H3C UG 系列路由器

用户手册

新华三技术有限公司
http://www.h3c.com

软件版本：R0130
资料版本：6W102-20221221

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

《H3C UG 系列路由器 用户手册》将会详细地介绍设备的外观、指示灯以及安装过程，另外也会指导您如何通过 Web 设置页面对设备进行本地管理。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 产品简介

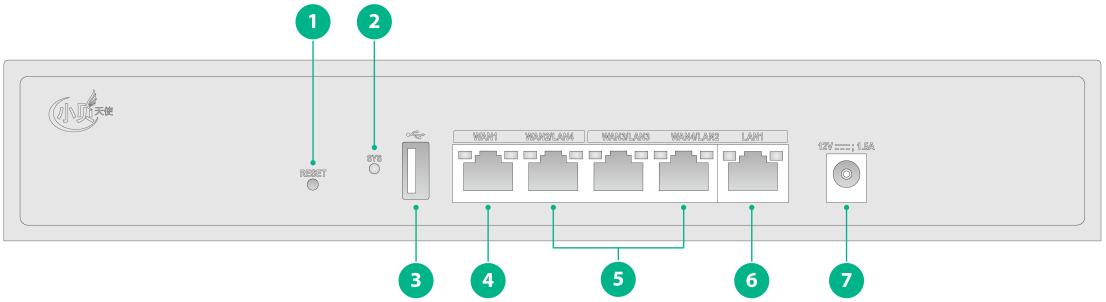
H3C UG 系列路由器包括如下产品型号。

名称	具体型号
H3C UG系列路由器	UG8103、UG8206、UG-1800W

1.1 设备外观

1.1.1 UG8103

图1-1 UG8103 设备前面板



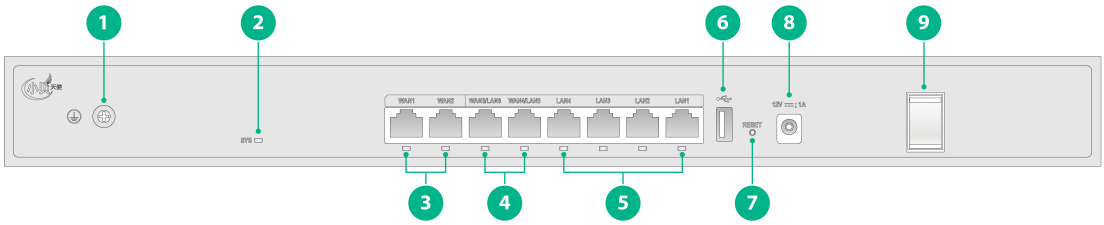
(1): 复位键（RESET）	(2): 系统指示灯（SYS）
(3): USB接口	(4): WAN接口及指示灯（10/100/1000Base-T电口）
(5): WAN/LAN接口及指示灯（10/100/1000Base-T电口）	(6): LAN接口及指示灯（10/100/1000Base-T电口）
(7): 电源接口	

图1-2 UG8103 设备后面板

(1): 接地螺钉

1.1.2 UG8206

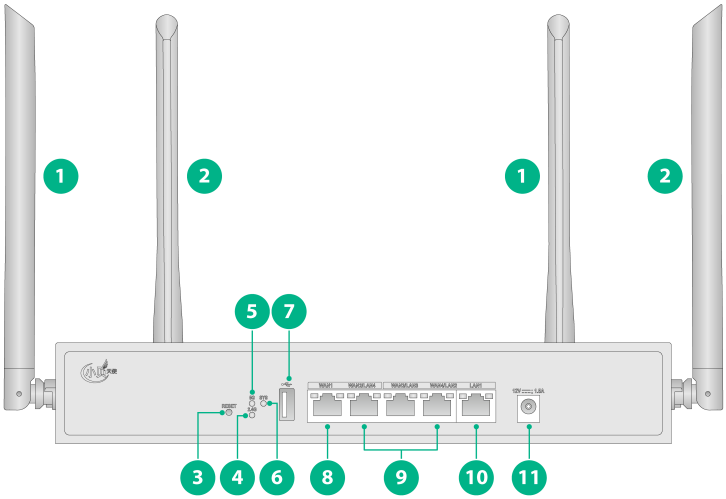
图1-3 UG8206 设备前面板



(1): 接地螺钉	(2): 系统指示灯（SYS）
(3): WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10/100/1000Base-T电口）
(5): LAN接口及指示灯（10/100/1000Base-T电口）	(6): USB接口
(7): 复位键（RESET）	(8): 电源接口
(9): 电源线固定卡扣	

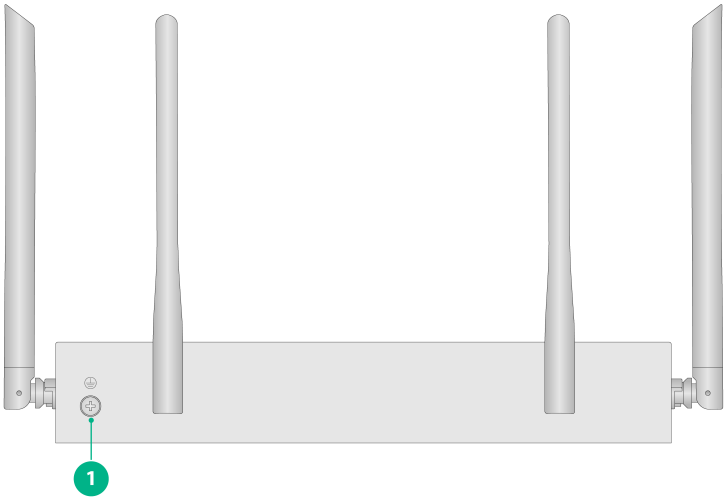
1.1.3 UG-1800W

图1-4 UG-1800W 设备前面板



(1): 2.4G天线	(2): 5G天线
(3): 复位键（RESET）	(4): 2.4G射频状态指示灯
(5): 5G射频状态指示灯	(6): 系统指示灯（SYS）
(7): USB接口	(8): WAN接口及指示灯（10/100/1000Base-T电口）
(9): WAN/LAN接口及指示灯（10/100/1000Base-T电口）	(10): LAN接口及指示灯（10/100/1000Base-T电口）
(11): 电源接口	

图1-5 UG-1800W 设备后面板



(1): 接地螺钉

1.2 指示灯说明

指示灯	状态	含义
系统指示灯（SYS）	绿色常亮	设备正常运行中
	黄色常亮	系统告警或故障
	黄色慢速闪烁	设备将恢复缺省Web登录密码
	黄色快速闪烁	设备将恢复出厂设置并重启
	灯灭	电源关闭、电源故障或设备硬件故障
WAN/LAN接口状态指示灯（LINK/ACT）（适用于UG8206）	绿色常亮	端口正常连接设备，且工作在1000Mbps速率下
	绿色闪烁	端口在接收或发送数据，且工作在1000Mbps速率下
	黄色常亮	端口正常连接设备，且工作在10/100Mbps速率下
	黄色闪烁	端口在接收或发送数据，且工作在10/100Mbps速率下
	灯灭	端口未连接设备
WAN/LAN接口状态指示灯（LINK/ACT）（适用于UG8103、UG-1800W）	绿色常亮、黄色常亮	端口正常连接设备，且工作在1000Mbps速率下
	绿色常亮、黄色闪烁	端口在接收或发送数据，且工作在1000Mbps速率下
	绿色灭、黄色常亮	端口正常连接设备，且工作在10/100Mbps速率下
	绿色灭、黄色闪烁	端口在接收或发送数据，且工作在10/100Mbps速率下
	灯灭	端口未连接设备
2.4G射频状态指示灯	绿色常亮	2.4G射频处于待机状态，但是没有连接客户端
	绿色闪烁	2.4G射频接口有客户端在线，且有数据收发

指示灯	状态	含义
	灯灭	2.4G射频关闭
5G射频状态指示灯	绿色常亮	5G射频处于待机状态，但是没有连接客户端
	绿色闪烁	5G射频接口有客户端在线，且有数据收发
	灯灭	5G射频关闭

1.3 接口说明

接口	用途
复位键（RESET）	• 短按（小于 5 秒），设备将重启 • 按住 5～10 秒，当 SYS 指示灯黄色慢速闪烁时，松开复位键，设备将恢复缺省 Web 登录密码 • 按住 10～15 秒，当 SYS 指示灯黄色快速闪烁时，松开复位键，设备将恢复出厂设置并重启 • 按住超过 15 秒，SYS 指示灯会恢复到绿色常亮，设备不执行任何恢复操作
USB接口	连接到存储介质（如U盘、移动硬盘等），可以快速备份或恢复设备配置，以及恢复软件版本
电源接口	连接到电源
LAN接口	连接计算机或下层交换机的以太网端口
WAN接口	连接到宽带运营商提供的网络接口，接入互联网
接地螺钉	用于连接接地线
WLAN接口（天线）	用于连接无线客户端

1.4 注意事项

为保证设备正常工作和延长使用寿命，请遵从以下注意事项：

- 设备仅允许在室内使用，请将其放置于干燥通风处；
- 设备的接口线缆要求在室内走线，禁止户外走线，以防止因雷电产生的过电压、过电流损坏设备的信号口；
- 请不要将设备放在不稳定的箱子或桌子上，一旦跌落，会对设备造成损害；
- 在设备周围应预留足够的空间（大于 10cm），以便于设备正常散热；
- 请保证设备工作环境的清洁，过多的灰尘会造成静电吸附，不但会影响设备寿命，而且容易造成通信故障；
- 设备工作地的接地装置最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；
- 设备工作地应远离强功率无线电发射台、雷达发射台、高频大电流设备；

- 请使用随产品附带的电源线，严禁使用其它非配套产品。电源电压必须满足专用电源线的输入电压范围。

1.5 安装设备

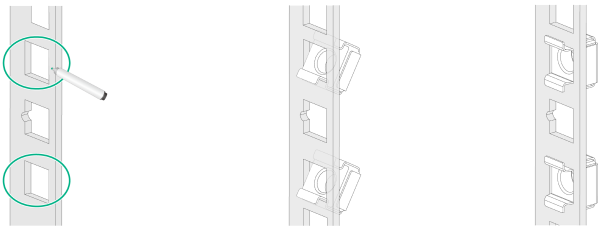
设备支持机柜安装和工作台安装两种方式，本文的安装过程以 UG8206 设备举例。

1.5.1 安装到机柜

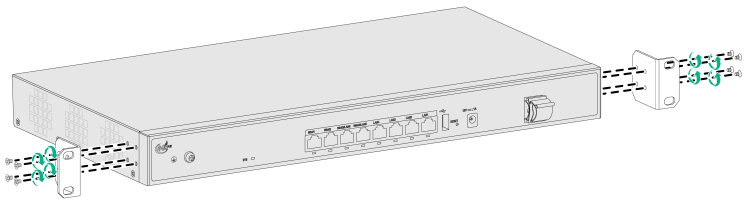
说明

仅 UG-1800W 不支持安装到机柜。

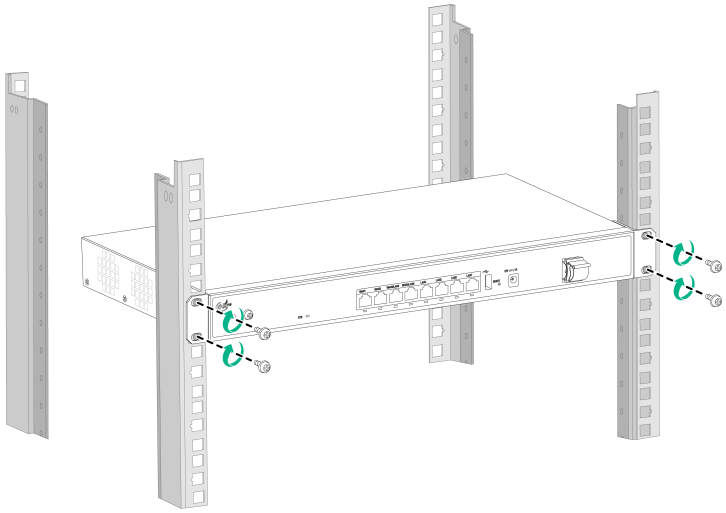
1. 安装浮动螺母



2. 安装挂耳



3. 安装设备到机柜

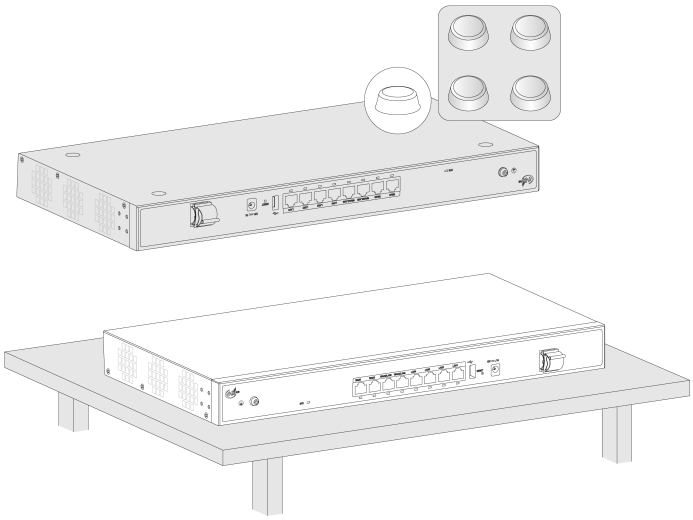


1.5.2 安装到工作台

注意

请保证工作台的平稳和良好接地，并且不要在设备上放置重物。

粘贴脚垫到设备底部，将设备翻转后水平放置于工作台上。



1.6 连接线缆

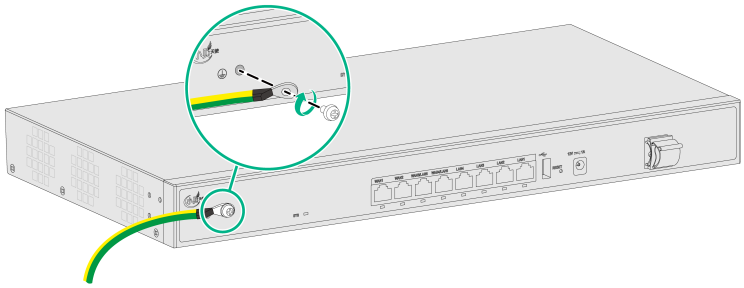
1.6.1 连接接地线

说明

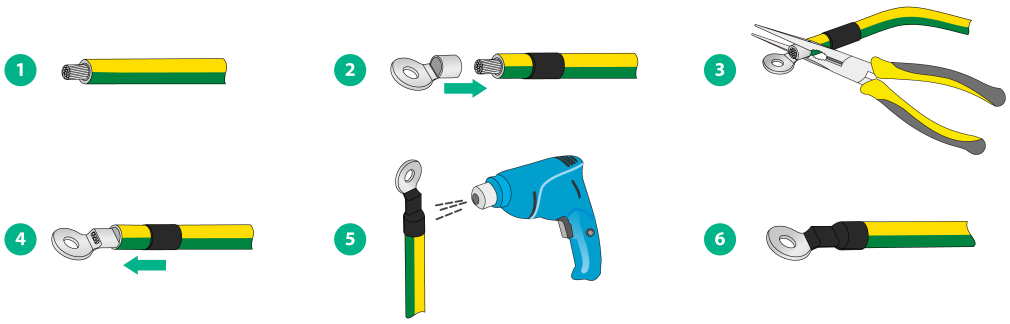
仅 UG-1800W 随机不附带接地线，只提供一个 OT 端子，接地线需要用户自行购买安装。

不同设备安装接地线方法基本相同，具体方法如下。需要注意的是，由于 UG-1800W 随机不附带接地线，需要先组装好 OT 端子，再将装配好 OT 端子的接地线安装到设备上。

(1) 将设备的接地线的一端安装到设备接地孔上。



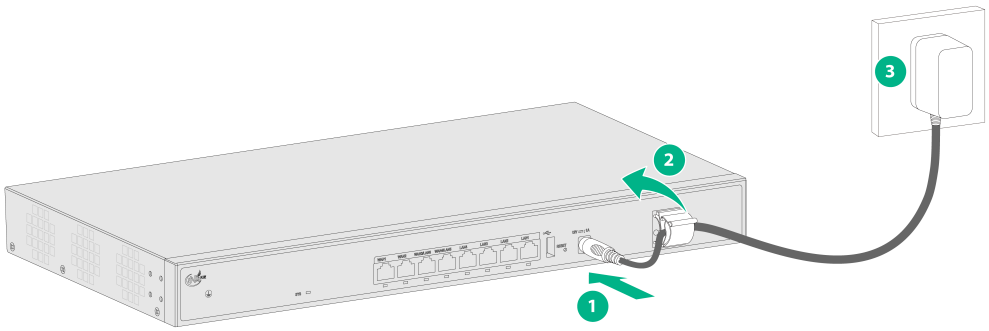
(2) 接地线的另一端可以直接缠绕在接地排上，或者与 OT 端子进行组装后再安装到接地排上，OT 端子的组装方法如下。



1.6.2 连接电源线

(1) 先将电源线一端插入到设备的电源接口，并用卡扣固定住电源线。部分设备面板上无卡扣，无需进行固定。

(2) 再将另一端连接到外部的交流电源插座上。



1.7 技术规格

项目	UG8103	UG8206	UG-1800W
外形尺寸（宽×深×高）	266mm×161mm×44mm	440mm×227mm×44mm	266mm×161mm×44mm
功耗	＜18W	＜11W	＜18W
额定输入电压	100V AC～240V AC，50/60Hz		
设备电源输入	12V/1.5A	12V/1A	12V/1.5A
重量	0.8Kg	1.7Kg	0.8Kg
USB接口	1个USB3.0接口	1个USB2.0接口	1个USB3.0接口
LAN接口	1个	4个	1个
LAN/WAN接口	3个	2个	3个
WAN接口	1个千兆电口	2个千兆电口	1个千兆电口
技术标准	-	-	• IEEE802.11ax/n/b/g • IEEE802.11ax/ac/a/n
WLAN接口	-	-	• 2 个 2.4G 天线接口 • 2 个 5G 天线接口
无线速率	-	-	1800Mbps
工作温度	0ºC～45ºC		
工作湿度	5%RH～95%RH，非凝露		
散热方式	自然散热		

2 登录设备

说明

建议使用 Internet Explorer 10 及以上版本、Chrome 57 及以上版本、Firefox 35 及以上版本的浏览器访问 Web 管理页面。

(1) 将 PC 连接到设备的 LAN 接口。

(2) 配置 PC 为自动获取 IP 地址（推荐）或手工配置 PC 的 IP 地址和 192.168.1.0/24 在同一网段。

(3) 检查 PC 的代理服务设置情况。如果当前 PC 使用代理服务器访问互联网，则首先必须禁止代理服务。

(4) 运行 Web 浏览器。请在浏览器地址栏中输入 http://192.168.1.1（设备缺省的管理 IP 地址，登录后可修改）并回车。

(5) 如下图所示，在弹出的窗口上输入管理员用户名和密码（缺省均为 admin），点击<登录>按钮。首次登录设备后，系统会自动弹出“修改密码”页面。输入缺省密码、新密码，并确认新密码，点击<确定>按钮完成密码的修改。

3 系统信息

3.1 简介

系统信息将展示设备的运行情况，基本功能的配置向导和技术支持信息。

3.2 CPU使用率和内存使用率

1. 配置需求

显示设备 CPU 使用率和内存使用率相关信息，包括：

- CPU 的当前使用率、平均使用率。
- 内存的当前使用率、平均使用率。
- 系统时间、运行时间。
- 产品型号、序列号、软件版本等信息。
- 存储介质上存储空间的使用情况。
- 端口状态：显示 WAN 口和 LAN 口的使用状态。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息显示页面。

(2) 单击页面上方的“CPU 使用率”区段或“内存使用率”区段，可查看 CPU 或内存的当前使用率、平均使用率。

3.3 接入终端

1. 配置需求

显示设备接入终端相关信息，包括：

- 实时流量排行 TOP5。
- 在线主机数和在线主机网络连接数。
- 在线主机信息表，表中包含终端 IP 地址、终端名、网络连接数、接入方式、接口、终端 MAC 地址等信息。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息显示页面。

(2) 单击页面上方的“接入终端”区段，可查看接入终端的相关信息。

3.4 上网流量

1. 配置需求

显示设备上网流量相关信息，例如：最近 5 分钟平均上行速度、最近 5 分钟平均下行速度、上网 WAN 接口的状态和上网参数等。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息显示页面。

(2) 单击页面上方的“上网流量”区段，可查看上网流量的相关信息。

3.5 系统信息

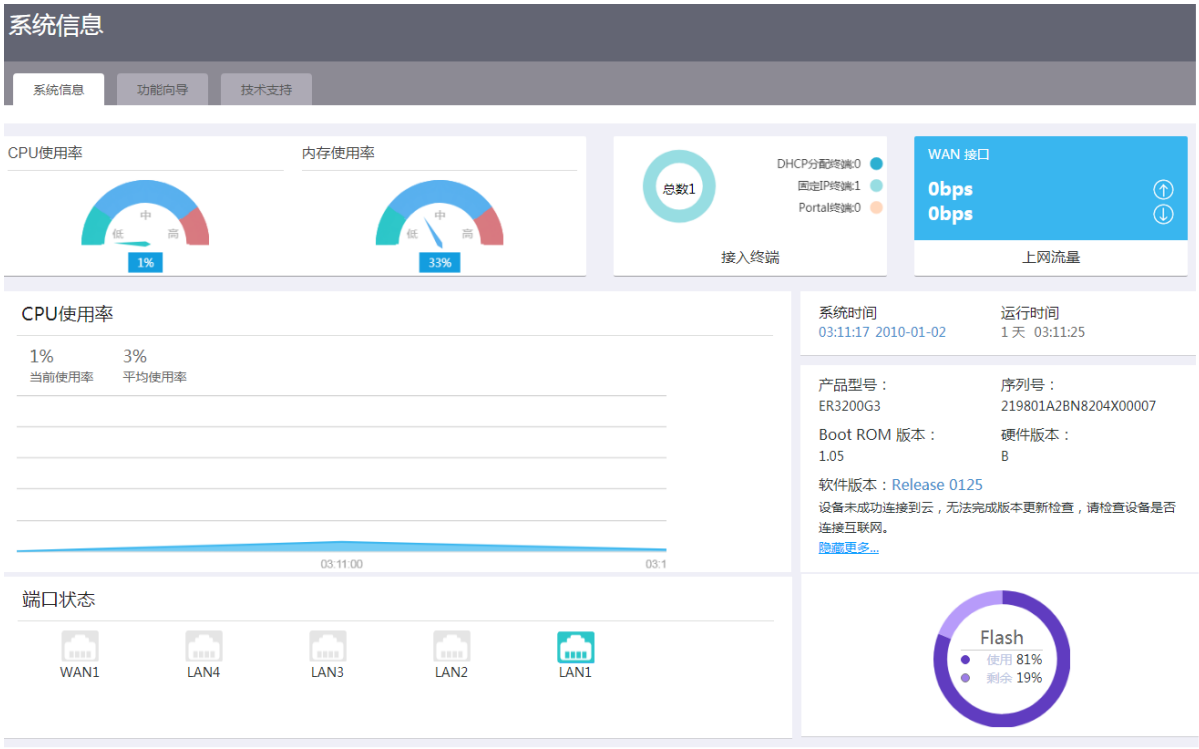
1. 配置需求

显示设备系统时间和产品型号等信息。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息页面。

(2) 在“系统时间”区段中，可查看系统时间和运行时间；在“产品型号”区段中，可查看产品型号、序列号、Boot ROM 版本、硬件版本和软件版本等信息。



3.6 端口状态

1. 配置需求

显示 WAN 口和 LAN 口的使用状态。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息显示页面。

(2) 在“端口状态”区段中，点击端口图标，可进入 WAN 或 LAN 配置页面。

3.7 Flash使用率

1. 配置需求

存储介质上存储空间的使用情况。

2. 配置步骤

(1) 单击导航树中[系统信息]菜单项，进入系统信息显示页面。

(2) 在页面右下方区段，可查看 Flash 上存储空间的使用率。

3.8 功能向导

通过功能向导帮助用户快速的配置网络。

(1) 单击导航树中[系统信息]菜单项，进入系统信息页面。

(2) 单击“功能向导”页签，进入功能向导页面。

(3) 根据需要点击功能对应的链接，配置向导如下：

- 上网配置
  - 连接到因特网：单击“连接到因特网”链接，页面自动跳转至外网配置页面。
  - 局域网(LAN)配置：单击“局域网(LAN)配置”链接，页面自动跳转至 LAN 配置页面。
  - NAT 配置：单击“NAT 配置”链接，页面自动跳转至 NAT 配置页面。
- 上网行为
  - 应用控制：单击“应用控制”链接，页面自动跳转至上网行为管理的应用控制页面。
  - 网址控制：单击“网址控制”链接，页面自动跳转至上网行为管理的网址控制页面。
  - 文件控制：单击“文件控制”链接，页面自动跳转至上网行为管理的文件控制页面。
  - 带宽限速：单击“带宽限速”链接，页面自动跳转至带宽管理的 IP 限速页面。
  - 连接限制：单击“连接限制”链接，页面自动跳转至连接限制的网络连接限制数页面。
  - 流量统计排名：单击“流量统计排名”链接，页面自动跳转至流量排行页面。
- 接入安全
  - ARP 安全：单击“ARP 安全”链接，页面自动跳转至 ARP 安全页面。

- Portal 认证：单击“Portal 认证”链接，页面自动跳转至 Portal 认证页面。
- 防火墙：单击“防火墙”链接，页面自动跳转至防火墙页面。
- VPN 设置：单击“VPN 设置”链接，页面自动跳转至 IPsec VPN 页面。
- MAC 地址过滤：单击“MAC 地址过滤”链接，页面自动跳转至 MAC 地址过滤页面。

- 设备维护
  - 配置管理：单击“配置管理”链接，页面自动跳转至配置管理页面。
  - 系统升级：单击“系统升级”链接，页面自动跳转至系统升级页面。
  - 重新启动：单击“重新启动”链接，页面自动跳转至重新启动页面。
  - 远程管理：单击“远程管理”链接，页面自动跳转至远程管理页面。
  - 网络诊断：单击“网络诊断”链接，页面自动跳转至网络诊断页面。
  - 用户 FAQ：单击“用户 FAQ”链接，页面自动跳转至用户 FAQ 页面。

3.9 获取技术支持

如果用户对产品存有疑问，可以通过本页签提供的联系方式联系我们。包括：

- 技术论坛
- 客服邮箱
- 微信公众号

技术支持

系统信息 | 功能向导 | 技术支持

新华三技术有限公司一直在努力提供最方便、最优质的产品，如果您遇到任何问题或疑问，请访问H3C技术支持论坛或者微信扫描下面的二维码关注微信公众号：新华三服务获取帮助。

- 技术论坛： zhiliao.h3c.com
- 客服邮箱： service@h3c.com
- 微信公众号： 新华三服务

微信公众号

4 快速设置

4.1 简介

通过快速设置完成广域网 WAN、局域网 LAN 和无线设置的基本配置后，局域网内的用户便可以访问外网。

4.2 配置WAN

1. 配置需求

设备支持单 WAN 和双 WAN 两种广域网接入场景（部分款型只支持双 WAN 场景，快速设置页面中无单 WAN 选项）。如果用户仅租用了一个运营商网络，则选择单 WAN 场景；如果用户租用了两个运营商网络，则使用双 WAN 场景。单 WAN 和双 WAN 场景的配置方法相同。

 说明

- UG8103 和 UG-1800W 设备的快速设置功能支持单 WAN 和双 WAN 场景，UG8206 设备的快速设置功能仅支持双 WAN 场景。
- 快速设置页面仅支持设置单 WAN 或双 WAN 场景，多 WAN 模式可在[网络设置/外网配置]菜单项中的配置接口模式页面中配置。

---

2. 配置步骤

(1) 单击导航树中[快速设置]菜单项，进入快速设置页面。

(2) 根据使用场景需求，选择“单 WAN 场景”或“双 WAN 场景”，设置广域网接入参数。

(3) 在“线路 1”或“线路 2”配置项处选择要接入广域网的物理接口 WANx。

(4) 根据用户实际的上网方式，在“连接模式”配置项处选择对应的连接模式：

- 如果选择连接模式为“PPPoE”：
  - 在“上网账号”配置项处，输入运营商提供的 PPPoE 接入用户名。
  - 在“上网密码”配置项处，输入运营商提供的 PPPoE 接入密码。
  - 在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。注意设备优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。
- 如果选择连接模式为“DHCP”：

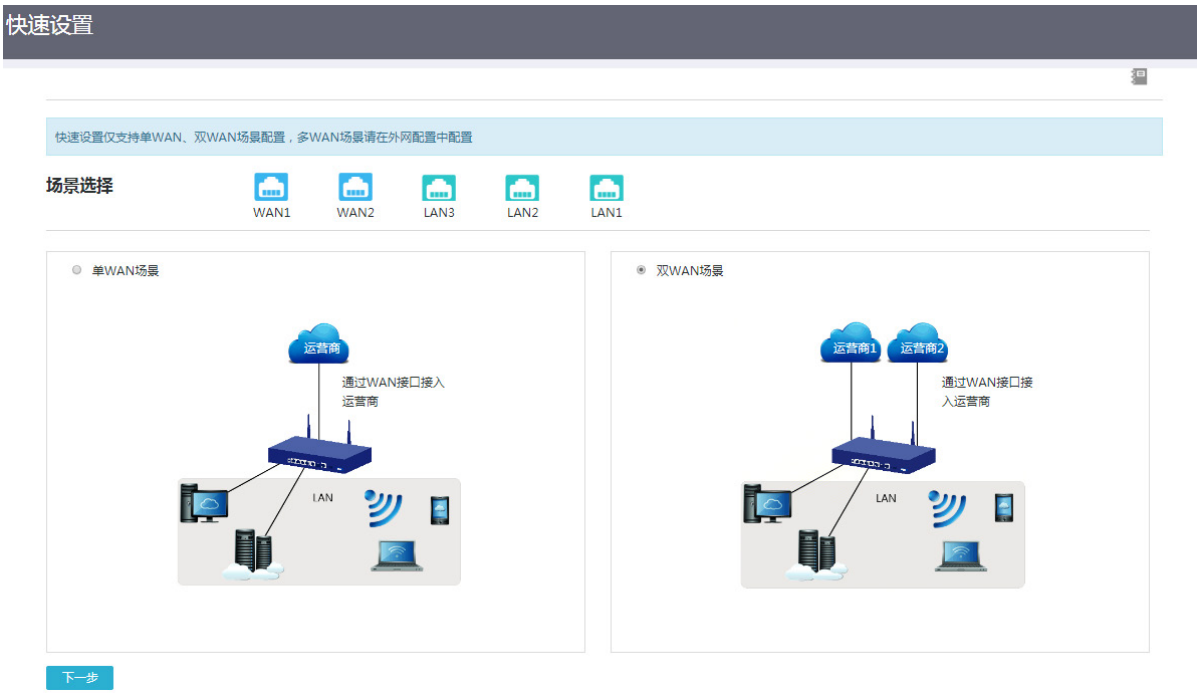
  在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。注意设备优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。
- 如果选择连接模式为“固定地址”：
  - 在“IP 地址”配置项处，输入接入广域网的固定 IP 地址，仅允许输入 A、B、C 类 IP 地址。
  - 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24,。

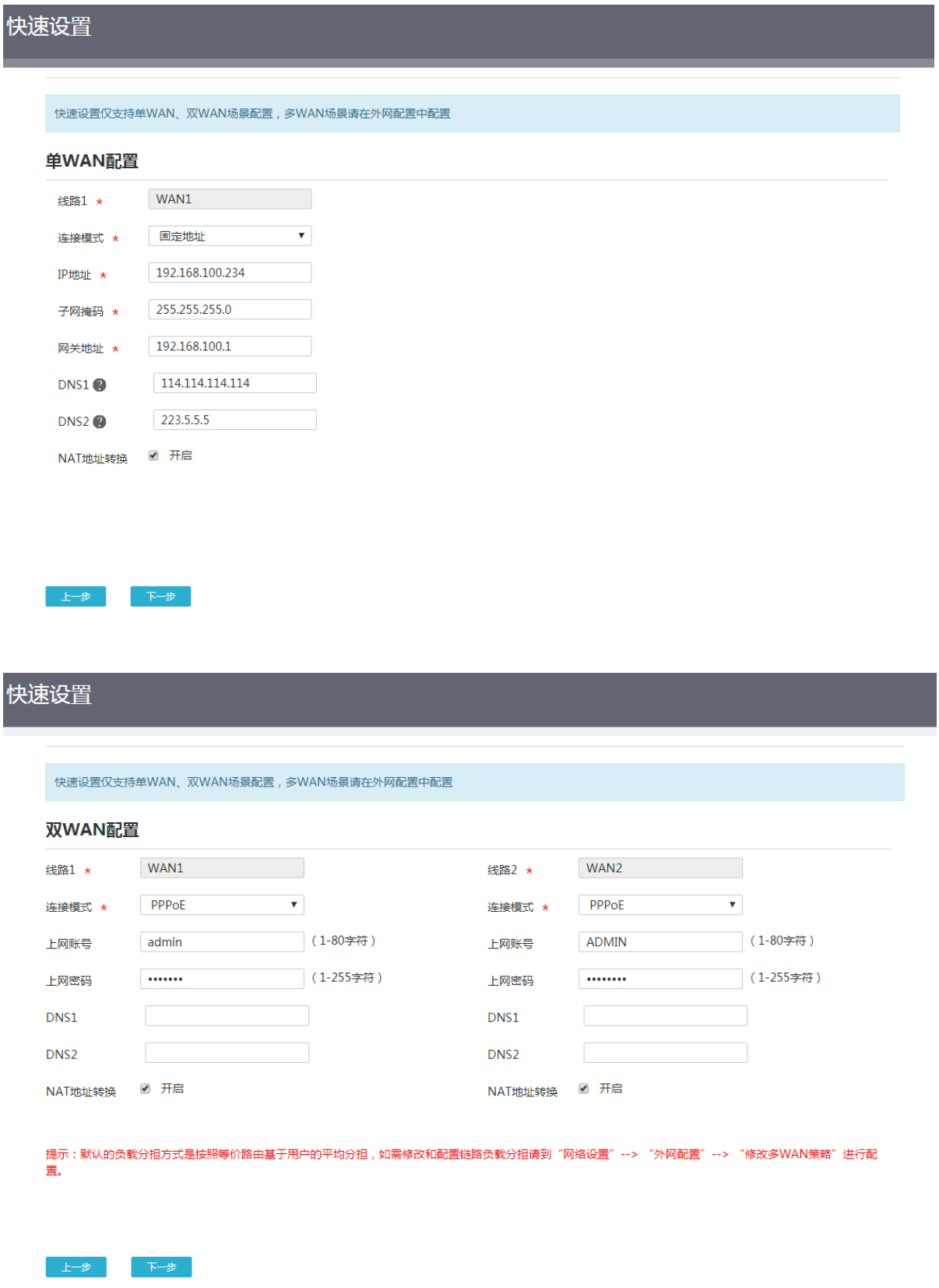
– 在“网关地址”配置项处，输入接入广域网的网关地址，仅允许输入 A、B、C 类 IP 地址。

– 在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。DNS1 缺省为 114.114.114.114，DNS2 缺省为 223.5.5.5。注意设备会优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。

(5) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时，需要启用此功能。

(6) 点击<下一步>按钮，完成 WAN 配置。




快速设置
快速设置仅支持单WAN、双WAN场景配置，多WAN场景请在外网配置中配置
单WAN配置
线路1 *
WAN1
连接模式 *
固定地址
IP地址 *
192.168.100.234
子网掩码 *
255.255.255.0
网关地址 *
192.168.100.1
DNS1
114.114.114.114
DNS2
223.5.5.5
NAT地址转换
开启
上一步
下一步

快速设置
快速设置仅支持单WAN、双WAN场景配置，多WAN场景请在外网配置中配置
双WAN配置
线路1 *
WAN1
连接模式 *
PPPoE
上网账号
admin
（1-80字符）
上网密码
（1-255字符）
DNS1
DNS2
NAT地址转换
开启
线路2 *
WAN2
连接模式 *
PPPoE
上网账号
ADMIN
（1-80字符）
上网密码
（1-255字符）
DNS1
DNS2
NAT地址转换
开启
提示：默认的负载分担方式是按照等价路由基于用户的平均分担，如需修改和配置链路负载分担请到“网络设置” --> “外网配置” --> “修改多WAN策略”进行配置。
上一步
下一步

4.3 配置LAN

完成 WAN 配置后，会进入到 LAN 配置的页面。

(1) 在“局域网 IP 地址”配置项处，输入设备在局域网中使用的 IP 地址。

(2) 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24，输入的掩码长度会被自动转换为点分十进制的掩码格式。

(3) 在“DHCP 服务”配置项处，选择是否“启用”选项。如果设备需要作为 DHCP 服务器为局域网中的主机分配 IP 地址，则需要选择“启用”。

- 如选择“启用”选项：
  - 在“IP 分配范围”配置项处，输入待分配地址的起始 IP 地址和结束 IP 地址；
  - 在“网关地址”配置项处，输入设备为 DHCP 客户端分配的网关地址；
  - 在“DNS”配置项处，输入设备为 DHCP 客户端分配的 DNS 服务器的 IP 地址。
- 如不选择“启用”，则表示不启用设备的 DHCP 功能。

(4) 设置完成后，点击<下一步>按钮，若路由器是有线款型，则进入完成配置页面，确认所有配置无误后，点击<完成>按钮，完成快速设置。若路由器是无线款型，则进入无线设置页面，需继续进行无线设置。

4.4 配置无线设置

说明

仅无线款型路由器支持此功能。

完成 LAN 配置后，会进入到无线设置的页面。

(1) 配置无线网络设置 SSID 设置-2.4G：

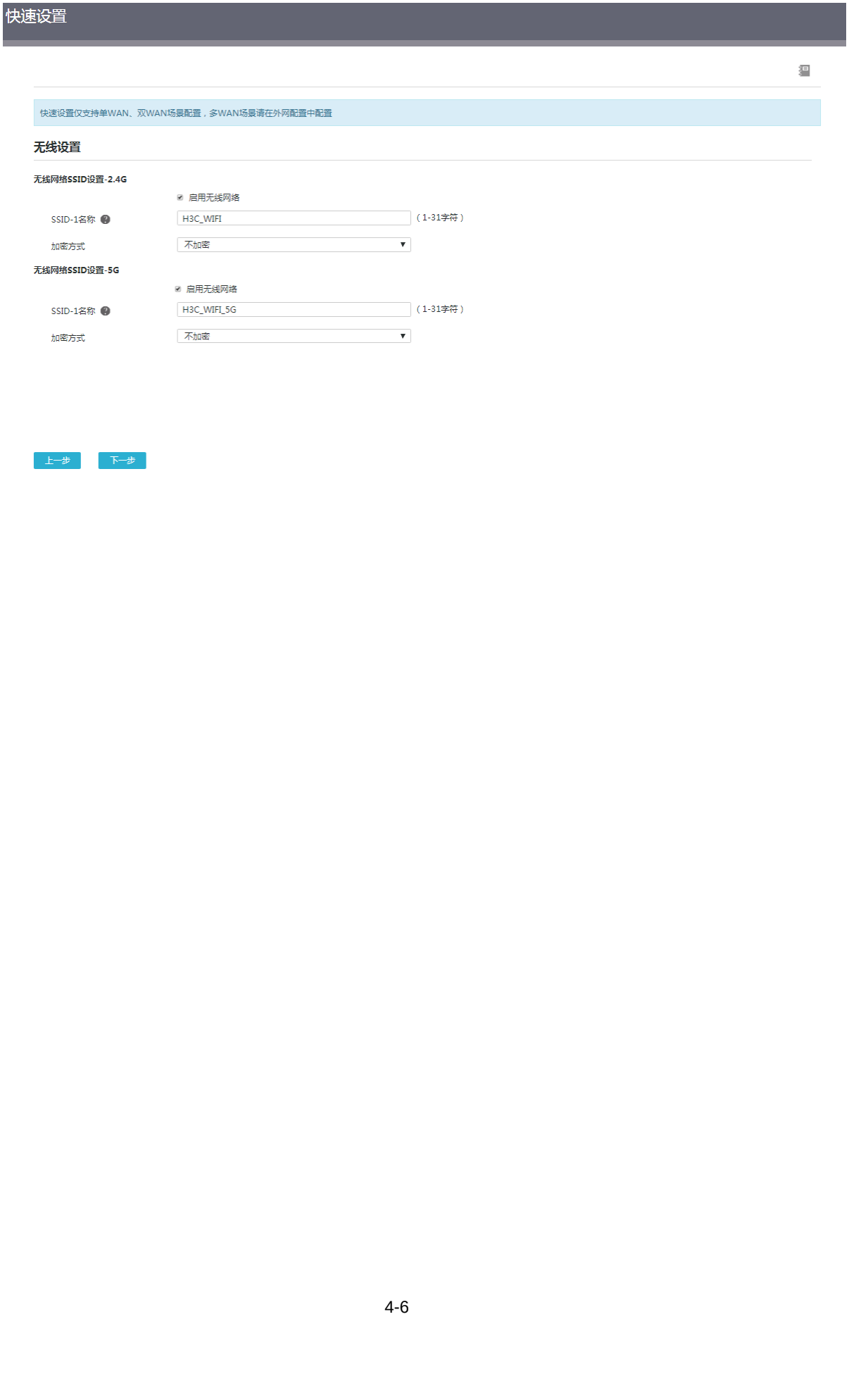
- 勾选“启用无线网络”选项，启用无线 2.4G 网络。
- 在“SSID-1 名称”配置项处，输入 2.4G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’<>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务：
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(2) 配置无线网络设置 SSID 设置-5G：

- 勾选“启用无线网络”选项，启用无线 5G 网络。
- 在“SSID-1 名称”配置项处，输入 5G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’<>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(3) 点击<下一步>按钮，会进入到完成配置的页面，显示用户在[快速设置]菜单项中的所有配置。

(4) 点击<完成>按钮，完成快速设置。


快速设置
快速设置仅支持单WAN、双WAN场景配置，多WAN场景请在外网配置中配置
无线设置
无线网络SSID设置-2.4G
启用无线网络
SSID-1名称
H3C_WIFI
（1-31字符）
加密方式
不加密
无线网络SSID设置-5G
启用无线网络
SSID-1名称
H3C_WIFI_5G
（1-31字符）
加密方式
不加密
上一步
下一步

5 系统监控

5.1 线路监控

5.1.1 简介

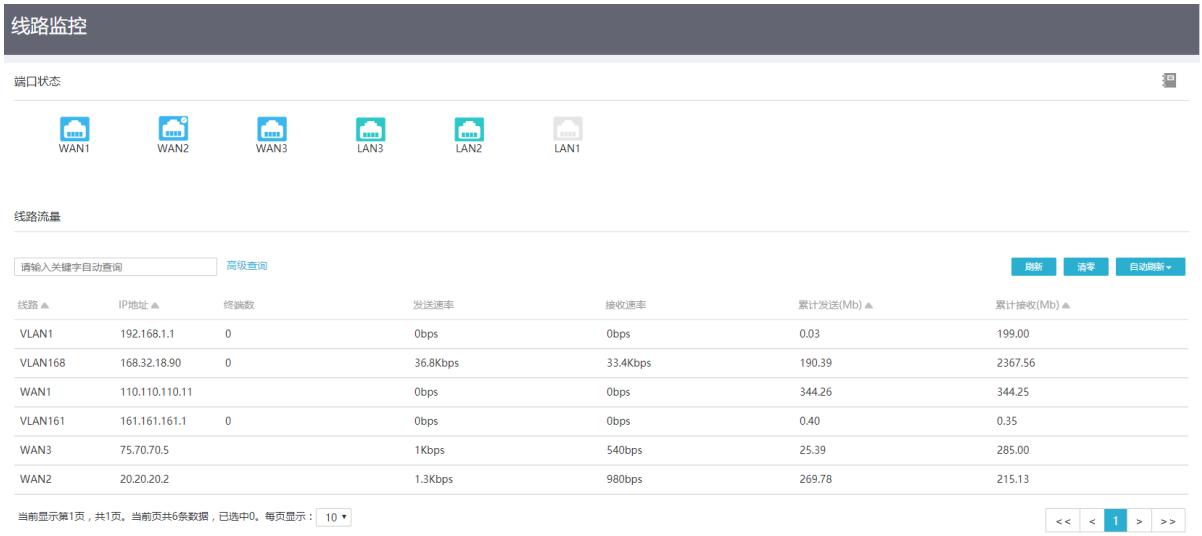
线路监控功能用来查看设备端口状态和各线路的流量情况，方便管理员对设备线路流量进行分析与审计。

5.1.2 配置步骤

(1) 单击导航树中[系统监控/线路监控]菜单项，进入线路监控页面。

(2) 在“端口状态”区段下，点击端口图标，可进入 WAN 或 LAN 配置页面。

(3) 在“线路流量”区段下，可以通过列表查看各线路的流量信息。



5.2 流量排行

5.2.1 简介

流量排行功能用来展示终端流量使用情况，可查看终端 IP 地址、当日总流量和在线时长等信息，方便管理员对用户的上网行为进行分析与审计。

5.2.2 注意事项

- 流量排行列表仅显示当前正在访问因特网的在线 IP 流量信息。
- 流量排行列表仅显示最近 5 分钟内连接过设备的终端的流量统计信息。
- 网络连接数统计是指内网 IP 向因特网发起的连接，对如下连接不予统计：向设备本身和内网其它 IP 发起的连接，以及由因特网向内网 IP 发起的连接。

- 流量排行列表中网络连接数包括 TCP 连接数、UDP 连接数和其他连接数（除了 TCP 和 UDP 之外的连接，如 ICMP）。
- 总流量是指当前 IP 持续通过的总体流量，如果 IP 持续一段时间没有访问因特网的业务进行，将进行重新统计。
- 流量统计的单位换算关系为 1G bit= 1,000M bit= 1,000,000K bit= 1,000,000,000 bit。

5.2.3 配置步骤

(1) 单击导航树中[系统监控/流量排行]菜单项，进入流量排行页面。

(2) 勾选“开启流量排行”选项，开启用户流量排行功能。

(3) 配置终端限速。

a. 在流量排行列表中，点击指定终端 IP 地址对应的操作列限速图标，弹出终端限速配置对话框。

b. 在“上传带宽”配置项处，设置终端的上传带宽。

c. 在“下载带宽”配置项处，设置终端的下载带宽。

d. 在“取消限速”配置项处，勾选此项，将取消对指定终端的限速。

e. 点击<确定>按钮，完成配置。

(4) 配置终端拉黑。

a. 在流量排行列表中，点击指定终端 IP 地址对应的操作列拉黑图标，弹出拉黑配置对话框。

b. 在“拉黑时间”配置项处，设置终端的拉黑时间。

c. 在“永久拉黑”配置项处，勾选此项，将指定终端永久拉黑。

d. 点击<确定>按钮，完成配置。

6 小贝 AP 管理

说明

若设备纳入快网络管理，小贝 AP 管理功能将无法使用。

6.1 配置任务导引

6.1.1 配置自定义的无线服务

当网络管理员需要自定义无线服务时，可根据如下步骤配置。

步骤	配置内容	详情
1	添加VLAN（可选）	添加无线业务VLAN（即桥接VLAN），具体配置方法请见参见配置VLAN。
2	启用AP管理功能（必选）	启用AP管理功能，使得AP上线，具体配置方法请见参见AP管理设置。
3	修改无线服务模板（必选）	根据需要修改无线服务模板，具体配置方法请参见WI-FI配置。

6.2 AP管理设置

6.2.1 简介

您可通过开启 AP 管理功能，集中管理接入的 AP 设备。

6.2.2 配置步骤

(1) 单击导航树中[小贝 AP 管理/AP 管理设置]菜单项，进入 AP 管理设置页面。

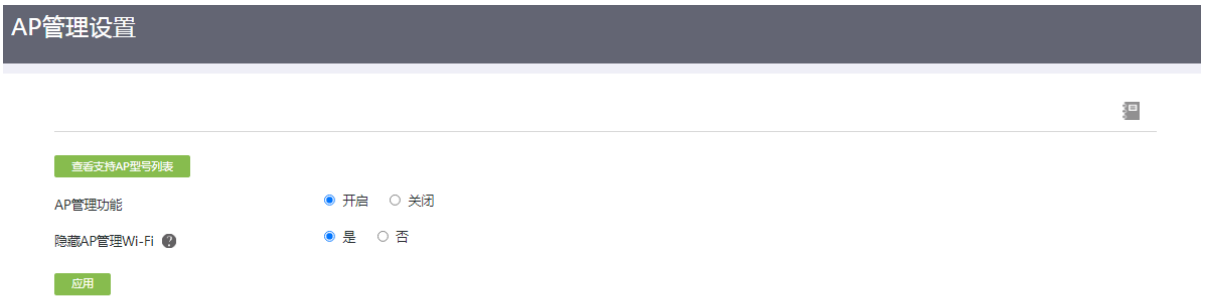
(2) 点击“查看支持 AP 型号列表”按钮，可查看设备支持的 AP 型号列表。

(3) 在“AP 管理功能”配置项处，选择“开启”选项。开启 AP 管理功能。

(4) 在“隐藏 AP 管理 Wi-Fi”配置项处，选择是否隐藏 AP 管理 Wi-Fi。

- 若选择“是”选项，客户端将无法搜索到用于管理 AP 的无线服务，如需对 AP 进行管理，用户需要向管理员获取管理 AP 的无线服务 SSID，通过手工输入 SSID 的方式接入网络。
- 若选择“否”选项，则客户端可以搜索到所有接入 AP 的 AP 管理无线服务。

(5) 点击<应用>按钮，完成配置。



6.3 WI-FI配置

6.3.1 简介

本功能用于显示设备的 Wi-Fi 配置，需要与 AP 绑定后，AP 才能提供对应的无线服务

6.3.2 配置步骤

(1) 单击导航树中[小贝 AP 管理/Wi-Fi 配置]菜单项，进入 Wi-Fi 配置页面。

(2) 在列表中点击 SSID 对应的<绑定>按钮，弹出 AP 绑定对话框。

(3) 在 AP 列表中选中待绑定的 AP。

(4) 点击<确定>按钮，完成该 SSID 和选中 AP 的绑定。

(5) 在 SSID 列表中，点击指定 SSID 对应的操作列编辑图标，弹出修改 Wi-Fi 配置对话框。

(6) 在“SSID”配置项处，可修改下发给 AP 的 SSID 名称。

(7) 在“工作状态”配置项处，选择是否开启该无线服务。

(8) 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务：

- 不加密：不对无线信号加密。
- 加密：对无线信号加密。

(9) 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择对无线信号进行加密时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(10) 在“VLAN”配置项处，输入 AP 的管理 VLAN，缺省为 1。

(11) 点击<确定>按钮，完成配置。

6.4 AP列表

6.4.1 简介

您可通过在线 AP 管理功能查看已上线的 AP 设备和客户端。本功能显示 AP 设备的详细信息。

6.4.2 配置步骤

(1) 单击导航树中[小贝 AP 管理/AP 列表]菜单项，进入 AP 列表配置页面。

(2) 在列表中点击 AP 对应的操作列“编辑”图标，弹出修改 AP 信息对话框。可修改 AP 的如下信息：

- 在“AP 名称”配置项处，修改 AP 的名称。
- 在“VLAN”配置项处，修改 AP 的业务 VLAN。
- 在“状态”配置项处，选择是否开启 AP 的无线服务。
- 在“信道”配置项处，修改无线网络的工作信道。
- 在“功率”配置项处，修改天线在无线介质中所辐射的功率。
- 在“频宽（MHz）”配置项处，修改无线网络频段带宽。
- 点击<确定>按钮，完成 AP 信息的修改。

(3) 在列表中选择需要删除的 AP，点击<删除>按钮，可删除选中的 AP。

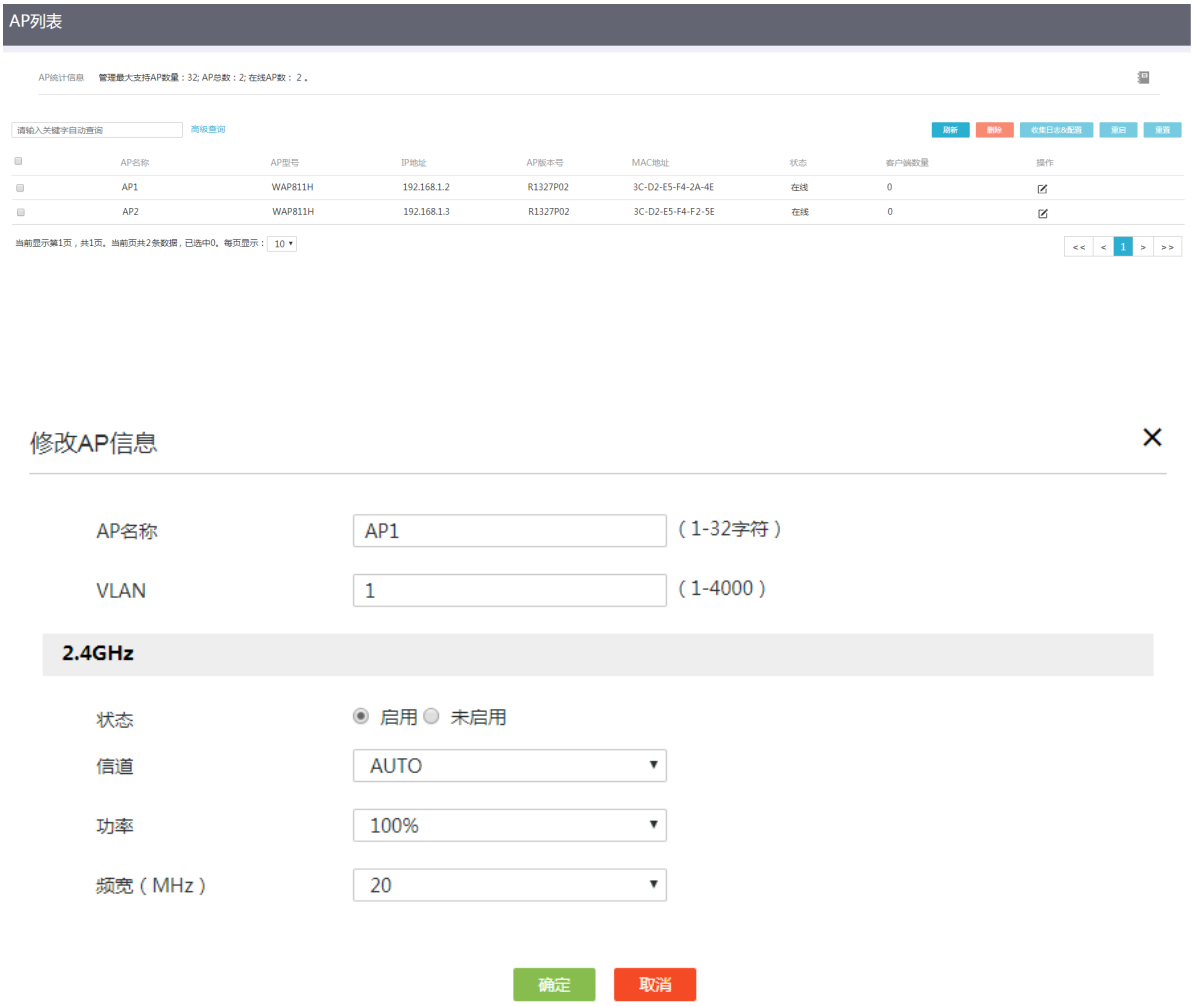
(4) 在列表中选择在线状态的 AP，点击<收集日志&配置>按钮，可对选中 AP 的日志和配置进行收集。

(5) 在列表中选择在线状态的 AP，点击<重启>按钮，可对选中的 AP 进行重启。

(6) 在列表中选择在线状态的 AP，点击<重置>按钮，观察列表中 AP 的状态。当 AP 状态为离线时，选中离线的 AP，点击<删除>按钮删除 AP 的记录，完成对 AP 恢复出厂设置的操作。待 AP 重启后，AP 将使用缺省的无线服务模板上线。

如果仅点击<重置>按钮，不删除 AP 记录，则无法对 AP 恢复出厂设置。

(7) 在“每页显示”配置项处，设置当前显示页面的 AP 数据条数。



6.5 AP版本管理

6.5.1 简介

AP 版本管理功能可以帮助您升级 AP 的软件版本。

6.5.2 注意事项

使用 AP 版本升级功能之前，请先将 AP 升级需要使用的软件版本上传到设备中。

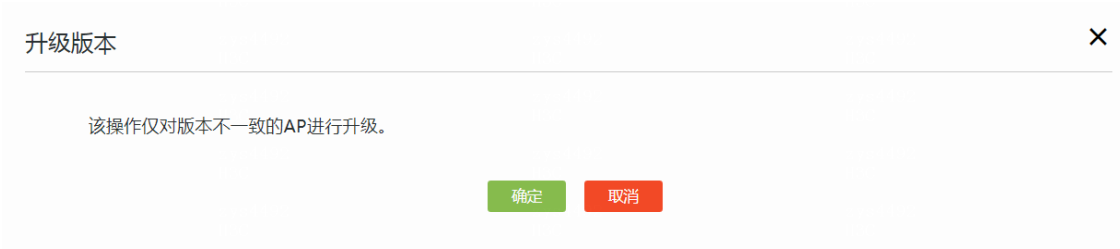
6.5.3 配置步骤

(1) 单击导航树中[小贝 AP 管理/AP 版本管理]菜单项，进入 AP 版本管理配置页面。

(2) 点击<版本上传>按钮，弹出版本上传对话框。

- 点击<选择文件>按钮，访问待上传的 AP 软件版本存放路径，并选择版本文件。
- 在“版本号”配置项处，显示在上传版本文件时设备自动校验版本文件生成的版本号，无需手工输入。
- 在“版本描述”配置项处，输入版本的描述信息。
- 在“设备型号”配置项处，选中对应 AP 的型号。
- 点击<确定>按钮，完成配置。

(3) 勾选 AP 型号前的复选框，点击<版本升级>按钮，设备下发软件版本并升级该 AP 设备。



7 无线设置

说明

仅 UG-1800W 设备支持无线设置功能。

7.1 配置任务导引

7.1.1 配置自定义的无线服务

当网络管理员需要自定义无线服务时，可根据如下步骤配置。

步骤	配置内容	详情
1	添加VLAN（可选）	根据需要添加无线业务VLAN（即桥接VLAN），具体配置方法请见参见配置VLAN。
2	配置内部网络和访客网络（可选）	根据需要配置内部网络和访客网络，具体配置方法请见参见基本设置。
3	配置无线名称和密码（必选）	根据需要配置2.4G或5G网络的无线名称和密码，具体配置方法请见参见无线射频管理。

7.2 基本设置

7.2.1 内部网络

1. 配置简介

您可以在基本设置的“内部网络”页签和“访客网络”页签中分别对 SSID 名称、加密方式和共享密钥三项参数进行配置。

2. 注意事项

配置无线服务模板时，需要同时配置 2.4G 与 5G 无线网络的相关参数信息。

3. 配置步骤

(1) 单击导航树中[无线设置/基本设置]菜单项，进入基本设置页面。

(2) 单击“内部网络”页签，进入内部网络的基本设置页面。

(3) 配置无线网络设置 SSID 设置-2.4G：

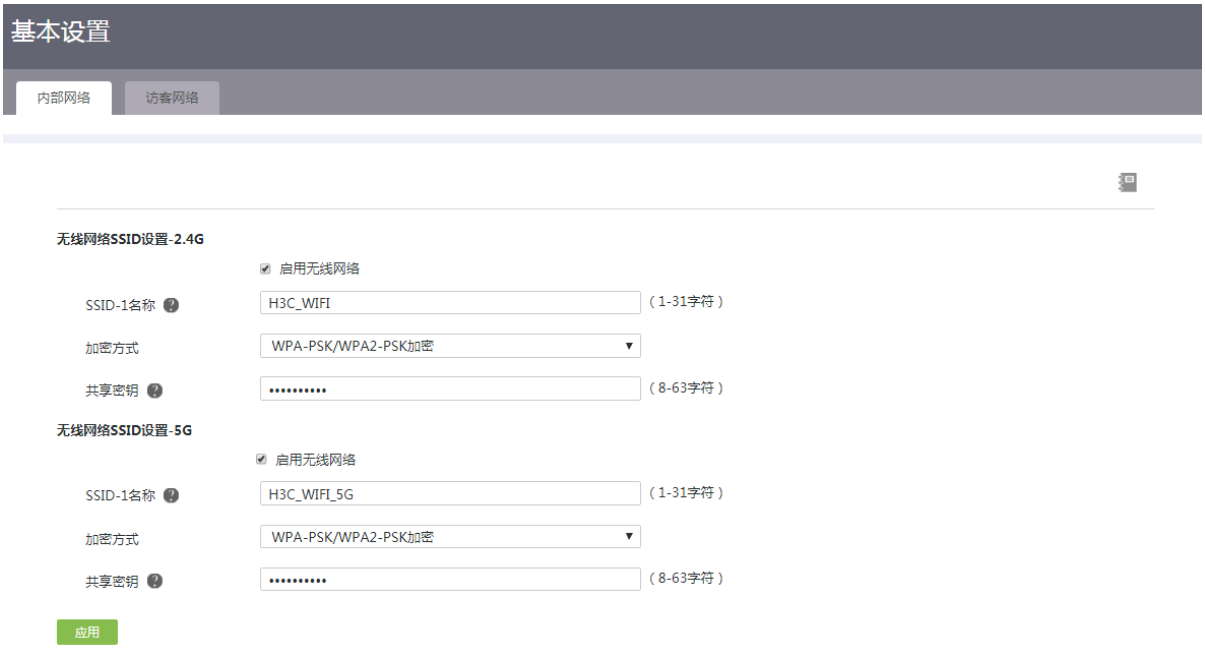
- 勾选“启用无线网络”选项，启用无线 2.4G 网络。
- 在“SSID-1 名称”配置项处，输入 2.4G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’ <>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。

- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务：
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(4) 配置无线网络设置 SSID 设置-5G：

- 勾选“启用无线网络”选项，启用无线 5G 网络。
- 在“SSID-1 名称”配置项处，输入 5G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’ <>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(5) 点击<应用>按钮，完成配置。



7.2.2 访客网络

1. 配置简介

访客网络的无线基本配置支持对 2.4G 网络和 5G 网络的 SSID 名称、加密方式和共享密钥三项参数进行配置。

2. 注意事项

配置无线服务模板时，需要同时配置 2.4G 与 5G 无线网络的相关参数信息。

3. 配置步骤

(1) 单击导航树中[无线设置/基本设置]菜单项，进入基本设置页面。

(2) 单击“访客网络”页签，进入访客网络的基本设置页面。

(3) 配置访客网络设置 SSID 设置-2.4G：

- 勾选“启用 SSID”选项，启用无线 2.4G 网络。
- 在“SSID-1 名称”配置项处，输入 2.4G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’ <>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。

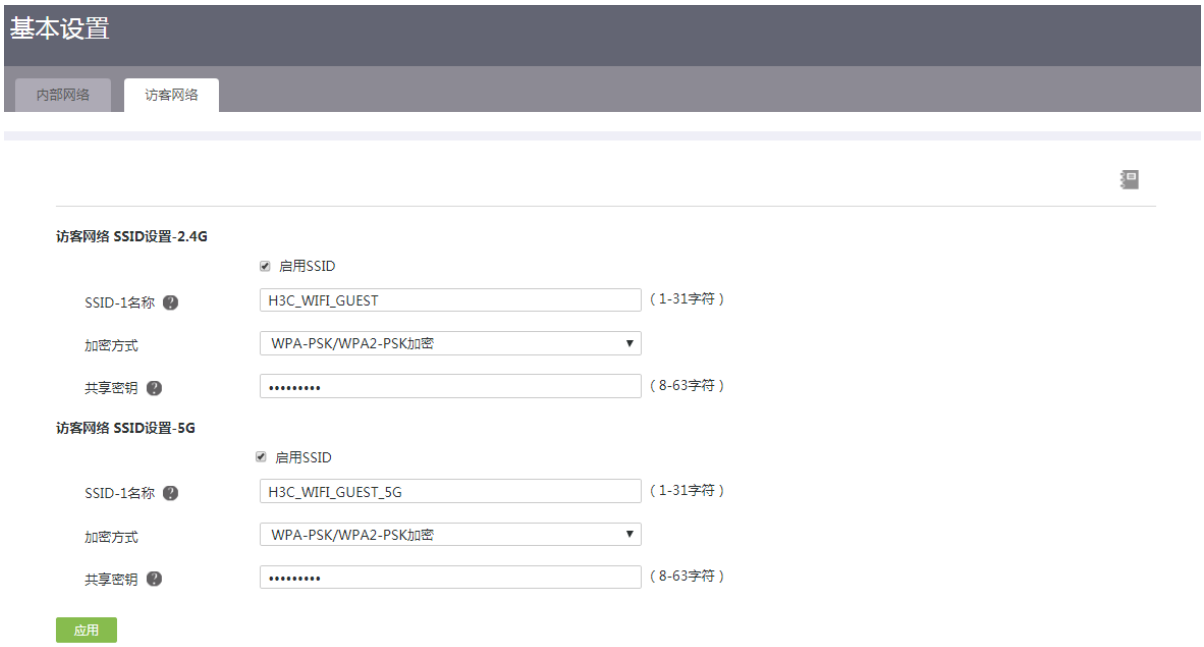
当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(4) 配置访客网络设置 SSID 设置-5G：

- 勾选“启用 SSID”选项，启用无线 5G 网络。
- 在“SSID-1 名称”配置项处，输入 5G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。

  当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

(5) 点击<应用>按钮，完成配置。



7.3 高级设置

7.3.1 无线射频管理

1. 配置简介

无线射频管理用来配置无线服务的更多参数（无线网络模式、无线网络信道频宽、无线信道、发射功率、修改 SSID 配置等）或创建及修改新的无线服务模板。

2. 注意事项

名称为“H3C_WIFI”、“H3C_WIFI_GUEST”、“H3C_WIFI_5G”和“H3C_WIFI_GUEST_5G”的 SSID 为系统默认的 SSID，不能被删除。

3. 配置步骤

(1) 单击导航树中[无线设置/高级设置]菜单项，进入高级设置页面。

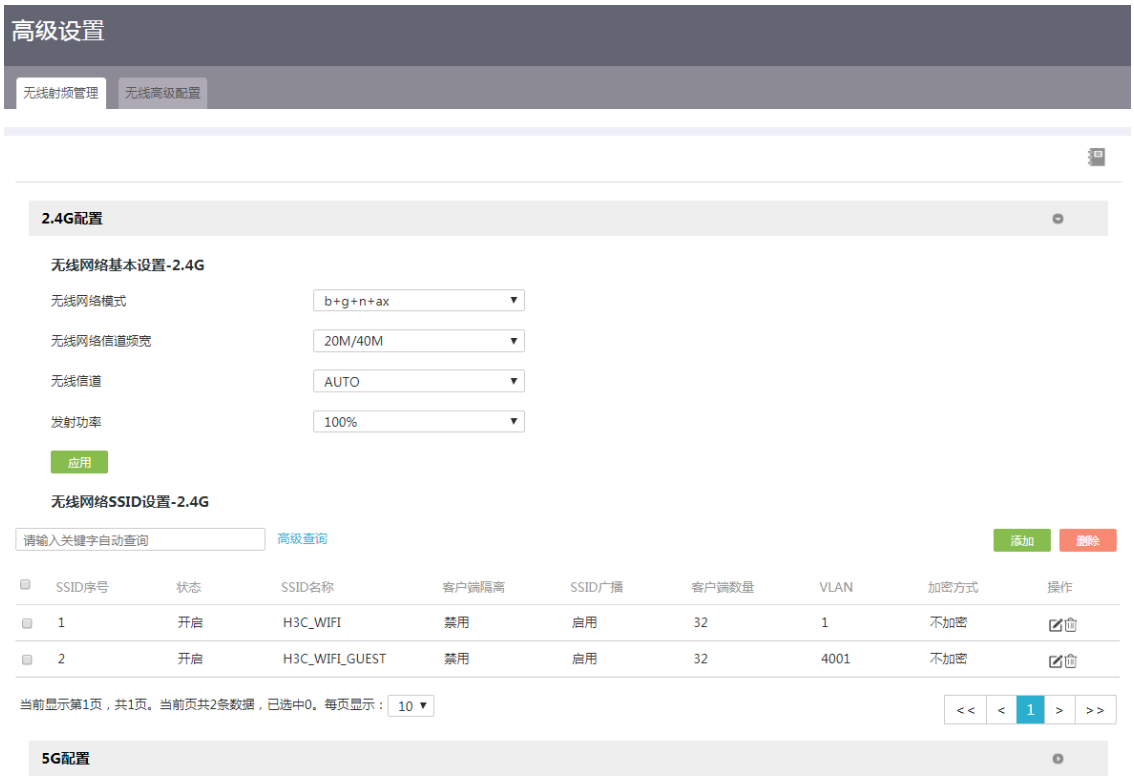
(2) 单击“无线射频管理”页签，进入无线射频管理页面。

(3) 配置无线网络设置 SSID 设置-2.4G：

在“无线网络基本设置-2.4G”配置项处，选择无线网络模式、频宽、信道和发射功率参数信息。通常情况下选择缺省配置即可，如需更改配置，请确保相关配置符合所在国家或区域的管制要求。配置完成后，点击<应用>按钮。

注意

发射功率是指天线在无线介质中所辐射的功率，反映的是 WLAN 设备辐射信号的强度。射频功率越大，射频覆盖的范围越广，客户端在同一位置收到的信号强度越强，也就越容易干扰邻近的网络。随着传输距离的增大，信号强度随之衰减。



(4) 添加 2.4G SSID 配置模板：

- 在“无线网络 SSID 设置-2.4G”配置项处，点击<添加>按钮，弹出“添加 SSID 配置”对话框。
- 勾选“启用 SSID”选项，启用无线 2.4G 网络。
- 在“SSID 名称”配置项处，输入 2.4G 无线服务的 SSID 名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’<>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。
- 在“加密协议”配置项处，选择加密机制来保护您的数据安全。
  - AES：在新无线网卡上使用，适用于 802.11n 无线传输协议，安全性更好。
  - TKIP：在老无线网卡上使用，适用于 802.11x 无线传输协议。
  - TKIP+AES：设备根据终端网卡情况自动选择加密协议。

AES 比 TKIP 采用更高级的加密技术，因此 AES 比 TKIP 的安全性更好，但 TKIP 对网卡的兼容性更好，部分老网卡可能不支持 AES，实际中请根据网卡的支持情况选择加密协议。

- 在“群组密钥更新周期”配置项处，设置群组密钥更新周期。

  设置密钥更新周期可以帮助您提高 WLAN 网络的安全性。

- 当您需要进一步设置客户端接入管理的相关功能时，请勾选“高级设置”选项。
  - 客户端隔离：选择与某个 SSID 建立连接的无线客户端之间是否可以互相通信。

    禁用：允许无线客户端之间进行通信。

    启用：禁止无线客户端之间进行通信。
  - SSID 广播：选择是否广播 SSID 功能。

    启用：当无线客户端搜寻本地可以接入的无线网络时，将检测到广播的 SSID，从而可以建立连接。

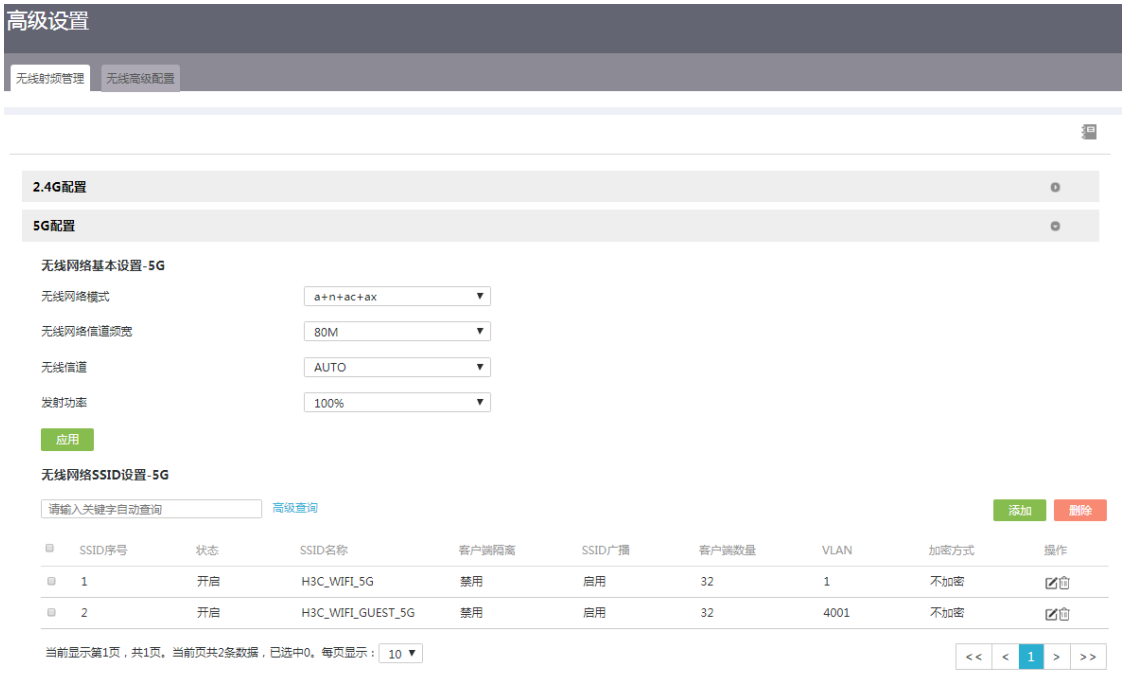
    禁用：管理员需要向客户端知会其 SSID 名称，客户端才可以根据 SSID 名称接入无线网络。
  - 最大客户端数量：设置 SSID 最大能够接入的无线客户端数量。
  - 桥接 VLAN：设置无线桥接 VLAN 的值。
- 点击<确定>按钮，完成配置。

(5) 配置无线网络设置 SSID 设置-5G：

在“无线网络基本设置-5G”配置项处，选择无线网络模式、频宽、信道和发射功率等参数信息。通常情况下选择缺省配置即可，如需更改配置，请确保相关配置符合所在国家或区域的管制要求。配置完成后，点击<应用>按钮。

注意

发射功率是指天线在无线介质中所辐射的功率，反映的是 WLAN 设备辐射信号的强度。射频功率越大，射频覆盖的范围越广，客户端在同一位置收到的信号强度越强，也就越容易干扰邻近的网络。随着传输距离的增大，信号强度随之衰减。



(6) 添加 5G SSID 配置模板：

- 在“无线网络 SSID 设置-5G”配置项处，点击<添加>按钮，弹出“添加 SSID 配置”对话框。
- 勾选“启用 SSID”选项，启用无线 5G 网络。
- 在“SSID 名称”配置项处，输入 5G 无线服务的 SSID 名称。SSID 名称长度为 1-31 个字符，可输入中文、英文字母[a-z,A-Z]、数字，以及特殊字符（空格~!@#$%^&*()_+-={}|[]:;’<>,./），其中 1 个中文字符占 3 个英文字符，英文字母区分大小写。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户在接入网络时需要输入此密钥。当您选择 WPA-PSK/WPA2-PSK 或 WPA2-PSK/WPA3-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写。

- 在“加密协议”配置项处，选择加密机制来保护您的数据安全。
- 在“群组密钥更新周期”配置项处，设置群组密钥更新周期。

  设置密钥更新周期可以帮助您提高 WLAN 网络的安全性。
- 当您需要进一步设置客户端接入管理的相关功能时，请勾选“高级设置”选项。
  - 客户端隔离：选择与某个 SSID 建立连接的无线客户端之间是否可以互相通信。

    禁用：允许无线客户端之间进行通信。

    启用：禁止无线客户端之间进行通信。
  - SSID 广播：选择是否广播 SSID 功能。

    启用：当无线客户端搜寻本地可以接入的无线网络时，将检测到广播的 SSID，从而可以建立连接。

    禁用：管理员需要向客户端知会其 SSID 名称，客户端才可以根据 SSID 名称接入无线网络。
  - 最大客户端数量：设置 SSID 最大能够接入的无线客户端数量。
  - 桥接 VLAN：设置无线桥接 VLAN 的值。
- 点击<确定>按钮，完成配置。

7.3.2 无线高级设置

1. 配置简介

无线高级配置用来配置禁止弱信号客户端接入和关闭广播探测高级需求。

2. 注意事项

- 客户端在设备内进行二层漫游时，要求两个AP处于相同的VLAN中，且AP绑定相同的SSID，即服务模板也保持一致。
- 配置禁止弱信号客户端接入功能，会导致信号强度低于指定门限值的无线客户端无法接入WLAN网络。

3. 配置步骤

(1) 单击导航树中[无线设置/高级设置]菜单项，进入高级设置页面。

(2) 单击“无线高级配置”页签，进入无线高级配置管理页面。您可视实际情况选择开启如下功能：

- 勾选“禁止弱信号客户端接入”选项，启用禁止弱信号客户端接入功能。
- 在“禁止接入信号强度”配置项处，设置信号强度，低于“禁止接入信号强度”的客户端将无法接入无线网络。

  在WLAN网络中，信号强度较弱的无线客户端虽然能够接入网络，但其所能获取到的网络性能和服务质量相比信号强的无线客户端要差很多。禁止弱信号客户端接入功能通过拒绝信号低于指定信号强度门限值的客户端接入，避免弱信号客户端占用较多的信道资源，减少对网络中其他客户端的影响，提升整网的用户体验。
- 勾选“关闭广播探测”选项，开启关闭广播探测功能，部分客户端将无法扫描到本设备接入AP的SSID。

(3) 点击<确定>按钮，完成配置。

7.4 客户端列表

1. 简介

本功能用于查看接入无线网络的客户端。

2. 配置步骤

(1) 单击导航树中[无线设置/客户端列表]菜单项，进入客户端列表配置页面。

(2) 勾选客户端前的复选框，点击<释放>按钮，断开客户端与无线服务的连接。

(3) 点击<全部释放>按钮，断开所有客户端与无线服务的连接。


客户端列表
请输入关键字自动查询
高级查询
刷新
自动刷新
释放
全部释放
客户端MAC地址
客户端IP地址
连接SSID
AP MAC地址
信号强度
发送速率
接收速率
连接时间
16-45-E1-9C-59-45
192.168.1.3
H3C_WIFI_5G
00-0C-43-26-46-45
(-78dBm)
216Mbps
6Mbps
00:00:10
当前显示第1页，共1页。当前页共1条数据，已选中0。每页显示：
10
<<
<
1
>
>>

8 网络设置

8.1 外网配置

8.1.1 简介

通常情况下，外网指的就是广域网（WAN，Wide Area Network），广域网是覆盖地理范围相对较广的数据通信网络，Internet 就是一个巨大的广域网。

通常在设备上会有多个 WAN 接口，通过配置 WAN 接口可以实现设备访问外网。

8.1.2 配置接口模式

说明

仅 UG8103 和 UG-1800W 设备支持单 WAN 模式，仅 UG8206 设备支持五 WAN 模式。

1. 配置需求

本功能用于配置设备 WAN 口接入的个数。

- 正常情况下，接口从 LAN 口转换到 WAN 口后，WAN 口的连接到互联网方式为 DHCP。接口相关的 VLAN 配置信息在接口转换后将会丢失。
- 正常情况下，接口转换会清除端口镜像配置信息，如你需要继续使用端口镜像功能，请在接口转换后重新配置。

2. 配置步骤

(1) 单击导航树中[网络设置/外网配置]菜单项，进入外网配置页面。

(2) 在“配置接口模式”页签下，勾选“单 WAN 模式”、“双 WAN 模式”、“三 WAN 模式”、“四 WAN 模式”或“五 WAN 模式”选项，设置设备支持的 WAN 口数量。

(3) 点击<应用>按钮，完成配置。

8.1.3 WAN 配置

(1) 单击导航树中[网络设置/外网配置]菜单项，进入外网配置页面。

(2) 单击“WAN 配置”页签，进入 WAN 配置页面。

(3) 在线路列表中，点击指定线路对应的操作列编辑图标，进入修改 WAN 配置页面。

(4) 根据用户实际的上网方式，在“连接模式”配置项处选择对应的连接模式：

- 如果选择连接模式为“PPPoE”：
  - 在“上网账号”配置项处，输入运营商提供的 PPPoE 接入用户名。
  - 在“上网密码”配置项处，输入运营商提供的 PPPoE 接入密码。
  - 在“LCP 主动检测”配置项处，选择在 PPPoE 链路处于异常状态时，是否开启保活报文检测功能。若选择“是”，表示开启，则每隔 20 秒钟检测一次；若选择“否”，表示关闭，则每隔 2 分钟检测一次。
  - “在线方式”为“始终在线”。

- 如果选择连接模式为“DHCP”，将自动从 DHCP 服务器获取接入外网的 IP 地址。
- 如果选择连接模式为“固定地址”：
  - 在“IP 地址”配置项处，输入接入广域网的固定 IP 地址，仅允许输入 A、B、C 类 IP 地址。
  - 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。
  - 在“网关地址”配置项处，输入接入广域网的网关地址，仅允许输入 A、B、C 类 IP 地址。
  - 在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。DNS1 缺省为 114.114.114.114，DNS2 缺省为 223.5.5.5。注意设备会优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。

(5) 在“MAC 地址”配置项处，根据实际需求选择“使用接口出厂 MAC 地址（例如：00-19-10-28-00-80）”或“使用静态指定的 MAC”。通过运营商分配的公网地址访问外网时，此处需选择“使用静态指定的 MAC”，并输入与运营商绑定的 MAC 地址。

(6) 在“网络上行带宽”和“网络下行带宽”配置项处，输入运营商提供的带宽值。

(7) 在“拨号方式”配置项处，选择 PPPoE 连接的拨号方式，如果选择自动拨号，配置完成后点击对话框下方的<确定>按钮，将会自动完成拨号；如果选择手动拨号，配置完成后需要点击对话框下方的<拨号>按钮才能完成拨号。当连接模式为“PPPoE”时，可配置该参数。

(8) 在“host-uniq”配置项处，设置 PPPoE client 呼叫报文是否携带 host-uniq 字段。

- 携带 host-uniq 字段：PPPoE client 呼叫报文中携带 host-uniq 字段。
- 不携带 host-uniq 字段：PPPoE client 呼叫报文中不携带 host-uniq 字段。

当连接模式为“PPPoE”时，当前设备将作为 PPPoE client 向 PPPoE server 发送呼叫报文，呼叫报文可以设置携带 host-uniq 字段，用来唯一标识发送呼叫报文的 PPPoE client。PPPoE server 收到携带 host-uniq 字段的报文后，必须在应答报文中携带 host-uniq 字段，内容和请求报文中的 host-uniq 字段相同。

当连接模式为“PPPoE”时，可配置该参数。因为在某些场景下，PPPoE server 会要求 PPPoE client 发送的呼叫报文中携带 host-uniq 字段，所以推荐选择“携带 host-uniq 字段”选项。

(9) 在“服务器名”配置项处，输入 PPPoE 连接的服务器名。当连接模式为“PPPoE”时，可配置该参数。

(10) 在“服务名”配置项处，输入 PPPoE 连接的服务名。当连接模式为“PPPoE”时，可配置该参数。

(11) 在“主机名”配置项处，输入需要通告给 DHCP 服务器的机器名。当连接模式为“DHCP”时，可配置该参数。

(12) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时，需要启用此功能。如果选择启用，可根据需要勾选“使用地址池转换”选项，并选择地址池。此处可选择的地址池是通过“网络设置-NAT 配置”中的“地址池”页签添加的。

(13) 在“TCP MSS”配置项处，设置接口的 TCP 报文段的最大长度，缺省为 1280 字节。

(14) 在“MTU”配置项处，输入接口允许通过的 MTU（Maximum Transmission Unit，最大传输单元）的大小。

(15) 在“链路探测”配置项处，可设置为未启用、ICMP 探测、DNS 探测和 NTP 探测。当选择 ICMP 探测、DNS 探测或 NTP 探测时，需设置如下参数：

- 在“探测地址”配置项处，输入链路探测的 IP 地址，如果链路探测配置为 DNS 探测，则也可以输入链路探测的域名。
- 在“探测间隔”配置项处，输入链路探测的时间间隔。
- 在“探测次数”配置项处，输入链路探测的探测次数。

启用链路探测功能后，可以对到达指定 IP 地址的链路状态进行判断，提高链路的可靠性。

(16) 点击<确定>按钮，完成 WAN 配置修改。

8.1.4 修改多 WAN 策略

1. 注意事项

只有多 WAN 场景可以进行本页面的配置。

2. 配置步骤

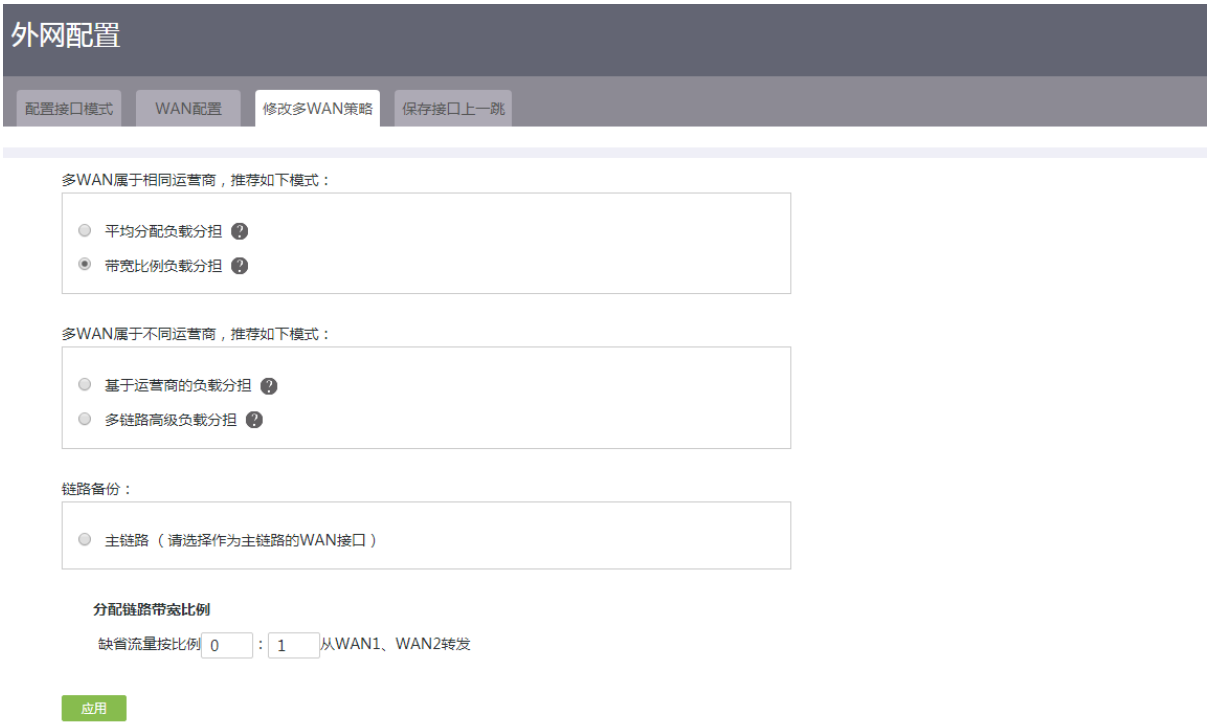
(1) 单击导航树中[网络设置/外网配置]菜单项，进入外网配置页面。

(2) 单击“修改多 WAN 策略”页签，进入修改多 WAN 策略配置页面。

(3) 根据实际应用，对多 WAN 策略进行修改：

- 如果多 WAN 属于相同的运营商，建议选择“平均分配负载分担”或“带宽比例负载分担”。如果多 WAN 链路的带宽一致，建议选择“平均分配负载分担”，否则选择“带宽比例负载分担”，并设置分配链路带宽比例。配置设备双 WAN 口上网时，如果 WAN1 和 WAN2 带宽比例设置为 0：1，此时所有流量仅通过 WAN2 口转发。
- 如果多 WAN 属于不同的运营商，建议选择“基于运营商的负载分担”或“多链路高级负载分担”。如果每个运营商提供的链路带宽一致，建议选择“基于运营商的负载分担”，否则选择“多链路高级负载分担”，并设置分配链路带宽比例。
- 为了保持网络的稳定性，可以进行链路备份，选择“主链路（请选择作为主链路的 WAN 接口）”以及对应的“WANn”，然后选择备份链路的“WANm”。注意 n 和 m 不能一致，否则不能实现链路备份。若所选的主链路已开启链路探测功能（在外网配置-WAN 配置中配置），系统会根据链路的探测结果更换实际生效的主链路；若所选的主链路未开启链路探测功能，系统会根据接口物理状态更换实际生效的主链路。

(4) 点击<应用>按钮，完成多 WAN 策略修改。



8.1.5 保存接口上一跳

(1) 单击导航树中[网络设置/外网配置]菜单项，进入外网配置页面。

(2) 单击“保存接口上一跳”页签，进入保存接口上一跳配置页面。

(3) 勾选“开启保存接口上一跳功能”或“关闭保存接口上一跳功能”选项。多 WAN 场景下，为了确保进入和离开局域网的报文通过同一个 WAN 接口转发，需要开启保存接口上一跳功能。

8.2 LAN配置

8.2.1 简介

本功能主要用于将设备的局域网接口加入 VLAN，配置 VLAN 接口参数，开启 DHCP 服务以及配置 DHCP 服务参数。

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网协议，主要用于为局域网内的主机分配 IP 地址。DHCP 支持动态及静态地址分配机制：

- 动态地址分配功能配置在接口上，此功能给用户主机动态分配 IP 地址，时间到期或主机明确表示放弃该地址时，该地址可以被其它主机使用。该分配方式适用于局域网的主机获取有一定有效期限的地址的组网环境。
- 静态分配的 IP 地址不与客户端的接口绑定，仅需要与主机的网卡 MAC 地址进行绑定，具有永久使用权限。该分配方式适用于局域网的主机获取租期为无限长的 IP 地址的组网环境。

8.2.2 配置 VLAN

1. 配置需求

需要将设备上的 LAN 接口加入指定的 VLAN，使得局域网内处于同一 VLAN 的主机能直接互通，处于不同 VLAN 的主机不能直接互通。

2. 注意事项

在详细端口配置页面配置端口的 PVID 时，只能指定已创建的 VLAN。

提示

PVID（Port VLAN ID，端口的缺省 VLAN）：当端口收到未携带 VLAN Tag 的报文时，即认为此报文所属的 VLAN 为端口的缺省 VLAN。

3. 配置准备

规划设备上 LAN 接口所属的 VLAN，并在 LAN 配置页面上，创建对应的 VLAN 接口。

4. 配置步骤

(1) 单击导航树中[网络设置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“VLAN 划分”页签，进入 VLAN 划分页面。

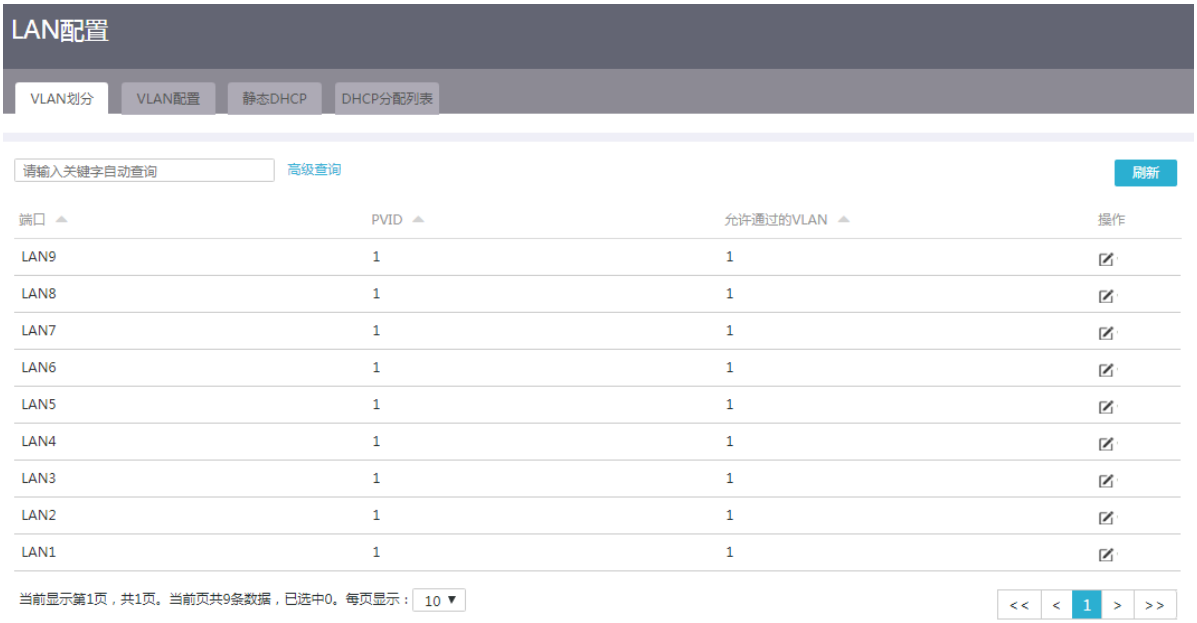
(3) 在端口列表中，点击指定端口上“操作”区段的按钮，弹出详细端口配置对话框。

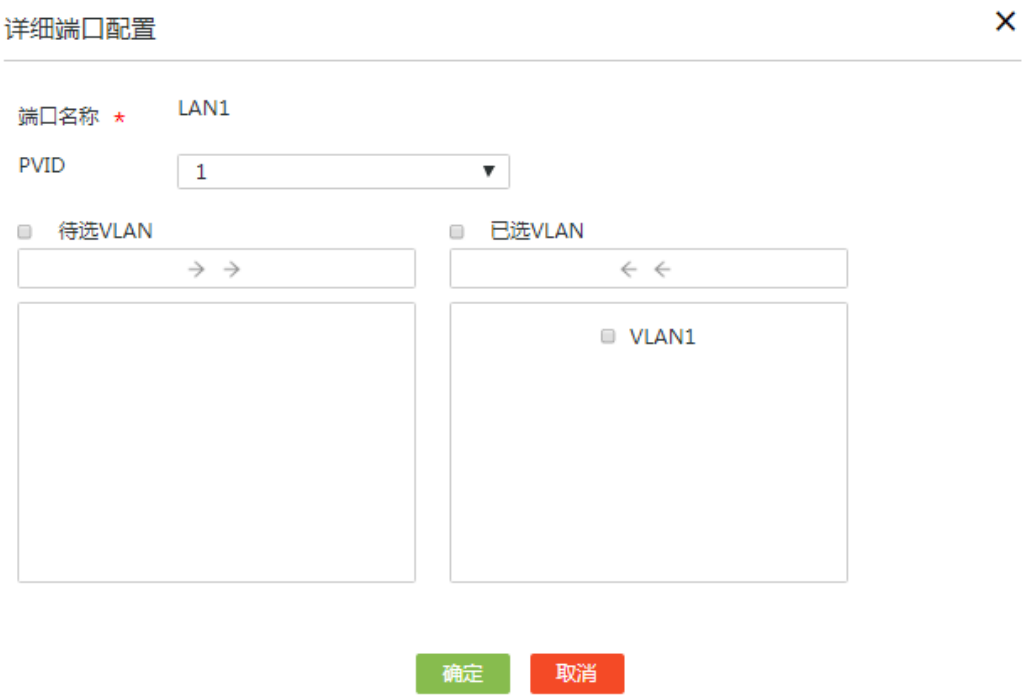
(4) 在“PVID”配置项处，通过下拉框修改端口的 PVID。

(5) 配置端口加入或移除 VLAN：

- 勾选“待选 VLAN”复选框下方的 VLAN 编号，或直接勾选“待选 VLAN”复选框以选中所有 VLAN，然后点击待选 VLAN 下方的向右方向按钮将端口加入所选 VLAN。
- 勾选“已选 VLAN”复选框下方的 VLAN 编号，或直接勾选“已选 VLAN”复选框以选中所有 VLAN，然后点击已选 VLAN 下方的向左方向按钮将端口从已加入的 VLAN 中移除。

(6) 点击<确定>按钮，完成配置。





8.2.3 配置 LAN 接口基本参数

1. 配置需求

为设备创建连接内网的 VLAN 接口，并可将 VLAN 接口作为内网设备的网关，提供 DHCP 服务。

2. 注意事项

若开启 VLAN 接口的 DHCP 服务后再关闭，则系统会同步删除静态 DHCP 页面中该 VLAN 接口已绑定的静态 DHCP。

3. 配置步骤

(1) 单击导航树中[网络设置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 已创建的 VLAN 接口显示在接口列表中，可以通过单击指定 VLAN 接口上“操作”区段的按钮进行编辑；通过单击指定 VLAN 接口上“操作”区段的按钮或勾选 VLAN 接口后单击“删除”按钮对选中的数据进行删除。

(4) 点击<添加>按钮，进入添加 LAN 接口页面。

(5) 在“VLAN ID”配置项处，输入 VLAN ID。

(6) 在“接口 IP 地址”配置项处，输入接口的 IP 地址。

(7) 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。

(8) 在“TCP MSS”配置项处，设置接口的 TCP 报文最大分段长度值，默认长度为 1280 字节。

(9) 在“MTU”配置项处，输入接口允许通过的 MTU 的大小。

(10) 勾选“开启 DHCP 服务”复选框，开启设备的 DHCP 服务，即为连接到设备的客户端（例如连接到设备的 PC 等）动态分配 IP 地址。根据实际情况，设置如下参数。

- 勾选“对 DHCP 分配的地址进行 ARP 保护（动态绑定）”复选框，为动态分配的 IP 地址绑定客户端的 MAC 地址。
- 在“地址池起始地址”和“地址池结束地址”配置项处，设置设备可分配给客户端的 IP 地址范围。
- 在“排除地址”配置项处，设置不能分配给客户端的 IP 地址。如果地址池范围内的某些 IP 地址（如网关地址）不能分配给客户端，就需要将其配置为排除地址。
- 在“客户端域名”配置项处，输入为客户端分配的域名后缀。
- 在“网关地址”和“DNS1”以及“DNS2”配置项处，输入客户端的网关地址和 DNS 服务器地址。
- 在“地址租约”配置项处，以分钟为单位设置 IP 地址的使用时间，比如设置 IP 地址租约为 5 天，则输入 7200。

(11) 点击<确定>按钮，完成配置。

8.2.4 配置静态 DHCP

1. 配置需求

如果需要为某些客户端分配固定的 IP 地址，则需要配置静态 DHCP 将客户端的硬件地址与 IP 地址进行绑定。

2. 注意事项

静态绑定的客户端 IP 地址不能是设备上 WAN 口的 IP 地址网段包含的 IP 地址。

3. 配置准备

在配置静态 DHCP 之前，需要先开启 VLAN 接口的 DHCP 服务。

4. 配置步骤

(1) 单击导航树中[网络设置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“静态 DHCP”页签，进入静态 DHCP 配置页面。

(3) 点击<添加>按钮，弹出新增 DHCP 静态绑定关系对话框。

(4) 在“接口”配置项处，选择开启 DHCP 服务器功能的接口。

(5) 在“客户端 MAC”配置项处，输入客户端的 MAC 地址。例如 PC 类型的客户端，可以在网卡信息中查询到 MAC 地址。

(6) 在“客户端 IP”配置项处，输入要分配给客户端的 IP 地址。

(7) 点击<确定>按钮，完成配置。

8.2.5 回收 DHCP 分配的 IP 地址

(1) 单击导航树中[网络设置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“DHCP 分配列表”页签，进入 DHCP 分配列表页面。

(3) 在列表中选中需要回收的 IP 地址。

(4) 点击<一键回收>按钮，在弹出的确认提示框中，点击<是>按钮，确认回收选中的 IP 地址。

8.2.6 静态绑定 DHCP 分配的 IP 地址

(1) 单击导航树中[网络设置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“DHCP 分配列表”页签，进入 DHCP 分配列表页面。

(3) 在列表中选中需要静态绑定的客户端 IP。

(4) 点击<静态分配>按钮，在弹出的确认提示框中，点击<是>按钮，确认将 DHCP 动态分配的 IP 地址设置为静态分配。

8.3 端口管理

8.3.1 简介

端口管理功能用来查看设备各个物理端口的端口类型、端口模式、速率、MAC 地址和广播风暴抑制等信息，设置 WAN 口的管理状态，以及修改端口配置。

8.3.2 配置步骤

(1) 单击导航树中[网络设置/端口管理]菜单项，进入端口管理页面。

(2) 在物理端口列表中，点击指定端口对应的操作列编辑图标，弹出修改端口配置对话框。

(3) 在“管理状态”配置项处，设置开启或者关闭该端口。

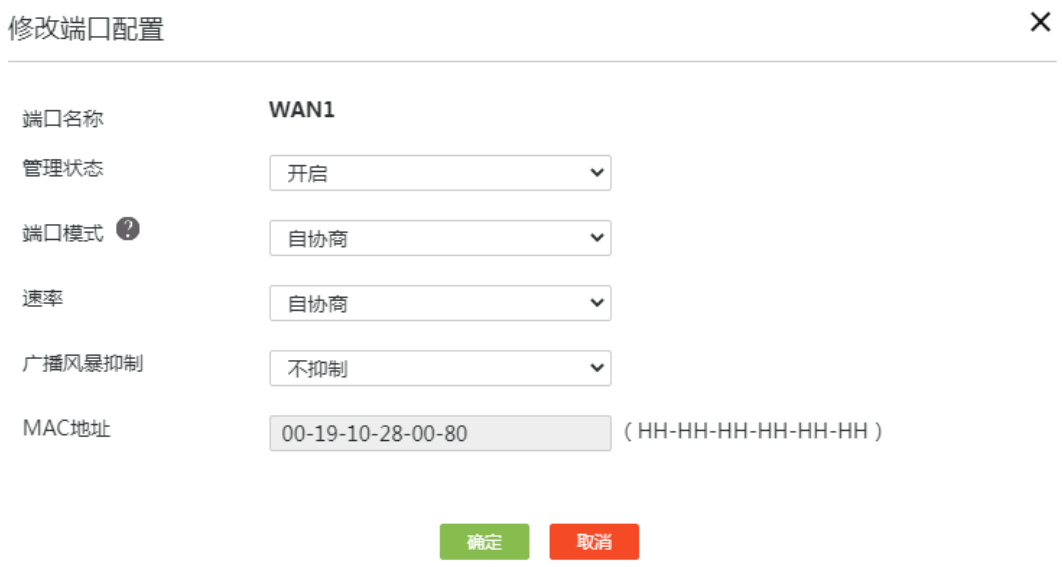
(4) 在“端口模式”配置项处，选择配置的端口模式。

(5) 在“速率”配置项处，选择配置的端口速率。

(6) 在“广播风暴抑制”配置项处，可根据需要选择不抑制或者抑制级别。抑制级别分为低、中、高，三个级别对应的允许通过的广播报文数量依次增加。

(7) 在“MAC 地址”配置项处，查看端口的 MAC 地址。

(8) 点击<确定>按钮，完成配置。



8.4 NAT配置

8.4.1 简介

NAT（Network Address Translation，网络地址转换）是一种将内部网络私有 IP 地址，转换成公网 IP 地址的技术。拥有私有 IP 地址的内网用户无法直接访问 Internet，如果希望内网用户使用运营商提供的公网 IP 访问外网，或者允许外网用户使用公网 IP 访问内网资源，则需要配置 NAT。

NAT 支持如下两种地址转换方式：

- 端口映射：通过这种转换方式，可以实现利用一个公网地址和不同的协议端口同时对外网提供多个内网服务器（例如 Web、Mail 或 FTP 服务器）资源的目的。这种方式可以节约设备的公网 IP 地址资源。端口映射可以将内网中的一组 IP 地址和不同的协议端口映射到一个公网 IP 地址和对应的协议端口上，使得一个公网 IP 地址可以同时分配给多个内网 IP 地址使用。
- 一对一映射：这种方式适用于内外网之间存在固定访问需求的环境，比如某个网络管理员必须使用一个固定的外网 IP 去远程访问位于内网中对外提供服务的设备。一对一映射可以在设备上建立一个固定的一对一的映射关系，将内网中的一个私有 IP 地址转换为一个公网 IP 地址。
- 端口触发：当局域网内的客户端访问因特网上的服务器时，对于某些应用（比如：IP 电话、视频会议等），客户端向服务器主动发起连接的同时，也需要服务器向客户端发起连接请求。而缺省情况下，设备收到 WAN 侧主动连接的请求都会拒绝，此时通信会被中断。通过设置设备的端口触发规则，当客户端访问服务器并触发规则后，设备会自动开放服务器需要向客户端请求的端口，从而可以保证通信正常。当客户端和设备长时间没有数据交互时，设备自动关闭之前对外开放的端口，既保证应用的正常使用，又能最大限度地保证局域网的安全。

NAT 还提供如下高级配置功能：

- NAT hairpin：如果您的某些内网服务器通过公网 IP 地址对外提供服务，同时内网用户也有访问这些服务器的需求，为了确保这些内网用户访问内网服务器的流量也经过网关控制，则可以开启 NAT hairpin 功能。开启该功能后，内网用户将与外网用户一样，都可以使用公网 IP 地址访问内网服务器。
- NAT ALG：如果内部网络与外部网络之间存在应用层业务，例如 FTP/RTSP，为了保证这些应用层协议的数据连接经过端口映射或一对一映射后还可以正确建立，就需要开启相应协议的 NAT ALG 功能。

8.4.2 配置虚拟服务器

(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“虚拟服务器”页签，进入虚拟服务器配置页面。

(3) 在“NAT DMZ 服务”配置项处，勾选“开启”选项，开启 NAT DMZ 服务。

(4) 在“主机地址”配置项处，输入 NAT DMZ 服务的主机地址。

(5) 点击<应用>按钮，完成配置。

(6) 点击<添加>按钮，弹出添加 NAT 端口映射对话框。

(7) 在“协议类型”配置项处，选择协议为“TCP”、“UDP”或“TCP+UDP”。此处需要根据内部服务器采用的传输层协议类型选择 TCP 或 UDP，例如 FTP 服务器采用 TCP 协议，TFTP 采用 UDP 协议。

(8) 在“外部地址”配置项处，可以选择使用当前端口的 IP 地址，也可以使用设备上的其它公网 IP 地址。

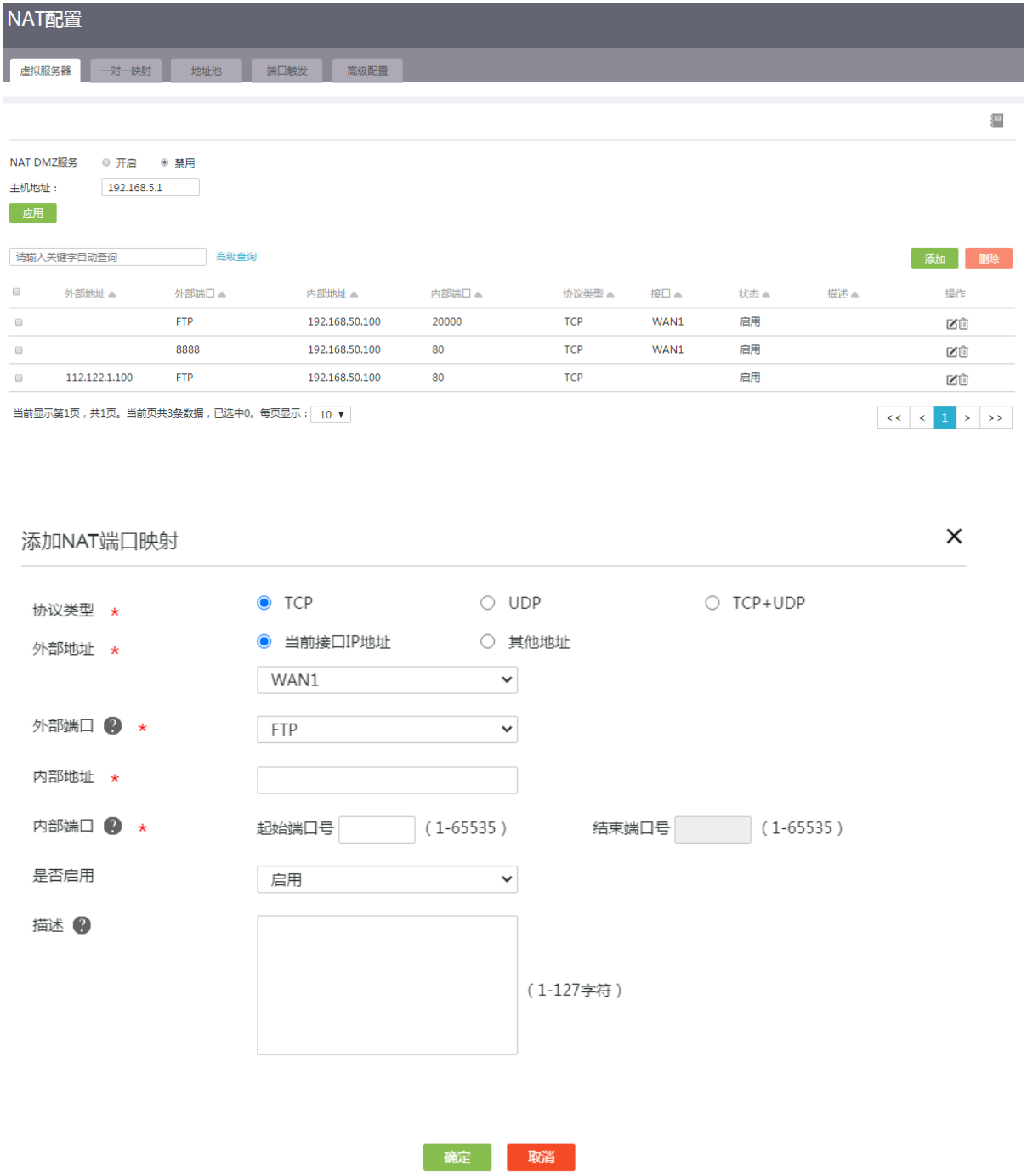
(9) 在“外部端口”配置项处，选择 FTP、Telnet 或自定义端口。如果您对外提供的服务不是 FTP 或 Telnet，请输入提供的服务所使用的端口号，比如 HTTP 服务端口号 80。

(10) 在“内部地址”配置项处，输入允许外部网络访问的内网 IP 地址。

(11) 在“内部端口”配置项处，输入内部网络资源使用的端口号。

(12) 在“是否启用”配置项处，选择是否立即启用映射。

(13) 点击<确定>按钮，完成配置。



8.4.3 配置一对一映射

1. 注意事项

如果设备上仅有一个公网 IP 地址，不建议配置一对一映射来占用公网 IP 地址。

2. 配置步骤

(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“一对一映射”页签，进入一对一映射配置页面。

(3) 在“一对一映射”配置项处，勾选“开启”选项，开启一对一映射服务。

(4) 点击<添加>按钮，弹出添加 NAT 一对一映射对话框。

(5) 在“内部地址”配置项处，输入内网 IP 地址。

(6) 在“外部地址”配置项处，输入拥有的公网 IP 地址。

(7) 在“接口”配置项处，选择配置映射的接口。若不设置此参数，则表示对所有 WAN 口生效。

(8) 在“是否启用”配置项处，选择是否立即启用映射。

(9) 点击<确定>按钮，完成配置。

8.4.4 配置地址池

(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“地址池”页签，进入地址池配置页面。

(3) 点击<添加>按钮，弹出添加 NAT 地址池对话框。

(4) 在“地址池名”配置项处，输入用于 NAT 转换的公网 IP 地址池名称，可以由中文、数字、字母、下划线组成。

(5) 在“IP 地址”配置项处，输入单个 IP 地址。

(6) 在“起始”配置项处，输入 IP 地址段的起始 IP 地址。

(7) 在“结束”配置项处，输入 IP 地址段的终止 IP 地址。单个 IP 地址段内的 IP 地址数量不能超过 256 个，且不能存在不合理的 IP 地址。

(8) 点击配置项右侧的<→→>按钮，提交配置的 IP 地址或 IP 地址段内容。

(9) 重复(5)、(6)、(7)、(8)步骤可完成多个地址池的添加。

(10) 点击<确定>按钮，完成配置。

8.4.5 配置端口触发

(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“端口触发”页签，进入端口触发配置页面。

(3) 点击<添加>按钮，弹出添加 NAT 端口触发对话框。

(4) 在“应用名称”配置项处，输入端口触发的应用名称。

(5) 在“生效接口”配置项处，选择用于接收外来报文的接口。

(6) 在“触发端口”配置项处，输入局域网内客户端向外网服务器发起请求的端口范围。

(7) 在“外来端口”配置项处，输入外网服务器需要向局域网内客户端主动发起请求的端口号。可设置单一端口、端口范围或两者的组合，端口间用英文逗号“,”隔开，例如：100,200-300,400。最多可输入 10 个端口或端口范围。

(8) 在“是否启用”配置项处，选择是否启用端口触发功能。

(9) 点击<确定>按钮，完成配置。

8.4.6 配置 NAT hairpin

1. 配置准备

在配置 NAT hairping 前，需要完成如下配置中的一项或多项：

- 在虚拟服务器配置页面上，配置内网服务器的 IP 地址/端口与公网 IP 地址/端口的映射关系。
- 在一对一映射配置页面上，配置内网用户 IP 地址与公网 IP 地址的映射关系。

2. 配置步骤

(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 高级配置页面。

(2) 完成“虚拟服务器”或“一对一映射”的配置。

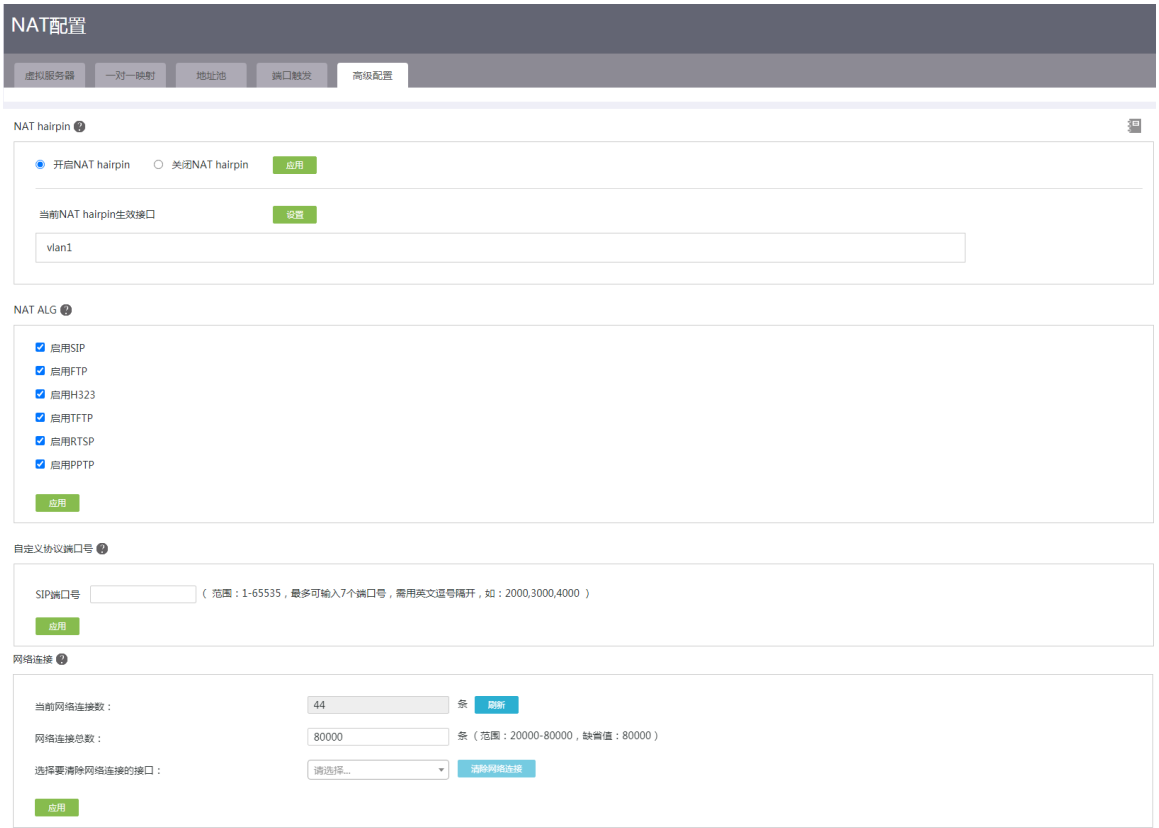
(3) 单击“高级配置”页签，进入高级配置页面。

(4) 勾选“开启 NAT hairpin”选项，点击<应用>按钮，启用 NAT hairpin 功能。

(5) 点击<设置>按钮，弹出修改 NAT hairpin 生效接口对话框。根据需要选择接口成为 NAT hairpin 功能的生效接口：

- 将接口设置为生效接口：勾选“待选接口”选项或者在待选接口列表中选中接口，点击<→→>按钮，再点击<确定>按钮，完成配置。
- 将接口设置为不生效接口：勾选“已选接口”选项或者在已选接口列表中选中接口，点击<←←>按钮，再点击<确定>按钮，完成配置。

(6) 点击<确定>按钮，完成配置。



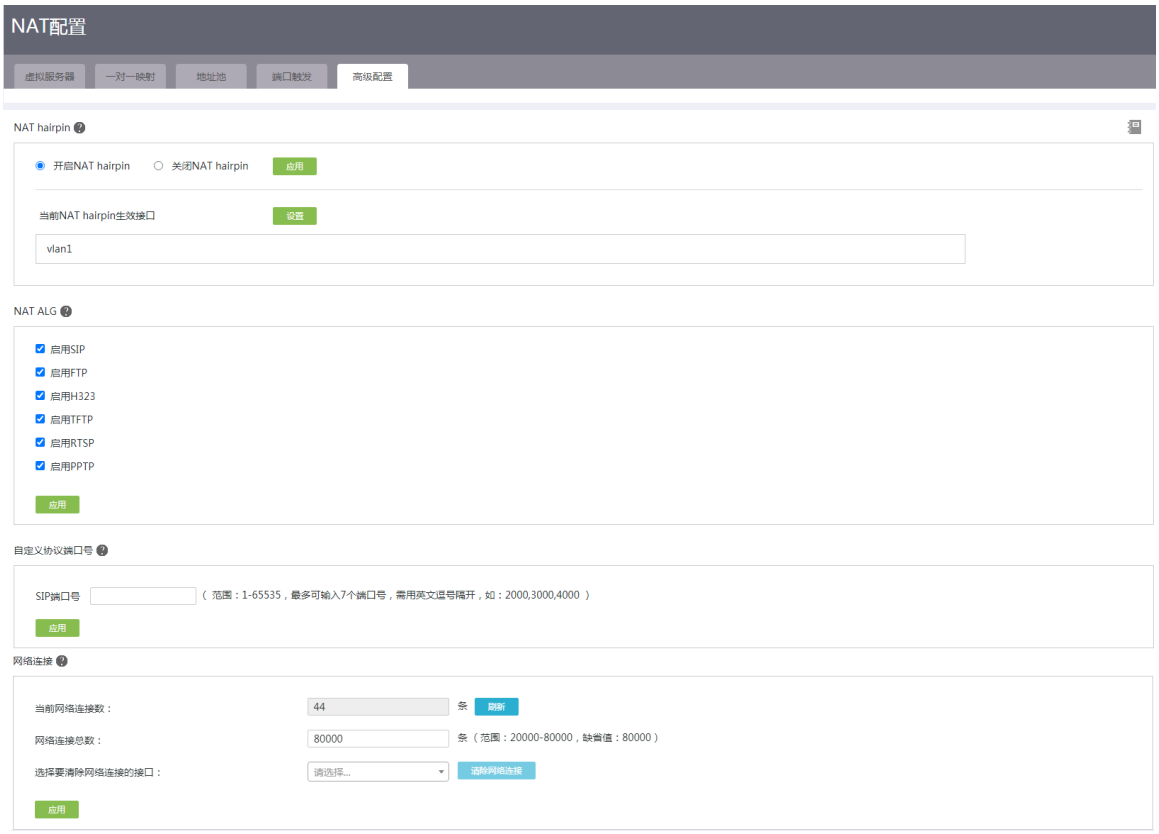
8.4.7 配置 NAT ALG

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“高级配置”页签，进入高级配置页面。

(3) 在 NAT ALG 区段，勾选对应的选项，启用指定协议的 NAT ALG 功能。

(4) 点击<应用>按钮，完成配置。



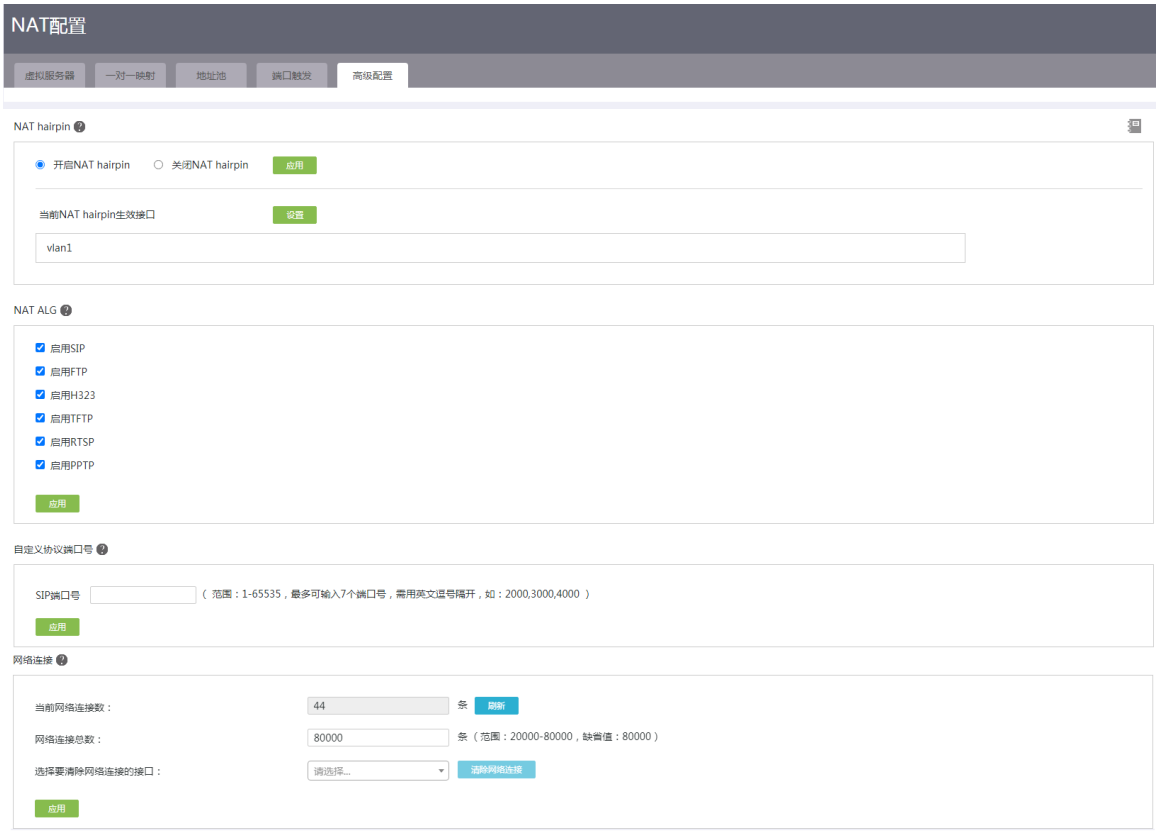
8.4.8 配置自定义协议端口号

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“高级配置”页签，进入高级配置页面。

(3) 在自定义协议端口号区段，根据需要设置“SIP 端口号”配置项，在搭建 SIP 服务器时，如果使用的 SIP 协议端口号不是 5060，则需要自定义 SIP 协议端口号。

(4) 点击<应用>按钮，完成配置。



8.4.9 配置网络连接

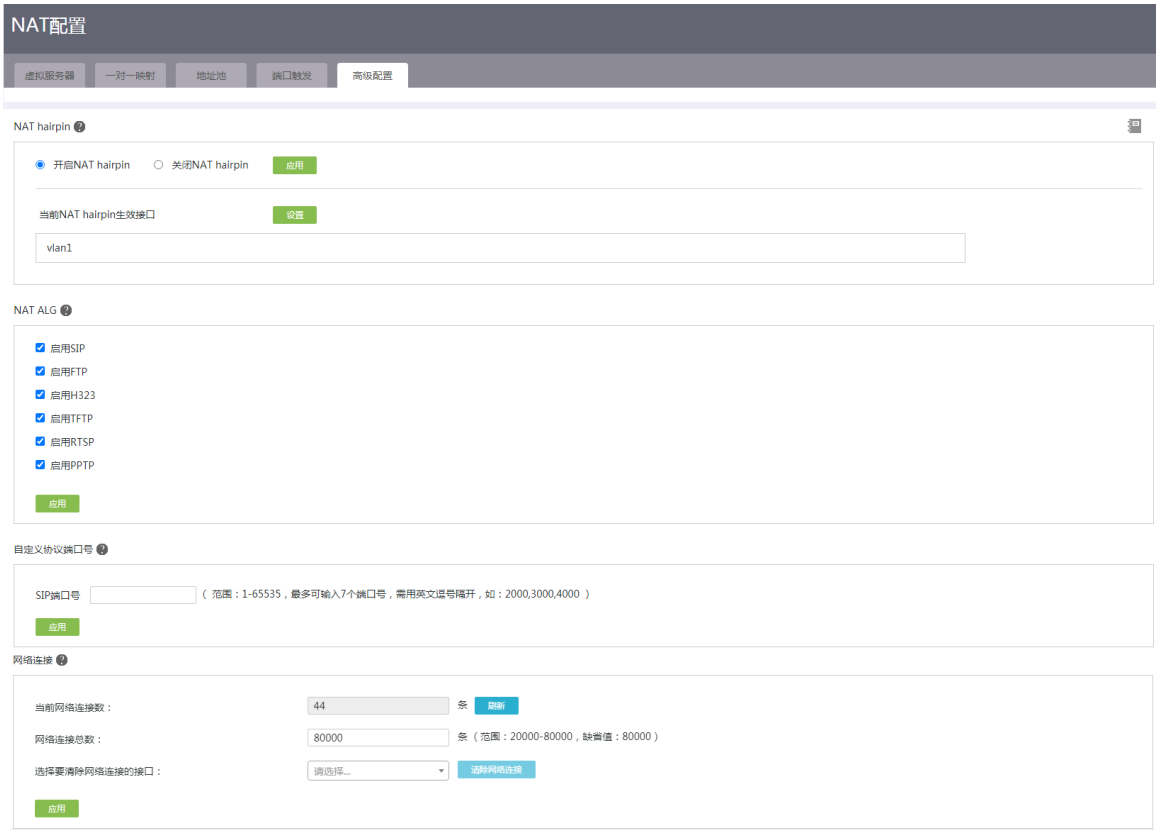
(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“高级配置”页签，进入高级配置页面。

(3) 在网络连接区段，设置如下参数：

- 在“当前网络连接数”配置项处，查看当前的网络连接数量，可点击<刷新>按钮刷新。
- 在“网络连接总数”配置项处，设置允许建立的网络连接总数，推荐使用缺省值。对于不同型号的设备，本参数的取值范围和缺省值可能会不同，请以 Web 页面实际显示情况为准。
- 在“选择要清除网络连接的接口”配置项处，选择需要清除网络连接的接口。

(4) 点击<应用>按钮，完成配置。



8.5 地址组

8.5.1 简介

地址组是一组主机名或 IP 地址的集合。每个地址组中可以添加若干成员，成员的类型包括 IP 地址和 IP 地址段。如果您的某些业务（例如带宽管理）需要使用地址组来识别用户报文，则需要提前配置符合业务需求的地址组。

8.5.2 注意事项

- 添加到地址组中的 IP 地址只支持 IPv4 地址格式，不支持 IPv6 地址格式。
- 添加到地址组中的 IP 地址段的起始地址必须小于结束地址。
- 单个 IP 地址段内的 IP 地址数量不能超过 256 个，且不能存在不合理的 IP 地址。

8.5.3 配置步骤

(1) 单击导航树中[网络设置/地址组]菜单项，进入地址组配置页面。

(2) 点击<添加>按钮，弹出添加地址组对话框。

(3) 在“地址组名称”配置项处，输入地址组的名称。

(4) 在“描述信息”配置项处，输入地址组的描述信息。

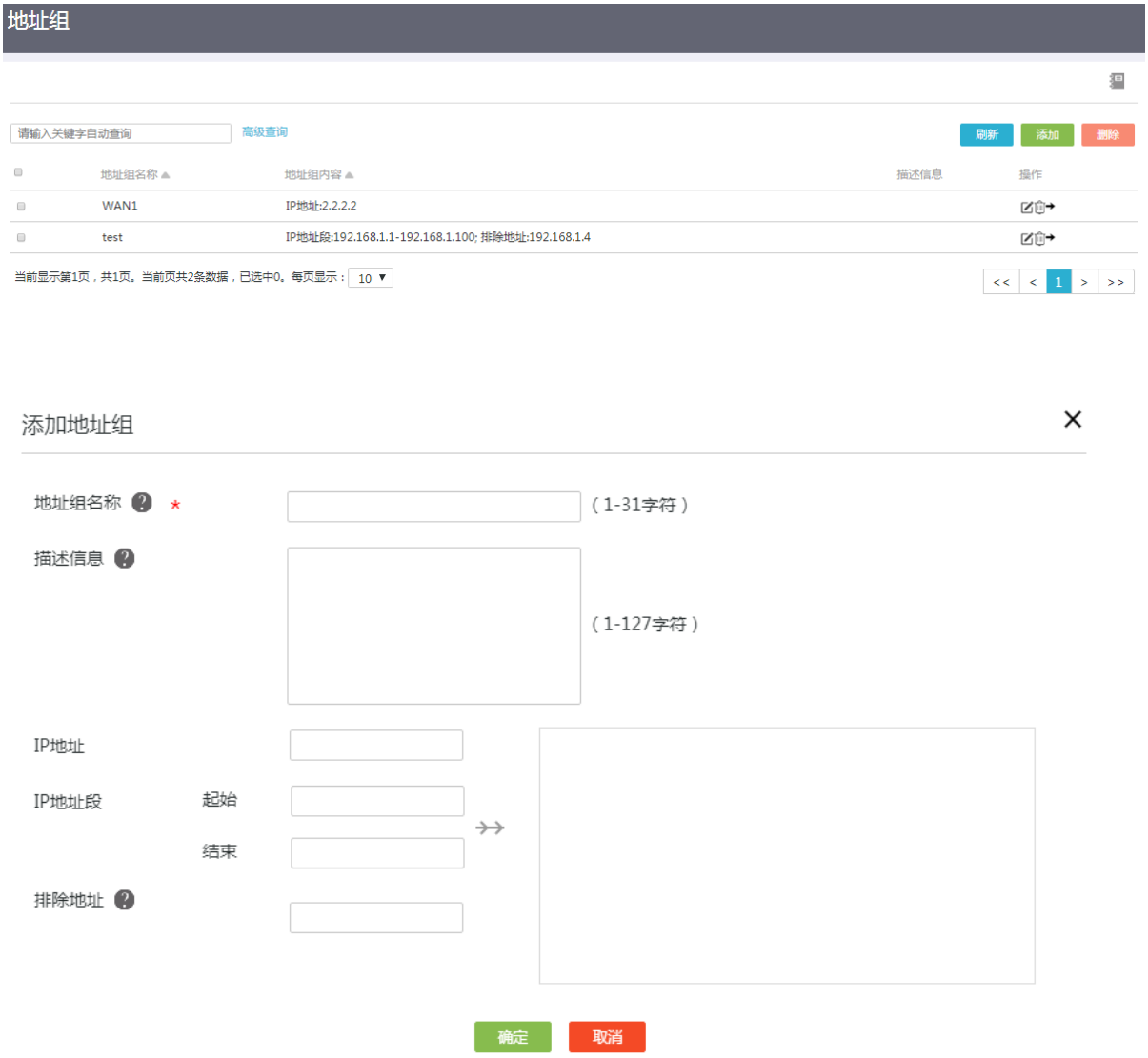
(5) 配置地址组内容：

- 配置添加到地址组的单个 IP 地址。
- 配置添加到地址组 IP 地址段的起始 IP 地址及结束 IP 地址。
- 配置地址组排除的 IP 地址。

(6) 点击配置项右侧的<→→>按钮，提交配置的地址组内容。

(7) 重复(5)、(6)步骤可完成多个同类型成员的添加。

(8) 点击<确定>按钮，完成地址组创建。



8.6 时间组

8.6.1 简介

如果您希望设备上的某些功能（例如带宽管理、上网行为管理）仅在特定时间生效，而其它时间不生效，可以创建一个时间组，并在配置相关功能时引用时间组。

一个时间组中可以配置一个或多个时间段。时间段的生效时间有如下两种方式：

- 周期性生效：以周作为周期，循环生效。例如，每周一的 8 至 12 点。
- 非周期生效：在指定的时间范围内生效。例如，2015 年 1 月 1 日至 2015 年 1 月 3 日每天的 8 点至 18 点。

8.6.2 注意事项

- 最多可以创建 64 个不同名称的时间组。
- 一个时间组内最多可以配置 16 个周期性生效的时间段或 16 个非周期生效的时间段。

8.6.3 配置步骤

(1) 单击导航树中[网络设置/时间组]菜单项，进入时间组配置页面。

(2) 点击<添加>按钮，弹出新建时间组对话框。

(3) 在“时间组名称”配置项处，输入时间组的名称。

(4) 在“生效时间”配置项处，选择“周期性生效”或“非周期性生效”，然后配置时间段。请选择其中一项进行配置。

- 周期性生效

  点选每周需要生效的具体星期，并在下面输入每天的具体生效时间，点击<+>按钮，完成本时间段的配置。

- 非周期性生效

  选择生效的起止日期，并在下面输入具体生效的起止时间，点击<+>按钮，完成本时间段的配置。

(5) 点击<确定>按钮，完成时间组创建。

8.7 应用组

8.7.1 简介

如果您希望设备上的带宽管理功能仅对特定的应用生效，而对其它的应用不生效，可以创建一个或者多个应用，将创建的应用添加到应用组，并在配置带宽管理时引用应用组。

8.7.2 自定义应用

1. 配置需求

对特定的应用协议和端口号进行严格的带宽管理。

2. 注意事项

自定义应用创建完成后，需要将其添加到“应用组”中，并在配置带宽管理时引用对应的应用组，才能实现对特性应用的带宽管理。

3. 配置步骤

(1) 单击导航树中[网络设置/应用组]菜单项，进入自定义应用配置页面。

(2) 点击<添加>按钮，弹出添加应用对话框。

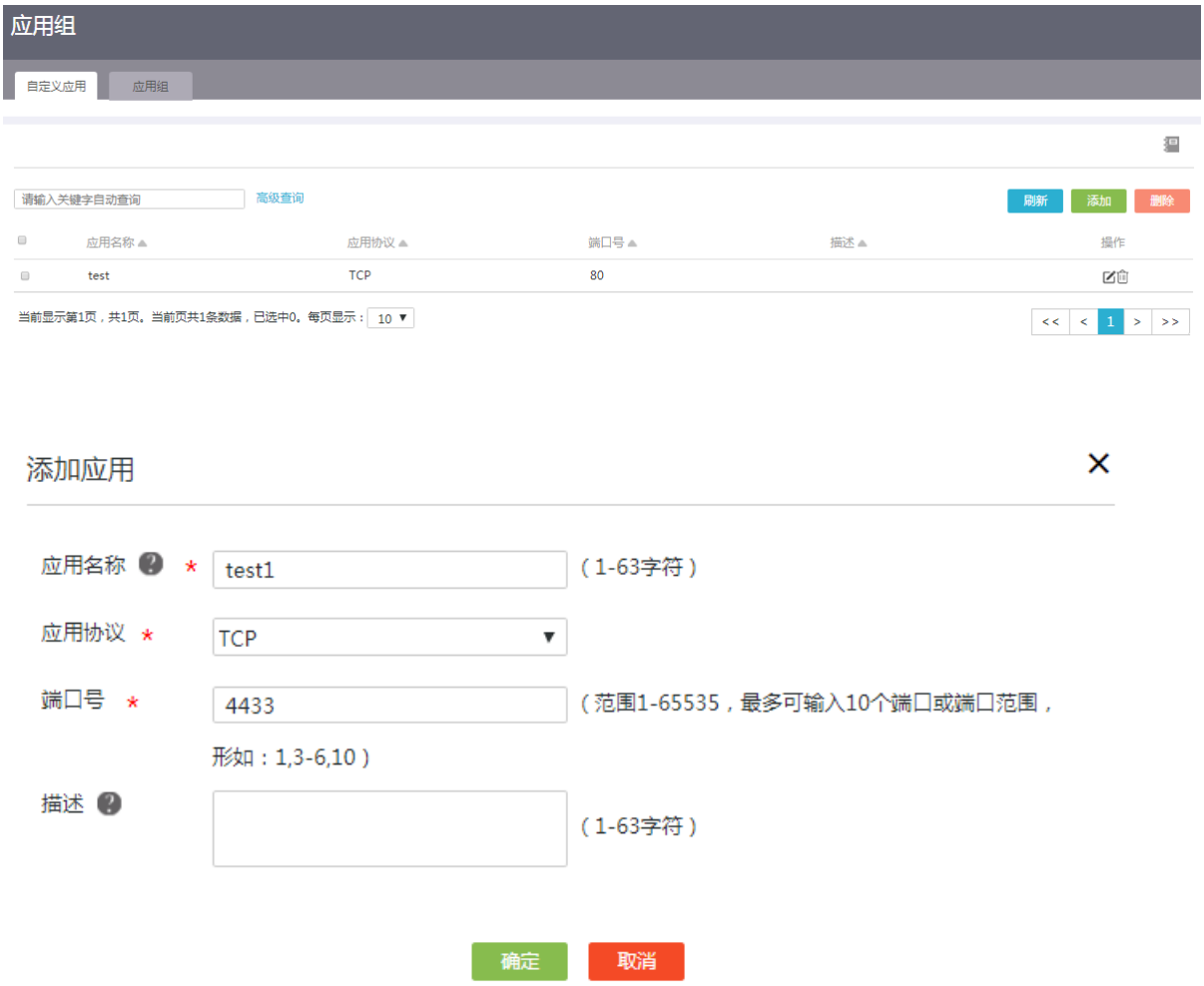
(3) 在“应用名称”配置项处，输入应用的名称。

(4) 在“应用协议”配置项处，选择“TCP”、“UDP”或“TCP+UDP”。

(5) 在“端口号”配置项处，输入应用的端口号。

(6) 在“描述”配置项处，输入应用的描述信息。

(7) 点击<确定>按钮，完成应用创建。



8.7.3 创建应用组

1. 配置需求

通过对自定义应用进行分组，实现对一组自定义应用进行严格的带宽管理。

2. 注意事项

应用组创建完成后，在配置带宽管理时引用应用组，才能实现对特定的一组自定义应用进行带宽管理。

3. 配置步骤

(1) 单击“应用组”页签，进入应用组配置页面。

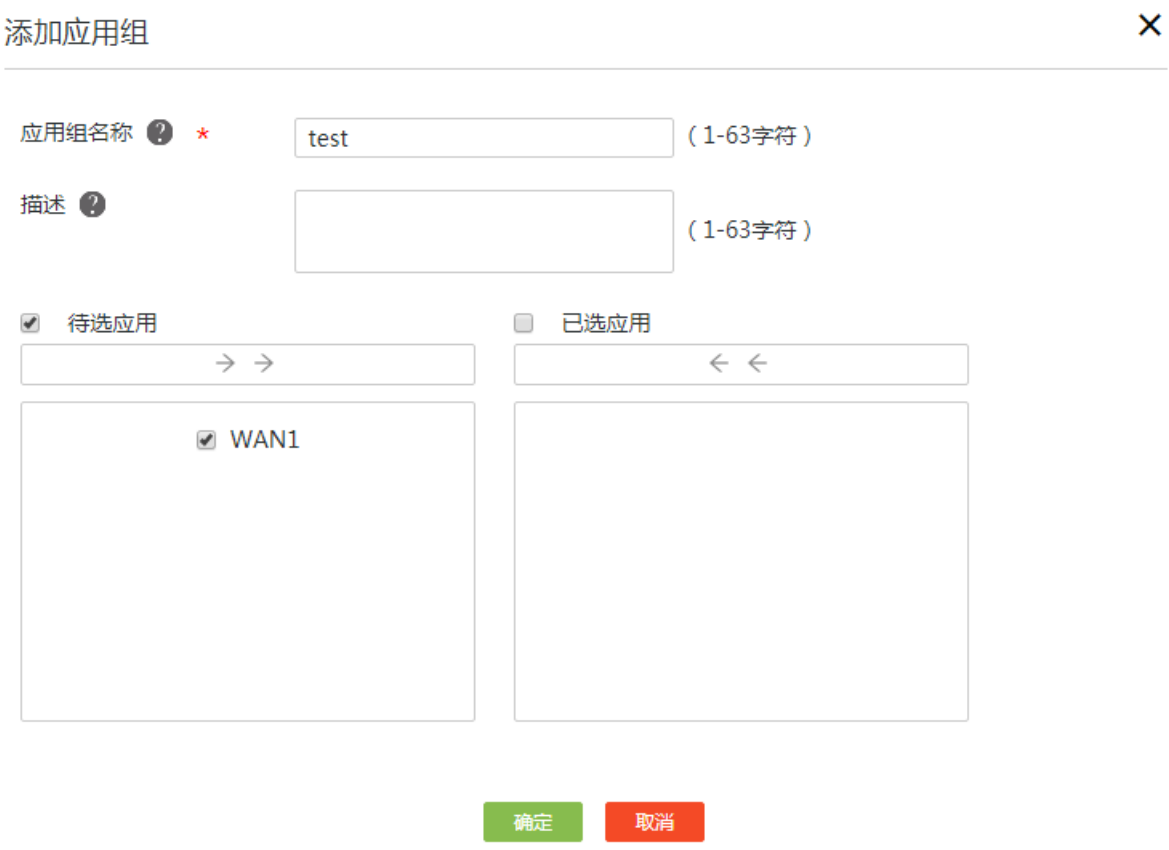
(2) 点击<添加>按钮，弹出新建应用组对话框。

(3) 在“应用组名称”配置项处，输入应用组的名称。

(4) 在“描述”配置项处，输入应用组的描述信息。

(5) 在“待选应用”选择框中，勾选应用，点击<→→>按钮，将应用添加到“已选应用”选择框中；在“已选应用”选择框中，勾选应用，点击<←←>按钮，将应用从“已选应用”选择框中移除。

(6) 点击<确定>按钮，完成应用组创建。



9 上网行为管理

9.1 配置任务导引

9.1.1 限制 WAN 口的带宽

当管理员需要限制特定 WAN 口的带宽时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	配置地址组（必选）	将需要限制带宽的用户IP地址加入到地址组中，具体配置方法请见参见地址组。
1	配置时间组（可选）	设定限制带宽的时间段，具体配置方法请见参见时间组。
2	配置IP限速（必选）	添加IP限速策略，设置各参数，选择地址组，具体配置方法请见参见配置IP限速。

9.1.2 限制某些应用的带宽

当管理员需要限制某些应用的带宽时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	添加自定义应用（必选）	添加需要限制带宽的应用到自定义应用列表中，具体配置方法请见参见自定义应用。
2	创建应用组（必选）	创建应用组，将需要限制带宽的应用加入到应用组中，具体配置方法请见参见创建应用组。
3	配置限制通道（必选）	启用限制通道流速上限，设置各参数，选择应用组，具体配置方法请见参见配置限制通道。

9.1.3 保障某些应用的带宽

当管理员需要保障某些应用的可用带宽时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	添加自定义应用（必选）	添加需要保障可用带宽的应用到自定义应用列表中，具体配置方法请见参见自定义应用。
2	创建应用组（必选）	创建应用组，将需要保障可用带宽的应用加入到应用组中，具体配置方法请见参见创建应用组。
3	配置绿色通道（必选）	启用绿色专用通道后，设置各参数，选择应用组，具体配置方法请见参见配置绿色通道。

9.1.4 限制用户可使用的应用

当管理员需要限制特定用户使用的某些应用时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	配置地址组（可选）	将需要设置的用户IP地址加入到地址组中，具体配置方法请见参见地址组。
2	配置时间组（可选）	设定限制用户使用应用的时间段，具体配置方法请见参见时间组。
3	配置应用控制（必选）	如果限制用户使用常见的应用，可以在配置应用控制时指定应用，具体配置方法请见参见配置应用控制；如果限制用户使用不常见的应用，需要先自定义网络应用，具体配置方法请见参见配置自定义网络应用，然后再配置应用控制。

9.1.5 通过白名单限制用户可访问的网址

当管理员需要为特定用户设置允许访问的网址时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	配置地址组（可选）	将需要设置的用户IP地址加入到地址组中，具体配置方法请见参见地址组。
2	配置时间组（可选）	设定允许用户访问网址的时间段，具体配置方法请见参见时间组。
3	配置网址控制（必选）	开启网址白名单模式，并添加自定义网址分类，具体配置方法请见参见配置网址控制。

9.1.6 通过黑名单设置用户禁止访问的网址

当管理员需要为特定用户设置禁止访问的网址时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	配置地址组（可选）	将需要设置的用户IP地址加入到地址组中，具体配置方法请见参见地址组。
2	配置时间组（可选）	设定禁止用户访问网址的时间段，具体配置方法请见参见时间组。
3	配置网址控制（必选）	开启网址黑名单模式，并添加自定义网址分类，具体配置方法请见参见配置网址控制。

9.1.7 限制用户可下载的文件类型

当管理员需要为特定用户设置允许下载的文件类型时，可以根据如下步骤进行配置。

步骤	配置内容	详情
1	配置地址组（可选）	将需要设置的用户IP地址加入到地址组中，具体配置方法请见参见地址组。
2	配置时间组（可选）	设定允许用户下载在指定类型文件的时间段，具体配置方法请见参见时间组。
3	配置文件控制（必选）	设置允许用户下载的文件类型，具体配置方法请见参见配置文件控制。

9.2 带宽管理

9.2.1 简介

带宽管理功能用于对流量进行管理，管理员可基于地址组和时间组等限制条件对用户流量进行精细控制。对于需要进行限速的报文，例如占用大量带宽的 P2P 下载报文，可选择开启限制通道功能，来限制其带宽。对于需要保证时延的交互性应用流量，可选中开启绿色通道功能来保证其带宽。

9.2.2 注意事项

- 一般应用场景下，可以把游戏报文、交互报文等对时延要求较高的应用流量通过绿色通道转发，把 BT 等对系统转发影响较大的 P2P 流量通过限制通道转发。其余流量会自动通过正常通道转发。
- 数据包匹配的优先级顺序如下：
  - 如果流量符合绿色通道的规则，则进入绿色通道进行处理。
  - 如果不符合绿色通道但符合限制通道的规则，则进入限制通道进行处理。
  - 如果绿色通道和限制通道的规则都不符合，则进入正常通道（IP 流量限制通道）发送，受到 IP 限速规则的限制。
- 配置的流量上限值是指所有进入限制通道的流量之和。
- 绿色通道识别流量时，如果数据包长度选择和端口选择同时启用，则符合其中一项即识别成功，并且数据包长度选择优先起作用。

9.2.3 配置 IP 限速

1. 配置需求

对指定接口或指定用户的流量进行带宽管理。

2. 配置准备

配置 IP 限速前，请先在[网络设置/外网配置]配置页面上的“WAN 配置”页签中设置线路的上下行带宽。如没有预先配置，也可以在“流量限制”配置项处点击“设置”链接，跳转到 WAN 配置页面配置当前线路的上下行带宽。

3. 配置步骤

(1) 单击导航树中[上网行为管理/带宽管理]菜单项，进入带宽管理配置页面。

(2) 在“IP 限速”页签下，点击<添加>按钮，弹出新建 IP 限速对话框。

(3) 在“应用接口”配置项处，选择接口，设备将基于该接口进行带宽管理。

(4) 在“用户范围”配置项处，选择地址组，设备将仅对该地址组内的成员进行带宽管理。

(5) 在“流量限制”配置项处，分别配置如下参数。

- 当前线路上行带宽：请根据运营商提供的实际上行带宽配置当前线路上行带宽。
- 当前线路下行带宽：请根据运营商提供的实际下行带宽配置当前线路下行带宽。
- 上传带宽：指定地址组内的用户上传方向的最大带宽值。
- 下载带宽：指定地址组内的用户下载方向的最大带宽值。
- 流量分配方式：设置流量的分配方式，包括如下类型：

- 共享式：分配的带宽为总带宽，由所有用户平均分配。
- 独占式：分配的带宽为单用户的带宽，由单个用户独享。

○ 在“弹性共享”配置项处，设置当用户实际流量带宽超过流量限制配置的带宽时，最大可以共享当前线路上下行带宽的百分比。流量分配选择共享式时，可根据需要配置该参数。。

○ 在“限制时段”配置项处，设置 IP 限速的生效时间段。

(6) 点击<确定>按钮，完成新建 IP 限速。

9.2.4 配置限制通道

1. 配置需求

对需要进行限速的应用流量（如占用大量带宽的 P2P 类应用）进行严格的带宽管理。

2. 注意事项

流量只有匹配“应用组”中配置的应用，限制通道功能才生效。

3. 配置步骤

(1) 单击“限制通道”页签，进入限制通道配置页面。

(2) 勾选“启用限制通道流速上限”选项，开启带宽管理的限制通道功能。

(3) 分别配置应用流量的上下行最大流速。

(4) 勾选“选择应用组”选项，选择已存在的匹配流量的应用分组，或点击<新增应用组>按钮，添加新的匹配流量的应用分组，点击“查看”链接，可以查看系统中已经创建的全部应用组。

(5) 点击<应用>按钮，完成限制通道的配置。

9.2.5 配置绿色通道

1. 注意事项

- 请勿将绿色通道带宽设置过大，以免对普通流量产生影响。
- 只有匹配“应用组”中配置的应用或符合“绿色通道数据包长度选择”中配置的流量数据包最大长度限制，绿色通道功能才生效。
- 一般应用场景下，可以把游戏报文、交互报文等对时延要求较高的应用流量通过绿色通道转发，把 BT 等对系统转发影响较大的 P2P 流量通过限制通道转发。其余流量会自动通过正常通道转发。
- 数据包匹配的优先级顺序如下：
  - 如果流量符合绿色通道的规则，则进入绿色通道进行处理。
  - 如果不符合绿色通道但符合限制通道的规则，则进入限制通道进行处理。
  - 如果绿色通道和限制通道的规则都不符合，则进入正常通道（IP 流量限制通道）发送，受到 IP 限速规则的限制。

2. 配置步骤

(1) 单击“绿色通道”页签，进入绿色通道配置页面。

(2) 勾选“启用绿色专用通道”选项，开启带宽管理的绿色通道功能，配置线路的上下行带宽。当带宽显示为未设置时，可通过点击“设置”链接进行设置。点击“设置”链接后，跳转到

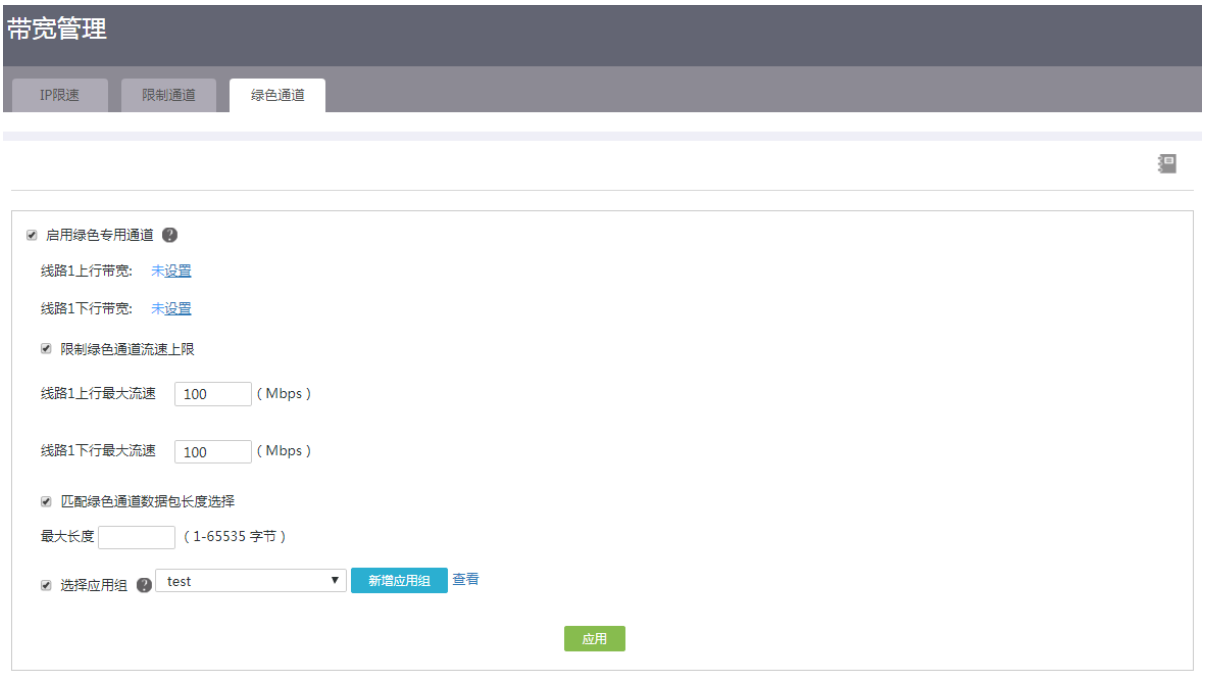
WAN 配置页面。在线路列表中，点击指定线路对应的操作列编辑图标，进入修改 WAN 配置页面，设置网络上行带宽、网络下行带宽后，点击<确定>按钮完成设置。

(3) 勾选“限制绿色通道流速上限”选项，分别配置各线路的上下行最大流速，为交互性应用流量提供带宽保障。

(4) 勾选“匹配绿色通道数据包长度选择”选项，配置流量数据包的最大长度。

(5) 勾选“选择应用组”选项，选择已存在的匹配流量的应用分组，或点击<新增应用组>按钮，添加新的匹配流量的应用分组，点击“查看”链接，可以查看系统中已经创建的全部应用组。

(6) 点击<应用>按钮，完成绿色通道的配置。



9.3 上网行为管理

9.3.1 简介

上网行为管理功能基于地址组、时间组以及应用等控制条件对用户的上网行为进行精细的管理。

9.3.2 配置应用控制

1. 配置步骤

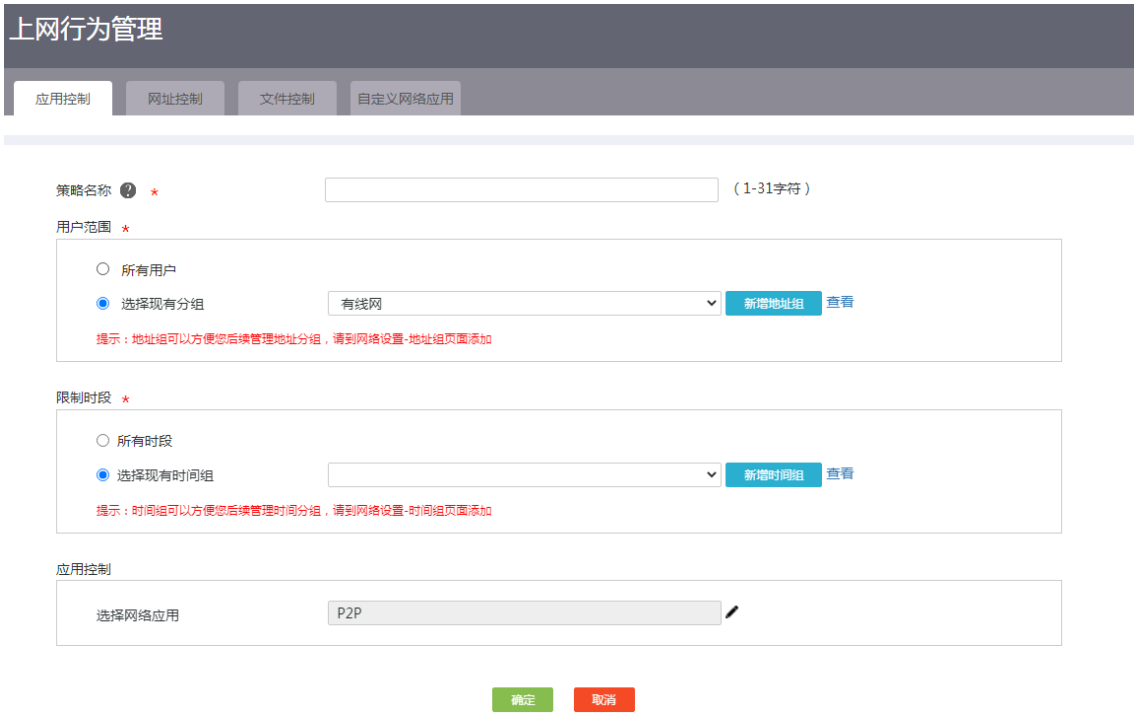
(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 单击“应用控制”页签，进入应用控制配置页面。

(3) 勾选“开启应用控制”选项，点击<确定>按钮，开启应用控制功能。

(4) 点击<添加>按钮，进入新建应用控制策略页面，配置如下参数。

- 在“策略名称”配置项处，输入应用控制策略的名称。
- 在“用户范围”配置项处，设置应用控制策略适用的地址组。
- 在“限制时段”配置项处，设置应用控制策略的时间组。



- 在“应用控制”配置项处，点击“选择网络应用”右侧的详情图标，选择网络应用，并配置对该应用的访问控制动作，包括如下：
  - 阻断：表示阻断用户对此应用的访问。
  - 不阻断不限速：表示不限制用户对此应用的访问。
  - 限速：表示对用户访问此应用进行限速，并可设置单个用户的最大上行带宽和最大下行带宽。

(5) 点击<确定>按钮，完成新建应用控制策略。

9.3.3 配置网址控制

1. 配置需求

当管理员仅允许用户访问指定网址或禁止用户访问指定网址时，可通过配置网址控制功能实现。

2. 注意事项

(1) 开启网址黑名单模式后，设备会禁止指定的用户在指定的时间段内访问自定义网址分类中指定的网址；对于不在网址分类中的网址，则可以正常访问。

假设管理员创建一个网址黑名单，其网址分类的名称为网址组 A，地址组的名称为用户组 A。用户的匹配规则如下：

- 如果用户 User1 属于用户组 A，则用户 User1 不允许访问网址组 A 中的网址；
- 如果用户 User2 不属于用户组 A，则用户 User2 允许访问任何网址。

(2) 开启网址白名单模式后，设备只允许指定的用户在指定的时间段内访问自定义网址分类中指定的网址；对于不在网址分类中的网址，则无法访问。

假设管理员创建如下两个网址白名单：

- 白名单 A：网址分类的名称为网址组 A，地址组的名称为用户组 A；
- 白名单 B：网址分类的名称为网址组 B，地址组的名称为用户组 B。

用户的匹配规则如下：

- 如果用户 User1 同时属于用户组 A 和用户组 B，则用户 User1 只允许访问网址组 A 和网址组 B 中的网址；
- 如果用户 User2 仅属于用户组 A，则用户 User2 只允许访问网址组 A 中的网址；
- 如果用户 User3 既不属于用户组 A 也不属于用户组 B，则用户 User3 不允许访问任何网址。

(3) 自定义网址支持导出功能，当使用 IE 浏览器进行导出时，如果出现无法启动 Excel 的错误提示，请参考如下步骤修改浏览器配置：

点击浏览器的<工具>按钮，选择“Internet 选项”，进入 Internet 选项窗口；选择“安全”页签，点击<自定义级别>按钮，找到“对为标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本”一项，选择“启用”。

(4) 配置网址关键字时，如需精确匹配网址，则关键字不加通配符*，例如 www.baidu.com；如需模糊匹配网址，则关键字添加通配符*，例如*.baidu.com、www.baidu*或*baidu*；如需配置所有网址，则关键字设置为*.*。

3. 配置步骤

(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 单击“网址控制”页签，进入网址控制配置页面。

(3) 根据需要勾选“关闭网址控制”、“网址黑名单模式”或“网址白名单模式”选项，勾选“网址黑名单模式”或“网址白名单模式”选项后，点击<确定>按钮，开启网址控制功能。

(4) 在“默认网址分类”下方的配置处，输入新建网址控制策略的网址分类名称。

(5) 在“所有用户”下方的配置处，选择网址控制策略适用的用户。

(6) 在“所有时间”下方的配置处，选择网址控制策略的生效时间。

(7) 点击右侧<+>按钮，新建一个空的网址分类成功。

(8) 为新建网址分类中添加网址：

- 点击新建网址分类对应的详情图标，弹出设置网址关键字对话框。在“网址关键字”输入框中，配置网址关键字，范围 1-63 个字符，可输入英文字母、数字，以及特殊字符（除/\'"<>;&`:和空格以外），英文字母不区分大小写。关键字不加通配符*时，网址控制策略将根据关键字做精确匹配，例如 www.baidu.com；关键字添加通配符*时，网址控制策略将根据关键字做模糊匹配，例如*.baidu.com、www.baidu*或*baidu*；关键字设置为*.*时，表示关键字

匹配所有网址。点击右侧的<+>按钮，逐条添加网址。点击<确定>按钮，完成添加网址关键字。

- 点击新建网址分类对应的导入图标，弹出导入自定义网址列表对话框。点击<选择文件>按钮，选择需导入的自定义网址列表，点击<是>按钮，完成向新建的网址分类中导入网址。

9.3.4 配置文件控制

1. 注意事项

文件控制功能仅能控制用户使用 HTTP 协议下载不同类型的文件。

2. 配置步骤

(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 单击“文件控制”页签，进入文件控制配置页面。

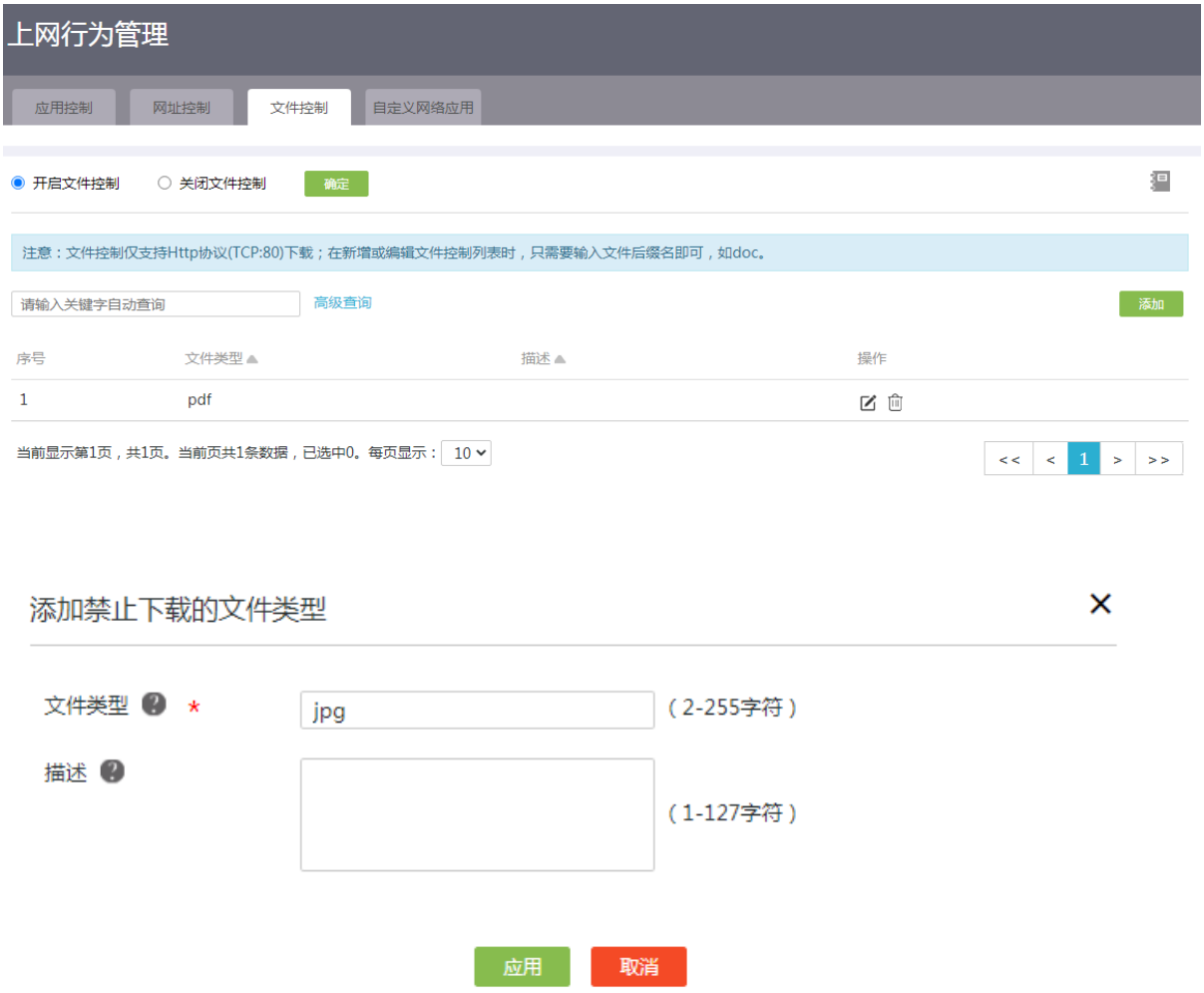
(3) 勾选“开启文件控制”选项，点击<确定>按钮，开启文件控制功能。

(4) 点击<添加>按钮，弹出添加禁止下载的文件类型对话框。

(5) 在“文件类型”配置项处，输入不允许下载文件的后缀名。

(6) 在“描述”配置项处，输入文件控制策略的描述信息。

(7) 点击<应用>按钮，完成添加文件控制策略。



9.3.5 配置自定义网络应用

1. 注意事项

- 管理员需要通过网络应用使用的报文特征来限制用户使用的网络应用时，可以添加自定义网络应用，并将其添加到应用控制策略中。
- 添加自定义网络应用后，需要在“应用控制”页签添加应用控制策略时，选择已添加的自定义网络应用，才能实现生效。
- 自定义网络应用被添加到应用控制策略后，自定义网络应用不允许删除。

2. 配置步骤

(1) 单击“自定义网络应用”页签，进入自定义网络应用配置页面。

(2) 点击<添加>按钮，弹出添加自定义网络应用对话框。

(3) 在“应用名称”配置项处，输入自定义网络应用的名称。

(4) 在“描述信息”配置项处，输入自定义网络应用的描述信息。

(5) 在“协议类型”配置项处，选择协议类型和报文方向。支持的协议类型包括：TCP、UDP、HTTP、HTTPS 和 SSL。当协议类型为 TCP、UDP 时，报文特征为必填项；当协议类型为

SSL 时，目的端口和 HOST 为必填项。报文方向包括：客户端、服务器和任意，选择“任意”时，表示设备接收的所有报文。

(6) 在“目的端口”配置项处，输入自定义网络应用的目的端口号和报文长度。

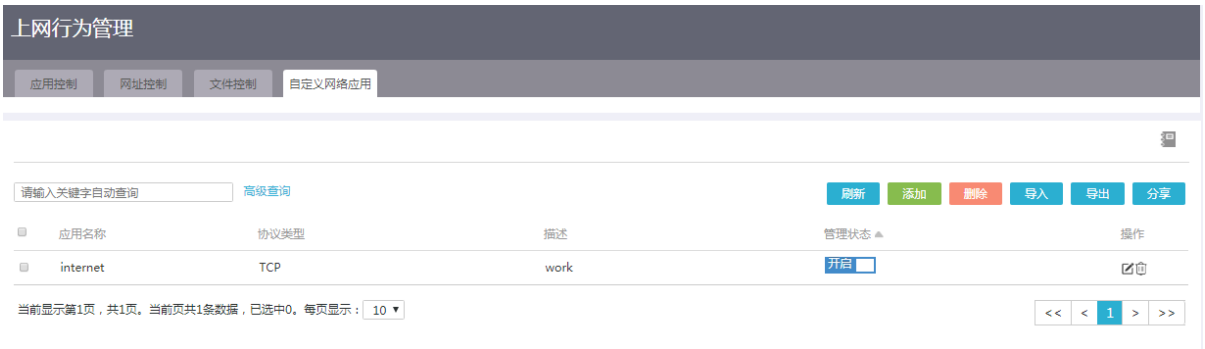
(7) 根据报文结构自定义网络应用的报文特征，主要包括：

- 报文特征：自定义 TCP、UDP 协议报文中的特征。
- URL：自定义 HTTP 协议报文中 URL 信息的特征。
- HOST：自定义 HTTP、HTTPS 和 SSL 协议报文中 HOST 信息的特征。
- UserAgent：自定义 HTTP 协议报文中 UserAgent 信息的特征。
- Referer：自定义 HTTP 协议报文中 Referer 信息的特征。
- Body：自定义 HTTP 协议报文中 Body 信息的特征。

(8) 设置完成后，点击<→→>按钮，将设置的报文特征添加到右侧方框中。

(9) 根据需要重复上述步骤，继续添加新的报文特征到右侧方框中。

(10) 完成报文特征的添加后，点击<确定>按钮，完成添加自定义网络应用。



9.4 审计日志

9.4.1 简介

审计日志功能用于对上网行为管理中的应用控制和网址控制的日志进行审计，并将日志发送到指定的服务器上。

9.4.2 应用审计日志

1. 配置需求

对上网行为管理中应用控制功能的日志进行审计。

2. 配置准备

在开启应用日志审计功能之前，需要先在上网行为管理中开启应用控制功能。

3. 配置步骤

(1) 单击导航树中[上网行为管理/审计日志]菜单项，进入应用审计日志配置页面。

(2) 勾选“开启审计日志”选项，开启应用的日志审计功能。

(3) 点击<清除日志>按钮，在确认提示框中，点击<是>按钮，清除所有的应用审计日志。

(4) 点击<导出 Excel>按钮，可将所有应用审计日志保存到 Excel 文件中。

9.4.3 网址过滤日志

1. 配置需求

对上网行为管理中网址控制功能的日志进行审计。

2. 配置准备

在开启网址过滤日志功能之前，需要先在上网行为管理中开启网址控制功能。

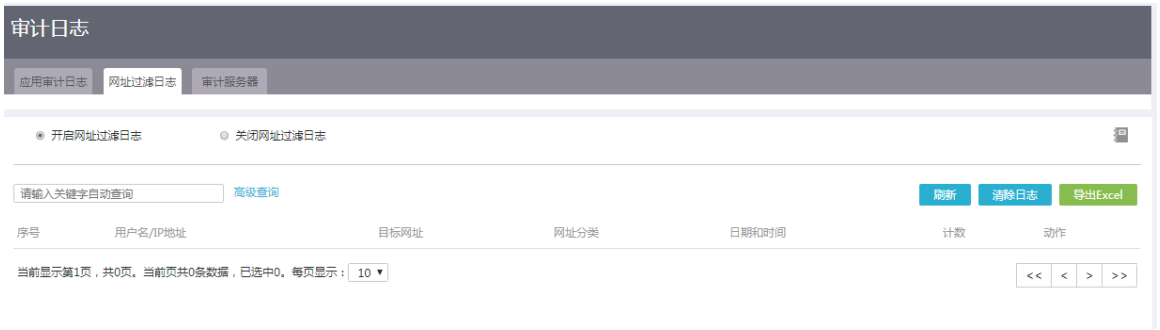
3. 配置步骤

(1) 单击“网址过滤日志”页签，进入网址过滤日志配置页面。

(2) 勾选“开启网址过滤日志”选项，开启网址过滤的日志审计功能。

(3) 点击<清除日志>按钮，在确认提示框中，点击<是>按钮，清除所有的网址过滤日志。

(4) 点击<导出 Excel>按钮，可将所有网址过滤日志保存到 Excel 文件中。



9.4.4 审计服务器

1. 配置需求

将审计日志发送到指定的服务器。

2. 配置准备

审计服务器的 IP 地址需要与当前路由器的 IP 地址互通。

3. 配置步骤

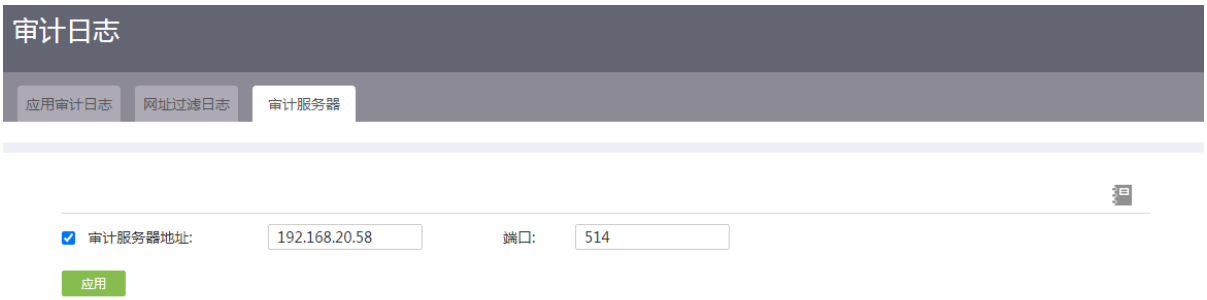
(1) 单击“审计服务器”页签，进入审计服务器页面。

(2) 勾选“审计服务器地址”选项，开启发送审计日志到服务器的功能。

(3) 在“审计服务器地址”配置项处，输入接收审计日志的服务器的 IP 地址。

(4) 在“端口”配置项处，输入接收审计日志的服务器的端口号。

(5) 点击<应用>按钮，完成审计服务器的配置。



10 网络安全

10.1 置任务导引

10.1.1 配置不同 VLAN 之间不能互访

当网络管理员需要禁止不同部门（VLAN）之间互访时，可以通过配置防火墙功能来实现。配置步骤如下：

步骤	配置内容	详情
1	添加VLAN（必选）	创建各个部门所使用的VLAN，具体配置方法请见参见配置VLAN。
2	添加防火墙策略（必选）	开启防火墙，并根据实际情况添加防火墙策略，使得各个部门VLAN之间不能互访，具体配置方法参见防火墙。

10.2 防火墙

10.2.1 简介

防火墙功能是通过一系列的安全规则匹配网络中的报文，并执行相应的动作，从而达到阻断非法报文传输、正常转发合法报文的目的，为用户的网络提供一道安全屏障。

10.2.2 注意事项

- 当报文匹配到一个防火墙安全规则后，则不会继续向下匹配，所以请合理安排安全规则的优先级，避免报文匹配错误的规则而导致执行相反动作。
- 当缺省过滤规则设置为允许时，用户不需要配置任何安全规则，接入当前设备的所有终端都可以相互访问，且可以访问外网。
- 当缺省过滤规则设置为允许时，如果用户需要限制指定终端的访问特定外网的权限，可根据需求配置指定的 VLAN 接口与 WAN 接口之间的安全规则；如果用户需要限制指定终端访问其它 VLAN 下终端的权限，可根据需求配置指定的 VLAN 接口到 VLAN 接口的安全规则。
- 当缺省过滤规则设置为禁止时，如果用户未配置任何安全规则，所有终端不能访问外网，不同 VLAN 下的终端不能相互访问。
- 当缺省过滤规则设置为禁止时，如果用户需要允许指定终端可以访问特定外网，则需要根据需求配置指定 VLAN 接口与 WAN 接口之间的安全规则，且必须配置双向规则，即出站方向和入站方向各一条。如果用户需要让指定终端能够访问其它 VLAN 下的终端，则需要配置指定本端 VLAN 接口与对端 VLAN 接口之间的安全规则，且必须配置双向规则。

10.2.3 配置准备

- 请提前完成外网配置页面的相关配置，才可创建防火墙安全规则。

- 若需指定防火墙安全规则的生效时间和生效地址，请提前在时间组页面和地址组页面创建相应的时间组。

10.2.4 配置步骤

(1) 单击导航树中[网络安全/防火墙]菜单项，进入防火墙配置页面。

(2) 勾选“开启防火墙”选项，进入防火墙配置页面。

(3) 在“缺省过滤规则”配置项处，选择对未匹配任何安全规则报文的处理方式。若选择“允许”，则允许该报文通过防火墙；若选择“禁止”，则禁止该报文通过防火墙。点击“应用”按钮完成配置。

(4) 点击<添加>按钮，弹出创建安全规则对话框。

(5) 在“接口”配置项处，选择应用的接口，该规则将对指定接口接收到的报文进行匹配。

(6) 在“方向”配置项处，显示安全规则的方向，包括入站方向和出站方向。当“接口”配置项处选择为 WAN 接口时，安全规则的方向为入站方向，即控制从公网侧进入设备的流量；当“接口”配置项处选择为 VLAN 接口时，安全规则的方向为出站方向，即控制从内网侧进入设备的流量。

(7) 在“协议类型”配置项处，选择该规则所匹配报文的协议类型。若需匹配某传输层协议的报文，则选择“TCP”或“UDP”；若需匹配 Ping、Tracert 等 ICMP 协议报文，则选择“ICMP”；若需匹配所有协议报文，则选择“所有协议”。

(8) 在“源地址分组”配置项处，选择该规则所匹配的源地址分组。如需新增地址分组，可通过点击右侧“新增地址组”按钮创建新的地址组。

(9) 在“目的地址分组”配置项处，选择该规则所匹配的目的地址分组。如需新增地址分组，可通过点击右侧“新增地址组”按钮创建新的地址组。

(10) 在“目的端口范围”配置项处，配置该规则所匹配报文的目的端口号范围。

(11) 在“规则生效时间”配置项处，选择该规则生效时间对应的时间组。

(12) 在“动作”配置项处，选择该规则所匹配报文的执行动作。

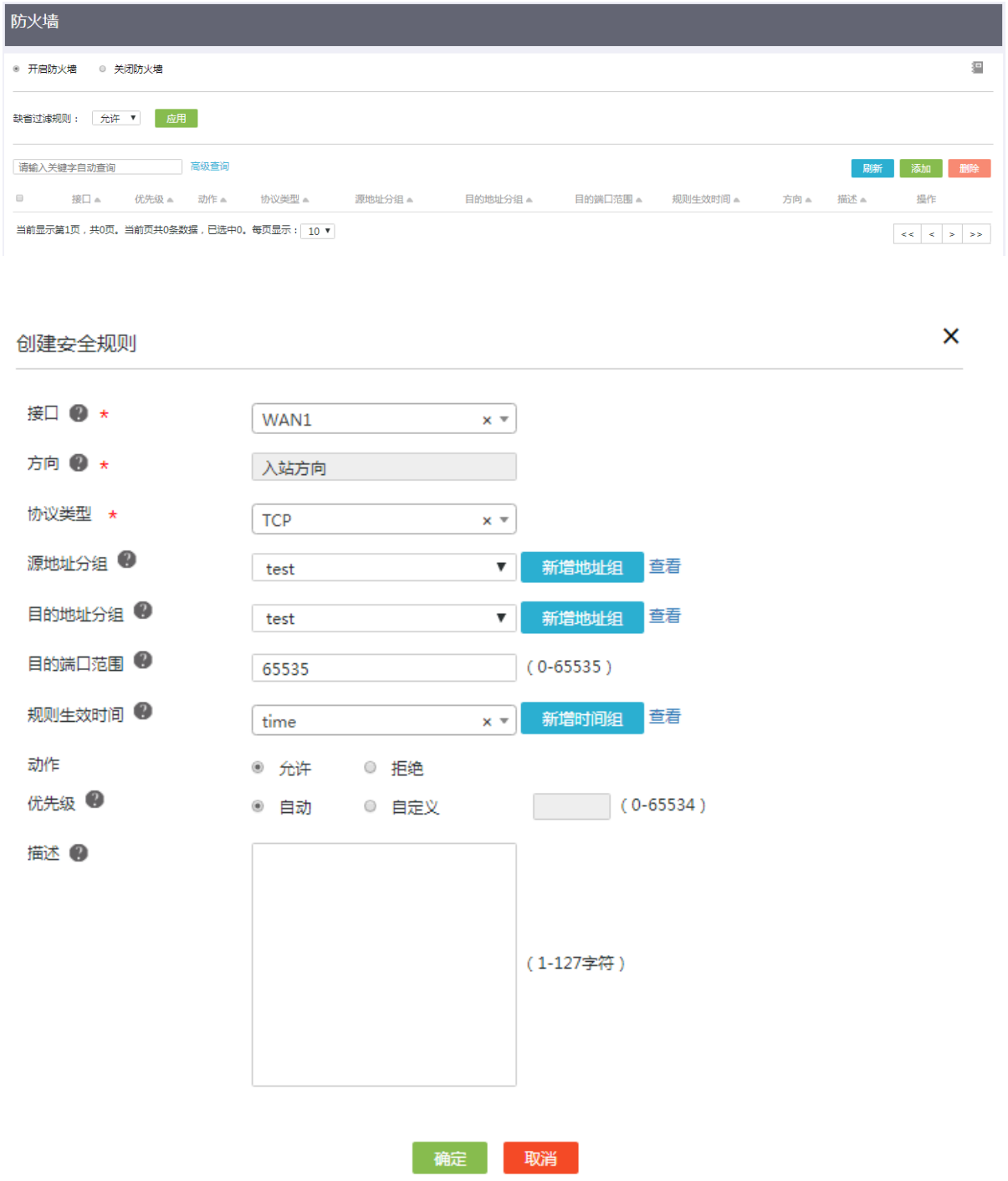
- 允许：允许报文通过防火墙。
- 拒绝：禁止报文通过防火墙。

(13) 在“优先级”配置项处，选择该规则的优先级类型。

- 自动：系统自动为该规则分配优先级，即根据规则的配置顺序以 5 为步长进行依次分配。
- 自定义：用户自定义规则的优先级，数值越小则优先级越高。

(14) 在“描述”配置项处，配置该安全规则的描述信息。

(15) 点击<确定>按钮，完成创建安全规则。



10.3 连接限制

10.3.1 简介

连接限制功能是一种安全机制，通过限制每个 IP 地址主动发起连接的个数，达到合理分配设备处理资源、防范恶意连接的效果。

如果设备发现来自某 IP 地址的 TCP 或 UDP 连接数目超过指定的数目，将禁止该连接建立。直到该连接数低于限制数时，其才被允许新建连接。

设备支持配置如下两种连接限制：

- 网络连接限制：在指定 IP 地址范围内，配置每个 IP 地址发起连接的个数限制。此方式用于对设备上的所有接口收到的连接进行控制。
- VLAN 网络连接限制：在指定 VLAN 接口上，配置每个 IP 地址发起连接的个数限制。此方式用于对指定 VLAN 接口收到的连接进行控制。

10.3.2 注意事项

- 每条网络连接数限制规则，如果是 IP 地址范围，表示该地址段内的每个 IP 最多建立的网络连接数都将限制到设定的上限值。如果起始地址和结束地址相同，表示仅限制该 IP 的网络连接数。
- 限制规则表中可以加入多条网络连接数限制规则，配置规则时允许某几条中的 IP 地址重叠，但以先加入的规则优先级为高。也就是对于相同的 IP 地址，后加入的网络连接数限制设置不会覆盖先前的设置，仍以先前配置的连接数限制为准。
- 允许在限制规则表中对先前配置的规则进行删除、修改等操作。但修改不能改变规则的优先级，生效规则仍以规则要点 2 的约定为准。
- 网络连接限速仅限制内网 IP 向因特网发起的网络连接；下列情形不在限制范围内：向设备本身和内网其它 IP 发起的连接，以及由因特网向内网 IP 发起的连接。
- 总连接数=TCP 连接数+UDP 连接数+其他连接数，其他连接指除 TCP 和 UDP 连接之外的连接，如 ICMP 等。某 IP 可以建立新连接的条件是：此 IP 已经建立的连接数未达到设置的上限值。比如某 IP 需要建立一条 TCP 连接，则必须满足此 IP 已经建立的总连接数未达到总连接数上限，TCP 连接数未达到 TCP 连接数上限，建立 UDP 连接和其他连接的条件跟 TCP 相同。
- TCP 连接数设为 0 和留空的区别是：设置为 0 表示不允许建立 TCP 连接，留空表示不对 TCP 连接数进行单独限制，但仍需满足总连接数限制条件。UDP 连接数情况类似。
- 每条 VLAN 网络连接限数规则，表示指定 VLAN 内最多建立的网络连接数都将被限制到设定的上限值。注意，这里设置的连接数上限指的是该 VLAN 内所有 IP 的连接数之和的上限，而非每 IP 各自的连接数上限
- 总连接数=TCP 连接数+UDP 连接数+其他连接数，其他连接指除 TCP 和 UDP 连接之外的连接，如 ICMP 等。某 VLAN 可以建立新连接的条件是：此 VLAN 内 IP 已经建立的连接数未达到设置的上限值。比如某 VLAN 内某个 IP 需要建立一条 TCP 连接，则必须满足此 VLAN 已经建立的总连接数未达到总连接数上限，TCP 连接数未达到 TCP 连接数上限，建立 UDP 连接的条件跟建立 TCP 连接类似。
- VLAN 网络连接限数仅限制 VLAN 内各 IP 向因特网发起的网络连接；下列情形不在限制范围内：向设备本身、同一个 VLAN 内不同 IP 之间发起的连接、不同 VLAN 内的 IP 相互发起的连接，以及由因特网向 VLAN 内的 IP 发起的连接。
- TCP 连接数设为 0 和留空的区别是：设置为 0 表示不允许建立 TCP 连接，留空表示不对 TCP 连接数进行单独限制，但仍需满足总连接数限制条件。UDP 连接数情况类似。

10.3.3 配置网络连接限制数

(1) 单击导航树中[网络安全/连接限制]菜单项，进入连接限制配置页面。

(2) 单击“网络连接限制数”页签，进入网络连接限制数配置页面。

(3) 勾选“开启网络连接限制数”选项，进入网络连接限制数配置页面。

(4) 点击<添加>按钮，弹出新建网络连接限制数规则对话框。

(5) 在“连接限制地址分组”配置项处，选择该规则所匹配的连接限制地址分组。如需新建地址分组，可通过点击右侧“新增地址组”按钮创建新的地址组。

(6) 在“每 IP 总连接数上限”配置项处，输入每个 IP 地址所允许发起连接的总个数上限。

相同源 IP，源端口、目的 IP、目的端口或报文协议不完全相同的连接均属于不同的连接。

(7) 在“每 IP TCP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 TCP 连接的个数上限。您可以在上面设置的总连接限制数下，对 TCP 连接数进行单独限制。

(8) 在“每 IP UDP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 UDP 连接的个数上限。您可以在上面设置的总连接限制数下，对 UDP 连接数进行单独限制。

(9) 在“描述”配置项处，输入规则描述信息。

(10) 点击<应用>按钮，完成配置。

10.3.4 配置 VLAN 网络连接限制数

(1) 单击导航树中[网络安全/连接限制]菜单项，进入连接限制配置页面。

(2) 单击“VLAN 网络连接限制数”页签，进入 VLAN 网络连接限制数配置页面。

(3) 勾选“开启 VLAN 网络连接限制数”选项，进入 VLAN 网络连接限制数配置页面。

(4) 点击<添加>按钮，弹出新建 VLAN 网络连接限制数规则对话框。

(5) 在“VLAN 接口”下拉菜单处，选择应用此规则的 VLAN 接口。

(6) 选择“启动连接限制功能”选项，启动连接限制功能。

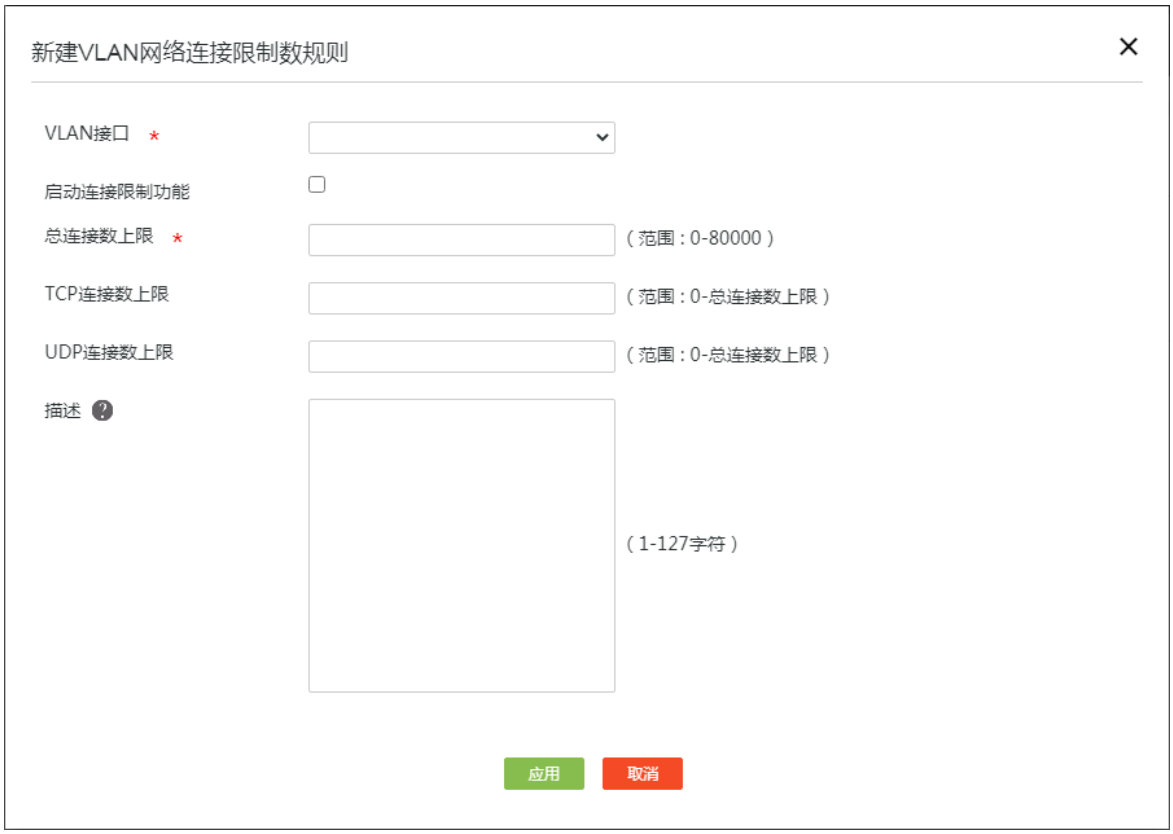
(7) 在“总连接数上限”配置项处，输入 VLAN 接口所允许发起连接的总个数上限。。
相同源 IP，源端口、目的 IP、目的端口或报文协议不完全相同的连接均属于不同的连接。

(8) 在“TCP 连接数上限”配置项处，输入 VLAN 接口所允许发起的 TCP 连接的个数上限。您可以在上面设置的总连接限制数下，对 TCP 连接数进行单独限制。

(9) 在“UDP 连接数上限”配置项处，输入 VLAN 接口所允许发起的 UDP 连接的个数上限。您可以在上面设置的总连接限制数下，对 UDP 连接数进行单独限制。

(10) 在“描述”配置项处，输入规则描述信息。

(11) 点击<应用>按钮，完成配置。



10.4 MAC地址过滤

10.4.1 简介

如果您希望对某些设备发送过来的报文进行限制（允许或禁止其通过），则可以在 VLAN 接口上配置 MAC 地址过滤功能，在开启 MAC 地址过滤功能后，本功能将根据 MAC 黑白名单对接收报文的源 MAC 地址进行过滤。

过滤方式有如下两种：

- 白名单：仅允许在白名单内的源 MAC 地址访问外网，其余禁止访问。
- 黑名单：仅禁止在黑名单内的源 MAC 地址访问外网，其余允许访问。

10.4.2 MAC 过滤设置

1. 注意事项

- 如果需要在管理员终端连接的接口上开启 MAC 地址过滤功能，请先确保管理员的终端 MAC 地址已添加到白名单中或未添加到黑名单。
- MAC 地址中的英文字符不区分大小写。

2. 配置步骤

(1) 单击导航树中[网络安全/MAC 地址过滤]菜单项，进入 MAC 地址过滤设置页面。

(2) 单击“MAC 过滤设置”页签，进入 MAC 过滤设置页面。

(3) 勾选“开启 MAC 地址过滤”选项，开启 MAC 地址过滤功能。

(4) 在指定接口的“过滤方式”列中选择“白名单”或“黑名单”选项，并在“开启和关闭”列中勾选“开启”选项。

(5) 点击<应用>按钮，开启 MAC 地址过滤。

10.4.3 MAC 黑白名单管理

1. 注意事项

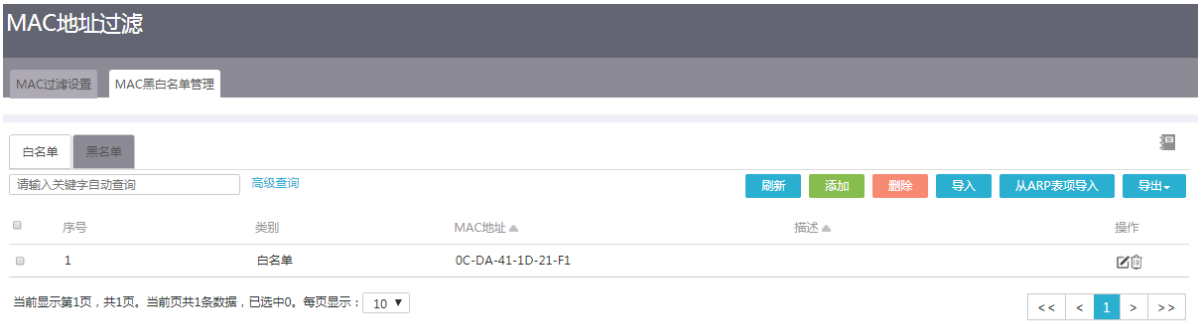
单个添加黑白名单的方法相同，下面以白名单为例介绍配置步骤。

2. 配置步骤

(1) 单击导航树中[网络安全/MAC 地址过滤]菜单项，进入 MAC 地址过滤设置页面。

(2) 单击“MAC 黑白名单管理”页签，进入 MAC 黑白名单管理页面。

(3) 单击“白名单”页签，进入白名单设置页面。



(4) 如果需要添加单个 MAC 地址，请执行以下步骤：

a. 点击<添加>按钮，弹出添加源 MAC 地址对话框。

b. 在“MAC 地址”配置项处，输入待过滤的源 MAC 地址。

c. 在“描述”配置项处，输入待过滤源 MAC 地址的描述信息。

d. 点击<确定>按钮，完成对白名单添加单个 MAC 地址的操作。

(5) 如果需要批量添加 MAC 地址，请执行以下步骤：

a. 点击<导出>按钮，选择“导出模板”菜单项。

b. 打开下载好的模板，添加待过滤的源 MAC 地址并在本地保存。

c. 点击<导入>按钮，弹出导入源 MAC 地址对话框。

d. 点击<浏览>按钮，弹出选择要加载的文件对话框。

e. 选中已编辑好的模板，点击<打开>按钮。

f. 点击<确定>按钮，完成对白名单批量添加 MAC 地址的操作。

(6) 如果需要从 ARP 表项导入 MAC 地址，请执行以下步骤：

a. 点击<从 ARP 表项导入>按钮，弹出导入 ARP MAC 表对话框。

b. 勾选需要导入的 MAC 地址。

c. 点击<导入>按钮，弹出确认提示对话框。

d. 点击<是>按钮，完成对白名单从 ARP 表项导入 MAC 地址的操作。

10.5 ARP安全

10.5.1 简介

ARP 协议本身存在缺陷，攻击者可以轻易地利用 ARP 协议的缺陷对其进行攻击。ARP 攻击防御技术提供了多种 ARP 攻击防御技术对局域网中的 ARP 攻击和 ARP 病毒进行防范、检测和解决。

ARP 安全功能包括：

- ARP 学习管理：本功能支持开启和关闭接口的动态 ARP 表项学习功能，当执行关闭接口的动态 ARP 表项学习功能后，该接口无法再学习新的动态 ARP 表项，提高了安全性。当设备的某个接口已经学到了该接口下所有合法用户的 ARP 表项时，建议关闭动态 ARP 表项学习功能。
- 动态 ARP 管理：包括动态 ARP 表项管理功能和 ARP 扫描、固化功能。ARP 扫描、固化功能即对局域网内的用户进行自动扫描，并将生成的动态 ARP 表项固化为静态 ARP 表项。建议环境稳定的小型网络（如网吧）中配置本功能。先配置 ARP 扫描、固化功能，再关闭动态 ARP 表项学习功能，可以防止设备学习到错误的 ARP 表项。
- 静态 ARP 管理：包括动态 ARP 表项管理、刷新、添加和导入导出功能。其中，刷新功能是指刷新静态 ARP 表项列表；添加功能是指手动新增静态 ARP 表项；导入功能是指从文件中批量获取静态 ARP 表项；导出功能是指将现有的静态 ARP 表项导出到本地文件中。

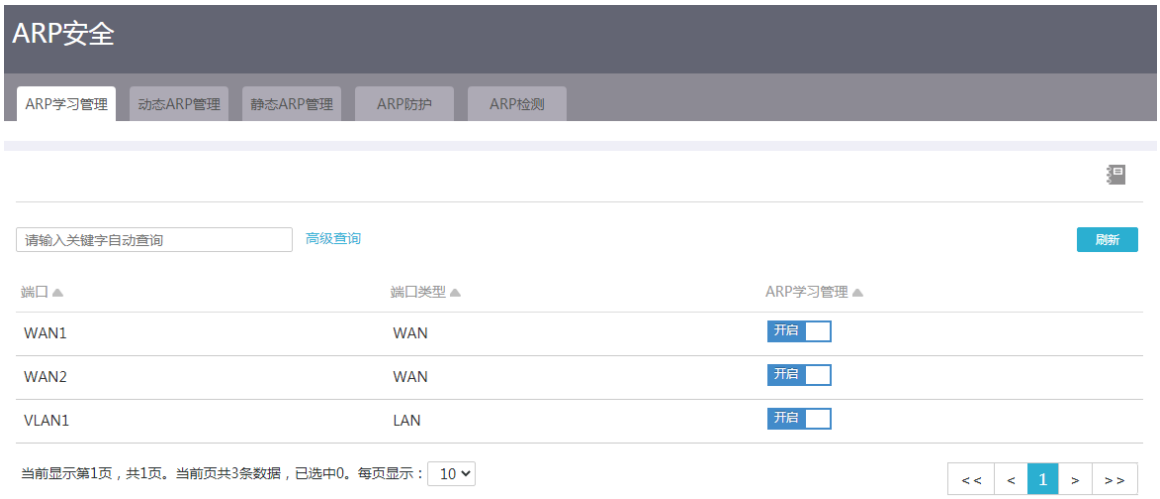
- ARP 防护：包括 ARP 报文合法性检查和免费 ARP 功能。ARP 报文合法性检查是通过设置规则验证 ARP 报文的合法性。免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机 IP 地址，报文源 MAC 地址是本机 MAC 地址，报文的目的 MAC 地址是广播地址。设备通过对外发送免费 ARP 报文来实现以下功能：
  - 确定其它设备的 IP 地址是否与本机的 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。
  - 设备改变了硬件地址，通过发送免费 ARP 报文通知其它设备更新 ARP 表项。
- ARP 检测：探测到指定接口下所有在线设备，同时还能检查这些设备的信息是否和已存在 ARP 表项冲突。根据搜索结果，可以进行 ARP 绑定操作。

10.5.2 ARP 学习管理

(1) 单击导航树中[网络安全/ARP 安全]菜单项，进入 ARP 安全配置页面。

(2) 单击“ARP 学习管理”页签，进入 ARP 学习管理配置页面。

(3) 在指定接口的“ARP 学习管理”列，设置是否允许接口学习动态 ARP 表项：
  - 点击按钮，将其设置为开启，则该接口允许学习动态 ARP 表项；
  - 点击按钮，将其设置为关闭，则该接口不允许学习动态 ARP 表项。



10.5.3 动态 ARP 管理

(1) 单击导航树中[网络安全/ARP 安全]菜单项，进入 ARP 安全配置页面。

(2) 单击“动态 ARP 管理”页签，进入动态 ARP 表项管理配置页面。

(3) 可对已有的动态 ARP 表项执行以下管理操作：

- 点击<刷新>按钮，则可以刷新当前动态 ARP 表项的显示信息。
- 选择指定的动态 ARP 表项，点击<删除>按钮，再点击<确定>按钮后，可以删除对应的动态 ARP 表项。
- 点击<扫描>按钮，弹出扫描配置对话框。

a. 在“接口”配置项处，选择需要执行 ARP 扫描操作的接口。

b. 在“开始 IP 地址”和“结束 IP 地址”配置项处，设置 ARP 扫描操作的起止 IP 地址。此处指定起止 IP 地址需要和接口的 IP 地址处于同一网段。

c. 点击<确定>按钮，完成扫描地址段的添加。

d. 选择指定的动态 ARP 表项，再点击<固化>按钮，则可以将这些动态 ARP 表项固化为静态 ARP 表项。

10.5.4 静态 ARP 管理

(1) 单击导航树中[网络安全/ARP 安全]菜单项，进入 ARP 安全配置页面。

(2) 单击“静态 ARP 管理”页签，进入静态 ARP 管理页面。

(3) 如果需要添加单个静态 ARP 表项，请执行以下步骤：

(4) 点击<添加>按钮，弹出添加 ARP 表项对话框。

a. 在“IP 地址”配置项处，输入静态 ARP 表项的 IP 地址。

b. 在“MAC 地址”配置项处，输入静态 ARP 表项的 MAC 地址。

c. 在“描述”配置项处，输入 ARP 表项的描述信息。

d. 点击<确定>按钮，完成静态 ARP 表项的添加。

(5) 如果需要批量添加静态 ARP 表项，请执行以下步骤：

a. 点击<导出>按钮，下载导出模板。

b. 打开下载好的模板，添加静态 ARP 表项并在本地保存。

c. 点击<导入>按钮，弹出导入 ARP 表项对话框。

d. 点击<选择文件>按钮，选择已编辑好的模板。

e. 点击<确定>按钮，完成静态 ARP 表项的批量添加。

10.5.5 ARP 防护

1. 注意事项

- 设备发送免费 ARP 可以防止 LAN 或 WAN 侧的主机受到 ARP 攻击和欺骗。设置免费 ARP 发送时间间隔越小，主机防止 ARP 攻击能力越强，但是占用网络资源越大，请合理设置免费 ARP 报文发送时间间隔。
- 由于有些设备（如交换机）可能会对 ARP 报文进行限制，过多的 ARP 报文可能会被判定为攻击，请确定是否开启主动发送免费 ARP 的功能，并进行合理的参数设置。
- 路由器支持定时发送免费 ARP 功能，这样可以及时通知其它设备更新 ARP 表项或者 MAC 地址表项，以防止仿冒网关的 ARP 攻击、防止主机 ARP 表项老化等。

2. 配置步骤

(1) 单击导航树中[网络安全/ARP 安全]菜单项，进入 ARP 安全配置页面。

(2) 单击“ARP 防护”页签，进入 ARP 防护配置页面。

(3) 在“ARP 报文合法性检查”区段，可进行如下设置：

- 勾选“丢弃发送端 MAC 地址不合法的 ARP 报文（LAN 口默认丢弃不合法的 ARP 报文）”选项，当设备接收的 ARP 报文中的源 MAC 地址为全零、组播、广播 MAC 地址时，则不学习该 ARP 报文，直接将该报文丢弃。
- 勾选“丢弃报文头中源 MAC 地址和报文中发送端 MAC 地址不一致的 ARP 报文”选项，当设备接收的 ARP 报文中的源 MAC 地址与该报文的二层源 MAC 地址不一致时，则不学习该 ARP 报文，直接将该报文丢弃。
- 勾选“ARP 报文学习抑制”选项，当设备发出一个 ARP 请求报文，收到了多个不同的 ARP 响应报文时，设备仅学习最先收到的 ARP 响应报文。

(4) 在“免费 ARP”区段，可进行如下设置：

- 勾选“检测到 ARP 欺骗时，发送免费 ARP 报文”选项，当设备检测到 ARP 欺骗时(比如源 IP 地址为设备接口 IP 地址但源 MAC 地址不是设备接口 MAC 地址的 ARP 报文)，则会主动发送免费 ARP 报文。
- 勾选“LAN 内主动发送免费 ARP 报文”选项，并在“发送间隔”配置项处，输入免费 ARP 报文的发送间隔。
- 勾选“WAN 口主动发送免费 ARP 报文”选项，并在“发送间隔”配置项处，输入免费 ARP 报文的发送间隔。

(5) 点击<应用>按钮，完成配置。

10.5.6 ARP 检测

(1) 单击导航树中[网络安全/ARP 安全]菜单项，进入 ARP 安全配置页面。

(2) 单击“ARP 检测”页签，进入 ARP 检测配置页面。

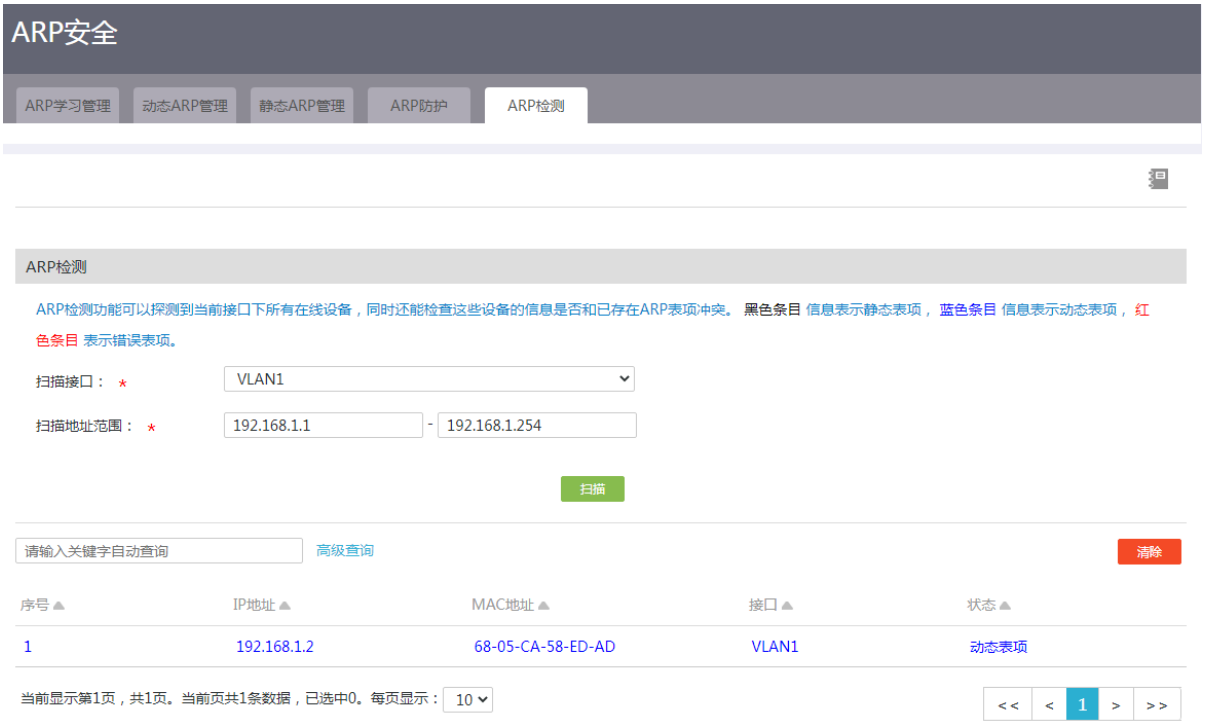
(3) 在“扫描接口”配置项处，选择扫描的接口。

(4) 在“扫描地址范围”配置项处，选择扫描的起始 IP 地址和结束 IP 地址。

(5) 点击<扫描>按钮，开始进行扫描检测。检测结果将会在列表中显示，其中黑色条目表示表项绑定，蓝色条目表示表项未绑定，红色条目表示错误表项。检测结果中 ARP 表项的状态分为：

- 静态表项：表示该条表项为手动配置的或自动绑定的 ARP 表项。
- 动态表项：表示该条表项为动态学习到的并且没有被自动绑定的 ARP 表项。
- 错误表项：表示存在 ARP 冲突表项。

(6) 点击<清除>按钮，可以清除当前的检测结果。



10.6 DDOS攻击防御

10.6.1 简介

DDoS 攻击是一类广泛存在于互联网中的攻击，能造成比传统 DoS 攻击（拒绝服务攻击）更大的危害，能让设备对来自外网和内网的常见攻击类型进行防护，丢弃攻击报文。同时，设备可以对相应的攻击事件以日志形式记录下来。

- 攻击防御：本功能能够让设备和网络免受如下 DDOS 攻击的困扰：
  - 单包攻击：攻击者利用畸形报文发起攻击，旨在瘫痪目标系统。例如 Land 攻击报文是源 IP 和目的 IP 均为攻击目标 IP 的 TCP 报文，此攻击将耗尽目标服务器的连接资源，使其无法处理正常业务。
  - 异常流攻击：攻击者向目标系统发送大量伪造请求，导致目标系统疲于应对无用信息，从而无法为合法用户提供正常服务。
  - 扫描攻击：攻击者对主机地址和端口进行扫描，探测目标网络拓扑以及开放的服务端口，为进一步侵入目标系统做准备。
- 攻击防御统计：本功能可以分别显示单包攻击防御和异常流量攻击防御的统计信息，可以导出 Excel 保存。
- 报文源认证：本功能是指设备对收到的内网报文的源 IP/MAC 进行认证，确认对端是否是一个合法的主机，以防止内网中可能存在的非法报文攻击，避免这些非法报文对设备资源和网络资源的消耗，提高整体网络的稳定性。
- 异常流量防护：本功能是指对内网异常大流量的主机进行控制，以防止该异常主机过度占用带宽和消耗系统性能。其中有三种防护等级，您可以根据你的实际网络状况选择较合适的级

别进行防护。为了防止非法伪装报文流量被统计到合法主机流量中，建议尽量开启报文源认证页面的相关认证功能。

10.6.2 攻击防御

1. 注意事项

- 开启日志记录功能将会降低部分系统抗攻击能力，建议不必要的情况下不用开启该功能。
- DDOS 攻击防御功能无法从 WAN 侧防御 L2TP 隧道封装的流量。
- 对于 PPPoE 连接的 WAN 口，无法配置单包攻击防御中的“Smurf 攻击防御”。

2. 配置步骤

(1) 单击导航树中[网络安全/DDOS 攻击防御]菜单项，进入 DDOS 攻击防御配置页面。

(2) 单击“攻击防御”页签，进入攻击防御配置页面。

(3) 勾选“开启 DDOS 攻击防御”选项，开启 DDOS 攻击防御功能。

(4) 点击<添加>按钮，弹出新建攻击防御对话框。

(5) 在“应用接口”配置项处，选择应用该 DDOS 攻击防御策略的接口。

(6) 在“单包攻击防御”配置项处，选择需要开启防御的单包攻击类型。建议开启全部单包攻击防御。

- Fraggle 攻击防御：启用该项后，设备可以有效防止 Fraggle 攻击。该攻击表现为攻击者向子网广播地址发送源地址为受害网络或者受害主机的 UDP 报文。子网内的每一个主机都会向受害网络或者主机发送响应报文，从而导致网络阻塞或者主机崩溃。
- Land 攻击防御：启用该项后，设备可以有效防止 Land 攻击。该攻击表现为攻击者向目标发送带有 SYN 标志的 TCP 报文，并且这些报文的源地址和目的地址都设为被攻击目标的 IP 地址，当被攻击目标机收到这样的报文后，开始重复的进行内部应答风暴，消耗大量的 CPU 资源。
- WinNuke 攻击防御：启用该项后，设备可以有效防止 WinNuke 攻击。该攻击表现为攻击者利用 NetBIOS 协议中 OOB（Out of Band）漏洞对目标进行攻击，可造成部分主机死机或蓝屏。

- TCP flag 攻击防御：启用该项后，设备可以有效防止 TCP flag 攻击。该攻击表现为攻击者发送带有非常规 TCP 标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。
- ICMP 不可达报文攻击防御：启用该项后，设备可以有效防止 ICMP 不可达报文攻击。该攻击表现为攻击者向目标发送 ICMP 不可达报文，达到切断目标主机网络连接的目的。
- ICMP 重定向报文攻击防御：启用该项后，设备可以有效防止 ICMP 重定向报文攻击。该攻击表现为攻击者向目标发送 ICMP 重定向报文，更改目标的路由表，干扰目标正常的 IP 报文转发。
- Smurf 攻击防御：启用该项后，设备可以有效防止 Smurf 攻击。该攻击与 Fraggle 攻击类似，表现为攻击者向一个网段广播一个 ICMP 回显请求（ICMP ECHO REQUEST）报文，而源地址为被攻击主机，当网段中的所有主机收到回显请求后，都会向被攻击主机响应 ICMP ECHO REPLY 报文，造成攻击目标网络阻塞或者系统崩溃。
- 带源路由选项的 IP 攻击防御：启用该项后，设备可以有效防止带源路由选项的 IP 攻击。该攻击表现为攻击者向目标发送带源路由选项的 IP 报文，达到探测网络结构的目的。
- 带路由记录选项的 IP 攻击防御：启用该项后，设备可以有效防止带路由记录选项的 IP 攻击。该攻击表现为攻击者向目标发送带路由记录选项的 IP 报文，达到探测网络结构的目的。
- 超大 ICMP 攻击防御：启用该项后，设备可以有效防止超大 ICMP 攻击。该攻击表现为攻击者向目标发送超大 ICMP 报文，使目标主机崩溃。
- 防止 IP Spoofing：启用该项后，设备可以有效防止 IP Spoofing 攻击。该攻击表现为攻击者使用相同的 IP 地址假冒网络上的合法主机，并访问关键信息。通常会伪装成 LAN 内的 IP。
- 防止 TearDrop：启用该项后，设备可以有效防止 TearDrop 攻击，缺省启用该项，无法取消。该攻击表现为攻击者向目标发送相互重叠的分片报文，目标主机处理这种分片时可能导致系统崩溃。
- 防止碎片包：启用该项后，设备可以有效防止碎片包攻击，缺省启用该项，无法取消。该攻击表现为攻击者向目标主机发送部分分片报文，而不发送所有的分片报文，这样目标主机会一直等待，直到计时器超时。如果攻击者发送了大量的分片报文，就会耗尽目标主机的资源，导致其不能响应正常的 IP 报文。

(7) 在“异常流攻击防御”配置项处，选择需要开启防御的异常流攻击类型。

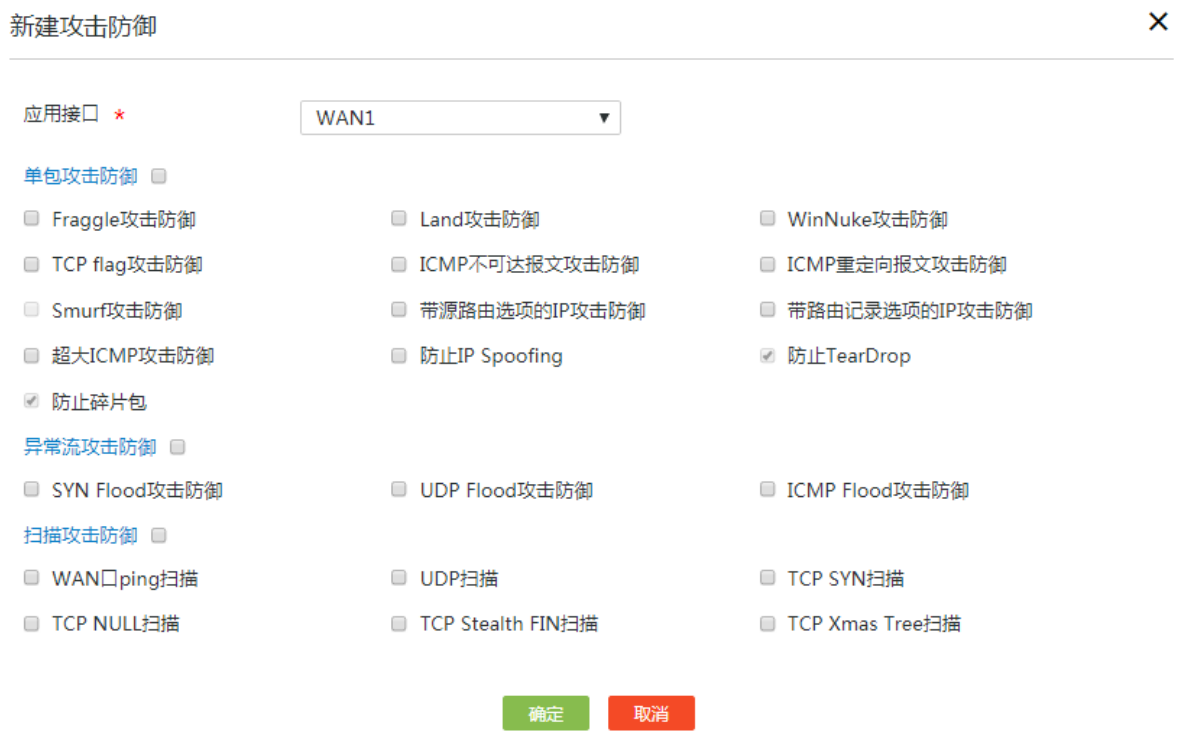
- SYN Flood 攻击防御：启用该项后，设备可以有效防止 SYN Flood 攻击。该攻击表现为攻击者向目标发送大量的 SYN 报文，消耗目标的连接资源，使目标系统无法再接受新连接。
- UDP Flood 攻击防御：启用该项后，设备可以有效防止 UDP Flood 攻击。该攻击表现为攻击者向目标发送大量的 UDP 报文，导致目标主机忙于处理这些 UDP 报文而无法继续处理正常的报文。
- ICMP Flood 攻击防御：启用该项后，设备可以有效防止 ICMP Flood 攻击。该攻击表现为攻击者向目标发送大量的 ICMP 报文，导致目标主机忙于处理这些 ICMP 报文而无法继续处理正常的报文。

(8) 在“扫描攻击防御”区段下，选择需要开启防御的扫描攻击类型。

- WAN 口 ping 扫描：启用该项后，设备不回应来自 Internet 的 Ping 请求，可以防止 Internet 上恶意的 Ping 探测。

- UDP 扫描：启用该项后，设备可以有效防止 UDP 扫描攻击。该攻击表现为攻击者向目标端口发送 UDP 报文，探测端口的开放情况。
- TCP SYN 扫描：启用该项后，设备可以有效防止 TCP SYN 扫描攻击。该攻击表现为攻击者像建立正常的 TCP 连接一样向目标端口发送 SYN 报文，然后等待目标主机的回应，借此探测端口的开放情况。
- TCP NULL 扫描：启用该项后，设备可以有效防止 TCP NULL 扫描。该攻击表现为攻击者向目标端口发送所有标志都不置位的 TCP 报文，然后等待目标主机的回应，借此探测端口的开放情况。
- TCP Stealth FIN 扫描：启用该项后，设备可以有效防止 TCP Stealth FIN 扫描。该攻击表现为攻击者向目标端口发送只有 FIN 标志置位的 TCP 报文，然后等待目标主机的回应，借此探测端口的开放情况。
- TCP Xmas Tree 扫描：启用该项后，设备可以有效防止 TCP Xmas Tree 扫描。该攻击表现为攻击者向目标端口发送 FIN、URG 和 PUSH 标志置位的 TCP 报文，然后等待目标主机的回应，借此探测端口的开放情况。

(9) 点击<确定>按钮，完成配置。



10.6.3 攻击防御统计

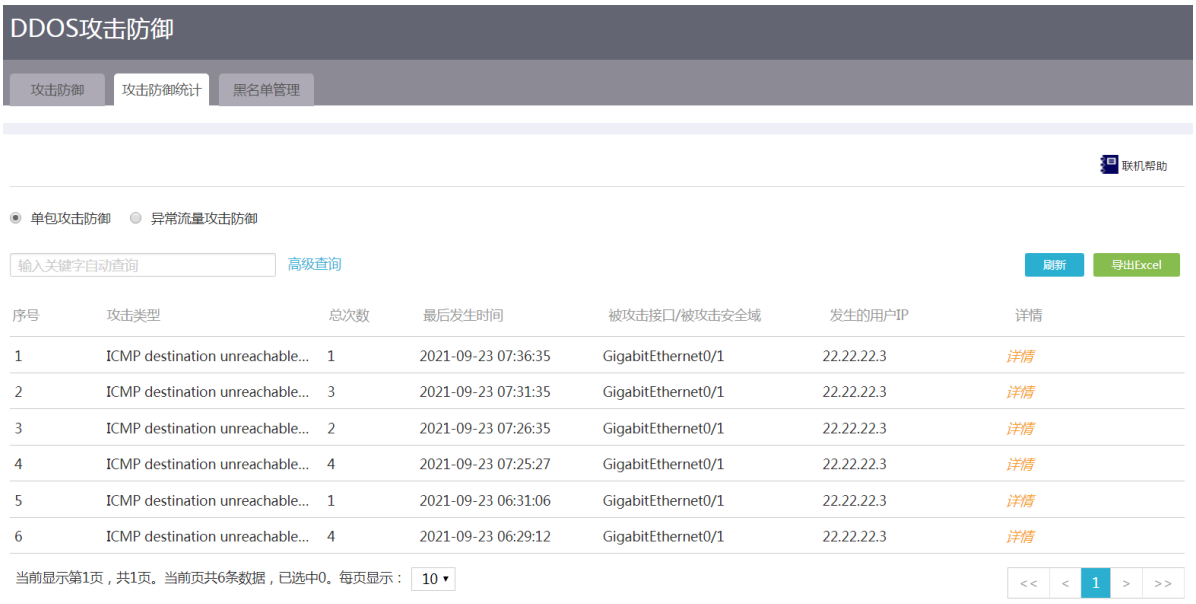
(1) 单击导航树中[网络安全/DDOS 攻击防御]菜单项，进入 DDOS 攻击防御配置页面。

(2) 单击“攻击防御统计”页签，进入攻击防御统计页面。

(3) 勾选“单包攻击防御”选项，列表将会显示单包攻击防御的统计信息。

(4) 勾选“异常流量攻击防御”选项，列表将会显示异常流量攻击防御的统计信息。

(5) 点击<导出 Excel>按钮，将攻击防御的统计信息导出到 Excel 中保存。



10.6.4 报文源认证

(1) 单击导航树中[网络安全/DDOS 攻击防御]菜单项，进入 DDOS 攻击防御配置页面。

(2) 单击“报文源认证”页签，进入报文源认证配置页面。

(3) 根据需要可设置如下参数：

- 启用基于静态路由的报文源认证功能：启用该项后，设备允许源 IP 与 LAN 接口同一网段或通过出接口为 LAN 口的静态路由表反向可达的内网路由器过来的流量通过，其它网段过来的数据包将被设备丢弃。
- 启用基于 ARP 绑定、DHCP 攻击防护报文源认证功能：启用该项后，设备将根据 ARP 绑定表中的静态绑定关系以及 DHCP 分配列表中的对应关系，来认证内网过来的数据包。如果数据包的源 IP/MAC 与 ARP 绑定表中的 IP/MAC 对应关系存在冲突，则该数据包将被设备丢弃。
- 启用基于动态 ARP 的报文源认证功能：启用该项后，设备将会对内网数据包的源 IP/MAC 进行智能认证，确认对端是否是存在的合法的主机，如果数据包的源 IP/MAC 与已确认的合法主机的 IP/MAC 冲突，则该数据包将被设备丢弃。如果网络中存在相同 MAC 对应不同 IP 的应用，请将对应的 IP/MAC 进行静态 ARP 绑定，否则可能影响正常业务访问。

(4) 点击<应用>按钮，完成配置。

10.6.5 异常流量防护

(1) 单击导航树中[网络安全/DDOS 攻击防御]菜单项，进入 DDOS 攻击防御配置页面。

(2) 单击“异常流量防护”页签，进入异常流量防护配置页面。

(3) 勾选“启用异常主机流量防护功能”选项，并设置异常流量阈值。

(4) 根据需要选择如下防护级别：

- 高：防护等级最高。高防护等级下，设备会进行异常主机流量检测，并且自动把检测到的攻击主机添加到黑名单中，在指定的生效时间范围内，禁止其访问本设备和 Internet，以尽量减少该异常主机对网络造成的影响。
- 中：防护等级居中。中防护等级下，设备会把单个内网主机的上行流量限制在异常流量阈值范围内，超过阈值的流量将被设备丢弃。
- 低：防护等级低。低防护等级下，设备仅记录异常流量日志，仍然允许相应主机访问设备和 Internet。

(5) 点击<应用>按钮，完成配置。

10.7 安全统计

10.7.1 简介

安全统计功能用于对设备接收到的非法或者可疑数据包进行统计，以方便查看网络环境是否存在欺骗或攻击行为。本功能支持统计如下类型的数据包：

- 报文源认证失败：表示由 LAN 网络中的非法主机发送的数据包。如需统计此类数据包，需先启用报文源认证的相关功能。
- LAN 侧可疑：表示由 LAN 网络中无法确定真实性的主机的发送数据包。
- WAN 侧非法：表示由 Intetnet 侧主动向设备 WAN 口发送的非法数据包。

10.7.2 配置步骤

(1) 单击导航树中[网络安全/安全统计]菜单项，进入安全统计配置页面。

(2) 勾选“开启安全统计”选项，列表中将会显示安全统计信息。

(3) 点击数据包类型对应的操作列<清除>按钮，清除该数据包类型的统计信息。

(4) 在弹出的确认提示对话框中，点击<是>按钮，完成清除操作。

10.8 黑名单管理

10.8.1 简介

黑名单管理功能用于查看和解除已添加的黑名单用户。

10.8.2 配置步骤

(1) 单击导航树中[网络安全/黑名单管理]菜单项，进入黑名单管理页面。

(2) 在列表中点击黑名单用户对应的动作列图标，可将用户从黑名单中删除。

10.9 终端接入控制

10.9.1 简介

终端接入控制功能可以同时对数据报文中的源 MAC 地址和源 IP 地址进行匹配，只有源 MAC 地址和源 IP 地址同时匹配的设备，才允许访问外网。

10.9.2 配置步骤

(1) 单击导航树中[网络安全/终端接入控制]菜单项，进入终端接入控制配置页面。

(2) 根据需要设置规则，具体如下：

- 仅允许 DHCP 服务器分配的客户端访问外网：用户可以指定仅允许 DHCP 服务器分配的客户端访问外网，使用此功能后不在 DHCP Server 分配的客户列表中的客户端将无法访问外网。因此需要注意，在使能该功能后如果出现无法访问外网，请将管理 PC 设置为 DHCP 方式获取 IP 地址。
- 仅允许 ARP 静态绑定的用户访问外网：用户可以指定仅允许 ARP 静态绑定规则表中的客户端访问外网，使用此功能后不在 ARP 静态绑定规则表中的客户端将无法访问外网。因此需要注意，在使能该功能前需要把管理 PC 的 IP 或者 MAC 加入到 ARP 静态绑定规则表中，否则启用该功能后，管理 PC 将无法访问外网。

(3) 点击<应用>按钮，完成配置。

11 认证管理

11.1 配置任务导引

11.1.1 实现接入设备的用户身份进行验证

当网络管理员需要对接入设备的用户身份进行验证时，可以通过配置 Portal 认证功能来实现，可根据如下步骤配置。

步骤	配置内容	详情
1	在云平台中绑定路由器（必选）	在云平台中绑定路由器的方法，具体配置方法请见参见《H3C ER G3系列路由器如何连接云平台配置举例》。
2	设置认证配置（必选）	在云平台中设置认证配置，具体配置方法请见参见《H3C云简网络部署手册》。
3	启用云认证功能（必选）	对指定的VLAN开启云认证功能，具体配置方法请见参见配置云认证。
4	配置免认证（可选）	根据需要对无需认证主机配置免认证，可选择基于IP地址或MAC地址进行免认证。具体配置方法请参见配置免认证MAC地址或配置免认证IP地址。

11.2 Portal认证

11.2.1 简介

Portal 是互联网接入的一种认证方式，通过对用户进行身份认证，以达到对用户访问进行控制的目的。本设备的 Portal 认证方式为云端认证方式，采用云端服务器来同时承担 Portal 认证服务器和 Portal Web 服务器的职责。

您可以为不需要通过 Portal 认证即可访问网络资源的用户设置免认证规则，免认证规则的匹配项包括 MAC 地址、IP 地址。

11.2.2 配置云认证

1. 配置准备

开启云认证之前，需要先完成云管理平台（H3C 云平台）上的认证模板的配置，并开启云服务。

有关云服务的配置，请在“系统工具>远程管理”中的“云服务”页签中配置。

2. 配置步骤

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“云认证”页签，进入认证设置页面。

(3) 在列表中的“开启和关闭”列的“开启/关闭”按钮，设置是否对接口下的 Portal 用户开启云认证功能。

11.2.3 配置免认证 MAC 地址

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“免认证 MAC 地址”页签，进入免认证 MAC 地址配置页面。

(3) 点击<添加>按钮，弹出添加免认证 MAC 地址对话框。

(4) 在“MAC 地址”配置项处，输入免认证 MAC 地址。

(5) 在“描述”配置项处，输入与本配置相关的描述。

(6) 点击<确定>按钮，完成配置。

11.2.4 配置免认证 IP 地址

1. 注意事项

在添加免认证 IP 地址时，免认证源 IP 地址分组或免认证目的地址分组不能为空。当系统不存在地址分组时，需要先新增地址组。

2. 配置步骤

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“免认证 IP 地址”页签，进入免认证 IP 地址配置页面。

(3) 点击<添加>按钮，弹出添加免认证 IP 地址对话框。

(4) 在“地址添加方式”配置项处，选择免认证 IP 地址的方式。

- 若选择“源 IP 地址组”选项，则需在“免认证源地址分组”配置项处，选择已存在的免认证源地址分组，或点击<新增地址组>按钮，添加新的免认证源地址组。点击“查看”链接，可以查看系统中已经创建的全部地址分组。
- 若选择“目的 IP 地址组”选项，则需在“免认证目的地址分组”配置项处，选择已存在的免认证目的地址分组，或点击<新增地址组>按钮，添加新免认证目的地址组。
- 选择“域名”选项，则需在“域名”配置项处，输入免认证的域名。

(5) 点击<确定>按钮，完成配置。


Portal认证
云认证
免认证MAC地址
免认证IP地址
请输入关键字自动查询
高级查询
刷新
添加
删除
免认证IP地址组
免认证域名
地址类型
描述
操作
test02
源IP地址组
55222
目的IP地址组
当前显示第1页，共1页。当前页共2条数据，已选中0。每页显示：
10
<<
<
1
>
>>
添加免认证IP地址
地址添加方式 *
源IP地址组
免认证源地址分组
test
新增地址组
查看
描述
(1-127字符)
确定
取消

12 虚拟专网(VPN)

12.1 配置任务导引

12.1.1 建立 IPsec VPN

建立 IPsec VPN 时，需要对两端设备进行配置。配置步骤如下：

步骤	配置内容	详情
1	完成LAN的基本配置（可选）	根据需要修改VLAN1的IP地址或创建新的VLAN，具体配置方法请见参见配置VLAN。
2	完成WAN的基本配置（必选）	将WAN接口连接Internet，完成WAN配置，具体配置方法请见参见WAN配置。
3	添加IPsec策略（必选）	根据实际需要添加IPsec策略，具体配置方法请见参见配置IPsec分支节点或配置IPsec中心节点。

12.1.2 建立 L2TP VPN

建立 L2TP VPN 时，需要对两端设备进行配置。一端配置为 L2TP 服务器，另一端配置为 L2TP 客户端，配置步骤如下：

步骤	配置内容	详情
1	完成WAN的基本配置（必选）	将WAN接口连接Internet，完成WAN配置，具体配置方法请见参见WAN配置。
2	启用并配置L2TP服务器端（必选）	启用L2TP服务器，并根据实际需要新建L2TP组和添加L2TP用户，具体配置方法请见参见L2TP服务器的L2TP配置或L2TP用户。
3	启用并配置L2TP客户端（必选）	启用L2TP客户端，并根据实际需要新建L2TP组，具体配置方法请见参见L2TP客户端的L2TP配置。

12.2 IPsec VPN

12.2.1 简介

IPsec VPN 是利用 IPsec 技术建立的虚拟专用网。IPsec 通过在特定通信方之间建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

IPsec 协议为 IP 层上的网络数据安全提供了一整套安全体系结构，包括安全协议 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）以及用于网络认证及加密的一些算法等。其中，AH 协议和 ESP 协议用于提供安全服务，IKE 协议用于密钥交换。

设备支持两种 IPsec VPN 组网方式：

- “中心—分支”方式组网：企业分支机构网关将主动与总部网关建立 IPsec 隧道，分支机构内部终端可以安全访问总部的网络资源。
- “分支—分支”方式组网：企业各分支网关之间均可主动建立 IPsec 隧道，来保护分支之间的数据通信。

12.2.2 配置 IPsec 分支节点

1. 配置需求

“分支—分支”方式组网环境中的设备之间均可主动建立 IPsec 隧道。

2. 配置步骤

IPsec 基本配置

(1) 单击导航树中[虚拟专网(VPN)/IPsec VPN]菜单项，进入 IPsec VPN 配置页面。

(2) 单击“IPsec 策略”页签，进入 IPsec 策略配置页面。

(3) 点击<添加>按钮，弹出添加 IPsec 策略对话框。

(4) 在“名称”配置项处，输入 IPsec 策略的名称。

(5) 在“接口”配置项处，选择应用 IPsec 策略的接口。请注意，此接口需要与对端设备路由可达。

(6) 在“组网方式”配置项处，选择“分支节点”选项。

(7) 在“对端网关地址”配置项处，输入 IPsec 隧道对端的 IP 地址或域名。通常为总部网关或对端分支机构网关的 WAN 口地址。

(8) 在“认证方式”配置项处，选择 IPsec 隧道的认证方式。此参数目前仅支持预共享密钥。

(9) 在“预共享密钥”配置项处，输入与对端设备相同的预共享密钥。该密钥需要提前进行协商和通告。

(10) 在“保护流措施”配置项处，进行如下配置：

a. 在“受保护协议”配置项处，选择受 IPsec 隧道保护的报文的协议类型。

b. 在“本端受保护网段/掩码”配置项处，输入本端受保护网段。

c. 在“本端受保护端口”配置项处，输入本端受保护端口。仅当受保护协议选择为 TCP 或 UDP 时支持配置。

由本端受保护网段内主机的受保护端口发送的报文将被设备进行 IPsec 隧道封装处理。

d. 在“对端受保护网段/掩码”配置项处，输入对端受保护网段。

e. 在“对端受保护端口”配置项处，输入对端受保护端口。仅当受保护协议选择为 TCP 或 UDP 时支持配置。

由对端受保护网段内主机的受保护端口发送的报文才可以被设备进行 IPsec 隧道解封装处理。

f. 根据需要可以在“操作”配置项处，添加多条保护流。

IKE 高级配置

如您需要改变设备的缺省 IKE 配置，可按如下方式进行配置。

(1) 按上述方式完成 IPsec 基本配置。

(2) 点击<显示高级配置>链接，弹出高级配置对话框。

(3) 单击“IKE 配置”页签，进入 IKE 配置页面。

(4) 在“IKE 版本”配置项处，选择 IKE 版本。

(5) 在“协商模式”配置项处，选择 IKE 协商模式：

- 主模式：协商步骤多，身份验证位于密钥交互过程之后进行，适用于对身份保护要求较高的场合。
- 野蛮模式：协商步骤少，身份验证与密钥交互同时进行，适用于对身份保护要求不高的场合。

当 IKE 版本为 V1 时，可配置此参数。若设备公网 IP 地址是动态分配的，建议您选择 IKE 协商模式为野蛮模式。

(6) 在“本端身份类型”配置项处，配置用于 IKE 认证的本端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与对端设备上执行步骤（7）配置的对端身份类型和身份标识一致。

如果您执行步骤（5）选择的 IKE 协商模式为主模式，您需要将本端设备身份类型配置为 IP 地址。

(7) 在“对端身份类型”配置项处，配置用于 IKE 认证的对端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与对端设备上执行步骤（6）配置的本端身份类型和身份标识一致。

(8) 在“对等体存活检测（DPD）”配置项处，选择是否开启对等体存活检测功能。该功能可用于检测对端是否存活，设备将拆除对端失活的 IPsec 隧道。建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况。

(9) 在“算法组合”配置项处，选择 IKE 协议交互所需的加密和认证算法。如果选择“推荐”选项，需要选择推荐的算法组合；如果选择“自定义”选项，需要设置自定义的认证算法、加密算法和 PFS 算法。

IPsec 隧道的两端所配置的认证算法、加密算法和 PFS 算法必须一致。

(10) 在“SA 生存时间”配置项处，输入 IKE 重新协商的时间间隔，超过所配时间将触发 IKE 相关参数的重新协商。建议 SA 生存时间设置不低于 600 秒。

IPsec 高级配置

如您需要改变设备的缺省 IPsec 高级配置，可按如下方式进行配置。

(1) 按上述方式完成 IPsec 基本配置。

(2) 单击“IPsec 配置”页签，进入 IPsec 配置页面。

(3) 在“算法组合”配置项处，选择 IPsec 协议交互使用的安全协议以及相应的加密和认证算法。如果选择“推荐”选项，需要选择推荐的算法组合；如果选择“自定义”选项，需要设置自定义的安全协议、ESP 认证算法和 ESP 加密算法。

IPsec 隧道的两端所配置的安全协议、认证算法、加密算法、封装模式和 PFS 算法必须一致。

(4) 在“封装模式”配置项处，选择 IPsec 隧道的封装模式。

若 IPsec 本端受保护网段与对端受保护网段均为私网网段，建议您选择封装模式为隧道模式。

IPsec 隧道的两端所配置的封装模式必须一致。

(5) 在“PFS”配置项处，选择 IPsec 隧道的 PFS 算法。

IPsec 隧道的两端所配置的 PFS 算法必须一致。

(6) 在“基于时间的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的时间间隔，超过所配时间将触发 IPsec 相关参数的重新协商。

(7) 在“基于流量的生存时间”配置项处，输入触发 IPsec 重新协商的流量大小，超过所配流量将触发 IPsec 相关参数的重新协商。

(8) 在“触发模式”配置项处，选择触发 IPsec 重新协商的模式。

(9) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(10) 点击<确定>按钮，完成配置。

12.2.3 配置 IPsec 中心节点

1. 配置需求

“中心—分支”方式组网环境中的分支节点设备需要主动建立 IPsec 隧道与中心节点通信。

2. 注意事项

当设备作为中心节点，一个接口下只能配置一条中心节点策略。在添加 IPsec 中心节点策略选择接口时，需选择未创建过中心节点策略的接口。

3. 配置步骤

IPsec 基本配置

(1) 单击导航树中[虚拟专网(VPN)/IPsec VPN]菜单项，进入 IPsec VPN 配置页面。

(2) 单击“IPsec 策略”页签，进入 IPsec 策略配置页面。

(3) 点击<添加>按钮，弹出添加 IPsec 策略对话框。

(4) 在“名称”配置项处，输入 IPsec 策略的名称。

(5) 在“接口”配置项处，选择应用 IPsec 策略的接口。请注意，此接口需要与分支节点设备路由可达。

(6) 在“组网方式”配置项处，选择“中心节点”选项。

(7) 在“预共享密钥”配置项处，输入与对端设备相同的预共享密钥。该密钥需要提前进行协商和通告。

IKE 配置

如您需要改变设备的缺省 IKE 配置，可按如下方式进行配置。

(1) 按上述方式完成 IPsec 基本配置。

(2) 点击<显示高级配置>链接，进入高级配置页面。

(3) 单击“IKE 配置”页签，进入 IKE 配置页面。

(4) 在“IKE 版本”配置项处，选择 IKE 版本。

(5) 在“协商模式”配置项处，选择 IKE 协商模式：

- 主模式：协商步骤多，身份验证位于密钥交互过程之后进行，适用于对身份保护要求较高的场合。
- 野蛮模式：协商步骤少，身份验证与密钥交互同时进行，适用于对身份保护要求不高的场合。

当 IKE 版本为 V1 时，可配置此参数。若设备公网 IP 地址是动态分配的，建议您选择 IKE 协商模式为野蛮模式。

(6) 在“本端身份类型”配置项处，配置用于 IKE 认证的本端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与分支节点设备上配置的对端身份类型和身份标识一致。

如果您执行步骤（5）选择的 IKE 协商模式为主模式，您需要将本端设备身份类型配置为 IP 地址。

(7) 在“对等体存活检测（DPD）”配置项处，选择是否开启对等体存活检测功能。该功能可用于检测对端是否存活，设备将拆除对端失活的 IPsec 隧道。建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况。

(8) 在“算法组合”配置项处，选择 IKE 协议交互所需的加密和认证算法。如果选择“推荐”选项，需要选择推荐的算法组合；如果选择“自定义”选项，需要设置自定义的认证算法、加密算法和 PFS 算法。

IPsec 隧道的两端所配置的认证算法、加密算法和 PFS 算法必须一致。

(9) 在“SA 生存时间”配置项处，输入 IKE 重新协商的时间间隔，超过所配时间将触发 IKE 相关参数的重新协商。建议 SA 生存时间设置不低于 600 秒。

IPsec 高级配置

如您需要改变设备的缺省 IPsec 高级配置，可按如下方式进行配置。

(1) 按上述方式完成 IPsec 基本配置。

(2) 单击“IPsec 配置”页签，进入 IPsec 配置页面。

(3) 在“算法组合”配置项处，选择 IPsec 协议交互使用的安全协议以及相应的加密和认证算法。如果选择“推荐”选项，需要选择推荐的算法组合；如果选择“自定义”选项，需要设置自定义的安全协议、ESP 认证算法和 ESP 加密算法。

IPsec 隧道的两端所配置的安全协议、ESP 认证算法和 ESP 加密算法必须一致。

(4) 在“封装模式”配置项处，选择 IPsec 隧道的封装模式。

若 IPsec 本端受保护网段与对端受保护网段均为私网网段，建议您选择封装模式为隧道模式。

IPsec 隧道的两端所配置的封装模式必须一致。

(5) 在“PFS”配置项处，选择 IPsec 隧道的 PFS 算法。

IPsec 隧道的两端所配置的 PFS 算法必须一致。

(6) 在“基于时间的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的时间间隔，超过所配时间将触发 IPsec 相关参数的重新协商。

(7) 在“基于流量的生存时间”配置项处，输入触发 IPsec 重新协商的流量大小，超过所配流量将触发 IPsec 相关参数的重新协商。

(8) 在“触发模式”配置项处，选择触发 IPsec 重新协商的模式。

(9) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(10) 点击<确定>按钮，完成配置。

12.2.4 监控信息

(1) 单击导航树中[虚拟专网(VPN)/IPsec VPN]菜单项，进入 IPsec VPN 配置页面。

(2) 单击“监控信息”页签，进入监控信息页面。

12.3 L2TP服务器端

12.3.1 简介

本功能主要用于配置 L2TP 服务器端基本参数，开启 L2TP 服务。

如果您希望为企业驻外机构和出差人员等远端用户，提供一种安全且经济的方式，让他们能够与企业内部网络通信，访问企业内部网络资源，那么您可以通过配置 L2TP 服务器端来实现上述需求。

L2TP 服务器端是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业内部网络的边缘。

12.3.2 L2TP 配置

(1) 单击导航树中[虚拟专网(VPN)/L2TP 服务器端]菜单项，进入 L2TP 服务器端页面。

(2) 单击“L2TP 配置”页签，进入 L2TP 配置页面。

(3) 选择“启用 L2TP 服务器”选项，点击<确定>按钮，开启 L2TP 服务。

(4) 点击<添加>按钮，弹出新建 L2TP 组对话框。

(5) 在“L2TP 配置”下，设置 L2TP 隧道参数：

- 根据需要决定是否勾选“对端隧道名称”，如勾选，则在配置项处输入 L2TP 客户端的隧道名称。
- 在“本端隧道名称”配置项处，输入 L2TP 服务器端的隧道名称。
- 在“隧道验证”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则需在“隧道验证密码”配置项处，输入验证密码。该方式更加安全，但需要 L2TP 服务器端和 L2TP 客户端都启用隧道验证，且密码一致。
  - 如选择“禁用”，则表示 L2TP 服务器端和 L2TP 客户端在建立隧道时无需验证。

(6) 在“PPP 认证配置”下的“PPP 认证方式”配置项处，根据需要选择认证方式为“None”、“PAP”或“CHAP”。

- 如选择“None”，则表示对用户免认证。该方式，安全性最低，请谨慎使用。
- 如选择“PAP”，则表示采用两次握手机制对用户进行认证。该方式，安全性中。
- 如选择“CHAP”，则表示采用三次握手机制对用户进行认证。该方式，安全性最高。

(7) 在“PPP 地址配置”下，设置 PPP 地址参数：

- 在“虚拟模板接口地址”配置项处，输入虚拟模板接口的 IP 地址，使 L2TP 服务器端具有为 L2TP 客户端或用户分配 IP 地址的能力。
- 在“子网掩码”配置项处，输入虚拟模板接口 IP 地址的子网掩码。
- 在“DNS1”配置项处，输入用于分配给 L2TP 客户端或用户的主 DNS。
- 在“DNS2”配置项处。输入用于分配给 L2TP 客户端或用户的备用 DNS。DNS1 与 DNS2 不能相同。
- 在“用户地址池”配置项处，输入用于分配给 L2TP 客户端或用户的 IP 地址。

(8) 点击<显示高级设置>按钮，展开高级配置页面。

(9) 在“高级配置”下的“Hello 报文间隔”配置项处，输入保活报文的时间间隔。为了检测 LAC 和 LNS 之间隧道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送 5 次仍没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要重新建立隧道连接；LNS 端可以配置与 LAC 端不同的 Hello 报文间隔；缺省情况下，Hello 报文间隔为 60 秒。

(10) 点击<确定>按钮，完成配置。

12.3.3 隧道信息

(1) 单击导航树中[虚拟专网(VPN)/L2TP 服务器端]菜单项，进入 L2TP 服务器端页面。

(2) 单击“隧道信息”页签，进入隧道信息页面。

12.3.4 L2TP 用户

(1) 单击导航树中[虚拟专网(VPN)/L2TP 服务器端]菜单项，进入 L2TP 服务器端页面。

(2) 单击“L2TP 用户”页签，进入 L2TP 用户配置页面。

(3) 如果需要添加单个 L2TP 用户，请执行以下步骤：

a. 点击<添加>按钮，弹出添加用户对话框。

b. 在“账号名”配置项处，输入用户的账号名。

c. 在“状态”配置项处，选择用户的状态是否可用。

d. 在“密码”配置项处，输入用户账号的密码。

e. 在“最大用户数”配置项处，输入用户的最大连接数。

f. 在“有效日期”配置项处，选择是否配置用户权限的到期日期。如果选择“配置”选项，则需在日期选择框中选择用户权限的到期日期。

g. 点击<确定>按钮，完成配置。

(4) 如果需要批量添加 L2TP 用户，请执行以下步骤：

a. 点击<导出>按钮，下载导出模板。

b. 打开下载好的模板，添加 L2TP 用户并在本地保存。

c. 点击<导入>按钮，弹出导入 L2TP 用户列表对话框。

d. 点击<选择文件>按钮，选择已编辑好的模板。

e. 点击<确定>按钮，完成 L2TP 用户的批量添加

12.4 L2TP客户端

12.4.1 简介

本功能主要用于配置 L2TP 客户端基本参数，开启 L2TP 服务。

如果您希望为企业驻外机构，提供一种安全且经济的方式，让他们能够与企业内部网络通信，访问企业内部网络资源，那么您可以通过配置 L2TP 客户端来实现上述需求。

L2TP 客户端是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业驻外机构网络的出口。

12.4.2 L2TP 配置

(1) 单击导航树中[虚拟专网(VPN)/L2TP 客户端]菜单项，进入 L2TP 客户端页面。

(2) 单击“L2TP 配置”页签，进入 L2TP 配置页面。

(3) 在“L2TP 客户端”配置项处，选择“启用 L2TP 客户端”选项，点击<确定>按钮，开启 L2TP 服务。

(4) 点击<添加>按钮，弹出新建 L2TP 组对话框。

(5) 在“L2TP 配置”下，设置 L2TP 隧道参数：

- 在“本端隧道名称”配置项处，输入 L2TP 客户端的隧道名称。
- 在“地址获取方式”配置项处，选择 LAC 会话建立成功后 PPP 接口的 IP 地址获取方式，若选择“静态”选项，则需输入 LAC 端手工设置一个 IP 地址（由远端的 LNS 管理员分配）；若选择“动态”选项，则 PPP 接口的 IP 地址由 LNS 分配。
- 在“隧道验证”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则需在“隧道验证密码”配置项处，输入验证密码。该方式更加安全，但需要 L2TP 服务器端和 L2TP 客户端都启用隧道验证，且密码一致。
  - 如选择“禁用”，则表示 L2TP 服务器端和 L2TP 客户端在建立隧道时无需验证。

(6) 在“PPP 认证配置”下的“PPP 认证方式”配置项处，根据需要选择认证方式为“None”、“PAP”或“CHAP”。

- 如选择“None”，则表示对用户免认证。该方式，安全性最低，请谨慎使用。
- 如选择“PAP”，则表示采用两次握手机制对用户进行认证。该方式，安全性中。需输入用户名和密码。
- 如选择“CHAP”，则表示采用三次握手机制对用户进行认证。该方式，安全性最高。需输入用户名和密码。

(7) 在“PPP 认证配置”下的“NAT 地址转换”配置项处，根据需要选择“启用”或“未启用”。

- 如选择“启用”，则 L2TP 服务器端不需配置到达客户端的路由。
- 如选择“未启用”，则 L2TP 服务器端需配置到达客户端的路由，L2TP 客户端才能正常访问服务端资源。

(8) 在“L2TP 服务器端配置”下的“L2TP 服务器端地址”配置项处，输入 L2TP 服务器端的 IP 地址。

(9) 在“高级配置”下的“Hello 报文间隔”配置项处，输入保活报文的时间间隔。为了检测 LAC 和 LNS 之间隧道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送 6 次仍没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要重新建立隧道连接；LNS 端可以配置与 LAC 端不同的 Hello 报文间隔；缺省情况下，Hello 报文间隔为 60 秒。

(10) 点击<确定>按钮，完成配置。

12.4.3 隧道信息

(1) 单击导航树中[虚拟专网(VPN)/L2TP 客户端]菜单项，进入 L2TP 客户端页面。

(2) 单击“隧道信息”页签，进入隧道信息页面。


L2TP客户端
L2TP配置
隧道信息
请输入关键字自动查询
高级查询
刷新
删除
账号名
本端隧道编号
对端隧道编号
对端隧道端口
本端地址
对端隧道IP地址
对端隧道名称
会话数目
上行流速(Mbps)
下行流速(Mbps)
操作
当前显示第1页，共0页。当前页共0条数据，已选中0。每页显示：
10
<<
<
>
>>

13 高级选项

13.1 配置任务导引

13.1.1 配置动态域名

当用户希望通过固定的域名访问设备提供的服务时，可以在设备提供服务的 WAN 接口上配置 DDNS 服务。配置步骤如下：

步骤	配置内容	详情
1	注册域名（必选）	在DDNS服务器（即DDNS服务提供商，如花生壳网站）上注册域名。
2	配置DDNS服务（必选）	将在DDNS服务器上注册的域名与设备上的提供服务的WAN接口进行绑定，具体配置方法请见参见配置动态DNS。

13.1.2 为特定目的 IP 地址的报文指定出接口

为特定目的 IP 地址的报文指定出接口，可根据如下步骤配置静态路由来实现。

步骤	配置内容	详情
1	添加VLAN（可选）	在路由器上添加用于互访的VLAN，并将对应的LAN口划分VLAN，具体配置方法请见参见配置VLAN。
2	添加静态路由（必选）	为主机所在子网添加静态路由，具体配置方法请见参见静态路由。

13.1.3 定制策略路由

当网络管理员需要在某个时间段将局域网指定的主机的上网流量从指定的 WAN 口发送出去时，可以通过定制策略路由来实现，配置步骤如下：

步骤	配置内容	详情
1	添加时间组（必选）	设定策略路由实现的时间段，具体配置方法请见参见时间组。
2	添加定策略路由（必选）	根据实际需要添加策略路由，具体配置方法请见参见策略路由。

13.1.4 配置 SNMP 实现 NMS 管理路由器

如需使用 NMS 对路由器进行监控管理，则需配置 SNMP，配置步骤如下：

步骤	配置内容	详情
1	连接NMS（必选）	将路由器的LAN口连接网络网管NMS。

2	配置SNMP基本配置（必选）	选择SNMP版本，并配置SNMP基本配置，具体配置方法请见参见基本配置。
3	添加团体名（可选）	当选择SNMP版本为SNMPv1或SNMPv2c版本时，可根据需要添加SNMP的团体名，具体配置方法请见参见团体名设置。
4	添加用户名（可选）	当选择SNMP版本为SNMPv3时，可根据需要添加SNMP的用户名，具体配置方法请见参见用户设置。
5	配置NMS的SNMP设置（必选）	在NMS中配置使用的SNMP版本、团体名等，需确保与路由器上的SNMP配置一致。

13.2 应用服务

应用服务提供对 DNS 的配置功能，DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。主要包括：静态 DNS、动态 DNS 和本地域名服务。

“域名”、“本地域名地址”和“服务器地址”的设置规则如下：

- “域名”和“服务器地址”长度为 1-253 个字符；“本地域名地址”长度为 1-250 个字符。
- “域名”、“本地域名地址”和“服务器地址”只能包含字母，数字，符号-，以及符号.。
- “域名”、“本地域名地址”和“服务器地址”不能以符号.或者符号-开头和结尾，不能连续使用两个以及上的符号.或者符号-。
- “域名”和“服务器地址”中必须包含符号.，且最后一个符号.后面的字符不能为全数字。

13.2.1 配置静态 DNS

1. 配置简介

静态 DNS 就是手工建立域名和 IP 地址之间的对应关系。当您使用域名访问设备提供的服务（Web、Mail 或者 FTP 等服务）时，系统会查找静态 DNS 解析表，从中获取指定域名对应的 IP 地址。

2. 配置步骤

(1) 单击导航树中[高级选项/应用服务]菜单项，进入应用服务配置页面。

(2) 单击“静态 DNS”页签，进入静态 DNS 配置页面。

(3) 点击<添加>按钮，弹出新建静态 DNS 对话框。

(4) 在“域名”配置项处，输入网络设备的域名。

(5) 在“IP 地址”配置项处，输入网络设备的 IP 地址。

(6) 点击<确定>按钮，完成设置。

13.2.2 配置动态 DNS

1. 配置简介

如果您通过设备的 WAN 接口来提供 Web、Mail 或者 FTP 等服务，且希望在设备 WAN 接口的 IP 发生变化的情况下（如宽带拨号方式下），用户仍然能够通过固定的域名访问设备提供的服务，那么需要在设备上的提供 Web、Mail 或者 FTP 等服务的 WAN 接口上配置 DDNS（Dynamic Domain Name System，动态域名系统）服务。

使用 DDNS 服务之前，需要提前在 DDNS 服务器（即 DDNS 服务提供商，如花生壳网站）上注册。之后，当设备 WAN 接口的 IP 地址变化时，设备会自动通知 DDNS 服务器更新记录的 IP 地址和固定域名的映射关系。

2. 注意事项

设备向 DDNS 服务器申请域名时，请保证 WAN 接口地址为公网 IP 地址。

3. 配置准备

请提前在动态域名服务提供商（如花生壳网站）处注册账户，设置密码。

4. 配置步骤

(1) 单击导航树中[高级选项/应用服务]菜单项，进入应用服务配置页面。

(2) 单击“动态 DNS”页签，进入动态 DNS 配置页面。

(3) 点击<添加>按钮，弹出新建动态 DNS 策略对话框。

(4) 在“WAN 接口”配置项处，选择设备上的提供 Web、Mail 或者 FTP 等服务的 WAN 接口。

(5) 在“域名”配置项处，输入设备的域名。

(6) 在“服务器配置”下，设置动态 DNS 服务器参数：

- 服务提供商：选择服务提供商，如花生壳等。
- 服务器地址：服务提供商的服务器地址。如果服务器地址与缺省情况不同，勾选“修改服务器地址”后进行修改。
- 更新间隔：设置设备向服务器发送更新请求的时间间隔。如果配置时间间隔为 0，设备只在 WAN 接口 IP 地址发生变化或者接口连接由 down 变为 up 时发送更新请求。

(7) 在“账户配置”下，输入在服务提供商处注册的用户名和密码。

(8) 点击<确定>按钮，完成设置。

13.2.3 配置本地域名服务

1. 配置简介

内网终端可以通过本地域名地址访问设备的 Web 管理页面。

2. 注意事项

设置的本地域名地址不能与互联网中已注册的域名重复。

3. 配置步骤

(1) 单击导航树中[高级选项/应用服务]菜单项，进入应用服务配置页面。

(2) 单击“本地域名服务”页签，进入本地域名服务页面。

(3) 在“本地域名服务”配置项处，选择“开启”选项，开启本地域名服务功能。

(4) 在“本地域名地址”配置项处，输入本地域名的地址。

(5) 点击<应用>按钮，完成配置。

13.3 UPnP

13.3.1 简介

UPnP（Universal Plug and Play，通用即插即用）功能是针对设备彼此间通讯而定制的一组协议的统称。设备作为 UPnP 网关，主要功能是完成端口自动映射，UPnP 实现端口自动映射需要满足三个条件：

- 设备必须开启 UPnP 功能；
- 内网主机的操作系统必须支持并开启 UPnP 功能；
- 应用程序必须支持并开启 UPnP 功能，如迅雷、BitComet、电骡 eMule、MSN 等软件都支持 UPnP 功能。

设备开启 UPnP 功能后，可以为支持该功能的应用程序自动添加端口映射，加速点对点的传输，还可以解决一些传统业务（比如，MSN）不能穿越 NAT 的问题。但开启 UPnP 功能也会为支持该功能的非法应用程序建立映射，存在安全隐患。

13.3.2 注意事项

如果您的操作系统或者应用程序不支持 UPnP 功能，可通过配置虚拟服务器或端口触发，手工配置完成端口映射的配置，其效果是一样的。

UPnP 映射失败的原因很多，比如：

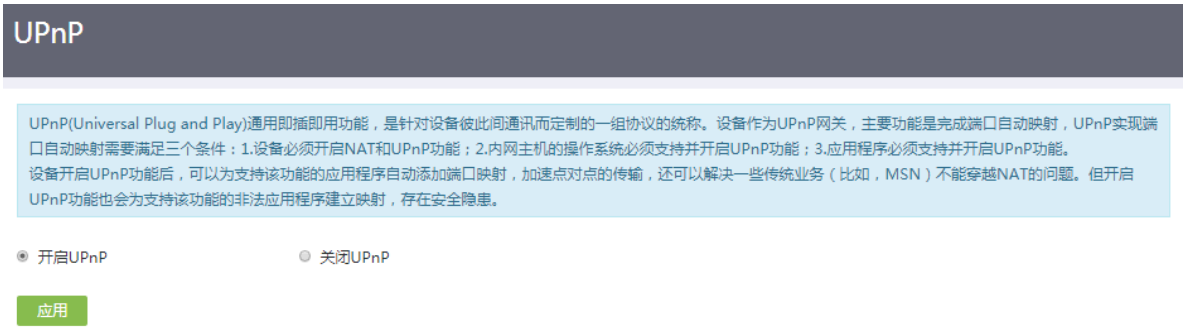
- 系统服务中禁止了 SSDP 服务（用于寻找 UPnP 设备），需要在系统服务中开启该服务。
- 开启了操作系统下的 SP1 的网络连接防火墙。操作系统的网络连接防火墙与 UPnP 设备发现有冲突，SP2 修复了这个问题，但是仍然需要在防火墙设置中允许例外：UPnP 框架。
- 应用软件或设备不支持 UPnP 功能。

13.3.3 配置步骤

(1) 单击导航树中[高级选项/UPnP]菜单项，进入 UPnP 页面。

(2) 选择“开启 UPnP”选项，开启 UPnP 功能。

(3) 点击<应用>按钮，完成设置。



13.4 静态路由

13.4.1 简介

- 静态路由是在路由器中通过手工方式设置的固定路由条目。当您的网络结构比较简单且比较稳定时，通过配置静态路由就可以实现网络互通。例如，当您知道网络的出接口，以及网关的 IP 地址时，设置静态路由即可实现正常通信。
- 当去往同一目的地存在多条静态路由时，如果您希望优先选用某条静态路由，可以调整静态路由的优先级。优先级的值越小，对应的静态路由的优先级越高。

13.4.2 注意事项

当静态路由中下一跳对应的接口失效时，本地的静态路由条目不会被删除，这种情况下需要您检查网络环境，然后修改静态路由的配置。

13.4.3 配置步骤

(1) 单击导航树中[高级选项/静态路由]菜单项，进入静态路由配置页面。

(2) 点击<添加>按钮，弹出添加 IPv4 静态路由对话框。

(3) 在“目的 IP 地址”配置项处，输入设备要访问的目的网络的 IP 地址。

(4) 在“掩码长度”配置项处，输入目的网络的掩码长度。

(5) 在“下一跳”配置项处，设置去往目的网络的出接口和下一跳 IP 地址。

- 选择出接口。当您不确定出接口时，可以不勾选“出接口”选项。通过设置下一跳 IP 地址，设备可以自己选择合适的出接口。
- 设置下一跳 IP 地址。

(6) 在“优先级”配置项处，输入静态路由的优先级。

(7) 在“描述”配置项处，输入静态路由的描述信息。

(8) 点击<确定>按钮，完成静态路由的添加。

(9) 点击“查看路由信息表”按钮，查看设备的路由信息。

13.5 策略路由

13.5.1 简介

与单纯按照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（源地址和目的地址等）的报文，执行指定的操

作（设置报文的下一跳和出接口等）。策略路由的匹配条件比普通路由更丰富，当需要按照报文的某些特征（如报文源地址和目的地址等）转发到不同的网络中时，可以配置策略路由功能。

策略路由的优先级会按照配置顺序生效，即先配置的策略路由优先级高于后配置的策略路由。

策略路由的优先级可以自定义配置，取值越小优先级越高。

13.5.2 配置步骤

(1) 单击导航树中[高级选项/策略路由]菜单项，进入策略路由配置页面。

(2) 点击<添加>按钮，弹出新增策略路由列表对话框。

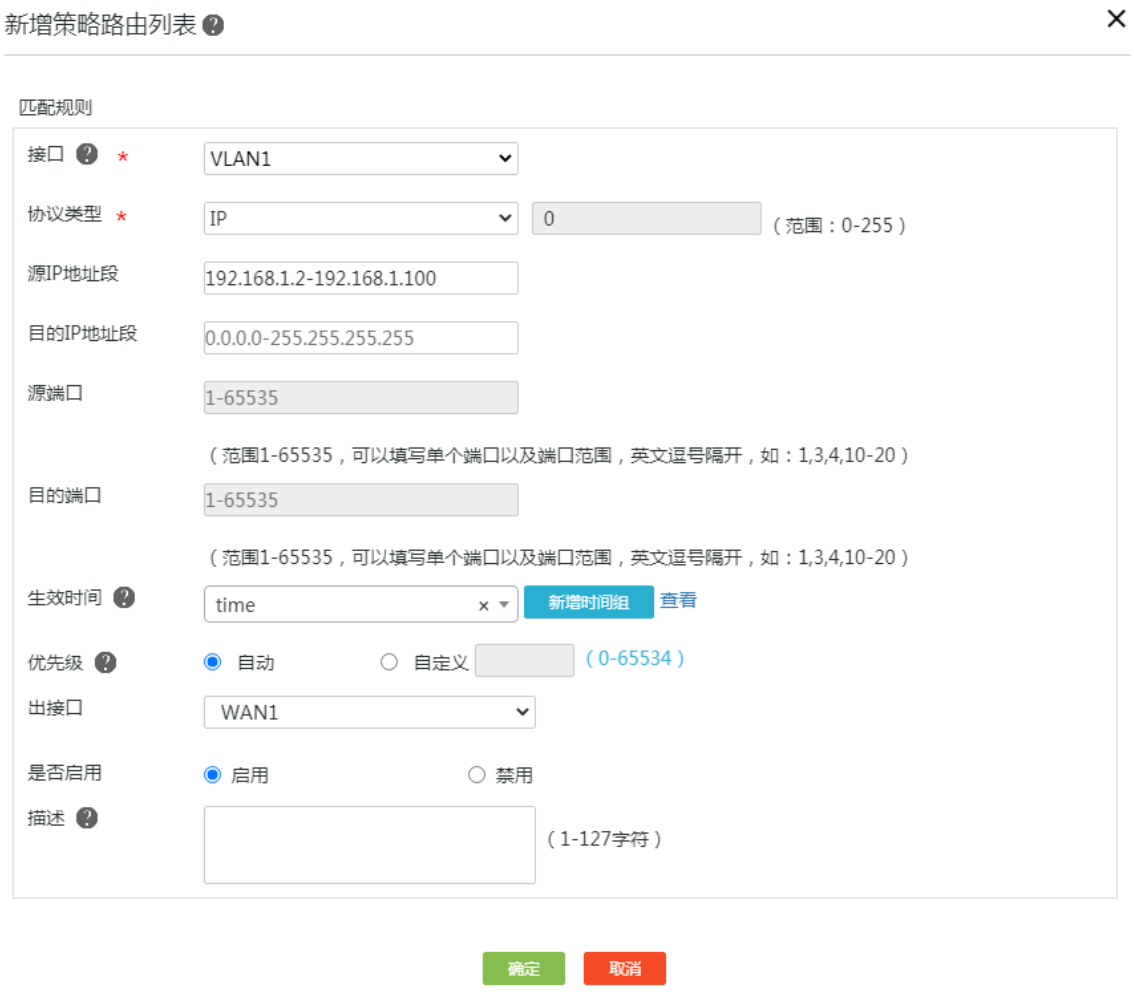
(3) 设置策略路由的匹配规则参数：

- 在“接口”配置项处，选择策略路由适用的接口。
- 在“协议类型”配置项处，选择匹配的协议类型，如果选择了“协议号”，则需要输入具体的协议编号。

  如果协议类型指定为“TCP”或“UDP”，则需要设置匹配报文的源端口和目的端口。
- 在“源 IP 地址段”和“目的 IP 地址段”配置项处，设置匹配报文的源 IP 地址范围和目的 IP 地址范围。输入地址段时，起始地址和结束地址间需要用短横线连接，如“1.1.1.1-1.1.1.2”，如果只指定一个地址，则起始地址和结束地址需要相同。如果在输入地址段或者地址前添加“!”，则表示取反，即除此地址段或者地址外的其它的地址都匹配，如“!1.1.1.1-1.1.1.10”。
- 在“源端口”和“目的端口”配置项处，设置匹配报文的源端口和目的端口。如果在输入端口号前添加“!”，则表示取反，即除此端口号外的其它的端口都匹配，如“!1-5000”。
- 在“生效时间”配置项处，设置匹配规则的时间组。
- 在“优先级”配置项处，设置策略路由的优先级。如果选择“自定义”选项，则需设置具体的优先级。
- 在“出接口”配置项处，设置匹配规则的报文通过指定出接口转发。
- 在“强制”配置项处，选择开启链路探测功能后，是否强制报文通过指定出接口转发。配置该参数时，可根据需要进行选择：
  - 若选择“强制”选项，则当链路探测结果为出接口不可用时，匹配报文仍从该接口转发。
  - 若未选择“强制”选项，则当链路探测结果为出接口不可用时，该条策略路由不生效，报文通过其他正常的路由转发。
- 在“是否启用”配置项处，设置策略路由是否启用。

- 在“描述”配置项处，输入策略路由的描述信息，当某些策略用于特殊用途时，管理员可以配置描述信息，方便后续查询使用。

(4) 点击<确定>按钮，完成配置。



13.6 SNMP

13.6.1 简介

SNMP（Simple Network Management Protocol，简单网络管理协议）广泛用于网络设备的远程管理和操作。SNMP 允许管理员通过 NMS 对网络上不同厂商、不同物理特性、采用不同互联技术的设备进行管理，包括状态监控、数据采集和故障处理。

1. 1.SNMP 网络架构

SNMP 网络架构由三部分组成：NMS、Agent 和 MIB。

- NMS（Network Management System，网络管理系统）是 SNMP 网络的管理者，能够提供友好的人机交互界面，来获取、设置 Agent 上参数的值，方便网络管理员完成大多数的网络管理工作。

- Agent 是 SNMP 网络的被管理者，负责接收、处理来自 NMS 的 SNMP 报文。在某些情况下，如接口状态发生改变时，Agent 也会主动向 NMS 发送告警信息。
- MIB（Management Information Base，管理信息库）是被管理对象的集合。NMS 管理设备的时候，通常会关注设备的一些参数，比如接口状态、CPU 利用率等，这些参数就是被管理对象，在 MIB 中称为节点。每个 Agent 都有自己的 MIB。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名称、访问权限和数据类型等。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。

2. 2.SNMP 版本

设备支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本，只有 NMS 和 Agent 使用的 SNMP 版本相同时，NMS 才能和 Agent 建立连接。

- SNMPv1 采用团体名（Community Name）认证机制。团体名类似于密码，用来限制 NMS 和 Agent 之间的通信。如果 NMS 配置的团体名和被管理设备上配置的团体名不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2c 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以配置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能可以为 NMS 和 Agent 之间的通信提供更高的安全性。

13.6.2 基本配置

(1) 单击导航树中[高级选项/SNMP]菜单项，进入基本配置页面。

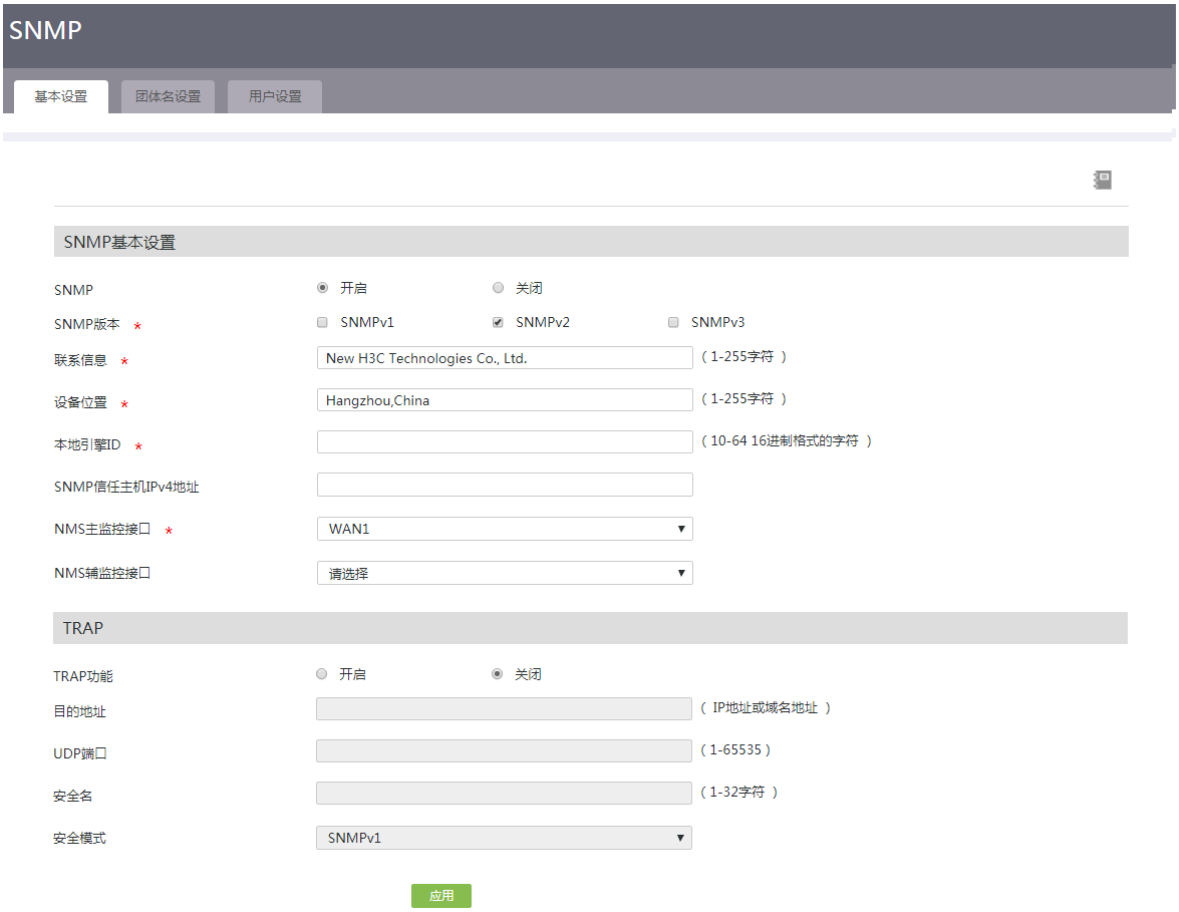
(2) 根据需要设置如下 SNMP 基本配置：

- 在“SNMP”配置项处，选择“开启”选项，开启 SNMP Agent 功能。
- 在“SNMP 版本”配置项处，勾选 SNMP 版本的版本。只有选择了相应的 SNMP 版本，设备才会处理对应版本的 SNMP 数据报文。
- 在“联系信息”配置项处，输入维护联系信息。联系信息长度为 1-255 个字符，不能为中文。
- 在“设备位置”配置项处，输入设备的位置信息。设备位置长度为 1-255 个字符，不能为中文。
- 在“本地引擎 ID”配置项处，输入设备的本地引擎 ID 信息。ID 信息为 10-64 位、16 进制格式的字符，只支持输入 0-9、a-f 和 A-F 字符，且字符数量必须为偶数。
- 在“SNMP 信任主机 IPv4 地址”配置项处，输入 SNMP Agent 信任的 NMS IP 地址，即允许指定的 NMS 对 SNMP Agent 进行访问。若不设置该项，即不对 NMS 进行限制。
- 在“NMS 主监控接口”配置项处，选择 NMS（网络管理工作站）管理本设备所用的主接口。
- 在“NMS 辅监控接口”配置项处，选择 NMS（网络管理工作站）管理本设备所用的备接口，当设备设置为单 WAN 口时，不支持该设置。

(3) 根据需要设置如下 TRAP 配置：

- 在“TRAP 功能”配置项处，选择“开启”选项，开启 SNMP TRAP 功能。
- 在“目的地址”配置项处，输入接收 TRAP 消息的主机地址或域名地址。
- 在“UDP 端口”配置项处，输入接收 TRAP 消息的 UDP 端口号。
- 在“安全名”配置项处，输入安全名称，可以是 SNMPv1、SNMPv2c 的团体名或 SNMPv3 的用户名。
- 在“安全模式”配置项处，选择安全名对应的 SNMP Agent 版本号。

(4) 点击<应用>按钮，完成设置。



13.6.3 团体名设置

1. 注意事项

团体名设置只支持 SNMPv1、SNMPv2c 版本。

2. 配置步骤

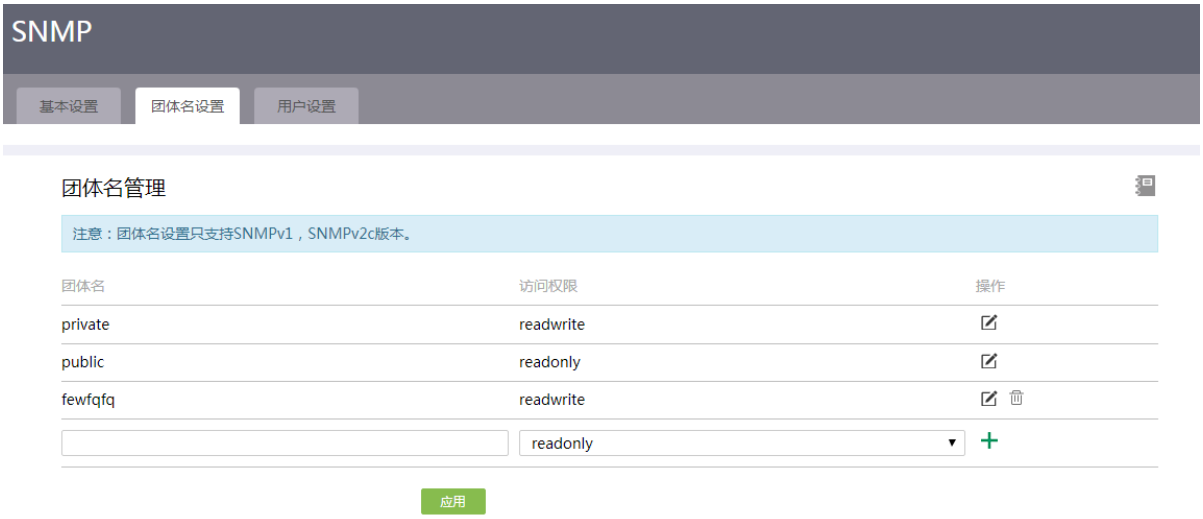
(1) 单击“团体名设置”页签，进入团体名设置页面。

(2) 在列表的最下方输入团体名，选择访问权限后，点击操作列的<+>按钮，完成团体名的添加。

(3) 点击团体名对应的操作列<修改>按钮，可以修改团体名及其访问权限。

(4) 点击团体名对应的操作列<删除>按钮，可以删除团体名

(5) 点击<应用>按钮，完成设置。



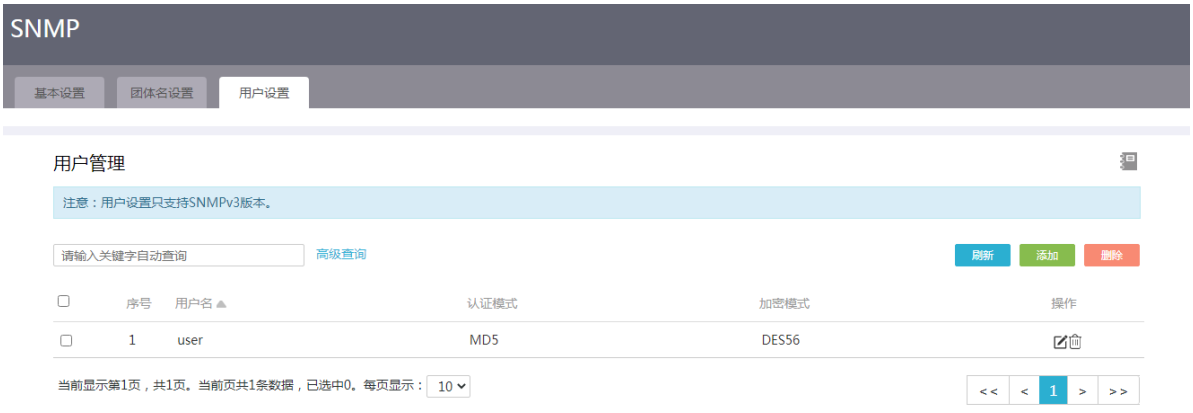
13.6.4 用户设置

1. 注意事项

用户设置只支持 SNMPv3 版本，用于添加 SNMPv3 版本的用户名。

2. 配置步骤

(1) 单击“用户设置”页签，进入用户设置页面。



(2) 点击<添加>按钮，弹出添加用户对话框。

(3) 根据需要配置如下参数：

- 在“用户名”配置项处，输入用户名。
- 在“认证模式”配置项处，选择认证算法，选项包括 MD5、SHA 和 None。如果选择 None，则表示不认证。

- 在“认证密码”配置项处，输入认证的密码。当认证模式设置为 MD5 或 SHA 时，需要配置此参数。密码长度为 1-64 个字符，只能包含英文字母[a-z,A-Z]、数字，以及~!@#$%^&*()_+`-={}|[]:'<>?,./字符；区分大小写。
- 在“认证密码确认”配置项处，再次输入在“认证密码”配置项处设置的密码。
- 在“加密模式”配置项处，选择加密模式，选项包括 DES56 和 None。如果选择 None，则表示不加密。
- 在“加密密码”配置项处，输入加密的密码。当加密模式设置为 DES56 时，需要配置此参数。密码长度为 1-64 个字符，只能包含英文字母[a-z,A-Z]、数字，以及~!@#$%^&*()_+`-={}|[]:'<>?,./字符；区分大小写。
- 在“加密密码确认”配置项处，再次输入在“加密密码”配置项处设置的密码。

(4) 点击<确定>按钮，完成添加。

14 系统工具

14.1 系统设置

14.1.1 简介

通过本功能可以设置设备信息和系统时间。设备信息包括设备名称、设备位置和设备管理员的联系信息，方便管理员管理和定位设备。系统时间包括日期、时间和时区等。为了便于管理设备，并保证本设备与其它网络设备协同工作，您需要为设备配置准确的系统时间。

系统时间的获取方式有两种：

- 手工设置日期和时间。该方式下，用户手工指定的日期和时间即为当前的系统时间。后续，设备使用内部时钟信号计时。如果设备重启，系统时间将恢复到出厂时间。
- 自动同步网络日期和时间。该方式下，设备使用从 NTP 服务器获取的时间作为当前的系统时间，并周期性地同步 NTP 服务器的时间，以便和 NTP 服务器的系统时间保持一致。即便本设备重启，设备也会迅速重新同步NTP服务器的系统时间。如果您管理的网络中有NTP服务器，推荐使用该方式，该方式获取的时间比手工配置的时间更精准。

14.1.2 配置设备信息

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“设备信息”页签，进入设备信息配置页面。

(3) 在“设备名称”配置项处，输入设备名称，例如以“设备型号.IP 地址”为设备名称。设备名称为 1-64 个字符，只支持数字、字母、下划线、中划线和空格，不能为中文，不能为全空格。

(4) 在“设备位置”配置项处，输入设备的位置信息。设备位置长度为 1-255 个字符，不能为中文。

(5) 在“联系信息”配置项处，输入设备管理员的联系信息。联系信息长度为 1-255 个字符，不能为中文。

(6) 点击<应用>按钮，完成配置。

14.1.3 手工设置日期和时间

1. 配置准备

了解设备所处的时区。全球分为 24 个时区，请将设备的时区配置为设备所在地理区域的时区。例如，设备在中国，请选择“北京,重庆,香港特别行政区,乌鲁木齐(GMT+08:00)”；如果设备位于美国，请选择“中部时间(美国和加拿大)(GMT-06:00)”。

2. 注意事项

如果设备重启，系统时间将恢复到出厂时间。

3. 配置步骤

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“日期和时间”页签，进入系统时间配置页面。

(3) 选择“手工设置日期和时间”选项。

(4) 将系统时间配置为设备所在地理区域的当前时间。

a. 选择年月日。

b. 选择时分秒。

(5) 将时区配置为设备所在地理区域的时区。

(6) 点击<应用>按钮，完成配置。

14.1.4 自动同步网络日期和时间

1. 配置准备

了解设备所处的时区。全球分为 24 个时区，请将设备的时区配置为设备所在地理区域的时区。例如，设备在中国，请选择“北京,重庆,香港特别行政区,乌鲁木齐(GMT+08:00)”；如果设备位于美国，请选择“中部时间(美国和加拿大)(GMT-06:00)”。

2. 注意事项

设备和 NTP 服务器上配置的时区必须相同，否则，会导致设备的系统时间和 NTP 服务器的系统时间不一致。

3. 配置步骤

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“日期和时间”页签，进入系统时间配置页面。

(3) 选择“自动同步网络日期和时间”选项。

(4) 在“NTP 服务器 1”配置项处，输入 NTP 服务器 1 的 IP 地址或者域名地址。

(5) 在“NTP 服务器 2”配置项处，输入 NTP 服务器 2 的 IP 地址或者域名地址。设备会自动从 NTP 服务器 1 和 NTP 服务器 2 中择优选取一台服务器的系统时间作为设备的系统时间。如果这台优选的服务器故障，则自动使用另一台 NTP 服务器的系统时间作为设备的系统时间。如果 NTP 服务器均故障，设备将使用内部时钟信号继续计时，待 NTP 服务器恢复后，再同步 NTP 服务器的时间。

(6) 点击“缺省 NTP 服务器列表”链接，弹出缺省 NTP 服务器对话框，查看设备内置的 NTP 服务器信息，点击<关闭>按钮，关闭对话框。

(7) 将时区配置为设备所在地理区域的时区。

(8) 点击<应用>按钮，完成配置。

14.2 网络诊断

14.2.1 简介

通过本功能可以对网络故障进行诊断，包括如下功能：

- Ping：用于检测网络，测试另一台设备或主机是否可达。
- Tracert：用于检查从设备到达目标主机所经过的路由情况。
- 系统自检：用于检查设备当前的运行和配置情况进行，反馈设备配置是否合理及设备运行是否正常等信息。
- 诊断：诊断信息为各功能模块的运行信息，用于定位问题。设备会将该信息以压缩文件的形式自动保存到您的终端设备。
- 端口镜像：用于将被镜像端口的报文自动复制到镜像端口，实时提供各端口传输状况的详细信息，方便网络管理人员进行流量监控、性能分析和故障诊断。
- 抓包工具：用于抓取网络数据报文，以便更有效地分析网络故障。抓包完成后，会自动导出抓取的文件“capture-******.pcap”供用户保存到本地。

14.2.2 Ping

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

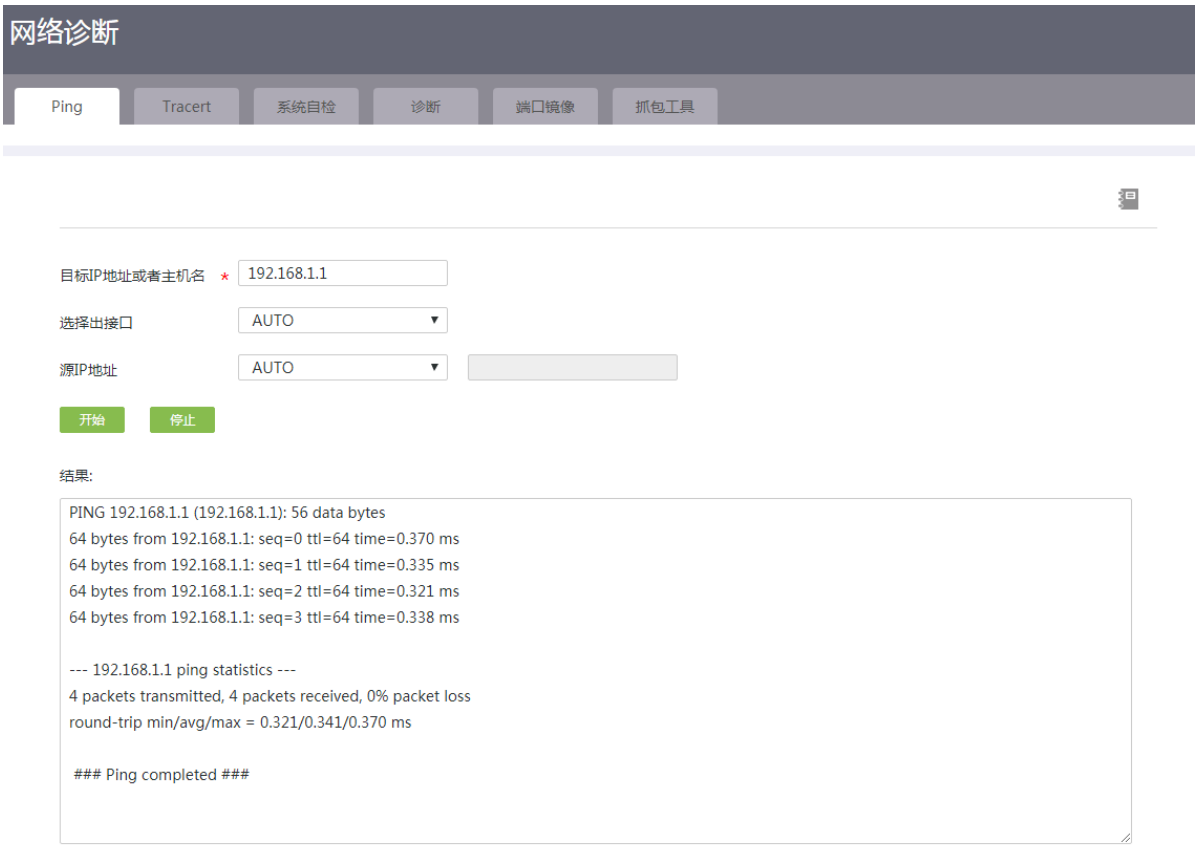
(2) 单击“Ping”页签，进入 Ping 通信测试页面。

(3) 在“目标 IP 地址或者主机名”配置项处，输入需要 Ping 的目标 IP 地址或者主机名。不支持输入\ ' " < > ; & ` #字符以及中文字符和空格。

(4) 在“选择出接口”配置项处，选择去往目标 IP 地址或者主机名的设备接口。当选择“AUTO”时，表示设备自动选择某一接口转发 Ping 报文。

(5) 在“源 IP 地址”配置项处，选择 Ping 操作的源 IP 地址。当选择“AUTO”时，表示设备自动选择 Ping 操作的源 IP 地址；当选择“源 IP 地址”时，需手动输入 Ping 操作的源 IP 地址。

(6) 点击<开始>按钮，系统开始进行检测。检测的过程和结果显示在当前页面，说明网络发包的测试情况和与测试主机的往返平均时延。



14.2.3 Tracert

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

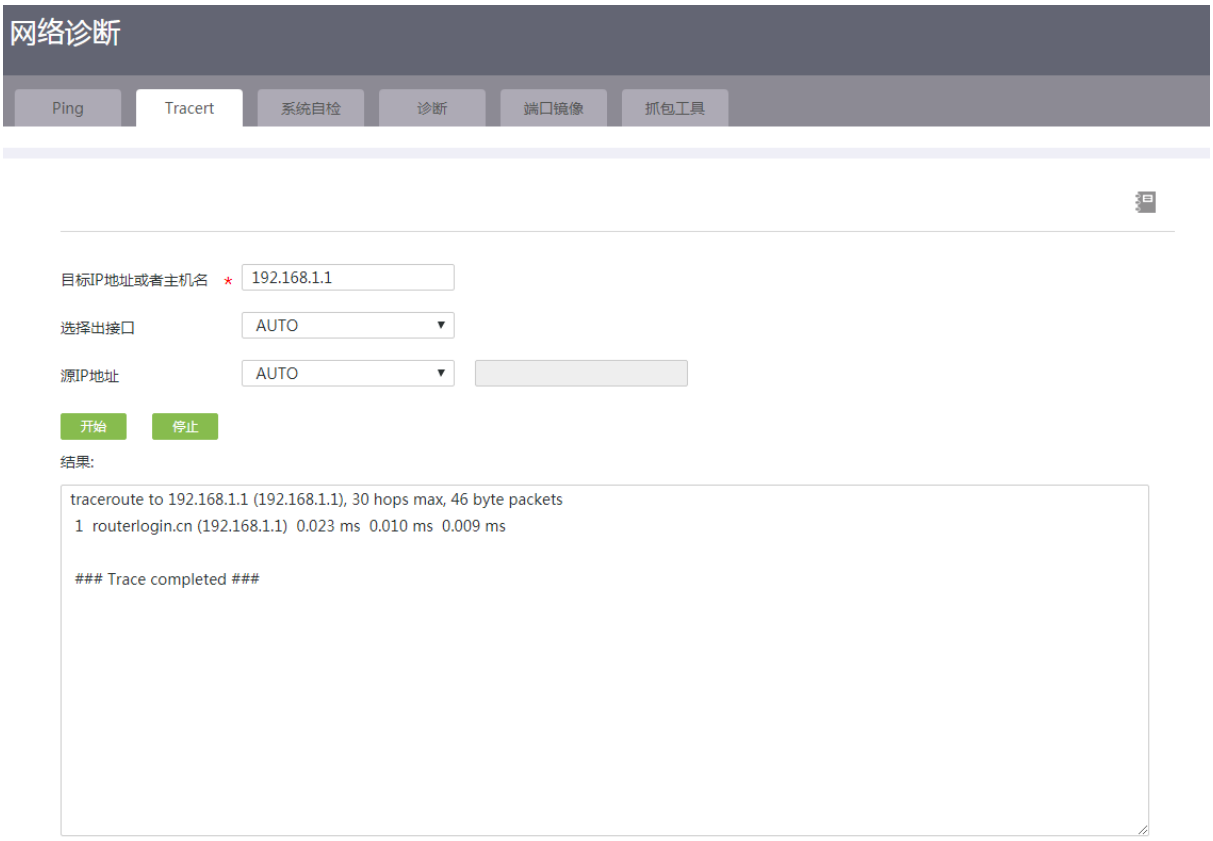
(2) 单击“Tracert”页签，进入 Tracert 通信测试页面。

(3) 在“目标 IP 地址或者主机名”配置项处，输入需要路由跟踪的目标 IP 地址或者主机名。

(4) 在“选择出接口”配置项处，选择去往目标 IP 地址或者主机名的设备接口。当选择“AUTO”时，表示设备自动选择某一接口转发 Tracert 报文。

(5) 在“源地址”配置项处，选择 Tracert 操作的源 IP 地址。当选择“AUTO”时，表示设备自动选择 Tracert 操作的源 IP 地址；当选择“源 IP 地址”时，需手动输入 Tracert 操作的源 IP 地址

(6) 点击<开始>按钮，系统开始进行检测。检测的过程和结果显示在当前页面。



14.2.4 系统自检

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(2) 单击“系统自检”页签，进入系统自检页面。

(3) 点击<自检>按钮，页面将会显示系统自检结果。

14.2.5 诊断

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(2) 单击“诊断”页签，进入搜集网络诊断信息页面。

(3) 点击<搜集诊断信息>按钮，系统开始收集诊断信息。

14.2.6 端口镜像

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(2) 单击“端口镜像”页签，进入端口镜像页面。

(3) 在“源端口”配置项处，选择镜像的源端口，即与数据监测设备相连的端口。

(4) 在“方向”配置项处，选择镜像的方向。

- 若选择“入方向”，表示仅复制源端口收到的报文。
- 若选择“出方向”，表示仅复制源端口发出的报文。
- 若选择“双方向”，表示对源端口收到和发出的报文都进行复制。

(5) 在“目的端口”配置项处，选择镜像的目的端口，即与数据监测设备相连的端口。

(6) 点击<确定>按钮，系统开始端口镜像。

14.2.7 抓包工具

1. 配置步骤

(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(2) 单击“抓包工具”页签，进入抓包工具页面。

(3) 在“接口”配置项处，选择需要抓取数据的接口，支持当前路由器的所有的 WAN、VLAN 等接口。

(4) 在“抓包长度”配置项处，输入数据包的抓取长度，单位为字节。如果数据包长度大于此数值，数据包将会被截断。需要注意的是，采用长的抓取长度，会增加包的处理时间，并且会减少可缓存的数据包的数量，从而会导致数据包的丢失。所以，在能抓取我们想要的包的前提下，抓取长度越小越好。

(5) 在“协议类型”配置项处，选择需要过滤的协议类型。如果选择 ALL，将抓取当前接口下所有报文。

(6) 在“抓包文件大小”配置项处，输入抓取报文的大小，单位为 MB。

(7) 在“抓包时间”配置项处，输入抓包的持续时长，单位为秒。

(8) 在“方向”配置项处，选择抓取报文的方向。主要分为：

- 入方向：表示仅抓取端口收到的报文。
- 出方向：表示仅抓取端口发送的报文。
- 双向：表示抓取端口收到和发送的报文。缺省为双向。

(9) 在“源主机”、“目的主机”、“过滤主机”配置项处，选择抓取报文时过滤发出或者接收报文的主机。

- 所有主机：对源或者目的主机进行过滤，即抓取所有的源/目的主机的报文。
- IP 地址过滤：选择此项时，需设置主机的 IP 地址。
- MAC 地址过滤：选择此项时，需设置主机的 MAC 地址。

(10) 点击<开始>按钮，系统开始进行抓包。抓包的过程和当前抓取的分组数显示在当前页面，在抓包的过程中，您可以点击<取消>按钮，终止当前的操作，并导出抓取的文件“capture-******.pacp”。

14.3 远程管理

14.3.1 简介

远程管理功能既可以用来检测网络的连通性，又可以为用户提供登录设备、管理设备的方式。远程管理功能包括：

- Ping：通过 ping 功能，可以检测网络的连通性，及时了解网络状况。

- Telnet：是一种实现远程登录服务的协议。用户可以在 PC 上通过 Telnet 方式登录设备，对设备进行远程管理。
- HTTP/HTTPS：是基于 HTTP、HTTPS 超文本传输协议的两种 Web 登录方式。HTTPS 登录方式的安全性能高于 HTTP 登录方式。用户可以在 PC 上使用 HTTP/HTTPS 协议登录设备的 Web 界面，通过 Web 界面直观地配置和管理设备。
- 云服务：实现设备在云平台中被管理。

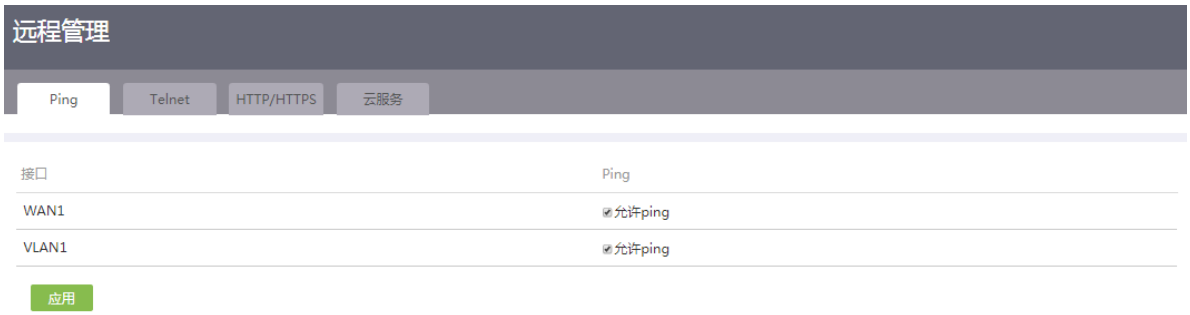
14.3.2 配置 Ping

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理页面。

(2) 单击“Ping”页签。

(3) 在列表中通过勾选接口对应的“允许 ping”选项，设置该接口允许接收 Ping 报文。

(4) 点击<应用>按钮，完成配置。



14.3.3 配置 Telnet

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。

(2) 单击“Telnet”页签，进入 Telnet 配置页面。

(3) 在“Telnet 服务”配置项处，点击按钮，使得按钮状态为“ON”，开启 Telnet 服务。

(4) 在“IPv4 端口”配置项处，输入 Telnet 方式远程管理设备的端口号，外部用户通过此端口 Telnet 方式登录设备进行管理。

(5) 在“管理员列表”区段，点击<添加/编辑>按钮，弹出添加/编辑管理员列表对话框。

a. 在“IP 地址”配置项处，输入允许通过 Telnet 访问设备的 IP 地址。

b. 在 IP 地址段“起始”和“结束”配置项处，分别输入允许通过 Telnet 访问设备的 IP 地址段的起始地址和结束地址。

c. 在“排除地址”配置项处，输入不允许通过 Telnet 访问设备的 IP 地址。

d. 点击配置项右侧的<→→>按钮，提交配置的地址段内容。

e. 重复 a、b、c、d 步骤可完成多个地址段的添加。

(6) 点击<确定>按钮，完成配置。

14.3.4 配置 HTTP/HTTPS

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。

(2) 单击“HTTP/HTTPS”页签，进入 HTTP/HTTPS 配置页面。

(3) 在“HTTP 登录端口”配置项处，输入 HTTP 方式登录设备对应的端口号，建议使用 10000 以上的端口号。

(4) 在“HTTPS 登录端口”配置项处，输入 HTTPS 方式登录设备对应的端口号，建议使用 10000 以上的端口号。

(5) 在“登录超时时间”配置项处，输入 Web 管理页面的闲置超时时间，缺省为 10 分钟。管理员登录 Web 管理页面后，当闲置时间超过登录超时时间时，系统会自动注销该管理员。配置此参数后，在管理员下一次登录时生效。

(6) 当允许所有用户访问 WEB 时，可勾选“允许所有用户访问 WEB”选项来设置。

(7) 在“VLAN1 管理地址”区段，点击<编辑>按钮，添加允许访问 Web 管理页面的管理员 IP 地址或地址段。在弹出的编辑 VLAN1 管理地址对话框中进行如下操作：

a. 在“IP 地址”配置项处，输入允许通过 HTTP/HTTPS 访问设备的 IP 地址。

b. 在 IP 地址段“起始”和“结束”配置项处，分别输入允许通过 HTTP/HTTPS 访问设备的 IP 地址段的起始地址和结束地址。

c. 点击配置项右侧的<→→>按钮，提交配置的地址段内容。

d. 重复 a、b、c 步骤可完成多个地址段的添加。

e. 点击<确定>按钮，完成配置。

(8) 在“自定义管理地址”区段，点击<添加/编辑>按钮，添加允许访问 Web 管理页面的管理员 IP 地址或地址段。在弹出的添加/编辑自定义管理地址对话框中进行如下操作：

a. 在“IP 地址”配置项处，输入允许通过 HTTP/HTTPS 访问设备的 IP 地址。

b. 在 IP 地址段“起始”和“结束”配置项处，分别输入允许通过 HTTP/HTTPS 访问设备的 IP 地址段的起始地址和结束地址。

c. 在“排除地址”配置项处，输入不允许通过 HTTP/HTTPS 访问设备的 IP 地址。

d. 点击配置项右侧的<→→>按钮，提交配置的地址段内容。

e. 重复 a、b、c、d 步骤可完成多个地址段的添加。

f. 点击<确定>按钮，完成配置。

14.3.5 配置云服务

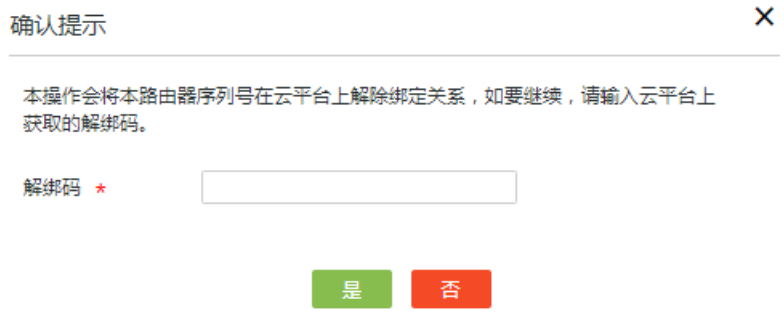
(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。

(2) 单击“云服务”页签，进入云服务配置页面。

(3) 点击<云服务解绑>按钮，在弹出的确认提示对话框中进行如下操作：

a. 在“解绑码”配置项处，输入从云平台上获取的解绑码。

b. 点击<是>按钮，完成配置。



(4) 在“云服务”配置项处，点击按钮，使得按钮状态为“ON”，开启云服务。

(5) 在“云平台服务器域名”配置项处，输入 H3C 云简网络平台的域名。

(6) 在“云场所定义”配置项处，输入设备的系统名称。云场所定义长度为 1-255 个字符，只支持数字、字母、下划线、中划线和空格，不能为中文，不能为全空格。

(7) 点击<应用>按钮，完成配置。

14.4 配置管理

14.4.1 简介

本功能用于对设备的配置文件进行管理。配置文件是指用来保存设备配置的文件。

主要功能包括：

- 恢复出厂配置：如果设备没有配置文件或者配置文件损坏时，希望设备能够正常启动运行，则需通过本功能将设备上的配置恢复到出厂状态。
- 从备份文件恢复：设备配置错误后，如果希望设备恢复到正确配置运行状态，则需通过本功能恢复设备配置。
- 导出当前配置：如果希望将当前配置文件导出作为备份配置文件，则需通过本功能将当前配置文件导出保存到指定路径。
- USB 快速备份：备份设备当前的配置到 U 盘上。
- USB 快速恢复：通过 U 盘中配置文件恢复设备配置。

14.4.2 恢复出厂配置

1. 注意事项

恢复到出厂设置后，当前的设置将会丢失。如果您不希望丢失当前设置信息，请先对路由器进行备份操作。恢复出厂设置后，路由器将会重新启动。在此期间请勿断开设备的电源。

2. 配置步骤

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“恢复出厂配置”页签，进入恢复出厂配置页面。

(3) 点击<恢复出厂配置>按钮，弹出恢复出厂配置对话框。

(4) 勾选“立即重启设备”选项，系统会立即重启设备。

(5) 点击<确定>按钮，完成恢复出厂配置并强制重启设备。

14.4.3 从备份文件恢复

1. 注意事项

- 从备份文件恢复设备配置时，需选择后缀名为.rar 的文件。
- 在恢复设备配置的过程中，请确保设备供电正常。
- 恢复设备配置完成后，设备会自动根据新的配置重新启动。

2. 配置步骤

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份/恢复配置”页签，进入备份恢复配置页面。

(3) 点击<从备份文件恢复>按钮，进入从备份文件恢复页面。

(4) 点击“选择文件”按钮，选择特定路径下的备份配置文件。

(5) 点击<确定>按钮，弹出确认提示对话框。

(6) 点击<确定>按钮，开始恢复配置。

14.4.4 导出当前配置

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份/恢复配置”页签，进入备份恢复配置页面。

(3) 点击<导出当前配置>按钮，选择保存路径，即可将当前配置保存到本地 PC。

14.4.5 USB 快速备份

1. 配置准备

- 目前仅支持 fat32 格式的 U 盘。
- 在执行快速恢复前，需先将 U 盘插入到设备上。

2. 注意事项

- 如果 U 盘存在多个分区，备份的配置文件将会保存在第一个分区中。
- 备份成功后的配置文件名称为 backup.data，如果多次执行 USB 快速备份操作，系统会覆盖之前的配置文件，即 U 盘中仅存在一个 backup.data 配置文件。

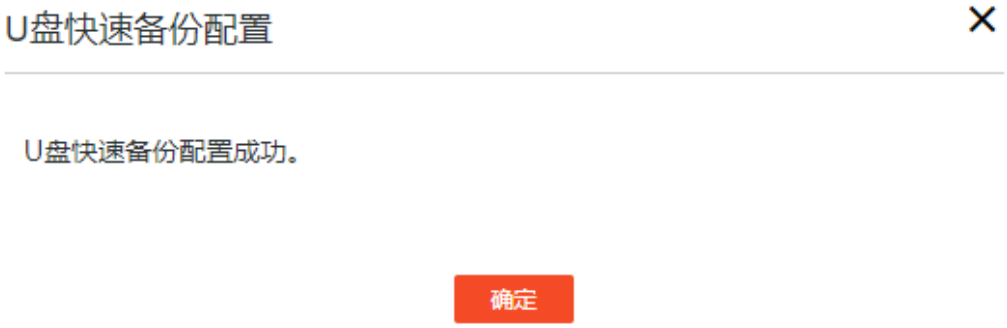
3. 配置步骤

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份/恢复配置”页签，进入备份恢复配置页面。

(3) 点击<USB 快速备份>按钮，开始备份配置。

(4) 备份完成后，在弹出备份配置成功的确认对话框中，点击<确定>按钮，关闭对话框。



14.4.6 USB 快速恢复

1. 配置准备

- 目前仅支持 fat32 格式的 U 盘。
- 在执行快速恢复前，需先将 U 盘插入到设备上，且该 U 盘中存有名称为 backup.data 的设备配置文件。设备将通过 backup.data 配置文件恢复设备配置。
- 如果 U 盘存在多个分区，用于恢复设备配置的配置文件 backup.data 需保存在第一个分区中。

2. 注意事项

- 在恢复设备配置的过程中，请确保设备供电正常。
- 恢复设备配置完成后，设备会自动根据新的配置重新启动。

3. 配置步骤

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份/恢复配置”页签，进入备份恢复配置页面。

(3) 点击<USB 快速恢复>按钮，开始恢复配置。

(4) 恢复完成后，在弹出恢复配置成功的确认对话框中，点击<确定>按钮，关闭对话框。

14.5 系统升级

14.5.1 简介

本功能用于对设备版本进行升级。如果希望完善当前软件版本漏洞或者更新应用功能，则需通过版本升级功能来实现。升级方式分为如下两种：

- 手动升级是通过特定路径下的系统软件文件对设备的系统软件进行升级。

- 自动升级是通过 H3C 云简网络平台对设备的系统软件进行升级。自动升级前，请确保设备与云平台已经连接。

14.5.2 注意事项

- 请您在软件升级之前备份路由器当前的设置信息。如果升级过程中出现问题，您可以用其来恢复到原来的设置。
- 上传完成后，设备自动更新软件，完成后将重新启动。
- 升级过程中请勿给路由器断电，否则可能会造成路由器不能正常工作。

14.5.3 手工升级

1. 注意事项

手工升级前，请先到“网络安全->DDOS 攻击防御->异常流量防护”页面确认是否启用了异常主机流量防护功能。如果已启用，需关闭异常主机流量防护功能后，再进行手工升级，否则将无法进行手工升级。

2. 配置步骤

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。

(2) 单击“手工升级”页签，进入手工升级配置页面。

(3) 点击<手工升级系统软件>按钮，弹出手工升级系统软件对话框。

(4) 点击<选择文件>按钮，选择特定路径下的系统软件文件。

(5) 若需要设备在升级系统软件之后恢复出厂配置，则勾选“恢复出厂配置”选项；若无需设备在升级系统软件之后恢复出厂配置，则不勾选“恢复出厂配置”选项。

(6) 点击<确定>按钮，开始软件升级。

14.5.4 立即自动升级

1. 配置步骤

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。

(2) 单击“自动升级”页签，进入自动升级配置页面。

(3) 点击<自动升级系统软件>按钮，弹出升级软件系统对话框。

(4) 点击<确定>按钮，进行升级操作。

14.5.5 预约自动升级

1. 注意事项

在进行自动升级前，需确保云连接状态为已连接，否则自动升级将会不成功。

2. 配置步骤

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。

(2) 单击“自动升级”页签，进入自动升级配置页面。

(3) 在“预约升级”配置项处，选择开启。

(4) 在“检测时间限制”配置项处，设置检测的时间，系统会根据设置的时间检测是否存在新版本软件。如果检测到新版本软件，系统将立即升级软件。

(5) 点击<应用>按钮，完成自动升级设置。

(6) 在“预约升级日志”配置项处，点击<查看>按钮，查看预约升级的日志信息。

14.5.6 使用 U 盘恢复软件版本

路由器使用过程中出现异常情况，例如升级过程中断电、设备无法正常运行等，可以使用 U 盘恢复软件版本。

注意

使用 U 盘恢复软件版本后，路由器将会恢复出厂设置，请谨慎使用此功能。

恢复方法如下：

(1) 准备文件格式为 FAT32，接口为 USB 2.0 或者 USB 3.0（同时向下兼容 USB 2.0）的 U 盘。

(2) 将待恢复的软件（后缀名为.bin）拷贝到 U 盘。在 U 盘中将.bin 文件命名为“recover.bin”。

(3) 先对路由器断电，再将 U 盘插入路由器的 USB 接口。

(4) 将路由器接通电源，等待 10 分钟左右，路由器正常启动后，即可重新登录。

14.6 重新启动

14.6.1 简介

重新启动功能用于立即和定时重新启动设备。

14.6.2 立即重启

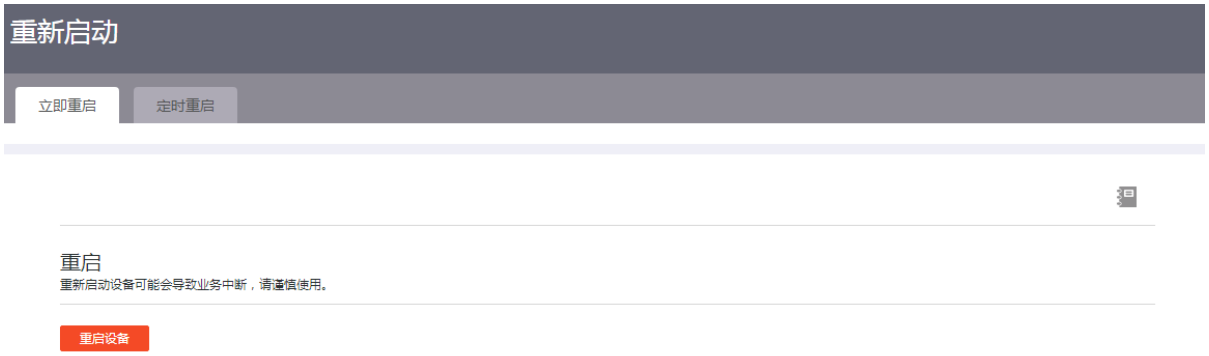
1. 注意事项

重新启动设备可能会导致业务中断，请谨慎使用。

2. 配置步骤

(1) 单击导航树中[系统工具/重新启动]菜单项，进入重新启动配置页面。

(2) 在“立即重启”页签下，点击<重新启动设备>按钮，在弹出的确认提示对话框中，点击<是>按钮，立即重新启动设备。



14.6.3 定时重启

1. 注意事项

在使用定时重启功能之前，需在“系统设置—日期和时间—自动同步网络日期和时间”中配置 NTP 服务器。

2. 配置步骤

(1) 单击导航树中[系统工具/重新启动]菜单项，进入重新启动配置页面。

(2) 单击“定时重启”页签，进入定时重启配置页面。

(3) 在“定时重启”配置处，选择“开启”选项。开启定时重启设备的功能。

(4) 在“生效周期”配置处，设定每周设备重启的具体时间。

(5) 点击<确定>按钮，设备将会在设定时间进行重启。

14.7 系统日志

14.7.1 简介

设备在运行过程中会生成系统日志。日志中记录了管理员在设备上进行的配置、设备的状态变化以及设备内部发生的重要事件等，为用户进行设备维护和故障诊断提供参考。

用户可以将日志发送到日志服务器集中管理，也可以直接在 Web 页面查看日志。

日志划分为如表 14-1 所示的五个级别，各级别的严重性依照数值从 0～4 依次降低。了解日志级别，能帮助您迅速筛选出重点日志。

表14-1 日志级别列表

数值	信息级别	描述
0	Error(0)	表示错误信息
1	Warning(1)	表示警告信息
2	Notification(2)	表示正常出现但是重要的信息
3	Informational(3)	表示需要记录的通知信息
4	Debugging(4)	表示调试过程产生的信息

14.7.2 将系统日志发往日志服务器

1. 配置准备

请确保设备和日志服务器能互相 ping 通，日志服务器才能收到设备发送的日志。

2. 配置步骤

(1) 单击导航树中[系统工具/系统日志]菜单项，进入系统日志配置页面。

(2) 在“日志记录等级”配置项处，选择日志记录的级别。

(3) 在“日志来源”配置项处，选择日志的来源，控制日志信息的输出。主要分为：

- 系统：记录设备运行中，记录所有功能模块的运行状态相关信息。缺省选择该参数，不可取消。
- 配置：记录设备配置发生变化的信息。
- 安全：记录设备防攻击、报文过滤、防火墙等相关信息。
- 流量信息：记录 IP、端口等流量信息。
- VPN：记录 VPN 相关信息。

(4) 根据需要勾选“是否将系统日志记录到存储介质”选项。

(5) 勾选“发送到日志服务器”选项，输入日志服务器的 IP 地址或者域名地址。

(6) 点击<应用>按钮，完成配置。

14.7.3 通过 Web 页面查看系统日志

(1) 单击导航树中[系统工具/系统日志]菜单项，进入系统日志配置页面。设备会逐条显示日志的生成时间、级别以及详细信息。

(2) 用户可使用高级查询功能，通过时间、级别、信息来源和详细信息这几个条件的任意组合来查找对应的系统日志。

(3) 点击<导出>按钮，可以将设备上已有的日志信息导出到登录 Web 管理页面的 PC 上。

14.7.4 清除系统日志

(1) 单击导航树中[系统工具/系统日志]菜单项，进入系统日志配置页面。

(2) 点击<清除>按钮，清除路由器所记录的日志信息。

15 管理员

15.1 简介

管理员设置功能是对登录设备的管理员账户信息进行管理，包括修改用户名和密码。

15.2 修改管理员

1. 注意事项

系统中仅能存在一个管理员账户。

仅允许修改管理员账户的名称和密码，不允许删除管理员账户。

2. 配置步骤

(1) 单击 Web 页面执行区域右上角的“管理员”图标，选择“设置”菜单项，进入管理员账户配置页面。

(2) 如果您需要修改当前管理员的用户名，请在“用户名”配置项处输入新用户名。需要注意的是，修改用户名后，您还必须修改当前管理员密码。

(3) 如果您需要修改当前管理员的密码，请依次执行以下操作：

a. 在“当前管理员密码”配置项处，输入旧密码。

b. 在“新密码”配置项处，输入新密码。密码设置规则如下：

- 密码长度为 10~63 个字符。
- 密码的组成元素包括以下 4 种类型：A～Z、a～z、0～9、特殊字符（空格 ~`!@#$%^&*()_+-={}|[]\:;'<>,./）。
- 至少包含 4 个不同的字符，且至少包含 2 种以上类型的字符。
- 不能包含用户名或者逆转用户名，且密码或倒序的密码是否为用户名的一部分，例如，用户名为 admin，则密码 admin12356、nimda12356 是不符合要求的。

c. 在“确认密码”配置项处，再次输入新密码，并确保与之一致。

(4) 如果您希望在此页面上显示帮助管理员记忆密码的提示信息，请在“密码提示”配置项处输入相关提示信息。

(5) 点击<确定>按钮，完成配置。


修改管理员
用户名 *
admin
（3-55 字符）
当前管理员密码 *
新密码 *
（10-63 字符）
确认密码 *
密码提示
（1-15 字符）
建议：强烈建议您填写密码提示，以便忘记密码后，根据密码提示找回密码。
确定
取消