H3C ER G3 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：F0165
资料版本：6W101-20250709

前 言

《H3C ER G3 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

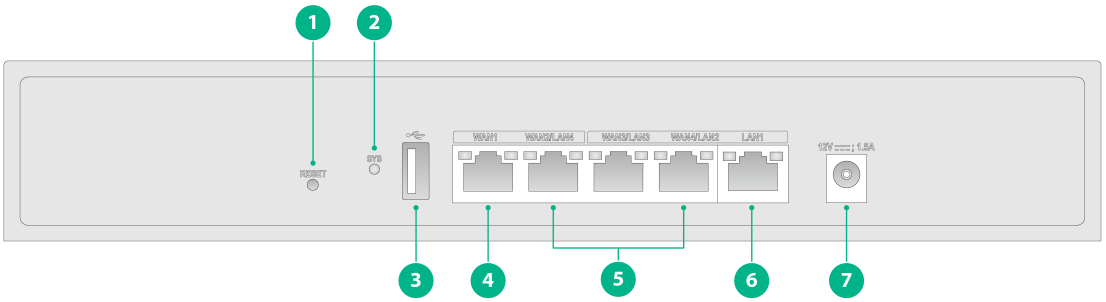
H3C ER G3 系列路由器包括如下产品型号。

名称	具体型号
H3C ER G3系列路由器	ER2200G3、ER3200G3、ER3200G3-X、ER3208G3、ER3208G3-P、ER3208G3-P-E、ER3208G3-X、ER3260G3、ER3260G3-X、ER5200G3、ER5200G3-X、ER6300G3、ER8300G3、ERG3-1800W

1.1 设备外观

1.1.1 ER2200G3

图1-1 ER2200G3 设备前面板



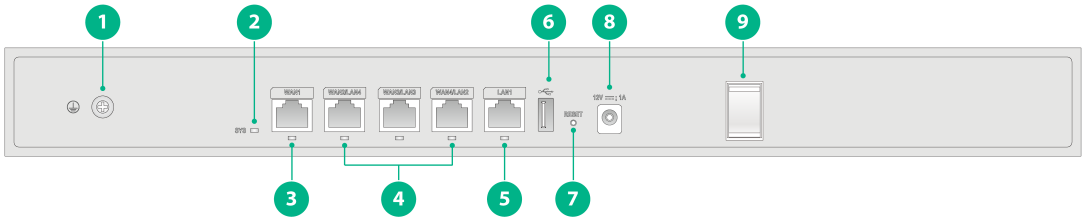
(1): 复位键（RESET）	(2): 系统指示灯（SYS）
(3): USB接口	(4): WAN接口及指示灯（10/100/1000Base-T电口）
(5): WAN/LAN接口及指示灯（10/100/1000Base-T电口）	(6): LAN接口及指示灯（10/100/1000Base-T电口）
(7): 电源接口	

图1-2 ER2200G3 设备后面板

(1): 接地螺钉

1.1.2 ER3200G3

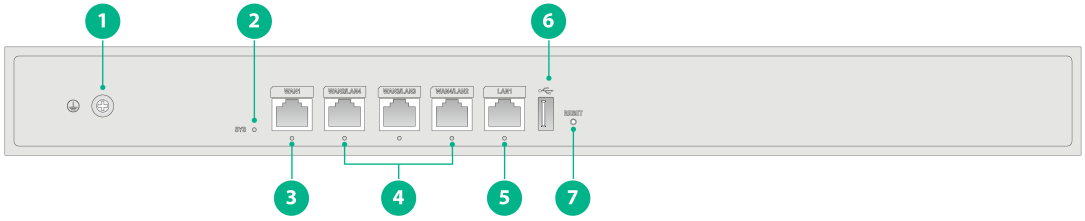
图1-3 ER3200G3 设备前面板



(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	

1.1.3 ER3200G3-X

图1-4 ER3200G3-X 设备前面板



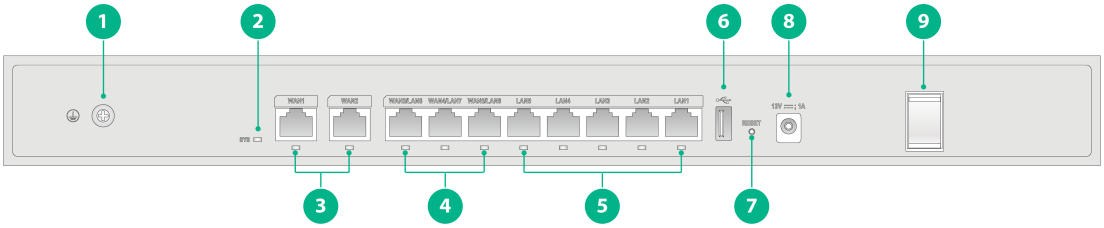
(1): 接地螺钉	(2): 系统指示灯（SYS）
(3): WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10/100/1000Base-T电口）
(5): LAN接口及指示灯（10/100/1000Base-T电口）	(6): USB接口
(7): 复位键（RESET）	

图1-5 ER3200G3-X 设备后面板

(1): 电源接口

1.1.4 ER3208G3

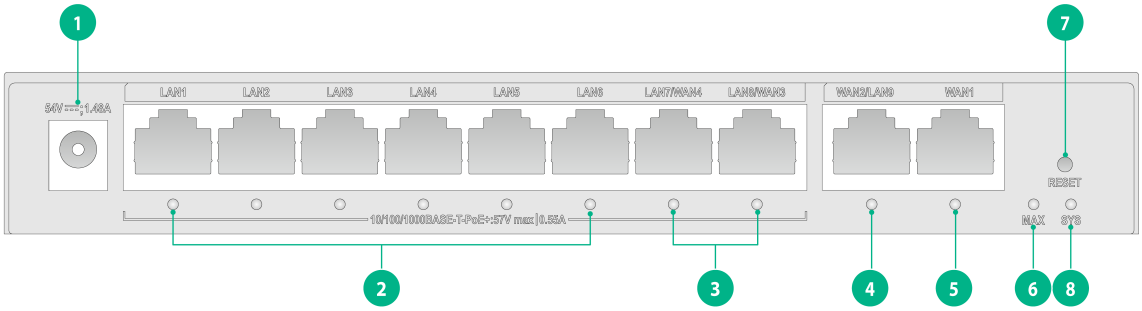
图1-6 ER3208G3 设备前面板



(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	

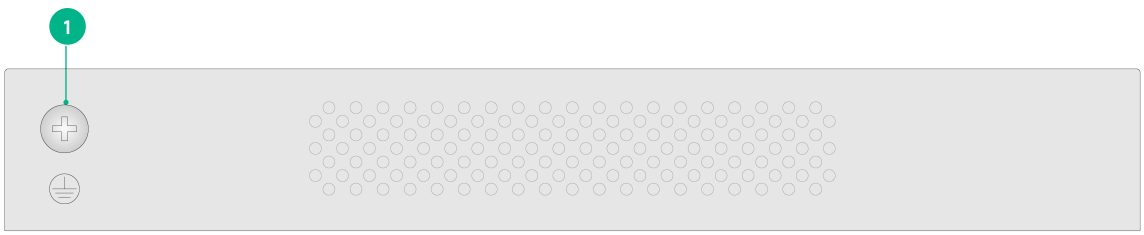
1.1.5 ER3208G3-P

图1-7 ER3208G3-P 设备前面板



(1): 电源接口	(2): LAN接口及指示灯（10/100/1000Base-T电口）
(3): LAN/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): WAN接口及指示灯（10/100/1000Base-T电口）	(6): PoE-MAX指示灯（MAX）
(7): 复位键（RESET）	(8): 系统指示灯（SYS）

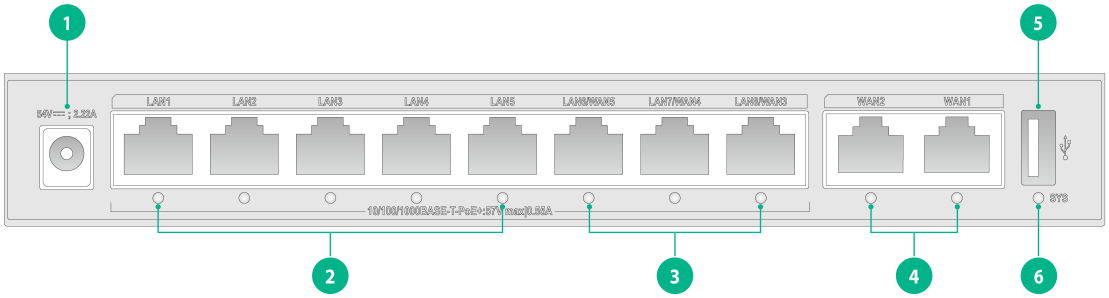
图1-8 ER3208G3-P 设备后面板



(1): 接地螺钉

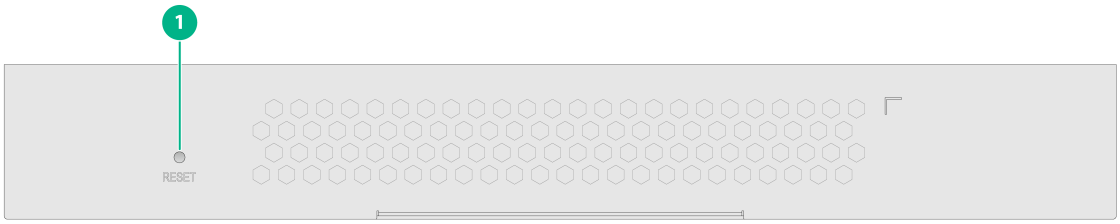
1.1.6 ER3208G3-P-E

图1-9 ER3208G3-P-E 设备前面板



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

图1-10 ER3208G3-P-E 设备后面板



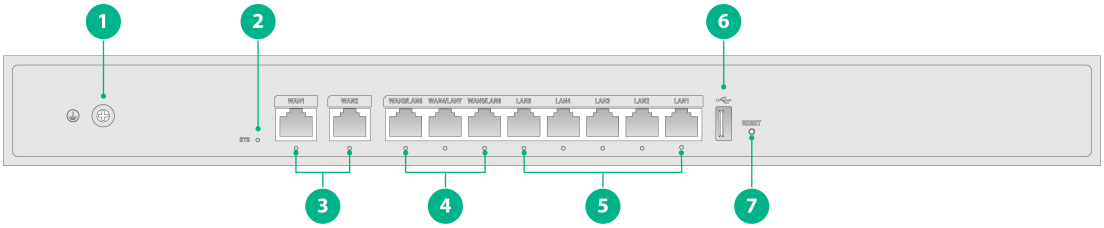
(1): 复位键（RESET）

图1-11 ER3208G3-P-E 设备右侧面板

(1): 接地螺钉

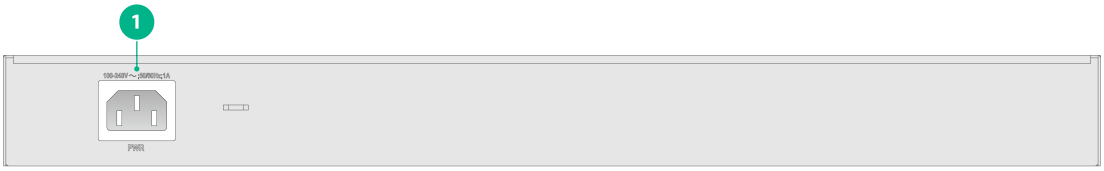
1.1.7 ER3208G3-X

图1-12 ER3208G3-X 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）	

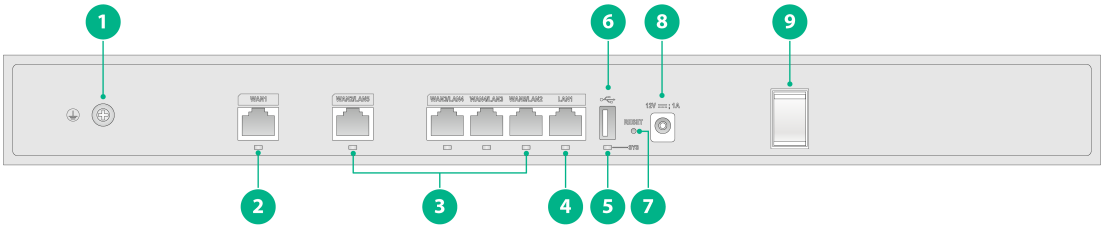
图1-13 ER3208G3-X 设备后面板



(1): 电源接口

1.1.8 ER3260G3

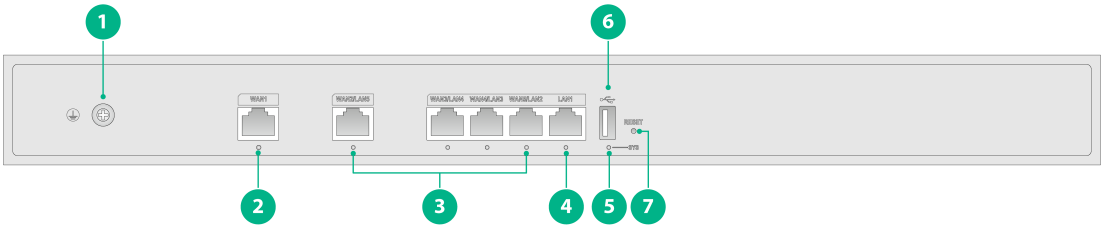
图1-14 ER3260G3 设备前面板



(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	

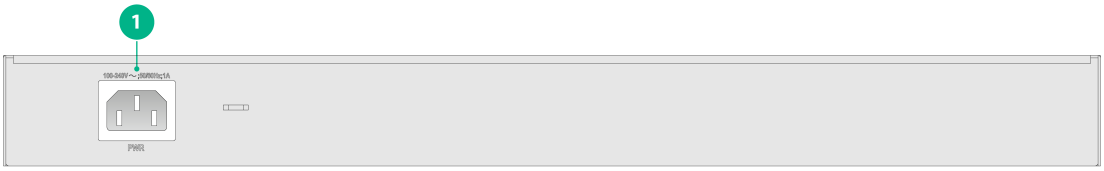
1.1.9 ER3260G3-X

图1-15 ER3260G3-X 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）	

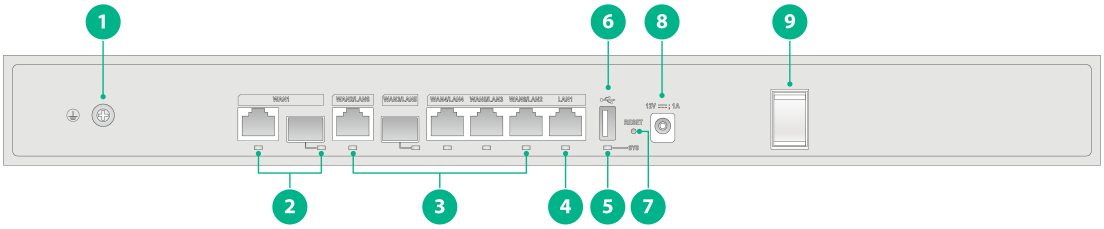
图1-16 ER3260G3-X 设备后面板



(1): 电源接口

1.1.10 ER5200G3

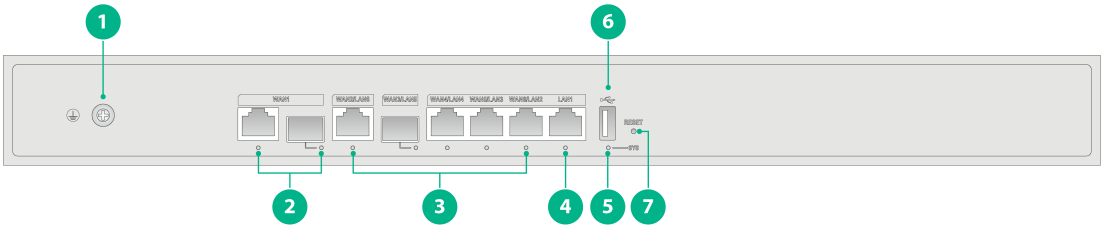
图1-17 ER5200G3 设备前面板



(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	

1.1.11 ER5200G3-X

图1-18 ER5200G3-X 设备前面板



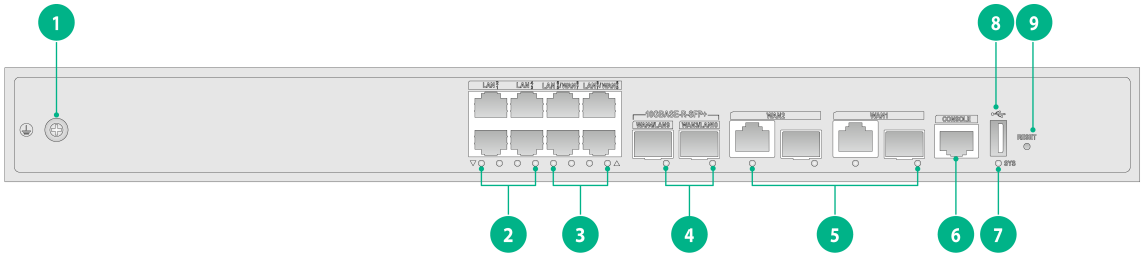
(1): 接地螺钉	(2): WAN接口及指示灯（Combo口）
(3): WAN/LAN接口及指示灯（10/100/1000Base-T电口、1000BASE-X-SFP光口）	(4): LAN接口及指示灯（10/100/1000Base-T电口）
(5): 系统指示灯（SYS）	(6): USB接口
(7): 复位键（RESET）	

图1-19 ER5200G3-X 设备后面板

(1): 电源接口

1.1.12 ER6300G3

图1-20 ER6300G3 设备前面板



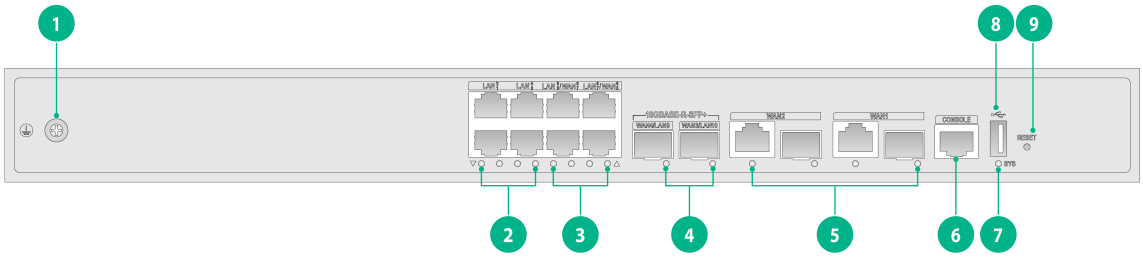
(1): 接地螺钉	(2): LAN接口及指示灯（10/100/1000Base-T电口）
(3): LAN/WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10GBASE-R-SFP+光口）
(5): WAN接口及指示灯（Combo口）	(6): Console接口
(7): 系统指示灯（SYS）	(8): USB接口
(9): 复位键（RESET）	

图1-21 ER6300G3 设备后面板

(1): 电源接口

1.1.13 ER8300G3

图1-22 ER8300G3 设备前面板



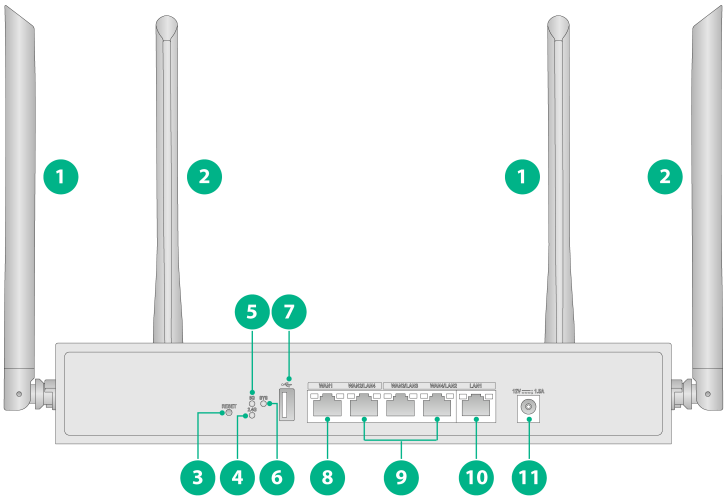
(1): 接地螺钉	(2): LAN接口及指示灯（10/100/1000Base-T电口）
(3): LAN/WAN接口及指示灯（10/100/1000Base-T电口）	(4): WAN/LAN接口及指示灯（10GBASE-R-SFP+光口）
(5): WAN接口及指示灯（Combo口）	(6): Console接口
(7): 系统指示灯（SYS）	(8): USB接口
(9): 复位键（RESET）	

图1-23 ER8300G3 设备后面板

(1): 电源接口

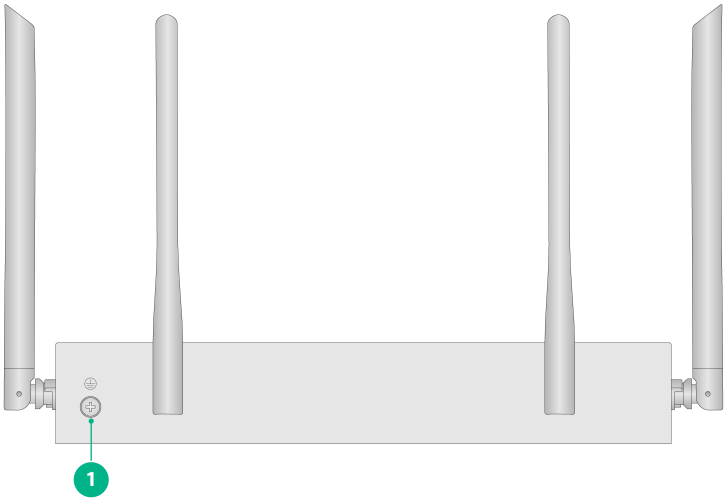
1.1.14 ERG3-1800W

图1-24 ERG3-1800W 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1-25 ERG3-1800W 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ER3200G3、ER3200G3-X、ER3208G3、ER3208G3-P、ER3208G3-P-E、ER3208G3-X、ER3260G3、ER3260G3-X、ER5200G3、ER5200G3-X、ER6300G3、ER8300G3）	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ER2200G3、ERG3-1800W）	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
SFP光口状态指示灯	绿色常亮	端口正常连接设备，且工作在1000Mbps速率下
	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+光口状态指示灯	绿色常亮	端口正常连接设备，且工作在10Gbps速率下
	绿色闪烁	端口在接收或发送数据，且工作在10Gbps速率下
	黄色常亮	端口正常连接设备，且工作在1000Mbps速率下
	黄色闪烁	端口在接收或发送数据，且工作在1000Mbps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
	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

指示灯	状态	含义
	灯灭	5G射频关闭
PoE-MAX指示灯	绿色常亮	PoE路由器供电的功率在其保护功率范围以内，保护功率范围为60W~75W
	灯灭	PoE路由器供电的功率未达到保护功率范围的最小值

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
LAN/WAN接口、WAN/LAN接口	• 既可以作为 LAN 接口使用，也可以作为 WAN 接口使用 • 该接口默认是 LAN 接口还是 WAN 接口，取决于该接口的颜色底纹。黄色底纹代表该接口默认为 WAN 接口；绿色底纹代表该接口默认为 LAN 接口
Console接口	计算机通过连接Console口登录路由器进行命令行设置
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 技术规格

项目	ER2200G3	ER3200G3	ER3200G3-X	ER3208G3
外形尺寸（宽×深×高）	266mm×161mm×44mm	440mm×230mm×44mm	440mm×230mm×44mm	440mm×230mm×44mm
功耗	＜18W	＜10W	＜12W	＜12W
电源适配器额定输入电压	100V AC～240V AC，50/60Hz	100V AC～240V AC，50/60Hz	-	100V AC～240V AC，50/60Hz
设备电源输入	12V±5% / 1.5A	12V±5% / 1A	100V AC～240V AC，50/60Hz	12V±5% / 1A

项目	ER2200G3	ER3200G3	ER3200G3-X	ER3208G3
单端口最大输出功率	-	-	-	-
PoE负载功率	-	-	-	-
重量	0.8Kg	3Kg	2.5Kg	3Kg
Console接口	-	-	-	-
USB接口	1个USB3.0接口	1个USB2.0接口	1个USB2.0接口	1个USB2.0接口
LAN接口	3个千兆电口（2个可切WAN）	3个千兆电口（2个可切WAN）	3个千兆电口（2个可切WAN）	8个千兆电口（3个可切WAN）
WAN接口	2个千兆电口（1个可切LAN）	2个千兆电口（1个可切LAN）	2个千兆电口（1个可切LAN）	2个千兆电口（不可切LAN）
技术标准	-	-	-	-
WLAN天接	-	-	-	-
无线速率	-	-	-	-
工作温度	0ºC～45ºC	0ºC～45ºC	0ºC～45ºC	0ºC～45ºC
工作湿度	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露
散热方式	自然散热	自然散热	自然散热	自然散热

项目	ER3208G3-P	ER3208G3-P-E	ER3208G3-X
外形尺寸（宽×深×高）	190mm×125mm×27mm	202mm×104mm×28mm	440mm×230mm×44mm
功耗	＜80W	＜120W	＜12W
电源适配器额定输入电压	100V AC～240V AC，50/60Hz	100V AC～240V AC，50/60Hz	-
设备电源输入	54V±5% / 1.48A	54V±5% / 2.22A	100V AC～240V AC，50/60Hz
单端口最大输出功率	30W	30W	-
PoE负载功率	75W	110W	-
重量	0.5Kg	0.7Kg	2.5Kg
Console接口	-	-	-
USB接口	-	1个USB2.0接口	1个USB2.0接口
LAN接口	8个千兆电口（2个可切WAN）	8个千兆电口（3个可切WAN）	8个千兆电口（3个可切WAN）
WAN接口	2个千兆电口（1个可切LAN）	2个千兆电口（1个可切LAN）	2个千兆电口（1个可切LAN）
技术标准	-	-	-

项目	ER3208G3-P	ER3208G3-P-E	ER3208G3-X
WLAN天线	-	-	-
无线速率	-	-	-
工作温度	0ºC～40ºC	0ºC～40ºC	0ºC～45ºC
工作湿度	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露
散热方式	自然散热	自然散热	自然散热

项目	ER3260G3	ER3260G3-X	ER5200G3	ER5200G3-X
外形尺寸（宽×深×高）	440mm×230mm×44mm	440mm×230mm×44mm	440mm×230mm×44mm	440mm×230mm×44mm
功耗	＜10W	＜12W	＜12W	＜12W
电源适配器额定输入电压	100V AC～240V AC，50/60Hz	-	100V AC～240V AC，50/60Hz	-
设备电源输入	12V±5% / 1A	100V AC～240V AC，50/60Hz	12V±5% / 1A	100V AC～240V AC，50/60Hz
重量	3Kg	2.5Kg	3Kg	2.5Kg
Console接口	-	-	-	-
USB接口	1个USB2.0接口	1个USB2.0接口	1个USB2.0接口	1个USB2.0接口
LAN接口	4个千兆电口（3个可切WAN）	4个千兆电口（3个可切WAN）	4个千兆电口（3个可切WAN）	4个千兆电口（3个可切WAN）
WAN接口	2个千兆电口（1个可切LAN）	2个千兆电口（1个可切LAN）	• 1 个 Combo 口（不可切 LAN） • 1 个千兆电口（可切 LAN） • 1 个千兆光口（可切 LAN）	• 1 个 Combo 口（不可切 LAN） • 1 个千兆电口（可切 LAN） • 1 个千兆光口（可切 LAN）
技术标准	-	-	-	-
WLAN天线	-	-	-	-
无线速率	-	-	-	-
工作温度	0ºC～45ºC	0ºC～45ºC	0ºC～45ºC	0ºC～45ºC
工作湿度	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露
散热方式	自然散热	自然散热	自然散热	自然散热

项目	ERG3-1800W	ER6300G3	ER8300G3
外形尺寸（宽×深×高）	266mm×161mm×44mm	440mm×230mm×44mm	440mm×230mm×44mm

项目	ERG3-1800W	ER6300G3	ER8300G3
功耗	＜18W	＜36W	＜36W
电源适配器额定输入电压	100V AC～240V AC，50/60Hz	-	-
设备电源输入	12V±5% / 1.5A	100V AC～240V AC，50/60Hz	100V AC～240V AC，50/60Hz
重量	0.8Kg	2.7Kg	2.85Kg
Console接口	-	1个	1个
USB接口	1个USB3.0接口	1个USB3.0接口	1个USB3.0接口
LAN接口	3个千兆电口（2个可切WAN）	8个千兆电口（4个可切WAN）	8个千兆电口（4个可切WAN）
WAN接口	2个千兆电口（1个可切LAN）	• 2 个 Combo 口（不可切 LAN） • 2 个万兆光口（可切 LAN）	• 2 个 Combo 口（不可切 LAN） • 2 个万兆光口（可切 LAN）
技术标准	• IEEE802.11ax/n/b/g • IEEE802.11ax/ac/a/n	-	-
WLAN天线	• 2 个 2.4G 高增益天线 • 2 个 5G 高增益天线	-	-
无线速率	1800Mbps	-	-
工作温度	0ºC～45ºC	0ºC～45ºC	0ºC～45ºC
工作湿度	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露	5%RH～95%RH，非凝露
散热方式	自然散热	风扇散热	风扇散热

2 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。

2.1 安装前注意事项

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：

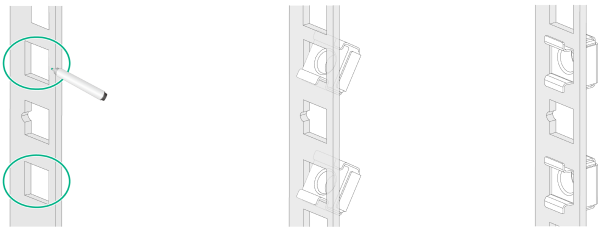
- 设备仅允许在室内使用，请将其放置于干燥通风处；
- 设备的接口线缆要求在室内走线，禁止户外走线，以防止因雷电产生的过电压、过电流损坏设备的信号口；
- 请不要将设备放在不稳定的箱子或桌子上，一旦跌落，会对设备造成损害；
- 在设备周围应预留足够的空间（大于 10cm），以便于设备正常散热；
- 请保证设备工作环境的清洁，过多的灰尘会造成静电吸附，不但会影响设备寿命，而且容易造成通信故障；
- 设备工作地的接地装置最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；
- 设备工作地应远离强功率无线电发射台、雷达发射台、高频大电流设备；
- 请使用随产品附带的电源线，严禁使用其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

2.2 安装到机柜

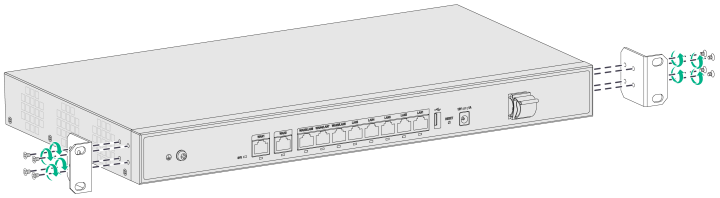
说明

仅 ER3208G3-P、ER3208G3-P-E 和 ERG3-1800W 不支持安装到机柜。

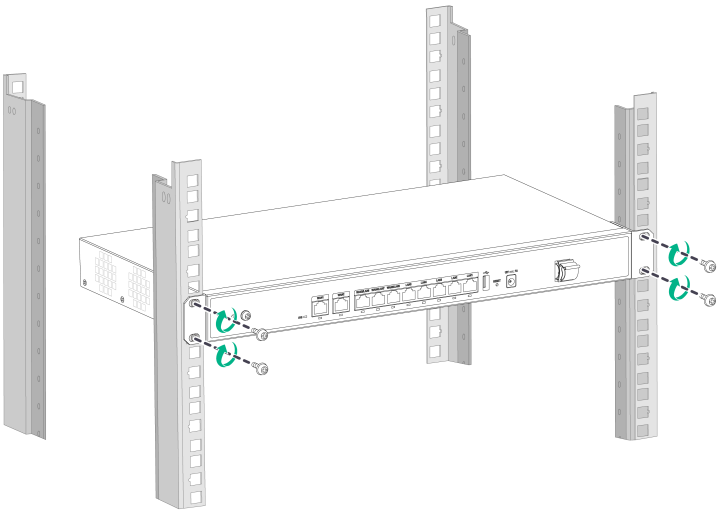
2.2.1 安装浮动螺母



2.2.2 安装挂耳



2.2.3 安装设备到机柜

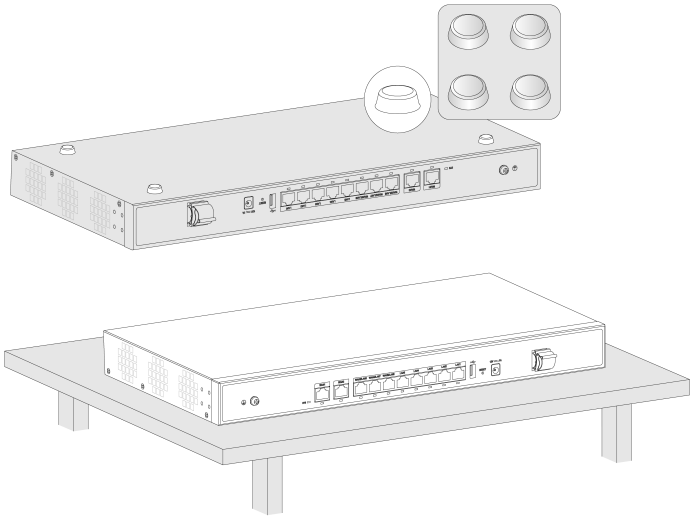


2.3 安装到工作台

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。



2.4 连接线缆

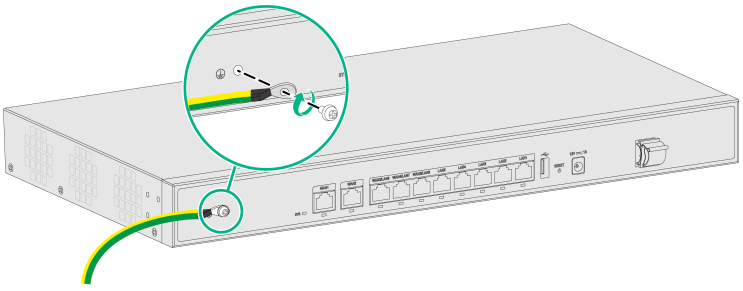
2.4.1 连接接地线

说明

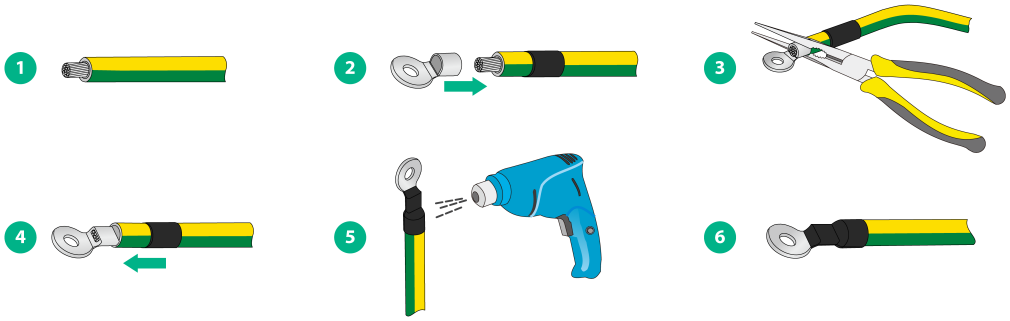
仅 ERG3-1800W 随机不附带接地线，只提供一个 OT 端子，接地线需要用户自行购买安装。

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 ERG3-1800W 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。



2.4.2 连接 Console 口电缆并设置配置终端参数

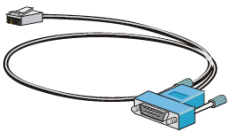
1. 配置串口线介绍

说明

- 仅 ER6300G3 和 ER8300G3 支持 Console 接口。
- Console 口配置电缆不随机提供，请用户根据实际需要自行选购。

设备提供了两种 Console 口配置电缆用于连接设备和配置终端，具体请参见下表。

表2-1 配置电缆介绍

配置电缆类型	图示	设备侧连接器类型	配置终端侧连接器类型	连接方法
DB9-to-RJ45 Console口配置电缆		DB-9孔式插头	RJ-45	请参见：2. 使用 DB9-to-RJ45 Console 口配置电缆进行连接
USB-to-RJ45 Console口配置电缆		USB口	RJ-45	请参见：3. 使用 USB-to-RJ45 Console 口配置电缆进行配置连接

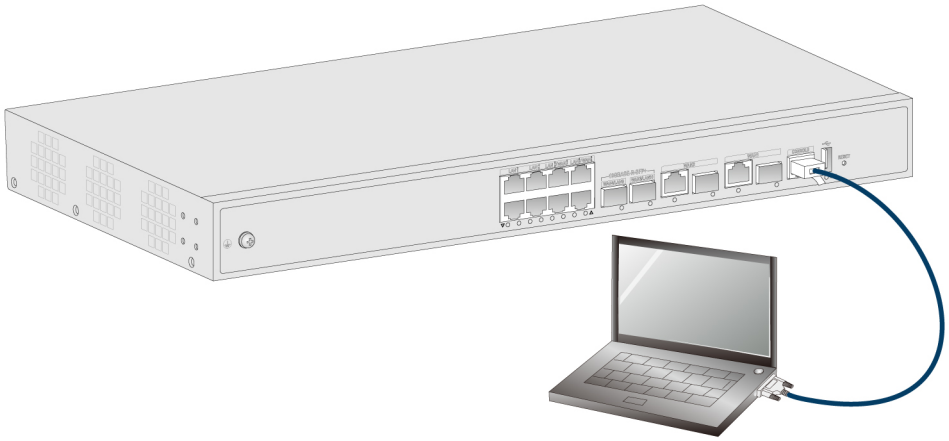
2. 使用 DB9-to-RJ45 Console 口配置电缆进行连接

通过配置串口线连接路由器的步骤如下：

(1) 选定配置终端，配置终端可以是标准的具有 RS-232 串口的字符终端，也可以是一台普通的 PC 机，更常用的是后者。

(2) 将 Console 口电缆带有 RJ45 连接器的一端连接到路由器的 Console 口，将带有 DB9（母）连接器的另一端连接到 PC 的串口。

图2-1 通过配置串口线连接路由器



注意

- PC 通过 Console 口电缆与路由器连接时，应先连接 Console 口电缆的 DB9 端到 PC 的 RS-232 接口，再连接 Console 口电缆的 RJ45 连接器到路由器的 Console 口。
- 当 PC 没有 RS-232 接口只有 USB 接口时，需要使用 USB 转 RS-232 转接器连接到 Console 口电缆，并正确安装相应的驱动程序。

3. 使用 USB-to-RJ45 Console 口配置电缆进行配置连接

说明

- 通过 USB-to-RJ45 口配置电缆进行配置连接时，用户需要到 H3C 官方网站或扫描电缆包装袋上的二维码下载对应的驱动程序，并将驱动程序安装到配置终端上。
- 请先安装驱动程序再连接配置电缆。若您安装驱动程序时，已完成配置电缆的安装，安装完驱动程序后，需要重新插拔配置终端侧的 USB 口。

以下以安装驱动程序到 Windows 系统为例进行介绍。安装驱动程序到其它操作系统的安装方式，请参照驱动程序压缩包中对应文件夹（文件夹按照操作系统类型命名）内的相关的安装指导文档。

USB-to-RJ45 Console 口配置电缆连接步骤如下：

(1) 通过单击如下链接或者将链接拷贝到浏览器的地址栏，登录到 USB-to-RJ45 Console 驱动的下载界面，将驱动程序下载并保存在本地。

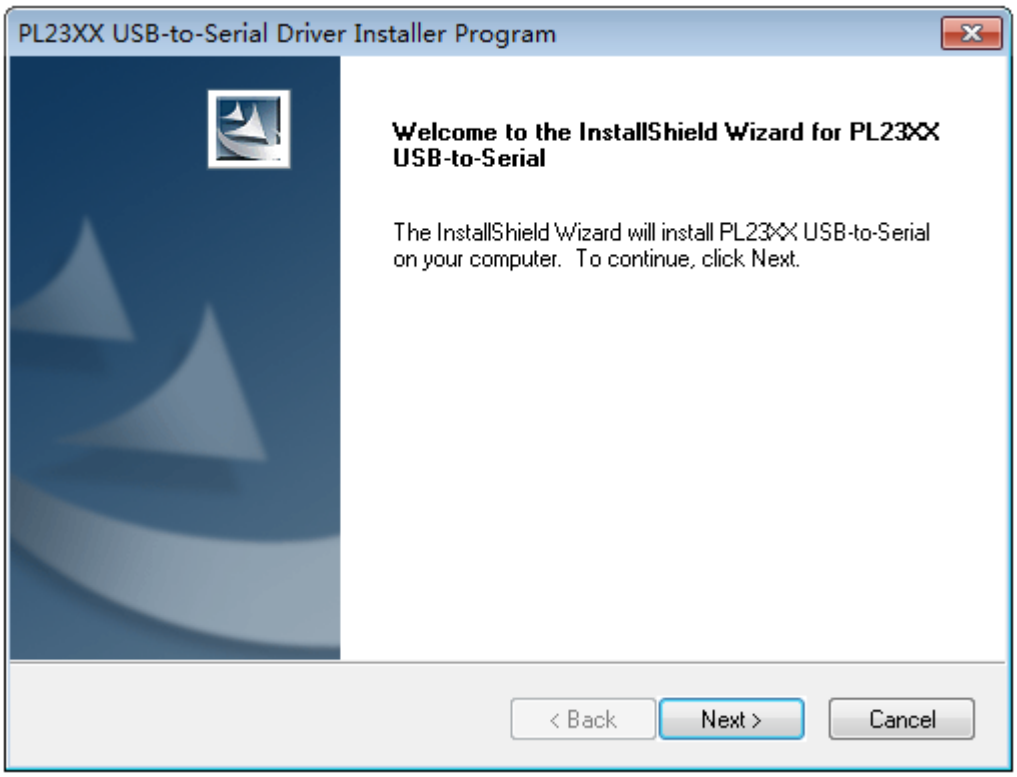
https://www.h3c.com/cn/Home/QR/USB_to_RJ45_Console.htm

(2) 通过查看 Windows 文件夹下的“Read me.txt”文件，判断配置终端操作系统软件版本是否支持该驱动程序。

(3) 如果支持，请安装驱动程序“PL23XX-M_LogoDriver_Setup_v200_20190815.exe”。

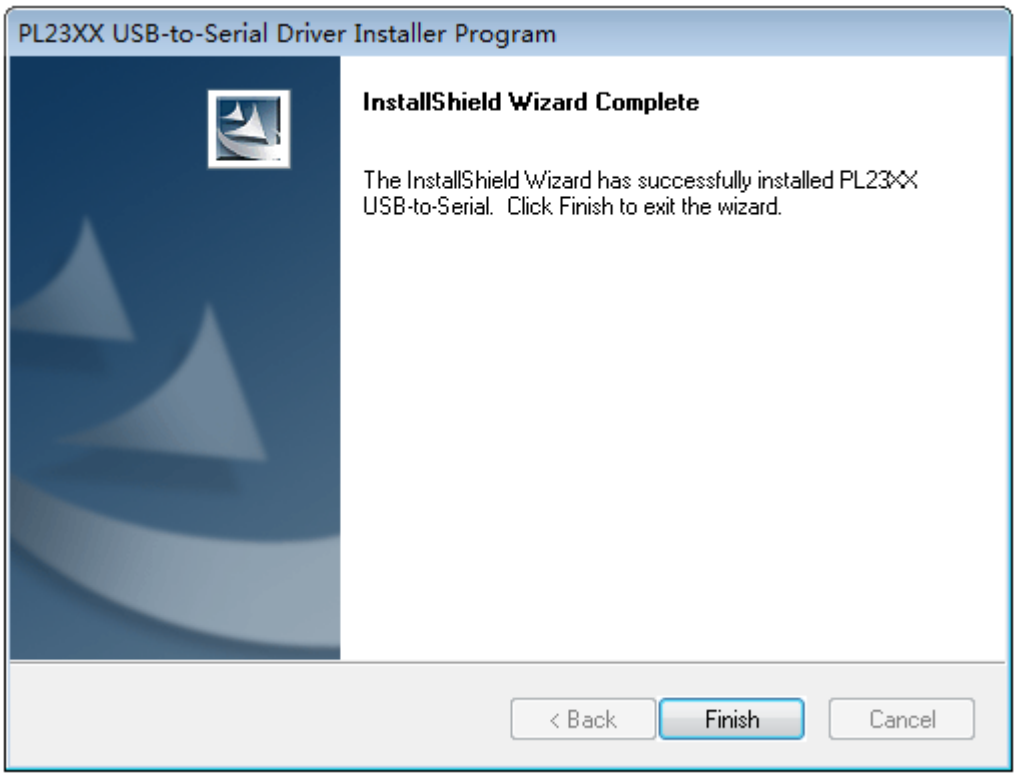
(4) 在安装向导的欢迎页面，点击<Next>按钮。

图2-2 安装向导欢迎页面



(5) 驱动程序安装完成，点击<Finish>按钮，退出向导。

图2-3 安装向导完成页面



(6) 将标准 USB 接头端连接 PC。

(7) 将另一端 RJ45 接头连接到设备的 Console 口。

4. 设置配置终端的参数

在通过 Console 口搭建本地配置环境时，需要通过超级终端或 PuTTY 等终端仿真程序与设备建立连接。用户可以运行这些程序来连接网络设备、Telnet 或 SSH 站点，这些程序的详细介绍和使用方法请参见该程序的使用指导。

打开终端仿真程序后，请按如下要求设置终端参数：

- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

2.4.3 连接电源线

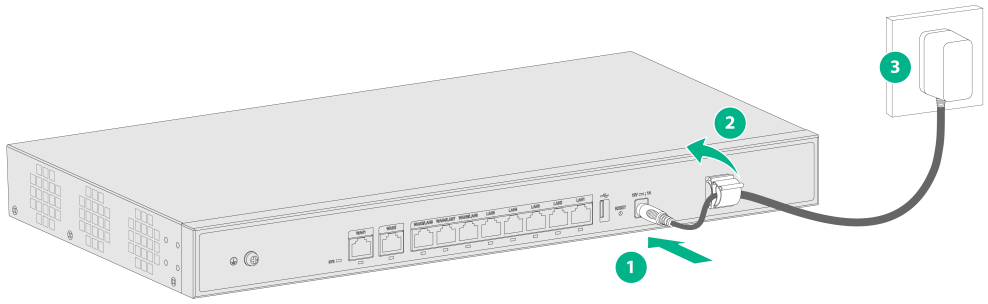
说明

- 仅 ER3200G3-X、ER3208G3-X、ER3260G3-X、ER5200G3-X、ER6300G3 和 ER8300G3 支持直接连接交流电源线，其它款型需要连接电源适配器进行供电。
- 请使用设备随机附带的电源适配器供电，避免因功率不足造成的适配器损毁。
- 连接电源线之前，请确保设备已正确接地。

1. 连接电源适配器

(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。

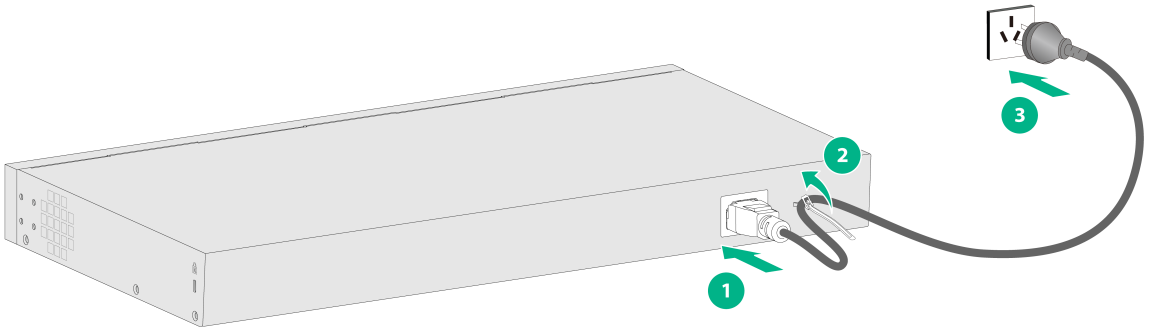
(2) 再将另一端连接到外部的交流电源插座上。



2. 连接交流电源线

(1) 将交流电源线一端插到路由器的交流电源插座上，并用扎带固定。

(2) 再将另一端连接到外部的交流电源插座上。



3 登录设备

说明

建议使用 Chrome 64 及以上版本、Firefox 78 及以上版本、Edge 79 及以上版本的浏览器访问 Web 管理页面。

设备登录步骤如下：

1. 将 PC 连接到设备的 LAN 接口
2. 配置 PC 为自动获取 IP 地址
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设备铭牌上显示的管理地址并回车
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）

6. 单击<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
7. 单击<确定>按钮完成密码的修改

4 系统信息

4.1 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。

4.2 系统信息

4.2.1 CPU 使用率和内存使用率

页面向导：系统信息→系统信息

查看CPU使用率和内存使用率	

页面中各参数的含义如下表所示。

表4-1 页面关键参数说明

关键参数	描述
CPU使用率	设备CPU的当前使用率。单击页面上方的“CPU使用率”区段，可查看CPU的当前使用率和平均使用率
内存使用率	设备内存的当前使用率。单击页面上方的“内存使用率”区段，可查看内存的当前使用率和平均使用率

4.2.2 接入终端

页面向导：系统信息→系统信息

查看接入终端的相关信息	

页面中各参数的含义如下表所示。

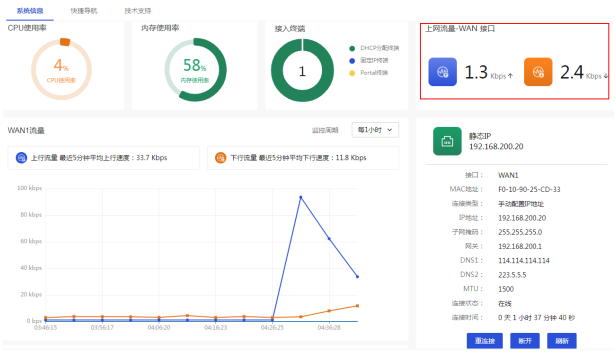
表4-2 页面关键参数说明

关键参数	描述
接入终端	局域网内接入终端的相关信息，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，主要包括： • 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
实时流量排行TOP5	接入终端使用流量的TOP5。点击右侧的“点击查看更多”链接，可以查看设备上当前所有接入终端的排行信息
在线主机数	局域网内在线主机的数量
在线主机网络连接数	局域网内所有在线主机连接网络的会话数
终端IP地址	接入终端的IP地址
终端名	接入终端的用户名
网络连接数	终端连接网络的会话数。主要分为： • 若终端传输的是 TCP 报文，则页面显示 TCP 报文的网络连接数 • 若终端传输的是 UDP 报文，则页面显示 UDP 报文的网络连接数 • 若终端传输的是其他报文，则页面显示其他报文的网络连接数
接入方式	终端接入网络使用的方式，主要分为： • 固定 IP：终端使用固定 IP 地址接入网络 • DHCP 分配：终端使用设备 DHCP 分配的 IP 地址接入网络 • PORTAL：一种认证方式，终端使用 Portal 认证的方式接入网络
接口	终端接入网络使用的设备接口，例如VLAN1
终端MAC地址	接入终端的MAC地址
上行流速	接入终端的上行流量速率
下行流速	接入终端的下行流量速率
在线时长	终端接入网络的时长
流量详情	该终端使用流量的详细信息

4.2.3 上网流量

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。

页面向导：系统信息→系统信息

可查看上网流量的相关信息	

页面中各参数的含义如下表所示。

表4-3 页面关键参数说明

关键参数	描述
上网流量	设备的上网流量情况，单击页面上方的“上网流量”区段，可查看各个WAN接口的上网流量信息和接口状态信息
最近5分钟平均上行速度	WAN 接口的最近 5 分钟平均上行速度，单位为 bps
最近5分钟平均下行速度	WAN 接口的最近 5 分钟平均上行速度，单位为 bps
监控周期	选择监控指定 WAN 接口流量的周期，包括：每 1 小时、每 1 天、每 1 个月
接口	设备接入广域网的接口
MAC地址	设备接入广域网使用的 MAC 地址
连接类型	用户实际的上网方式，选项包括： • PPPoE：宽带拨号上网方式 • DHCP：从 DHCP 服务器自动获取地址来接入广域网的上网方式 • 固定地址：由运营商提供固定地址来接入广域网的上网方式
用户名	身份验证使用的用户名。此参数由运营商提供。当连接模式设置为 PPPoE 时，需配置此参数
IP地址	设备接入广域网的 IP 地址
子网掩码	IP 地址的掩码或掩码长度
网关	设备接入广域网的网关地址
DNS1和DNS2	设备接入广域网的 DNS 服务器地址。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
MTU	设备接口允许通过的 MTU（Maximum Transmission Unit，最大传输单元）的大小。单位为字节
连接状态	设备接口与广域网的连接状态，主要分为： • 在线：该接口已连接到广域网 • 离线：该接口未连接到广域网
连接时间	该接口连入广域网的时长

4.2.4 系统信息

显示设备系统时间和产品型号等信息。

页面向导：系统信息→系统信息

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、工作模式和软件版本等信息	

页面中各参数的含义如下表所示。

表4-4 页面关键参数说明

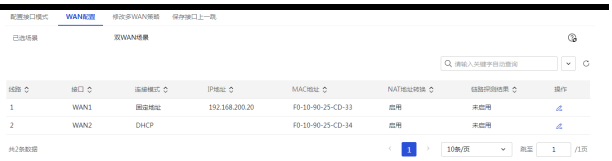
关键项	描述
系统时间	显示设备的系统时间
运行时间	显示设备的运行时间
产品型号	显示产品型号信息
序列号	显示设备的序列号信息
Boot ROM版本	显示设备的 Boot ROM 版本信息，点击“显示更多...”可查看
硬件版本	显示设备的硬件版本信息，点击“显示更多...”可查看
软件版本	显示设备的软件版本信息
模式选择	设备支持两种工作模式：路由模式、AC 模式。系统会根据工作模式呈现不同的菜单项

4.2.5 端口状态

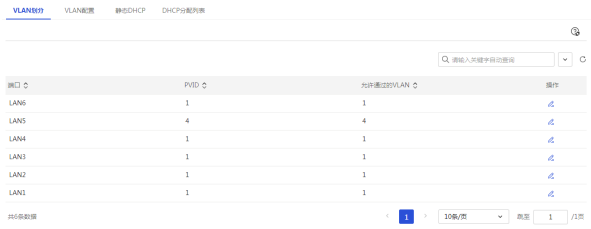
显示 WAN 口和 LAN 口的使用状态。

页面向导：系统信息→系统信息

在“端口状态”区段中，点击端口图标，可进入WAN或LAN配置页面	• WAN 配置界面:



- LAN 配置界面:



页面中各参数的含义如下表所示。

表4-5 页面关键参数说明

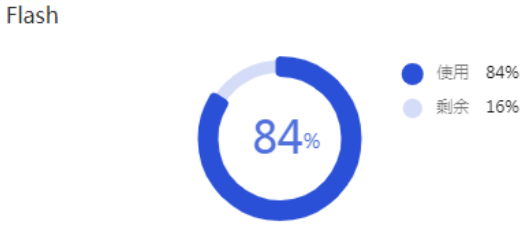
关键项	描述
端口状态	WAN 口和 LAN 口的当前使用状态。在“端口状态”区段中，点击端口图标，可进入 WAN 或 LAN 配置页面

4.2.6 Flash 使用率

存储介质上存储空间的使用情况。

页面向导：系统信息→系统信息

可查看Flash上存储空间的使用率



页面中各参数的含义如下表所示。

表4-6 页面关键参数说明

关键项	描述
存储介质	设备存储空间的当前使用状态。在页面右下方区段，可查看存储介质上存储空间的使用率

4.3 快捷导航

通过快捷导航帮助用户快速的配置网络。

在快捷导航页面，根据需要点击功能对应的链接	

页面中关键参数的含义如下表所示。

表4-7 页面关键参数说明

关键参数	描述
上网配置	设备上网的配置功能，主要包括： • 连接到因特网：单击"连接到因特网"，页面自动跳转至连接到因特网页面 • 局域网(LAN)设置：单击"局域网(LAN)设置"，页面自动跳转至局域网设置页面 • NAT 配置：单击"NAT 配置"，页面自动跳转至局域网设置页面
上网行为	设备上网行为管理的功能，主要包括： • 应用控制：单击"应用控制"，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"，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"，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"，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"，页面自动跳转至连接限制页面 • 流量统计排名：单击"流量统计排名"，页面自动跳转至流量排行页面
接入安全	用户接入网络的安全功能，主要包括： • ARP 安全：单击"ARP 安全"，页面自动跳转至 ARP 安全页面 • Portal 认证：单击"Portal 认证"，页面自动跳转至 Portal 认证页面 • 防火墙：单击"防火墙"，页面自动跳转至防火墙页面 • VPN 设置：单击"VPN 设置"，页面自动跳转至 IPsec VPN 页面 • MAC 地址过滤：单击"MAC 地址过滤"，页面自动跳转至 MAC 地址过滤页面
设备维护	设备的运行维护功能，主要包括： • 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

4.4 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

5 快速设置

5.1 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。

5.2 场景选择

5.2.1 WAN 配置

说明

- 快速设置页面仅支持设置单 WAN 或双 WAN 场景，部分款型如果只支持双 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。
- 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。
- 不同款型的设备，在快速设置中对单 WAN 和双 WAN 场景的支持情况不同，请以设备的实际情况为准。

设备支持 PPPoE、DHCP 和固定地址三种接入广域网方式。

表5-1 接入广域网方式介绍

接入方式	描述	应用场景
PPPoE	PPPoE是一种在以太网上建立点对点连接的协议，通常用于在宽带接入环境下实现认证和拨号连接 使用PPPoE方式接入广域网时，用户需要提供特定账号和密码信息，通过路由器对用户进行拨号连接，从而实现接入到互联网	PPPoE方式适用于家庭宽带接入适用于家庭用户、小型企业等需要拨号连接的网络环境，用户可以通过宽带调制解调器（如ADSL调制解调器）进行拨号连接，将家庭局域网与互联网进行连接
DHCP	DHCP是一种动态分配IP地址的网络连接方式，当设备连接到网络时，它会向DHCP服务器发送请求，服务器会动态分配IP地址、子网掩码、网关和DNS服务器等网络参数，使设备能够快速连接到网络并获取必要的IP配置信息	DHCP方式适用于大型局域网或企业网络环境，通过网络中的DHCP服务器自动分配IP地址，可以方便地管理大量设备的IP地址分配，并减少了手动配置IP地址的工作量
固定地址	固定地址是指手动配置的静态IP地址，子网掩码、网关和DNS服务器等网络参数，这些配置不会随着设备连接情况而改变	固定地址方式需要手动为网络设备配置固定的IP地址，确保设备始终使用同一IP地址。这种方式通常适用于需要长期稳定的IP地址分配和不需要频繁变化的网络设备够稳定地进行访问

页面向导：快速设置→场景选择

通过PPPoE方式接入广域网	
通过DHCP方式接入广域网	
通过固定地址方式接入广域网	

页面中各参数的含义如下表所示。

表5-2 页面关键参数说明

关键参数	描述
场景选择	设备接入广域网的场景选择，配置该参数时，可根据需要进行选择： • 若用户仅租用了一个运营商网络，则选择“单 WAN 场景” • 若用户租用了两个运营商网络，则选择“双 WAN 场景” 单WAN和双WAN场景的配置方法相同
“线路1”或“线路2	设备接入广域网的物理接口WANx
连接模式	用户实际的上网方式，选项包括： • PPPoE：宽带拨号上网方式 • DHCP：从 DHCP 服务器自动获取地址来接入广域网的上网方式 • 固定地址：由运营商提供固定地址来接入广域网的上网方式
上网账号	身份验证使用的用户名。此参数由运营商提供。当连接模式设置为PPPoE时，需配置此参数
上网密码	身份验证使用的密码。此参数由运营商提供。当连接模式设置为PPPoE时，需配置此参数
IP地址	设备接入广域网的固定IP地址，仅允许输入A、B、C类IP地址。当连接模式设置为固定地址时，该参数为必填项
子网掩码	IP地址的掩码或掩码长度，例如255.255.255.0。当连接模式设置为固定地址时，该参数为必填项
网关地址	设备接入广域网的网关地址，仅允许输入A、B、C类IP地址。当连接模式设置为固定地址时，该参数为必填项
DNS1和DNS2	设备接入广域网的DNS服务器地址。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
NAT地址转换	是否开启NAT地址转换功能，若开启该功能，则局域网中的多台设备是否共用同一个公网IP
是否为专线	选择是否将当前线路设置为专线。专线通常是不能访问外网的专用线路，例如医务专线、公安专线等 • 是：将当前线路设置为专线。设置专线后，用户需要手工配置静态路由 • 否：不将当前线路设置为专线

5.2.2 配置 LAN

完成 WAN 配置后，会进入到 LAN 配置的页面。

页面向导：快速设置→WAN 配置→LAN 配置

LAN配置：配置局域网IP地址、子网掩码等参数

页面中各参数的含义如下表所示。

表5-3 页面关键参数说明

关键参数	描述
局域网IP地址	设备在局域网中使用的IP地址
子网掩码	IP地址的掩码或掩码长度，例如：255.255.255.0
DHCP服务	是否启用DHCP服务，若开启该服务，设备将作为DHCP服务器为局域网中的主机分配IP地址
IP分配范围	待分配地址的起始IP地址和结束IP地址
排除地址	设备不能分配给客户端的IP地址。例如：网关地址
网关地址	设备为局域网中的主机分配的网关地址
DNS1和DNS2	DHCP服务器分配IP地址时所携带的DNS服务器地址，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

5.2.3 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。

页面向导：快速设置→WAN 配置→LAN 配置→无线设置

SSID设置-2.4G

1. 勾选“启用无线网络”选项，启用无线 2.4G 网络
1. 设置 SSID、加密方式和共享密钥等参数

SSID设置-5G

1. 勾选“启用无线网络”选项，启用无线 5G 网络
2. 设置 SSID、加密方式和共享密钥等

页面中各参数的含义如下表所示。

表5-4 页面关键参数说明

关键参数	描述
启用无线网络	选择是否启用无线网络
SSID-1名称	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。主要分为： • 2.4G SSID：2.4G 无线服务的 SSID 名称 • 5G SSID：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~!@#$%^&*()_+-={}|[]:;’ <>,./），其中1个中文字符占3个英文字符，英文字母区分大小写
加密方式	无线服务的加密方式，配置该参数时，可根据需要进行选择： • 不加密：不对无线信号加密 • WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密 • WPA2/WPA3 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2/WPA3 加密
共享密钥	无线服务密钥，即无线用户接入网络时需要输入此密钥，若选择通过加密方式接入无线服务时，需要设置共享密钥。密钥长度为8-63个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写

6 系统监控

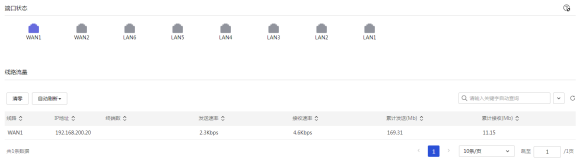
6.1 线路监控

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。

页面向导：系统监控→线路监控

端口状态：点击端口图标，可进入WAN或LAN配置页面

线路流量：可以通过列表查看各线路的流量信息



页面中各参数的含义如下表所示。

表6-1 页面关键参数说明

关键项	描述
端口状态	WAN口和LAN口的当前使用状态，点击端口图标，可进入WAN或LAN配置页面
线路	设备上的三层接口，例如WAN和VLAN接口
IP地址	该线路的接口IP地址。部分设备款型不支持显示此参数
终端数	该线路下连接的终端数量。部分设备款型不支持显示此参数
发送速率	该线路发送报文速率
接收速率	该线路接收报文速率
累计发送	该线路下累计发送报文大小。单位为Mb
累计接收	该线路下累计接收报文大小。单位为Mb

6.2 流量排行

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。

注意

- 此功能会消耗设备一定资源，请谨慎开启！。
- 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。

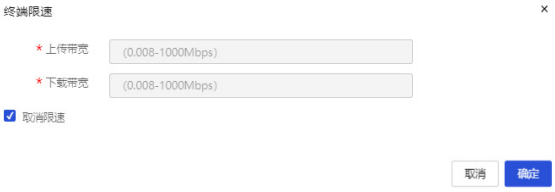
流量统计的单位换算关系为 1G bit= 1,000M bit= 1,000,000K bit= 1,000,000,000 bit。

页面向导：系统监控→流量排行

勾选“开启流量排行”选项，开启用户流量排行功能	

配置终端限速：

1. 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，设置上下传带宽和取消限速等参数
2. 单击<确定>按钮，完成配置



配置终端拉黑

1. 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，设置拉黑时间和永久拉黑等参数
2. 单击<确定>按钮，完成配置

表6-2 页面关键参数说明

关键项	描述
流量排行	是否开启流量排行功能。若开启该功能，页面会显示接入终端的流量信息
终端IP地址	接入终端的IP地址
终端名	接入终端的用户名
网络连接数(TCP/UDP/其他)	终端连接网络的会话数。主要包括： • 若终端传输的是 TCP 报文，则页面显示 TCP 报文的网络连接数 • 若终端传输的是 UDP 报文，则页面显示 UDP 报文的网络连接数 • 若终端传输的是其他报文，则页面显示其他报文的网络连接数
接入方式	终端接入网络使用的方式，主要分为： • 固定 IP：终端使用固定 IP 地址接入网络 • DHCP 分配：终端使用设备 DHCP 分配的 IP 地址接入网络 • PORTAL：一种认证方式，终端使用 Portal 认证的方式接入网络
接口	终端接入网络使用的设备接口，例如VLAN1
终端MAC地址	接入终端的MAC地址
上行流速	接入终端的上行流量速率
下行流速	接入终端的下行流量速率
当日总流量	接入终端的当日总传输流量
在线时长	终端接入网络的时长

操作	对该终端IP地址的操作，主要包括：
	• 限速：对终端进行限速操作
	  ○ 上传带宽：设置终端的上传带宽
	  ○ 下载带宽：设置终端的下载带宽
	  ○ 取消限速：勾选此项，将取消该对终端的限速
	• 拉黑：将终端加入黑名单管理列表，并禁止其访问互联网
	  ○ 拉黑时间：设置终端的拉黑时间
	  ○ 永久拉黑：将终端永久拉黑

6.3 网络连接数

网络连接数曲线图用于展示近一小时终端连接网络的会话数，每隔 10 秒自动刷新数据。

页面向导：系统监控→网络连接数

查看近一小时连接数曲线图	

页面中各参数的含义如下表所示。

表6-3 页面关键参数说明

关键项	描述
网络连接数	终端连接网络的会话数

7 MiniAP 管理

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）	添加无线业务VLAN（即桥接VLAN），具体配置方法请见参见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	配置无线服务模板（必选）	根据需要配置无线服务模板，具体配置方法请参见配置模板管理。
4	下发无线服务模板（必选）	为上线AP选择绑定的无线服务模板，具体配置方法请参见AP配置管理。

7.2 AP管理设置

7.2.1 简介

您可通过开启 AP 管理功能，集中管理接入的 AP 设备。

7.2.2 注意事项

AP 管理功能的默认管理 VLAN 为 VLAN1，如需选择其它 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。

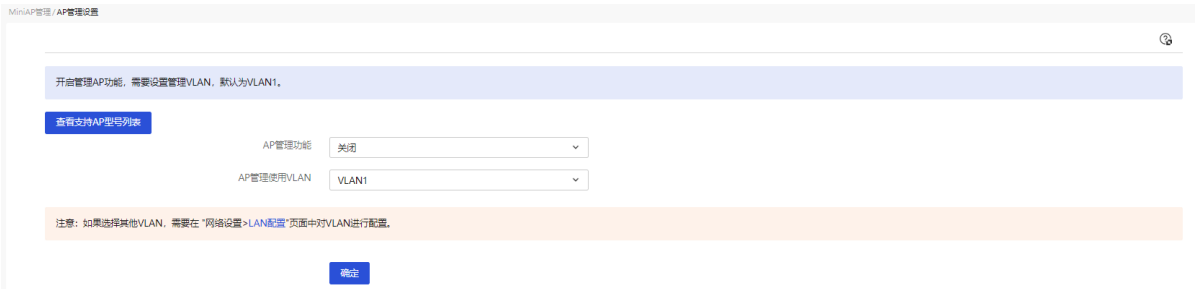
7.2.3 配置步骤

(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) 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“启用”。

(4) 在“AP 管理使用 VLAN”配置项处，选择 AP 管理使用的管理 VLAN。



7.3 在线AP管理

7.3.1 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，支持定时重启 AP。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。

7.3.2 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) 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 需要绑定的已经创建的无线服务模板或者手工配置。
- 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<重新启动>按钮，重启 AP 设备。
- 点击<射频管理>按钮，可根据需要开启或关闭 2.4GHz 射频和 5GHz 射频。

(4) 在“每页显示”配置项处，设置当前显示页面的 AP 数据条数。

7.3.3 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) 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。

(4) 点击<全部释放>按钮，断开所有客户端与无线服务的连接。

7.3.4 定时重启 AP

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[MiniAP 管理/在线 AP 管理]菜单项，进入在线 AP 管理页面。

(2) 单击“定时重启 AP”页签，进入定时重启 AP 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 AP 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。

7.4 配置管理

7.4.1 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、加密方式和共享密钥三项参数进行配置。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、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，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。

7.4.2 无线基本配置

1. 配置简介

无线基本配置只对 default 模板中 2.4G 网络和 5G 网络的 SSID-1 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，如果 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) 配置无线网络设置 SSID 设置-2.4G：

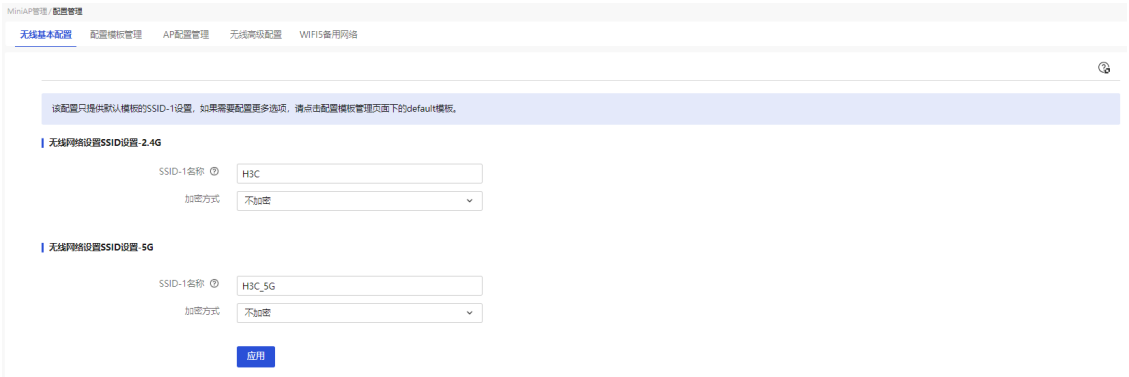
- 在“SSID-1 名称”配置项处，输入 2.4G 无线服务的 SSID 名称，即无线用户接入网络时搜索到的网络名称。支持英文字母[a-z,A-Z]、数字、中文、下划线、连接符、英文句号和空格。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务：
  - 不加密：不对无线信号加密。
  - WPA-PSK/WPA2-PSK 加密：若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密。
  - WPA2-PSK/WPA3-PSK 加密：若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密。
- 在“共享密钥”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 SSID 设置-5G：

- 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。支持英文字母[a-z,A-Z]、数字、中文、下划线、连接符、英文句号和空格。
- 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。



7.4.3 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。

- 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。
  - 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。

  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。选择禁用，允许无线客户端之间进行通信。选择启用，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。选择启用，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。选择禁用，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。

- 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。
- 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。
– 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”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。选择禁用，允许无线客户端之间进行通信。选择启用，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。选择启用，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。选择禁用，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。

(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“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，或者点击模板名称对应的操作列删除图标删除当前无线服务模板。注意，名称为“default”的缺省服务模板无法删除。

7.4.4 AP 配置管理

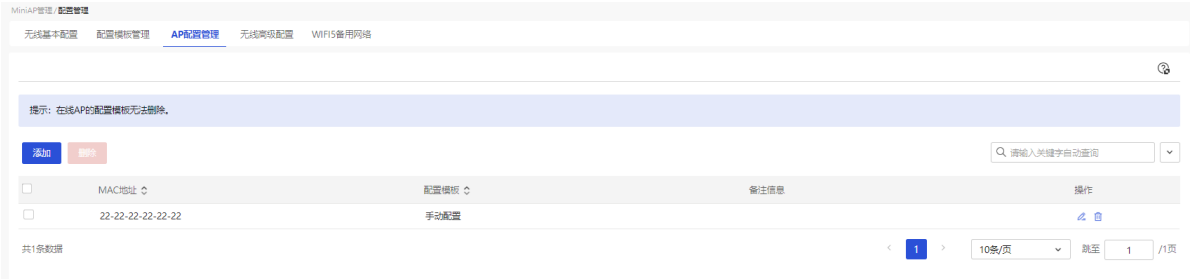
1. 配置简介

AP 配置管理用来添加、修改、删除 AP。

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) 点击<添加>按钮，弹出“添加 AP 配置模板”对话框。

(4) 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。

(5) 在“备注信息”配置项处，填写配置信息。

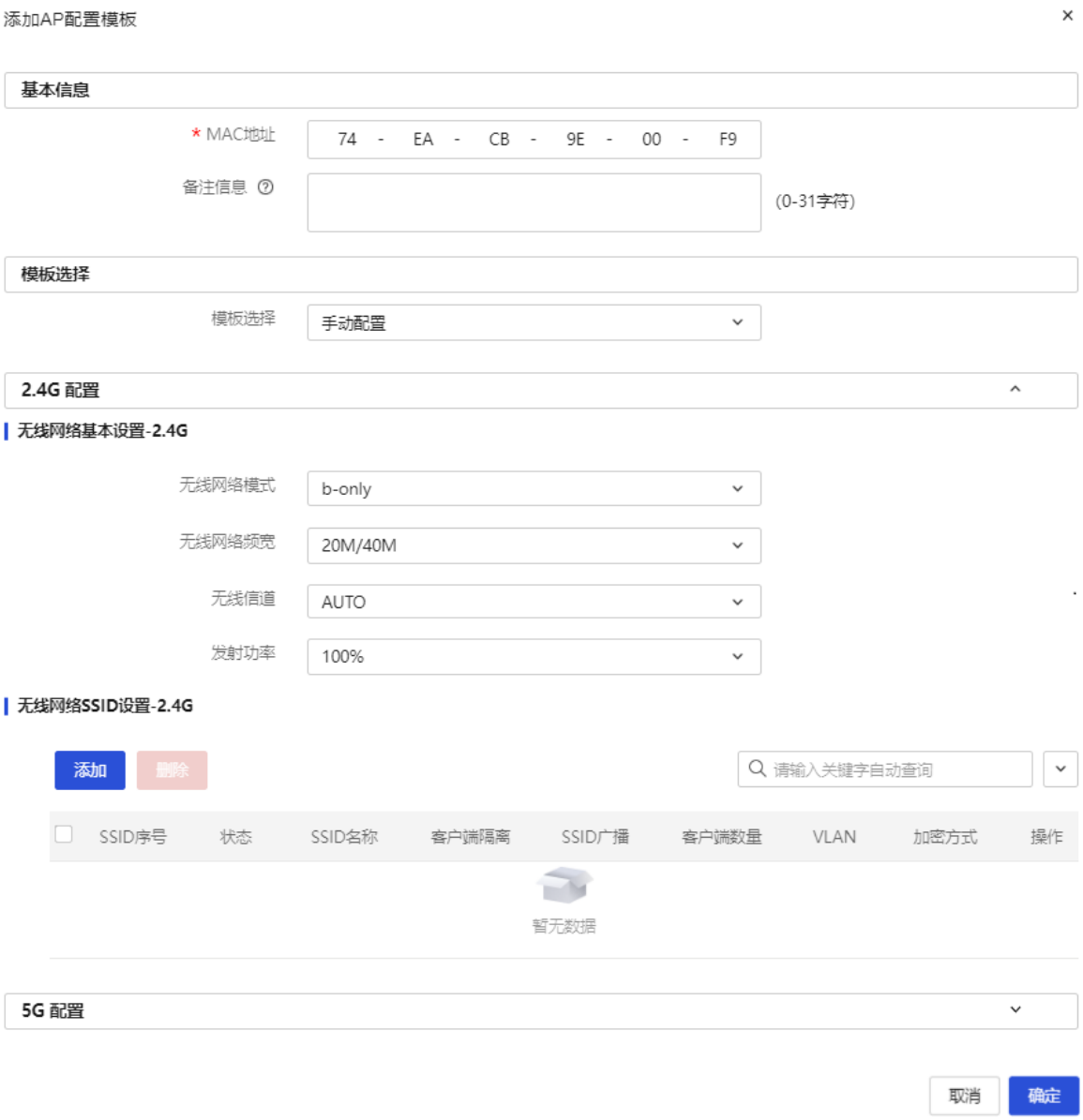
(6) 在“模板选择”配置项处，选择 AP 需要绑定的已经创建的无线服务模板。

(7) 设置 2.4G 配置和 5G 配置，具体请参见“配置模板管理”页签的相关配置。

(8) 点击<确定>按钮，完成配置。

(9) 如需修改配置好的 AP 配置模板，则在“AP 配置管理”页签下，点击 AP MAC 地址对应的操作列编辑图标，进入 AP 配置模板修改页面进行相关参数修改即可。

(10) 如需删除 AP 配置模板，则在“AP 配置管理”页签下，勾选要删除的 AP MAC 地址前的复选框，然后单击页面右上角的<删除>按钮即可，或者点击 AP MAC 地址对应的操作列删除图标删除当前 AP 配置模板。注意，在线 AP 的配置模板无法删除。



7.4.5 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”功能将不生效。
- 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”选项，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”选项，开启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，减少对网络中其它客户端的影响，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。

7.4.6 WIFI5 备用网络

1. 配置简介

Wi-Fi5 备用网络配置提供 2.4G 和 5G 射频的 Wi-Fi5 备用网络 SSID 配置，当部分终端无法扫描到 Wi-Fi6 信号时，可以连接备用的 Wi-Fi5 兼容信号。

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“WIFI5 备用网络”页签，进入 Wi-Fi5 备用网络配置页面。

(3) 配置 2.4G Wi-Fi5 备用网络 SSID：

- 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，即无线用户接入网络时搜索到的网络名称。支持英文字母[a-z,A-Z]、数字、中文、下划线、连接符、英文句号和空格。
- 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。
- 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。

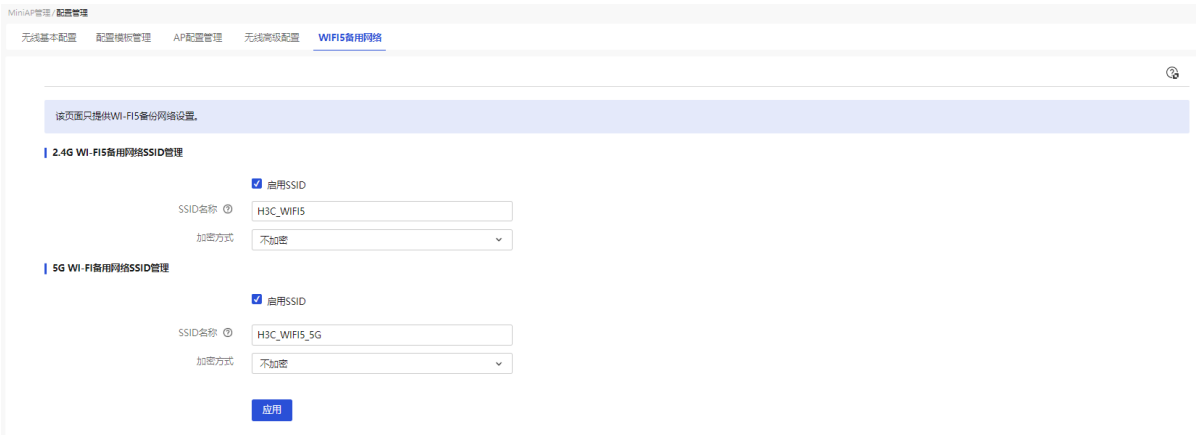
  当您选择 WPA-PSK/WPA2-PSK 加密方式时，需要设置共享密钥。密钥长度为 8-63 个字符，只能包含英文字母[a-z,A-Z]、数字，下划线，区分大小写。

(4) 配置 5G WI-FI5 备用网络 SSID：

- 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，即无线用户接入网络时搜索到的网络名称。支持英文字母[a-z,A-Z]、数字、中文、下划线、连接符、英文句号和空格。
- 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。
- 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 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，下划线，区分大小写。

(5) 点击<应用>按钮，完成配置。



7.5 版本管理

7.5.1 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。

7.5.2 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

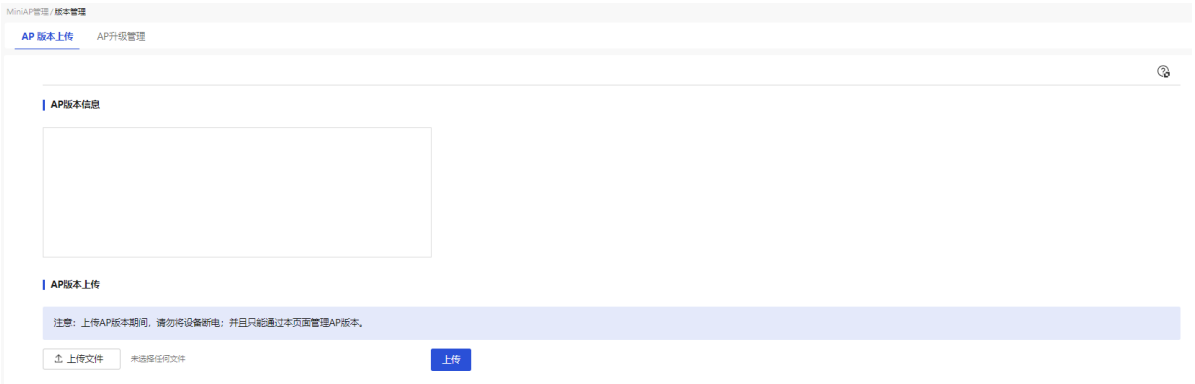
(1) 单击导航树中[MiniAP 管理/版本管理]菜单项，进入版本管理配置页面。

(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，访问待上传的 AP 软件版本存放路径，并选择版本文件。

(4) 点击<上传>按钮，将待上传的 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。



7.5.3 AP 升级管理

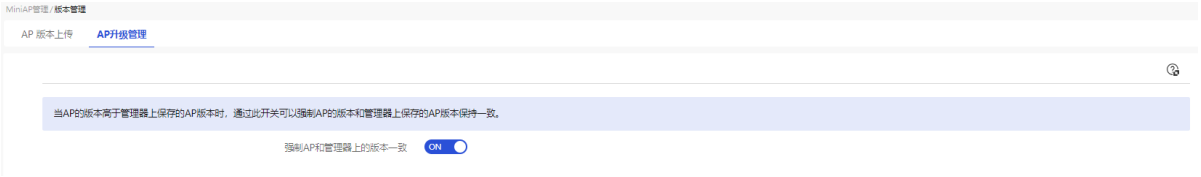
1. 配置步骤

(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，使得按钮状态为“ON”，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”功能，AP 才能自动升级到该软件版本。



7.6 高级管理

7.6.1 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。

7.6.2 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管理器统一下发的登录密码配置。
- 配置 IP 地址时，请确保不要与网络上其它 IP 地址发生冲突。例如，可先通过“系统工具”->“网络诊断”页面的“ping”功能，检测网络上是否有相同的 IP 地址。
- 配置 AP 管理地址池时，起始地址不得大于结束地址；AP 管理地址和地址池必须在同一网段。

7.6.3 地址管理设置

1. 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) 单击“地址管理设置”页签，进入地址管理设置页面。

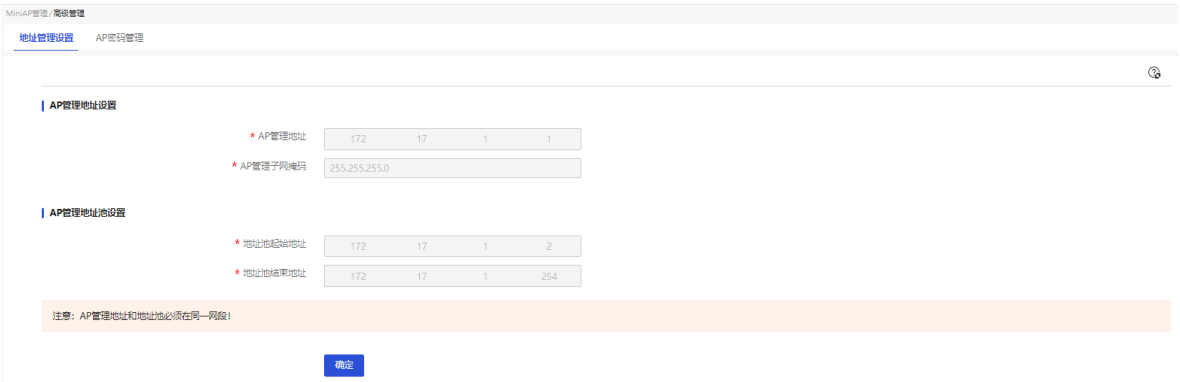
(3) 在“AP 管理地址”配置项处，输入管理 VLAN 的 IP 地址。

(4) 在“AP 管理子网掩码”配置项处，输入管理 VLAN 的子网掩码，例如 255.255.255.0。

(5) 在“地址池起始地址”配置项处，配置 AP 上线后获取 IP 地址的地址池起始地址。

(6) 在“地址池结束地址”配置项处，配置 AP 上线后获取 IP 地址的地址池结束地址。

(7) 点击<确定>按钮，完成地址管理设置服务。



7.6.4 AP 密码管理

1. 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) 单击“AP 密码管理”页签，进入 AP 密码管理配置页面。

(3) 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，密码长度为 1-31 个字符，只能包含英文字母[a-z,A-Z]、数字，下划线，区分大小写。

(4) 在“确认密码”配置项处，再次输入新密码。

(5) 在“密码提示”配置项处，输入密码提示信息。

(6) 点击<确定>按钮，完成配置。

7.7 无线优化

7.7.1 简介

无线优化功能提供了 AP 统计功能，对 AP 进行一键部署、一键优化和网络分析功能。

7.7.2 注意事项

在对 AP 进行一键部署和一键优化之前，需要先将 AP 的无线信道设置为 AUTO。

7.7.3 配置步骤

(1) 单击导航树中[MiniAP 管理/无线优化]菜单项，进入无线优化配置页面。

(2) 点击<一键部署>按钮，可将所有在线且无线信道类型为 AUTO 的 AP 自动分配无线信道。

(3) 在列表中勾选需要优化的 AP 后，点击<一键优化>按钮，可对所选 AP 的无线网络进行优化。

(4) 在列表中勾选需要分析的 AP 后，点击<网络分析>按钮，可对所选 AP 的无线网络质量进行分析并评分。


MiniAP管理 / 无线优化
AP统计信息 当前已接入AP数量：1。
<一键部署>：为所有在线且无线信道类型为AUTO的AP自动分配无线信道。
<一键优化>：对指定AP的无线网络进行优化。优化之前，需将AP的无线信道设置为AUTO。
<网络分析>：分析指定AP的无线网络质量，并进行评分。
自动刷新
一键部署
一键优化
网络分析
请输入关键字自动查询
AP型号 IP地址 MAC地址 状态 2.4G信道 5G信道 2.4G信道利用率 5G信道利用率 2.4G网络质量评分 5G网络质量评分 备注
A60 172.17.1.2 78-2C-29-1C-F8-48 运行中 1 44 15% 19%
共1条数据
1
10条/页
跳至 1 /1页

8 无线设置

说明

不同款型的设备对本功能的支持情况不同，请以设备的实际情况为准。

8.1 无线配置

8.1.1 内部网络

内部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。

注意

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。

页面向导：无线设置→无线配置→内部网络

1. 在无线网络 SSID 设置-2.4G 区段配置 2.4G 的 SSID、加密方式和共享密钥
2. 在无线网络 SSID 设置-5G 区段配置 5G 的 SSID、加密方式和共享密钥
3. 单击<应用>按钮，完成配置

页面中各参数的含义如下表所示。

表8-1 页面参数描述

关键参数	描述
启用无线网络	选择是否启用无线网络
SSID-1名称	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。主要分为： • 2.4G SSID：2.4G 无线服务的 SSID 名称 • 5G SSID：5G 无线服务的 SSID 名称

	注意 SSID名称长度为1-32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~!@#$%^&*()_+-={}|[]:;’ <>,./），其中1个中文字符占3个英文字符，英文字母区分大小写
加密方式	无线服务的加密方式，配置该参数时，可根据需要进行选择： • 不加密 • WPA-PSK/WPA2-PSK 加密 • WPA2-PSK/WPA3-PSK 加密 缺省情况下，加密方式为不加密。 当选择对无线服务进行加密时： • 若无线客户端支持 WIFI5 无线协议，推荐使用 WPA-PSK/WPA2-PSK 加密 • 若无线客户端支持 WIFI6 无线协议，推荐使用 WPA2-PSK/WPA3-PSK 加密
共享密钥	无线服务密钥，即无线用户接入网络时需要输入此密钥，若选择通过加密方式接入无线服务时，需要设置共享密钥 注意 密钥长度为8-63个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写

8.1.2 访客网络

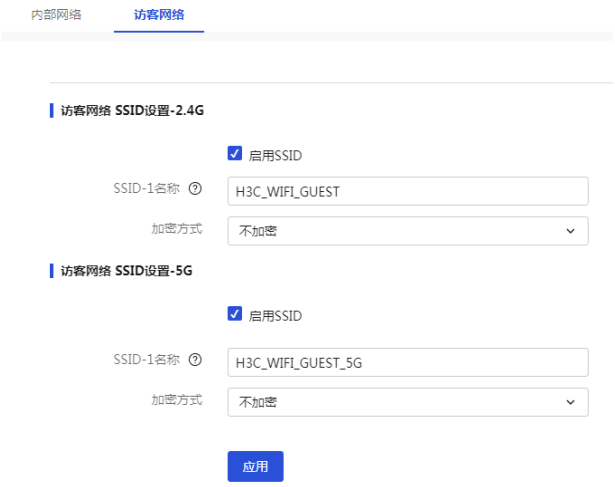
访客网络的无线基本配置支持对 2.4G 网络和 5G 网络的 SSID 名称、加密方式和共享密钥三项参数进行配置。

注意

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。

页面向导：无线设置→无线配置→访客网络

1. 在无线网络 SSID 设置-2.4G 区段配置 2.4G 的 SSID、加密方式和共享密钥
2. 在无线网络 SSID 设置-5G 区段配置 5G 的 SSID、加密方式和共享密钥
3. 单击<应用>按钮，完成配置



页面中各参数的含义如下表所示。

表8-2 页面参数描述

关键参数	描述
启用无线网络	选择是否启用无线网络
SSID-1名称	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。主要分为： • 2.4G SSID：2.4G 无线服务的 SSID 名称 • 5G SSID：5G 无线服务的 SSID 名称 注意 SSID名称长度为1-32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~!@#$%^&*()_+-={}|[]:;’ <>,./），其中1个中文字符占3个英文字符，英文字母区分大小写
加密方式	无线服务的加密方式，配置该参数时，可根据需要进行选择： • 不加密 • WPA-PSK/WPA2-PSK 加密 • WPA2-PSK/WPA3-PSK 加密 缺省情况下，加密方式为不加密
共享密钥	无线服务密钥，即无线用户接入网络时需要输入此密钥，若选择通过加密方式接入无线服务时，需要设置共享密钥 注意 密钥长度为8-63个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写

8.2 高级设置

8.2.1 无线射频管理

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。

注意

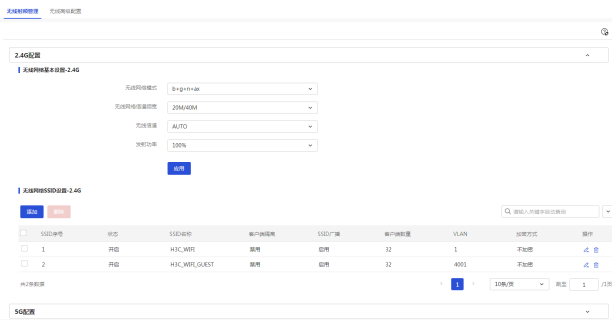
名称为“H3C_WIFI”、“H3C_WIFI_GUEST”、“H3C_WIFI_5G”和“H3C_WIFI_GUEST_5G”的 SSID 为系统默认的 SSID，不能被删除。

1. 2.4G 配置

页面向导：无线设置→高级设置→无线射频管理→2.4G 配置

本页面为您提供如下主要功能：

- 显示 2.4G 无线网络基本设置和 SSID 设置
- 修改 2.4G 无线网络基本设置（无线网络模式、无线网络信道频宽、无线信道、发射功率）
- 修改缺省的 2.4G 无线网络 SSID
- 添加 2.4G 无线网络 SSID



修改缺省的2.4G无线网络SSID：

1. 单击缺省的 2.4G 无线网络 SSID（H3C_WIFI 或 H3C_WIFI_GUEST）对应操作列的编辑图标，弹出修改 SSID 配置对话框，修改相关配置
2. 单击<确定>按钮，完成配置

添加2.4G无线网络SSID：

1. 单击<添加>按钮，弹出添加 SSID 配置对话框，配置相关参数
2. 单击<确定>按钮，完成配置

2. 5G 配置

页面向导：无线设置→高级设置→无线射频管理→5G 配置

5G 配置页面相关功能配置步骤以及页面参数和 2.4G 配置类似，可参考 2.4G 进行配置，此处不做描述。

页面中各参数的含义如下表所示。

表8-3 页面参数描述

页面参数	描述
无线网络模式	选择无线网络的工作模式 缺省情况下2.4G无线网络为b+g+n+ax模式，5G无线网络为a+n+ac+ax模式
无线网络信道频宽	选择无线网络频段带宽。 缺省情况下2.4G无线网络为20/40M，5G无线网络请以设备实际情况为准
无线信道	选择无线网络的工作信道 缺省为AUTO

发射功率	选择无线网络的发射功率 缺省情况下为 100% 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
启用SSID	选择是否启用 SSID
SSID名称	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。主要分为： • 2.4G SSID：2.4G 无线服务的 SSID 名称 • 5G SSID：5G 无线服务的 SSID 名称 注意 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~!@#$%^&*()_+-={}|[]:;’ <>,./），其中1个中文字符占3个英文字符，英文字母区分大小写
加密方式	无线服务的加密方式，主要分为： • 不加密 • WPA-PSK/WPA2-PSK 加密 • WPA2-PSK/WPA3-PSK 加密 缺省为不加密
共享密钥	无线服务密钥，即无线用户接入网络时需要输入此密钥，若选择通过加密方式接入无线服务时，需要设置共享密钥 注意 密钥长度为8-63个字符，只能包含英文字母[a-z,A-Z]、数字，以及特殊字符（~!@#$%^&*()_+-={}|[]:<>,./），区分大小写
加密协议	选择加密机制来保护您的数据安全。主要分为： • 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 缺省情况下为 AES
群组密钥更新周期	群组密钥更新周期 缺省情况为 3600
高级设置	选择是否设置客户端接入管理的相关功能
客户端隔离	与同一SSID建立连接的无线客户端之间是否可以互相通信的功能。主要分为： • 启用：禁止无线客户端之间互相通信 • 关闭：允许无线客户端之间互相通信 缺省情况下，关闭客户端隔离功能
SSID广播	选择是否启用SSID广播。 • 若启用 SSID 广播功能，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，则可以关闭 SSID 广播功能

	• 若关闭 SSID 广播功能，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。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
最大客户端数量	接入无线服务的最大无线客户端数量。配置该参数时，可以防止SSID接入的客户端数量过多而过载，缺省为32
桥接VLAN	选择桥接VLAN，即将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

8.2.2 无线高级配置

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。

注意

- 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。

页面向导：无线设置→高级设置→无线高级配置

配置无线高级配置：

1. 选择是否启用禁止弱信号客户端接入和关闭广播探测功能
2. 单击<确定>按钮，完成配置

页面中各参数的含义如下表所示。

表8-4 页面参数描述

页面参数	描述
禁止弱信号客户端接入	选择是否禁止弱信号客户端接入 缺省为关闭状态
禁止接入信号强度	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
关闭广播探测	选择是否关闭广播探测。勾选该选项后，部分客户端将无法扫描到本设备接入AP的SSID

8.3 客户端列表

本功能用于查看接入无线网络的客户端。

页面向导：无线设置→客户端列表

显示接入无线网络的客户端信息

页面中各参数的含义如下表所示。

表8-5 页面参数描述

页面参数	描述
释放	选中接入设备的客户端，使其下线
全部释放	使接入设备的全部客户端下线
客户端MAC地址	已接入设备的客户端MAC地址
客户端IP地址	已接入设备的客户端IP地址
连接SSID	客户端连接的无线信号名称
信号强度	设备无线信号的信号强度。单位为dBm
发送速率	客户端发送数据的速率。单位为Mbps。该速率指的是设备下发的无线与无线终端网卡之间协商的速率，而非接口实际的传输速率
接收速率	客户端接收数据的速率。单位为Mbps。该速率指的是设备下发的无线与无线终端网卡之间协商的速率，而非接口实际的传输速率
连接时间	客户端接入设备的持续时间

9 网络设置

9.1 外网配置

9.1.1 功能简介

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。

9.1.2 配置接口模式

说明

不同款型的设备对接口模式切换的支持情况不同，具体以设备实际情况为准。

1. 注意事项

本功能用于配置设备 WAN/LAN 口的接口模式。

- 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

页面向导：[网络设置/外网配置/配置接口模式]

配置设备WAN/LAN口的接口模式：

1. 点击接口下 WAN/LAN 的按钮进行切换
2. 单击<确定>按钮，完成配置

3. 参数解释

表9-1 页面各参数项描述

页面参数	描述
接口模式	配置接口模式切换，设置设备支持的WAN/LAN口

9.1.3 WAN 配置

1. 功能简介

设备支持 PPPoE、DHCP 和固定地址三种接入广域网方式。

2. 使用场景

表9-2 接入广域网方式介绍

接入方式	描述	应用场景
PPPoE	PPPoE是一种在以太网上建立点对点连接的协议，通常用于在宽带接入环境下实现认证和拨号连接 使用PPPoE方式接入广域网时，用户需要提供特定账号和密码信息，通过路由器对用户进行拨号连接，从而实现接入到互联网	PPPoE方式适用于家庭宽带接入适用于家庭用户、小型企业等需要拨号连接的网络环境，用户可以通过宽带调制解调器（如ADSL调制解调器）进行拨号连接，将家庭局域网与互联网进行连接
DHCP	DHCP是一种动态分配IP地址的网络连接方式，当设备连接到网络时，它会向DHCP服务器发送请求，服务器会动态分配IP地址、子网掩码、网关和DNS服务器等网络参数，使设备能够快速连接到网络并获取必要的IP配置信息	DHCP方式适用于大型局域网或企业网络环境，通过网络中的DHCP服务器自动分配IP地址，可以方便地管理大量设备的IP地址分配，并减少了手动配置IP地址的工作量
固定地址	固定地址是指手动配置的静态IP地址，子网掩码、网关和DNS服务器等网络参数，这些配置不会随着设备连接情况而改变	固定地址方式需要手动为网络设备配置固定的IP地址，确保设备始终使用同一IP地址。这种方式通常适用于需要长期稳定的IP地址分配和不需要频繁变化的网络设备够稳定地进行访问

3. 配置步骤

页面向导：[网络设置/外网配置/WAN 配置]

关键项	描述
WAN口通过PPPoE方式连接到广域网	

WAN口通过DHCP方式连接到广域网	

WAN口通过固定地址方式连接到广域网	

4. 参数解释

表9-3 页面各参数项描述

页面参数	描述
线路	设备接入广域网的线路序号
WAN接口	设备接入广域网的接口
连接模式	用户实际的上网方式，选项包括： • PPPoE：宽带拨号上网方式

	• DHCP：从 DHCP 服务器自动获取地址来接入广域网的上网方式 • 固定地址：由运营商提供固定地址来接入广域网的上网方式
上网账号	身份验证使用的用户名。此参数由运营商提供。当连接模式设置为PPPoE时，可配置该参数
上网密码	身份验证使用的密码。此参数由运营商提供。当连接模式设置为PPPoE时，可配置该参数
LCP主动检测	检测PPPoE链路异常状态，选项包括： • 是：开启该功能，则每隔 20 秒钟检测一次链路状态 • 否：关闭该功能，则每隔 2 分钟检测一次链路状态 当连接模式设置为PPPoE时，可配置该参数
在线方式	当前在线方式仅支持“始终在线”。当连接模式设置为PPPoE时，缺省启用该项，无法取消
拨号方式	PPPoE连接的拨号方式，选项包括： • 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 • 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 当连接模式设置为PPPoE时，可配置该参数
host-uniq	上网方式为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。本参数用于设置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 当连接模式设置为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
服务器名	PPPoE服务器名称，由运营商提供，缺省为空。当连接模式设置为PPPoE时，可配置该参数
服务名称	PPPoE服务器的服务名称，由运营商提供，缺省为空。当连接模式设置为PPPoE时，可配置该参数
IP地址	设备接入广域网的固定IP地址，仅允许输入A、B、C类IP地址。当连接模式设置为固定地址时，需配置此参数
子网掩码	IP地址的掩码或掩码长度，例如255.255.255.0。当连接模式设置为固定地址时，需配置此参数
网关地址	设备接入广域网的网关地址，仅允许输入A、B、C类IP地址。当连接模式设置为固定地址时，需配置此参数
DNS1和DNS2	设备接入广域网的DNS服务器地址。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
网络上行带宽	实际线路的上行带宽值，请咨询当地运营商确认
网络下行带宽	实际线路的下行带宽值，请咨询当地运营商确认
主机名	设备需要通告给DHCP服务器的机器名。当连接模式设置为DHCP时，可配置该参数
NAT地址转换	选择是否启用NAT地址转换
使用地址池转换	设置局域网中的多台设备是否共用同一个公网IP。当NAT地址转换启用时，可根据需要进行选择： • 若设备公网 IP 仅有一个，则不选择“使用地址池转换” • 若设备公网 IP 有多个，则选择“使用地址池转换”，需选择已创建的 NAT 地址池。如需

	新增地址池，可通过点击<添加>按钮创建新的地址池
端口范围	当NAT地址转换启用时，可通过配置端口范围，限制NAT地址转换后的源端口范围
链路探测结果	对指定IP地址或域名链路状态的探测结果，主要分为： • 成功：表示成功探测指定 IP 地址或域名的链路状态 • 失败：表示未成功探测指定 IP 地址或域名的链路状态 • 未启用：表示未启用链路探测功能
TCP MSS	设备接口的TCP报文段的最大长度，缺省为1280
MTU	设备接口允许通过的MTU（Maximum Transmission Unit，最大传输单元）的大小
链路探测	对到达指定IP地址或域名的链路状态进行判断，提高链路的可靠性，配置该参数时，可根据需要进行选择： • 若需使用 ICMP 报文探测链路状态，则选择“ICMP 探测” • 若需使用 DNS 报文探测链路状态，则选择“DNS 探测” • 若需使用 NTP 报文探测链路状态，则选择“NTP 探测” • 若不需探测链路状态，则选择“不启用”
探测地址	链路探测的IP地址或域名。当链路探测设置为ICMP探测、DNS探测或NTP探测时，需配置此参数
探测间隔	链路探测的时间间隔。当链路探测设置为ICMP探测、DNS探测或NTP探测时，需配置此参数
探测次数	链路探测的探测次数。当链路探测设置为ICMP探测、DNS探测或NTP探测时，可配置该参数
是否为专线	选择是否将当前线路设置为专线。专线通常是不能访问外网的专用线路，例如医务专线、公安专线等 • 是：将当前线路设置为专线。设置专线后，用户需要手工配置静态路由 • 否：不将当前线路设置为专线
MAC地址	设备接入广域网使用的MAC地址
操作	可对该配置进行编辑操作

9.1.4 修改多 WAN 策略

1. 功能简介

只有多 WAN 场景可以进行本页面的配置。

2. 使用场景

设备支持五种多 WAN 策略。

表9-4 多 WAN 口负载分担策略介绍

多 WAN 策略	描述	应用场景
平均分配负载分担	每条链路负载分担相同	WAN口属于相同运营商，各条链路带宽一致
带宽比例负载分担	每条链路按照比例负载分担	WAN口属于相同运营商，各条链路带宽不一致
基于运营商的负载分	基于流量访问的目的地址进行负载分担	WAN口属于不同运营商，每个运营商提供的

多 WAN 策略	描述	应用场景
担		链路带宽一致
多链路高级负载分担	基于流量访问的目的地址进行负载分担	WAN口属于不同运营商，每个运营商提供的链路带宽不一致
链路备份	一条链路为主链路，其它为备份链路，以保持网络的稳定性	如对网络稳定性要求比较高，可以设置备份链路。

3. 配置步骤

页面向导：[网络设置/外网配置/修改多 WAN 策略]

设置多 WAN 同运营商接入模式：

1. 选择“平均分配负载分担”或“带宽比例负载分担”模式
2. 点击<应用>按钮，完成配置

设置多 WAN 不同运营商接入模式：

1. 选择“基于运营商的负载分担”或“多链路高级负载分担”模式
2. 点击<应用>按钮，完成配置

设置链路备份：

1. 选择主链路和备份链路
2. 点击<应用>按钮，完成配置

4. 参数解释

表9-5 页面参数描述

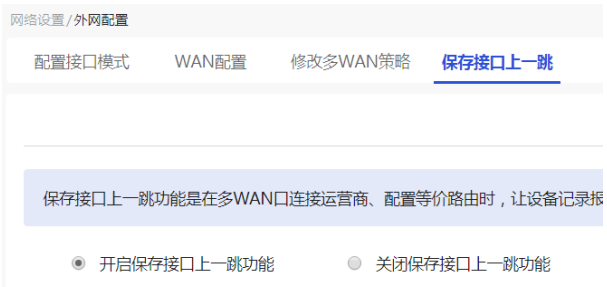
关键项	描述
多WAN属于相同运营商	设备多个WAN口接入相同运营商线路，可根据需要选择负载分担模式： • 若各条链路带宽一致，建议选择“平均分配负载分担” • 若各条链路带宽不一致，建议选择“带宽比例负载分担”，并设置分配链路带宽比例 设置完成，需点击“应用”按钮，使配置生效
多WAN属于不同运营商	设备多个WAN口接入不同运营商线路，可根据需要选择负载分担模式：

	• 若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”。并选择 WAN 口对应的运营商和默认链路 • 若每个运营商提供的链路带宽不一致，建议选择“多链路高级负载分担”，并设置分配链路带宽比例，选择 WAN 口对应的运营商和默认链路 设置完成，需点击“应用”按钮，使配置生效
链路备份	多WAN接入时，其中一条链路为主链路，其它为备份链路，以保持网络的稳定性。配置该参数时，先选择“主链路（请选择作为主链路的WAN接口）”以及对应的“链路n”，然后选择其中备份链路的“链路m”。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
分配链路带宽比例	设置各链路缺省的带宽比例。设置此参数时，需确保至少有一个链路的带宽比例不为0 当多WAN策略设置为“带宽比例负载分担”或“多链路高级负载分担”时，需要设置此参数 注意：该参数的输入范围为0-100的整数

9.1.5 保存接口上一跳

1. 配置步骤

页面向导：[网络设置/外网配置/保存接口上一跳]

设置 WAN 口保存接口上一跳功能	

2. 参数解释

表9-6 页面各参数项描述

页面参数	描述
开启保存接口上一跳功能	是否开启保存接口上一跳功能，若开启该功能，多WAN场景下，进入和离开局域网的报文将通过同一个WAN接口转发

9.2 LAN配置

说明

AC 模式下，仅支持 VLAN 划分、VLAN 配置。

9.2.1 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。

9.2.2 VLAN 划分

1. 功能简介

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

(1) 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。

(2) 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。

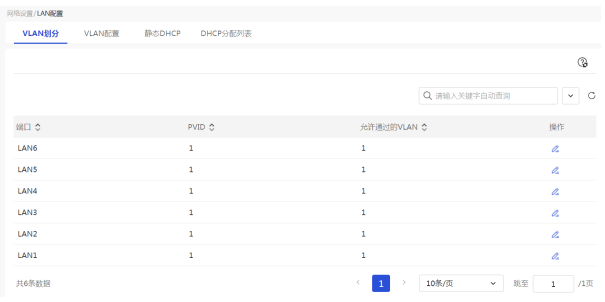
(3) PVID（Port VLAN ID，端口的缺省 VLAN）：当端口收到未携带 VLAN Tag 的报文时，即认为此报文所属的 VLAN 为端口的缺省 VLAN。

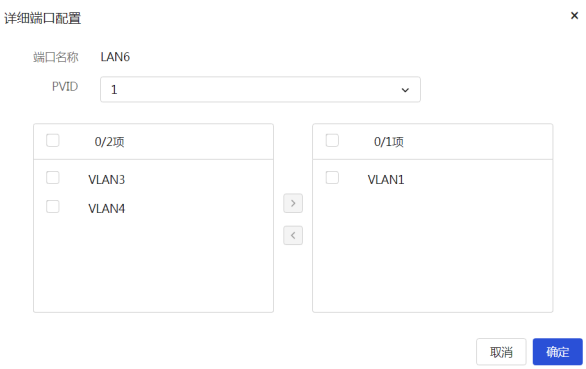
3. 配置步骤

页面向导：[网络设置/LAN 配置/VLAN 划分]

本页面为您提供如下主要功能：

- 显示端口允许通过 VLAN 的信息
- 设置端口允许通过的 VLAN



设置端口允许通过的VLAN	

4. 参数解释

表9-7 页面各参数项描述

关键项	描述
端口名称	需划分VLAN的LAN接口
PVID	该端口的缺省VLAN
允许通过的VLAN	该LAN口允许通过的所有VLAN
待选VLAN	设备上已创建的所有VLAN。配置该参数时，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
已选VLAN	该端口已被划分的VLAN。配置该参数时，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
操作	可对该配置进行编辑操作

9.2.3 VLAN 配置

1. 功能简介

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

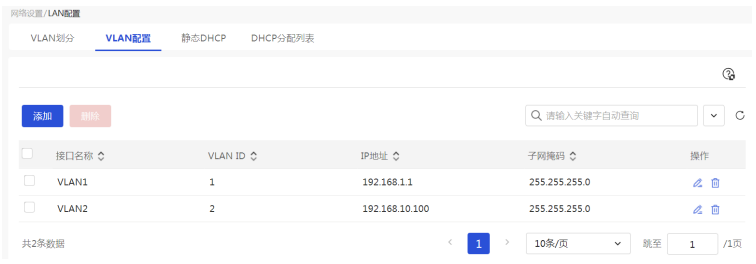
- 若开启 VLAN 接口的 DHCP 服务后再关闭，则系统会同步删除静态 DHCP 页面中该 VLAN 接口已绑定的静态 DHCP。
- AC 模式下，不支持配置 DHCP 服务相关参数。

3. 配置步骤

页面向导：[网络设置/LAN 配置/VLAN 配置]

本页面为您提供如下主要功能：

- 显示已添加 VLAN 的详细信息
- 添加 VLAN
- 删除已添加的 VLAN
- 修改已添加的 VLAN



添加VLAN：

1. 单击<添加>按钮，弹出 VLAN 对话框，设置 VLAN ID、IP 地址、子网掩码等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的 VLAN：

1. 勾选需要删除的 VLAN 前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的VLAN：

1. 点击需要修改的 VLAN 对应操作列的编辑图标，弹出修改 VLAN 对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

4. 参数解释

表9-8 页面各参数项描述

关键项	描述
接口名称	该VLAN接口的名称
VLAN ID	该VLAN接口的ID号
连接模式	设备获取IP地址的方式，选项包括： • DHCP：设备从 DHCP 服务器获取 IP 地址，选择该选项时，网络环境中需要存在 DHCP 服务器 • 固定地址：手动创建 VLAN 接口的 IP 地址、子网掩码等信息
接口IP地址	该VLAN接口的IP地址
子网掩码	该IP地址的掩码或掩码长度，例如255.255.255.0
TCP MSS	该VLAN接口的TCP报文最大分段长度值，缺省为1280
MTU	该VLAN接口允许通过的MTU值的大小
开启DHCP服务	是否开启DHCP服务功能。若开启该功能，设备将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。缺省关闭DHCP服务功能
对DHCP分配的地址进行ARP保护(动态绑定)	是否开启对DHCP分配的地址进行ARP保护(动态绑定)功能。若开启该功能，设备将为动态分配的IP地址绑定客户端的MAC地址。缺省关闭对DHCP分配的地址进行ARP保护(动态绑定)功能
地址池起始地址	DHCP服务器地址池的起始IP地址
地址池结束地址	DHCP服务器地址池的结束IP地址，地址池结束地址不能小于地址池起始地址
排除地址	设备不能分配给客户端的IP地址。例如：网关地址
网关地址	地址池对应的网关地址，若不配置网关地址，有可能造成网络不通
客户端域名	设备为客户端分配的域名后缀。客户端域名允许设置的字符包括英文字母[a-z,A-Z]、数字，以及符号-和.，不能以符号.开头或结尾 • 包含符号.时，符号.前后的字符长度都不能超过 63 个字符。如果同时存在多个符号.时，则符号.不能连续输入，例如.. • 不包括符号.时，取值为 1-63 个字符
DNS1和DNS2	DHCP服务器分配IP地址时所携带的DNS服务器地址，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
地址租约	DHCP服务器分配给客户端IP地址的租借期限。当租借期满后，DHCP服务器会收回该IP地址，客户端必须重新向路由器申请（客户端一般会自动申请）
操作	可对该配置进行编辑和删除操作

9.2.4 配置静态 DHCP

1. 功能简介

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

(1) 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。

(2) 配置静态 DHCP 时，如果设置的客户端 IP 地址已被其他终端占用，那么客户端 MAC 对应的终端上线时会被分配其他 IP 地址。当此前设置的客户端 IP 地址被释放后，客户端 MAC 对应的终端会被重新分配设定的 IP 地址。

(3) 在配置静态 DHCP 之前，需要先开启 VLAN 接口的 DHCP 服务。

3. 配置步骤

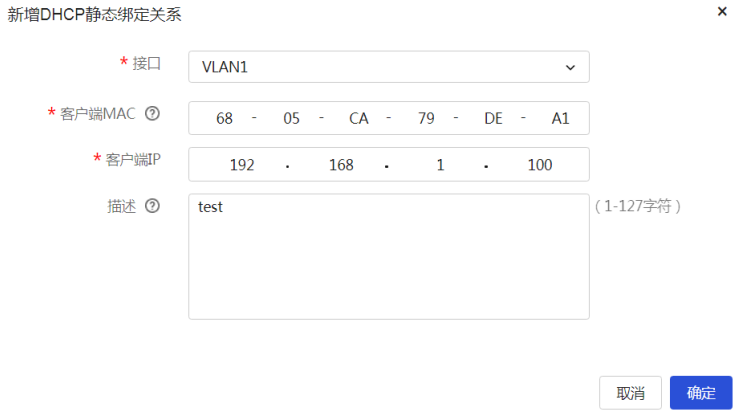
页面向导：[网络设置/LAN 配置/静态 DHCP]

本页面为您提供如下主要功能：

- 显示已添加 DHCP 静态绑定关系的详细信息
- 添加 DHCP 静态绑定关系
- 删除 DHCP 静态绑定关系
- 修改已添加的 DHCP 静态绑定关系
- 导入静态 DHCP 地址表

添加 DHCP 静态绑定关系：

1. 单击<添加>按钮，弹出新增 DHCP 静态绑定关系对话框，设置接口、客户端 MAC 地址、客户端 IP 等参数信息
2. 点击<确定>按钮，完成配置



删除已添加的 DHCP 静态绑定关系：

1. 勾选需要删除的 DHCP 静态绑定关系前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的DHCP静态绑定关系：

1. 点击需要修改的 DHCP 静态绑定关系对应操作列的编辑图标，弹出 DHCP 静态绑定关系对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

导入静态DHCP地址表：

1. 点击界面的导入图标，弹出导入静态DHCP地址表对话框。点击<上传文件>按钮，选择需导入的静态DHCP地址表
2. 点击<确定>按钮，完成配置

4. 参数解释

表9-9 页面各参数项描述

关键项	描述
序号	静态DHCP策略的编号
接口	设备上已创建的VLAN接口。即策略对从某一接口获取的IP地址和MAC地址进行绑定
客户端MAC	客户端的MAC地址。此处不支持全0或全F的MAC地址
客户端IP	分配给该客户端的IP地址
子网掩码	该IP地址的掩码或掩码长度。例如255.255.255.0
描述	策略的描述信息，可对策略进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

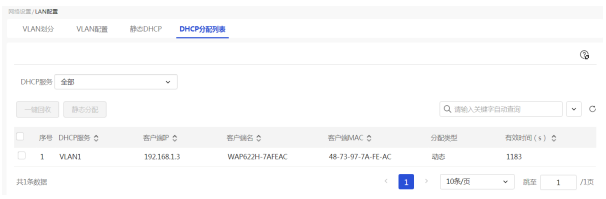
9.2.5 DHCP 分配列表

1. 配置步骤

页面向导：[网络设置/LAN 配置/DHCP 分配列表]

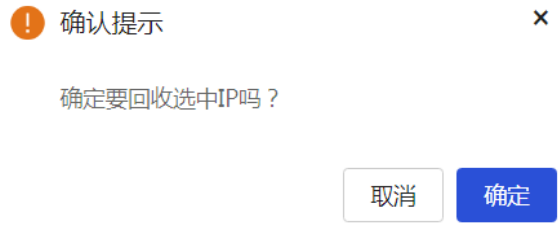
本页面为您提供如下主要功能：

- 显示设备 DHCP 分配的详细信息
- 一键回收 IP 地址
- 静态分配 IP 地址



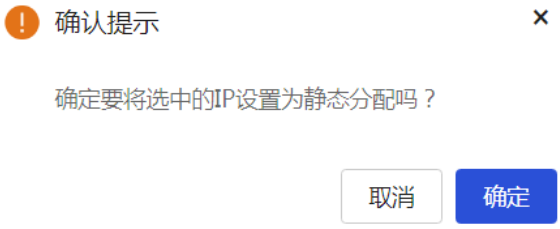
一键回收 IP 地址：

1. 在列表中选中需要回收的 IP 地址
2. 单击<一键回收>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置



静态分配 IP 地址：

1. 在列表中选中需要静态分配的 IP 地址
2. 单击<静态分配>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置



2. 参数解释

表9-10 页面各参数项描述

页面参数	描述
序号	DHCP分配信息的编号
DHCP服务	设备上开启DHCP服务的VLAN接口
客户端IP	客户端的IP地址
客户端名	客户端的主机名
客户端MAC	客户端的MAC地址
有效时间	DHCP服务器分配给客户端IP地址的租借期限。当租借期满后，DHCP服务器会收回该IP地址，客户端必须重新向路由器申请（客户端一般会自动申请）
一键回收	回收DHCP服务器分配的IP地址。配置该参数时，列表中选中需要回收的IP地址，点击<一键回收>按钮，在弹出的确认提示框中，点击<确定>按钮，确认回收选中的IP地址
静态分配	将DHCP服务器动态分配的IP地址进行静态绑定。配置该参数时，在列表中选中需要静态绑定的客户端IP，点击<静态分配>按钮，在弹出的确认提示框中，点击<确定>按钮，确认将DHCP动态分配的IP地址设置为静态分配

9.3 端口管理

1. 功能简介

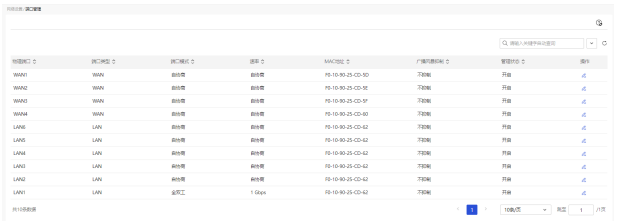
端口管理功能用来查看设备各个物理端口的端口类型、端口模式、速率、MAC 地址和广播风暴抑制等信息，设置 WAN 口的管理状态，以及修改端口配置。

2. 配置步骤

页面向导：[网络设置/端口管理]

本页面为您提供如下主要功能：

- 显示设备端口的详细信息
- 修改端口配置



修改端口配置：

1. 点击需要修改的端口对应操作列的编辑图标，弹出修改端口对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

3. 参数解释

表9-11 页面各参数项描述

关键项	描述
物理端口	设备的物理端口。例如WAN1、LAN1
端口名称	设备的物理端口名称
端口类型	设备的端口类型，主要分为： • WAN：接入广域网的接口 • LAN：接入局域网的接口
端口模式	端口的工作模式，主要分为： • 自协商：双工和速率状态均由本端口和对端端口自动协商而定 • 全双工：端口在发送数据包的同时可以接收数据包 • 半双工：端口同一时刻只能发送数据包或接收数据包
速率	端口的速率，包括自协商、10Mbps、100Mbps、1Gbps
MAC地址	端口的MAC地址
广播风暴抑制	抑制局域网内大量广播报文传播的功能，可避免网络拥塞，保证网络业务的正常运行。可根据需要进行选择抑制程度：“不抑制”、“低”、“中”、“高”
管理状态	端口的工作状态，主要分为： • 开启：设备开启此端口 • 关闭：设备关闭此端口 当端口类型为LAN时，此参数不支持修改，缺省为开启状态

9.4 NAT配置

9.4.1 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。

9.4.2 配置虚拟服务器

1. 配置步骤

页面向导：[网络设置/NAT 配置/虚拟服务器]

本页面为您提供如下主要功能：

- 显示已添加虚拟服务器的详细信息
- 启用 NAT DMZ 服务器
- 添加 NAT 端口映射
- 删除已添加的 NAT 端口映射
- 修改已添加的 NAT 端口映射

启用 NAT DMZ 服务器：

1. 勾选“开启”选项，设置主机地址参数
2. 单击<应用>按钮，完成配置

添加 NAT 端口映射：

1. 单击<添加>按钮，弹出添加 NAT 端口映射对话框，设置协议类型、外部地址、外部端口等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的 NAT 端口映射：

1. 勾选需要删除的 NAT 端口映射前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的 NAT 端口映射：

1. 点击需要修改的 NAT 端口映射对应操作列的编辑图标，弹出修改 NAT 端口对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

2. 参数解释

表9-12 页面各参数项描述

页面参数	描述
NAT DMZ服务	虚拟服务器功能，可提高局域网安全性。配置该参数时，可根据需要进行选择： • 若开启该功能，则本设备收到一个来自外部网络的请求，首先查询虚拟服务列表，如有匹配则发送到对应的 IP 地址，若无匹配，转发到 DMZ 主机上 • 若禁用 NAT DMZ 服务：当外部请求和虚拟服务列表不匹配，则直接丢弃请求消息
主机地址	DMZ主机的IP地址
协议类型	内网主机使用的传输协议，配置该参数时，可根据需要进行选择： • 若内网主机使用的是 TCP 传输协议，则选择“TCP” • 若内网主机使用的是 UDP 传输协议，则选择“UDP” • 若内网主机使用的是 TCP 和 UDP 传输协议，则选择“TCP+UDP”
外部地址	设备上的公网地址，设置方式有两种： • 当前接口 IP 地址：当前设备 WAN 口的 IP 地址 • 其他地址：设备上的其他公网 IP 地址
接口	选择接口时可直接使用WAN接口IP地址作为外部地址
外部端口	内网主机映射到外部地址上，外部地址开放的端口，配置该参数时，可根据需要进行选择： • 若对外提供的是 FTP 服务，则选择“FTP” • 若对外提供的是 TELNET 服务，则选择“TELNET” • 若对外提供的是其他的服务，则输入服务所使用的端口号范围。配置该参数时，起始端口号不能大于结束端口号
内部地址	内网主机的IP地址。即该主机需要对外提供指定服务
内部端口	内网主机上真实开放的服务端口
是否启用	此策略的执行动作，主要分为： • 启用：表示启用此策略，配置完成后，策略立即生效 • 未启用：表示暂不启用此策略
描述	策略的描述信息，可对策略进行简单的描述，方便使用

操作	可对该配置进行编辑和删除操作

9.4.3 配置一对一映射

1. 功能简介

如果需要一个内网 IP 地址一对一映射到一个公网 IP 地址上，则可以设置该功能。

2. 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。

3. 配置步骤

页面向导：[网络设置/NAT 配置/一对一映射]

本页面为您提供如下主要功能：

- 显示已添加的一对一映射详细信息
- 启用一对一映射
- 添加 NAT 一对一映射
- 删除已添加的 NAT 一对一映射
- 修改已添加的 NAT 一对一映射

1. 勾选“开启”选项，启用一对一映射功能

添加 NAT 一对一映射：

1. 单击<添加>按钮，弹出添加 NAT 一对一映射对话框，设置内部地址、外部地址、接口等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的 NAT 一对一映射：

1. 勾选需要删除的 NAT 一对一映射前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的NAT一对一映射：

1. 点击需要修改的 NAT 一对一映射对应操作列的编辑图标，弹出修改应用对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

4. 参数解释

表9-13 页面各参数项描述

页面参数	描述
内部地址	内网主机的IP地址。即该主机需要对外提供指定服务
外部地址	设备上的公网IP地址
接口	内网主机对外映射的设备WAN口。既报文经过此接口进行映射。若不设置此参数，则表示对所有WAN口生效
状态	此策略的执行动作，主要分为： • 启用：表示启用此策略，配置完成后，策略立即生效 • 未启用：表示暂不启用此策略
描述	策略的描述信息，可对策略进行简单的描述，方便使用

9.4.4 配置地址池

1. 配置步骤

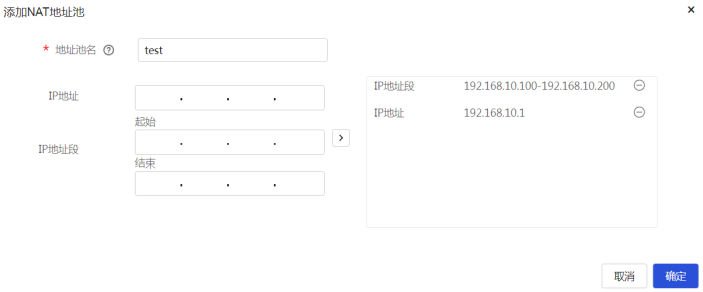
页面向导：[网络设置/NAT 配置/地址池]

本页面为您提供如下主要功能：

- 显示已添加的地址池详细信息
- 添加 NAT 地址池
- 删除已添加的 NAT 地址池
- 修改已添加的 NAT 地址池

添加 NAT 地址池：

1. 单击<添加>按钮，弹出添加 NAT 地址池对话框，设置地址池名、IP 地址、等参数信息
2. 点击<确定>按钮，完成配置

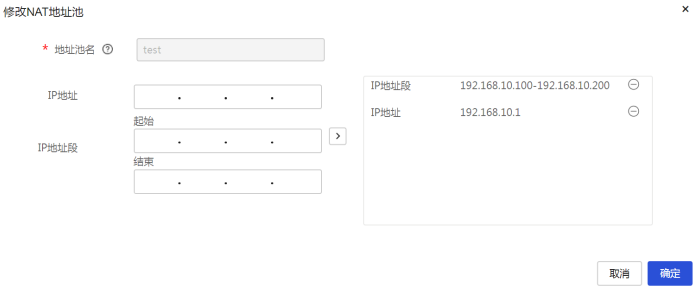


删除已添加的 NAT 地址池：

1. 勾选需要删除的 NAT 地址池前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的NAT地址池：

1. 点击需要修改的 NAT 地址池对应操作列的编辑图标，弹出修改应用对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



2. 参数解释

表9-14 页面各参数项描述

页面参数	描述
地址池名	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
IP地址	运营商提供的公网IP地址。配置该参数时，输入IP地址后，需点击配置项右侧的“>”按钮，提交配置的地址池内容
IP地址段	公网IP地址范围。若运营商提供多个公网IP地址，需配置此项。配置该参数时，输入起始和结束IP地址后，需点击配置项右侧的“>”按钮，提交配置的地址池内容。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

9.4.5 配置端口触发

1. 注意事项

当触发端口包含多个端口时，外来端口的连接只能对最后一个触发端口生效。

2. 配置步骤

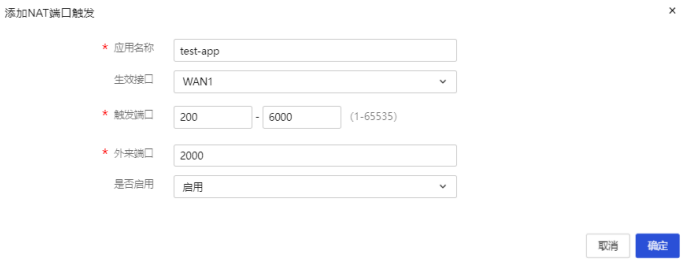
页面向导：[网络设置/NAT 配置/端口触发]

本页面为您提供如下主要功能：

- 显示已添加的端口触发详细信息
- 添加 NAT 端口触发
- 删除已添加的 NAT 端口触发
- 修改已添加的 NAT 端口触发

添加 NAT 端口触发：

1. 单击<添加>按钮，弹出添加端口触发对话框，设置应用名称、生效接口、触发端口等参数信息
2. 点击<确定>按钮，完成配置

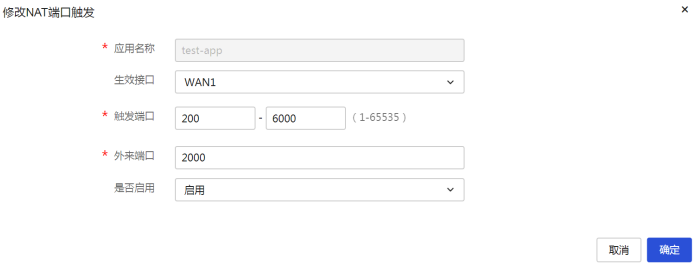


删除已添加的 NAT 端口触发：

1. 勾选需要删除的 NAT 地址池前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的NAT端口触发：

1. 点击需要修改的 NAT 端口触发对应操作列的编辑图标，弹出修改应用对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



3. 参数解释

表9-15 页面各参数项描述

页面参数	描述
应用名称	端口触发规则的名称
生效接口	报文的来源接口，即规则对从某一接口收到的数据包进行控制
触发端口	局域网内的客户端向外网服务器发起请求的端口。配置该参数时，端口范围必须从小到大。如果只有一个端口，则左右两边的文本框请填写同一端口号
外来端口	外网服务器需要主动向局域网内客户端请求的端口。配置该参数时，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
是否开启	此策略的执行动作，主要分为： • 启用：表示启用此策略，配置完成后，策略立即生效 • 未启用：表示暂不启用此策略

操作	可对该配置进行编辑和删除操作

9.4.6 配置 NAT hairpin

1. 功能简介

如果内网用户需要与外网用户一样，使用公网 IP 地址访问内网服务器，则可以开启 NAT hairpin 功能。

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

页面向导：[网络设置/NAT 配置/高级配置]

设置 NAT hairping：

1. 启用 NAT hairping 功能，设置当前 NAT hairping 生效接口
2. 单击<应用>按钮，完成配置

3. 参数解释

表9-16 页面各参数项描述

页面参数	描述
NAT hairpin	选择是否开启NAT hairpin功能，点击<应用>按钮完成配置。若开启NAT hairpin功能，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。配置NAT hairpin功能时，需设置NAT hairpin生效接口。点击<设置>按钮，在弹出的对话框中，通过如下两种方式设置NAT hairpin生效接口： • 勾选“待选接口”选项，点击“待选接口”选项下方的“>”按钮，待选接口列表中的所有接口都会被放入已选接口列表，表示修改所有接口的 NAT hairpin 功能 • 勾选待选接口列表中的一个或多个接口，点击“待选接口”选项下方的“>”按钮，表示修改选中接口的 NAT hairpin 功能 • 如果想要取消某个选中接口，在已选接口列表中勾选此接口，点击“待选接口”选项下方的“<”按钮，该接口会被放入待选接口列表，表示不会修改此接口的 NAT hairpin 功能 设置完成，点击<确定>按钮使配置生效

9.4.7 配置 NAT ALG

1. 配置步骤

页面向导：[网络设置/NAT 配置/高级配置]

设置 NAT ALG：

1. 启用指定协议的NAT ALG功能。
2. 单击<应用>按钮，完成配置

2. 参数解释

表9-17 页面各参数项描述

页面参数	描述
NAT ALG	为了保证一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，需启用指定协议的NAT ALG功能 配置该参数时，可根据需要进行选择： • 若报文使用的是 SIP 协议，则选择“启用 SIP” • 若报文使用的是 FTP 协议，则选择“启用 FTP” • 若报文使用的是 H323 协议，则选择“启用 H323” • 若报文使用的是 TFTP 协议，则选择“启用 TFTP” • 若报文使用的是 RTSP 协议，则选择“启用 RTSP” • 若报文使用的是 PPTP 协议，则选择“启用 PPTP” 设置完成，需点击“应用”按钮，使配置生效

9.4.8 配置自定义协议端口号

1. 配置步骤

页面向导：[网络设置/NAT 配置/高级配置]

设置自定义协议端口号：

1. 设置自定义的 SIP 端口号
2. 单击<应用>按钮，完成配置

2. 参数解释

表9-18 页面各参数项描述

页面参数	描述
自定义协议端口号	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 SIP端口号的输入范围为1-65535，最多可输入7个端口号，需用英文逗号隔开，如：2000,3000,4000

9.4.9 配置网络连接

1. 配置步骤

页面向导：[网络设置/NAT 配置/高级配置]

设置网络连接：

1. 设置当前网络连接数、网络连接总数、选择要清除网络连接的接口等参数信息
2. 单击<应用>按钮，完成配

2. 参数解释

表9-19 页面各参数项描述

页面参数	描述
网络连接	当前网络连接数：当前设备已建立的网络连接总数 网络连接总数：设备可创建的网络连接总数，即会话总数，当设置值小于当前已建立的网络连接总数时会影响新连接的建立 选择要清除网络连接的接口：需要清除网络连接的接口。当存在网络攻击影响业务运行或者修改防火墙规则、策略路由、NAT配置等未即时生效时，可以尝试清除网络连接。配置该参数时，由于清除网络连接会影响现有业务的正常运行，设备正常运行时，请谨慎操作

9.5 PoE供电

说明

不同款型的设备对本功能的支持情况不同，请以设备的实际情况为准。

9.5.1 功能简介

PoE（Power over Ethernet，以太网供电），是指设备通过以太网电口，利用双绞线对外接 PD（Powered Device，受电设备）进行供电。

9.5.2 配置 PoE 供电

1. 配置步骤

页面向导：[网络设置/POE 供电]

1. 开启设备 PoE 端口的供电功能

2. 参数解释

表9-20 页面参数描述

页面参数	描述
整机PoE供电功率使用率	整机当前已使用供电功率占整机最大供电功率的百分比
最大供电功率	整机最大供电功率
当前使用功率	整机当前已使用的供电功率
当前剩余功率	整机当前未使用的供电功率
当前功率	PoE端口当前使用的供电功率
端口状态	PoE端口的供电状态，包括： • 端口 Down-PoE 供电：开启 • 端口 Down-PoE 供电：关闭 • 端口 Up-PoE 供电：开启 • 端口 Up-PoE 供电：开启（供电异常：总功率过载/端口功率过载）。 • 端口 Up-PoE 供电：关闭
PoE开关	开启或关闭PoE端口的供电功能

9.6 IPv6配置

9.6.1 简介

本功能主要用于开启设备的 IPv6 功能，配置 WAN 接口、VLAN 接口参数以及配置静态 DHCPv6。

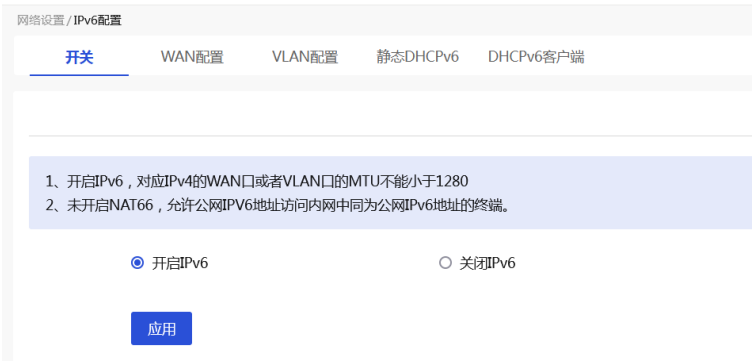
IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议）。它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。

9.6.2 开关

1. 配置步骤

页面向导：[网络设置/IPv6 配置/开关]

开启设备的IPv6功能



2. 参数解释

表9-21 页面参数描述

关键项	描述
开关	是否开启IPv6功能。若开启该功能，设备在具有IPv6地址后，可以与其他启用了IPv6的设备进行通信。缺省关闭IPv6功能。 设置完成，需点击“应用”按钮，使配置生效。

9.6.3 WAN 配置

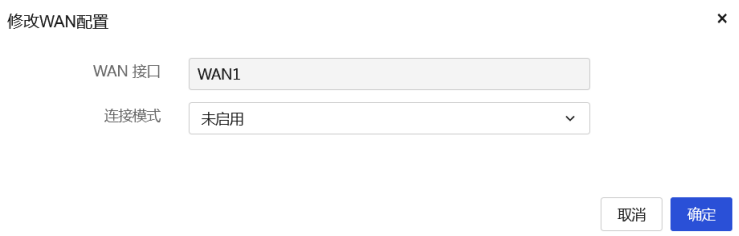
1. 注意事项

(1) WAN 接口连接模式设置为自动获取时，DHCPv6 报文会携带 IANA 以及 IAPD，且 IAPD 中不携带 IA Prefix，是否可获取到 IPv6 前缀以及 IPv6 前缀长度将由服务端算法决定。

(2) WAN 接口连接模式设置为固定地址时，若 IPv6 前缀长度输入范围为 48~64，则该地址将作为前缀使用。

2. 配置步骤

页面向导：[网络设置/IPv6 配置/WAN 配置]

WAN口不启用IPv6访问外网功能	
WAN口通过自动获取的方式获取IPv6地址	
WAN口通过手动输入的方式获取IPv6地址	

3. 参数解释

表9-22 页面参数描述

关键项	描述
线路	设备接入广域网的线路序号。
接口	设备接入广域网的接口。
连接模式	设备WAN口获取IPv6地址的方式，包括： • 未启用：表示该 WAN 口不启用 IPv6 访问外网功能。 • 自动获取：从 DHCPv6 服务器自动获取接入广域网的公网 IPv6 地址。 ○ NAT66 地址转换：根据实际需求选择是否启用该功能。当需要在 IPv6 网络中隐藏内部网络的 IPv6 地址时，可启用此功能。

	• 固定地址：手动输入 IPv6 地址、IPv6 前缀长度、网关地址等信息。
	  ○ IPv6 地址：接入广域网的固定 IPv6 地址
	  ○ IPv6 前缀长度：IPv6 地址的前缀长度，取值为 48~64。
	  ○ 网关地址：接入广域网的 IPv6 网关地址
	  ○ DNS1 和 DNS2：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。
	  ○ NAT66 地址转换：根据实际需求选择是否启用该功能。当需要在 IPv6 网络中隐藏内部网络的 IPv6 地址时，可启用此功能。

链路本地地址	用于同一链路内通信的特定于链路的IPv6地址。
操作	可对该配置进行编辑操作。

9.6.4 VLAN 配置

1. 功能简介

为设备创建连接内网的 VLAN 与 VLAN 接口，并可将 VLAN 接口作为内网设备的网关，提供 DHCPv6 服务。

2. 注意事项

(1) VLAN 接口进行 DHCPv6 分配时，若设置 VLAN 接口的 IPv6 前缀长度属于[0,32]以及[64,128]时，将无法分出 IPv6 前缀，若设置的 VLAN 接口的 IPv6 前缀长度属于(64,128]时，将无法分出 IPv6 地址。

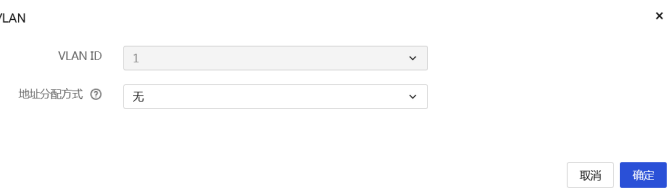
(2) VLAN 接口在进行 IPv6 前缀分配时，若 VLAN 接口设置的 IPv6 前缀长度小于 62 且收到的 DHCPv6 报文中的 IAPD 不携带 IA Prefix，则 VLAN 接口将默认分出前缀长度为 62 的前缀，若 VLAN 接口设置的 IPv6 前缀长度等于 62 将默认分出前缀长度为 63 的前缀，以此类推，VLAN 接口最多分出前缀长度为 64 的前缀。

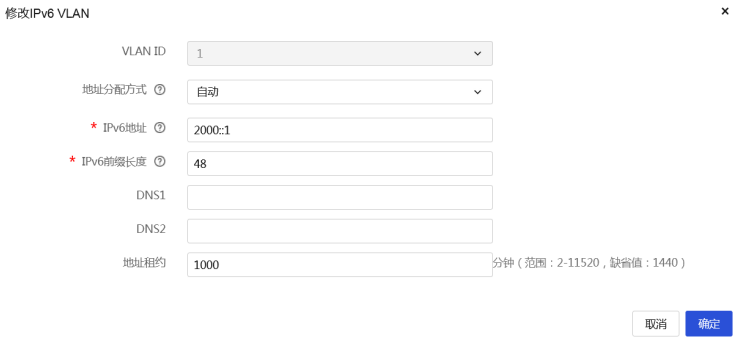
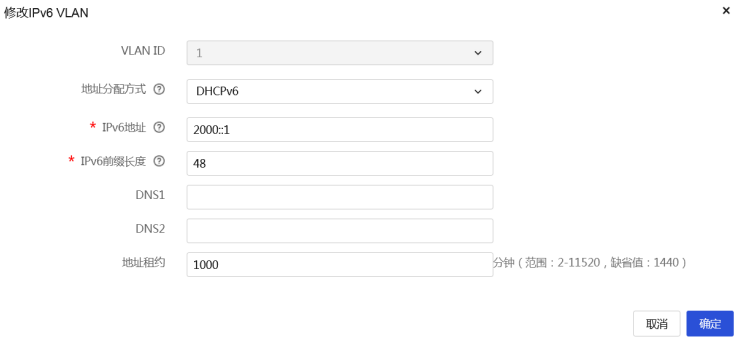
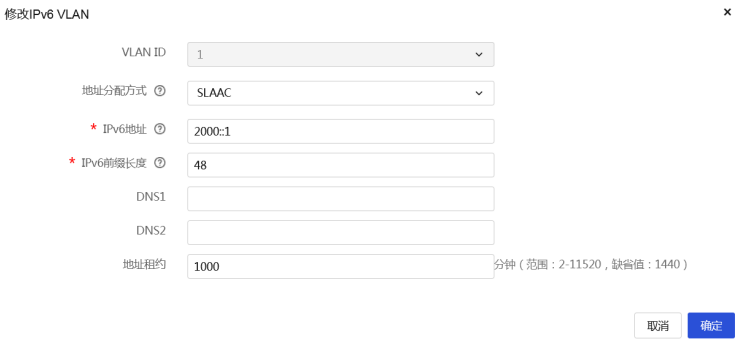
(3) IPv6 前缀长度输入范围为 48~64，则该地址将作为前缀使用。

3. 配置步骤

页面向导：[网络设置/IPv6 配置/VLAN 配置]

不配置IPv6 VLAN



同时使用DHCPv6和SLAAC方式分配IPv6地址	
通过 DHCPv6 服务器分配 IPv6 地址	
根据设备的链路层地址及路由器发布的前缀信息自动配置IPv6地址	
通过从指定WAN接口获取前缀后再生成接口的IPv6地址	

4. 参数解释

表9-23 页面参数描述

关键项	描述
VLAN ID	该VLAN接口的ID号。

地址分配方式	设备获取IPv6地址的方式，选项包括：
	• 无：不进行 IPv6 地址配置。
	• 自动：同时使用 DHCPv6 和 SLAAC 方式分配 IPv6 地址。
	  ○ IPv6 地址：分配给该 VLAN 接口的 IPv6 地址。
	  ○ IPv6 前缀长度：IPv6 地址的前缀长度，取值为 48~64。
	  ○ DNS1 和 DNS2：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。
	  ○ 地址租约：IPv6 地址的租用时间。
	• DHCPv6：设备从 DHCPv6 服务器获取 IP 地址，选择该选项时，网络环境中需要存在 DHCPv6 服务器。为动态分配 IPv6 地址
	  ○ IPv6 地址：分配给该 VLAN 接口的 IPv6 地址。
	  ○ IPv6 前缀长度：IPv6 地址的前缀长度，取值为 48~64。
	  ○ DNS1 和 DNS2：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。
	  ○ 地址租约：IPv6 地址的租用时间。
	• SLAAC：将根据设备的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址。
	  ○ IPv6 地址：分配给该 VLAN 接口的 IPv6 地址。
	  ○ IPv6 前缀长度：IPv6 地址的前缀长度，取值为 48~64。
	  ○ DNS1 和 DNS2：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。
	  ○ 地址租约：IPv6 地址的租用时间。
	• DHCPv6-PD：通过从指定 WAN 接口获取前缀后再生成接口的 IPv6 地址
	  ○ 子网前缀名称：子网的标识名称，可设置从哪一个 WAN 接口获取前缀，默认为全部接口。
	  ○ 子网前缀长度：指定子网掩码的长度，用于定义子网范围，取值为 48~64。
	  ○ 子网 ID：指定特定子网的标识符。
	  ○ DNS1 和 DNS2：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。
	  ○ 地址租约：IPv6 地址的租用时间。

链路本地地址	用于同一网络链路内通信的专用IPv6地址。
操作	可对该配置进行编辑和删除操作。

9.6.5 配置静态 DHCPv6

1. 功能简介

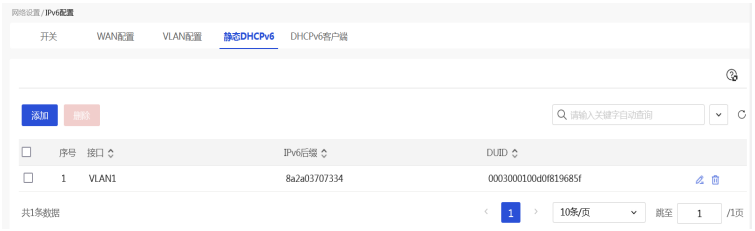
如果需要为某些客户端分配固定的 IPv6 地址，则需要配置静态 DHCPv6 将客户端的 DUID 与 IPv6 地址进行绑定。

2. 配置步骤

页面向导：[网络设置/IPv6 配置/静态 DHCPv6]

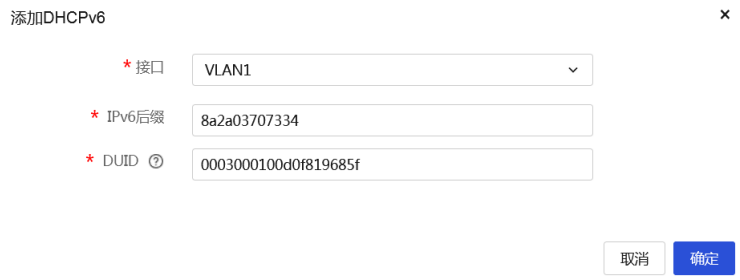
本页面为您提供如下主要功能：

- 显示已添加 DHCPv6 静态绑定关系的详细信息
- 添加 DHCPv6 静态绑定关系
- 删除 DHCPv6 静态绑定关系
- 修改已添加的 DHCPv6 静态绑定关系



添加 DHCPv6 静态绑定关系：

1. 单击<添加>按钮，弹出添加 DHCPv6 对话框，设置接口、IPv6 后缀、DUID 的参数信息
2. 点击<确定>按钮，完成配置

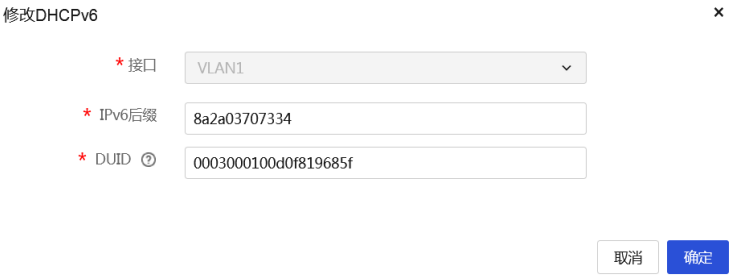


删除已添加的 DHCPv6 静态绑定关系：

1. 勾选需要删除的 DHCPv6 静态绑定关系前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的DHCPv6静态绑定关系：

1. 点击需要修改的 DHCPv6 静态绑定关系对应操作列的编辑图标，弹出 DHCP 静态绑定关系对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



3. 参数解释

表9-24 页面参数描述

关键项	描述
序号	该VLAN接口的ID号。
接口	设备上已创建的VLAN接口。
IPv6后缀	与IPv6前缀共同生成IPv6地址的接口标识，即IPv6后缀。
DUID	客户端的唯一标识符 (DHCP Unique Identifier)，用于区分不同设备。

9.6.6 DHCPv6 客户端配置

1. 功能简介

DHCPv6 服务器通过动态分配或者静态绑定为 DHCPv6 客户端分配 IPv6 地址后，可以通过本页面查看分配给 DHCPv6 客户端的 IPv6 地址信息。

2. 配置步骤

页面向导：[网络设置/IPv6 配置/DHCPv6 客户端]

显示设备DHCP分配的详细信息	

3. 参数解释

表9-25 页面参数描述

关键项	描述
序号	DHCPv6分配信息的编号。
DHCPv6服务	设备上开启 DHCPv6 服务的 VLAN 接口。
IPv6地址	分配给客户端设备的IPv6地址。
DUID	客户端的唯一标识符，用于区分不同设备。
有效时间	地址租约的剩余有效时间，以秒为单位。

9.7 地址组

9.7.1 功能简介

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。

9.7.2 注意事项

(1) 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。

(2) 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。

(3) 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。

9.7.3 配置步骤

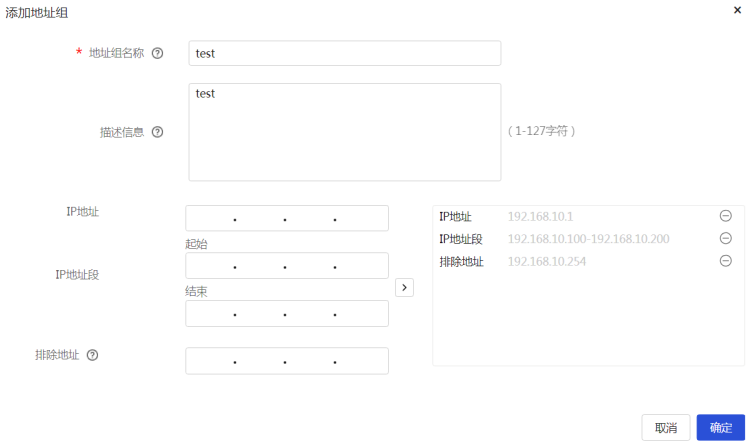
页面向导：[网络设置/地址组]

本页面为您提供如下主要功能：

- 显示已添加的地址组详细信息
- 添加地址组
- 删除已添加的地址组
- 修改已添加的地址组

添加地址组：

1. 单击<添加>按钮，弹出添加地址组对话框，输入地址组的名称、描述信息、ip 地址等参数信息
2. 点击<确定>按钮，完成配置

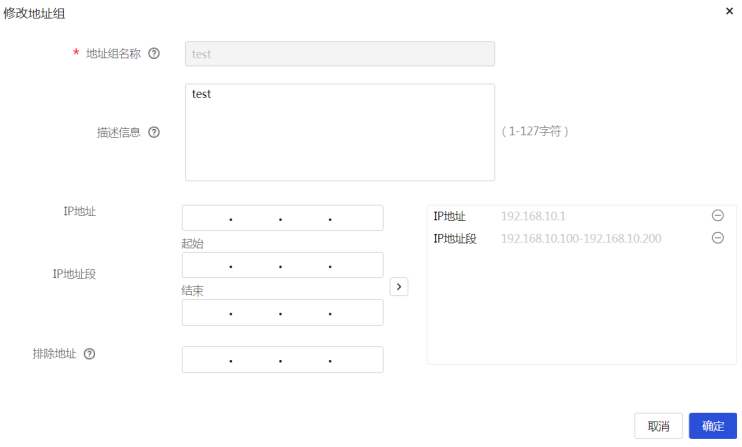


删除已添加的时间组：

1. 勾选需要删除的地址组前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的地址组：

1. 点击需要修改的时间组对应操作列的编辑图标，弹出修改时间组对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



9.7.4 参数解释

表9-26 页面各参数项描述

页面参数	描述
地址组名称	一组用户主机名或IP地址集合的名称。配置该参数时，该名称可以提示用户该地址组中的地址特征。地址组名称不支持命名为any（不区分大小写）
描述信息	地址组的描述信息，可对地址组进行简单的描述，方便使用
IP地址	添加到地址组的单个IP地址。配置该参数时，输入IP地址后，需点击配置项右侧的“>”按钮，提交配置的地址池内容
IP地址段	添加到地址组中的IP地址范围，配置该参数时，输入起始IP地址和结束IP后，需点击配置项右侧的“>”按钮，提交配置的地址池内容
排除地址	地址组中需排除的IP地址。配置该参数时，输入排除地址后，需点击配置项右侧的“>”按钮，提交配置的地址池内容
操作	可对该配置进行编辑、删除和查看详情操作

9.8 时间组

9.8.1 功能简介

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。

9.8.2 注意事项

(1) 最多可以创建 64 个不同名称的时间组。

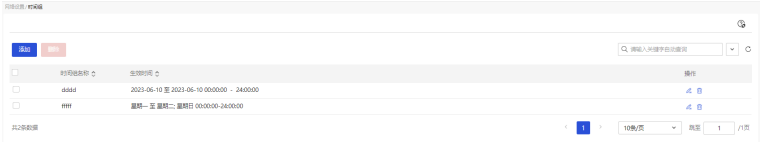
(2) 一个时间组内最多可以配置 16 个周期性生效的时间段或 16 个非周期生效的时间段。

9.8.3 配置步骤

页面向导：[网络设置/时间组]

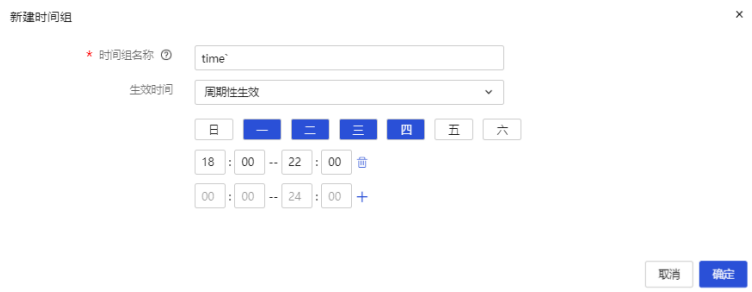
本页面为您提供如下主要功能：

- 显示已添加的时间组详细信息
- 添加时间组
- 删除已添加的时间组
- 修改已添加的时间组



添加时间组：

1. 单击<添加>按钮，弹出新建时间组对话框，输入时间组的名称、生效时间等参数信息
2. 点击<确定>按钮，完成配置

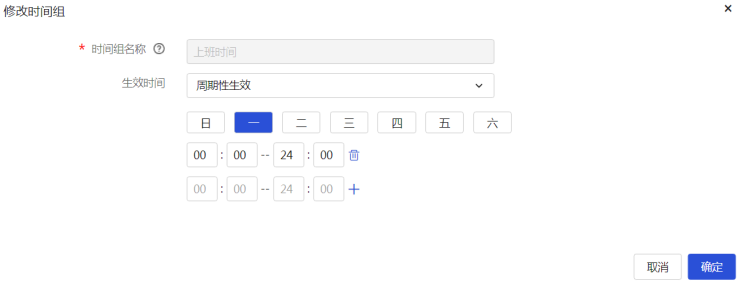


删除已添加的时间组：

1. 勾选需要删除的时间组前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的时间组：

1. 点击需要修改的时间组对应操作列的编辑图标，弹出修改时间组对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



9.8.4 参数解释

表9-27 页面参数描述

页面参数	描述
时间组名称	特定时间段的名称。配置该参数时，该名称可以提示用户该时间段中的时间段特征。时间组名称不支持命名为any（不区分大小写）
生效时间	该时间组的生效时间，设置方式有两种： • 周期性生效：以周作为周期，循环生效。配置该参数时，选择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，点击<确定>按钮，完成本时间段的配置 • 非周期生效：在指定的时间范围内生效。配置该参数时，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，点击<确定>按钮，完成本时间段的配置
操作	可对该配置进行编辑或者删除操作

9.9 应用组

9.9.1 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。

9.9.2 自定义应用

1. 功能简介

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

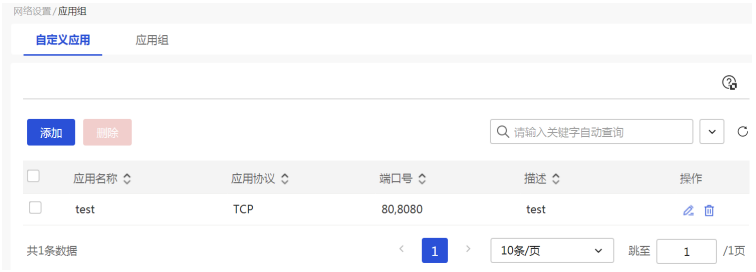
自定义应用创建完成后，需要将其添加到“应用组”中，并在配置带宽管理时引用对应的应用组，才能实现对特性应用的带宽管理。

3. 配置步骤

页面向导：[网络设置/应用组/自定义应用]

本页面为您提供如下主要功能：

- 显示已添加应用的详细信息
- 添加应用
- 删除已添加的应用
- 修改已添加的应用



添加应用：

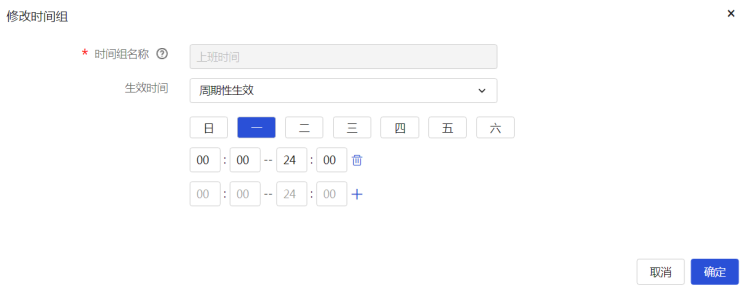
1. 单击<添加>按钮，弹出添加应用对话框，输入应用的名称、应用协议、端口号和描述等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的应用：

1. 勾选需要删除的应用前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的应用：

1. 点击需要修改的应用对应操作列的编辑图标，弹出修改应用对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



4. 参数解释

表9-28 页面参数描述

页面参数	描述
应用名称	特定应用的名称
应用协议	应用使用的协议类型，配置该参数时，可根据需要进行选择： • 若应用为 TCP 报文，则选择“TCP”或“UDP” • 若应用为 UDP 报文，则选择“TCP”或“UDP” • 若应用为 TCP 和 UDP 报文，则选择“TCP+UDP”
端口号	应用实际使用的端口号
描述信息	配置的描述信息，可对配置进行简单的描述，方便使用
操作	可对该配置进行编辑或者删除操作

9.9.3 创建应用组

1. 功能简介

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

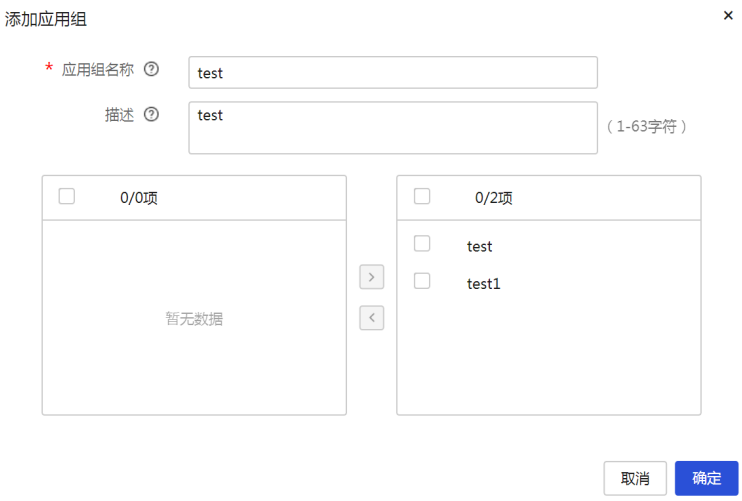
页面向导：网络设置→应用组→应用组[网络设置/应用组/应用组]

本页面为您提供如下主要功能：

- 显示已添加应用组的详细信息
- 添加应用组
- 删除已添加的应用组
- 修改已添加的应用组

添加应用：

1. 单击<添加>按钮，弹出添加应用对话框，输入应用的名称和描述信息。在左侧选择框中，勾选应用，点击< > >按钮，将应用添加到右侧选择框中，说明应用已被添加。在右侧选择框中，勾选应用，点击< < >按钮，将应用移至左侧选择框中，说明应用已被移除
2. 点击<确定>按钮，完成配置

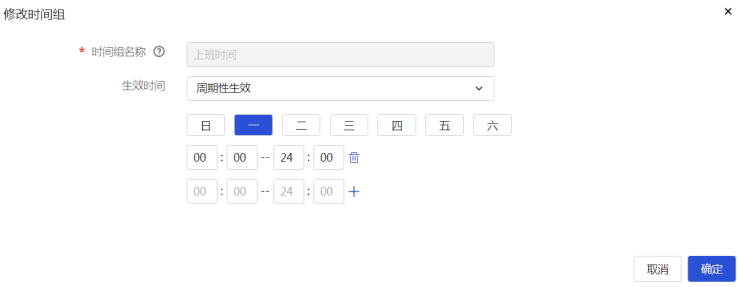


删除已添加的应用组：

1. 勾选需要删除的应用前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的应用组：

1. 点击需要修改的应用组对应操作列的编辑图标，弹出修改应用组对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



4. 参数解释

表9-29 页面参数描述

页面参数	描述
应用组名称	一组特定应用集合的名称。配置该参数时，该名称可以提示用户该应用组中的应用组特征。应用组名称不支持命名为any（不区分大小写）
描述信息	该应用组的描述信息，可对应用组进行简单的描述，方便使用
待选应用	设备上已创建的所有应用，配置该参数时，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
已选应用	划分到该应用组的应用，配置该参数时，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
操作	可对该配置进行编辑或者删除操作

10 上网行为管理

10.1 带宽管理

10.1.1 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。

10.1.2 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。

10.1.3 配置 IP 限速

1. 功能简介

对指定接口或指定用户的流量进行带宽管理。

2. 注意事项

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

页面向导：[上网行为管理/带宽管理/IP 限速]

本页面为您提供如下主要功能：

- 显示已添加 IP 限速的详细信息
- 添加 IP 限速
- 删除已添加的 IP 限速
- 修改已添加的 IP 限速

添加IP限速策略：

1. 单击<添加>按钮，弹出添加 IP 限速策略对话框，设置应用接口、用户范围、流量限制和限制时段等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的 IP 限速：

1. 勾选需要删除的 IP 限速前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的IP限速：

1. 点击需要修改的 IP 限速对应操作列的编辑图标，弹出修改 IP 限速对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

4. 参数解释

表10-1 页面参数描述

页面参数	描述
应用接口	报文的来源接口，即规则对从某一接口收到的数据包进行控制
用户范围	规则需要控制的地址组。配置该参数时，需选择已创建的地址组。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
上传带宽	地址组内的用户上传方向的最大带宽值。单位为Mbps。配置此参数之前，需根据运营商提供的实际上行带宽配置当前线路上行带宽
下载带宽	地址组内的用户下载方向的最大带宽值。单位为Mbps。配置此参数之前，需根据运营商提供的实际上行带宽配置当前线路下行带宽
流量分配	流量的分配方式：主要分为： • 共享式：指定地址组内的所有计算机共享给定的带宽 • 独占式：指定地址组内的每台计算机各自占有给定的带宽（即流量上限）
弹性共享	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
限制时段	IP限速的生效时间段，配置该参数时，可选择： • 所有时段 • 选择已创建的时间组。如需新增时间分组，可通过点击右侧<新增时间组>按钮创建新的时间组
操作	可对此规则进行编辑和删除操作

10.1.4 配置限制通道

1. 功能简介

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

页面向导：[上网行为管理/带宽管理/限制通道]

设置限制通道：

1. 启用限制通道功能，设置每接口上下行最大流速和应用组信息
2. 单击<应用>按钮，完成配置

4. 参数解释

表10-2 页面参数描述

页面参数	描述
启用限制通道	是否开启限制通道流速上限功能。若开启该功能，设备将按照配置的规则进行工作。缺省关闭功能限制通道流速上限功能
线路*N*上行带宽	显示线路*N*的上行带宽。如需设置此参数，请到WAN配置页面中进行配置（单击导航树中[网络设置/外网配置]菜单项，单击“WAN配置”页签，进入WAN配置页面）
线路*N*下行带宽	显示线路*N*的下行带宽。如需设置此参数，请到WAN配置页面中进行配置（单击导航树中[网络设置/外网配置]菜单项，单击“WAN配置”页签，进入WAN配置页面）
每接口上行最大流速	各接口允许报文上行通过的最大数据流量。如果已设置线路*N*的上行带宽，则每接口上行最大流速需要小于或等于线路*N*上行带宽的最小值
每接口下行最大流速	各接口允许报文下行通过的最大数据流量。如果已设置线路*N*的下行带宽，则每接口下行最大流速需要小于或等于线路*N*下行带宽的最小值

选择应用组	匹配通道流速上限限制的应用组。配置该参数时，需选择已创建的应用组。如需新增应用组，可通过点击右侧<新增应用组>按钮创建新的应用组

10.1.5 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

页面向导：[上网行为管理/带宽管理/绿色通道]

设置绿色通道：

1. 启用绿色专用通道功能，配置线路的上下行带宽、流量数据包的最大长度和应用组信息
2. 单击<应用>按钮，完成配置

3. 参数解释

表10-3 页面参数描述

页面参数	描述
启用绿色专用通道	是否开启绿色专用通道功能。若开启该功能，该通道中的业务数据流将保证使用设定的带宽值 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
限制绿色通道流速上限	报文通过绿色通道的流速上限。可根据需要配置该参数，若开启该功能，则设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
匹配绿色通道数据包长度选择	报文通过绿色通道的最大长度，可根据需要配置该参数。若开启该功能，路由器会根据设置的报文长度来识别报文，小于该长度的报文将通过绿色专用通道转发
选择应用组	绿色专用通道限制规则需要控制的应用组。配置该参数时，需选择已创建的应用组。如需新增应用组，可通过点击右侧<新增应用组>按钮创建新的应用组

10.2 上网行为管理

10.2.1 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。

10.2.2 配置应用控制

1. 配置步骤

页面向导：[上网行为管理/上网行为管理/应用控制]

3. 页面为您提供如下主要功能：

- 开启应用控制
- 添加应用控制
- 删除已添加的应用控制
- 修改已添加的应用

添加应用控制：

1. 单击<添加>按钮，配置策略名称、用户范围、限制时段和网络应用信息
2. 点击<确定>按钮，完成配置

删除已添加的应用控制：

1. 勾选需要删除的应用控制前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的应用控制：

1. 点击需要修改的应用控制对应操作列的编辑图标，修改相关配置项
2. 单击<确定>按钮，完成配置

2. 参数解释

表10-4 页面参数描述

页面参数	描述
开启应用控制	是否开启应用控制功能。若开启该功能，设备将按照配置的应用控制策略及规则进行工作。缺省关闭应用控制功能
策略名称	应用控制策略的名称
用户范围	策略需要控制的地址范围。配置该参数时，需选择已创建的地址组。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
限制时段	规则的生效时间。配置该参数时，可选择所有时段，或选择已创建的时间组。如需新增时间组，可通过点击右侧的<新增时间组>按钮创建新的时间组
应用控制	策略需要控制的网络应用，并配置对该应用的访问控制的动作，主要分为： • 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
操作	可对该策略进行编辑或者删除操作

10.2.3 配置网址控制

1. 功能简介

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*.*。注意通配符不能配置在字符串中间或者只配置通配符，例如 aaa*11 和*，否则会导致配置无法下发。

3. 配置步骤

页面向导：[上网行为管理/上网行为管理/网址控制]

本页面为您提供如下主要功能：

- 开启网址黑白名单模式
- 配置自定义网址分类
- 删除已添加的网址分类
- 导入自定义网址列表

开启网址黑白名单模式：

1. 勾选“网址黑名单模式”或“网址白名单模式”选项
2. 点击<确定>按钮，完成配置

配置自定义网址分类：

1. 设置自定义网址分类名称、地址组和时间组
2. 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。配置网址关键字
3. 单击<确定>按钮。完成配置

删除已添加的网址分类：

1. 选择需要删除的网址分类，点击<删除>按钮
2. 弹出确认提示对话框，单击<确定>按钮，完成配置

导入自定义网址列表

1. 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<上传文件>按钮，选择需导入的自定义网址列表
2. 点击<确定>按钮，完成配置

4. 参数解释

表10-5 页面参数描述

页面参数	描述
网址白名单	若开启该功能，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
网址黑名单	若开启该功能，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
序号	网址控制策略的编号
网址分类	网址关键字对话框。输入相应的网址，单击右侧的<+>按钮，网址添加成功。单击<确定>按钮，完成添加网址关键字
地址组	策略需要控制的IP地址组。
时间组	策略的生效时间
操作	可对该条策略进行如下操作： • 删除：删除此条策略 • 详情：设置网址关键字 • 导入：若自定义网址分类策略数量过多，可先导出 CSV 格式的自定义网址列表，填好策略后，再导入设备中 • 导出：导出 CSV 格式的自定义网址列表
网址关键字	策略的网址关键字。点击网址控制策略对应的操作列详情图标，在弹出的设置网址关键字对话框中，可设置网址关键字。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

10.2.4 配置文件控制

1. 功能简介

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，且仅对 HTTP 协议默认的 80 和 8080 端口生效。

2. 注意事项

支持文件下载控制需要满足以下两个条件：

- URL 字段长度小于 512 字节。

- 使用 HTTP Get 方法，文件类型必须在 URL 的尾部，如 http://serveraddr.com?filename=xxx.txt。

3. 配置步骤

页面向导：[上网行为管理/上网行为管理/文件控制]

本页面为您提供如下主要功能：

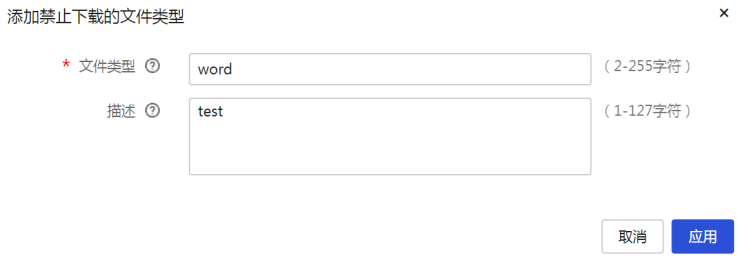
- 开启文件控制
- 添加禁止下载的文件类型
- 删除已添加的文件控制表项
- 修改已添加的文件控制表项

开启文件控制：

1. 勾选“开启文件控制”选项
2. 点击<确定>按钮，完成配置

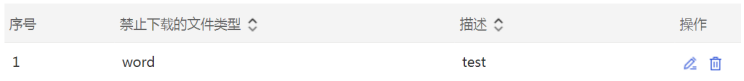
添加文件控制：

1. 单击<添加>按钮，弹出添加文件控制对话框，输入文件类型和描述信息
2. 点击<应用>按钮，完成配置



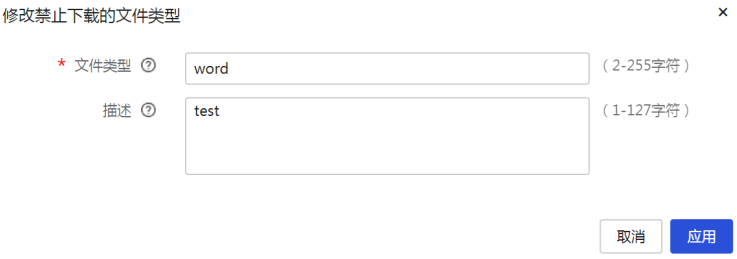
删除已添加的文件控制：

1. 选择需要删除的文件控制，点击<删除>按钮
2. 弹出确认提示对话框，单击<确定>按钮，完成配置



修改已添加的文件控制表项：

1. 点击需要修改的文件控制表项对应操作列的编辑图标，弹出禁止下载的文件类型对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



4. 参数解释

表10-6 页面参数描述

页面参数	描述
文件控制	是否开启文件控制功能。若开启该功能，设备将按照配置的文件控制策略及规则进行工作。缺省开启文件控制功能
序号	文件控制策略的编号
文件类型	不允许下载的文件后缀类型。例如.jpg
描述	策略的描述信息，可对策略进行简单的描述，方便使用
操作	可对该策略进行编辑或者删除操作

10.2.5 配置自定义网络应用

1. 注意事项

(1) 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。

(2) 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。

(3) 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。

(4) 在添加自定义网络应用时，建议只输入受限制网址的域名，避免输入资源路径，以免影响应用控制功能。

2. 配置步骤

页面向导：[上网行为管理/上网行为管理/自定义网络应用]

本页面为您提供如下主要功能：

- 显示已添加自定义网络应用的详细信息
- 添加自定义网络应用
- 删除已添加的自定义网络应用
- 修改已添加的自定义网络应用
- 导入自定义网络应用列表

添加自定义网络应用：

1. 单击<添加>按钮，弹出添加自定义网络应用对话框，输入应用名称、描述信息、协议类型、目的端口等参数信息
2. 点击<确定>按钮，完成配置

删除已添加的自定义网络应用：

1. 勾选需要删除的自定义网络应用前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置

修改已添加的自定义网络应用：

1. 点击需要修改的自定义网络应用对应操作列的编辑图标，弹出修改自定义网络应用对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

3. 参数解释

表10-7 页面参数描述

页面参数	描述
应用名称	自定义网络应用的名称
描述信息	规则的描述信息，可对规则进行简单的描述，方便使用
协议类型	该网络应用支持的协议类型，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	报文的转发方向，主要分为： • 客户端：表示设备发送的报文 • 服务器：表示设备接收的报文 • 任意：选择“任意”时，表示设备接收的所有报文
目的端口	该网络应用的目的端口号
报文长度	该网络应用的报文长度
目的IP	该网络应用的目的IP地址
报文特征	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 报文特征不支持输入“和{}字符，设置完成后，单击“>”按钮，将设置的报文特征添加到右侧方框中
管理状态	策略的开启或关闭状态
操作	可对该策略进行编辑或者删除操作

10.3 审计日志

10.3.1 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。

10.3.2 应用审计日志

1. 注意事项

对上网行为管理中应用控制功能的日志进行审计。

2. 配置步骤

页面向导：[上网行为管理/审计日志/应用审计日志]

勾选“开启审计日志”选项，开启应用的日志审计功能	
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	

3. 参数解释

表10-8 页面参数描述

页面参数	描述
序号	日志信息的编号
用户名/IP地址	触发应用控制规则的用户名或IP地址
应用类型	触发应用控制规则的网络应用
日期和时间	日志生成时的日期和具体时间
计数	生成此类日志的总数
动作	应用控制策略对需要控制的报文的执行动作，主要分为： • 阻断：表示策略拒绝报文通过，并记录日志 • 限速：表示策略限速报文通过，并记录日志

10.3.3 网址过滤日志

1. 功能简介

对上网行为管理中网址控制功能的日志进行审计。

2. 注意事项

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

页面向导：[上网行为管理/审计日志/网址过滤日志]

勾选“开启网址过滤日志”选项，网址过滤的日志审计功能	
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. 参数解释

表10-9 页面参数描述

页面参数	描述
序号	日志信息的编号
用户名/IP地址	触发应用控制规则的用户名或IP地址
目标网址	网址过滤规则中被禁止访问的网址
网址分类	目标网址的所属类别，例如：搜索门户等
日期和时间	日志生成时的日期和具体时间
计数	生成此类日志的总数
动作	应用控制策略对需要控制的报文的执行动作，主要分为： • 阻断：表示策略拒绝报文通过，并记录日志 • 允许：表示策略允许报文通过，并记录日志

10.3.4 审计服务器

1. 功能简介

将审计日志发送到指定的服务器。

2. 注意事项

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

页面向导：[上网行为管理/审计日志/审计服务器]

设置审计服务器：

1. 启用发送审计日志到服务器的功能，设置审计服务器地址和端口号
2. 单击<应用>按钮，完成配置

4. 参数解释

表10-10 页面参数描述

页面参数	描述
审计服务器	接收审计日志的指定服务器。若开启此功能，应用审计日志和网址过滤日志将会发送到此服务器
审计服务器地址	审计日志的服务器的IP地址或域名地址
端口	接收审计日志的服务器的端口号

11 网络安全

11.1 防火墙

1. 功能简介

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。

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。

3. 配置步骤

页面向导：[网络安全/防火墙]

本页面为您提供如下主要功能：

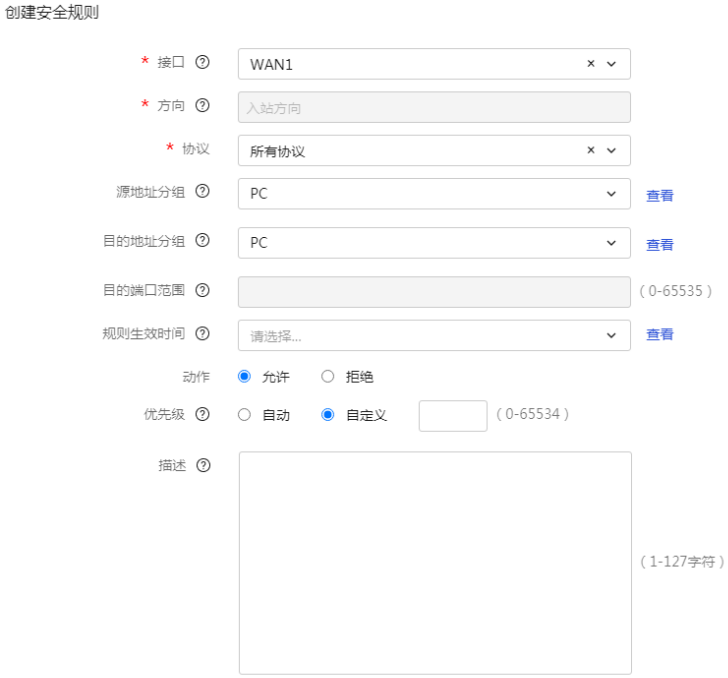
- 开启或关闭防火墙
- 设置缺省过滤规则
- 添加安全规则
- 删除安全规则
- 修改已创建的安全规则
- 显示已创建的安全规则信息

勾选“开启防火墙”单选框，开启防火墙功能

在缺省过滤规则配置项处，设置缺省过滤规则，单击<应用>按钮，保存配置

添加安全规则：

1. 单击<添加>按钮，弹出创建安全规则页面，配置接口、方向、优先级等参数信息
2. 单击<确定>按钮，完成配置



删除安全规则：

1. 勾选需要删除的安全规则
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改安全规则：

1. 单击需要修改的安全规则操作列的编辑图标，弹出修改安全规则对话框，修改相关参数
2. 单击<确定>按钮，完成配置

4. 参数解释

表11-1 页面参数描述

页面参数	描述
开启防火墙	是否开启防火墙功能。若开启该功能，设备将按照配置的防火墙及规则进行工作 缺省情况下为关闭状态
缺省过滤规则	对未匹配任何规则报文的处理方式，即当一个报文在未匹配任何规则时，设备对该报文的执行动作，主要分为： • 允许：允许报文通过防火墙 • 禁止：禁止报文通过防火墙 设置完成，需单击“应用”按钮，使配置生效 缺省状态为允许
接口	报文的来源接口，即规则对从某一接口收到的数据包进行控制
方向	显示安全规则的方向，包括入站方向和出站方向。 • 当“接口”参数选择为 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”参数选择为 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
协议类型	规则需要控制的报文协议类型。配置该参数时，可根据需要进行选择： • 若需控制某传输层协议的报文，则选择“TCP”或“UDP” • 若需控制 Ping、Tracert 等 ICMP 协议报文，则选择“ICMP” • 若需控制所有协议报文，则选择“所有协议”
源地址分组	规则需要控制的源IP地址范围。配置该参数时，需选择已创建的地址组。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
目的地址分组	规则需要控制的目的IP地址范围。配置该参数时，需选择已创建的地址组。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
目的端口范围	规则需要控制的目的端口号范围。配置该参数时，起始端口号不能大于结束端口号
规则生效时间	规则的生效时间。配置该参数时，需选择已创建的时间组。如需新增时间组，可通过点击右侧的<新增时间组>按钮创建新的时间组

动作	规则对需要控制的报文的执行动作，主要分为： • 允许：表示规则允许报文通过 • 拒绝：表示规则拒绝报文通过
优先级	规则的优先级。设置方式有两种： • 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
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对此条规则进行编辑、删除或者复制操作

11.2 连接限制

11.2.1 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。

11.2.2 网络连接限制数

1. 功能简介

网络连接限制是指在指定 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。

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

3. 配置步骤

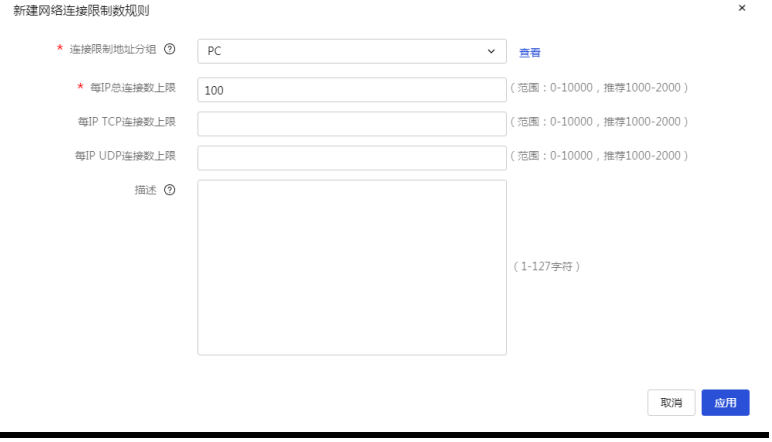
页面向导：[网络安全/连接限制/网络连接限制数]

本页面为您提供如下主要功能：

- 开启或关闭网络连接限制数
- 添加网络连接限制数规则
- 删除网络连接限制数规则
- 修改已添加的网络限制数规则
- 显示添加的网络连接限制数规则相关信息

添加网络连接限制数规则：

1. 单击<添加>按钮，弹出新建网络连接限制数规则对话框，配置相关参数
2. 单击<应用>按钮，完成配置



删除网络连接限制数规则：

1. 勾选需要删除的网络连接限制数规则，单击<删除>按钮，弹出确认提示对话框
2. 单击<确定>按钮，完成配置

修改网络连接限制数规则：

1. 单击需要修改的网络连接限制数规则对应操作列的编辑图标，弹出修改网络连接限制数规则对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

4. 参数解释

表11-2 页面参数描述

页面参数	描述
开启网络连接限制数	是否开启网络连接限制数功能。若开启该功能，设备将按照配置的网络连接限制数规则进行工作，缺省关闭网络连接数限制数功能
连接限制地址分组	规则需要控制的IP地址范围
每IP总连接数上限	允许每个IP地址发起的最大网络连接数
每IP TCP连接数上限	允许每个IP地址发起的最大TCP网络连接数
每IP UDP连接数上限	允许每个IP地址发起的最大UDP网络连接数
描述	规则的描述信息，可对规则进行简单的描述，方便使用

11.2.3 VLAN 网络连接限制数

1. 功能简介

VLAN 网络连接限制是指在指定 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。

2. 配置步骤

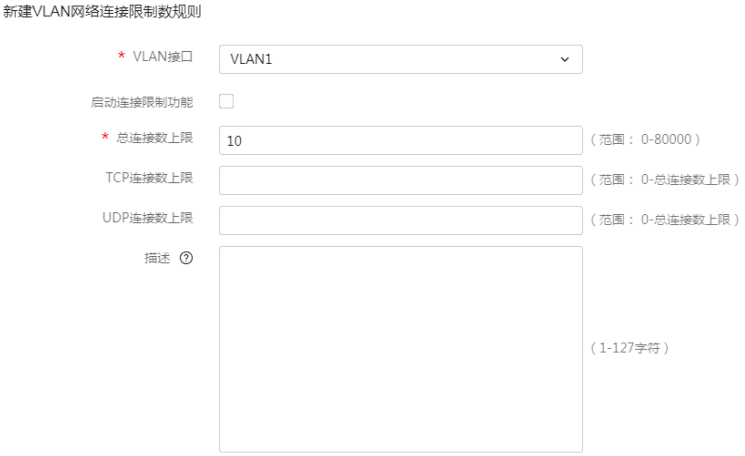
页面向导：[网络安全/连接限制/ VLAN 网络连接限制数]

本页面为您提供如下主要功能：

- 开启或关闭 VLAN 网络连接限制数
- 添加 VLAN 网络连接限制数规则
- 删除 VLAN 网络连接限制数规则
- 修改已添加的 VLAN 网络限制数规则
- 显示添加的 VLAN 网络连接限制数规则相关信息

添加VLAN网络连接限制数规则：

1. 单击<添加>按钮，弹出新建 VLAN 网络连接限制数规则对话框，配置相关参数
2. 单击<应用>按钮，完成配置



删除VLAN网络连接限制数规则：

1. 勾选需要删除的 VLAN 网络连接限制数规则，单击<删除>按钮，弹出确认提示对话框
2. 单击<确定>按钮，完成配置

修改VLAN网络连接限制数规则：

1. 单击需要修改的 VLAN 网络连接限制数规则对应操作列的编辑图标，弹出修改 VLAN 网络连接限制数规则对话框，修改相关配置项
2. 单击<确定>按钮，完成配置

3. 参数解释

表11-3 页面参数描述

页面参数	描述
开启VLAN网络连接限制	是否开启VLAN网络连接限制功能。若开启该功能，设备将按照配置的VLAN网络连接限制规则进行工作，缺省关闭VLAN网络连接限制数功能
VLAN接口	规则需要控制的VLAN接口
总连接数上限	允许指定的VLAN接口占用的最大网络连接数，避免个别VLAN占用过多的资源
TCP连接数上限	允许指定的VLAN接口发起的最大TCP网络连接数
UDP连接数上限	允许指定的VLAN接口发起的最大UDP网络连接数
描述	规则的描述信息，可对规则进行简单的描述，方便使用

11.3 MAC地址过滤

11.3.1 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 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。

11.3.2 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。

页面向导：[网络安全/MAC 地址过滤/MAC 过滤设置]

设置MAC地址过滤：

1. 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
2. 单击<应用>按钮，完成配置

2. 参数解释

表11-4 页面参数描述

页面参数	描述
端口	匹配MAC地址过滤策略的接口
过滤方式	设备进行MAC地址过滤的方式,主要分为： • 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
开启和关闭	是否开启MAC地址过滤功能： • 若开启该功能，设备将根据 MAC 地址列表中的 MAC 地址控制内网计算机访问因特网 • 若不开启该功能，局域网内的所有计算机都可以不受限制地访问因特网

11.3.3 MAC 黑白名单管理

1. 功能简介

添加或删除白名单。

2. 配置白名单

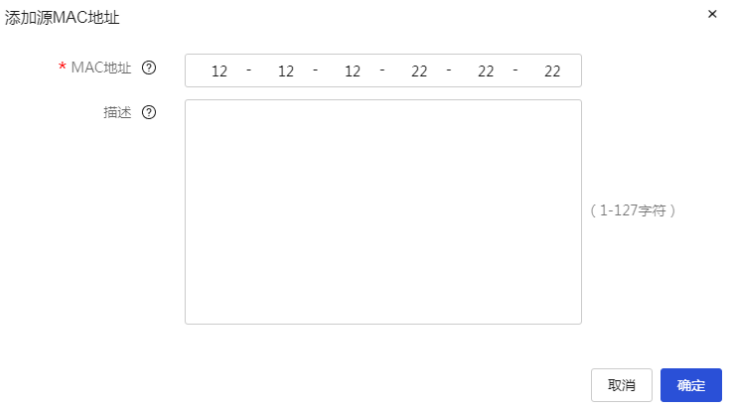
页面向导：[网络安全/MA 地址过滤/MAC 过滤设置/MAC 黑白名单管理/白名单]

本页面为您提供如下主要功能：

- 显示已添加到白名单中的 MAC 地址详细信息
- 添加单个 MAC 地址到白名单
- 批量添加 MAC 地址到白名单
- 从 ARP 表项中添加 MAC 地址到白名单
- 导出当前添加到白名单中的所有 MAC 地址
- 删除已添加到白名单中的 MAC 地址
- 修改已添加到白名单中的 MaC 地址

添加单个MAC地址到白名单：

1. 单击<添加>按钮，弹出添加源 MAC 地址对话框，输入需要添加的 MAC 地址和描述。
2. 单击<确定>按钮，完成操作。



批量添加MAC地址到白名单：

1. 单击<导出>按钮，选择“导出模板”菜单项。
2. 打开下载好的模板，添加待过滤的源 MAC 地址并在本地保存。
3. 单击<导入>按钮，弹出导入源 MAC 地址对话框。
4. 单击<上传文件>按钮，弹出选择要加载的文件对话框，选中已编辑好的模板
5. 单击<确定>按钮，完成对白名单批量添加 MAC 地址的操作。

从ARP表项导入MAC地址：

1. 单击<从 ARP 表项导入>按钮，弹出导入 ARP MAC 表对话框。
2. 勾选需要导入的 MAC 地址后单击<导入>按钮，弹出确认提示对话框。
3. 单击<确定>按钮，完成操作。

导出当前添加到白名单中的所有MAC地址：、

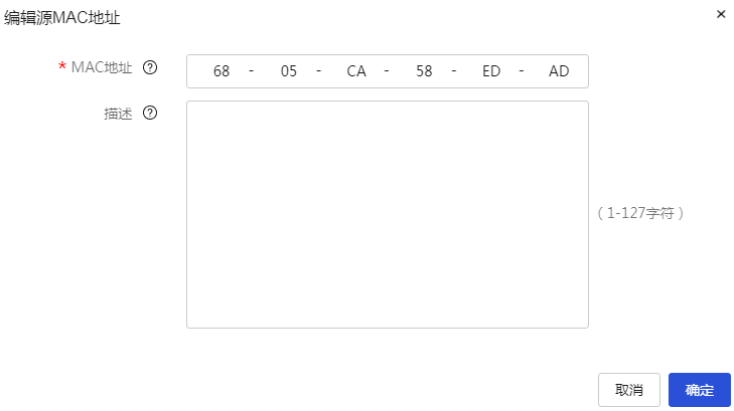
1. 勾选所有表项
2. 单击<导出>按钮，选择“导出选定过滤模式的所有数据”菜单项

删除已添加到白名单中的MAC地址：

1. 单击需要删除的 MAC 地址前方单选框
2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置。

修改已添加到白名单中的MaC地址：

1. 勾选需要修改的 MAC 地址对应操作列的编辑图标，弹出编辑源 MAC 地址对话框，修改相关配置项
2. 单击<确定>按钮，完成配置



3. 参数解释

表11-5 页面参数描述

页面参数	描述
序号	MAC黑白名单管理策略的编号
类别	MAC地址过滤策略的类别，主要分为： • 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
MAC地址	策略需要控制的MAC地址。此处不支持全0或全F的MAC地址
描述	策略的描述信息，可对策略进行简单的描述，方便使用

操作	可对添加的策略进行编辑和删除操作

4. 黑名单

页面向导：[网络安全/MA 地址过滤/MAC 过滤设置/MAC 黑白名单管理/黑名单]

黑名单页面相关功能配置步骤和页面参数和白名单类似，可参考黑名单进行配置，此处不做描述。

11.4 ARP安全

11.4.1 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。

11.4.2 ARP 学习管理

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ARP 安全/ARP 学习管理]

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

3. 参数解释

表11-6 页面参数描述

页面参数	描述
端口	接口，例如WAN1、VLAN1
端口类型	设备的接口类型，主要分为WAN和LAN口

ARP学习管理	动态ARP表项的学习功能，主要分为： • 开启：允许该接口学习动态 ARP 表项 • 关闭：不允许该接口学习动态 ARP 表项 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。当DHCP分配IP地址时会临时生成动态ARP表项，该表项会在动态ARP管理页面中显示，不受接口的ARP学习管理开关控制

11.4.3 动态 ARP 管理

1. 功能简介

本功能包括动态 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。

2. 配置步骤

页面向导：[网络安全/ARP 安全/动态 ARP 管理]

本页面为您提供如下主要功能：

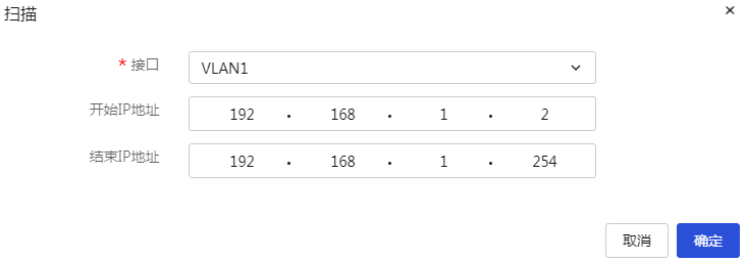
- 显示指定接口的动态 ARP 信息
- 删除指定的动态 ARP
- 扫描指定接口、指定 IP 地址范围内的动态 ARP
- 固化动态 ARP

删除指定的动态ARP：

1. 勾选动态 ARP 列表中的指定选项，单击<删除>按钮，弹出确认提示对话框
2. 单击<确定>按钮，完成配置

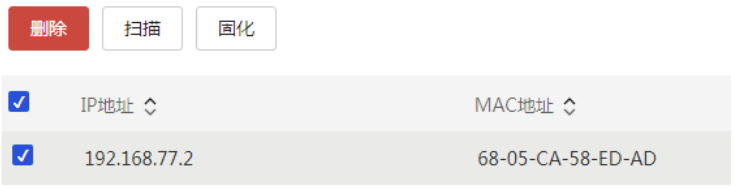
扫描指定接口、指定IP地址范围内的动态ARP：

1. 单击<扫描>按钮，弹出扫描对话框，选择指定接口，输入指定的IP 地址范围
2. 单击<确定>按钮，完成配置



固化指定的动态ARP：

1. 勾选动态 ARP 列表中的指定选项
2. 单击<固化>按钮，完成配置



3. 参数解释

表11-7 页面参数描述

页面参数	描述
IP地址	该动态ARP信息中的IP地址
MAC地址	该动态ARP信息中的MAC地址
类型	该动态ARP信息的所属类型，主要分为： • 未绑定：表示该条表项为动态学习到的 ARP 表项 • 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
VLAN	该动态ARP信息的所属VLAN
接口	该动态ARP信息的所属接口
操作	可对此动态ARP信息进行编辑操作

11.4.4 静态 ARP 管理

1. 功能简介

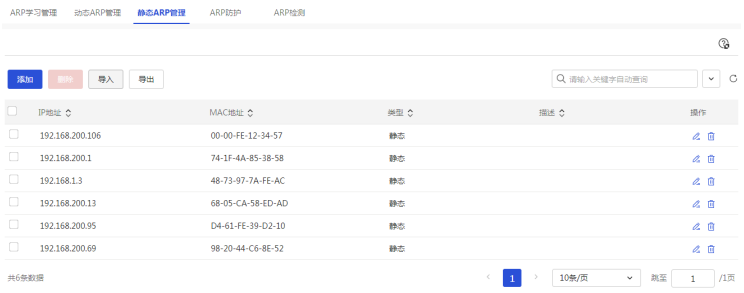
本功能包括静态 ARP 表项管理、刷新、添加和导入导出功能。其中，刷新功能是指刷新静态 ARP 表项列表；添加功能是指手动新增静态 ARP 表项；导入功能是指从文件中批量获取静态 ARP 表项；导出功能是指将现有的静态 ARP 表项导出到本地文件中。

2. 配置步骤

页面向导：[网络安全/ARP 安全/静态 ARP 管理]

本页面为您提供如下主要功能：

- 显示静态 ARP 信息
- 添加静态 ARP 表项
- 删除静态 ARP 表项
- 导入静态 ARP 表项
- 导出静态 ARP 表项
- 修改 ARP 表项

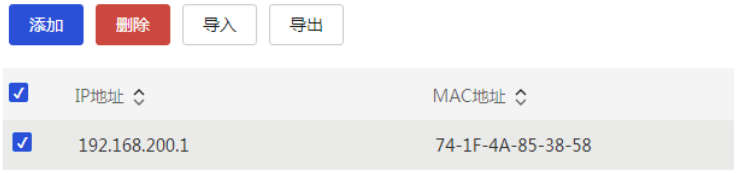


添加静态ARP表项：

1. 单击<添加>按钮，弹出添加 ARP 表项对话框，输入 IP 地址和 MAC 地址
2. 单击<确定>按钮，完成配置

删除静态ARP表项：

1. 勾选需要删除的静态 ARP 表项，单击<删除>按钮，弹出确认提示对话框
2. 单击<确定>按钮，完成配置

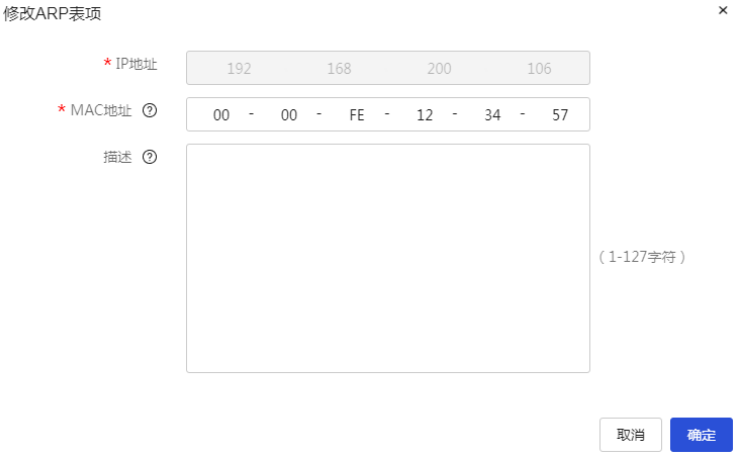


导入静态ARP表项：

1. 单击<导入>按钮，弹出导入 ARP 表项对话框，单击<上传文件>按钮，上传 ARP 表项
2. 单击<确定>按钮，完成配置

修改ARP表项：

1. 单击需要修改的 ARP 表项对应操作列的编辑图标，弹出修改 ARP 表项对话框，输入需要修改的配置项
2. 单击<确定>按钮，完成配置



页面中各参数的含义如下表所示。

表11-8 页面参数描述

关键项	描述
IP地址	该静态ARP信息中的IP地址
MAC地址	该静态ARP信息中的MAC地址。此处不支持全0或全F的MAC地址
类型	该静态ARP信息的所属类型，取值为静态，表示将设备的IP地址与MAC地址进行绑定，形成静态ARP表项
描述	ARP表项的描述信息，可对表项进行简单的描述，方便使用
操作	可对此静态ARP信息进行编辑或者删除操作

11.4.5 ARP 防护

1. 功能简介

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。

2. 注意事项

- 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。

3. 配置步骤

页面向导：[网络安全/ARP 安全/ ARP 防护]

1. 设置 ARP 报文合法性检查和免费 ARP

- 单击<应用>按钮，完配置

4. 参数解释

表11-9 页面参数描述

页面参数	描述
ARP报文合法性检查	通过设置规则验证ARP报文的合法性，主要分为： • 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）：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 • 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：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 • ARP 报文学习抑制：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
免费ARP	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。主要分为： • 检测到 ARP 欺骗时，发送免费 ARP 报文：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 • LAN 内主动发送免费 ARP 报文：并在“发送间隔”配置项处，输入免费 ARP 报文的发送间隔 • WAN 口主动发送免费 ARP 报文：并在“发送间隔”配置项处，输入免费 ARP 报文的发送间隔。当 WAN 口处于固定地址/DHCP 连接模式上网时，主动发送免费 ARP 报文；处于 PPPoE 连接模式上网时，不支持发送免费 ARP 报文

11.4.6 ARP 检测

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ARP 安全/ARP 检测]

1. 选择指定接口，输入指定 IP 地址范围

2. 单击<扫描>按钮，进行 ARP 检测

3. 参数解释

表11-10 页面参数描述

页面参数	描述
扫描接口	设备进行ARP检测的接口
扫描地址范围	进行ARP检测的起始IP地址和结束IP地址 设置完成，需点击“扫描”按钮，进行ARP检测
序号	检测到的ARP表项的编号
IP地址	该ARP信息中的IP地址
MAC地址	该ARP信息中的MAC地址
接口	该ARP信息的所属接口
状态	ARP检测结果状态，主要分为： • 静态表项：该条表项为黑色条目，表示手动配置的或自动绑定的 ARP 表项 • 动态表项：该条表项为蓝色条目，表示动态学习到的并且没有被自动绑定的 ARP 表项 • 错误表项：该条表项为红色条目，表示存在 ARP 冲突表项

11.5 DDOS攻击防御

11.5.1 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。

11.5.2 攻击防御

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ DDOS 攻击防御/攻击防御]

本页面提供如下主要功能：

- 显示已添加的 DDOS 攻击防御策略
- 开启或关闭 DDOS 攻击防御
- 添加 DDOS 攻击防御策略
- 删除 DDOS 攻击防御策略
- 编辑已添加的 DDOS 攻击防御策略

添加DDOS攻击防御策略：

1. 单击<添加>按钮，弹出新建攻击防御对话框，选择应用接口和攻击防御类型
2. 单击<确定>按钮，完成配置

删除DDOS攻击防御策略：

1. 勾选需要删除的攻击防御策略后单击<删除>按钮，弹出确认提示对话框
2. 单击<确定>按钮，完成配置

编辑已添加的DDOS攻击防御策略：

1. 单需要编辑的攻击防御对应操作列的编辑图标，弹出编辑攻击防御对话框，修改相关配置
2. 单击<确定>按钮，完成配置

3. 参数解释

表11-11 页面参数描述

页面参数	描述
DDoS攻击防御	是否开启该功能，若开启该功能，设备将对来自外网和内网的常见DDoS攻击进行防御，丢弃攻击报文，并以日志形式记录相应的攻击事件
应用接口	攻击报文的来源接口，即规则对从某一接口收到的数据包进行DDoS攻击防御

攻击防御	设备进行DDoS攻击防御的类型，主要分为：
	• 单包攻击防御：防御攻击者利用畸形报文发起攻击，导致瘫痪目标系统。主要包括：
	  ○ 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 地址
	  ○ 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
	• 异常流攻击防御：防御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。主要包括： ○ SYN Flood 攻击防御：勾选该选项，并设置启用防止 SYN Flood 攻击的阈值。当流量速率超过该阈值，设备将启用 SYN Flood 攻击防御。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：勾选该选项，并设置启用防止 UDP Flood 攻击的阈值。当流量速率超过该阈值，设备将启用 UDP Flood 攻击防御。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：勾选该选项，并设置启用防止 ICMP Flood 攻击的阈值。当流量速率超过该阈值，设备将启用 ICMP Flood 攻击防御。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 • 扫描攻击防御：防御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。主要包括： ○ 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

11.5.3 攻击防御统计

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ DDOS 攻击防御/攻击防御统计]

查看“单包攻击防御”和“异常攻击防御”的详细信息，并支持将这些信息以Excel形式导出。

3. 参数解释

表11-12 页面参数描述

页面参数	描述
序号	设备遭受攻击的编号
攻击类型	设备遭受攻击的类型。包括单包攻击防御和异常流量攻击防御中的具体攻击类型
总次数	设备遭受此类攻击的总次数。查看单包攻击防御统计时，显示该参数
最后发生时间	设备最后遭受此类攻击的具体时间
被攻击接口/被攻击安全域	设备被攻击的接口或安全区域
发生的用户IP	发动攻击的用户IP地址
详情	该攻击的详细信息，包括：序号、攻击类型、源地址、目的地址、防御动作、日期和时间

11.5.4 报文源认证

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ DDOS 攻击防御/报文源认证]

1. 选择报文源认证方式
2. 单击<应用>按钮，完成配置

3. 参数解释

表11-13 页面参数描述

页面参数	描述
报文源认证	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。主要分为： • 启用基于静态路由的报文源认证功能：应用该项后，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，其它内网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：应用该项后，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：应用该项后，设备将会对内网数据包的源 IP/MAC 进行智能认证，确认对端是否为合法主机，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

11.5.5 异常流量防护

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/ DDOS 攻击防御/异常流量防护]

配置异常流量防护。	

3. 参数解释

表11-14 页面参数描述

页面参数	描述
异常流量防护	对内网主机发来的异常大流量进行控制，以防止其过度占用设备带宽，消耗设备处理性能。防护等级主要分为： • 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
异常流量阈值	异常流量的最大值，超过设定的阈值，设备将会对此异常流量做出控制

11.6 IPv6邻居列表

1. 功能简介

IPv6 邻居列表是 IPv6 网络中的一个重要概念，它用于跟踪和管理 IPv6 网络中邻居设备的信息。每个 IPv6 设备都会维护一个邻居列表，其中包含了与本设备直接相连的其他 IPv6 设备的信息，如 MAC 地址、邻居状态、以及可达性状态等。邻居列表在 IPv6 网络中扮演着重要的角色，它可以帮助设备进行数据包转发、地址解析和邻居发现等功能，同时也有助于网络管理和故障排查。

邻居表项保存的是设备在链路范围内的邻居信息，除了通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建邻居表项外，还可以通过手工配置来静态创建邻居表项。

2. 配置步骤

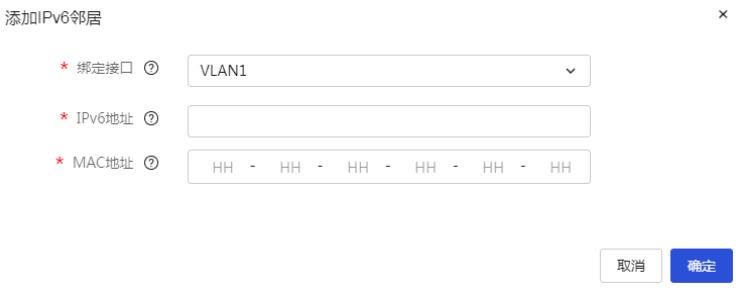
页面向导：[网络安全/IPv6 邻居列表]

本页面提供如下主要功能：

- 显示已创建的 IPv6 邻居表项
- 添加静态 IPv6 邻居
- 编辑 IPv6 邻居表项
- 删除 IPv6 邻居表项

添加静态IPv6邻居：

1. 单击<添加>按钮，弹出添加 IPv6 邻居对话框，选择绑定接口、输入 IPv6 地址和 MAC 地址
2. 单击<确定>按钮，完成添加



3. 参数解释

表11-15 页面参数描述

关键项	描述
绑定接口	本节点的三层接口，请选择VLAN划分里设置过的VLAN
IPv6地址	本节点的三层接口相连的邻居节点的IPv6地址
MAC地址	本节点的三层接口相连的邻居节点的MAC地址
绑定开关	对于动态生成的IPv6邻居表项，开启绑定开关后可将其转化为静态IPv6邻居表项

11.7 黑名单管理

1. 功能简介

黑名单管理功能用于查看和解除已添加的黑名单用户。

2. 配置步骤

页面向导：[网络安全/黑名单管理]

查看加入到黑名单用户信息，并支持将其从黑名单中解除。

3. 参数解释

表11-16 页面参数描述

关键项	描述
黑名单用户	黑名单用户的IP地址
MAC地址	黑名单用户的MAC地址
类型	黑名单用户的类型，主要分为： 静态黑名单：在设备Web导航栏“系统监控 > 流量排行”页面中终端对应操作列的拉黑按钮手工拉黑的用户，类型为“静态黑名单” 动态黑名单：在设备Web导航栏“网络安全 > DDOS攻击防御”页面中启用异常主机流量防护功能，并设置“防护等级”为“高”，当设备接收到的异常流量超过设定的阈值时就会将异常的主机添加到黑名单管理，类型为“动态黑名单”
动作	对此黑名单用户的处理操作，若此黑名单用户为正常访问用户，可将此黑名单解除

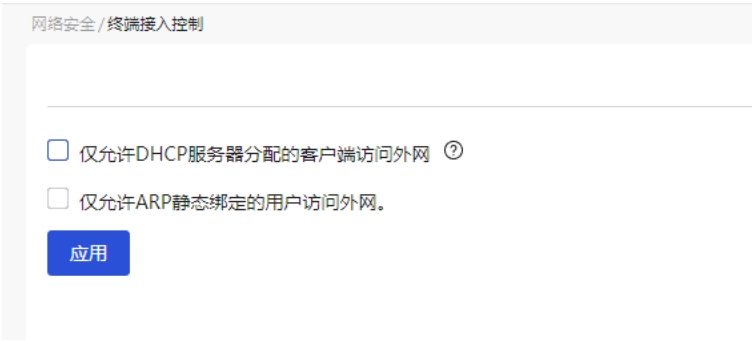
11.8 终端接入控制

1. 功能简介

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。

2. 配置步骤

页面向导：[网络安全/终端接入控制]

配置终端接入控制	

3. 参数解释

表11-17 页面参数描述

关键项	描述
仅允许DHCP服务器分配的客户端访问外网	若开启此功能，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 设置完成，需单击<应用>按钮，使配置生效
仅允许ARP静态绑定的用户访问外网	若开启此功能，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 设置完成，需单击<应用>按钮，使配置生效
IP地址	策略控制的IP地址
MAC地址	策略控制的MAC地址
终端类型	用户接入网络的控制方式，主要分为： • DHCP 动态分配：表示允许 DHCP 服务器动态分配的客户端访问外网 • DHCP 静态分配：表示允许 DHCP 服务器静态分配的客户端访问外网 • ARP 静态绑定：表示允许 ARP 静态绑定规则表中的客户端访问外网

12 认证管理

12.1 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。

12.1.1 云认证

1. 注意事项

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

页面向导：[控制认证管理/Portal 认证]

开启接口的云认证功能

3. 参数解释

表12-1 页面参数描述

页面参数	描述
接口名称	设备的VLAN接口
IP地址	VLAN接口的IP地址
子网掩码	该IP地址的子网掩码
云认证功能	是否开启云认证功能，若开启该功能，本设备的Portal认证方式为云端认证方式，将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

12.1.2 免认证 MAC 地址

页面向导：认证管理→Portal 认证→免认证 MAC 地址

本页面为您提供如下主要功能：

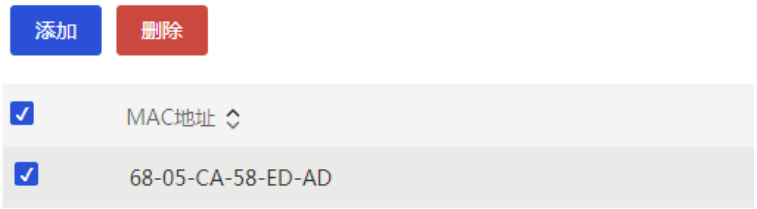
- 显示已添加的免认证 MAC 地址
- 添加免认证 MAC 地址
- 删除免认证 MAC 地址
- 编辑已添加的 MAC 地址

添加免认证MAC地址：

1. 单击<添加>按钮，弹出添加免认证 MAC 地址对话框，输入 MAC 地址
2. 单击<确定>按钮，完成配置

删除免认证MAC地址：

1. 勾选需要删除的免认证 MAC 地址，单击<删除>按钮，弹出确认提示按钮
2. 单击<确定>按钮，完成配置



编辑已添加的MAC地址:

1. 单击需要编辑的免认证 MAC 地址对应操作列的编辑图标，弹出修改免认证 MAC 地址对话框
2. 单击<确定>按钮，完成配置

页面中各参数的含义如下表所示。

表12-2 页面参数描述

页面参数	描述
MAC地址	规则需要控制的MAC地址，即该MAC地址不需要通过Portal认证即可访问网络资源。此处不支持全0或全F的MAC地址
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑或者删除操作

12.1.3 配置免认证 IP 地址

注意

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。

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。

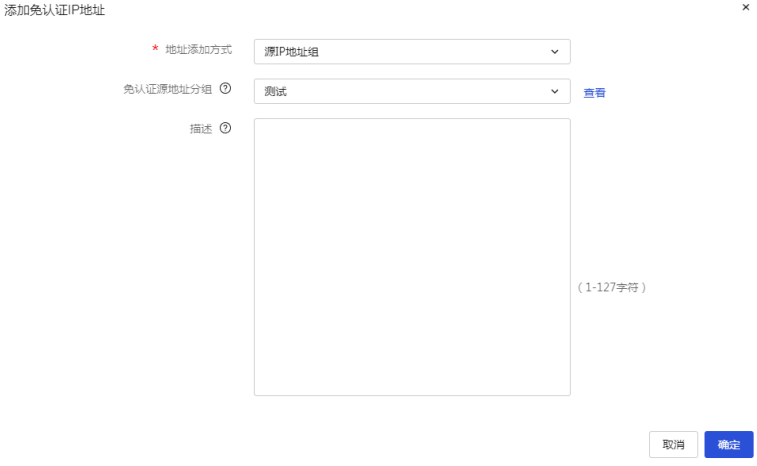
页面向导：认证管理→Portal 认证→免认证 IP 地址

本页面为您提供如下主要功能：

- 显示已添加的免认证 IP 地址
- 添加免认证 IP 地址
- 删除免认证 IP 地址
- 编辑已添加的 IP 地址

添加免认证IP地址：

1. 单击<添加>按钮，配置相关参数
2. 单击<确定>按钮，完成配置

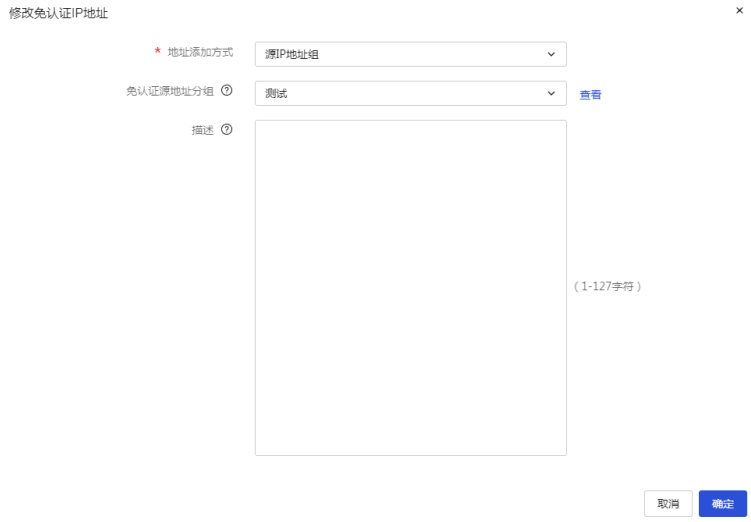


删除免认证IP地址：

1. 勾选需要删除的免认证 IP 地址，单击<删除>按钮，弹出确认提示按钮
2. 单击<确定>按钮，完成配置

编辑已添加的IP地址:

1. 单击需要编辑的免认证 IP 地址对应操作列的编辑图标，弹出修改免认证 IP 地址对话框
2. 单击<确定>按钮，完成配置



页面中各参数的含义如下表所示。

表12-3 页面参数描述

页面参数	描述
地址添加方式	免认证IP地址的添加方式。主要分为： • 源 IP 地址组：规则需要控制的源 IP 地址范围。配置该参数时，需在“免认证源地址分组”配置项处，选择已创建的地址分组。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 • 目的 IP 地址组：规则需要控制的目的 IP 地址范围。配置该参数时，需在“免认证目的地址分组”配置项处，选择已创建的地址分组。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 • 域名：规则需要控制的域名。配置该参数时，需要在“域名”配置项处，输入免认证的域名
免认证IP地址组	规则需要控制的IP地址组
地址类型	免认证IP地址的添加方式。包括源IP地址组、目的IP地址组、域名三种
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑或者删除操作

13 虚拟专网(VPN)

13.1 IPsec VPN

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：

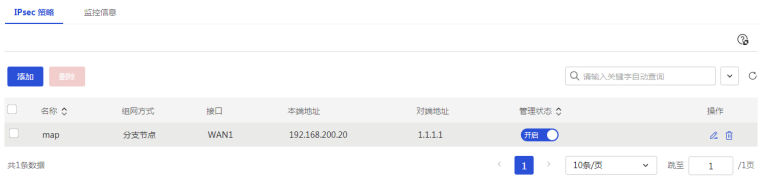
- “中心—分支”方式组网：企业分支机构网关将主动与总部网关建立 IPsec 隧道，分支机构内部终端可以安全访问总部的网络资源。
- “分支—分支”方式组网：企业各分支网关之间均可主动建立 IPsec 隧道，来保护分支之间的数据通信。

13.1.1 添加 IPsec 策略

页面向导：虚拟专网（VPN）→IPsec VPN→IPsec 策略

本页面为您提供如下主要功能：

- 显示已添加的 IPsec 策略信息
- 添加 IPsec 策略（包括 IPsec 基本配置、IKE 配置和 IPsec 配置）
- 删除 IPsec 策略
- 编辑已添加的 IPsec 策略

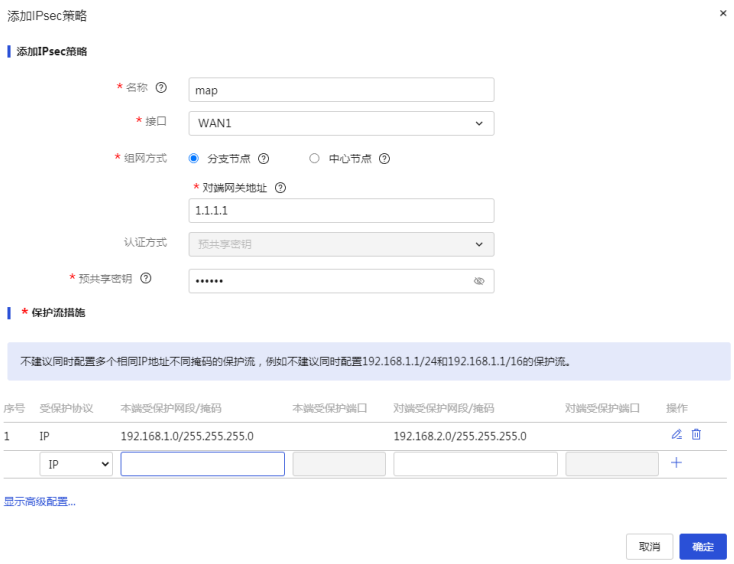


1. 添加 IPsec 策略（IPsec 基本配置）

注意

- 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。
- 在添加保护流措施时，不建议同时配置多个相同 IP 地址不同掩码的保护流，例如不建议同时配置 192.168.1.1/24 和 192.168.1.1/16 的保护流。

1. 单击<添加>按钮，弹出添加IPsec 策略对话框，配置相关参数
2. 单击<显示高级配置>按钮，完成配置，并进入 IKE 配置页面。



页面中各参数的含义如下表所示。

表13-1 页面参数描述

页面参数	描述
接口	报文的来源接口，即规则对从某一接口收到的数据包进行控制。配置该参数时，此接口需要与对端设备路由可达
组网方式	IPsec VPN网络的组建方式，主要分为： • 分支节点：设备作为分支节点，与中心节点建立 IPsec 隧道。配置该参数时，需设置 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 • 中心节点：设备作为中心节点，与分支节点建立 IPsec 隧道
认证方式	IPsec隧道的认证方式。此参数目前仅支持预共享密钥
预共享密钥	IPsec隧道的认证密码。配置该参数时，需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
序号	受保护流量的编号
受保护协议	受IPsec隧道保护的报文的协议类型。主要分为： • 若需控制某网络层协议的报文，则选择“IP”、“IGMP”、“GRE”“IPINIP”或者“OSPF” • 若需控制某传输层协议的报文，则选择“TCP”或“UDP” • 若需控制 Ping、Tracert 等 ICMP 协议报文，则选择“ICMP”
本端受保护网段/掩码	本端受保护网段。例如1.1.1.1/24
本端受保护端口	本端受保护端口。当受保护协议选择为TCP或UDP时。需配置此参数
对端受保护网段/掩码	对端节点受保护网段。例如2.2.2.2/24
对端受保护端口	对端节点受保护端口。当受保护协议选择为TCP或UDP时。需配置此参数

2. 添加 IPsec 策略（IKE 配置）

1. 配置 IKE 相关参数
2. 单击 IPsec 页签，进入 IPSec 配置页面

页面中各参数的含义如下表所示。

表13-2 页面参数描述

页面参数	描述
IKE版本	Internet密钥交换协议的版本，主要分为： • 若对端节点使用的 IKE 版本为 V1，则本端选择“V1” • 若对端节点使用的 IKE 版本为 V2，则本端选择“V2”
协商模式：	对等体的协商模式。主要分为： • 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，建议选择IKE协商模式为野蛮模式
本端身份类型	IKE认证的本端设备身份类型和身份标识。主要分为： • 若对端节点 IKE 身份类型为 IP 地址，则本端选择“IP 地址”，IKE 协商模式若设置为主模式，需要将本端设备身份类型配置为 IP 地址。缺省使用设备出接口 IP 地址 • 若对端节点 IKE 身份类型为 FQDN，则本端选择“FQDN”，即为标识本端身份的 FQDN 名称 • 若对端节点 IKE 身份类型为 User-FQDN，则本端选择“User-FQDN”，即为标识本端身份的 User FQDN 名称

对端身份类型	IKE认证的对端设备身份类型和身份标识。主要分为： • 若对端节点 IKE 身份类型为 IP 地址，则本端选择“IP 地址”，IKE 协商模式若设置为主模式，需要将本端设备身份类型配置为 IP 地址。一般使用设备出接口 IP 地址 • 若对端节点 IKE 身份类型为 FQDN，则本端选择“FQDN”，即为标识本端身份的 FQDN 名称 • 若对端节点 IKE 身份类型为 User-FQDN，则本端选择“User-FQDN”，即为标识本端身份的 User FQDN 名称
对等体存活检测（DPD）	是否开启对等体存活检测（DPD）功能，若开启该功能，设备将检测隧道对端是否存活，拆除对端失活的IPsec隧道。配置该参数时，需配置： • 探测时间：每隔一个探测时间，设备将进行一次存活检测。取值为 1~60，单位为秒 • 超时时间：超过该时间阈值，设备检测不到对端，则认定对端失活。取值为 2~300，单位为秒

算法组合(IKE)	IKE协议交互所需的加密和认证算法，设置方式有两种：
	• 推荐：设备推荐的算法组合。-IPsec 隧道的两端所配置的推荐算法组合需保持一致
	• 自定义：用户自定义的 IKE 的算法，选项包括：
	  ○ 认证算法：IKE 的认证算法。IPsec 隧道的两端所配置的认证算法需保持一致
	  ○ 加密方式：IKE 的加密算法。IPsec 隧道的两端所配置的加密算法需保持一致
	  ○ PFS：指一个密钥被破解，并不影响其他密钥的安全特性。IPsec 隧道的两端所配置的 PFS 算法需保持一致

SA生存时间	IKE重新协商的时间间隔，即超过该时间间隔将触发IKE相关参数的重新协商。建议SA生存时间设置不低于600秒

3. 添加 IPsec 策略（IPsec 配置）

配置IPsec相关参数。

页面中各参数的含义如下表所示。

表13-3 页面参数描述

页面参数	描述
算法组合（IPSEC配置）	IPsec隧道的加密和认证算法，设置方式有两种： • 推荐：设备推荐的算法组合。-IPsec 隧道的两端所配置的推荐算法组合需保持一致 • 自定义：用户自定义的 IKE 的算法，主要分为： ○ 安全协议：对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。IPsec 隧道的两端所配置的安全协议需保持一致 ○ ESP 认证算法：ESP 的认证算法。IPsec 隧道的两端所配置的 ESP 认证算法需保持一致 ○ ESP 加密算法：ESP 的加密算法。IPsec 隧道的两端所配置的 ESP 加密算法需保持一致
封装模式	IPsec隧道的封装模式，主要分为： • 传输模式：适用于主机与主机之间建立隧道 • 隧道模式：适用于网关和网关之间 建立隧道 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
PFS	IPsec隧道的PFS算法。如果本端配置了PFS特性，则发起协商的对端也必须配置PFS特性，而且本端和对端指定的DH组必须一致，否则协商会失败
基于时间的SA生存时间	触发IPsec重新协商的时间间隔，即超过所配时间将触发IPsec相关参数的重新协商
基于流量的生存时间	触发IPsec重新协商的流量大小，即超过所配流量将触发IPsec相关参数的重新协商
触发模式	触发IPsec重新协商的模式，主要分为： • 流量触发：IKE 隧道配置下发后，不会自动建立隧道，会等待兴趣流来触发隧道建立。 • 自协商模式：IKE 隧道配置下发后或隧道异常断开后，会自动触发隧道建立，并且保证隧道长时间建立，不需等待兴趣流触发
管理状态	IPsec策略的使用状态，主要分为： • 开启：启用此策略 • 关闭：禁用此策略
操作	可对该策略进行编辑和删除操作

13.1.2 监控信息

页面向导：虚拟专网（VPN）→IPsec VPN→监控信息

显示已添加的IPsec策略信息。

页面中各参数的含义如下表所示。

表13-4 页面参数描述

页面参数	描述
策略名称	已建立的IPSEC隧道策略的名称
状态	已建立的IPsec VPN隧道的状态。仅显示建立成功的IPsec VPN隧道，状态为UP
接口	报文的来源接口，即规则对从某一接口收到的数据包进行控制
本端地址	本端设备出口地址
对端地址	对端设备出口地址
安全提议	IPsec VPN使用的算法信息
操作	可对该隧道信息进行删除操作

13.2 L2TP服务器端

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。

13.2.1 L2TP 配置

页面向导：虚拟专网（VPN）→L2TP 服务器端→L2TP 配置

本页面为您提供如下主要功能：

- 启用和关闭 L2TP 服务器端
- 添加 L2TP 组
- 删除 L2TP 组
- 编辑已添加的 L2TP 组

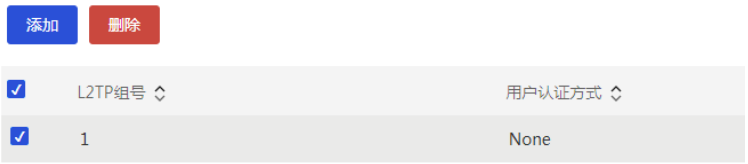
勾选“启用L2TP服务器端”前方单选框，单击<确定>按钮，开启L2TP服务器端

添加L2TP组：

1. 单击<添加>按钮，弹出新建L2TP 组页面，配置相关参数
2. 单击<确定>按钮，完成配置

删除L2TP组：

1. 勾选需要删除的 L2TP 组前方单选框，弹出确认提示对话框
2. 单击<确定>按钮，完成配置



编辑已添加的L2TP组：

1. 单击需要编辑的 L2TP 组对应操作列的编辑图标，弹出修改L2TP 组对话框，修改相关参数。
2. 单击<确定>按钮，完成配置

页面中各参数的含义如下表所示。

表13-5 页面参数描述

页面参数	描述
启用L2TP服务器端	是否开启L2TP服务器端功能。若开启该功能，设备将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。缺省关闭L2TP服务器端功能

对端隧道名称	L2TP客户端的隧道名称。可根据需要进行选择是否勾该配置项，配置该参数时，则在配置项处输入L2TP客户端的隧道名称。取值为1~31个字符，不支持输入#、英文分号和空格
本端隧道名称	L2TP服务器端的隧道名称。取值为1~31个字符，仅支持英文字母[a-z,A-Z]、数字和下划线
隧道验证	是否开启L2TP隧道验证功能，若开启该功能，则需输入隧道验证密码。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。隧道验证密码不支持输入#、英文问号、英文分号和空格
PPP认证方式	L2TP用户的认证方式，主要分为： • None：对用户免认证。该方式，安全性最低，请谨慎使用 • PAP：采用两次握手机制对用户进行认证。该方式，安全性中 • CHAP：采用三次握手机制对用户进行认证。该方式，安全性最高 • MSCHAP：采用了对称加密来增强安全性 • MSCHAPv2：MS-CHAP 的改进版本，采用了更强的哈希算法并加强了加密过程
用户名	认证使用的用户名。取值为1~55个字符，不能包含英文问号（?）。当“PPP认证方式”选择PAP、CHAP、MSCHAP或MSCHAPv2时，需设置该参数
密码	认证使用的用户名对应的密码。取值为1~63个字符。当“PPP认证方式”选择PAP、CHAP、MSCHAP或MSCHAPv2时，需设置该参数
虚拟模板接口地址	虚拟模板接口的IP地址，即L2TP服务器端可为L2TP客户端或用户分配IP地址
子网掩码	虚拟模板接口IP地址的子网掩码，例如255.255.255.0
DNS1和DNS2	分配给L2TP客户端或用户的主备DNS。DNS1与DNS2不能相同
用户地址池	给L2TP客户端分配地址所用的地址池。用户地址池中不能包含已配置的虚拟模板接口地址
Hello报文间隔	L2TP服务端和客户端之间发送Hello报文的时间间隔，Hello报文用于检测LAC和LNS之间隧道的连通性，单位为秒

13.2.2 隧道信息

页面向导：虚拟专网（VPN）→L2TP 服务器端→隧道信息

显示L2TP隧道信息	

页面中各参数的含义如下表所示。

表13-6 页面参数描述

页面参数	描述
账号名	L2TP客户端的用户名
本端隧道编号	本端已建立隧道的ID号
对端隧道编号	对端已建立隧道的ID号

对端隧道端口	L2TP客户端和服务端建立连接使用的服务端口
对端隧道IP地址	L2TP客户端的IP地址
会话数目	L2TP服务端和客户端之间建立会话的数目
对端隧道名称	L2TP客户端的隧道名称
操作	可对该隧道信息做删除操作

13.2.3 L2TP 用户

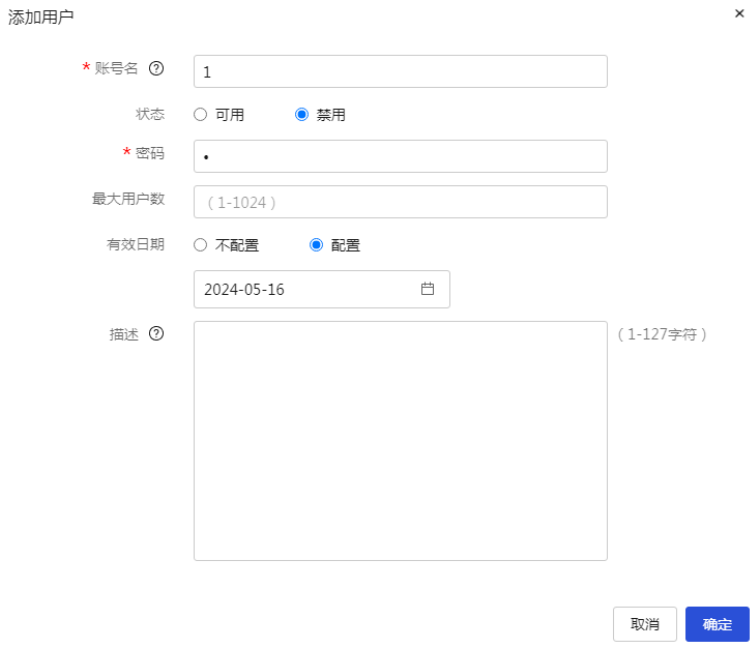
页面向导：虚拟专网（VPN）→L2TP 服务器端→L2TP 用户

本页面为您提供如下主要功能：

- 显示已添加的 L2TP 用户信息
- 单个添加 L2TP 用户
- 批量导入 L2TP 用户
- 删除 L2TP 用户
- 导出 L2TP 用户

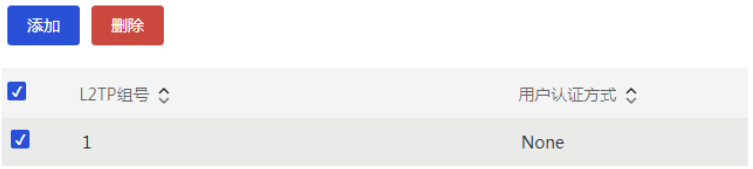
单个添加L2TP用户：

1. 单击<添加>按钮，弹出添加用户对话框，输入相关配置项
2. 单击<确定>按钮，完成操作



批量导入L2TP用户：

1. 单击<导入>按钮，弹出 L2TP 用户列表对话框
2. 点击<上传文件>按钮，弹出选择要加载的文件对话框，选中已编辑好的模板
3. 单击<确定>按钮，完成配置

导出当前L2TP用户（单击<导出>按钮，系统会自动导出当前L2TP用户列表。）	
删除L2TP用户组： 1. 勾选需要删除的 L2TP 用户前方单选框 2. 单击<删除>按钮，弹出确认提示对话框，单击<确定>按钮，完成配置	

页面中各参数的含义如下表所示。

表13-7 页面参数描述

页面参数	描述
账号名	L2TP客户端的用户名。取值为1~55个字符，仅支持英文字母[a-z,A-Z]、数字和下划线
状态	L2TP客户端的状态。主要分为： • 可用：允许 L2TP 客户端使用该用户建立会话 • 禁用：禁止 L2TP 客户端使用该用户建立会话
密码	L2TP客户端的账号密码
最大用户数	最多允许多少个L2TP客户端连入企业内部网络
有效日期	L2TP客户端权限的到期日期。主要分为： • 配置：需在日期选择框中选择用户权限的到期日期 • 不配置：用户权限一直有效
当前连接数量	L2TP客户端的在线数量
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

13.3 L2TP客户端

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。

13.3.1 L2TP 配置

页面向导：虚拟专网（VPN）→L2TP 客户端→L2TP 配置

本页面为您提供如下主要功能：

- 启用和关闭 L2TP 客户端
- 添加 L2TP 组
- 删除 L2TP 组
- 编辑已添加的 L2TP 组

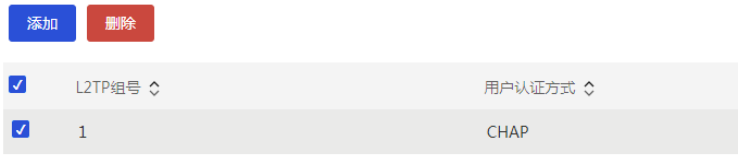
勾选“启用L2TP客户端”前方单选框，单击<确定>按钮，开启L2TP客户端

添加L2TP组：

1. 单击<添加>按钮，弹出新建 L2TP 组页面，配置相关参数
2. 单击<确定>按钮，完成配置

删除L2TP组：

1. 勾选需要删除的 L2TP 组前方单选框，弹出确认提示对话框
2. 单击<确定>按钮，完成配置



编辑已添加的L2TP组：

1. 单击需要编辑的 L2TP 组对应操作列的编辑图标，弹出修改 L2TP 组对话框，修改相关参数。
2. 单击<确定>按钮，完成配置

页面中各参数的含义如下表所示。

表13-8 页面参数描述

页面参数	描述
L2TP组号	L2TP客户端规则的编号
L2TP客户端	是否开启L2TP客户端功能。若开启该功能，设备将作为L2TP客户端访问企业内部网络资源
本端隧道名称	L2TP客户端的隧道名称。取值为1~31个字符，仅支持英文字母[a-z,A-Z]、数字和下划线
地址获取方式	L2TP隧道建立成功后PPP接口的IP地址获取方式， 主要分为： • 静态：L2TP 客户端手工设置一个 IP（由 L2TP 服务端管理员分配） • 动态：由 L2TP 服务端为虚拟 PPP 接口动态分配 IP 地址。缺省为动态获取
隧道验证	是否开启L2TP隧道验证功能。若开启该功能，则需输入隧道验证密码，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。隧道验证密码不支持输入#、英文问号、英文分号和空格
PPP认证方式	L2TP用户的认证方式，主要分为： • None：对用户免认证。该方式，安全性最低，请谨慎使用 • PAP：采用两次握手机制对用户进行认证。该方式，安全性中 • CHAP：采用三次握手机制对用户进行认证。该方式，安全性最高 • MSCHAP：采用了对称加密来增强安全性 • MSCHAPv2：MS-CHAP 的改进版本，采用了更强的哈希算法并加强了加密过程
用户名	认证使用的用户名。取值为1~55个字符，不能包含英文问号（?）。当“PPP认证方式”选择PAP、CHAP、MSCHAP或MSCHAPv2时，需设置该参数
密码	认证使用的用户名对应的密码。取值为1~63个字符。当“PPP认证方式”选择PAP、CHAP、MSCHAP或MSCHAPv2时，需设置该参数
NAT地址转换	地址转换功能，配置该参数时，可根据实际需求选择是否启用该功能 • 若启用该功能，则 L2TP 服务器端不需配置到达客户端的路由

	• 若未启用该功能，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
L2TP服务器端地址	L2TP服务端的IP地址或域名
Hello报文间隔	L2TP服务端和客户端之间发送Hello报文的时间间隔，hello报文用于检测LAC和LNS之间隧道的连通性，单位为秒
操作	可对该隧道信息做编辑和删除操作

13.3.2 隧道信息

页面向导：虚拟专网（VPN）→L2TP 客户端→L2TP 配置

显示L2TP隧道信息	

页面中各参数的含义如下表所示。

表13-9 页面参数描述

页面参数	描述
账号名	L2TP客户端的用户名
本端隧道编号	本端已建立隧道的ID号
对端隧道编号	对端已建立隧道的ID号
对端隧道端口	L2TP客户端和服务端建立连接使用的服务端口
本端地址	L2TP客户端的IP地址
对端隧道IP地址	L2TP服务端的IP地址
对端隧道名称	L2TP服务端的隧道名称
会话数目	L2TP服务端和客户端之间建立会话的数目
上行流速（Mbps）	L2TP客户端访问企业内部网络的上行流量速率
下行流速（Mbps）	L2TP客户端访问企业内部网络的下行流量速率
操作	可对该隧道信息做删除操作

13.4 蒲公英

13.4.1 简介

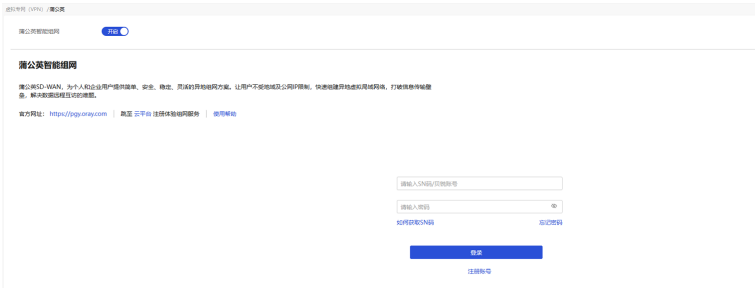
蒲公英 SD-WAN，为个人和企业用户提供简单、安全、稳定、灵活的异地组网方案。让用户不受地域及公网 IP 限制，快速组建异地虚拟局域网络，打破信息传输壁垒，解决数据远程互访的难题。

13.4.2 蒲公英智能组网

页面向导：虚拟专网（VPN）→蒲公英

本页面为您提供如下主要功能：

- 开启/关闭蒲公英智能组网
- 输入贝锐账号或 SN 码、密码后单击<登录>按钮，快速组建异地虚拟局域网络



- 登录成功后，单击<查看网络>按钮，可跳转至蒲公英管理平台查看组网详情
- 单击<退出登录>按钮，设备将自动退出蒲公英智能组网

页面中各参数的含义如下表所示。

表13-10 页面参数描述

页面参数	描述
蒲公英智能组网	是否开启蒲公英智能组网功能。若开启该功能，可通过登录贝锐账号或SN码，快速组建异地虚拟局域网络
注册账号	跳转至贝锐账号注册界面，根据实际情况选择账号类型，进行注册
登录	• 使用贝锐账号登录：登录后会自动生成一个 SN 码，实现设备组网 • 使用 SN 码登录：在蒲公英管理平台完成创建 SN 码和组网后，使用创建的 SN 码登录，实现设备组网。注意：若使用相同的 SN 码在不同的设备上登录，会导致先前的设备退出组网
查看网络	跳转至蒲公英管理平台，查看组网详情。
退出登录	退出登录后，设备将自动退出蒲公英智能组网。

14 高级选项

14.1 静态路由

1. 功能简介

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。

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。

3. 配置步骤

页面向导：[高级选项/静态路由]

本页面为您提供如下主要功能：

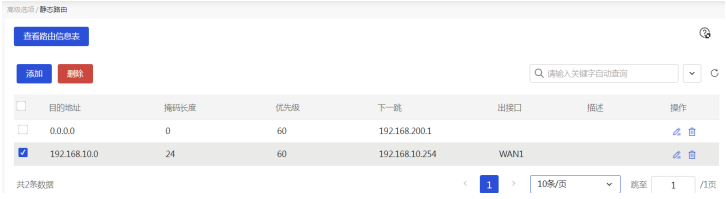
- 显示已添加的静态路由详细信息
- 添加静态路由
- 删除已添加的静态路由
- 修改已添加的静态路由
- 查看路由信息表

添加静态路由：

1. 单击<添加>按钮，弹出添加 IPv4 静态路由对话框，输入目的 IP 地址、掩码长度和下一跳等信息
2. 单击<确定>按钮，完成配置

删除静态路由：

1. 勾选需要删除的静态路由条目
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

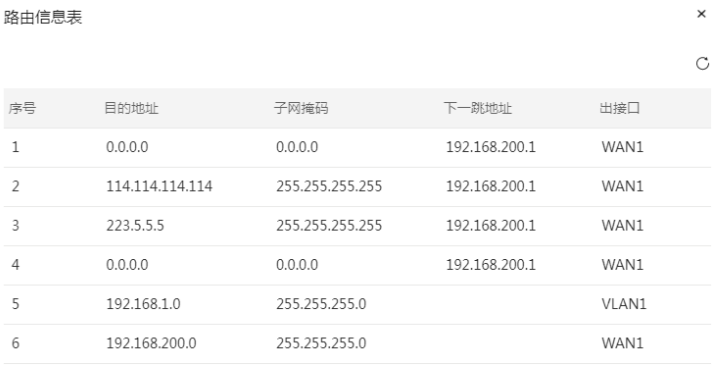


修改静态路由：

1. 单击需要修改的静态路由操作列的编辑图标，弹出修改 IPv4 静态路由对话框，修改相关参数
2. 单击<确定>按钮，完成配置

查看路由信息表：

单击<查看路由信息表>按钮，可查看路由信息表



序号	目的地址	子网掩码	下一跳地址	出接口
1	0.0.0.0	0.0.0.0	192.168.200.1	WAN1
2	114.114.114.114	255.255.255.255	192.168.200.1	WAN1
3	223.5.5.5	255.255.255.255	192.168.200.1	WAN1
4	0.0.0.0	0.0.0.0	192.168.200.1	WAN1
5	192.168.1.0	255.255.255.0		VLAN1
6	192.168.200.0	255.255.255.0		WAN1

4. 参数解释

表14-1 页面参数描述

页面参数	描述
目的IP地址	设备要访问的目的网络的IP地址
掩码长度	目的网络的掩码长度，例如24
下一跳	数据在到达目的地址前，需要经过的下一个路由器的IP地址。配置该参数时，可根据需要选择是否勾选“出接口”选项 • 若确定数据经过的设备出口，则勾选“出接口”选项，并设置下一跳 IP 地址，下一跳地址必须和所选接口在相同网段 • 若不确定出接口时，则不勾选“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
优先级	静态路由的优先级，配置该参数时，数值越小则优先级越高
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

14.2 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、本地域名服务和终端自动访问 Web 服务。

“域名”、“本地域名地址”、“服务器地址”和“终端自动访问地址”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；“终端自动访问地址”长度为 1-127 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”、“本地域名地址”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。
- “终端自动访问地址”不支持中文字符和空格。

14.2.1 配置静态 DNS

1. 功能简介

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

页面向导：[高级选项/应用服务/静态 DNS]

本页面为您提供如下主要功能：

- 显示已添加的静态 DNS 详细信息
- 添加静态 DNS
- 删除已添加的静态 DNS
- 修改已添加的静态 DNS

添加静态 DNS：

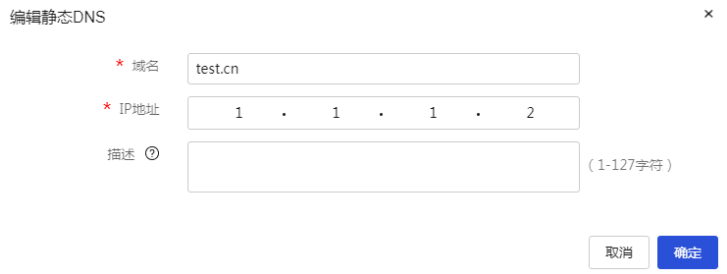
1. 单击<添加>按钮，弹出新建静态 DNS 对话框，输入网络设备的域名和 IP 地址
2. 单击<确定>按钮，完成配置

删除静态DNS：

1. 勾选需要删除的静态 DNS
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改静态 DNS：

1. 单击需要修改的静态 DNS 操作列的编辑图标，弹出修改静态 DNS 对话框，修改相关参数
2. 单击<确定>按钮，完成配置



3. 参数解释

表14-2 页面参数描述

页面参数	描述
域名	为设备分配的域名。配置该参数时，该域名需与设备IP地址一一对应
IP地址	设备的IP地址，即域名对应的IP地址
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

14.2.2 配置动态 DNS

1. 功能简介

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）上注册账户，设置密码。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。
- 为保证动态 DNS 正常运行，如果用户在阿里云和腾讯云中为域名配置了多个 IP 地址，设备将自动清除相关记录。
- 使用阿里云和腾讯云的动态 DNS 时，请确保设备系统时间同步准确。

3. 配置步骤

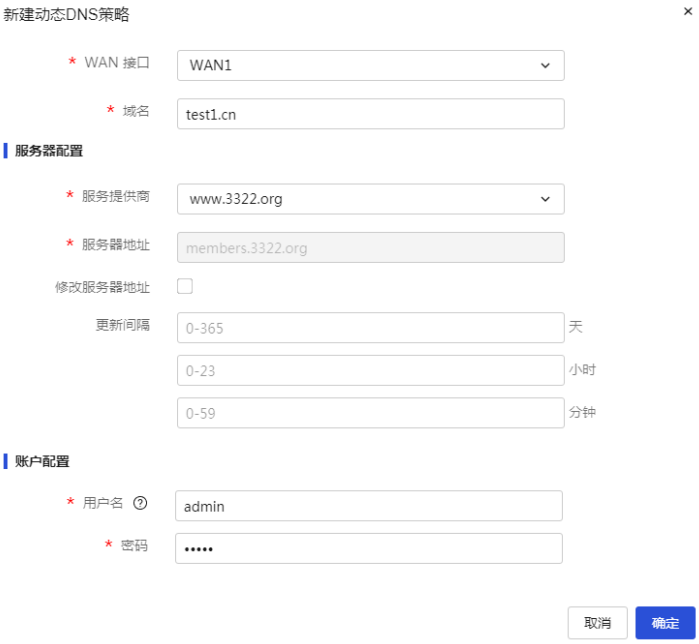
页面向导：[高级选项/应用服务/动态 DNS]

本页面为您提供如下主要功能：

- 显示已添加的动态 DNS 详细信息
- 添加动态 DNS
- 删除已添加的动态 DNS
- 修改已添加的动态 DNS

添加动态DNS：

1. 单击<添加>按钮，弹出新建动态 DNS 策略对话框，选择设备上提供相应服务的 WAN 接口，并输入服务提供商处注册的域名、用户名和密码等信息
2. 单击<确定>按钮，完成配置

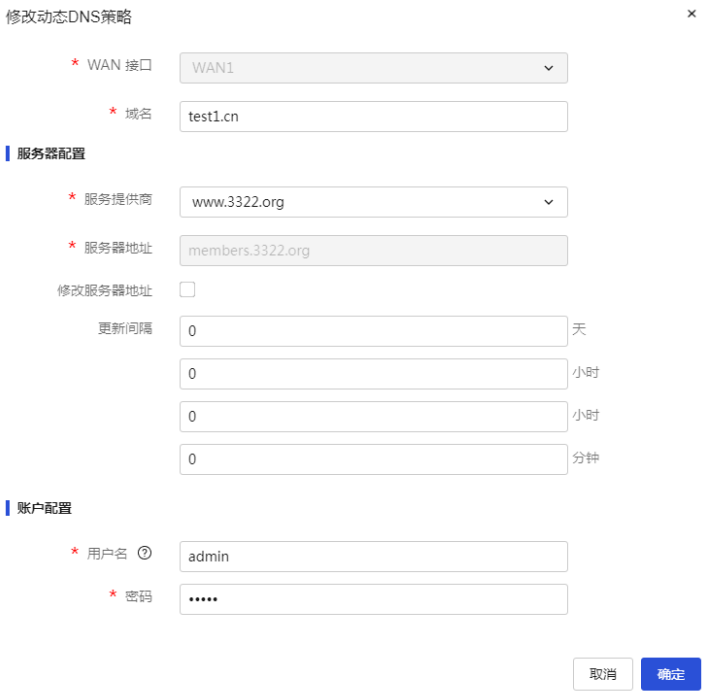


删除动态DNS：

1. 勾选需要删除的动态 DNS
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改动态DNS：

1. 单击需要修改的动态 DNS 操作列的编辑图标，弹出修改动态 DNS 策略对话框，修改相关参数
2. 单击<确定>按钮，完成配置



4. 参数解释

表14-3 页面参数描述

页面参数	描述
WAN接口	设备上提供服务的WAN接口，例如WAN1口
域名	为设备分配的域名，配置该参数时，需提前在DDNS服务器（即DDNS服务提供商，如花生壳网站）上注册
服务提供商	动态 DNS 服务提供商，主要包括： • www.3322.org、ORAY(花生壳)、Alibaba Cloud、Tencent Cloud：若服务器地址与缺省情况不同，需勾选“修改服务器地址”后，在“服务器地址”配置项处修改 DDNS 服务器地址 • Others：选择此选项，需在“服务器地址”配置项处手动输入 DDNS 服务器地址
更新间隔	设备向服务器发送更新请求的时间间隔。配置该参数时，需配置天数、小时和分钟，若配置时间间隔为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
账户配置	动态DNS的账户信息。 www.3322.org、ORAY(花生壳)、Others主要包括： • 用户名：在动态 DNS 服务提供商处注册的用户名。 • 密码：在动态 DNS 服务提供商处注册的密码。 Alibaba Cloud、Tencent Cloud 主要包括： • 用户名：在动态 DNS 服务提供商处生成的 API 秘钥 ID。 • 密码：在动态 DNS 服务提供商处生成的 API 密钥。

DDNS功能	是否开启DDNS功能。若开启该功能，设备将按照配置的DDNS策略及规则进行工作。缺省开启DDNS功能
状态	动态DNS的连接状态，主要分为： • 已连接：该 WAN 接口已与域名建立动态 DNS 连接 • 未连接：该 WAN 接口未与域名建立动态 DNS 连接
操作	可对该配置进行编辑和删除操作

14.2.3 配置本地域名服务

1. 功能简介

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

页面向导：[高级选项/应用服务/本地域名服务]

设置本地域名服务：

1. 开启本地域名服务功能
2. 设置本地域名地址
3. 单击<应用>按钮，完成配置

4. 参数解释

表14-4 页面各参数项描述

页面参数	描述
本地域名服务	选择是否开启本地域名服务。缺省为开启
本地域名地址	内网终端用于访问设备Web管理页面的域名

14.2.4 终端自动访问 Web 服务

1. 功能简介

内网终端在连接无线热点时可以自动跳转设置的终端自动访问地址，该地址既可以是内网服务器的 IP 地址、域名或者 URL，也可以是公网的 IP 地址、域名或者 URL。

2. 注意事项

- 当配置访问地址为域名或者 URL 时，请确保域名部分能够正确解析为 IP 地址，否则可能会导致无法正常跳转。
- 此功能通常用于跳转至内部服务器地址，不建议配置公网地址，某些公网网站（例如百度，淘宝等）无法正常使用该功能。

3. 配置步骤

页面向导：[高级选项/应用服务/终端自动访问 Web 服务]

设置终端自动访问Web服务：

1. 开启终端自动访问 Web 服务功能
2. 输入内网终端用于自动跳转的 Web 页面的域名或者 IP 地址
3. 单击<应用>按钮，完成配置

4. 参数解释

表14-5 页面各参数项描述

页面参数	描述
终端自动访问Web服务	选择是否开启终端自动访问Web服务。缺省为关闭
终端自动访问地址	内网终端用于自动跳转的Web页面的IP地址、域名或者URL

14.3 PPPoE服务器

14.3.1 简介

PPPoE（Point-to-Point Protocol over Ethernet，在以太网上承载 PPP 协议）是一种将 PPP 协议应用于以太网的扩展技术。通过为用户分配宽带账号和密码，并结合认证与计费服务，实现对每台接入设备的控制、认证和计费功能。目前，这项技术被广泛应用于小区网络和租户环境。

14.3.2 配置管理

1. 注意事项

- PPPoE 服务器的地址池范围不能与其他接口的 IP 地址和网段冲突。
- 基于 VLAN 的防火墙规则、流量排行等功能暂时无法对 PPPoE 虚拟接口生效。

2. 配置步骤

页面向导：[高级选项/PPPoE 服务器/配置管理]

本页面为您提供如下主要功能：

- 开启/关闭 PPPoE 服务器功能
- 配置 PPPoE 服务器相关参数
- 单击<应用>按钮，完成配置

3. 参数解释

表14-6 页面参数描述

页面参数	描述
PPPoE服务器	启用或关闭PPPoE服务器功能。
强制PPPoE拨号	启用或关闭强制拨号功能。启用后，该VLAN下仅拨号用户和例外IP的用户可以访问网络。
IP地址	PPPoE服务器的地址
地址池起始地址	为客户端分配的IP地址池的起始地址。
地址池结束地址	为客户端分配的IP地址池的结束地址。
VLAN	需要进行PPPoE拨号的局域网VLAN。
DNS1	首选DNS服务器地址。
DNS2	备选DNS服务器地址。
最大未应答LCP包数	最大未响应链路控制协议包数量。当一个连接的未响应LCP包数超过此数值时，PPPoE服务器将自动断开该连接。
认证方式	对用户身份验证的认证方式，包括PAP、CHAP、MSCHAP和MSCHAPv2，使用时至少选择一种。

14.3.3 账户管理

1. 注意事项

最多配置账户管理数据 300 条，最多同时登录人数 80 人。

2. 配置步骤

页面向导：[高级选项/PPPoE 服务器/账户管理]

本页面为您提供如下主要功能：

- 显示已添加的账户详细信息
- 添加账户
- 删除已添加的账户
- 修改已添加的账户

添加账户：

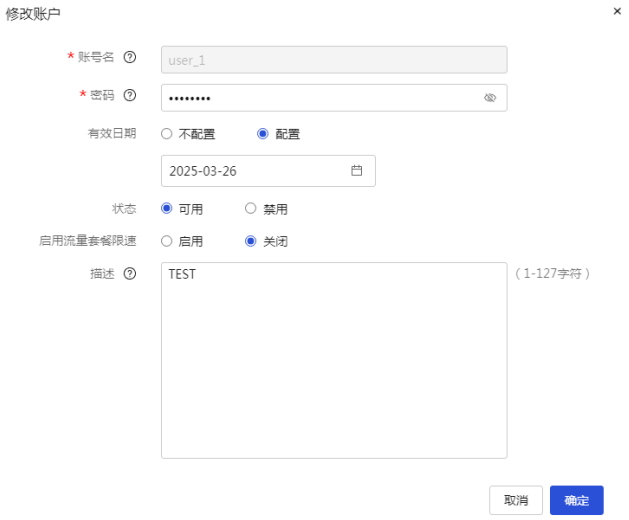
1. 单击<添加>按钮，弹出添加账户对话框，设置账户名、密码、有效日期、状态等信息
2. 单击<确定>按钮，完成配置

删除账户：

1. 勾选需要删除的账户
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改账户：

1. 单击需要修改的账户操作列的编辑图标，弹出修改账户对话框，修改相关参数
2. 单击<确定>按钮，完成配置



3. 参数解释

表14-7 页面参数描述

页面参数	描述
账号名	自定义用户拨号所使用的用户名。
密码	自定义用户拨号所使用的密码。
有效日期	账户的到期时间。
状态	账户的当前状态。
启用流量套餐限速	启用或禁用流量套餐限速功能。启动后，可选择特定账户套餐，对PPPoE拨号用户进行带宽限制。
描述	规则的描述信息，可对规则进行简单的描述，方便使用。
操作	可对该配置进行编辑和删除操作。

14.3.4 账号套餐

1. 配置简介

对 PPPoE 拨号上网用户进行共享带宽限速，该账户套餐内的所有用户共同使用设定的限制带宽。

2. 配置步骤

页面向导：[高级选项/PPPoE 服务器/账号套餐]

本页面为您提供如下主要功能：

- 显示已添加的套餐信息
- 添加套餐
- 删除已添加的套餐
- 修改已添加的套餐

添加套餐：

1. 单击<添加>按钮，弹出添加套餐对话框，设置套餐名称、上下行带宽、应用接口等信息
2. 单击<确定>按钮，完成配置

删除套餐：

1. 勾选需要删除的套餐
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改套餐：

1. 单击需要修改的套餐操作列的编辑图标，弹出修改套餐对话框，修改相关参数
2. 单击<确定>按钮，完成配置

3. 参数解释

表14-8 页面参数描述

页面参数	描述
套餐名称	自定义账户套餐的名称。

上行保证带宽	当线路拥塞时，套餐内所有用户上传方向可共享的最大带宽值。
上行弹性最大带宽	当线路空闲时，套餐内所有用户上传方向可共享的最大带宽值。
下行保证带宽	当线路拥塞时，套餐内所有用户下载方向可共享的最大带宽值。
下行弹性最大带宽	当线路空闲时，套餐内所有用户下载方向可共享的最大带宽值。
应用接口	选择应用此套餐的网络接口。
操作	可对该配置进行编辑和删除操作。

14.3.5 例外 IP 管理

1. 配置简介

例外 IP 管理的用户无需拨号即可上网，即使启用了强制 PPPoE 拨号功能。

2. 注意事项

例外 IP 管理中的 IP 地址为局域网用户终端的本地 IP 地址。

3. 配置步骤

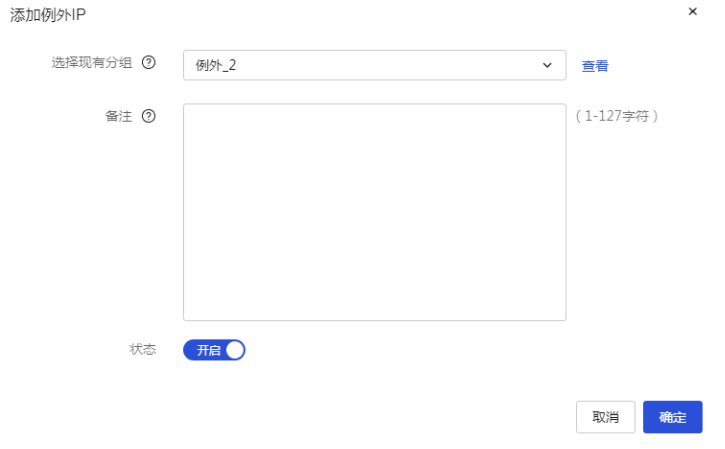
页面向导：[高级选项/PPPoE 服务器/例外 IP 管理]

本页面为您提供如下主要功能：

- 显示已添加的例外 IP 地址信息
- 添加例外 IP
- 删除已添加的例外 IP
- 修改已添加的例外 IP

添加例外IP：

1. 单击<添加>按钮，弹出添加例外 IP 对话框，选择现有地址组或新创建地址组、设置该例外 IP 状态
2. 单击<确定>按钮，完成配置

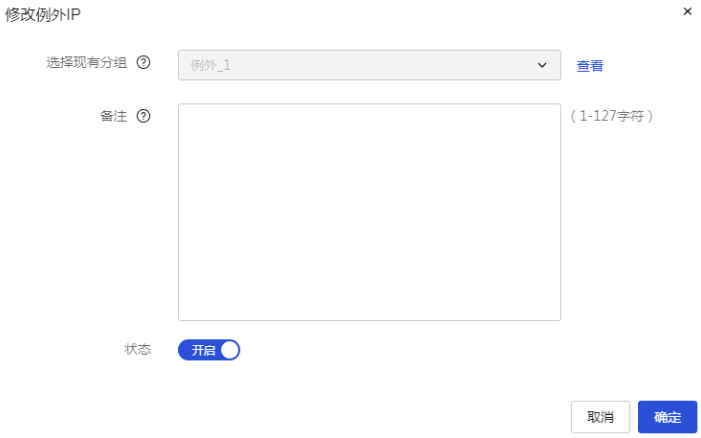


删除例外IP：

1. 勾选需要删除的例外 IP
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改例外IP：

1. 单击需要修改的例外 IP 操作列的编辑图标，弹出修改例外 IP 对话框，修改相关参数
2. 单击<确定>按钮，完成配置



4. 参数解释

表14-9 页面参数描述

页面参数	描述
选择现有分组	选择IP所属的分组。
备注	对该例外IP的备注说明。
状态	开启或关闭此例外IP的功能。

14.3.6 在线用户

1. 配置步骤

页面向导：[高级选项/PPPoE 服务器/在线用户]

本页面为您提供如下主要功能：

- 显示当前通过 PPPoE 拨号上网的用户信息
- 断开用户与 PPPoE 服务器的连接

2. 参数解释

表14-10 页面参数描述

页面参数	描述
用户名	PPPoE拨号的账户名。
用户地址	为已拨号客户端分配的PPPoE地址。
用户MAC	客户端MAC地址。
上线日期	客户端拨号上网的日期。
断开连接	可对在线用户进行断开连接操作。

14.4 UpnP

1. 功能简介

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。

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。

3. 配置步骤

页面向导：[高级选项/UpnP]

设置UPnP：

1. 开启 UPnP 功能
2. 单击<应用>按钮，完成配置

4. 参数解释

表14-11 页面参数项述

页面参数	描述
UPnP	是否开启UPnP功能。若开启该功能，设备将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。缺省关闭UPnP功能 设置完成，需点击“应用”按钮，使配置生效

14.5 策略路由

1. 功能简介

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。

2. 注意事项

- 在开启策略路由的强制功能前，请确保已启用 WAN 接口的链路探测功能，以便设备判断该接口的外网连通状态。
- 策略路由中引用的 WAN 接口物理状态必须为 UP，否则策略路由将无法生效。

3. 配置步骤

页面向导：[高级选项/策略路由]

本页面为您提供如下主要功能：

- 显示已添加的策略路由详细信息
- 添加策略路由
- 删除已添加的策略路由
- 修改已添加的策略路由

添加策略路由：

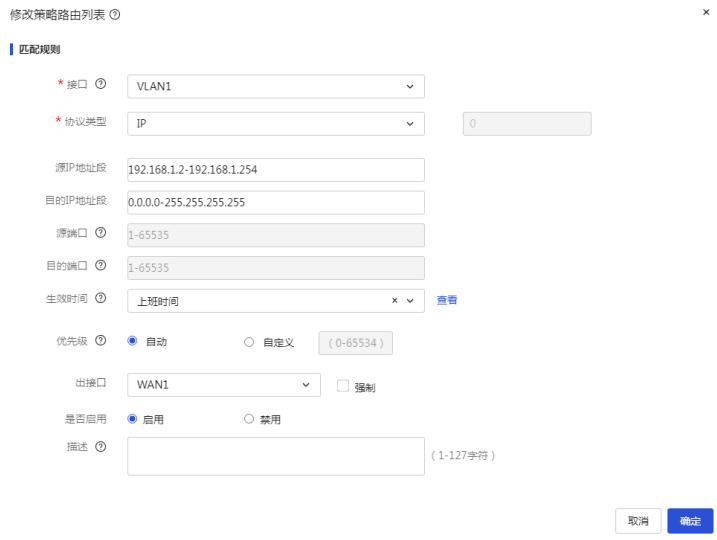
1. 单击<添加>按钮，弹出新增策略路由列表对话框，设置接口、协议类型、源和目的 IP 地址段等信息
2. 单击<确定>按钮，完成配置

删除策略路由：

1. 勾选需要删除的策略路由条目
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改策略路由：

1. 单击需要修改的策略路由操作列的编辑图标，弹出修改策略路由列表对话框，修改相关参数
2. 单击<确定>按钮，完成配置



4. 参数解释

表14-12 页面参数描述

页面参数	描述
接口	报文的来源接口，即策略对从某一接口收到的数据包进行控制

协议类型	策略需要控制的报文协议类型。配置该参数时，可根据需要进行选择： • 若需控制某传输层协议的报文，则选择“TCP”或“UDP” • 若需控制某网络层协议的报文，则选择“IP” • 若需控制 Ping、Tracert 等 ICMP 协议报文，则选择“ICMP” • 若需控制其他协议报文，则选择“协议号”并配置协议号编号
源IP地址段	规则需要控制的源IP地址范围。配置该参数时，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” • 若只指定一个地址，则起始地址和结束地址需要相同 • 若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他的地址都匹配，如“!1.1.1.1-1.1.1.10”
目的IP地址段	规则需要控制的目的IP地址范围。配置该参数时，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” • 若只指定一个地址，则起始地址和结束地址需要相同 • 若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他的地址都匹配，如“!1.1.1.1-1.1.1.10”
源端口	规则需要控制的源端口。仅当协议类型指定为“TCP”或“UDP”，才需配置该参数。若在输入端口号前添加“!”，则表示取反，即除此端口号外的其他的端口都匹配，如“!1-5000”
目的端口	规则需要控制的目的端口。仅当协议类型指定为“TCP”或“UDP”，才需配置该参数。若在输入端口号前添加“!”，则表示取反，即除此端口号外的其他的端口都匹配，如“!1-5000”
生效时间	规则的生效时间。配置该参数时，需选择已创建的时间组。如需新增时间组，可通过点击右侧的<新增时间组>按钮创建新的时间组
优先级	规则的优先级。设置方式有两种： • 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
出接口	报文的转发接口，即匹配规则的报文通过指定出接口转发
强制	当WAN口的端口状态为外网未连通时，指向该WAN口的策略路由会失效。通过配置该参数，可以使策略路由在WAN口的端口状态为外网未连通时强制生效。 • 若选择了“强制”选项，当 WAN 口的端口状态为外网未连通时，则当前策略路由仍然会生效，转发数据 • 若未选择“强制”选项，当 WAN 口的端口状态为外网未连通时，则当前策略路由不会生效
是否启用	是否开启该路由规则。若启用该规则，设备将按照配置的路由策略及规则进行工作
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

14.6 IPv6静态路由

1. 功能简介

IPv6 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 IPv6 网络结构比较简单且比较稳定时，通过配置 IPv6 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 IPv6 地址时，设置 IPv6 静态路由即可实现正常通信。

当去往同一目的地存在多条 IPv6 静态路由时，如果您希望优先选用某条 IPv6 静态路由，可以调整 IPv6 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。

2. 注意事项

当 IPv6 静态路由中下一跳对应的接口失效时，本地的 IPv6 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 IPv6 静态路由的配置。

3. 配置步骤

页面向导：[高级选项/IPv6 静态路由]

本页面为您提供如下主要功能：

- 显示已添加的 IPv6 静态路由详细信息
- 添加 IPv6 静态路由
- 删除已添加的 IPv6 静态路由
- 修改已添加的 IPv6 静态路由
- 查看 IPv6 路由信息表

添加IPv6静态路由：

1. 单击<添加>按钮，弹出添加 IPv6 静态路由对话框，输入目的 IP 地址、IPv6 前缀长度和下一跳等信息
2. 单击<确定>按钮，完成配置

删除IPv6静态路由：

1. 勾选需要删除的 IPv6 静态路由条目
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置

修改IPv6静态路由：

1. 单击需要修改的 IPv6 静态路由操作列的编辑图标，弹出修改 IPv6 静态路由对话框，修改相关参数
2. 单击<确定>按钮，完成配置

查看IPv6路由信息表：

单击<查看IPv6路由信息表>按钮，可查看路由信息表

4. 参数解释

表14-13 页面参数描述

页面参数	描述
目的IP地址	设备要访问的目的网络的IP地址
IPv6前缀长度	目的网络的IPv6前缀长度，例如64
下一跳	数据在到达目的地址前，需要经过的下一个路由器的IP地址。配置该参数时，可根据需要选择是否勾选“出接口”选项 • 若确定数据经过的设备出口，则勾选“出接口”选项，并设置下一跳 IP 地址，下一跳地址必须和所选接口在相同网段 • 若不确定出接口时，则不勾选“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
优先级	IPv6静态路由的优先级，配置该参数时，数值越小则优先级越高
描述	规则的描述信息，可对规则进行简单的描述，方便使用
操作	可对该配置进行编辑和删除操作

14.7 SNMP

14.7.1 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. 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. 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。

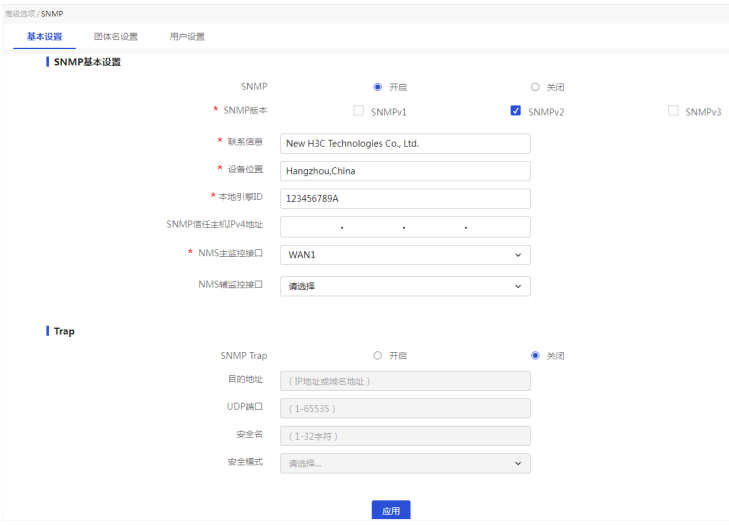
14.7.2 基本设置

1. 配置步骤

页面向导：[高级选项/SNMP/基本设置]

SNMP基本设置：

1. 开启 SNMP 功能，并设置 SNMP 版本、联系信息、设备位置和本地引擎 ID 等信息
2. 单击<应用>按钮，完成配置



2. 参数解释

表14-14 页面参数描述

页面参数	描述
SNMP	是否开启SNMP功能。若开启该功能，设备将允许管理员通过NMS（网络管理系统）对SNMP Agent进行管理，包括状态监控、数据采集和故障处理
SNMP版本	设备使用的SNMP版本号，配置该参数时，可根据需要进行选择： • 若 NMS（网络管理系统）使用的是 SNMPv1 版本，则选择“SNMPv1” • 若 NMS（网络管理系统）使用的是 SNMPv2 版本，则选择“SNMPv2” • 若 NMS（网络管理系统）使用的是 SNMPv3 版本，则选择“SNMPv3”
联系信息	设备维护联系信息。若设备发生故障，维护人员可利用维护联系信息，及时与设备生产厂商取得联系。联系信息长度为1-255个字符，不支持中文、英文格式的问号、全空格，以及换行符
设备位置	设备物理位置的信息。设备位置长度为1-255个字符，不支持中文、英文格式的问号、全空格，以及换行符
本地引擎ID	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，且长度必须为偶数
SNMP信任主机IPv4地址	NMS（网络管理系统）的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
NMS主监控接口	NMS（网络管理系统）管理SNMP Agent所用到的Agent的主接口。例如：WAN1
NMS辅监控接口	NMS（网络管理系统）管理SNMP Agent所用到的Agent的备用接口。当设备设置为单WAN口时，不支持该设置
TRAP功能	是否开启TRAP功能。若开启该功能，当SNMP Agent出现特定事件，例如性能问题或者网络设备接口宕机等，SNMP Agent会主动给NMS（网络管理系统）发送告警信息
目的地址	NMS（网络管理系统）的IP地址或域名地址。即接收设备TRAP消息的主机地址
UDP端口	TRAP消息转发使用的UDP端口号，缺省为162。若不使用缺省端口号，可以自定义端口号，取值为1~65535

安全名	SNMPv1、SNMPv2c的团体名或SNMPv3的用户名
安全模式	安全名对应的SNMP Agent版本号

14.7.3 团体名设置

1. 注意事项

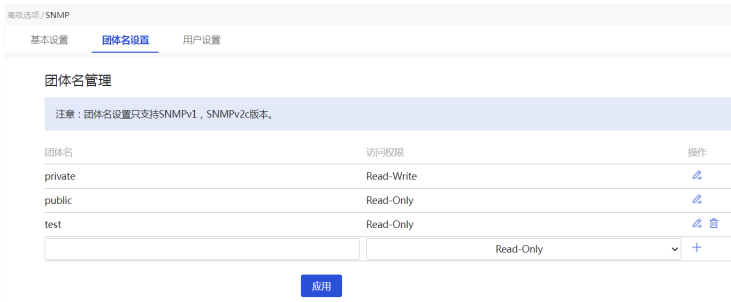
团体名设置只支持 SNMPv1、SNMPv2c 版本。

2. 配置步骤

页面向导：[高级选项/SNMP/团体名设置]

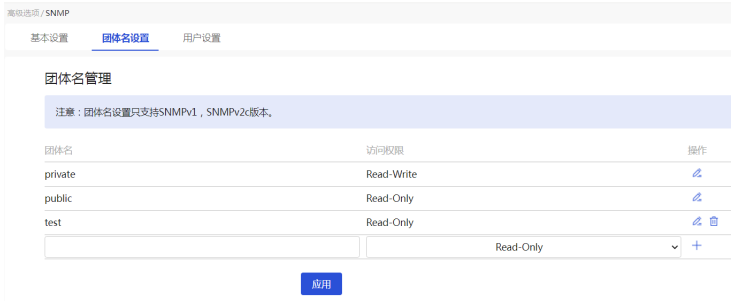
本页面为您提供如下主要功能：

- 显示已添加的团体名详细信息
- 添加团体名
- 删除已添加的团体名
- 修改已添加的团体名



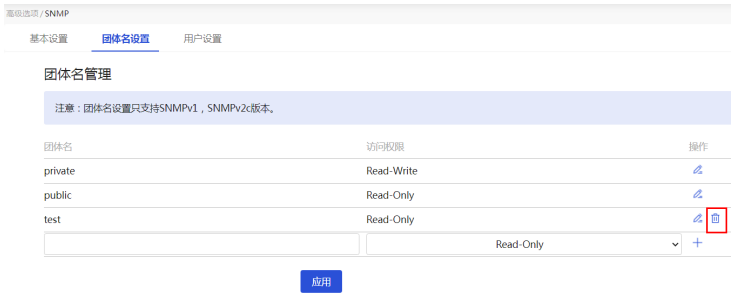
添加团体名：

1. 设置团体名和访问权限
2. 单击团体名操作列<+>图标
3. 单击<应用>按钮，完成配置



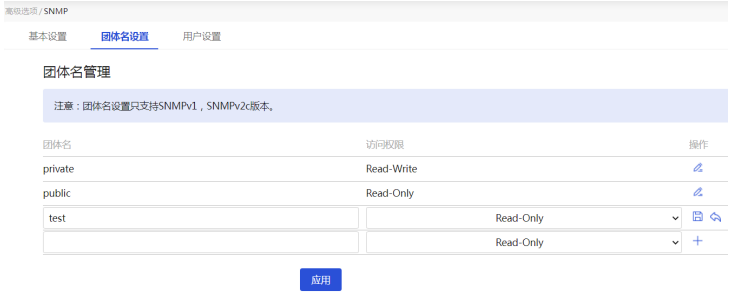
删除团体名：

1. 单击已添加的团体名操作列的删除图标，弹出提示对话框
2. 单击<确定>按钮，完成配置



修改团体名：

1. 单击需要修改的团体名操作列的编辑图标，修改相关参数
2. 单击团体名操作列的更新图标
3. 单击<应用>按钮，完成配置



3. 参数解释

表14-15 页面参数描述

页面参数	描述
团体名	SNMPv1、SNMPv2c版本采用的认证机制，用于SNMP Agent对NMS（网络管理系统）进行认证。配置该参数时，NMS上配置的团体名和SNMP Agent上配置的团体名需一致
访问权限	该团体的访问权限，主要分为： • Read-Only：只读权限 • Read-Write：读写权限 配置该参数时，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 设置完成，需点击“应用”按钮，使配置生效
操作	可对该配置进行编辑操作

14.7.4 用户设置

1. 注意事项

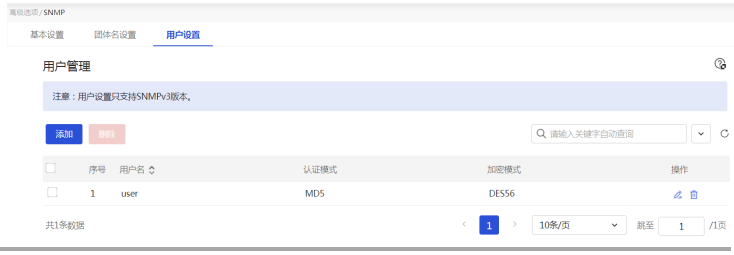
用户设置只支持 SNMPv3 版本，用于添加 SNMPv3 版本的用户名。

2. 配置步骤

页面向导：[高级选项/SNMP/用户设置]

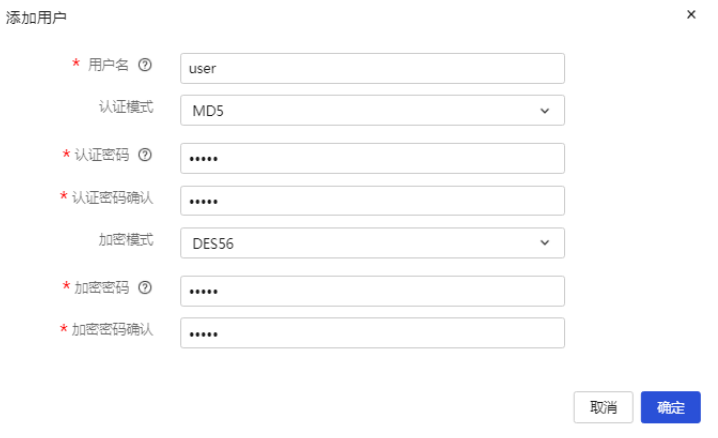
本页面为您提供如下主要功能：

- 显示已添加的用户设置详细信息
- 添加用户信息
- 删除已添加的用户信息
- 修改已添加的用户信息



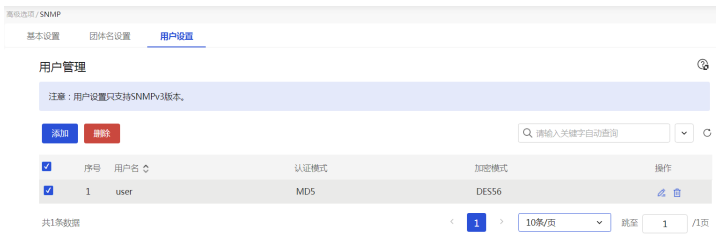
添加用户信息：

1. 单击<添加>按钮，弹出添加用户对话框，输入用户名、认证密码和加密密码等信息
2. 单击<确定>按钮，完成配置



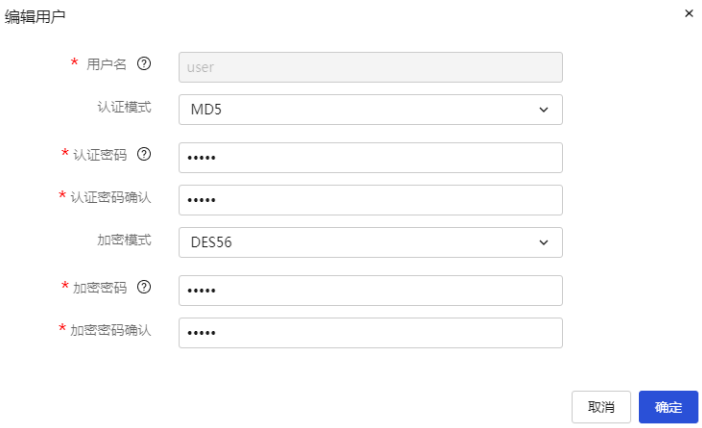
删除用户信息：

1. 勾选需要删除的用户信息
2. 单击<删除>按钮，弹出提示对话框
3. 单击<确定>按钮，完成配置



修改用户信息：

1. 单击需要修改的用户信息操作列的编辑图标，弹出编辑用户对话框，修改相关参数
2. 单击<确定>按钮，完成配置



3. 参数解释

表14-16 页面参数描述

页面参数	描述
序号	SNMPv3版本用户的编号
用户名	SNMPv3版本的用户名
认证模式	用户认证的算法，主要分为： • MD5：表示采用 MD5 认证算法 • SHA：表示采用 SHA 认证算法 • None：表示不认证
认证密码	用户认证的密码。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，能包含英文字母[a-z,A-Z]、数字，以及~!@#$%^&*()_+`-={}|[]:'<>?,./字符；区分大小写
认证密码确认	再次输入认证密码
加密模式	用户认证的加密模式，主要分为： • DES56：表示采用 DES56 加密模式 • None：表示不加密
加密密码	加密的密码。当认证模式和加密模式设置不为None时，需配置此参数。密码长度为1-64个字符，能包含英文字母[a-z,A-Z]、数字，以及~!@#$%^&*()_+`-={}|[]:'<>?,./字符；区分大小写
加密密码确认	再次输入加密密码

15 系统工具

15.1 系统设置

15.1.1 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、设备位置和网络管理员的联系信息，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。

15.1.2 设备信息

1. 功能简介

为了更便于网络管理员管理网络中的设备，需要设置设备信息，其中包括设备的名称、位置以及网络管理员的联系信息。

2. 配置步骤

页面向导：[系统工具/系统设置/设备信息]

设置设备信息，包括设备名称、设备位置和网络管理员的联系信息

3. 参数解释

页面中各参数的含义如下表所示。

表15-1 页面参数描述

页面参数	描述
设备名称	输入设备的名称
设备位置	输入设备的位置
联系信息	输入网络管理员的联系信息

15.1.3 日期和时间

1. 功能简介

设置系统时间，包括以下两种方式：

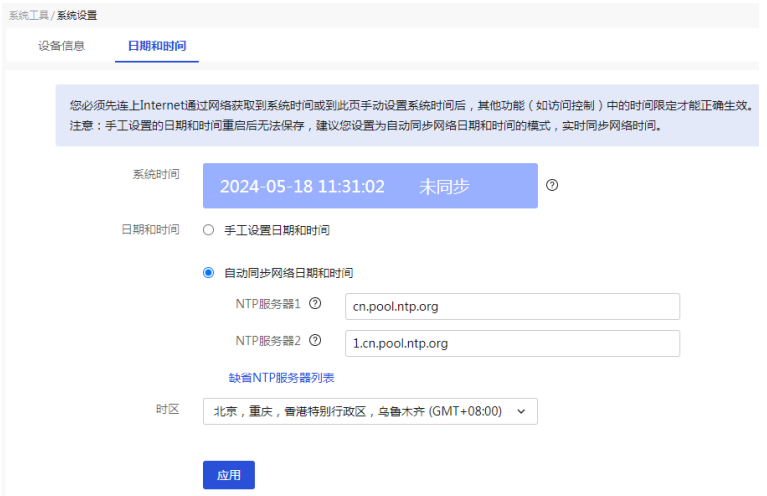
- 手工设置日期和时间。
- 自动同步网络日期和时间。

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. 配置步骤

页面向导：[系统工具/系统设置/日期和时间]

设置系统时间



单击“手工设置日期和时间”，将系统时间配置为设备所在地理区域的当前时间：

1. 选择年月日
2. 选择时分秒
3. 将时区配置为设备所在地理区域的时区
4. 单击<应用>按钮，完成配置

选择“自动同步网络日期和时间”选项，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：

1. 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
2. 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。将时区配置为设备所在地理区域的时区
3. 将时区配置为设备所在地理区域的时区
4. 单击<应用>按钮，完成配置

3. 参数解释

页面中各参数的含义如下表所示。

表15-2 页面参数描述

页面参数	描述
系统时间	当前系统实际
手工设置日期和时间	手工设置系统日期和时间，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	自动同步网络日期和时间，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
NTP服务器1	输入NTP服务器1的IP地址或者域名地址
NTP服务器2	输入NTP服务器2的IP地址或者域名地址
缺省NTP服务器列表	查看设备内置的NTP服务器信息

时区	设备所处的时区
应用	完成配置

15.2 网络诊断

15.2.1 Ping

1. 配置步骤

页面向导：[系统工具/网络诊断/Ping]

用于检测网络，测试另一台设备或主机是否可达

2. 参数解释

页面中各参数的含义如下表所示。

表15-3 页面参数描述

页面参数	描述
类型	Ping操作的类型
IPv4	使用IPv4协议进行操作，报文类型及地址格式为IPv4
IPv6	使用IPv6协议进行操作，报文类型及地址格式为IPv6
目标IP地址或者主机名	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。如果目标IP地址是设备的源IP地址，请选择接口为AUTO。
选择出接口	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
源IP地址	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
开始	系统开始检测
停止	系统停止检测
结果	显示检测的过程和结果，说明网络发包的测试情况和与测试主机的往返平均时延

15.2.2 Tracert

1. 配置步骤

页面向导：[系统工具/网络诊断/Tracert]

用于检查从设备到达目标主机所经过的路由情况

2. 参数解释

页面中各参数的含义如下表所示。

表15-4 页面参数描述

页面参数	描述
类型	Tracert操作的类型
IPv4	使用IPv4协议进行操作，报文类型及地址格式为IPv4
IPv6	使用IPv6协议进行操作，报文类型及地址格式为IPv6
目标IP地址或者主机名	输入需要路由跟踪的目标IP地址或者主机名
选择出接口	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
源地址	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
开始	系统开始检测
停止	系统停止检测
结果	显示检测的过程和结果

15.2.3 诊断

1. 配置步骤

页面向导：[系统工具/网络诊断/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

2. 参数解释

页面中各参数的含义如下表所示。

表15-5 页面参数描述

页面参数	描述
搜集诊断信息	系统开始收集诊断信息

15.2.4 系统自检

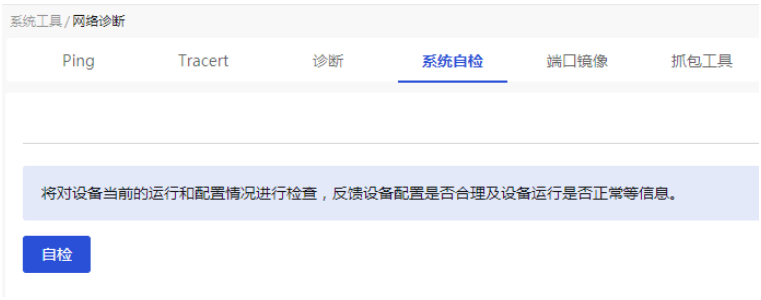
说明

AC 模式下，不支持系统自检。

1. 配置步骤

页面向导：[系统工具/网络诊断/系统自检]

用于检查设备当前的运行和配置情况，反馈设备配置是否合理及设备运行是否正常等信息



2. 参数解释

页面中各参数的含义如下表所示。

表15-6 页面参数描述

页面参数	描述
自检	系统进行自检并显示系统自检结果

15.2.5 端口镜像

1. 配置步骤

页面向导：[系统工具/网络诊断/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

2. 参数解释

页面中各参数的含义如下表所示。

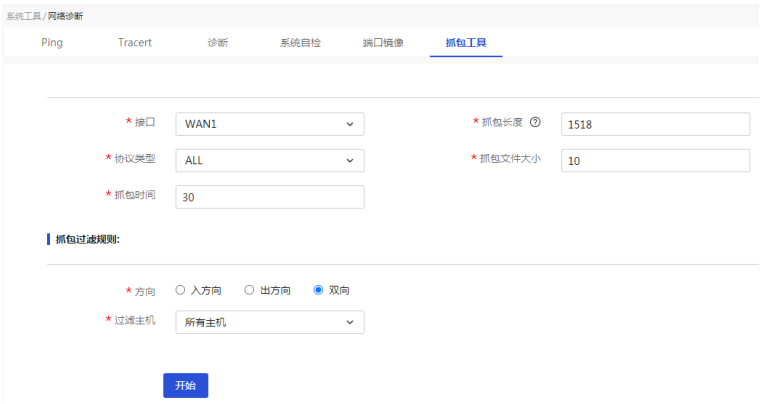
表15-7 页面参数描述

页面参数	描述
源端口	选择镜像的源端口，即被监测的端口
方向	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
目的端口	选择镜像的目的端口，即与数据监测设备相连的端口
确定	系统开始端口镜像

15.2.6 抓包工具

1. 配置步骤

页面向导：[系统工具/网络诊断/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	

2. 参数解释

页面中各参数的含义如下表所示。

表15-8 页面参数描述

页面参数	描述
接口	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
抓包长度	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
协议类型	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
抓包文件大小	输入抓取报文的大小，单位为MB
抓包时间	输入抓包的持续时长，单位为秒
方向	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
源主机	选择抓取报文的源主机
目的主机	选择抓取报文的目的主机
过滤主机	选择抓取报文的过滤主机
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	需要设置主机的IP地址
MAC地址过滤	需要设置主机的MAC地址
开始	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
取消	在抓包的过程中，您可以，终止当前的操作，并导出抓取的文件“capture-******.pacp”

15.3 远程管理

15.3.1 Ping

1. 配置步骤

页面向导：[系统工具/远程管理/Ping]

通过ping功能，可以检测网络的连通性，及时了解网络状况

2. 参数解释

页面中各参数的含义如下表所示。

表15-9 页面参数描述

页面参数	描述
允许ping	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
应用	完成配置

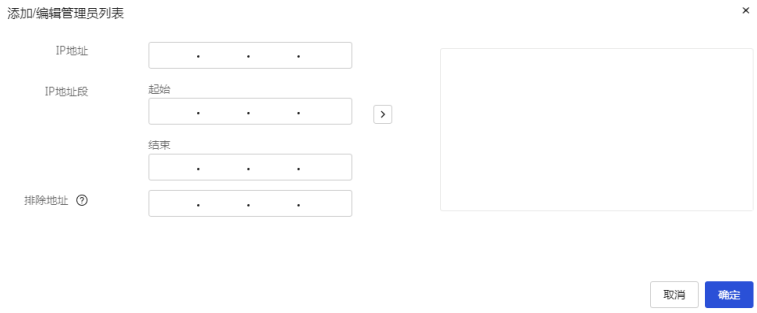
15.3.2 SSH

1. 配置步骤

页面向导：[系统工具/远程管理/Telnet]

SSH（Secure Shell）是一种加密的网络协议，用于在不安全的网络中安全地进行远程登录、文件传输和命令执行

“管理员列表”区段，单击<添加/编辑>按钮，弹出添加/编辑管理员列表



2. 参数解释

页面中各参数的含义如下表所示。

表15-10 页面参数描述

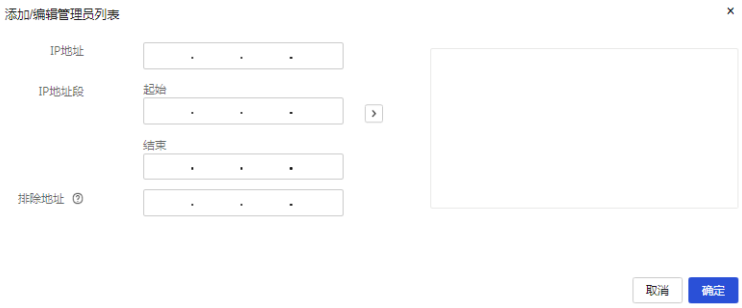
页面参数	描述
SSH服务	是否开启SSH服务，若开启该服务，则允许计算机通过WAN口远程SSH管理此设备
IPv4端口	SSH方式远程管理设备的端口号，外部用户通过此端口号SSH方式登录设备进行管理，缺省值为22
IP地址	通过SSH访问设备的IP地址。配置该参数时，输入IP地址后，需点击配置项右侧的>按钮，提交配置的地址内容
IP地址段	通过SSH访问设备的IP地址段的起始和结束地址。配置该参数时，输入IP地址段后，点击配置项右侧的>按钮，提交配置的地址内容
排除地址	不允许通过SSH访问设备的IP地址。配置该参数时，输入排除地址段后，点击配置项右侧的>按钮，提交配置的地址内容

15.3.3 Telnet

1. 配置步骤

页面向导：[系统工具/远程管理/Telnet]

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

“管理员列表”区段，单击<添加/编辑>按钮，弹出添加/编辑管理员列表	

2. 参数解释

页面中各参数的含义如下表所示。

表15-11 页面参数描述

页面参数	描述
Telnet服务	• 单击按钮，使得按钮状态为“ON”，开启 Telnet 服务 • 单击按钮，使得按钮状态为“OFF”，关闭 Telnet 服务
IPv4端口	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
添加/编辑	单击<添加/编辑>按钮，弹出添加/编辑管理员列表对话框
IP地址	输入允许通过Telnet访问设备的IP地址
IP地址段	允许通过Telnet访问设备的IP地址段
起始	允许通过Telnet访问设备的IP地址段的起始地址
结束	允许通过Telnet访问设备的IP地址段的结束地址
排除地址	输入不允许通过Telnet访问设备的IP地址
确定	完成配置

15.3.4 HTTP/HTTPS

说明

- 当管理员更改 VLAN1 的所在网段时，VLAN1 管理地址范围会自动随之更改。
- AC 模式下，仅支持配置“HTTP 登录端口”、“HTTPS 登录端口”和“登录超时时间”。

1. 配置步骤

页面向导：[系统工具/远程管理/HTTP/HTTPS]

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

在“VLAN1管理地址”区段，单击<编辑>按钮，编辑VLAN1管理地址

在“自定义管理地址”区段，点击<添加/编辑>按钮，添加/编辑自定义管理地址

2. 参数解释

页面中各参数的含义如下表所示。

表15-12 页面参数描述

页面参数	描述
HTTP登录端口	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
HTTPS登录端口	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
登录超时时间	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
允许所有用户访问WEB	勾选该选项时，允许所有用户访问WEB
VLAN1管理地址	编辑VLAN1管理地址
编辑	添加允许访问Web管理页面的管理员IP地址或地址段
IP地址	输入允许通过HTTP/HTTPS访问设备的IP地址
IP地址段	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
起始	输入允许通过HTTP/HTTPS访问设备的IP地址段的起始地址

结束	输入允许通过HTTP/HTTPS访问设备的IP地址段的结束地址
自定义管理地址	添加/编辑自定义管理地址
添加/编辑	添加允许访问Web管理页面的管理员IP地址或地址段
IP地址	输入允许通过HTTP/HTTPS访问设备的IP地址
IP地址段	输入允许通过HTTP/HTTPS访问设备的IP地址段
起始	输入允许通过HTTP/HTTPS访问设备的IP地址段的起始地址
结束	输入允许通过HTTP/HTTPS访问设备的IP地址段的结束地址
排除地址	输入不允许通过HTTP/HTTPS访问设备的IP地址
确定	完成配置

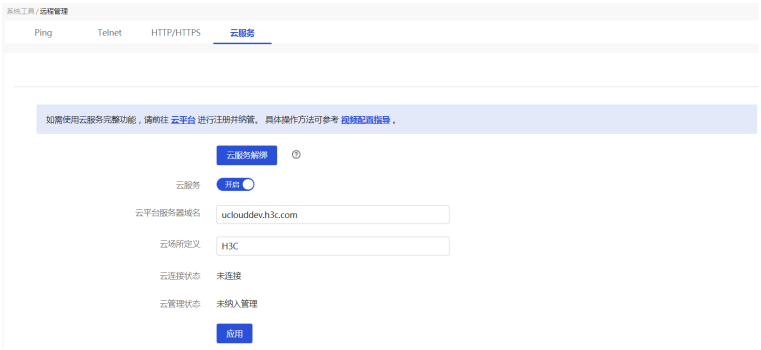
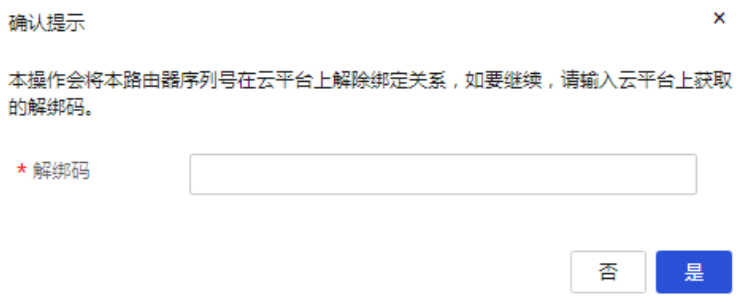
15.3.5 云服务

说明

AC 模式下，仅支持显示云连接状态。

1. 配置步骤

页面向导：[系统工具/远程管理/云服务]

实现设备在云平台中被管理	
云服务解绑，解除云服务绑定关系	

2. 参数解释

页面中各参数的含义如下表所示。

表15-13 页面参数描述

页面参数	描述
云服务解绑	解除云服务绑定关系
解绑码	输入从云平台上获取的解绑码
云服务	• 按钮状态为“开启”，则开启云服务 • 按钮状态为“关闭”，则关闭云服务
云平台服务器域名	输入H3C云简网络平台的域名
云场所定义	输入设备的系统名称。云场所定义长度为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
云连接状态	当前云连接状态
云管理状态	当前云管理状态
应用	完成配置

15.4 配置管理

说明

对于不同型号的设备，上述功能的支持情况可能会不同，请以 Web 页面实际显示情况为准。

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。

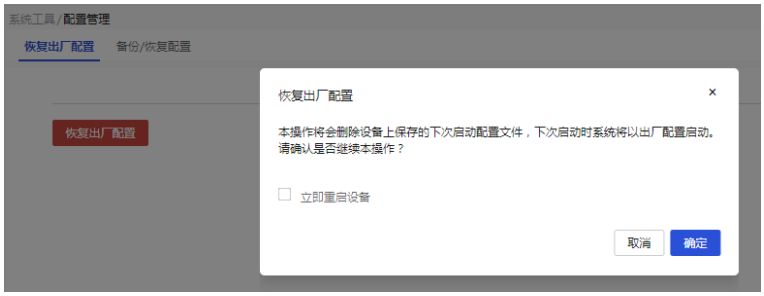
主要功能包括：

- 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。
- 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。

15.4.1 恢复出厂配置

1. 配置步骤

页面向导：[系统工具/配置管理/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	

2. 参数解释

页面中各参数的含义如下表所示。

表15-14 页面参数描述

页面参数	描述
恢复出厂配置	将设备上的配置恢复到出厂状态
立即重启设备	系统会立即重启设备
确定	执行该操作
取消	取消该操作

15.4.2 备份/恢复配置

说明

- 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。

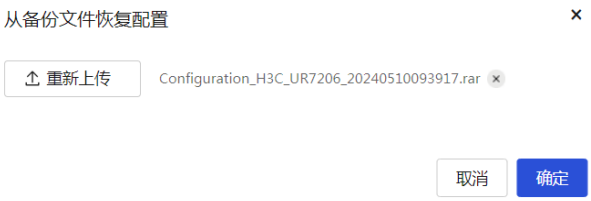
1. 配置步骤

页面向导：[系统工具/配置管理/备份/恢复配置]

- 设备配置错误后，如果希望设备恢复到正确配置运行状态，则需使用“从备份文件恢复”功能，恢复设备配置
- 如果希望将当前配置文件导出作为备份配置文件，则需使用“导出当前配置”功能，将当前配置文件导出
- 使用“USB 快速备份”功能，备份设备当前的配置到 U 盘上
- 使用“USB 快速恢复”功能，通过 U 盘中配置文件恢复设备配置

单击<从备份文件恢复>按钮，进入从备份文件恢复页面：

1. 单击“上传文件”按钮，选择特定路径下的备份配置文件
2. 单击<确定>按钮，开始恢复配置



单击<导出当前配置>按钮，即可将当前配置导出

单击<USB快速备份>按钮，开始备份配置，备份设备当前的配置到U盘上：

- 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
- 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

单击<USB快速恢复>按钮，开始恢复配置：

- 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
- 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

2. 参数解释

页面中各参数的含义如下表所示。

表15-15 页面参数描述

页面参数	描述
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
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

15.5 系统升级

说明

- 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。
- 如果升级使用版本号更小或发布时间更早的版本文件，设备可能会出现配置兼容问题，不建议这样操作。

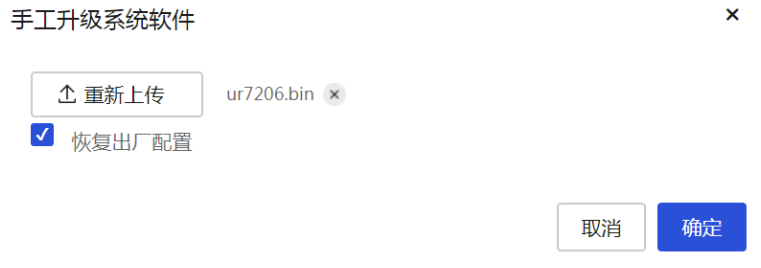
15.5.1 手工升级

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

页面向导：[系统工具/系统升级/手工升级]

通过手工升级方式，对设备版本进行升级，完善当前软件版本漏洞或者更新应用功能	
单击<手工升级系统软件>按钮，弹出手工升级系统软件对话框： • 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 • 单击<确定>按钮，开始软件升级	

3. 参数解释

页面中各参数的含义如下表所示。

表15-16 页面参数描述

页面参数	描述
手工升级系统软件	通过手工升级系统软件，对设备版本进行升级
恢复出厂配置	设备在升级系统软件之后恢复出厂配置
确定	开始软件升级

15.5.2 自动升级

1. 配置步骤

页面向导：[系统工具/系统升级/自动升级]

通过H3C云简网络平台对设备上的系统软件进行自动升级，完善当前软件版本漏洞或者更新应用功能

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

2. 参数解释

页面中各参数的含义如下表所示。

表15-17 页面参数描述

页面参数	描述
自动升级系统软件	立即对系统软件进行自动升级操作
预约升级	通过检测时间设置，预约对系统软件进行自动升级操作。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
检测时间设置	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
应用	完成配置
查看	查看预约升级日志

15.5.3 使用 U 盘恢复软件版本

1. 功能简介

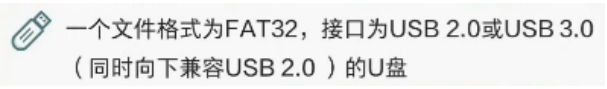
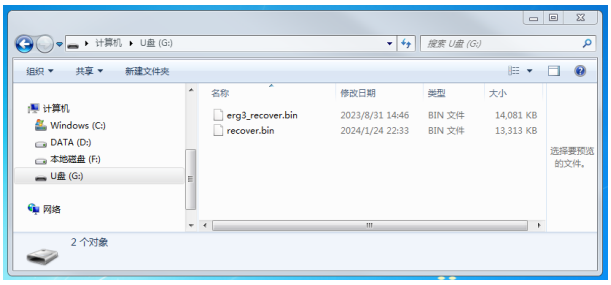
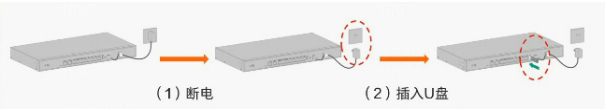
路由器使用过程中出现异常情况，例如升级过程中断电、设备无法正常运行等，可以使用 U 盘恢复软件版本。

2. 注意事项

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。

3. 配置步骤

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（.bin）拷贝到 U 盘。在 U 盘中将.bin 复制两份，再将两份文件分别命名为“erg3_recover.bin”和“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	

15.6 重新启动

重新启动功能用于立即和定时重新启动设备。

15.6.1 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

页面向导：[系统工具/重新启动/立即重启]

立即重新启动设备

3. 参数解释

页面中各参数的含义如下表所示。

表15-18 页面参数描述

页面参数	描述
立即重启	立即重新启动设备

15.6.2 定时重启

说明

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。

1. 配置步骤

页面向导：[系统工具/重新启动/定时重启]

定时重新启动设备	

2. 参数解释

页面中各参数的含义如下表所示。

表15-19 页面参数描述

页面参数	描述
定时重启	定时重新启动设备
开启	开启定时重启设备的功能
关闭	关闭定时重启设备的功能
生效周期	设定每周设备重启的具体时间
确定	设备将会在设定时间进行重启

15.7 系统日志

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。

日志划分为如下表所示的五个级别，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15-20 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

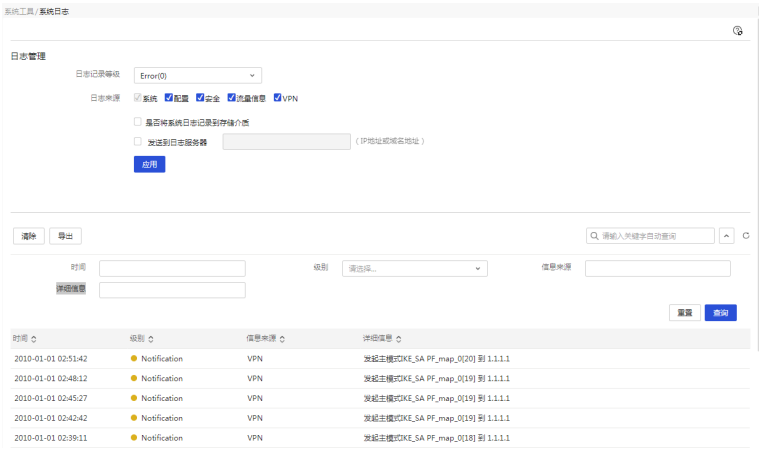
15.7.1 系统日志

1. 注意事项

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

页面向导：[系统工具/系统日志]

管理及显示日志信息	

3. 参数解释

页面中各参数的含义如下表所示。

表15-21 页面参数描述

页面参数	描述
日志管理	日志管理
日志记录等级	选择日志记录的级别
日志来源	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，记录部分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 AC模式下，日志来源仅支持“系统”、“配置”。
是否将系统日志记录到存储介质	• 勾选此选项，表示将系统日志记录到存储介质 • 不勾选，表示不将系统日志记录到存储介质
发送到日志服务器	输入日志服务器的IP地址或者域名地址
应用	完成配置
高级查询	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

时间	通过时间查找对应的系统日志
级别	通过级别查找对应的系统日志
信息来源	通过信息来源查找对应的系统日志
详细信息	通过详细信息查找对应的系统日志
清除	清除路由器所记录的日志信息
导出	将设备上已有的日志信息导出到登录Web管理页面的PC上

16 管理员

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。

16.1 修改管理员

注意

- 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密码，不允许删除管理员账户。
- 在整网管理模式下，设备不支持修改用户名，但支持在整网管理页面修改管理员密码。

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密码，请依次执行以下操作：
3. 在“当前管理员密码”配置项处，输入旧密码
4. 在“新密码”配置项处，输入新密码。密码长度为 10~63 个字符，只能包含数字、英文字母或英文符号（除“空格”、“?”、“”、“”、“\”字符之外）。密码必须包含至少两种类型的组合，并且不能包含 admin 的顺序或反序组合
5. 在“确认密码”配置项处，再次输入新密码，并确保与之一致
6. 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。密码提示不能与新密码相同
7. 单击<确定>按钮，完成配置

页面中各参数的含义如下表所示。

表16-1 页面参数描述

页面参数	描述
用户名	管理员的用户名
当前管理员密码	管理员当前的登录密码
新密码	管理员新的登录密码。密码长度为10~63个字符，只能包含数字、英文字母或英文符号（除“空格”、“?”、“”、“”、“\”字符之外）。密码必须包含至少两种类型的组合，并且不能包含admin的顺序或反序组合
确认密码	再次输入新密码，并确保与之前输入的新密码保持一致
密码提示	帮助管理员记忆密码的提示信息。密码提示不能与新密码相同

17 典型配置案例集

17.1 配置视频

表17-1 配置视频名称和链接

名称	链接
虚拟服务器(端口映射)配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1764
IPsec VPN典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1765
L2TP VPN典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1766
小贝AP典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1767
Portal认证典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1768
防火墙典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1769
策略路由典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1770
应用控制典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1771
网址控制典型配置举例 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1772
如何将设备绑定到云平台 演示视频	http://www.h3c.com/cn/home/qr/default.htm?id=1773
Web 登录 演示视频	https://www.h3c.com/cn/Service/Document_

	Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/01/?CHID=1000666
DHCP 方式接入 Internet 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/02/
PPPoE 方式接入 Internet 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/03/
固定地址方式接入 Internet 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/04/
VLAN 划分配置 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/05/
下联交换机实现不同 VLAN 互通配置 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/06/
带宽管理绿色通道配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/07/
配置文件备份与恢复 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/08/
恢复出厂配置 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/09/
一对一映射典型配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/10/
无线网络多网段划分配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/11/
如何使用 U 盘恢复软件版本 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/12/
带宽管理 IP 限速配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/

	00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/13/
如何修改 Web 登录密码 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/14/
带宽管理限制通道配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/15/
快速上网典型配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/16/
配置 DDNS 应用服务 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/17/
如何查看流量排行 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/18/
如何配置网络连接限制数 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/19/
文件控制功能配置举例 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/20/
MAC 地址过滤功能 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/21/
通过 UR 路由器对 AP 进行升级操作 演示视频	https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Routers/00-Public/Videos/Web_Video_Configure_Case/H3C_UR_Web_CE_Video-Long/22/

17.2 配置案例

表17-2 配置案例名称和链接

名称	链接
端口映射典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1754

IPsec VPN 典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1755
L2TP VPN 典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1756
小贝 AP 管理典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1757
Portal 认证典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1758
防火墙典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1759
策略路由典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1760
应用控制典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1761
网址控制典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1762
如何连接云平台典型配置举例	http://www.h3c.com/cn/home/qr/default.htm?id=1763

18 附录 - 命令行设置

说明

不同款型的设备对本功能的支持情况不同，请以设备的实际情况为准。

您可以在局域网内通过 Console 口或 Telnet 本地登录路由器进行命令行设置。

- 通过 Console 口本地登录：需要您先搭建配置环境，相关操作请参见“通过 Console 口搭建配置环境”。
- 通过 Telnet 本地登录：请先确保管理计算机与路由器之间网络连通。然后在管理计算机上单击屏幕左下角<开始>按钮进入“开始”菜单。选择[运行]，在弹出的“运行”对话框中输入“telnet *ip-address*”（*ip-address* 为路由器 LAN 口的 IP 地址）。回车后按界面提示输入用户名和密码（缺省情况下，两者均为 admin）即可登录路由器进行设置，具体命令行介绍请参见“命令行在线帮助”。

路由器为您提供以下简单的命令行维护。

表18-1 命令行索引

命令行	请参见
display ip address	查看路由器LAN口的IP地址
display sysinfo	显示路由器系统资源使用情况
display version	显示路由器软件/硬件版本信息

命令行	请参见
ping	网络连通性测试
quit	退出当前视图
reboot	重新启动路由器

18.1 通过Console口搭建配置环境

1. 连接管理计算机到路由器

将管理计算机的串口通过配置线缆与路由器的 Console 口相连。

2. 设置终端参数

在通过 Console 口搭建本地配置环境时，需要通过超级终端或 PuTTY 等终端仿真程序与设备建立连接。用户可以运行这些程序来连接网络设备、Telnet 或 SSH 站点，这些程序的详细介绍和使用方法请参见该程序的使用指导。

打开 PC，在 PC 上运行终端仿真程序，并设置终端参数。参数设置要求如下：

- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

18.2 命令行在线帮助

(1) 在任一视图下，键入<?>获取该视图下所有的命令及其简单描述。

```
<System> ?
 ping                ping function
 display             display system information
 quit                quit current view
 reboot              reboot the system
```

(2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。

```
<System> display ip ?
 address        Display IP addresses
```

(3) 键入一字符串，其后紧接<?>，列出以该字符串开头的所有命令。

```
<System> di?
 display
```

(4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。

```
<System> di  ←按下<Tab>键
<System> display
```

18.3 命令行操作

18.3.1 查看路由器 LAN 口的 IP 地址

输入 **display ip address** 命令并回车，即可显示路由器 LAN 口的 IP 地址信息。

18.3.2 显示路由器系统资源使用情况

输入 **display sysinfo** 命令并回车，显示路由器的 CPU 和内存使用情况。

18.3.3 显示路由器软件/硬件版本信息

输入 **display version** 命令并回车。

18.3.4 网络连通性测试

输入 **ping** * *host* [**-c** *count*] [**-i** *interface-name*] [**-s** *packet-size*]

表18-2 Ping 命令参数项描述

参数	描述
host	目的端的IP地址或主机名，主机名为1～31个字符的字符串
-c *count*	指定ICMP回显请求报文的发送次数，取值范围为1～4294967295，缺省值为4
-i *interface-name*	指定发送ICMP回显请求报文的路由器接口名称。不指定该参数时，将根据目的IP查找路由表或者转发表来确定发送ICMP回显请求报文的接口
-s *packet-size*	指定发送的ICMP回显请求报文的长度（不包括IP和ICMP报文头），取值范围为20～8100，单位为字节，缺省值为56字节

18.3.5 退出当前视图

输入 **quit** 命令并回车。

18.3.6 重新启动路由器

输入 **reboot** 命令并回车，确认后，路由器将重新启动。