目 录

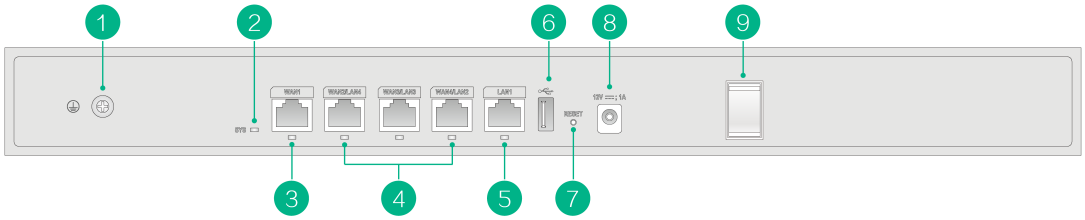
1 产品简介

H3C ER G3 系列路由器包括如下产品型号。

名称	具体型号
H3C ER G3系列路由器	ER3200G3、ER3208G3、ER3260G3、ER5200G3

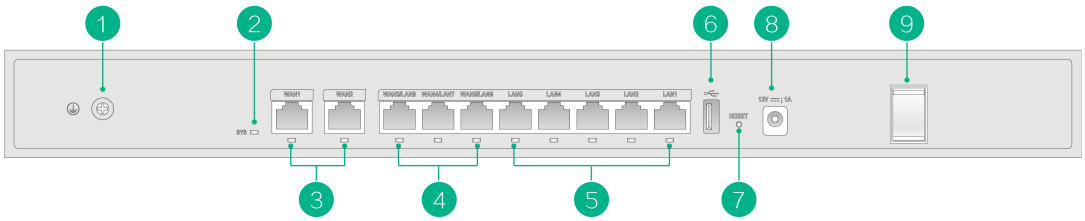
1.1 前面板

图1-1 ER3200G3 设备前面板



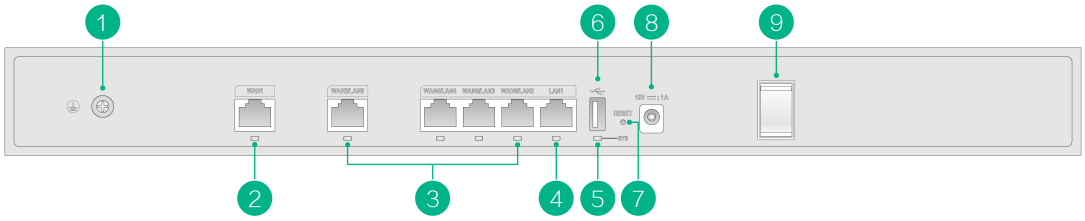
(1): 接地螺钉	(2): 系统指示灯（SYS）
(3): WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10/100/1000Base-T电口）
(5): LAN接口及指示灯（10/100/1000Base-T电口）	(6): USB接口
(7): 复位键（RESET）	(8): 电源接口
(9): 电源线固定卡扣	

图1-2 ER3208G3 设备前面板



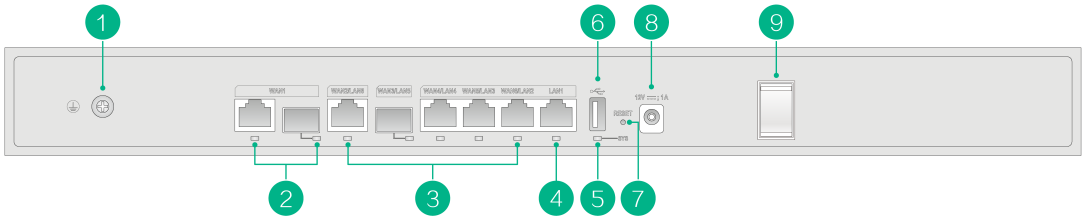
(1): 接地螺钉	(2): 系统指示灯（SYS）
(3): WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10/100/1000Base-T电口）
(5): LAN接口及指示灯（10/100/1000Base-T电口）	(6): USB接口
(7): 复位键（RESET）	(8): 电源接口
(9): 电源线固定卡扣	

图1-3 ER3260G3 设备前面板



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

图1-4 ER5200G3 设备前面板



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

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
	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）	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
SFP接口状态指示灯	绿色常亮	端口正常连接设备，且工作在1000Mbps速率下

指示灯	状态	含义
	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

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 秒左右，SYS 指示灯黄色慢速闪烁（1Hz），设备将恢复缺省 Web 登录密码 • 按住 10 秒左右，SYS 指示灯黄色快速闪烁（8Hz），设备将恢复出厂设置并重启 • 按住 15 秒左右，SYS 指示灯恢复到绿色常亮，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，以及恢复版本软件
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

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：

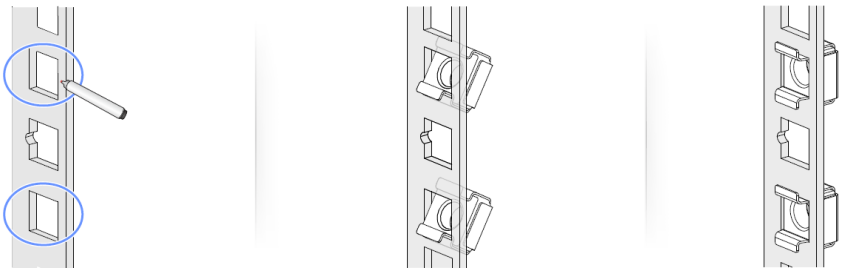
- 设备仅允许在室内使用，请将其放置于干燥通风处；
- 设备的接口线缆要求在室内走线，禁止户外走线，以防止因雷电产生的过电压、过电流损坏设备的信号口；
- 请不要将设备放在不稳定的箱子或桌子上，一旦跌落，会对设备造成损害；
- 在设备周围应预留足够的空间（大于 10cm），以便于设备正常散热；
- 请保证设备工作环境的清洁，过多的灰尘会造成静电吸附，不但会影响设备寿命，而且容易造成通信故障；
- 设备工作地最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；
- 设备工作地应远离强功率无线电发射台、雷达发射台、高频大电流设备；
- 请使用随产品附带的电源线，严禁使用其它非配套产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

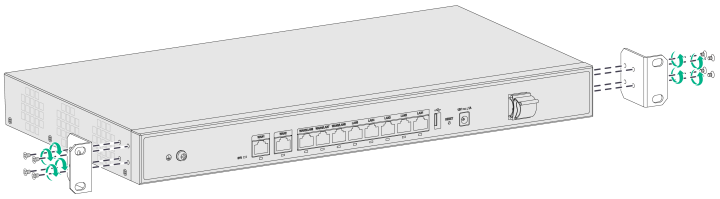
设备支持机柜安装和工作台安装两种方式，本文的安装过程以 ER3208G3 设备举例。

1.5.1 安装到机柜

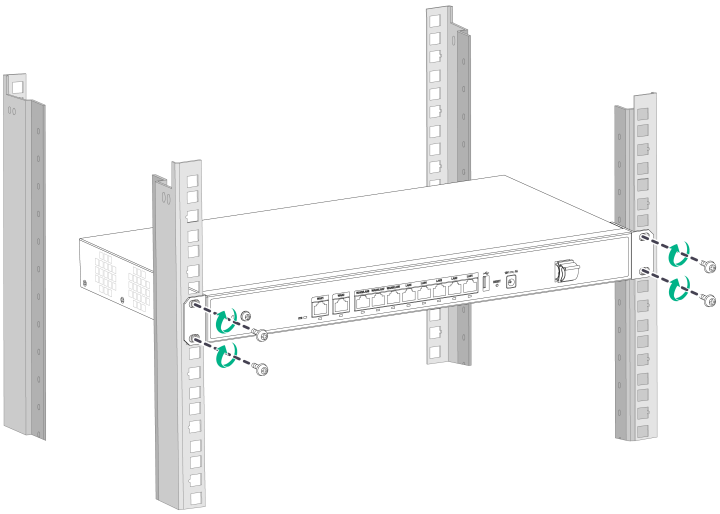
1. 安装浮动螺母



2. 安装挂耳



3. 安装设备到机柜

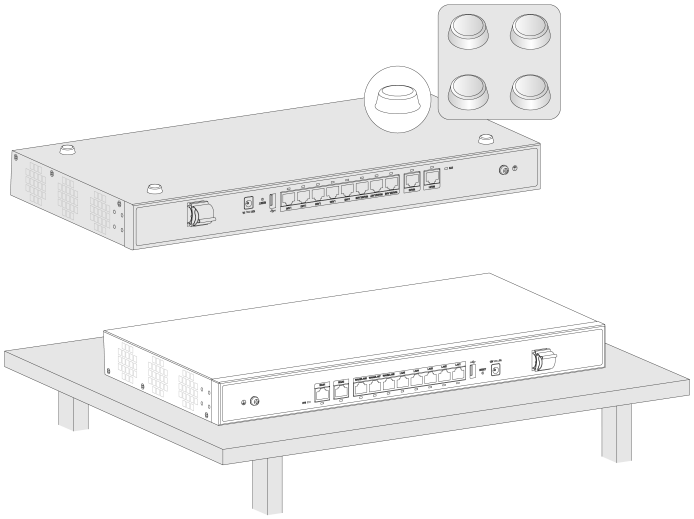


1.5.2 安装到工作台

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。

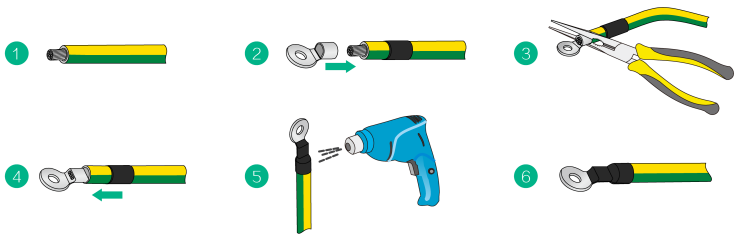


1.6 连接线缆

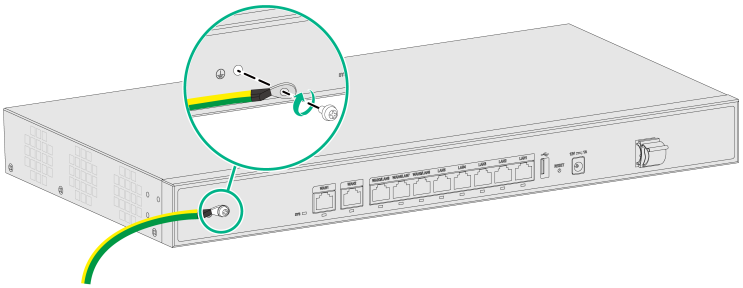
1.6.1 连接接地线

1. 装配 OT 端子

设备随机不提供接地线和 OT 端子，需要用户自行购买安装。

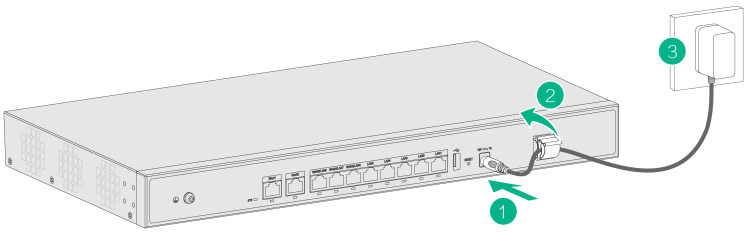


2. 连接接地线



1.6.2 连接电源线

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。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	ER3200G3	ER3208G3	ER3260G3	ER5200G3
外形尺寸（宽×深×高）	440mm×230mm×44mm			
功耗	＜10W	＜12W	＜10W	＜12W
电源	100V AC～240V AC，50/60Hz			
重量	3Kg			
USB接口	1个USB2.0接口			
LAN接口	1个	5个	1个	1个
LAN/WAN接口	3个	3个	4个	5个
WAN接口	1个千兆电口	2个千兆电口	1个千兆电口	1个Combo口
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

- 将计算机连接到设备的 LAN 接口。
- 配置计算机为自动获取 IP 地址或手工配置计算机的 IP 地址和 192.168.1.1/24 在同一网段。
- 检查计算机的代理服务设置情况。如果当前计算机使用代理服务器访问互联网，则首先必须禁止代理服务。
- 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。
- 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。输入旧密码、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

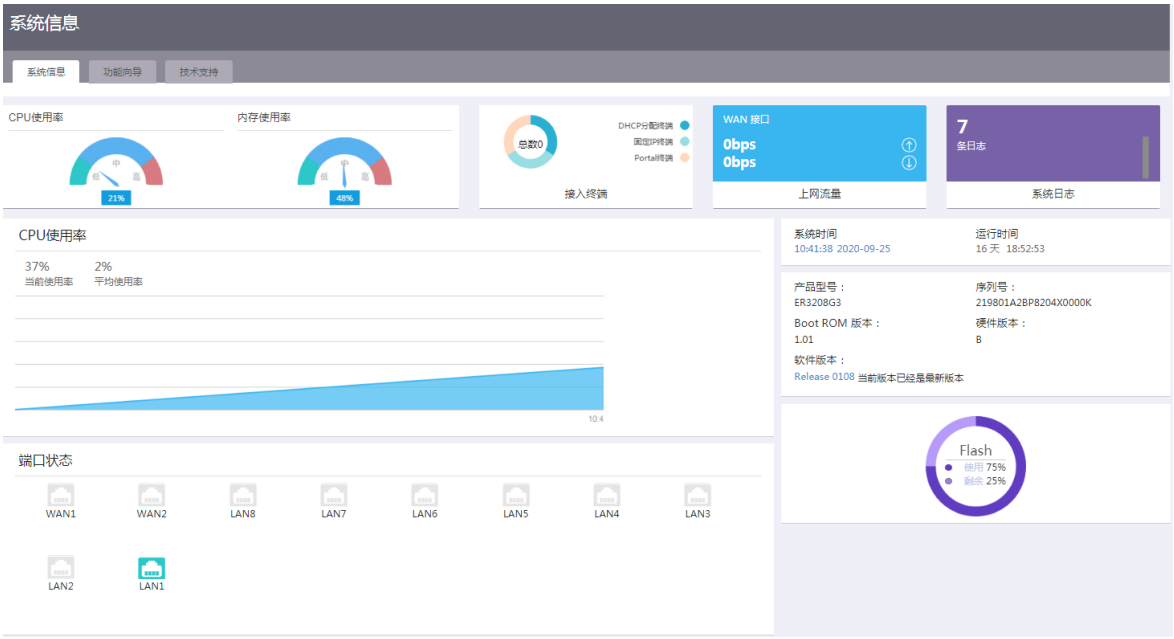
3.1 简介

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 系统信息

通过该功能可以查看设备的运行情况。

(1) 单击导航树中[系统信息]菜单项，进入系统信息页面。



3.3 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)设置：单击“局域网(LAN)设置”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页面。
- 接入安全
  - 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。
  - ARP 安全：单击“ARP 安全”链接，页面自动跳转至 ARP 安全页面。
- 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。
- 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。
- 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。

4 快速设置

4.1 简介

通过快速设置完成广域网 WAN 和局域网 LAN 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）。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。

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) 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：

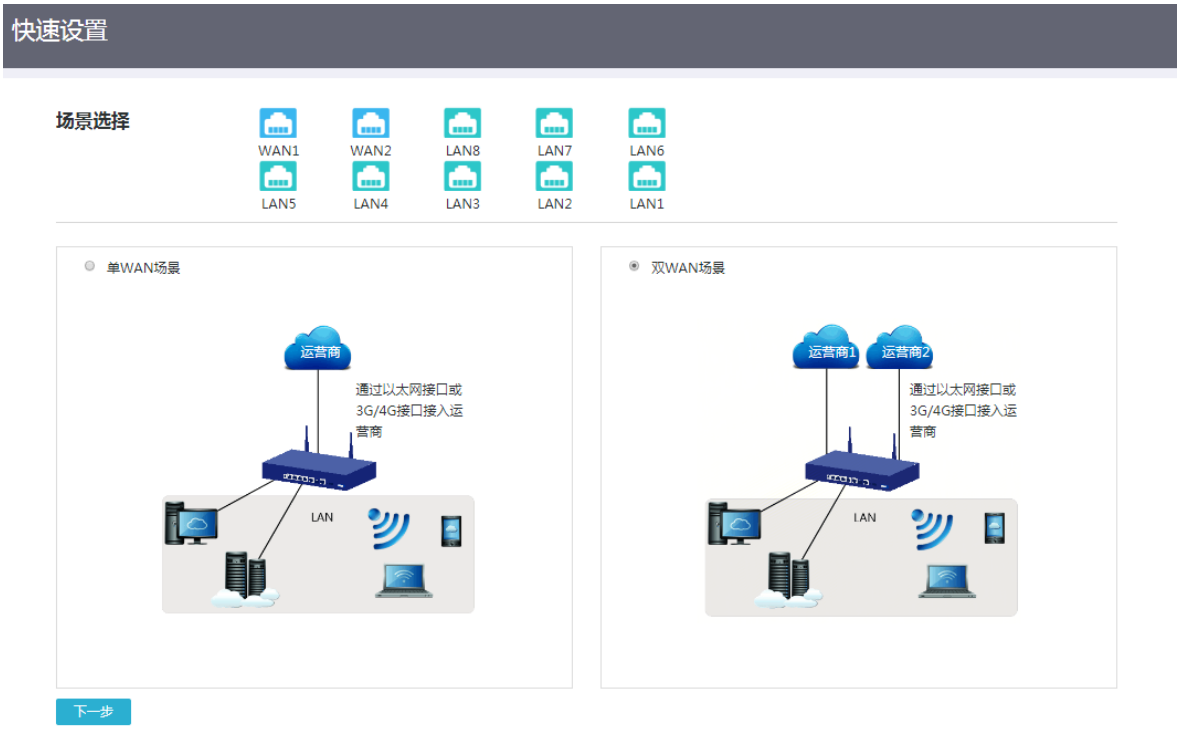
- 如果选择连接模式为“PPPoE”：
  - 在“上网账号”配置项处，输入运营商提供的 PPPoE 接入用户名。

- 在“上网密码”配置项处，输入运营商提供的 PPPoE 接入密码。

- 如果选择连接模式为“DHCP”，将自动从 DHCP 服务器获取接入广域网的公网 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。
  - 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。
  - 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。

(4) 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。

(5) 点击<下一步>按钮，完成 WAN 配置。




快速设置
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
DNS2
NAT地址转换
开启
上一步
下一步


快速设置
双WAN配置
线路1 *
WAN1
连接模式 *
PPPoE
上网帐号
admin
(1-80字符)
上网密码
(1-255字符)
NAT地址转换
开启
线路2 *
WAN2
连接模式 *
PPPoE
上网帐号
test
(1-80字符)
上网密码
(1-255字符)
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。

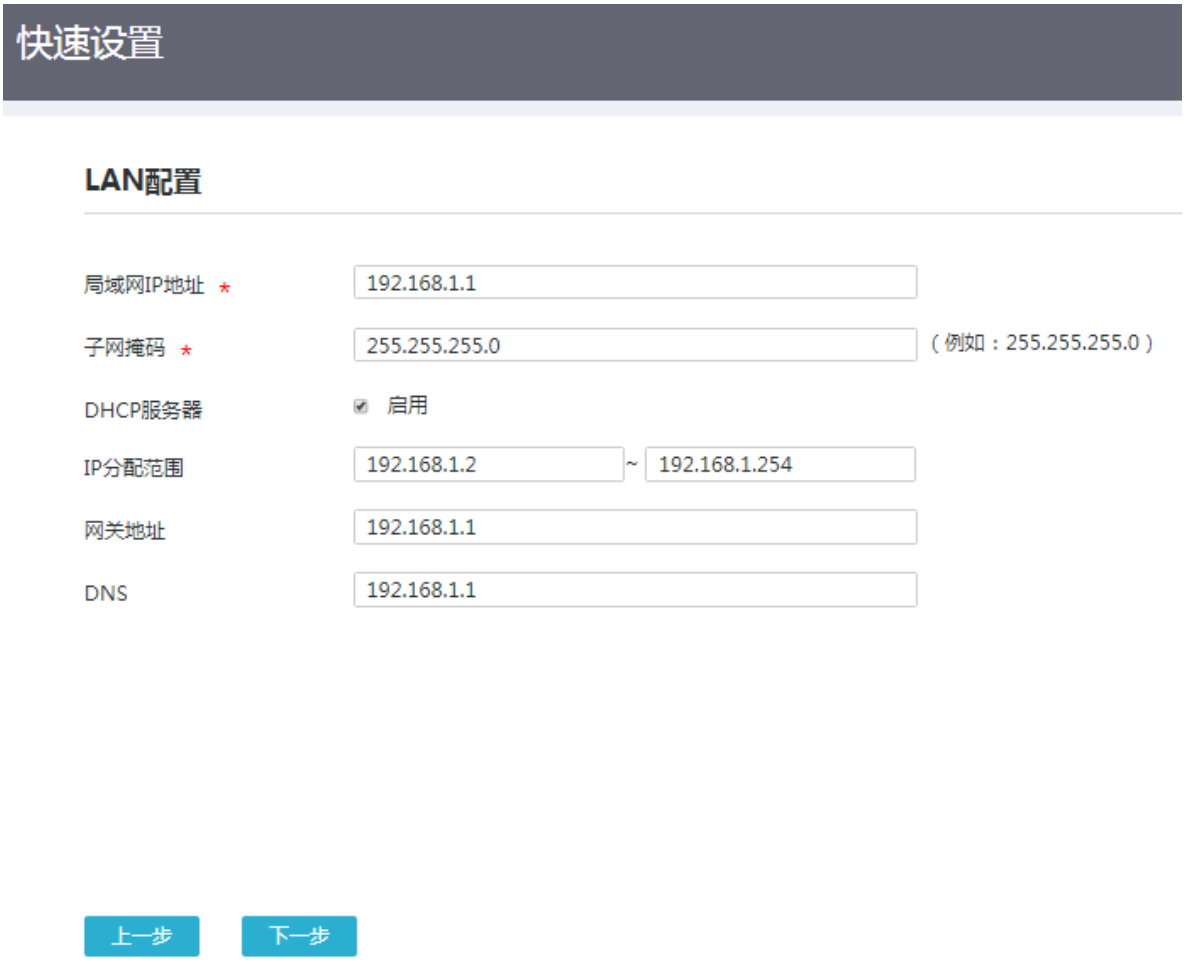
(1) 在“局域网 IP 地址”配置项处，输入设备在局域网中使用的 IP 地址。

(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。

(3) 在“DHCP 服务器”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) 点击<下一步>按钮，完成 LAN 配置。



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

流量排行功能用来查看终端流量排行，方便管理员对用户的上网行为进行分析与审计。

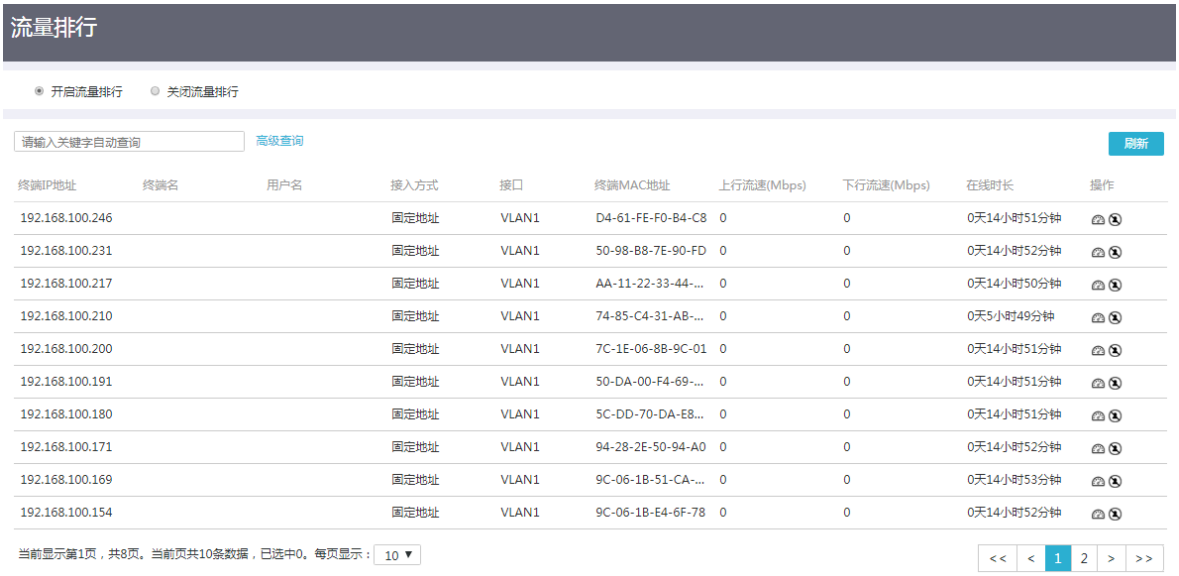
5.2.2 注意事项

流量排行表中只会显示近 5 分钟内连接过设备的终端流量统计信息。

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。



6 MiniAP 管理

6.1 AP管理设置

6.1.1 简介

您可通过开启 AP 管理功能，集中管理不同 VLAN 下接入的 AP 设备。

6.1.2 注意事项

AP 管理功能的默认管理 VLAN 为 VLAN1，如需选择其他 VLAN，请先单击导航树中的[网络设置]菜单项，进入 LAN 配置页面进行配置。

6.1.3 配置步骤

(1) 单击导航树中[MiniAP 管理/AP 管理设置]菜单项，进入 AP 管理设置页面。
(2) 在“AP 管理功能”配置项处，选择“启用”。
(3) 在“AP 管理使用 VLAN”配置项处，选择设备需要管理的 VLAN。
(4) 在“AP 管理地址”配置项处，输入管理 AP 的 IP 地址。
(5) 在“AP 管理子网掩码”配置项处，输入管理 AP 的子网掩码。
(6) 在“地址池起始地址”配置项处，选择 AP 上线后获取 IP 地址的地址池起始地址。
(7) 在“地址池结束地址”配置项处，选择 AP 上线后获取 IP 地址的地址池结束地址。
(8) 点击<确定>按钮，开启 AP 管理设置服务。

6.2 在线AP管理

6.2.1 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。本页面显示 AP 设备与客户端的详细信息，支持管理客户端的上线状态。用户可使用在线 AP 管理功能，选择 AP 绑定的服务模板，手动升级 AP 版本或 AP 同步 AC 下发的配置。

6.2.2 在线 AP 列表

1. 注意事项

- 使用版本升级功能之前，请先将 AP 升级需要使用的软件版本上传到设备中。具体操作步骤，请单击导航树中[MiniAP 管理/版本管理]菜单项，进入版本管理页面进行相关配置。
- 未开启“强制 AP 和管理器上的版本一致”功能时，版本升级功能仅用于 AP 设备从低版本到高版本的升级操作。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/在线 AP 管理]菜单项，进入在线 AP 管理页面。

(2) 单击“在线 AP 列表”页签，进入在线 AP 列表页面。

(3) 在关键字自动查询配置项处，输入待查询 AP 设备的关键字，页面会自动显示出与关键字相关的 AP 设备列表。

(4) 单击“高级查询”按钮，进入高级查询配置页面，本页面可设定与 AP 设备相关的多个筛选条目，点击<查询>按钮，完成查询。

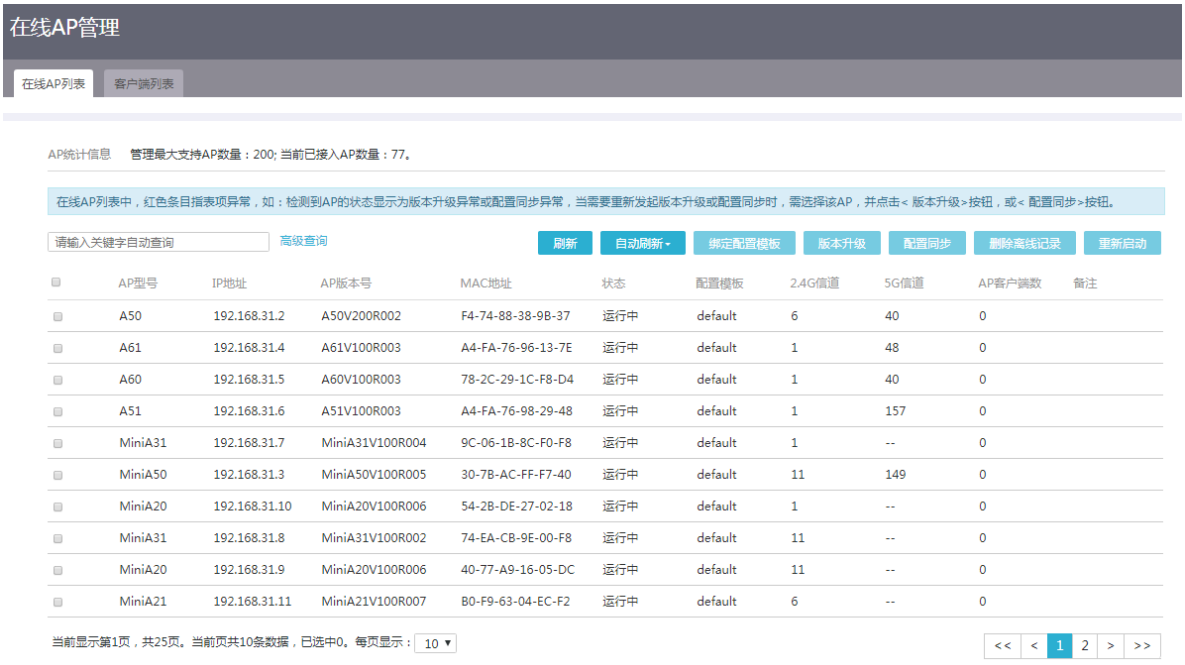
(5) 点击<刷新>按钮，完成在线 AP 列表的刷新。

(6) 在“自动刷新”配置项处，可设置在线 AP 列表自动刷新的时间。

(7) 勾选 AP 型号前的复选框，可进行如下功能配置：

- 点击<绑定配置模板>按钮，选择 AP 绑定的服务模板。
- 点击<版本升级>按钮，AC 下发软件版本并升级该 AP 设备。
- 点击<配置同步>按钮，手动触发 AP 同步 AC 下发的配置。
- 点击<删除离线记录>按钮，删除离线设备的状态显示项。
- 点击<重启>按钮，重启 AP 设备。

(8) 在“每页显示”配置项处，设置当前显示页面的 AP 数据条数。



6.2.3 客户端列表

1. 配置步骤

(1) 单击导航树中[MiniAP 管理/在线 AP 管理]菜单项，进入在线 AP 管理页面。

(2) 单击“客户端列表”页签，进入客户端列表配置页面。

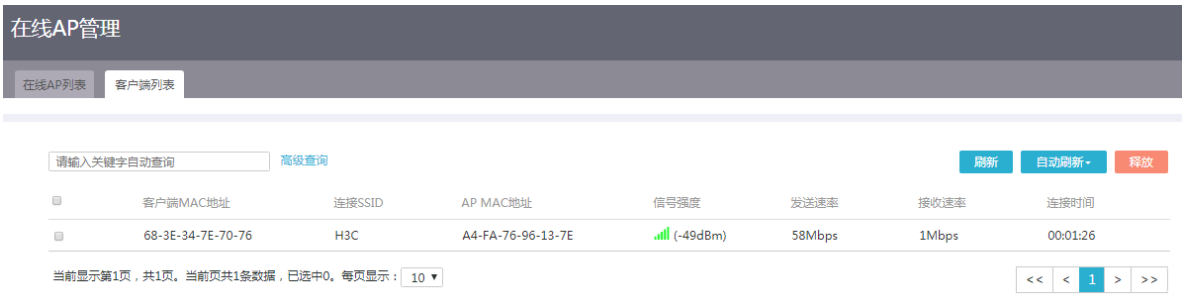
(3) 在关键字自动查询配置项处，输入待查询客户端的关键字，页面会自动显示出与关键字相关的客户端列表。

(4) 单击<高级查询>按钮，进入高级查询配置页面，本页面可设定与客户端相关的多个筛选条目，点击<查询>按钮，完成查询。

(5) 点击<刷新>按钮，完成在线客户端列表的刷新。

(6) 在“自动刷新”配置项处，设置在线客户端列表自动刷新的时间。

(7) 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。



6.3 配置管理

6.3.1 简介

当您需要手动增加 AP、修改无线网络各种参数以便对无线网络进行优化或需要进行无线漫游时，可以使用配置管理功能。

为了方便您进行快速设置，设备提供了一套缺省的无线服务模板“default”。defalt 模板中提供了一个 2.4G 网络配置和一个 5G 网络配置，您可以在“无线基本配置”页签”中对 SSID 名称、加密方式、共享密钥和无线信道四项参数进行配置。如果您想配置 default 模板的更多参数（无线网络模式、无线网络频宽、发射功率、修改 SSID 配置等）或创建及修改新的无线服务模板，可以到“配置模板管理”页签配置。

配置完无线服务模板后，如果需要增加手工 AP 或为上线的 AP 分配无线服务模板，请到“AP 配置管理”页签中配置。

完成上述配置后，如果对无线网络还有二层漫游、禁止弱信号客户端接入以及关闭广播探测等高级需求，请到“无线高级配置”页签下进行配置。

6.3.2 无线基本配置

1. 配置简介

无线基本配置主要对 default 模板中 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

- 修改服务模板中的加密方式、共享配置密钥等无线服务属性后，如 AP 中的配置未自动同步，需要手动点击<配置同步>按钮，将配置下发到 AP 设备。如需使用<配置同步>功能，请参考“在线 AP 管理”的联机帮助。
- 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[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“无线基本配置”页签，进入无线基本配置页面。

(3) 配置无线网络 SSID 设置-2.4G：

- 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。
- 在“中文编码”配置项处，选择中文编码的方式。当配置的“SSID-1 名称”包含中文字符，必须配置此参数。通过 iOS 系统接入无线网络时，此处推荐使用“GB2312”编码方式；通过 Android 系统接入无线网络时，此处推荐使用“UTF-8”编码方式。
- 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。
- 为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户接入网络时需要输入此密钥。当您选择通过加密方式接入无线服务时，需要设置共享密钥。

(4) 配置无线网络 SSID 设置-5G：

- 在“5G-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“中文编码”配置项处，选择中文编码的方式。当配置的“SSID-1 名称”包含中文字符，必须配置此参数。通过 iOS 系统接入无线网络时，此处推荐使用“GB2312”编码方式；通过 Android 系统接入无线网络时，此处推荐使用“UTF-8”编码方式。
- 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。
- 为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
- 在“共享密钥”配置项处，输入无线服务密钥，无线用户接入网络时需要输入此密钥。当您选择通过加密方式接入无线服务时，需要设置共享密钥。

(5) 点击<应用>按钮，完成配置。

6.3.3 配置模板管理

说明

一个模板可以配置多个 SSID，最多配置 8 个 2.4G 的 SSID 和 8 个 5G 的 SSID。如果 AP 支持 N 个 SSID（N 小于等于 8），则 AP 只会同步前 N 个 SSID。

1. 配置简介

配置模板管理用来配置 default 模板的更多参数（无线网络模式、无线网络频宽、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. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“配置模板管理”页签，进入配置模板管理页面。

(3) 点击<添加>按钮，弹出添加配置模板对话框。

- 在“模板名称”配置项处，输入无线服务模板的名称。
- 在“模板描述”配置项处，输入该无线服务模板的相关描述信息。
- 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。需要注意的是，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。
  - 点击<添加>按钮，弹出添加 SSID 配置对话框。
  - 勾选“启用 SSID”复选框，在“SSID 名称”配置项处，输入 2.4G 无线服务的 SSID 名称。
  - 在“中文编码”配置项处，选择中文编码的方式。当配置的“SSID-1 名称”包含中文字符，必须配置此参数。通过 iOS 系统接入无线网络时，此处推荐使用“GB2312”编码方式；通过 Android 系统接入无线网络时，此处推荐使用“UTF-8”编码方式。
  - 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。
  - 为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
  - 在“共享密钥”配置项处，输入无线服务密钥。
  - 当您选择通过加密方式接入无线服务时，需要设置共享密钥。
  - 在“加密协议”配置项处，选择加密机制来保护您的数据安全。
  - 设备提供的加密协议包括 TKIP、AES 及 TKIP+AES。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，设置加密密钥更新周期。
  - 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，请勾选高级设置复选框。启用客户端隔离功能可以开启基于 SSID 的用户隔离，即对使用同一公共无线服务进行通信的用户进行报文隔离，从而达到提高用户安全性、缓解设备转发压力和减少射频资源消耗的目的；启用 SSID 广播功能时，AP 将 SSID 置于 Beacon 帧中向外广播发送。若 BSS 一段时间内不可用即客户端不能上线或不希望其它客户端上线，则可以配置关闭 SSID 广播。若关闭 SSID 广播，AP 在 Beacon 帧中广播的 SSID 信息为空，可以借此保护网络免遭攻击。为了进一步保护无线网络，AP 对于广播 Probe Request 帧也不会回复。此时客户端若想连接此 BSS，则需要手工指定该 SSID，这时客户端会直接向该 AP 发送认证及关联报文连接该 BSS；设置客户端数量可以防止 SSID 接入的客户端数量过多而过载；设置桥接 VLAN 可以将 SSID 接入的客户端划分在不同广播域中，充分利用有限的 IP 地址资源。
- 点击<确定>按钮，完成配置。

o 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。需要注意的是，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。

- 点击<添加>按钮，弹出添加 SSID 配置对话框。
- 勾选“启用 SSID”复选框，在“SSID 名称”配置项处，输入 5G 无线服务的 SSID 名称。
- 在“中文编码”配置项处，选择中文编码的方式。当配置的“SSID-1 名称”包含中文字符，必须配置此参数。通过 iOS 系统接入无线网络时，此处推荐使用“GB2312”编码方式；通过 Android 系统接入无线网络时，此处推荐使用“UTF-8”编码方式。
- 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。
- 为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
- 在“共享密钥”配置项处，输入无线服务密钥。
- 当您选择通过加密方式接入无线服务时，需要设置共享密钥。
- 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，设置加密密钥更新周期。
- 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，请勾选高级设置复选框。启用客户端隔离功能可以开启基于 SSID 的用户隔离，即对使用同一公共无线服务进行通信的用户进行报文隔离，从而达到提高用户安全性、缓解设备转发压力和减少射频资源消耗的目的；启用 SSID 广播功能时，AP 将 SSID 置于 Beacon 帧中向外广播发送。若 BSS 一段时间内不可用即客户端不能上线或不希望其它客户端上线，则可以配置关闭 SSID 广播。关闭 SSID 广播功能时，AP 在 Beacon 帧中广播的 SSID 信息为空，可以借此保护网络免遭攻击。为了进一步保护无线网络，AP 对于广播 Probe Request 帧也不会回复。此时客户端若想连接此 BSS，则需要手工指定该 SSID，这时客户端会直接向该 AP 发送认证及关联报文连接该 BSS；设置客户端数量可以防止 SSID 接入的客户端数量过

多而过载；设置桥接 VLAN 可以将 SSID 接入的客户端划分在不同广播域中，充分利用有限的 IP 地址资源。

– 点击<确定>按钮，完成配置。

(4) 点击<确定>按钮，完成服务模板的配置。

(5) 如需修改配置好的无线服务模板，则在“配置模板管理”页签下，点击模板名称对应的操作列编辑图标，进入无线服务模板修改页面进行相关参数修改即可。

(6) 如需删除无线服务模板，则在则在“配置模板管理”页签下，勾选要删除的模板名称前的复选框，然后单击页面右上角的<删除>按钮即可。注意，名称为“default”的缺省服务模板无法删除。

6.3.4 AP 配置管理

1. 配置简介

AP 配置管理用来增加手工 AP 或为上线的 AP 分配无线服务模板。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“AP 配置管理”页签，进入 AP 配置管理页面。

(3) 在关键字自动查询配置项处，输入待查询 AP 的关键字，页面会自动显示出与关键字相关的 AP 列表。

(4) 单击<高级查询>按钮，进入高级查询配置页面，本页面可设定与 AP 相关的多个筛选条目，点击<查询>按钮，完成查询。

(5) 点击<添加>按钮，弹出添加 AP 配置模板对话框。

(6) 在“MAC 地址”配置项处，输入 AP 设备的 MAC 地址。

您可通过 AP 机身查找 AP 设备的 MAC 地址。

(7) 在“备注信息”配置项处，填写配置信息。

(8) 在“模板选择”配置项处，选择 AP 需要绑定的无线服务模板。

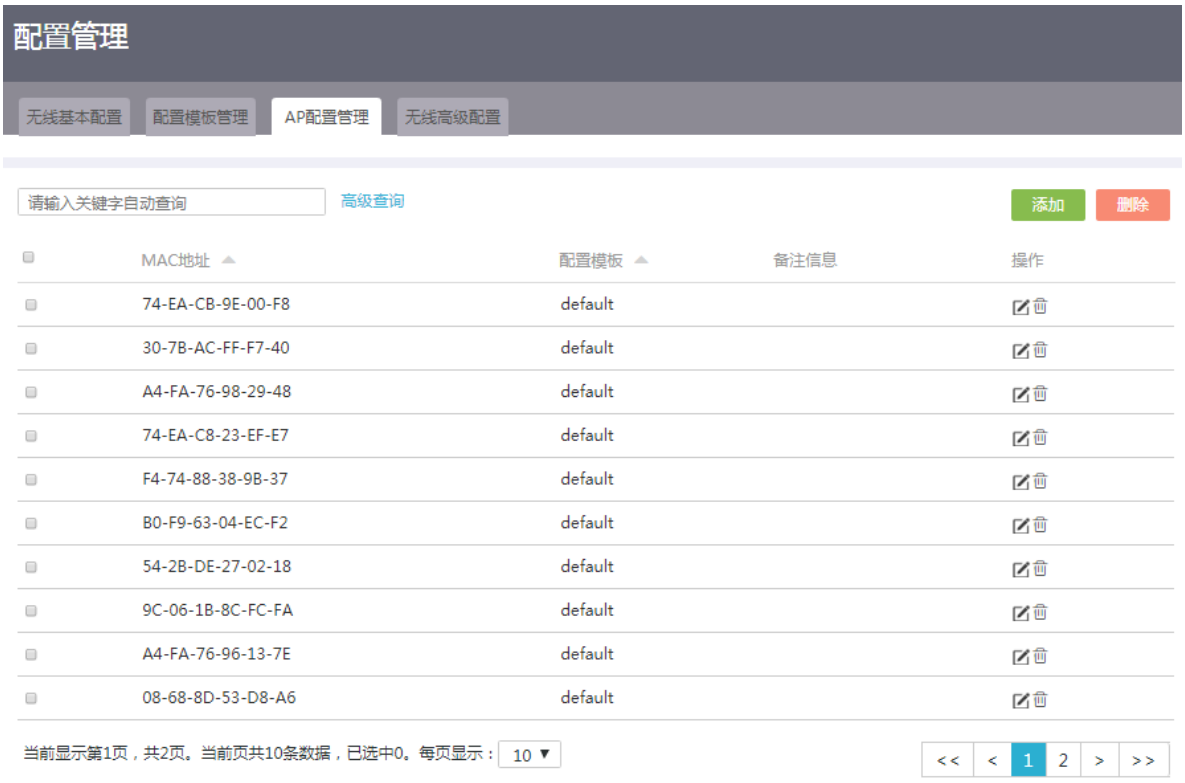
(9) 设置 2.4G 配置和 5G 配置，具体配置如下：

a. 无线网络基本设置

- 无线网络模式：选择无线网络的模式。
- 无线网络频宽：选择无线网络的频宽。
- 无线信道：选择无线网络的信道。
- 发射功率：选择无线设备的天线在无线介质中所辐射的功率，即无线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。

b. 无线网络 SSID 设置：在列表中选择需要配置的 SSID。

(10) 点击<确定>按钮，完成配置。



6.3.5 无线高级配置

1. 配置简介

无线高级配置用来配置二层漫游、禁止弱信号客户端接入以及关闭广播探测等高级需求。

2. 注意事项

- 若同时启用“二层漫游”与“禁止弱信号客户端接入”功能时，“禁止弱信号客户端接入”需要比“信号切换阈值”低，否则“二层漫游”功能不生效。
- 客户端在 AC 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[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(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“二层漫游”复选框，开启二层漫游功能。在“信号切换阀值”配置项处，输入信号切换阀值。
- WLAN 客户端从一个 AP 上接入转移到另一个 AP 上接入的过程称为漫游。在漫游期间，客户端的 IP 地址、授权信息等维持不变。开启“二层漫游”功能时，低于“信号切换阀值”的客户端会进行信号切换。
- 勾选“禁止弱信号客户端接入”复选框，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，避免低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”复选框，该功能关闭后，部分客户端无法扫描到本设备下挂 AP 的 SSID。

(3) 点击<确定>按钮，完成配置。

6.4 版本管理

6.4.1 简介

版本管理功能可以帮助您升级 AP 的软件版本或者强制 AP 同步管理器上的软件版本。

6.4.2 AP 版本上传

1. 注意事项

- AP 断电重连后会自动同步设备管理器中的软件版本。
- 升级 AP 的软件版本时，如果设备管理器中待升级的软件版本高于 AP 的软件版本，AP 会自动升级软件版本；反之，则需要开启“强制 AP 和管理器上的版本一致”，AP 才能自动升级到该软件版本。

2. 配置步骤

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

(2) 单击“AP 版本上传”页签，进入 AP 版本上传配置页面。

(3) 点击<选择文件>按钮，访问待升级的 AP 软件版本存放路径，选中版本文件，点击确定。

(4) 点击<上传>按钮，将待升级的 AP 软件版本上传到设备中。

(5) 点击版本文件右侧的<删除>按钮，点击<确认>按钮，即可删除设备中的版本文件。

6.4.3 AP 升级管理

1. 配置步骤

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

(2) 单击“AP 升级管理”页签，进入 AP 升级管理页面。

(3) 点击按钮并向右滑动，开启“强制 AP 和管理器上的版本一致”功能。

当设备管理器中待升级的软件版本低于 AP 的软件版本时，需要开启“强制 AP 和管理器上的版本一致”，AP 才能自动升级到该软件版本。

6.5 高级管理

6.5.1 简介

若需要通过 Web 管理页面登录 AP 设备，可通过高级管理功能统一设置下挂 AP 的 Web 管理页面登录密码。

6.5.2 注意事项

终端连接 AP 设备后单独设置的登录密码优先级高于 AC 统一下发的登录密码配置。

6.5.3 配置步骤

(1) 单击导航树中[MiniAP 管理/高级管理]菜单项，进入高级管理配置页面。

(2) 勾选启用 AP 密码设置功能（手动设置 AP 密码），在“新密码”配置项处，输入新密码，在“确认密码”配置项处，再次输入新密码。在“密码提示”配置项处，输入密码提示信息。

(3) 点击<确认>按钮，完成配置。

7 网络设置

7.1 外网配置

7.1.1 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。

7.1.2 配置接口模式

1. 配置需求

本功能用于配置设备 WAN 口接入的个数。

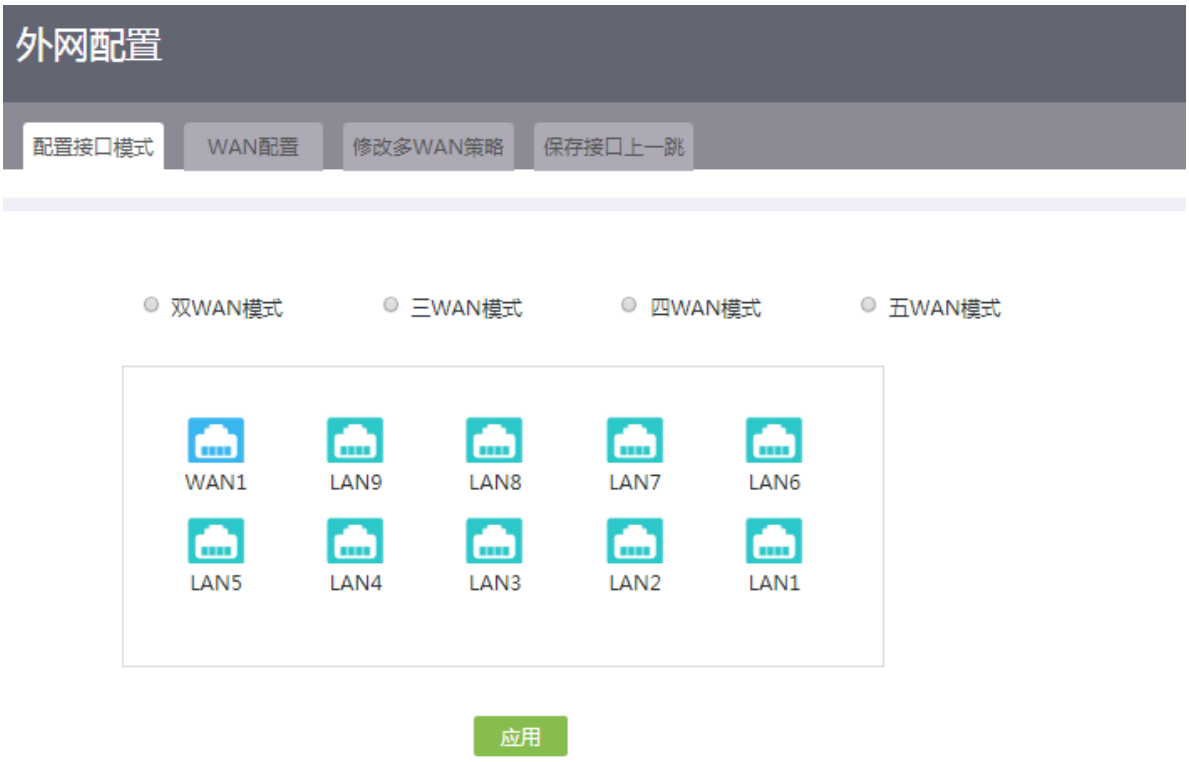
- 正常情况下，LAN 口到 WAN 口的转换，WAN 口的连接到互联网方式为禁用，启用前请配置 WAN 口连接参数。接口相关的 VLAN 配置信息将会丢失。
- 正常情况下，接口转换，会清除端口镜像配置信息，如你需要继续使用端口镜像功能，请重新配置。

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“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。



7.1.3 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 服务器获取接入广域网的公网 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。
  - 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。
  - 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。

(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“网络带宽”配置项处，输入实际线路的带宽值，请咨询当地运营商。

(7) 在“主机名”配置项处，输入需要通告给 DHCP 服务器的机器名。

(8) 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。

(9) 在“TCP MSS”配置项处，设置接口的 TCP 报文段的最大长度。

(10) 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。

(11) 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。

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。

(12) 点击<确定>按钮，完成 WAN 配置修改。

7.1.4 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，可以选择“平均分配负载分担”，否则选择“带宽比例负载分担”。

- 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，可以选择“基于运营商的负载分担”，否则选择“多链路高级负载分担”。
- 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。

(4) 点击<应用>按钮，完成多 WAN 策略修改。

7.1.5 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。

7.2 LAN配置

7.2.1 简介

本功能主要用于配置设备连接内网的 LAN 接口参数，开启 DHCP 服务，以及将接口加入 VLAN。

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，该地址可以被其他主机使用。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。

7.2.2 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。

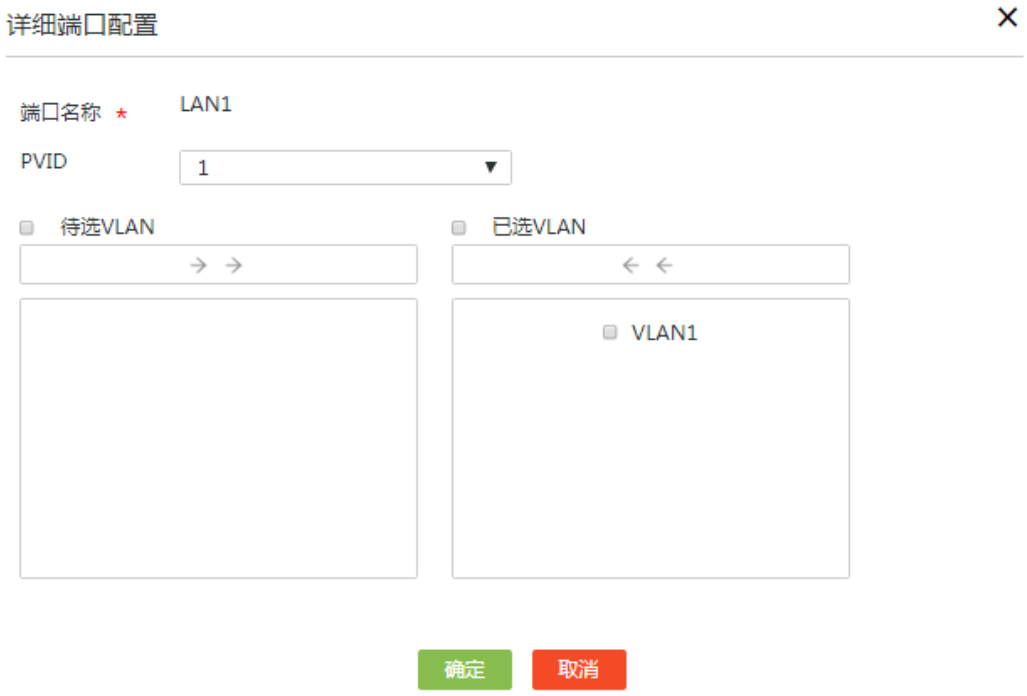
(3) 在端口列表中，点击指定端口对应的操作列修改图标，弹出详细端口配置对话框。

(4) 在“PVID”配置项处，通过下拉框修改端口的 PVID。

(5) 将当前端口加入 VLAN：勾选待选 VLAN 选项或者勾选待选 VLAN 区域框中的 VLAN 选项后，点击向右方向按钮，将当前端口加入所有的待选 VLAN 或者指定 VLAN。

(6) 将当前端口从 VLAN 中移除：勾选已选 VLAN 选项或者勾选已选 VLAN 区域框中的 VLAN 选项后，点击向左方向按钮，将当前端口从所有的已选 VLAN 或者指定 VLAN 中移除。

(7) 点击<确定>按钮，完成配置。



7.2.3 配置 LAN 接口基本参数

1. 配置需求

为设备连接内网的 LAN 接口配置 IP 地址，或创建 VLAN 与 VLAN 接口。

2. 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) 点击<添加>按钮，进入添加 LAN 接口页面。

(4) 在“VLAN ID”配置项处，输入 VLAN ID。

(5) 在“接口 IP 地址”配置项处，输入接口的 IP 地址。

(6) 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。

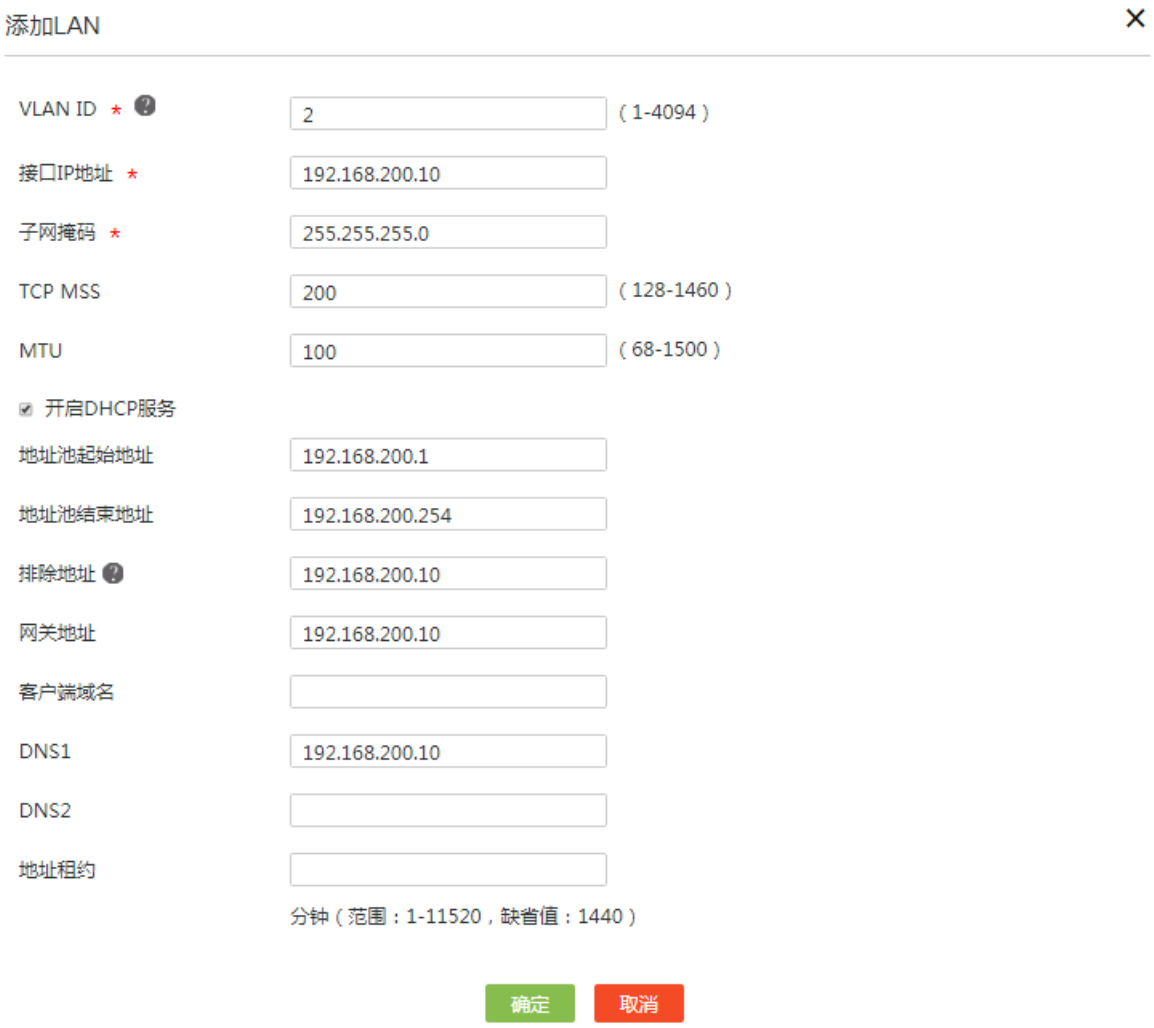
(7) 在“TCP MSS”配置项处，设置接口的 TCP 报文最大分段长度值。

(8) 在“MTU”配置项处，输入接口允许通过的 MTU 的大小。

(9) 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（例如连接到设备的计算机等）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，为客户端绑定动态分配的 IP 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，输入客户端的域名。
- 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。

(10) 点击<确定>按钮，完成配置。



7.2.4 配置接口上的 DHCP 服务

1. 配置需求

如果希望设备可以为连接到该接口的客户端（如连接到设备的计算机等）动态分配 IP 地址，则需要开启指定接口上的 DHCP 服务。

2. 注意事项

接口上指定的地址池的地址范围不能与设备上 WAN 口的 IP 地址网段包含相同的 IP 地址。

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。

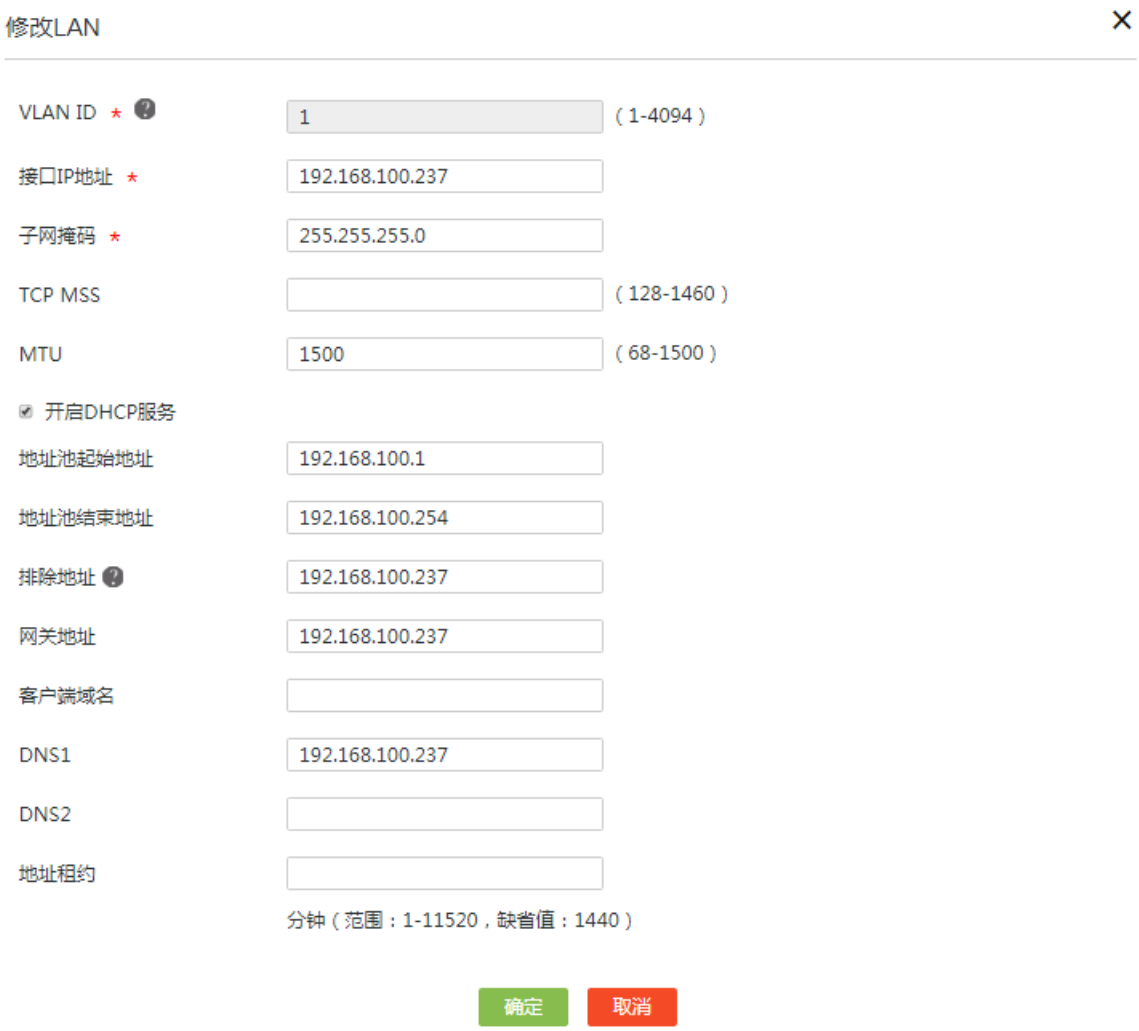
(2) 单击“VLAN 配置”页签，进入 VLAN 配置页面。

(3) 在接口列表中，点击指定接口对应的操作列编辑图标，进入修改接口配置页面。

(4) 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（例如连接到设备的计算机等）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，为客户端绑定动态分配的 IP 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，输入客户端的域名。
- 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。

(5) 点击<确定>按钮，完成配置。



7.2.5 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

在任何一个接口上开启 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。对于 PC 类型的客户端，可以在网卡信息中查询到 MAC 地址；对于设备类型的客户端，可以通过 display interface 命令查询接口的 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。

7.2.6 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，确认回收所有 IP 地址。

7.2.7 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 DHCP 服务。

(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 分配的 IP 地址设置为静态分配。

7.3 端口管理

7.3.1 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 地址等信息，设置 WAN 口的管理状态，以及修改端口配置。

7.3.2 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管理状态列按钮，设置开启或者关闭该端口。

(3) 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。

(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，设置端口是否抑制或者抑制级别。

(7) 点击<确定>按钮，完成配置。

7.4 NAT配置

7.4.1 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。

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/DNS，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。

7.4.2 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“接口”配置项处，选择用于连接 Internet 的端口。

(8) 在“协议类型”配置项处，选择协议为“TCP”或“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。

(9) 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。

(10) 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。

(11) 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。

(12) 在“内部端口”配置项处，输入内部网络资源使用的端口号。

(13) 点击<确定>按钮，完成配置。

7.4.3 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“启用”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。

(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。

7.4.4 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。

(5) 在“起始地址”配置项处，输入地址池的起始 IP 地址。

(6) 在“终止地址”配置项处，输入地址池的终止 IP 地址。

(7) 点击配置项右侧的<→>按钮，提交配置的地址组内容。

(8) 重复(5)、(6)步骤可完成多个地址池的添加。

(9) 点击<确定>按钮，完成配置。

7.4.5 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，弹出添加端口触发列表对话框。

(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。

(8) 在“是否开启”配置项处，选择是否开启端口触发功能。

(9) 点击<确定>按钮，完成配置。

7.4.6 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

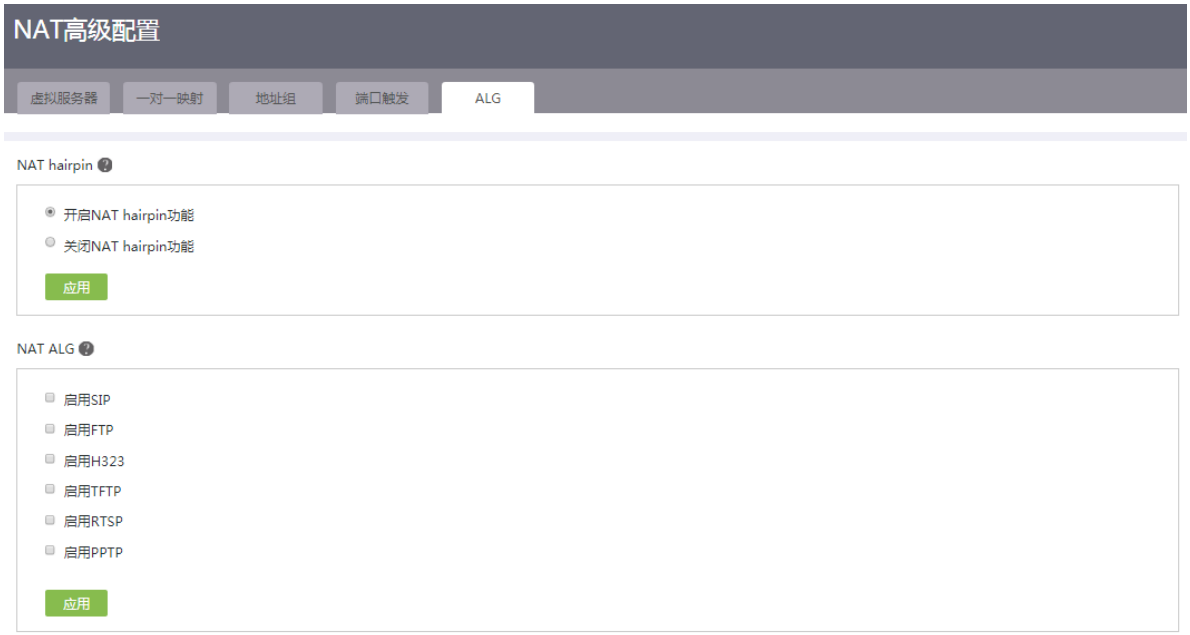
(1) 单击导航树中[网络设置/NAT 配置]菜单项，进入 NAT 高级配置页面。

(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) 在 NAT hairpin 区段，勾选“开启 NAT hairpin 功能”选项，开启 NAT hairpin 功能。

(5) 点击<应用>按钮，完成配置。



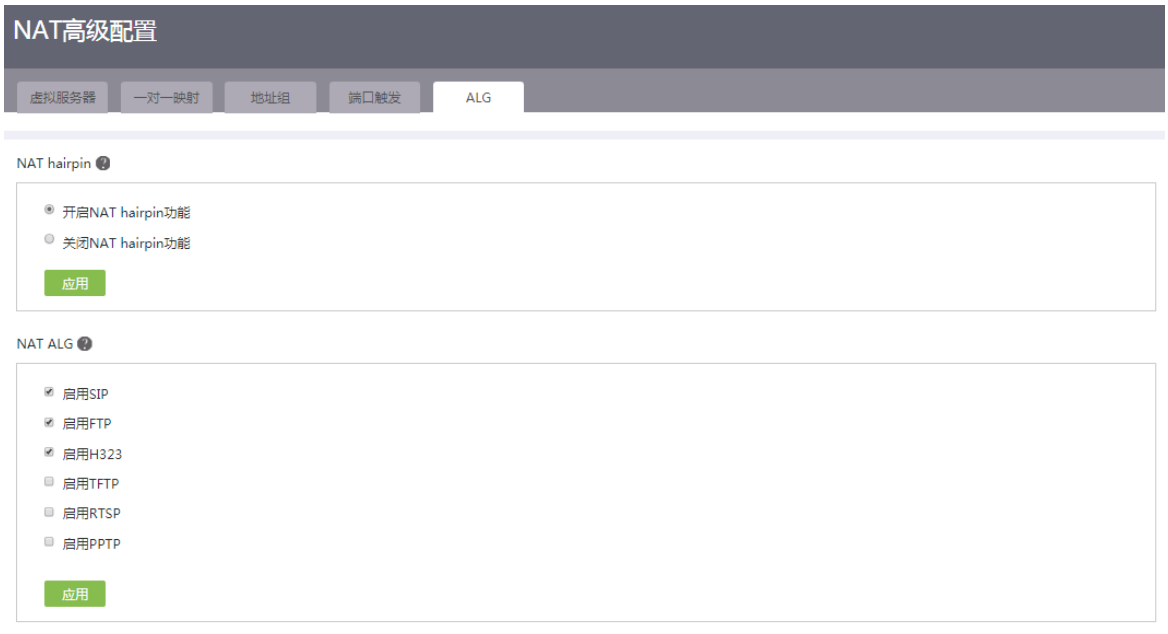
7.4.7 配置 NAT ALG

(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。



7.5 地址组

7.5.1 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。

7.5.2 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。

7.5.3 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，弹出新建地址组对话框。

(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，完成新建地址组。

7.6 时间组

7.6.1 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，而其他时间不生效，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。

7.6.2 注意事项

- 您最多可以创建 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。

7.6.3 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”，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天数，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 上网行为管理

8.1 带宽管理

8.1.1 简介

带宽管理功能用于对流量进行限速，用户可基于地址组和时间段等限制条件对流量进行精细控制。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，可选择从本通道传输，即通过启用限制通道功能来保证带宽。对于需要保证时延的交互性应用流量，可通过启用绿色通道功能来保证带宽。

8.1.2 配置 IP 限速

(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。配置流量限制之前，需要先在 WAN 配置中设置网络带宽。

- 上传带宽：上传方向的最大带宽值。若不设置上传带宽值，则表示不对上传方向的带宽进行限速。
- 下载带宽：下载方向的最大带宽值。若不设置下载带宽值，则表示不对下载方向的带宽进行限速。
- 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。
- 弹性共享：选择是否弹性共享带宽，若勾选“弹性共享”选项，则需设置可弹性共享当前线路带宽的百分比。
- 在“限制时段”配置项处，设置 IP 限速的生效时间。

(6) 点击<确定>按钮，完成新建 IP 限速策略。

8.1.3 配置限制通道

(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) 单击“限制通道”页签，进入限制通道配置页面。

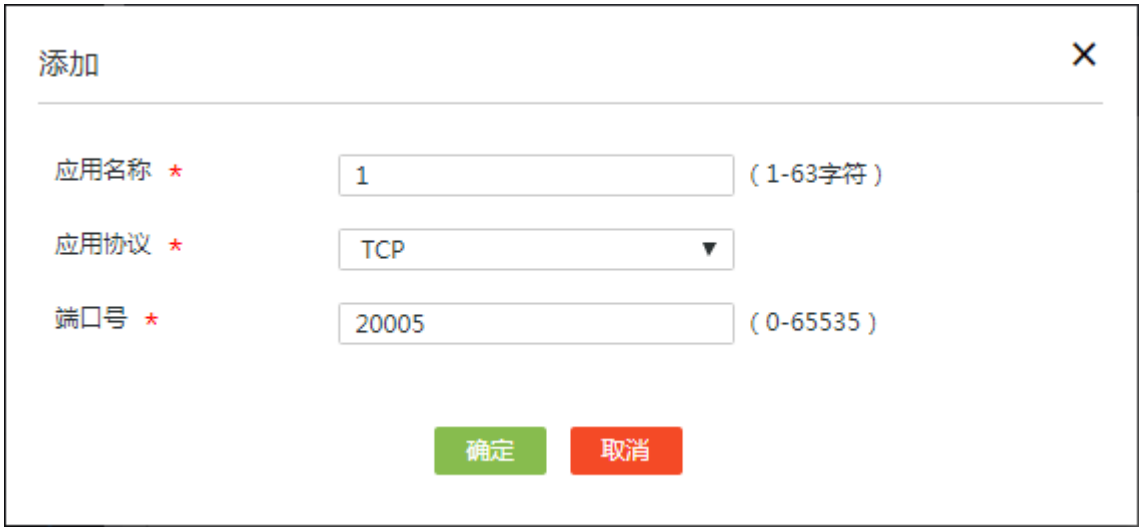
(3) 勾选“启用限制通道”选项，开启带宽管理的限制通道功能。

(4) 在“限制通道流速上限”配置项处，输入限制通道的流速上限。

(5) 对于需要保证时延的交互性应用流量，需要用户根据实际情况自行配置应用的协议和端口号。只有匹配应用的流量才能进入限制通道传输，具体配置步骤如下：

- 勾选“自定义应用端口匹配限制通道”选项，开启自定义应用端口匹配限制通道功能。
- 点击自定义应用端口配置项右侧的<添加>按钮，弹出添加对话框。
- 在“应用名称”配置项处，输入自定义应用的名称。
- 在“应用协议”配置项处，输入自定义应用的传输层协议。
- 在“端口号”配置项处，输入自定义应用的端口号。
- 点击<确定>按钮，完成添加自定义应用。

(6) 点击<应用>按钮，完成限制通道的配置。



8.1.4 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。

2. 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) 单击“绿色通道”页签，进入绿色通道配置页面。

(3) 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。

(4) 配置绿色通道中需要传输的应用后，还可以针对通道中所有应用进行如下限制：

- 如果还希望对绿色通道中的流速上限进行限制，则需要勾选“限制绿色通道流速上限”复选框，并配置最大流速。

- 如果还希望对绿色通道中传输的数据包长度进行限制，则需要勾选“匹配绿色通道数据包长度选择 ”复选框，并配置数据包的最大长度。超过最大长度的数据包不会进入绿色通道传输。

(5) 对于需要保证时延的交互性应用流量，需要用户根据实际情况自行配置应用的协议和端口号。只有匹配应用的流量才能进入绿色通道传输，具体配置步骤如下：

- 勾选“自定义应用端口匹配绿色通道”选项，开启自定义应用端口匹配绿色通道功能。
- 点击自定义应用端口配置项右侧的<添加>按钮，弹出添加对话框。
- 在“应用名称”配置项处，输入自定义应用的名称。
- 在“传输层协议”配置项处，输入自定义应用的传输层协议。
- 在“端口号”配置项处，输入自定义应用的端口号。
- 点击<确定>按钮，完成添加自定义应用。

(6) 点击<应用>按钮，完成绿色通道的配置。

8.2 上网行为管理

8.2.1 简介

上网行为管理功能用于对用户访问的应用以及网址进行控制，并可基于地址组和时间段等限制条件对用户的上网行为进行更精细的控制。

8.2.2 配置应用控制

1. 注意事项

因为网址过滤功能基于 HTTP 协议，所以应用控制功能中不能将 HTTP 协议阻断，否则将影响设备对网址的识别，导致网址过滤功能不生效。

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“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。

- 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，选择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生效时间。
- 在“应用控制”配置项处，点击“选择网络应用”右侧的详情图标，选择网址应用，并配置对该应用的访问执行的动作，包括如下：
  - 阻断：阻断对应用的访问。
  - 不阻断：不对应用的访问进行限制。

(5) 点击<确定>按钮，完成新建应用控制策略。

8.2.3 配置网址控制

1. 配置需求

当设备已有的网址分类不能满足用户需求时，可通过自定义网址分类的方式按需添加网址。

2. 注意事项

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，单击<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”。

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，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。

8.2.4 配置文件控制

(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，弹出添加文件控制策略对话框。

(5) 在“文件后缀类型”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<确定>按钮，完成添加文件控制策略。

9 网络安全

9.1 防火墙

9.1.1 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。

9.1.2 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。

9.1.3 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，请提前在时间组页面创建相应的时间组。

9.1.4 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) 点击<添加>按钮，弹出创建安全规则对话框。

(4) 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。

(5) 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”。

(6) 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。

(7) 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。

(8) 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。

(9) 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。

(10) 在“动作”配置项处，选择该规则所匹配报文的执行动作。

(11) 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。

(12) 在“描述”配置项处，配置该安全规则的描述信息。

(13) 点击<确定>按钮，完成创建安全规则。

9.2 连接限制

9.2.1 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。

9.2.2 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。

(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。

9.2.3 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。

(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。

(7) 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。

(8) 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。

(9) 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。

(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。

9.3 MAC地址过滤

9.3.1 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），则可以在三层接口上配置 MAC 地址过滤功能，本功能将根据接收报文的源 MAC 地址对其过滤。

配置方式有如下两种：

- 白名单：允许源 MAC 地址在白名单内的报文通过，其余禁止通过。

- 黑名单：禁止源 MAC 地址在黑名单内的报文通过，其余允许通过。

9.3.2 注意事项

如果需要在管理员终端连接的接口上开启白名单方式的 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。

9.3.3 MAC 过滤设置

MAC 地址过滤的配置方式有白名单和黑名单两种，下面以白名单为例进行配置步骤的讲解，黑名单的配置步骤同白名单。

(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”列上，选择“白名单”，并在“开启和关闭”列上勾选“开启”。

(5) 点击<应用>按钮，开启 MAC 地址过滤。

9.3.4 MAC 黑白名单管理

(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. 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<选择文件>按钮，选择已编辑好的模板。

e. 点击<确定>按钮，完成对白名单批量添加 MAC 地址的操作。


MAC地址过滤
MAC过滤设置
MAC黑白名单管理
开启MAC地址过滤
关闭MAC地址过滤
请确保管理终端的MAC地址已添加至白名单列表中
端口
过滤方式
开启和关闭
VLAN1
白名单
开启
关闭
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
>
>>
应用


MAC地址过滤
MAC过滤设置
MAC黑白名单管理
白名单
黑名单
请输入关键字自动查询
高级查询
刷新
添加
删除
导入
导出
序号
MAC地址
描述
操作
1
00-0C-29-91-26-2E
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
>
>>


添加源MAC地址
MAC地址
00-0C-29-91-26-29
描述
（1-127字符）
确定
取消

9.4 ARP安全

9.4.1 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。
- 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 报文通知其他设备更新 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。

9.4.2 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。

9.4.3 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。
- 点击<清除>按钮，则可以清除当前显示的所有静态 ARP 表项，动态 ARP 表项或者全部 ARP 表项。
- 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。

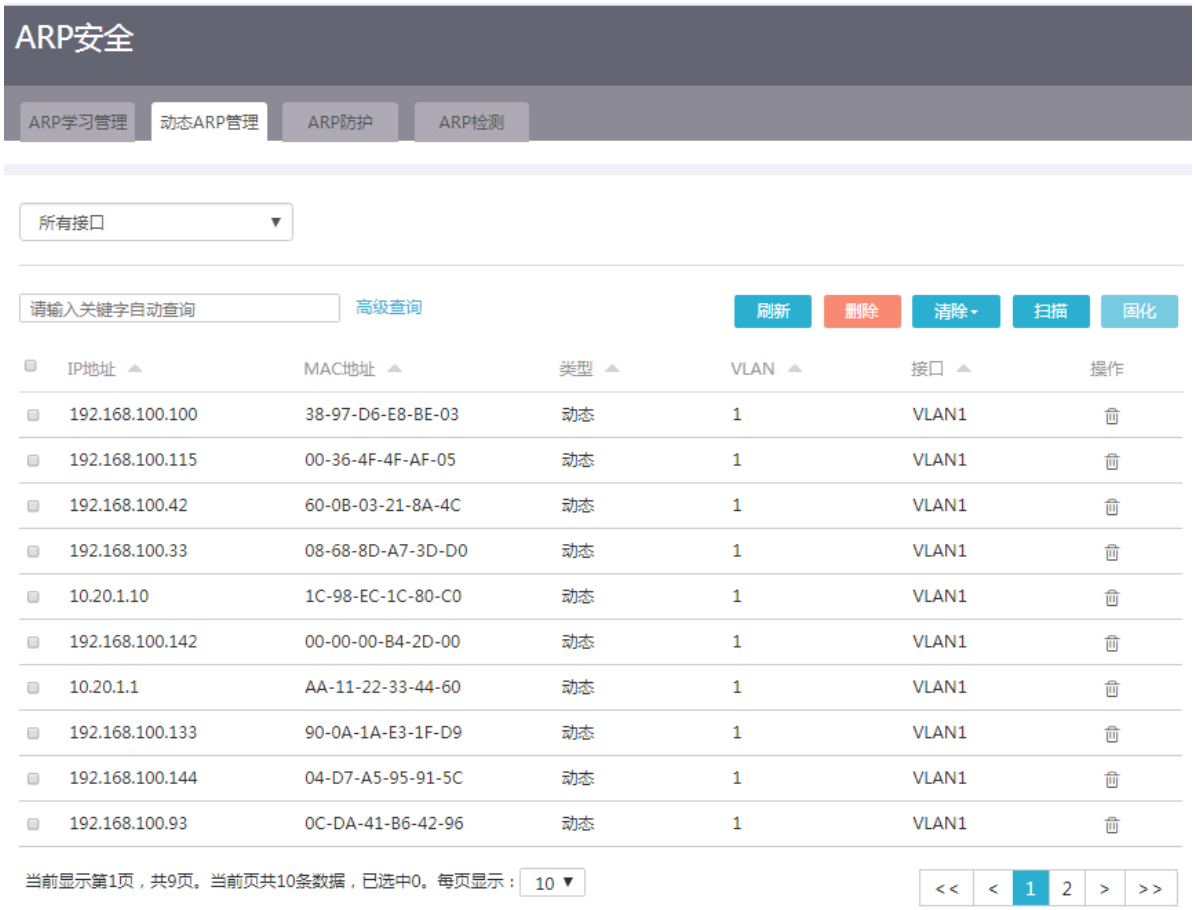
(4) 可对已有的动态 ARP 表项执行以下管理操作：

a. 点击<扫描>按钮，弹出扫描配置对话框。

b. 在“接口”配置项处，选择需要执行 ARP 扫描操作的接口。

c. 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。

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。



9.4.4 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：

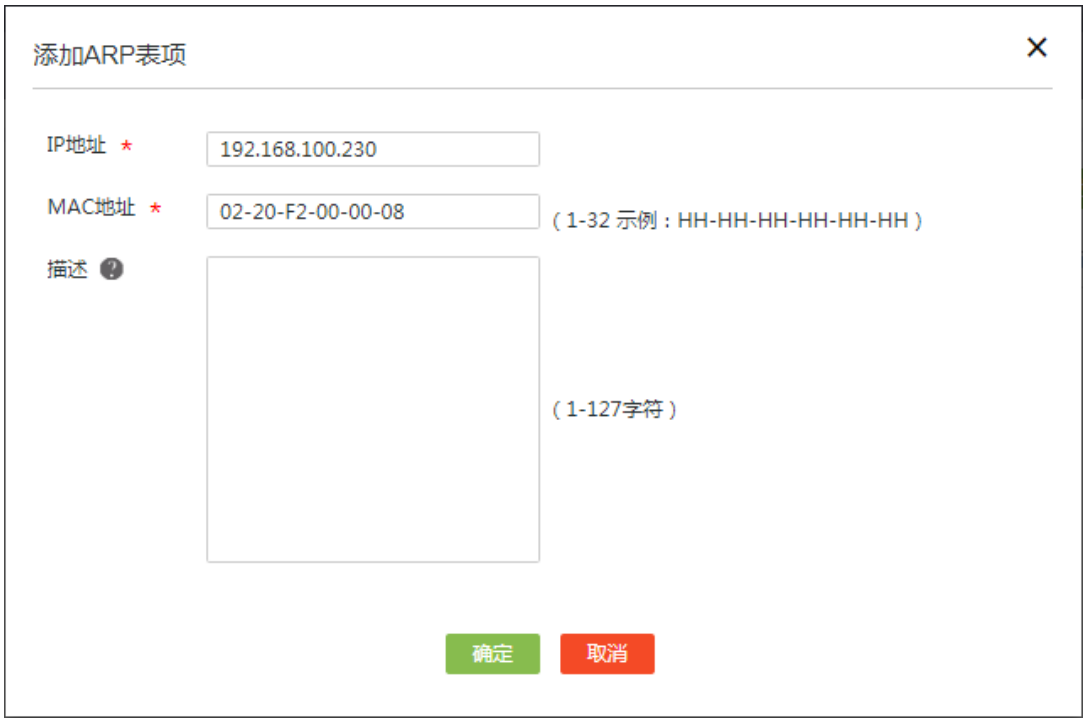
a. 点击<导出>按钮，选择“导出模板”菜单项。

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。



9.4.5 ARP 防护

1. 配置限制和指导

- 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”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。

9.4.6 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。

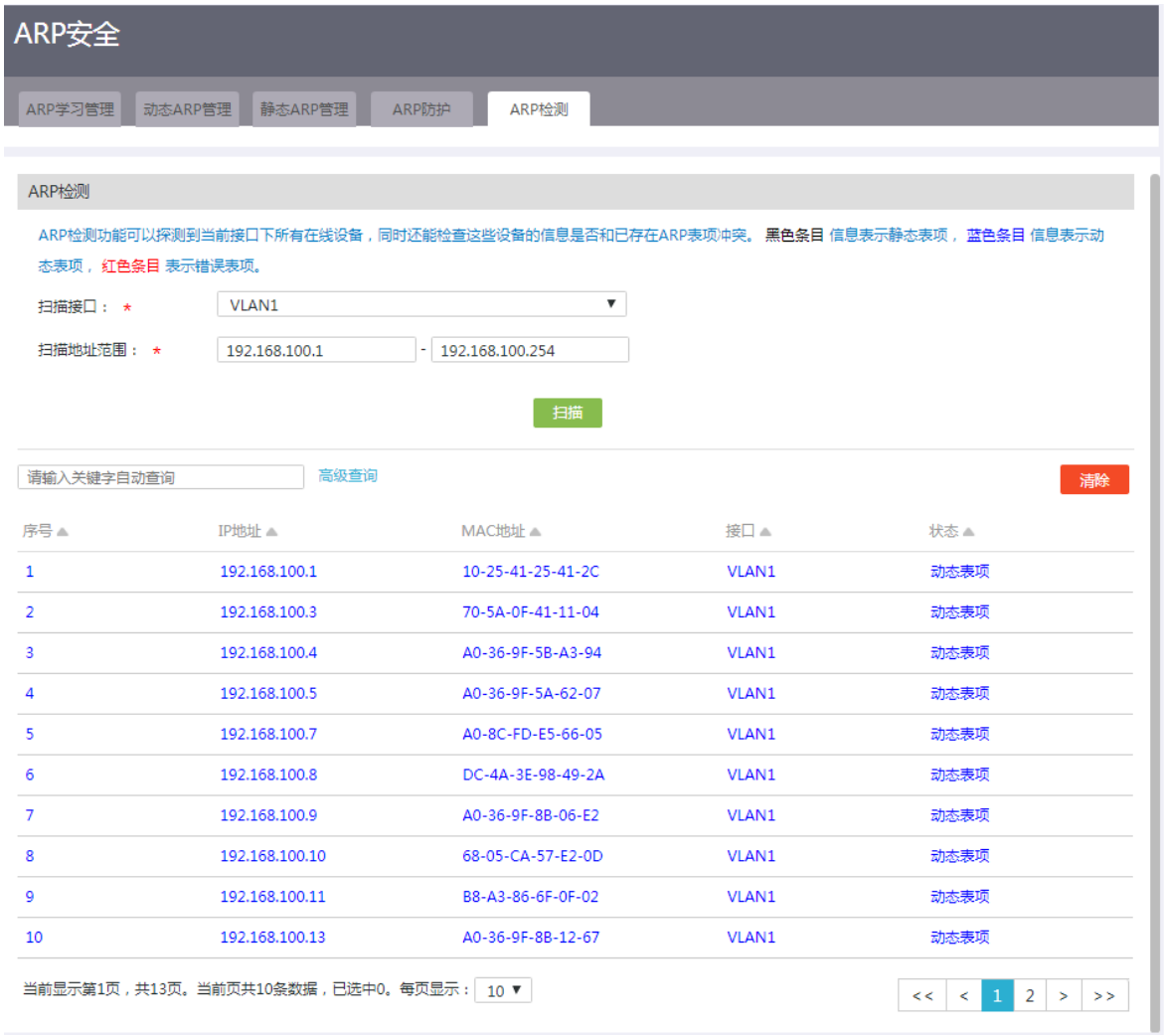
(3) 在“扫描接口”配置项处，选择扫描的接口。

(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，其中黑色条目信息表示静态表项，蓝色条目信息表示动态表项，红色条目表示错误表项。检测结果中 ARP 表项的状态分为：

- 静态绑定：表示该条表项已手动配置为静态绑定。
- 动态绑定：表示该条表项为对 DHCP 分配的地址进行 ARP 保护时自动进行了绑定。
- 未绑定：表示该条表项为动态学习到的 ARP 表项。

(6) 点击<清除>按钮，可以清除当前的检测结果。



9.5 DDoS攻击防御

9.5.1 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。

9.5.2 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。

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，设备可以有效的防止恶意的 Fraggle 攻击。Fraggle 攻击与 Smurf 攻击类似，只是它使用 UDP 消息， 而不是 ICMP 报文。UDP 端口 7（echo）和端口 19（Charge）在收到 UDP 报文后都会产生回应。在 UDP 的 7 号端口收到报文后，会回应收到的内容，19 号端口收到 UDP 报文后会产生一串字符。它们都同 ICMP 一样，会

产生大量无用的应答报文，占用网络带宽。攻击者可以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，使用端口号为 7 或者 19。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，从而引发大量报文，导致网络阻塞或者主机崩溃；子网上没有启用该功能的主机会产生 ICMP 端口不可达消息，仍然消耗带宽。也可以将源端口改为 19，目的端口为 7，这样会不停产生回应报文，危害性更大。

- Land 攻击防御：启用该项后，设备可以有效的防止恶意的 Land 攻击。默认开启该功能。系统在检测到攻击将直接丢弃攻击报文，不再进行安全统计及日志告警。Land 攻击是一种古老而又经典的攻击，它是通过发送带有 SYN 标志的 TCP 报文到被攻击目标的开放端口，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，设备可以有效的防止恶意的 WinNuke 攻击。WinNuke 是利用 NetBIOS 协议中一个 OOB（Out of Band）的漏洞，也就是所谓的带外数据漏洞而进行的，它的原理是通过 TCP/IP 协议传递一个 Urgent(紧急)数据包到计算机的 135、137、138 或 139 端口，当 win95/NT 收到这个数据包之后就会瞬间死机或蓝屏，不重新启动计算机就无法继续使用 TCP/IP 协议来访问网络。
- TCP flag 攻击防御：启用该项后，设备可以有效的防止恶意的 TCP flag 攻击。不同操作系统对于非常规的 TCP 标志位有不同的处理。攻击者通过发送带有非常规 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，设备可以有效的防止恶意的 ICMP 不可达报文攻击。某些系统在收到不可达的 ICMP 报文后，对于后续发往此目的地的报文判断为不可达并切断对应的网络连接。攻击者通过发送 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，设备可以有效的防止恶意的 ICMP 重定向报文攻击。攻击者向用户发送 ICMP 重定向报文，更改用户主机的路由表，干扰用户主机正常的 IP 报文转发。
- Smurf 攻击防御：启用该项后，设备可以有效的防止恶意的 Smurf 攻击。攻击者会向一个网段广播一个 ICMP 回显请求（ICMP ECHO REQUEST）报文，而源地址指向被攻击主机，当网段中的所有主机收到回显请求后，都会向被攻击机响应 ICMP ECHO REPLY 报文，如果这个网段有 N 台主机,则攻击者只要伪造一个请求报文， 被攻击机就会收到 N 份响应报文，如攻击机同时发送大量的类似请求，被攻击机最终会来不及处理响应而当机。
- 带源路由选项的 IP 攻击防御：启用该项后，设备可以有效的防止恶意的带源路由选项的 IP 攻击。攻击者通过构造选项为 loose-source-routing、strict-source-routing 类型的 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，设备可以有效的防止恶意的带路由记录选项的 IP 攻击。攻击者通过构造选项为 record packet route 类型的 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，设备可以有效的防止恶意的超大 ICMP 攻击。某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大 ICMP 报文，让目标主机崩溃，达到攻击目的。

- 防止 IP Spoofing：启用该项后，设备可以有效的防止恶意的 IP Spoofing 攻击。IP Spoofing 节点间的信任关系有时会根据 IP 地址来建立，攻击者使用相同的 IP 地址可以假冒网络上合法主机，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，设备可以有效的防止恶意的 TearDrop 攻击。默认开启该功能。系统在检测到攻击将直接丢弃攻击报文，不再进行安全统计及日志告警。Tear drop 也是一种碎片攻击，发出的包是经过分片的，而这些碎片的位移是相互重叠的，这种畸形数据包会造成目标主机不知道如何处理缓存分片信息，发现碎片报文，直接丢弃。
- 防止碎片包：启用该项后，设备可以有效的防止恶意的碎片包攻击。默认开启该功能。系统在检测到攻击将直接丢弃攻击报文，不再进行安全统计及日志告警。为了传送一个大的 IP 报文，IP 协议栈需要根据链路接口的 MTU 对该 IP 报文进行分片，通过填充适当的 IP 头中的分片指示字段，接收计算机可以很容易的把这些 IP 分片报文组装起来。目标计算机在处理这些分片报文的时候，会把先到的分片报文缓存起来，然后一直等待后续的分片报文，这个过程会消耗掉一部分内存， 以及一些 IP 协议栈的数据结构。如果攻击者给目标计算机只发送一片分片报文，而不发送所有的分片报文，这样被攻击的计算机便会一直等待（直到一个内部计时器到时），如果攻击者发送了大量的分片报文，就会消耗掉目标计算机的资源，而导致不能响应正常的 IP 报文。碎片包攻击也是一种 DOS 攻击。

(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。启动扫描攻击防御后，可选择将源 IP 地址加入黑名单。在一定时间内，来自扫描攻击源的报文将被设备直接丢弃。被加入黑名单的 IP 地址可在黑名单管理页面查看。建议根据网络流量类型开启对应的泛洪攻击防御。

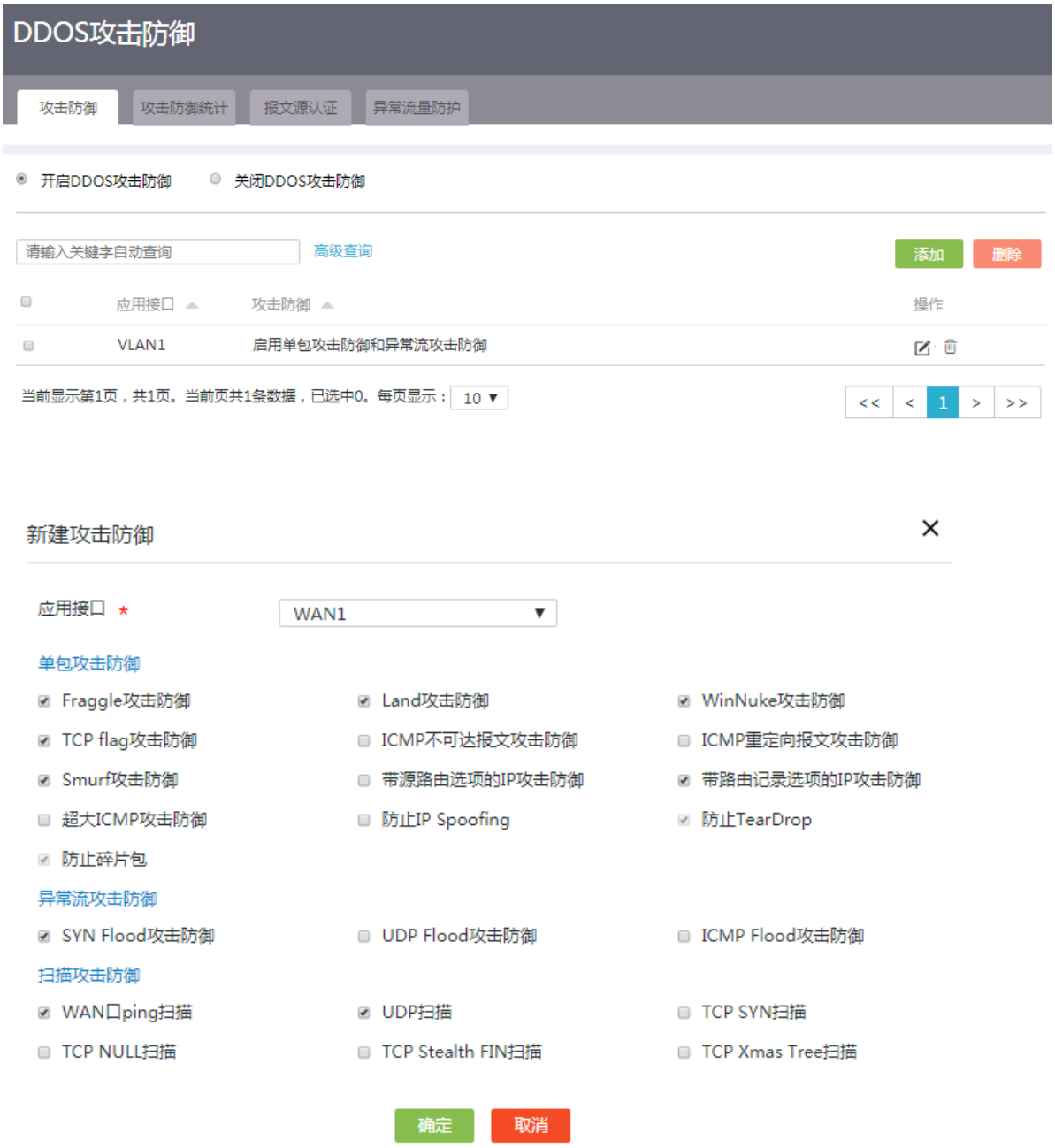
- SYN Flood 攻击防御：启用该项后，设备可以有效的防止恶意的 SYN FLOOD 攻击。SYN FLOOD 攻击通过发送大量的 SYN 报文，使被攻击服务器中的数据结构逐渐会被填满，这样系统将无法再接受任何传入的新连接。
- UDP Flood 攻击防御：启用该项后，设备可以有效的防止恶意的 UDP FLOOD 攻击。UDP FLOOD 攻击的原理与 SYN FLOOD 类似，攻击者通过发送大量的 UDP 报文给目标计算机，导致目标计算机忙于处理这些 UDP 报文而无法继续处理正常的报文。
- ICMP Flood 攻击防御：启用该项后，设备可以有效的防止恶意的 ICMP FLOOD 攻击。ICMP FLOOD 的原理与 SYN FLOOD 类似，攻击者通过发送大量的 ICMP 报文给目标计算机，导致目标计算机忙于处理这些 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，设备不回应来自因特网的 Ping 请求，可以防止因特网上恶意的 Ping 探测。
- UDP 扫描：启用该项后，设备可以有效的防止恶意的 UDP 扫描。UDP 扫描是用来探测目标主机上有哪些 UDP 端口是开放的。攻击者向目标主机的某个端口发送 UDP 报文，如果目标主机返回 ICMP 端口不可达报文，则说明这个端口是关闭的，否则这个端口是开放的。
- TCP SYN 扫描：启用该项后，设备可以有效的防止恶意的 TCP SYN 扫描。TCP SYN 扫描，通常也叫做半连接扫描，因为它并不建立一个完整的 TCP 连接。攻击者象建立正常的 TCP 连接一样向某个端口发送一个 SYN 报文， 然后等待目标主机的回应，如果目标主机回应 SYN|ACK 报文，则说明这个端口是开放的；如果回应 RST 报文，则说明该端口没有开放。当收到的是 SYN|ACK 报文时，攻击者立即回送一个 RST 报文将连接中止，这就是它叫做半连接扫描的原因。其扫描原理是依据 RFC 793。

- TCP NULL 扫描：启用该项后，设备可以有效的防止恶意的 TCP NULL 扫描。TCP NULL 扫描和 TCP SYN 扫描原理一样，只是发送所有标志都不置位的 TCP 报文。其扫描原理是依据 RFC 793。
- TCP Stealth FIN 扫描：启用该项后，设备可以有效的防止恶意的 TCP Stealth FIN 扫描。TCP Stealth FIN 扫描和 TCP SYN 扫描原理一样，只是发送只有 FIN 标志置位的 TCP 报文。其扫描原理是依据 RFC 793。
- TCP Xmas Tree 扫描：启用该项后，设备可以有效的防止恶意的 TCP Xmas Tree 扫描。TCP Xmas Tree 扫描：和 TCP SYN 扫描原理一样，只是发送 FIN、URG 和 PUSH 标志置位的 TCP 报文。其扫描原理是依据 RFC 793。

(9) 点击<确定>按钮，完成配置。



9.5.3 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。

9.5.4 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。

9.5.5 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。设备会进行异常主机流量检查，并且自动把检查到的攻击主机添加到攻击列表中，在指定的生效时间范围内，禁止其访问本设备和 Internet，以尽量减少这台异常主机对网络造成的影响。
- 中：防护等级居中。设备会把内网主机上行流量分别限制在异常流量阈值范围内，超过阈值的流量将被设备所丢弃。
- 低：防护等级低。设备仅对超过异常流量阈值的事件记入日志，仍然允许对应的主机访问设备和 Internet。

(5) 点击<应用>按钮，完成配置。

9.6 安全统计

9.6.1 简介

安全统计功能是用于统计设备接收到的非法或者可疑数据包，能够统计数据包的类型如下：

- 报文源认证失败：指在 LAN 内网络环境中，设备认为是非法的主机发送的数据包。
- LAN 侧可疑：指在 LAN 内网络中，无法确定是否是真实存在的主机发送数据包。
- WAN 侧非法：指 IntetNet 上，主动发送设备 WAN 口的非法数据包。

9.6.2 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。

9.7 黑名单管理

9.7.1 简介

黑名单管理用于对已经添加的黑名单用户进行管理。

9.7.2 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。

9.8 终端接入控制

9.8.1 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。

9.8.2 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 静态绑定的客户端访问外网：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。
- 不限制：不对终端接入进行控制。

(3) 点击<应用>按钮，完成配置。

10 认证管理

10.1 Portal认证

10.1.1 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。

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。

10.1.2 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上的配置，并开启云服务。

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，设置接口是否开启云服务功能。

10.1.3 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。

10.1.4 配置免认证 IP 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 IP 地址”页签，进入免认证 IP 地址配置页面。

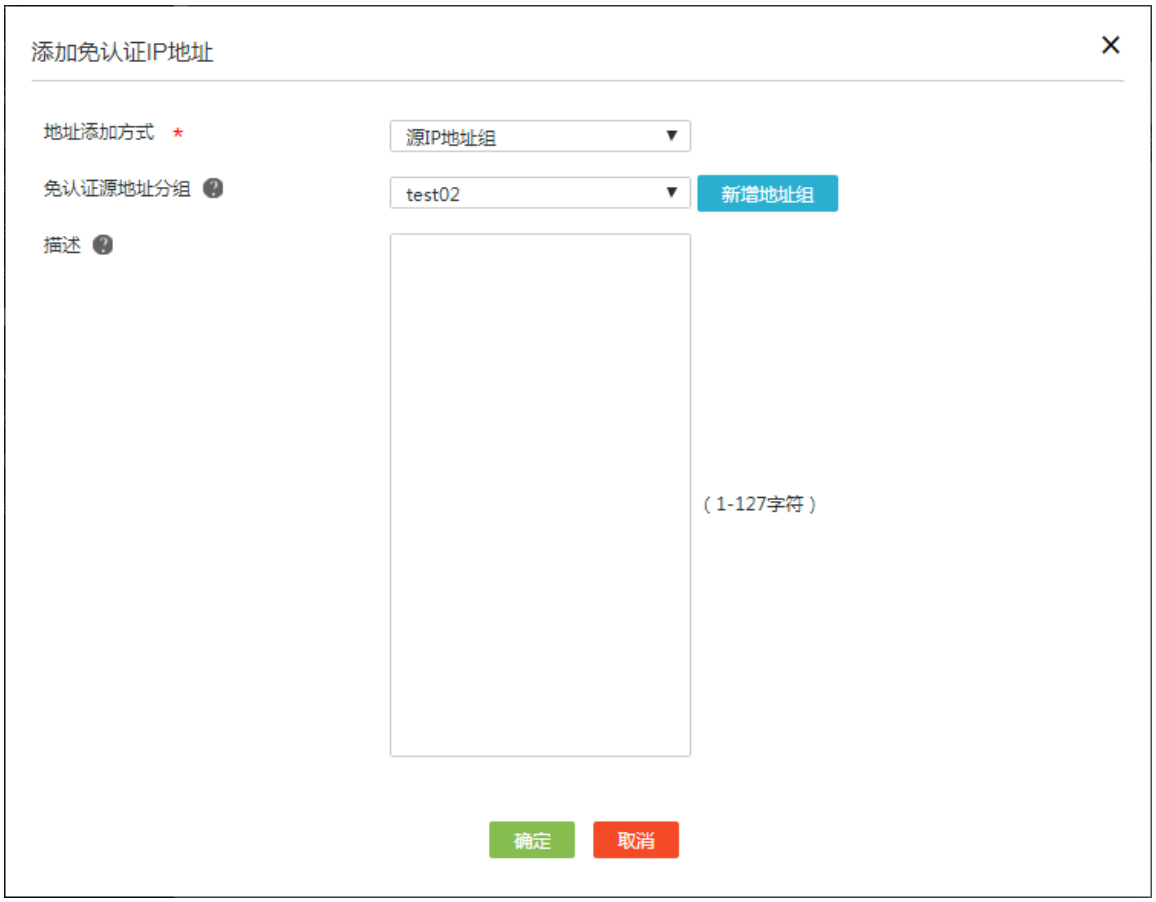
(3) 点击<添加>按钮，弹出添加免认证 IP 地址对话框。

(4) 在“地址添加方式”配置项处，选择免认证 IP 地址的方式。

- 选择“源 IP 地址组”选项，则需在“免认证源地址分组”配置项处，选择地址分组，或点击<新增地址组>按钮，添加新的地址组。

- 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，选择地址分组，或点击<新增地址组>按钮，添加新的地址组。
- 选择“域名”选项，则需在“域名”配置项处，输入域名。

(5) 点击<确定>按钮，完成配置。



11 虚拟专网(VPN)

11.1 IPsec VPN

11.1.1 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。
- 对等方式组网：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。

11.1.2 配置 IPsec 分支节点

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。

对等方式组网环境中的设备需要与对端设备主动建立 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. 可以通过多次执行步骤（9）添加多条保护流。

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，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。

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（6）配置的对端身份类型和身份标识一致。

如果您执行步骤（4）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（5）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。您可选择推荐的算法组合亦可自定义认证算法、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。

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。您可选择推荐的算法组合亦可自定义安全协议、认证算法、加密算法、封装模式和 PFS 算法。

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“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。

(5) 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。

(6) 在“触发模式”配置项处，选择触发 IPsec 重新协商的模式。

(7) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(8) 点击<确定>按钮，完成配置。

11.1.3 配置 IPsec 中心节点

1. 配置需求

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

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。

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（4）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。您可选择推荐的算法组合亦可自定义认证算法、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。

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。您可选择推荐的算法组合亦可自定义安全协议、认证算法、加密算法、封装模式和 PFS 算法。

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“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。

(5) 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。

(6) 在“触发模式”配置项处，选择触发 IPsec 重新协商的模式。

(7) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(8) 点击<确定>按钮，完成配置。

11.1.4 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。

11.2 L2TP服务器端

11.2.1 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。

11.2.2 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) 在“L2TP 服务器端”配置项处，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。

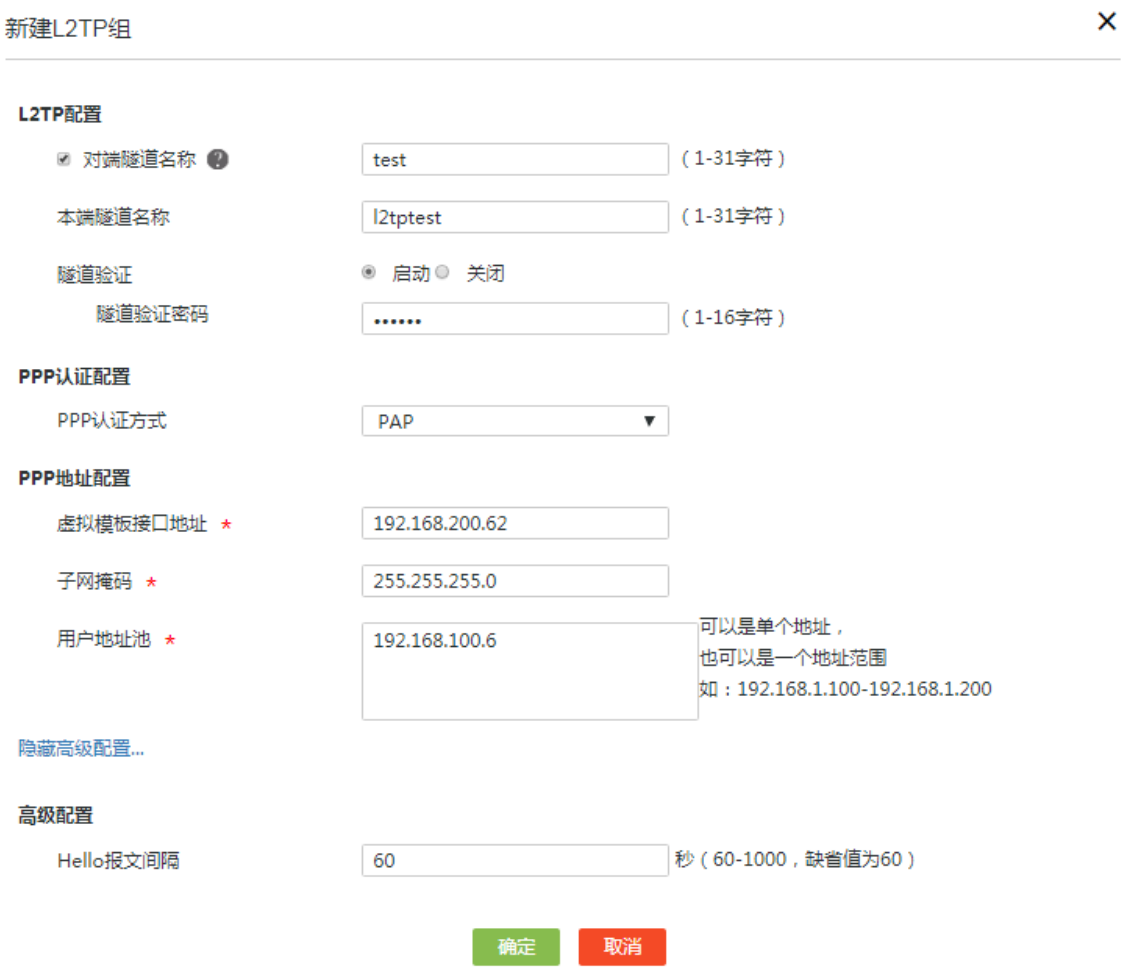
(7) 在“PPP 地址配置”下，设置 PPP 地址参数：

- 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“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) 单击<显示高级设置>按钮，展开高级配置页面。

(9) 在“高级配置”下“Hello 报文间隔”配置项处，输入保活报文的时间间隔。

(10) 点击<确定>按钮，完成配置。



11.2.3 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。

11.2.4 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) 点击<添加>按钮，弹出添加用户对话框。

(4) 在“帐号名”配置项处，输入用户的帐号名。

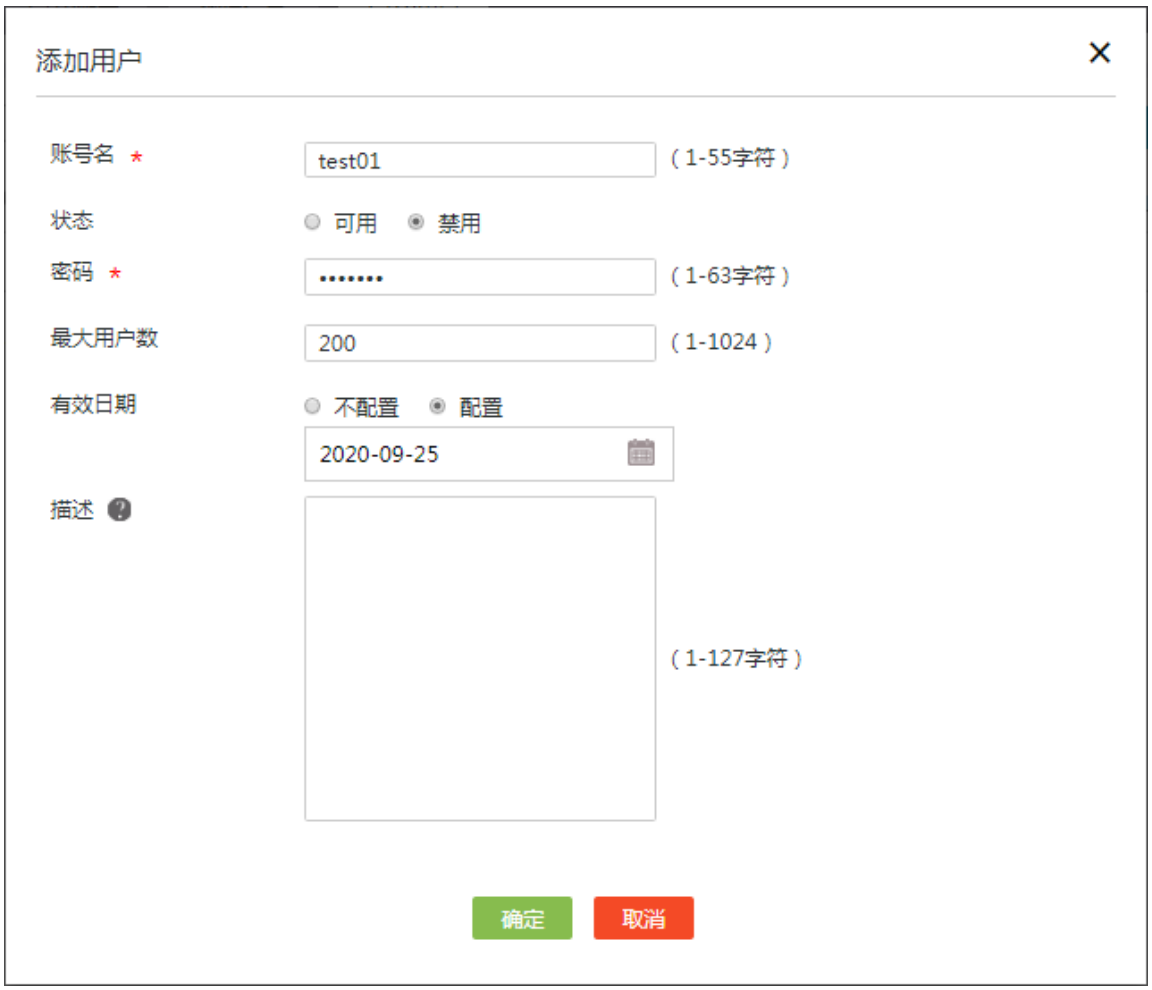
(5) 在“状态”配置项处，选择用户的状态是否可用。

(6) 在“密码”配置项处，输入用户帐号的密码。

(7) 在“最大用户数”配置项处，输入用户的最大连接数。

(8) 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。

(9) 点击<确定>按钮，完成配置。



11.3 L2TP客户端

11.3.1 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 服务器端来实现上述需求。

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。

11.3.2 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“开启”或“关闭”选项。
  - 如选择“开启”，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“关闭”，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“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。

(8) 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。

(9) 点击<确定>按钮，完成配置。

11.3.3 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。

12 高级选项

12.1 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：

1. 静态 DNS

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. 动态 DNS

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。

12.1.2 配置静态 DNS

(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。

12.1.3 配置动态 DNS

1. 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。

2. 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。

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“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。

12.2 UPnP

12.2.1 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。

12.2.2 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：

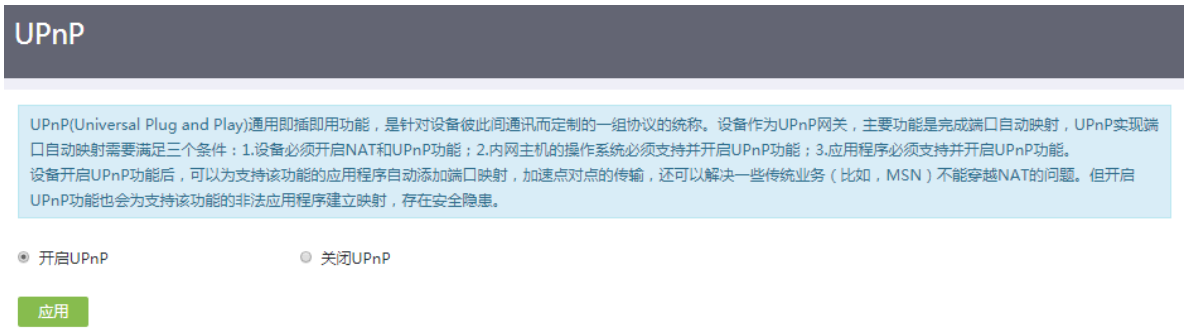
- 系统服务中禁止了 SSDP 服务（用于寻找 UPnP 设备），需要在系统服务中开启该服务。
- 开启了操作系统下的 SP1 的网络连接防火墙。操作系统的网络连接防火墙与 UPnP 设备发现有冲突，SP2 修复了这个问题，但是仍然需要在防火墙设置中允许例外：UPnP 框架。
- 应用软件或设备不支持 UPnP 功能。

12.2.3 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”，开启 UPnP 功能。

(3) 点击<应用>按钮，应用设置。



12.3 静态路由

12.3.1 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。

12.3.2 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。

12.3.3 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。

(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。

12.4 策略路由

12.4.1 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。

12.4.2 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。

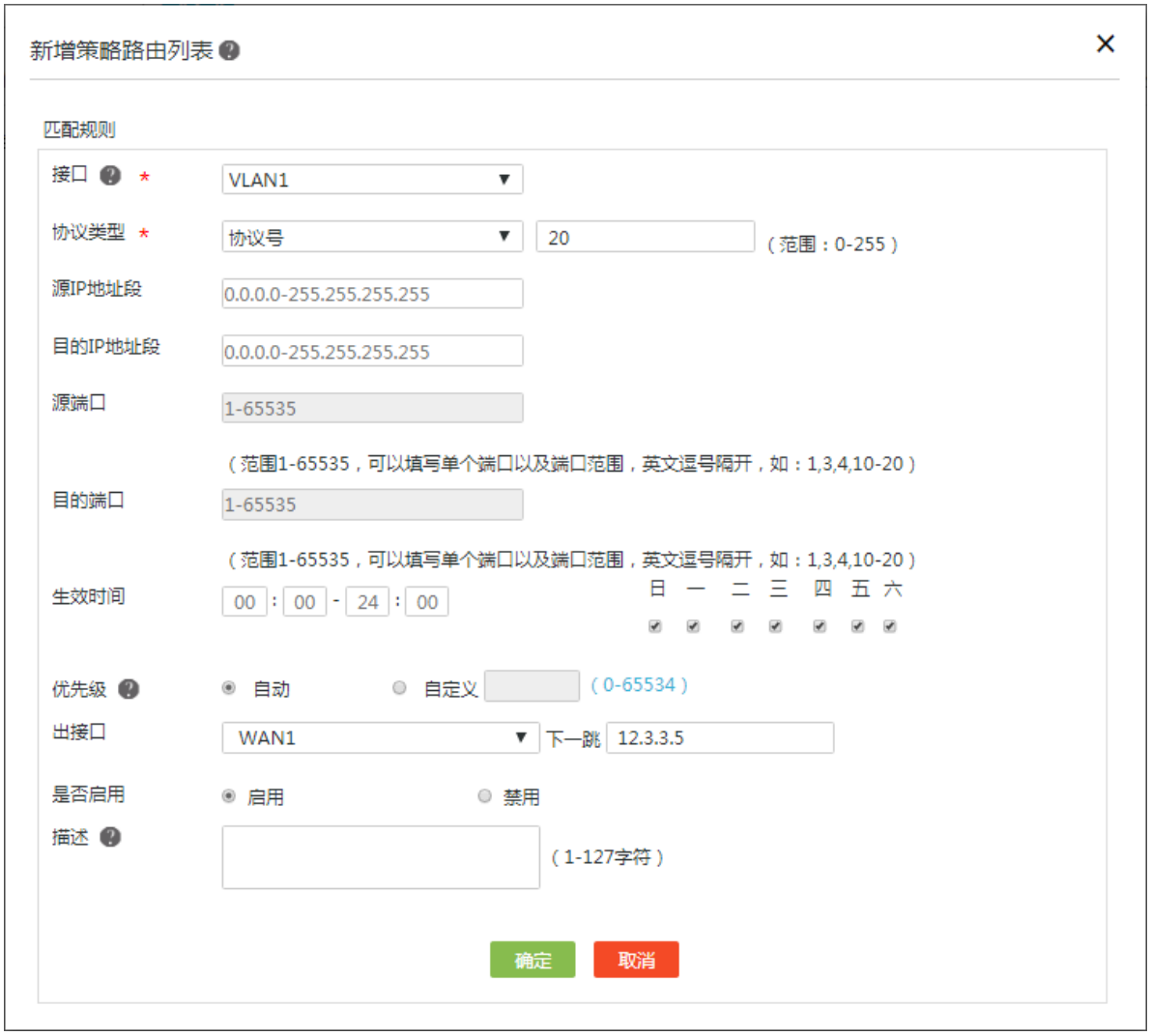
(2) 点击<添加>按钮，弹出新增策略路由列表对话框。

(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 HTTP 的协议号为 80。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。
- 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。

- 在“生效时间”配置项处，设置匹配规则的生效时间。如果策略需要全天生效，则设置为00:00-23:59。
- 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”或“下一跳”配置项处，设置匹配规则的报文通过指定出接口转发或转发到指定的下一跳。
- 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 系统工具

13.1 系统设置

13.1.1 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方式，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。

13.1.2 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。

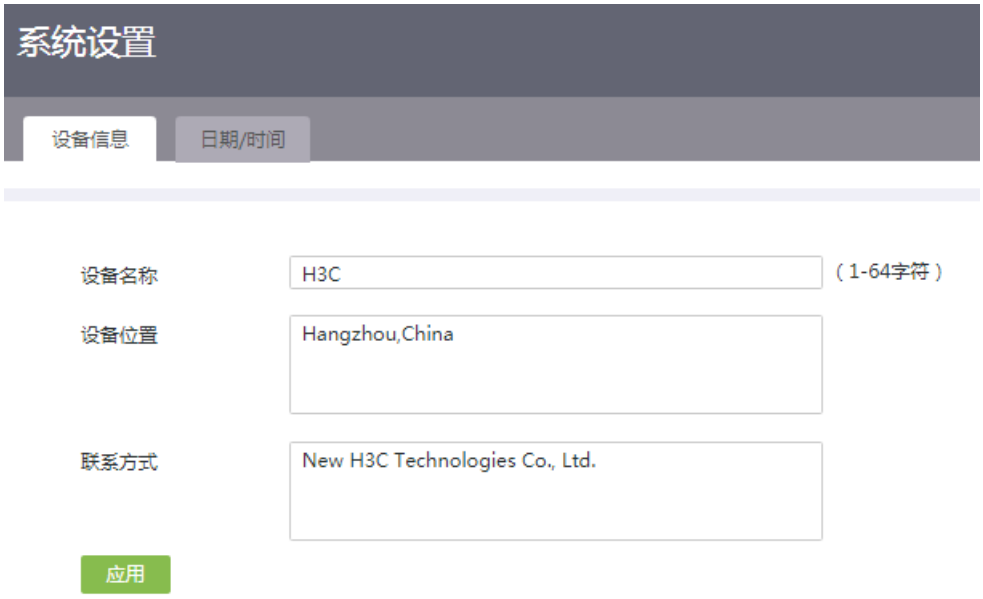
(2) 单击“设备信息”页签，进入设备信息配置页面。

(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。

(4) 在“设备位置”配置项处，输入设备的位置信息。

(5) 在“联系方式”配置项处，输入设备管理员的联系方式。

(6) 点击<应用>按钮，完成配置。



13.1.3 手工设置日期和时间

1. 注意事项

如果设备重启，系统时间将恢复到出厂时间。

2. 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)”。

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。

13.1.4 自动同步网络日期和时间

1. 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。

2. 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)”。

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。

(5) 在“NTP 服务器 2”配置项处，输入 NTP 服务器 2 的 IP 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。

13.2 网络诊断

13.2.1 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 通信测试：用于检测网络，测试另一台设备或主机是否可达。
- Tracert 通信测试：用于检查从设备到达目标主机所经过的路由情况。
- 诊断信息：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。
- 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。
- 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。本抓包工具使用 tcpdump 在后台运行，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。

13.2.2 Ping 通信测试

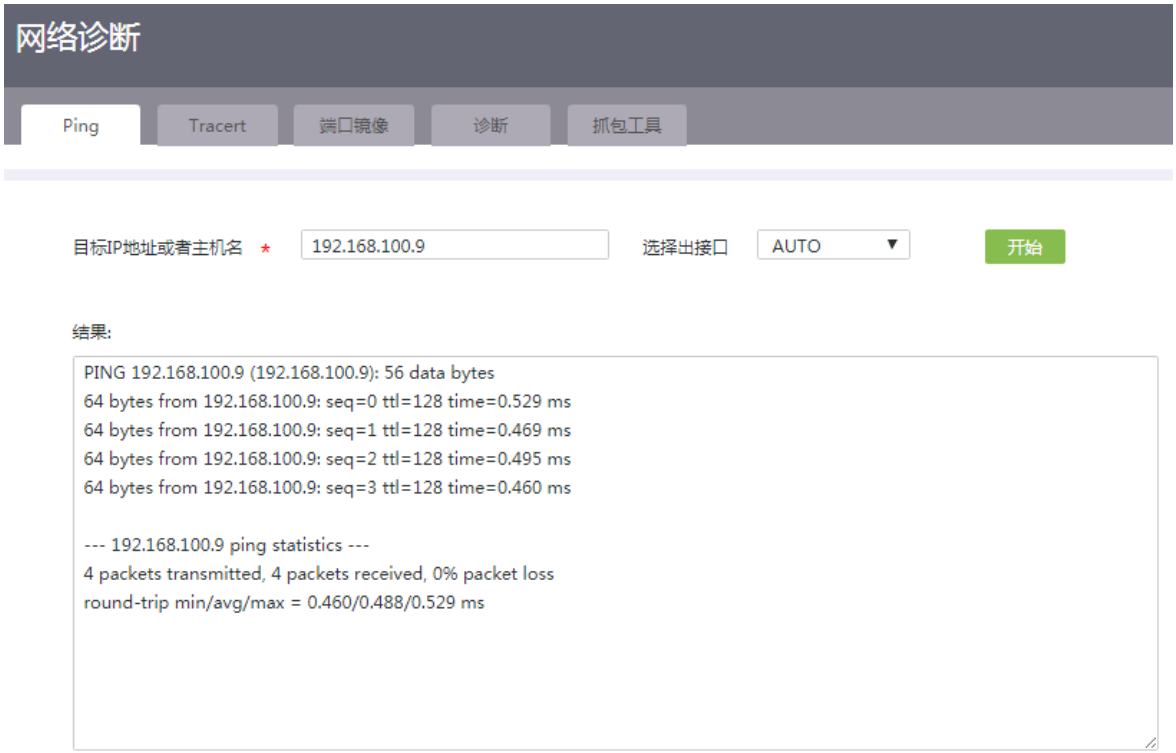
(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(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。

(4) 在“选择出接口”配置项处，选择需要检测的接口。

(5) 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。



13.2.3 Tracert 通信测试

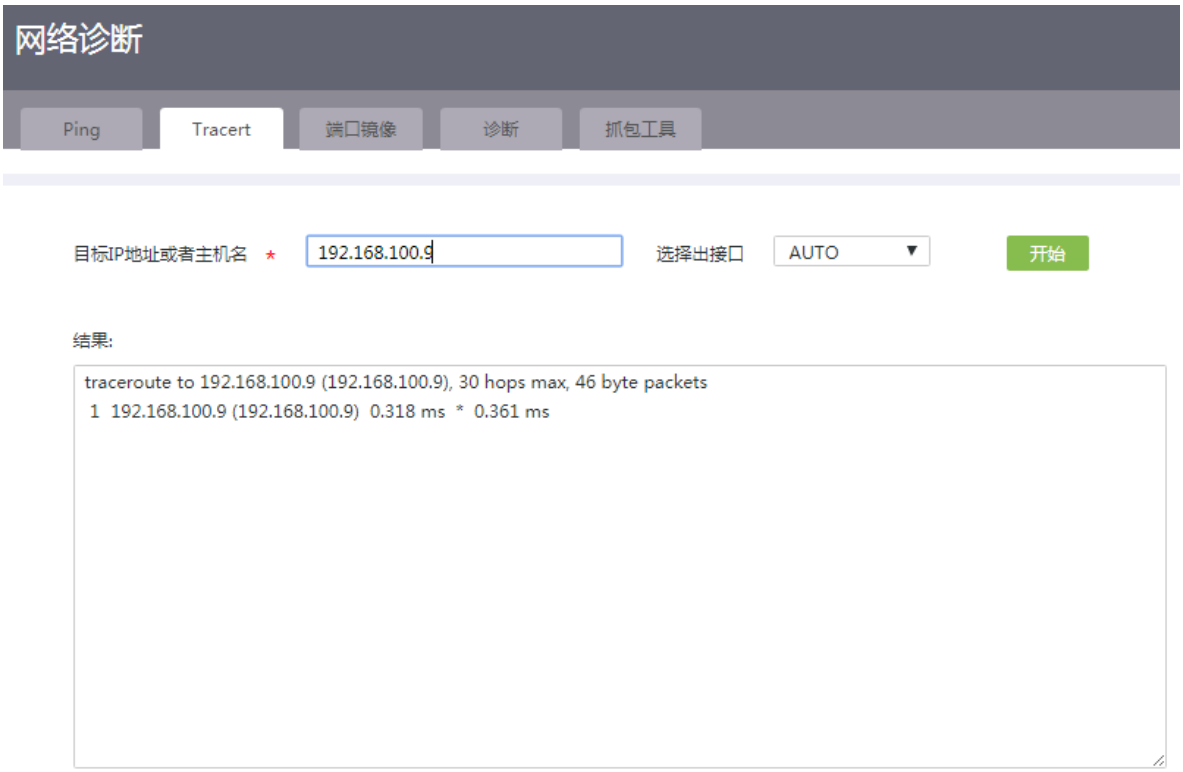
(1) 单击导航树中[系统工具/网络诊断]菜单项，进入网络诊断页面。

(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，选择需要检测的接口。

(5) 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。



13.2.4 诊断信息

(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。

13.2.5 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。

13.2.6 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。

(4) 在“方向”配置项处，选择镜像的方向。

(5) 在“目的端口”配置项处，选择镜像的目的端口。

(6) 点击<确定>按钮，系统开始端口镜像。

13.2.7 抓包工具

1. 注意事项

使用本页面进行抓包时，将会把抓取到的临时文件保存到系统中。随着临时文件占用空间持续增加到某个阀值时，系统会主动停止抓包并导出抓取的文件。

2. 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 tcpdump 数据包的抓取长度。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 tcpdump 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。

(7) 在“抓包时间”配置项处，输入抓包的持续时长。

(8) 在“方向”配置项处，选择抓取报文的方向。

(9) 在“源主机”、“目的主机”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”。

13.3 远程管理

13.3.1 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：实现设备在绿洲平台中被管理。

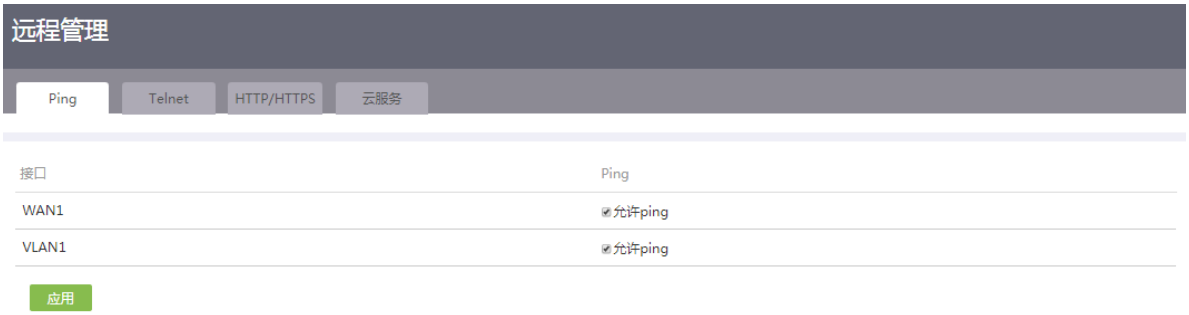
13.3.2 配置 Ping

(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。



13.3.3 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“管理员列表”区段，点击<添加/编辑>按钮，弹出添加/编辑管理员 IP 地址对话框。

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

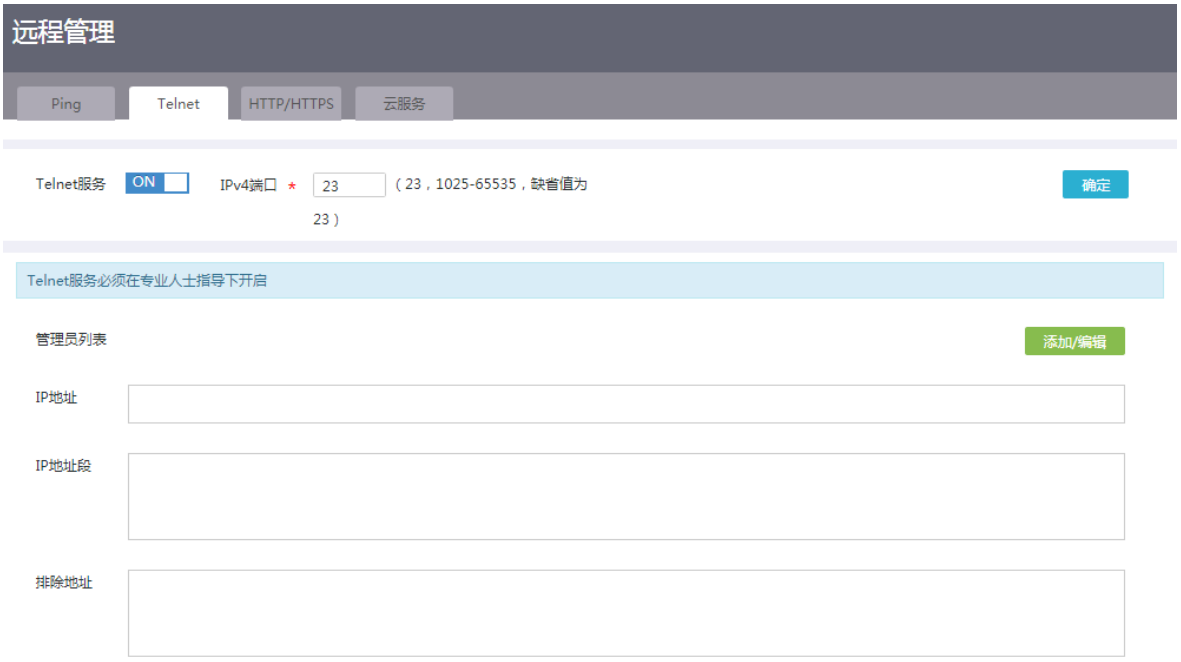
(6) 在 IP 地址范围“起始”和“结束”配置项处，分别输入允许通过 Telnet 访问设备的 IP 地址段的起始地址和结束地址。

(7) 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。

(8) 点击配置项右侧的<→>按钮，提交配置的地址组内容。

(9) 重复(5)、(6)、(7)步骤可完成多个地址组的添加。

(10) 点击<确定>按钮，完成配置。



13.3.4 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 管理界面的闲置超时时间，缺省为 10 分钟。管理员登录 Web 管理界面后，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。

(6) 在“管理员列表”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/编辑管理员 IP 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 地址范围“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，提交配置的地址组内容。

e. 重复(7)、(8)、(9)步骤可完成多个地址组的添加。

f. 点击<应用>按钮，完成配置。

(7) 在添加管理员列表完成后，若无需对 Web 管理页面的管理员 IP 地址或地址段进行限制，则勾选“不限制”选项即可。

13.3.5 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) 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。

(4) 在“云平台服务器域名”配置项处，输入绿洲平台的域名。

(5) 在“云场所定义”配置项处，输入设备的系统名称。

(6) 点击<应用>按钮，完成配置。

13.4 配置管理

13.4.1 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。

13.4.2 恢复出厂配置

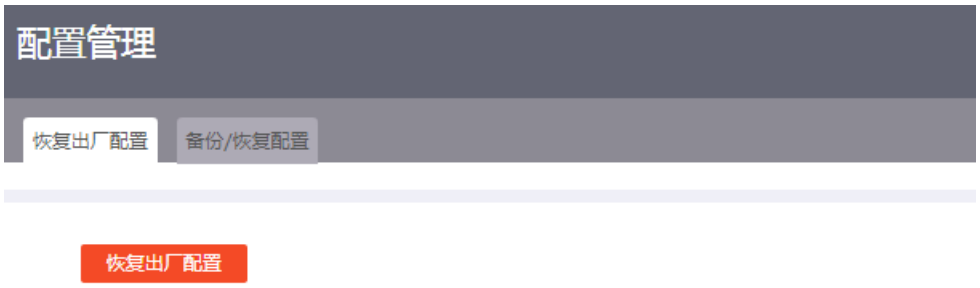
(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“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。



13.4.3 从备份文件恢复

(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。

- 勾选“立即执行导入后的配置文件”选项，系统会立即用导入的配置替换当前允许的配置，无需重启设备。点击<确定>按钮，立即开始恢复配置
- 不勾选“立即执行导入后的配置文件”选项，点击<确定>按钮后，需手动重启设备，才可以恢复配置。

13.4.4 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。

13.4.5 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。

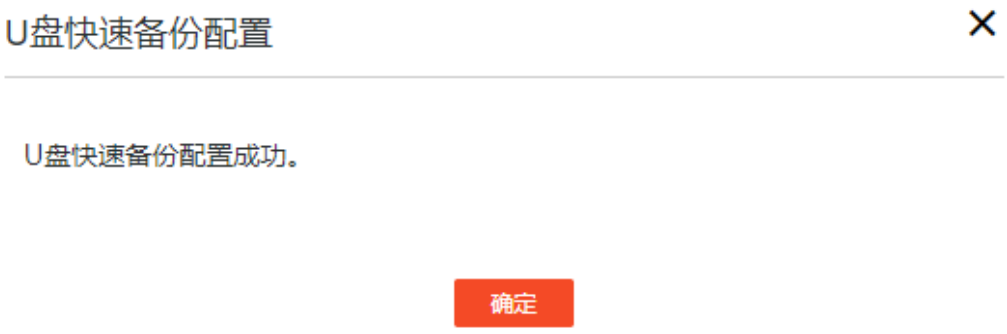
3. 配置步骤

(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。



13.4.6 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。

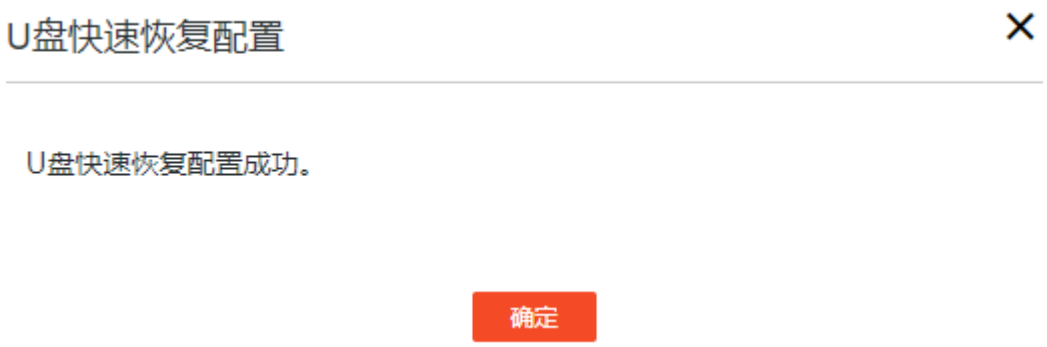
2. 配置步骤

(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。



13.5 系统升级

13.5.1 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。

13.5.2 软件升级

1. 注意事项

升级后的软件需要在设备重启后才能生效。请确保设备当前启动软件包列表存在备份的启动软件包，防止升级失败时能够使用备份的软件包。

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) 自动升级是通过绿洲云平台对设备的系统软件进行升级。自动升级前，设备需先连接云平台，并在云平台上传最新设备系统软件。升级步骤如下：

a. 点击<自动升级系统软件>按钮，弹出系统升级软件对话框。

b. 点击<确定>按钮，进行升级操作。

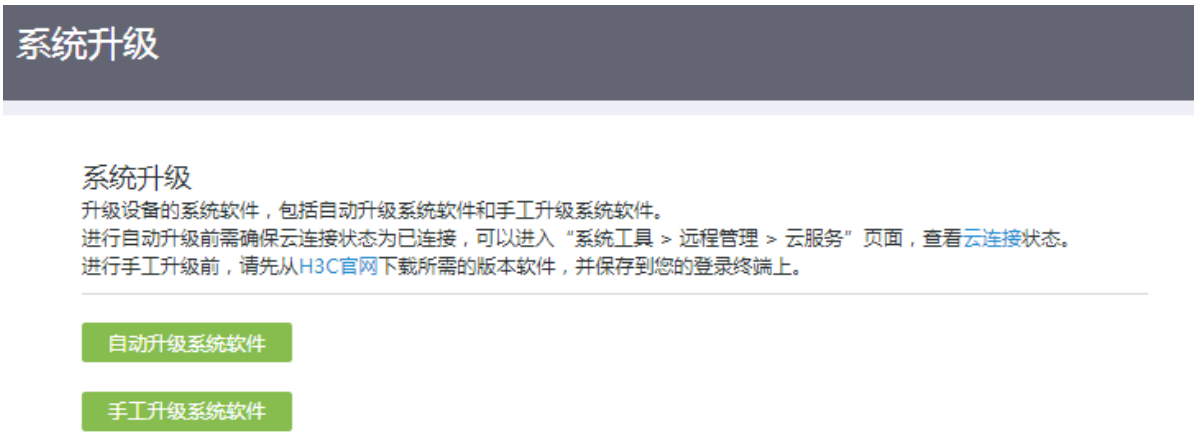
(3) 手动升级是通过特定路径下的系统软件文件对设备的系统软件进行升级。升级步骤如下：

a. 点击<手动升级系统软件>按钮，弹出升级系统文件对话框。

b. 点击“选择文件”按钮，选择特定路径下的系统软件文件。

c. 若需要保存当前设备的配置，则勾选“保存当前配置”选项；若无需保存当前设备的配置，则不勾选“保存当前配置”选项。

d. 点击<确定>按钮，开始软件升级。



13.6 重新启动

13.6.1 简介

重新启动功能用于立即和定时重新启动设备。

13.6.2 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。

13.6.3 定时重启

(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。

13.7 系统日志

13.7.1 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 13-1 所示的八个级别，各级别的严重性依照数值从 0～7 依次降低。了解日志级别，能帮助您迅速筛选出重点日志。

表13-1 日志级别列表

数值	信息级别	描述
0	emergency	表示设备不可用的信息，如系统授权已到期
1	alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	error	表示错误信息，如接口链路状态变化等
4	warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行ping命令的日志信息等
7	debugging	表示调试过程产生的信息

13.7.2 将系统日志发往日志服务器

1. 配置准备

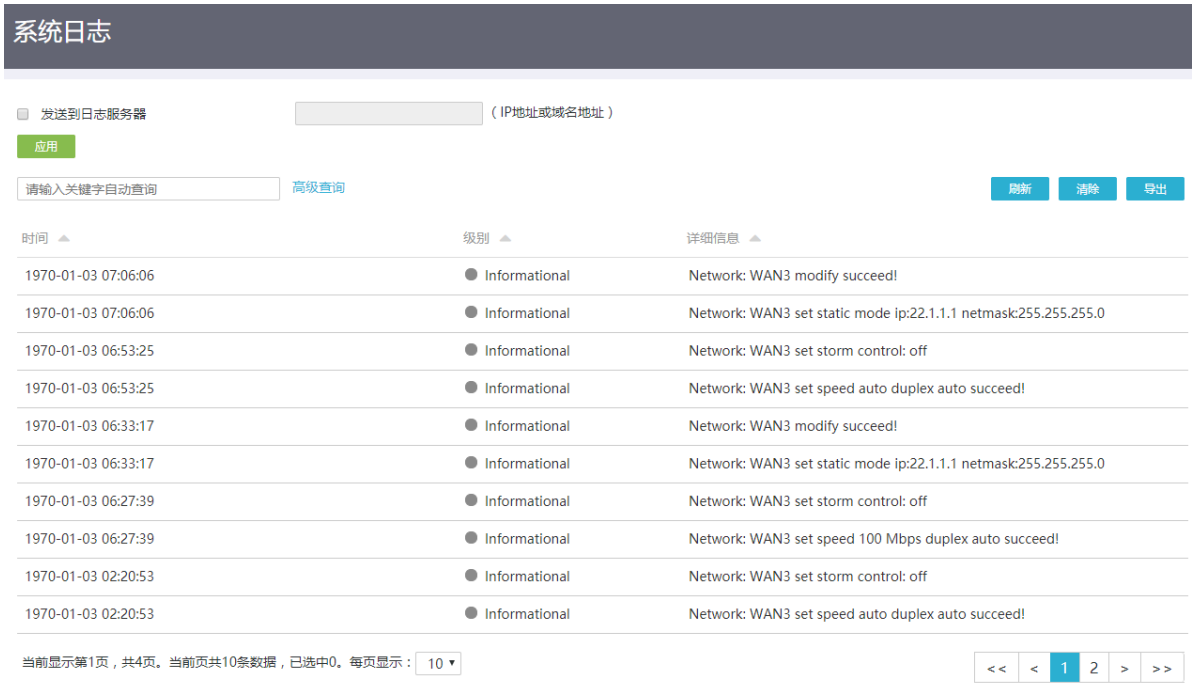
请确保设备和日志服务器能互相 ping 通，日志服务器才能收到设备发送的日志。

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) 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。

(3) 点击<应用>按钮，完成配置。



13.7.3 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) 点击<导出>按钮，可以将设备上已有的日志信息导出到登录 PC 上。

13.7.4 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。