据中心）的通信，通信数据受 IPSEC 保护。

（2）网络拓扑

（3）Device1 配置

步骤 1：配置各接口的 IP 地址和路由。（略）

步骤 2：配置 L2TP LAC，服务器 IP 151.25.24.24，PPP 认证用户名密码：test/test。

```
rg2000# configure terminal
rg2000(config)# interface virtual-ppp l2tpc
rg2000(config-if-virtual-ppp)#    pseudowire    151.25.24.24    pw-class    l2tp
out-interface vlan0010
rg2000(config-if-virtual-ppp)# ppp pap sent-username test password test
```

以下为 OVER IPSEC 配置，如果不使用 IPSEC，只需要使用命令 l2tpoipsec disable 即可。

IKE 认证方式使用 PSK，PSK 密码 123456，身份认证使用 NAME 方式，所以协商方式使用 aggressive。本地身份标识 client，对端身份标识 server。

```
rg2000(config-if-virtual-ppp)# l2tpoipsec enable
rg2000(config-if-virtual-ppp)# ike-authentication preshared psk-key 123456
rg2000(config-if-virtual-ppp)# ike-mode aggressive
rg2000(config-if-virtual-ppp)# ike-proposal encryption 3des integrity sha1 group
group5
rg2000(config-if-virtual-ppp)# ipsec-proposal esp encryption des integrity sha1
rg2000(config-if-virtual-ppp)# local-id enable id client
rg2000(config-if-virtual-ppp)# peer-id enable id server
rg2000(config-if-virtual-ppp)# exit
rg2000(config)# show interface virtual-ppp l2tpc
                  description : l2tpc
                   out net-if : vlan0010
              peer ip address : 151.25.24.24
            ppp auth username : test
            ppp auth password : test
              L2TP over ipsec : enable
                 ike-proposal : 3des-sha1-modp1536
                  negotiation : aggressive
              authentication  : preshared
                     psk key  : 123456
               ipsec-proposal : ESP-des-sha1
```

```
                local id type : name
                local id Name : client
               remote id type : name
               remote id Name : server
```

（4）Device2 配置

步骤 1：配置各接口的 IP 地址和路由。（略）

步骤 2：配置 L2TP LNC，PPP 认证用户名密码：test/test，IP 池 10.0.0.1-10.0.0.2。

```
rg2000# configure terminal
rg2000(config)# vpdn enable
rg2000(config)# vpdn-group lns
rg2000(config-vpdn)# accept-dialin
rg2000(config-vpdn-acc-in)# ppp auth_user test auth_password test
rg2000(config-vpdn-acc-in)# ippool start 10.0.0.1 end 10.0.0.2
```

以下为 OVER IPSEC 配置，如果不使用 IPSEC，只需要使用命令 l2tpoipsec disable 即可。

IKE 认证方式使用 PSK，PSK 密码 123456，身份认证使用 NAME 方式，所以协商方式使用 aggressive。本地身份标识 server，对端身份标识 client。

```
rg2000(config-vpdn-acc-in)# l2tpoipsec enable
rg2000(config-vpdn-acc-in)# ike-authentication preshared psk-key 123456
rg2000(config-vpdn-acc-in)# ike-mode aggressive
rg2000(config-vpdn-acc-in)# ike-proposal encryption 3des integrity sha1 group
group5
rg2000(config-vpdn-acc-in)# ipsec-proposal esp encryption des integrity sha1
rg2000(config-vpdn-acc-in)# local-id enable id server
rg2000(config-vpdn-acc-in)# peer-id enable id client

rg2000(cconfig-vpdn-acc-in)# exit
rg2000(config-vpdn)# exit
rg2000(config)# show vpdn-group lns
                  L2TP server : enable
                      ip pool : 10.0.0.1-10.0.0.2
             ppp auth username : test
             ppp auth password : test
               L2TP over ipsec : enable
                  ike-proposal : 3des-sha1-modp1536
                   negotiation : aggressive
               authentication  : preshared
                      psk key  : 123456
```

```
ipsec-proposal : ESP-des-sha1
 local id type : name
 local id Name : server
remote id Name : client
```

5.3.9 SNMP 参数配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
关闭 SNMP 全局配置	**no snmp-server**	
开启 SNMP 全局配置	**snmp-server start**	
设备位置信息	**snmp-server location** *location*	
配置团体名	**snmp-server community** *community*	默认为 public
TRAP 目标主机配置	**snmp-server host** *ip-addr* **traps version** *1|2*	
关闭 TRAP	**no snmp-server traps**	
开启私有 TRAP 配置以及 TRAP 间隔	**snmp-server privatetrap interval** *second*	
关闭私有 TRAP	**no snmp-server privatetrap**	
查看 SNMP 配置和状态	**show snmp-server**	

5.3.10 NTP 配置

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
启用 NTP 功能，包括客户端和服务器	**ntp enable**	
禁用 NTP 功能，包括客户端和服务器	**no ntp**	
配置 NTP 服务器地址	**ntp server1** *WORD* [**server2** *WORD*]	
查看 NTP 配置	**show ntp**	

5.3.11 系统信息

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
查看设备信息	**show device info**	

例：

```
RG2000(config)# show device info
************************************************
                Device Name : RG2000
           Software Version : 1.0.0
              Software Date : Apr 11 2017 18:33:56
```

```
                    Cpu Used : 0%
                      Memory : 29%(total:47484 kB,used:13804 kB)
                 System Time : 2017-04-12 08:30:50
                    Run Time : 0 Day 12:07:24
************************************************
                 Wan 0 Ifname : vlan0010
                   Wan 0 MAC : 00:0b:d4:0a:0b:0c
                Wan 0 ip mode : Static ip
              Wan 0 active ip : 172.16.0.1
          Wan 0 active netmask : 255.255.0.0
        Wan 0 default gateway : 172.16.0.20
                        Dns1 : 192.168.1.1
                        Dns2 : 192.168.10.1
```

5.3.12 日志信息

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
查看 log 配置信息	**show logging**	
开启 log 功能	**log on**	
关闭 log 功能	**no log on**	
设置 telnet 日志信息等级	**log monitor** (*emergencies|alerts|critical|errors|warnings|notifications|informational|debugging*)	
关闭 telnet 日志信息等级	**no log monitor**	
开启 telnet 日志信息查看	**terminal monitor**	此两条命令在特权模式 RG2000#下进行设置，且只有第一个登录到设备的 telnet 界面可查看日志信息。
关闭 telnet 日志信息查看	**no terminal monitor**	
设置本地日志信息等级	**log file** (*emergencies|alerts|critical|errors|warnings|notifications|informational|debugging*)	
关闭本地日志信息	**no log file**	
设置 syslog 日志等级	**log syslog** (*emergencies|alerts|critical|errors|warnings|notifications|informational|debugging*)	
开启 syslog 服务器	**log server** *A.B.C.D* <*1-65535*>	默认端口为 514。

步骤	命令	说明
关闭 syslog 服务器	**no log server**	
导出本地日志信息	**tftp export log** *A.B.C.D*	

5.3.13 软件升级

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
从 TFTP 服务器 A.B.C.D 上下载固件进行升级	**tftp import sys** *A.B.C.D filename*	filename 为升级固件名称，需带后缀名。

5.3.14 设备参数

1. 导入配置文件

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
从 TFTP 服务器 A.B.C.D 上下载参数	**tftp import cfg** *A.B.C.D filename*	filename 为参数文件名称，需带后缀名。

2. 导出配置文件

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
导出参数到 TFTP 服务器 A.B.C.D	**tftp export cfg** *A.B.C.D filename*	

3. 恢复默认参数

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
恢复默认参数	**restore system-configure**	

4. 保存参数

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
保存参数	**write**	

5.3.15 重启设备

步骤	命令	说明
进入全局配置模式	**configure terminal**	-
重启设备	**reload**	