RG-EG 系列路由设备

ReyessOS 1.95 Web 管理手册

文档版本 V1.0

归档日期 2022-02-17

版权声明

免责声明

前　言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷睿易官方网站：https://www.ruijiery.com/
- 锐捷睿易在线客服：https://ocs.ruijie.com.cn/?p=smb
- 锐捷网络官方网站服务与支持版块：https://www.ruijie.com.cn/service.aspx
- 7天无休技术服务热线：4001-000-078
- 常见问题搜索：https://www.ruijie.com.cn/service/know.aspx
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络文档支持与反馈信箱：doc@ruijie.com.cn
- 锐捷网络服务公众号：【锐捷服务】扫码关注

本书约定

1. 图形界面格式约定

界面图标	解释	举例
<>	按钮	<确定>
[]	菜单项，弹窗名称，页面名称，标签页的名称	菜单项“系统设置”可简化[系统设置]
>>	分级页面，子菜单项	选择[系统设置]>>[系统管理员]
“”	配置项，提示信息，链接	如提示框提示“保存配置成功” 点击“开启”选项 点击“忘记密码”链接

2. 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

表示用户必须严格遵守的规则。如果忽视此类信息，可能导致数据丢失或设备损坏。

注意

表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。

说明

用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。

产品/版本支持情况

用于提供产品或版本支持情况的说明。

3. 说明

本手册中展示的部分信息（如产品型号、描述、端口类型、软件界面等）仅供参考，具体信息请以实际使用的产品版本为准。

文档修订记录

修订日期	修订版本号	修订描述	修订人

1 登录设备

1.1 配置环境要求

1.1.1 PC 的要求

- 浏览器：支持Google chrome、IE9.0、IE10.0、IE11.0以及部分基于谷歌/IE内核的浏览器（如360安全浏览器，推荐使用极速模式）。使用其它浏览器登录Web管理时，可能出现乱码或格式错误等异常。

1.2 缺省配置

表1-1 缺省 Web 配置

功能特性	缺省值
设备IP	192.168.110.1
用户/密码	首次登录时无需账号密码，可直接开始配置

1.3 使用 PC 登录 Web

1.3.1 连接设备

将管理客户端与设备建立网络连接才能进入管理页面完成网关配置。连接设备可选择以下两种方式。

- 有线方式

将设备LAN口与电脑网口相连，设置电脑IP地址，请参考1.3.2 章节。

- 无线方式

将设备LAN口与AP上联口相连，AP上电后，通过手机或笔记本电脑，搜索Wi-Fi名称为@Ruijie-mXXXX的无线网络，XXXX为设备的MAC地址后四位。MAC地址可在网关设备底部查看。以无线方式连接设备不需要设置管理客户端的IP地址，跳过1.3.2 步骤。

1.3.2 配置管理客户端 IP

为管理客户端配置一个与设备默认IP（设备默认IP地址：192.168.110.1，子网掩码：255.255.255.0）在同一网段的IP地址，使管理客户端能够访问设备。如设置管理客户端的IP地址为192.168.110.200。

1.3.3 登录 Web

(1) 在浏览器地址栏中输入设备的IP地址（默认192.168.110.1），进入登录页面。

> 说明
>
> 若用户修改了设备的静态IP地址，或者设备动态获取到了新的IP地址，只要保证管理计算机和设备处于同一局域网，且IP地址处于同一网段，就可以使用新的IP地址访问设备的Web管理系统。

(2) Web输入密码后点击<登录>，进入Web管理系统首页。

首次登录Web管理系统时无需账号密码，可直接开始配置。

为了保障设备安全，建议在首次登录Web管理系统后及时设置管理密码。设置密码后，再次登录Web管理系统时需要输入密码才能访问设备。

若忘记IP或密码，可在设备接通电源的情况下长按设备面板上的reset键5秒以上使设备恢复出厂设置，恢复后即可使用默认IP和密码登录。

注意

恢复出厂设置将删除已有配置，再次登录需重新配置，请谨慎操作。

1.4 工作模式介绍

设备的工作模式分为路由模式和AC模式，不同的工作模式下系统菜单页面和配置功能范围有所不同。EG设备默认处于路由模式。如需修改工作模式请参考3.1 。

1.4.1 路由模式

设备支持NAT路由转发以及VPN、行为管理等路由功能。可为下联设备分配地址，网络数据经设备路由转发，并支持NAT转换。

路由模式下设备支持PPPoE拨号、动态IP和静态IP三种方式联网，可直接连接入户网线或上级设备提供网络，并对下联设备进行管理。

1.4.2 AC 模式

设备做二层转发，无路由及DHCP服务器功能，WAN口默认通过DHCP方式获取地址。适用于当前网络已正常工作的场景，AC模式下设备作为设备管理控制器，可通过旁挂方式接入网络，对AP进行管理。

1.5 上网设置（路由模式）

1.5.1 配置前的准备

(1) 设备连接电源，用网线将设备WAN口与上级设备连接，或直接连接入户网线。

(2) 上网模式需根据当地网络运营商的要求进行配置，否则可能设置失败导致无法上网。建议先联系当地网络运营商确认上网方式：

- 确认上网方式是动态IP方式、宽带方式还是静态IP方式。
- 如果是宽带上网，则需要宽带账号和宽带密码。
- 如果是静态IP，则需要IP地址、子网掩码、网关和DNS。

1.5.2 配置步骤

1. 添加设备至网络

出厂配置下，用户可以对组网中所有设备进行批量设置和集中管理，因此在开始配置前，需要查看并确认全网在线设备的数量和网络状态。

说明

一般情况下，多台新设备上电接入（例如接在PoE交换机下）会自动互联成一个网络，用户只需要确认设备数量无误即可。

若网络中存在未加入当前网络的其他设备，可以点击<添加到我的网络>并输入所添加设备的管理密码，将对应设备手动添加至设备所在网络中，再开始全网配置。

2. 创建网络项目

点击<开始配置>，设置设备的联网方式和管理密码等。

(1) **项目名称**：用于标识设备所在的网络。

(2) **上网方式**：选择与运营商确认的上网方式。

- **动态IP方式**：设备默认检测DHCP能否获取地址上网，若成功联网，则无需输入账号。
- **宽带上网方式**：PPPoE拨号上网，输入已准备好的宽带账号和宽带密码。
- **静态IP方式**：输入已准备好的IP地址，掩码，网关IP地址和DNS服务器地址。

(3) **管理密码**：设置登录管理页面的密码。

(4) **国家码**：请选择实际所在的国家或地区。

(5) **时区**：设置系统时间，默认开启网络时间服务器提供时间服务。请选择实际所在的时区。

点击<创建项目并连通网络>，设备将下发初始化相关配置，并检测网络。完成快速配置后，新设备已联网，可继续将设备绑定云端账号，进行远程管理，具体操作请参考页面指引登录诺客云平台进行配置。

说明

- 若您的网络暂未联网，可以点击页面右上角<退出>，先退出配置向导。
- 修改管理密码后需要重新访问设备管理地址，使用新密码登录设备。

1.5.3 忘记宽带账号密码的解决方案

(1) 请联系当地运营商咨询。

(2) 如果是旧设备替换为新设备，可以点击<从旧设备中获取账号密码>。将旧路由器和新路由器插电启动。用网线一头插入旧路由器的WAN口，另一头插入本设备的LAN口，点击<开始获取>，若获取成功则配置页面将自动填入旧设备宽带上网的账号和密码。点击<保存>即可生效。

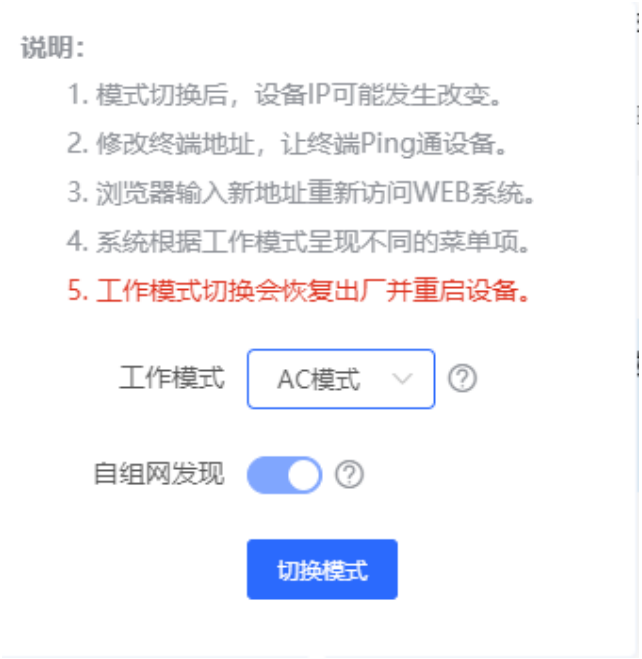
1.6 上网设置（AC 模式）

1.6.1 配置前的准备

- 设备连接电源，用网线将设备网口与上级设备连接
- 确认上级设备能够正常上网，当前网络已联网。

1.6.2 配置步骤

(1) 在工作模式设置页面，切换路由模式为AC模式。请参考3.1 章节。



(2) 切换模式后，设备将重启。重启后，设备WAN口默认通过DHCP方式获取地址，以动态IP方式接入网络。上网方式可保持默认的动态IP，或者手动为WAN口设置一个静态IP地址，请参考1.5.2 章节。

1.7 切换管理页面

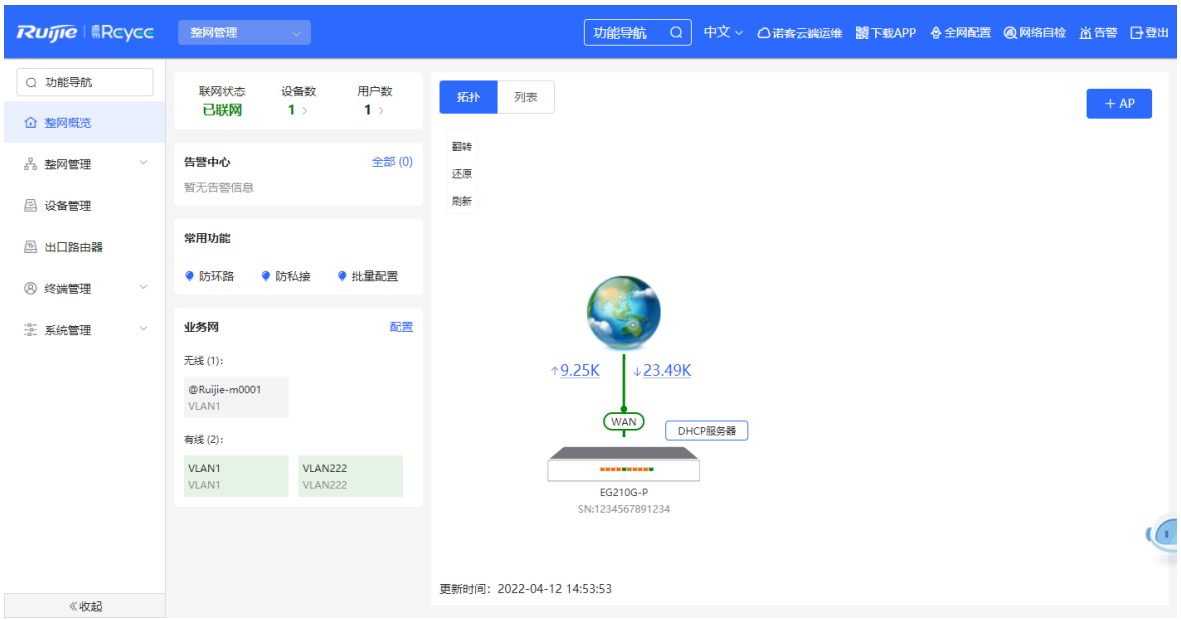
关闭自组网发现（出厂默认开启，详见3.1 修改工作模式），Web页面处于本机管理模式；

开启自组网发现，Web页面可在整网管理页面与本机管理页面间切换。点击导航栏中当前管理模式，在下拉框中选择模式进行切换。

整网管理：查看网络中所有设备的管理信息，基于整网视角对当前网络中的所有设备进行配置；

本机管理：仅对当前登录设备进行配置。

整网管理页面：



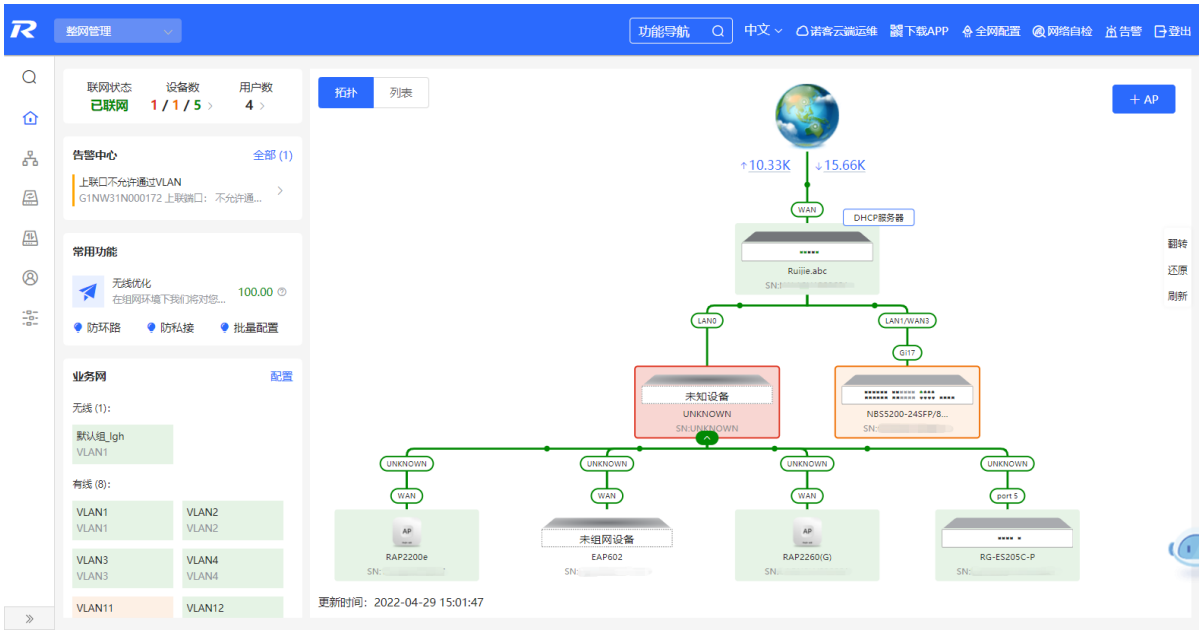
本机管理页面：


Ruijie | Rcycc
本机管理(EG210G)
中文
诺客云端运维
下载APP
全网配置
网络自检
告警
登出
设备概览
基本管理
安全管理
行为管理
VPN管理
高级管理
故障诊断
系统管理
收起
设备概况
内存使用率
30%
在线用户数
1
联网状态： 已联网
系统运行： 59 分 7 秒
系统时间： 2022-04-12 15:51:51
设备详细信息
设备型号： EG210G-P
MAC地址： 58:69:6C:00:00:01
硬件版本： 1.00
设备名称： Ruijie
工作模式： 路由模式
软件版本： ReyeeOS 1.86.1608
SN号： 1234567891234
自组网角色： 主AC
端口信息
已连接
未连接
LAN0
LAN1
LAN2
LAN3
LAN4
LAN5
LAN6
LAN7
WAN1
WAN
192.168.110.1
172.26.30.192

2 整网监控

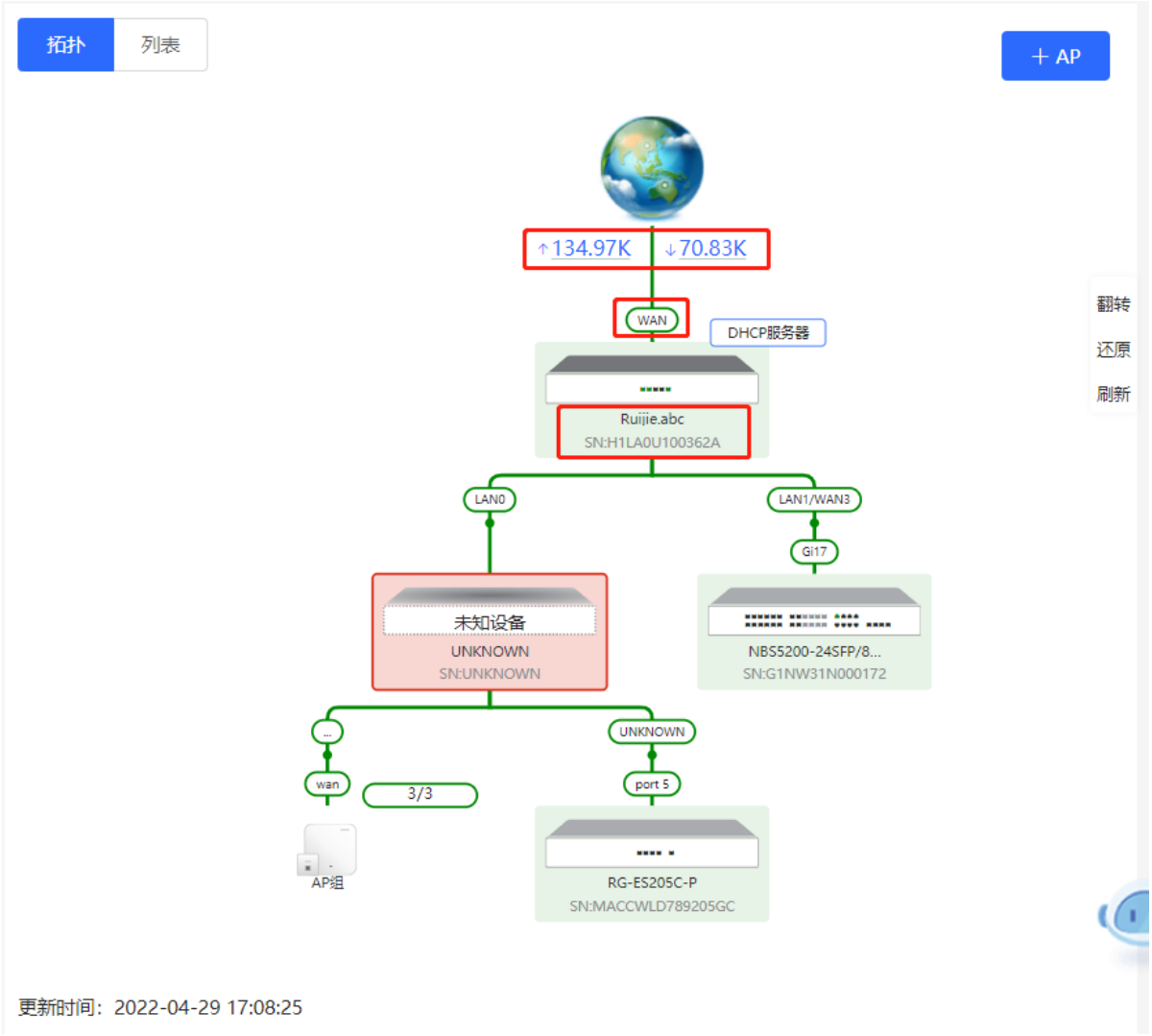
【整网管理-页面向导】整网概览

整网概览页面可视化地展现了当前网络的拓扑结构、上下行实时流量、联网状态、用户数等信息，并提供了网络与设备的快捷设置入口。用户可以在当前页面对整网的网络状态进行监控、配置与管理。

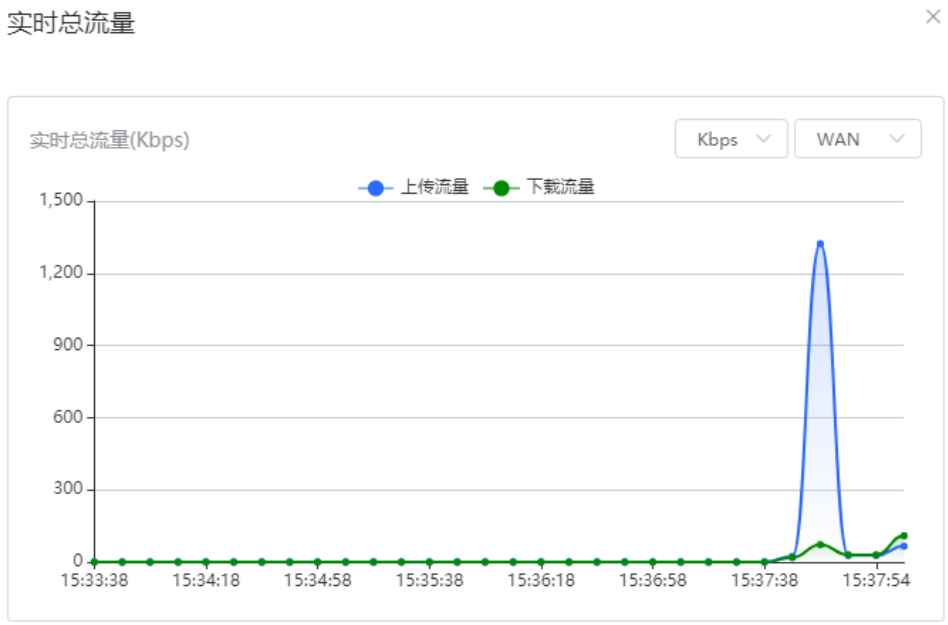


2.1 查看组网信息

组网拓扑图包含了在线设备、连接端口号、设备SN号和上下行实时流量等信息。

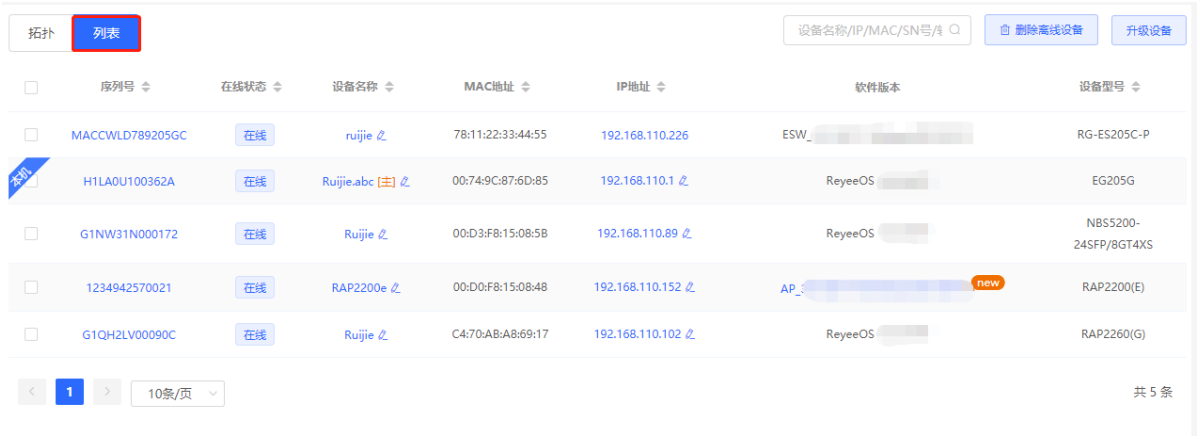


- 点击流量数据，可查看实时总流量信息。

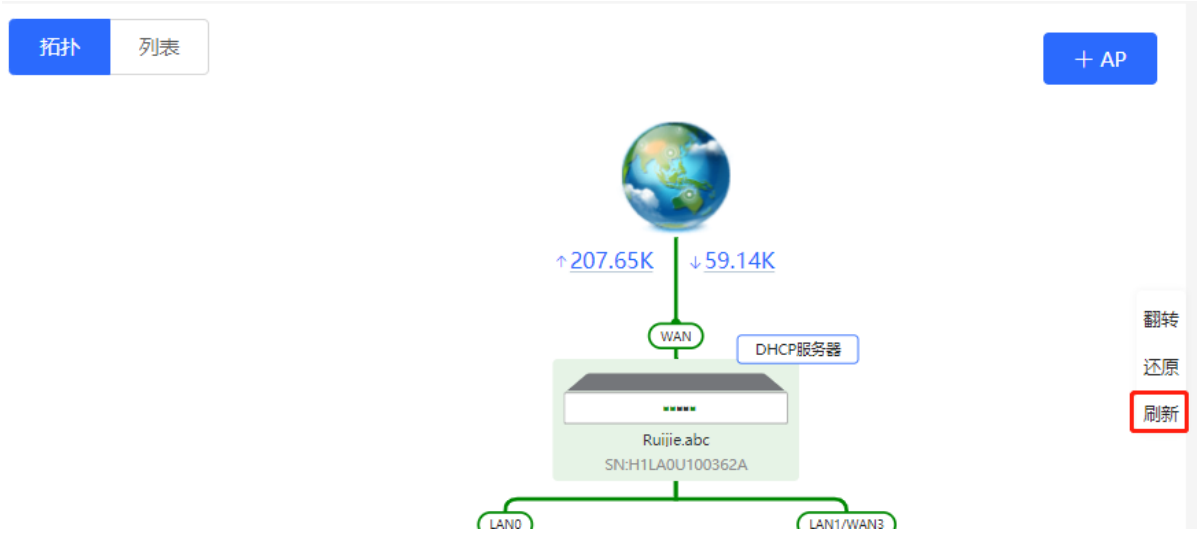


- 点击拓扑中的设备，可查看设备的运行状态和配置信息，并对设备功能进行配置。设备名称默认为产品型号，点击 可将设备名称修改为便于区分的描述信息。

- 点击拓扑左上角的“列表”切换至设备列表视图，可查看当前组网中的设备信息。点击表项，可进行单独配置管理。



- 拓扑图左下角为该拓扑的更新时间。点击“刷新”可更新拓扑图为最新状态。更新拓扑数据需要一定时间，请耐心等待。

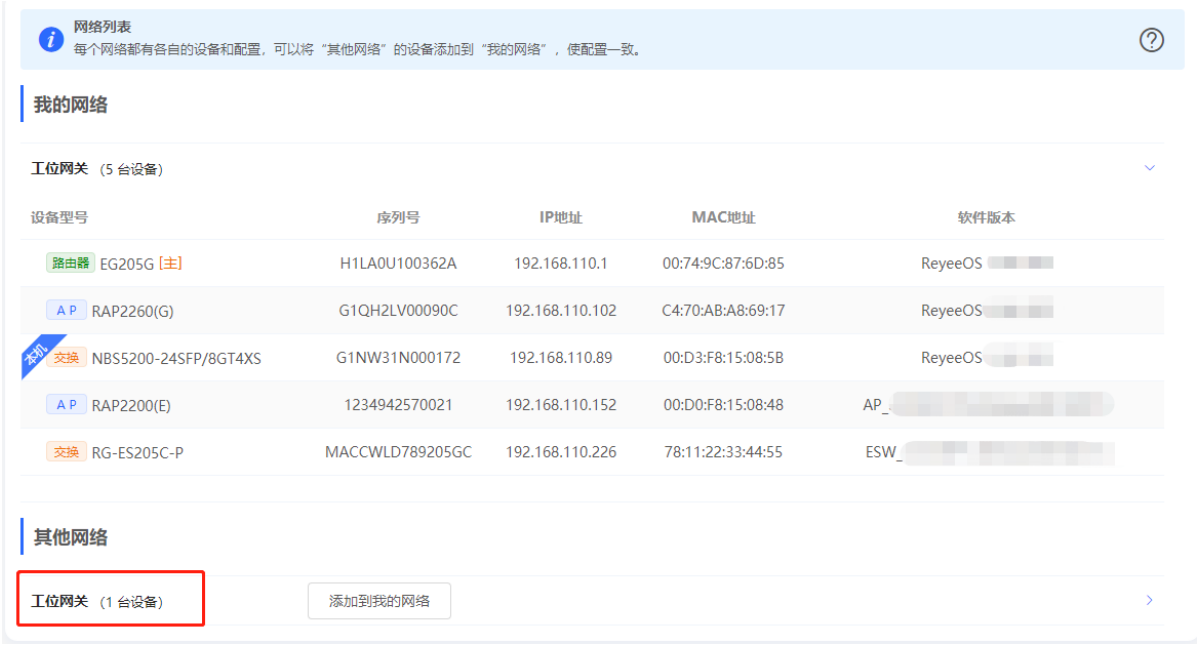


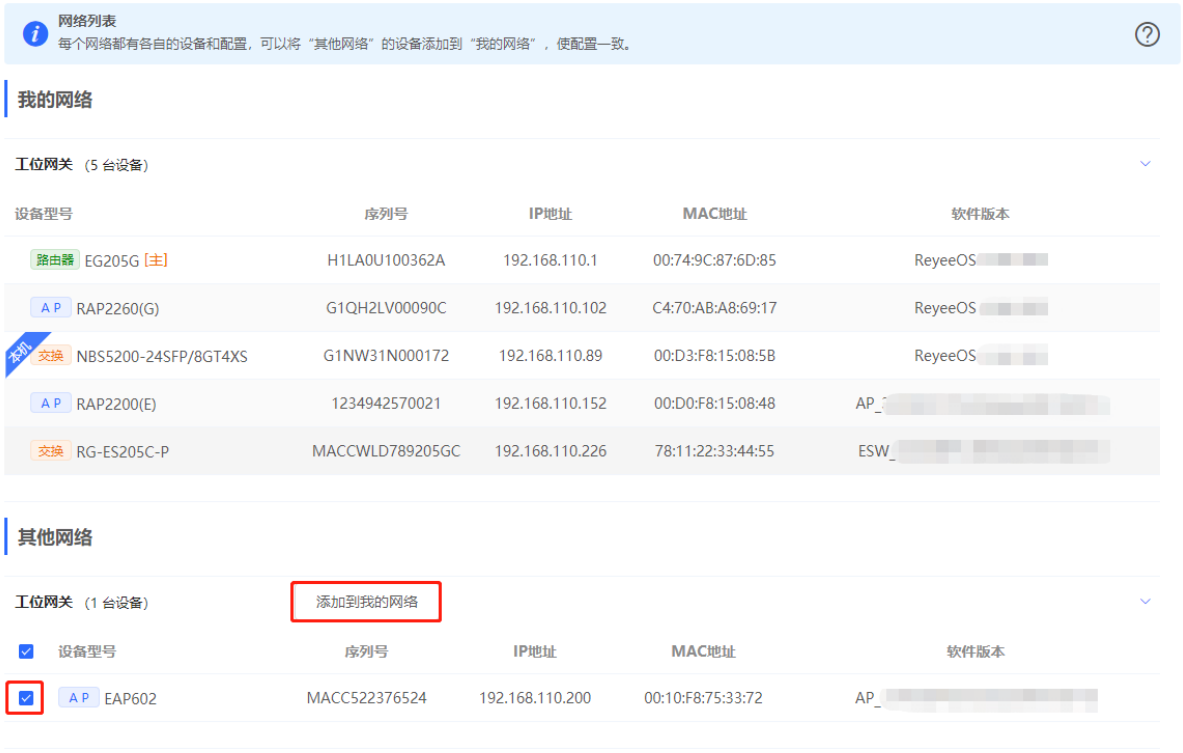
2.2 添加组网设备

2.2.1 有线连接

(1) 新设备以有线方式连接网络中的设备时，系统将弹出提示信息，提示网络中出现未组网的其他网络设备，并在页面左上角“设备数”中显示（橙色数字表示发现的未组网设备数量），点击“点击去处理>>”可设置加入当前网络。

(2) 跳转到网络列表页面后，点击展开“其他网络”中的信息，勾选待添加的设备，点击<添加到我的网络>。





(3) 添加出厂新设备不需要输入密码，而添加有密码的设备需要输入该设备的管理密码。密码错误将添加失败。

2.2.2 AP Mesh

对于支持AP Mesh易联功能的AP，上电后无需连线，可直接通过易联方式添加到当前组网中，与其他无线设备进行Mesh组网，并自动同步Wi-Fi配置。

注意

当前网络需开启易联功能（参考4.10 ）才可以扫描到AP，AP需在附近上电，距离太远或有障碍物遮挡将导致AP无法被扫描到。

(1) 新AP上电后放置在已有AP附近（能够接收到AP的Wi-Fi信号），登录组网中的设备，在整网概览页面点击拓扑右上角的<+AP>，扫描周围不属于当前网络且未接网线的AP。

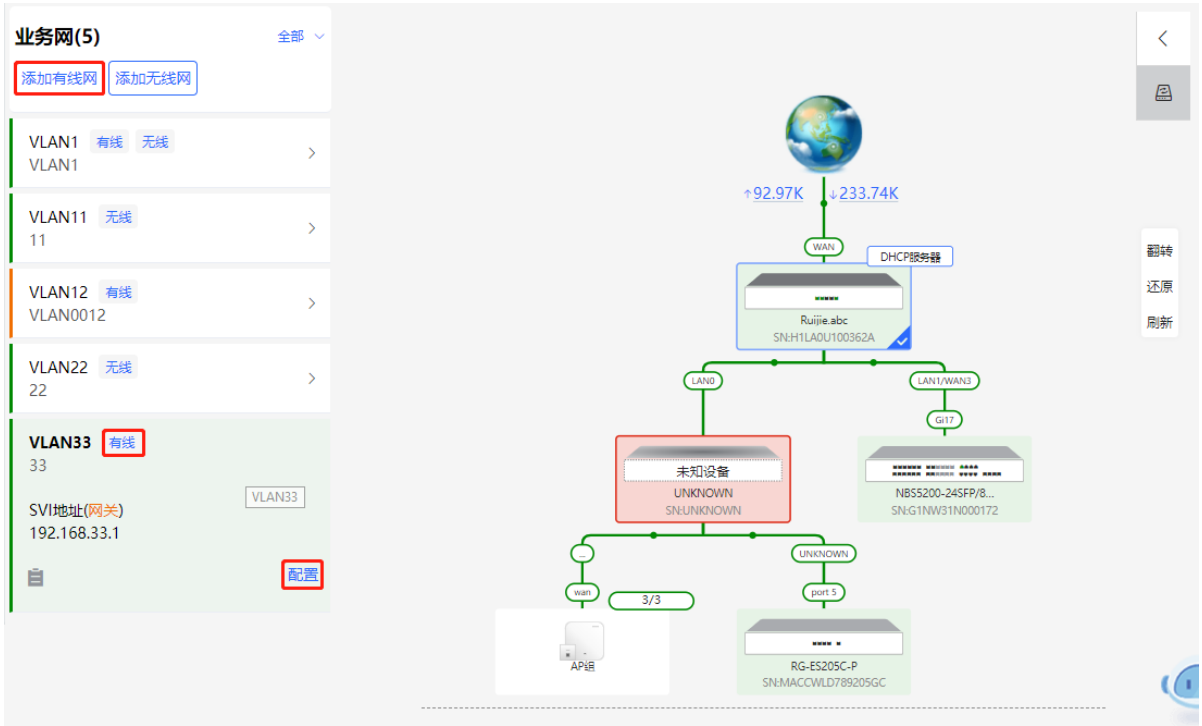
(2) 选择需要添加的AP，添加至当前网络。添加新设备不需要输入密码，添加有密码的设备需要输入该设备的管理密码。

2.3 设置业务网

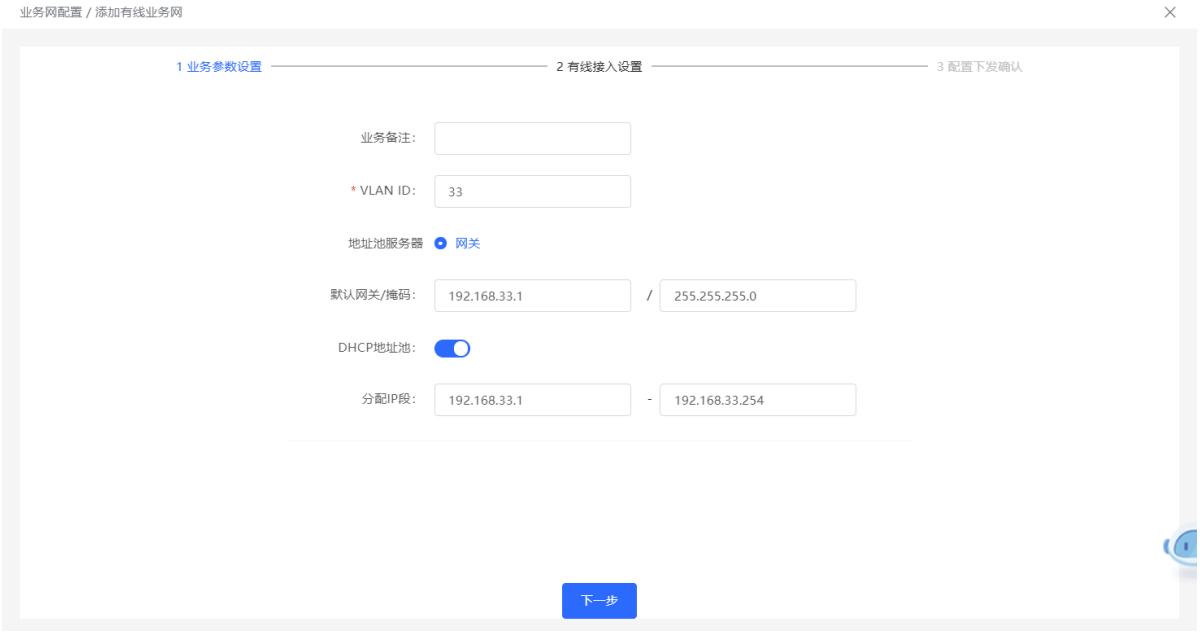
整网概览页面左下方显示当前网络中的无线网络和有线网络配置。点击“配置”可跳转至业务网配置页面（整网管理>>业务网）。

2.3.1 设置有线网

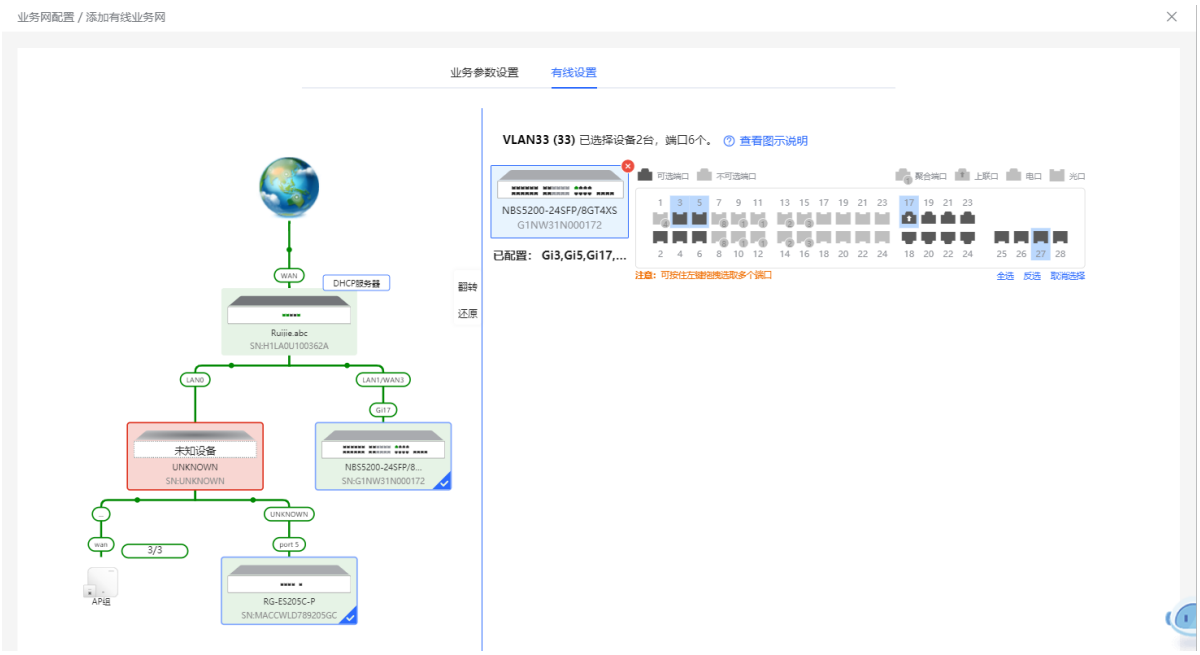
(1) 点击“添加有线网”为当前网络添加有线网络配置，或选择已创建的有线网络VLAN，点击“配置”进行修改。



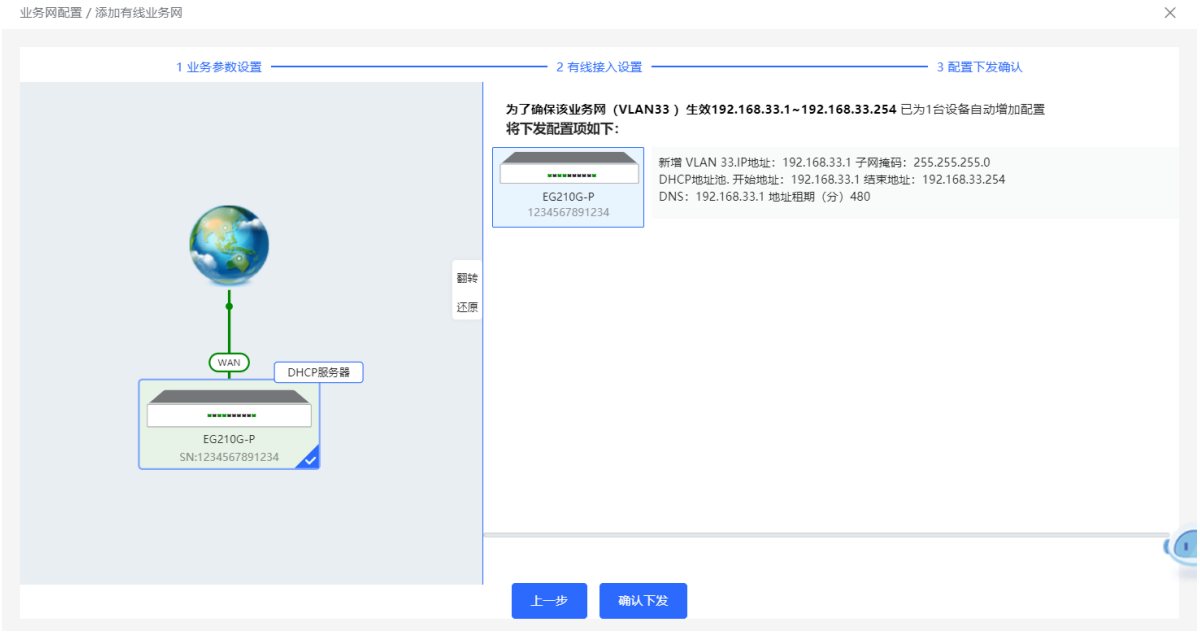
(2) 设置用于有线接入的VLAN、该VLAN下接入终端的地址池服务器以及是否创建新的DHCP地址池。默认网关设备作为地址池服务器为接入终端分配地址，当组网中存在接入交换机，可选择交换机作为地址池服务器。完成业务参数设置后，点击<下一步>。



(3) 在拓扑中选择需要配置的交换机，并选择VLAN所包含的交换机端口，点击<下一步>。

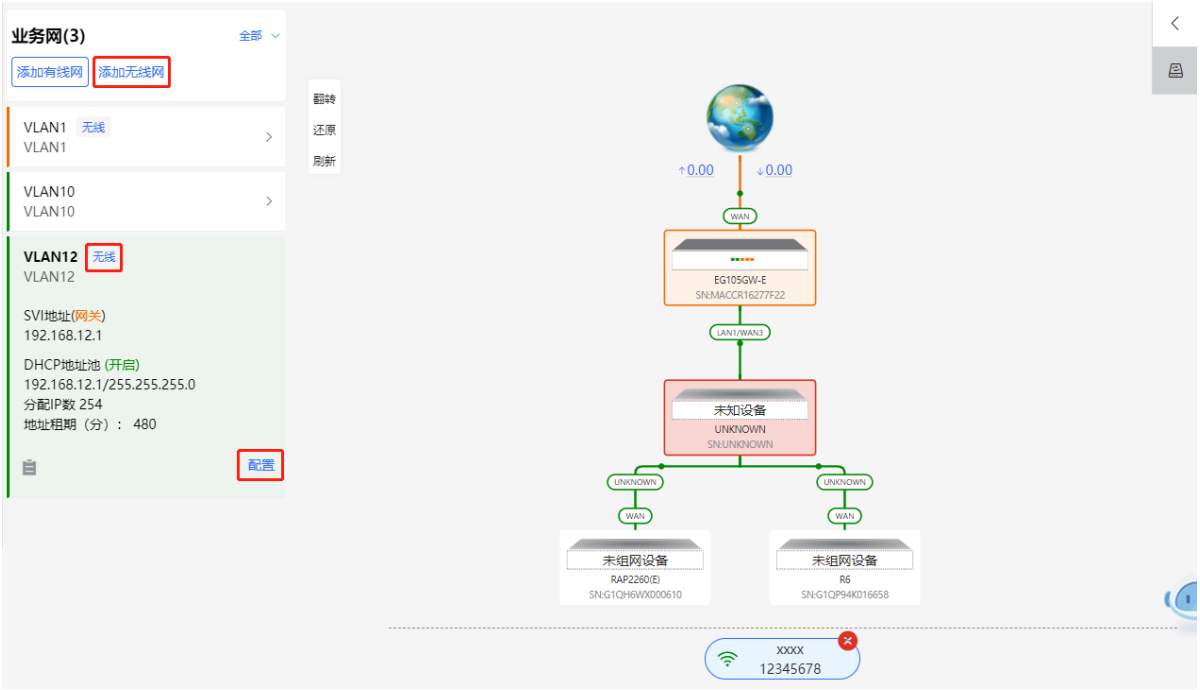


(4) 请确认将下发的配置项是否正确，确认无误后点击<确认下发>，稍等片刻等待配置生效。

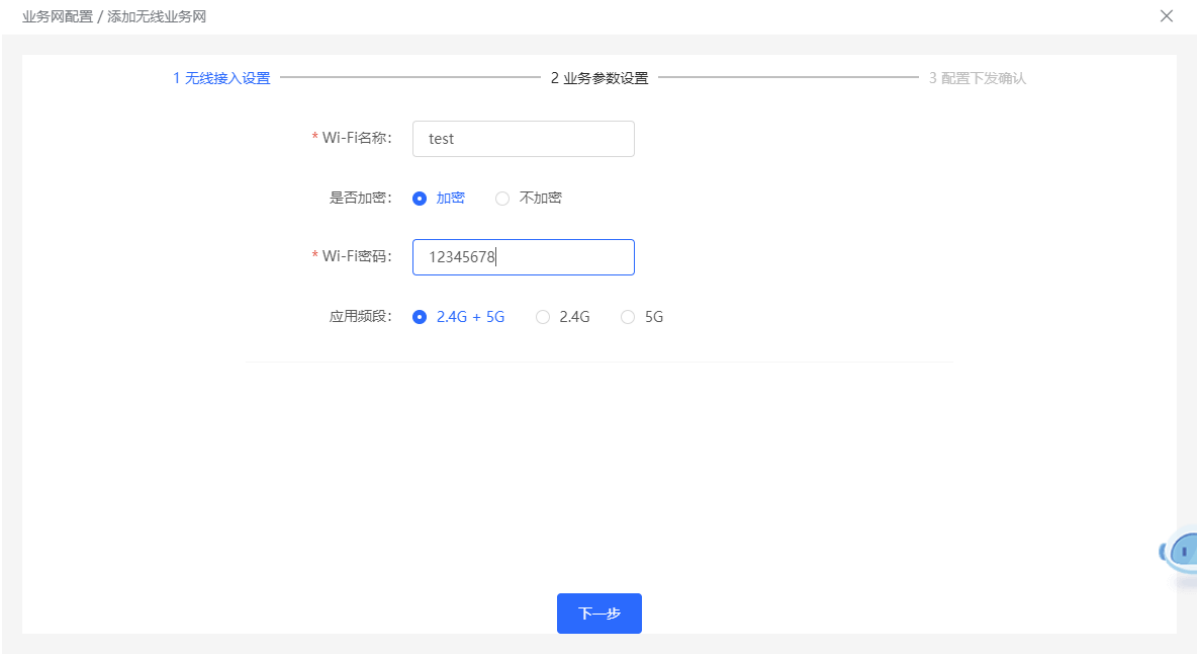


2.3.2 设置无线网

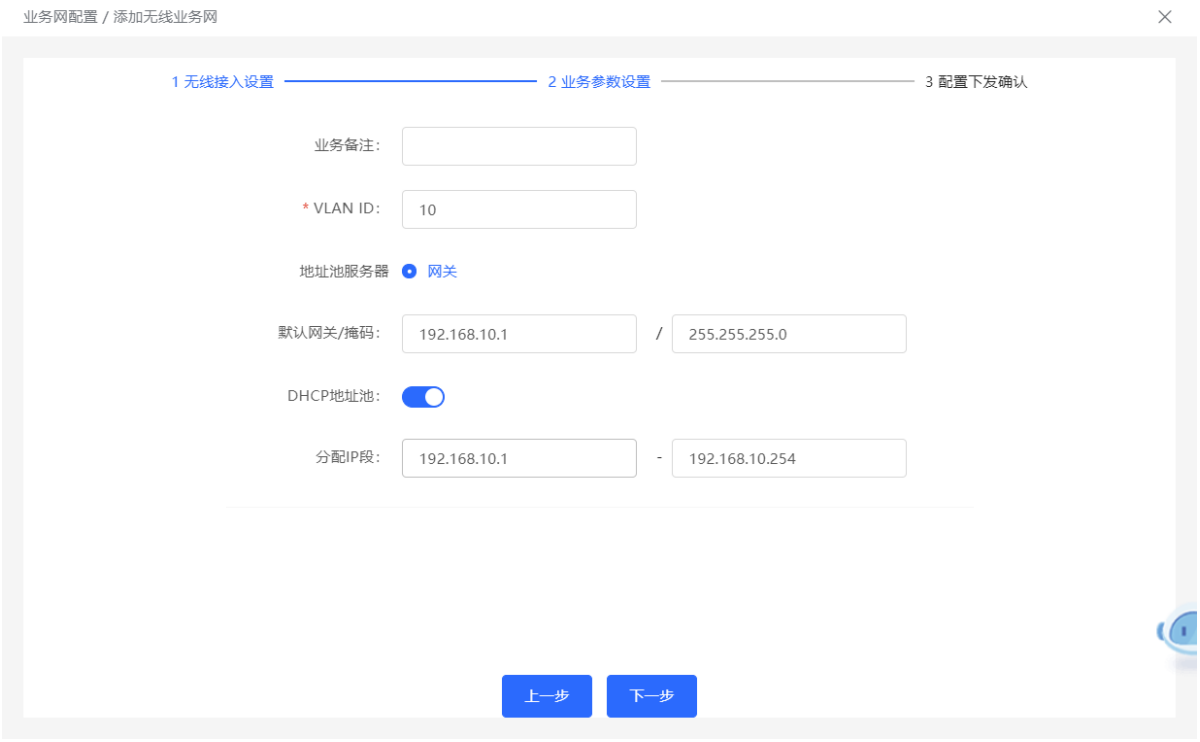
(1) 点击“添加无线网”为当前网络添加无线网络配置，或选择已创建的无线网络VLAN，点击“配置”进行修改。



(2) 设置Wi-Fi名称、Wi-Fi密码和应用频段。点击<下一步>。



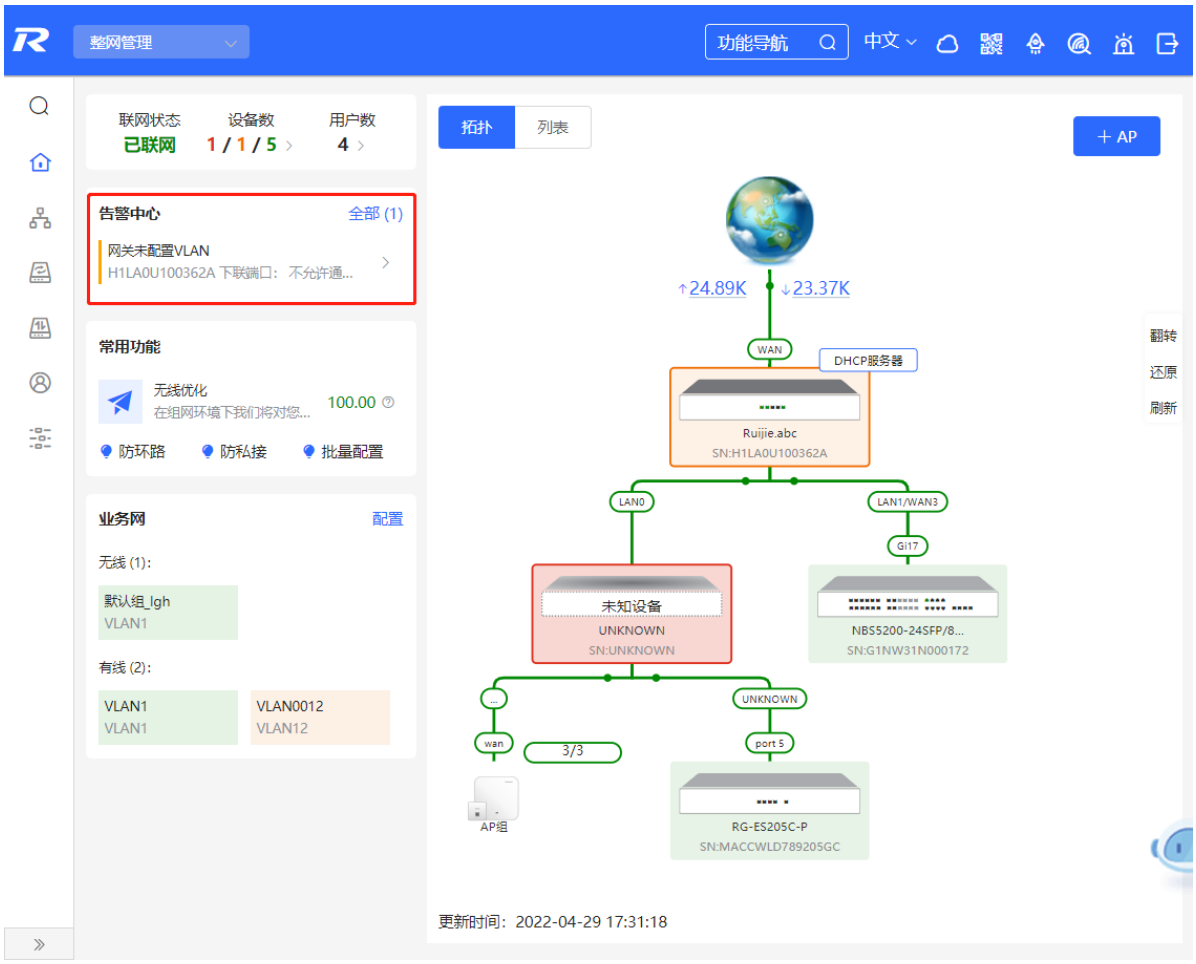
(3) 设置用于无线接入的VLAN、该VLAN下接入终端的地址池服务器以及是否创建新的DHCP地址池。默认网关设备作为地址池服务器为接入终端分配地址，当组网中存在接入交换机，可选择交换机作为地址池服务器。完成业务参数设置后，点击<下一步>。



(4) 请确认将下发的配置项是否正确，确认无误后点击<确认下发>，稍等片刻等待配置生效。

2.4 告警信息处理

当网络存在异常，整网概览页面将对异常信息进行告警提示，并给出相应解决方案。点击“告警中心”的告警提示，可查看故障设备、问题详情及解决方案，请参考解决方案进行故障排查与处理。


整网管理
功能导航
中文
联网状态
已联网
设备数
1 / 1 / 5
用户数
4
拓扑
列表
+ AP
告警中心
全部 (1)
网关未配置VLAN
H1LA0U100362A 下联端口：不允许通...
常用功能
无线优化
在组网环境下我们将对您...
100.00
防环路
防私接
批量配置
业务网
配置
无线 (1):
默认组_lgh
VLAN1
有线 (2):
VLAN1
VLAN1
VLAN0012
VLAN12
↑24.89K
↓23.37K
WAN
DHCP服务器
Ruijie.abc
SN:H1LA0U100362A
LAN0
LAN1/WAN3
Gi17
未知设备
UNKNOWN
SN:UNKNOWN
NBS5200-24SFP/8...
SN:G1NW31N000172
UNKNOWN
wan
3/3
port 5
AP组
RG-ES205C-P
SN:MACCWLD789205GC
翻转
还原
刷新
更新时间：2022-04-29 17:31:18


整网管理
联网状态
已联网
设备数
1 / 1 / 5
用户数
4
告警中心
全部 (1)
网关未配置VLAN
H1LA0U100362A 下联端口：不允许通...
常用功能
无线优化
在组网环境下我们将对您...
100.00
防环路
防私接
批量配置
业务网
配置
无线 (1):
默认组_lgh
VLAN1
有线 (2):
VLAN1
VLAN1
VLAN0012
VLAN12
告警信息
当前告警
H1LA0U100362A 下联端口：LAN1/WAN3 不允许通过vlan12
解决方案：
请配置LAN口网段。
翻转
还原

3 网络设置

3.1 修改工作模式

3.1.1 工作模式

相关介绍请参考1.4 工作模式介绍。

3.1.2 自组网发现

在设置工作模式的同时，可以设置是否开启自组网发现功能。默认开启。

开启自组网发现功能，设备能够在网络中被发现和发现网络中其他设备，设备间根据设备状态进行自组网并同步全局配置。登录设备的Web管理页面，可以查看到整网设备的管理信息。开启后能够帮助用户更高效地对当前网络进行运维和管理，建议保持开启。

关闭自组网发现功能，设备在网络中将不被发现，此时设备作为独立模式运行。登录Web后只能对当前登录设备进行配置和管理。若仅配置单台设备，或不希望设备被同步全局配置，可关闭自组网发现功能。

说明

- AC模式默认开启自组网发现。
- 开启自组网发现，可在设备信息页面查看设备的自组网角色。
- 开启和关闭自组网发现功能，设备Web页面菜单项可能存在差异（详见1.7 ），请参考配置步骤中的页面向导说明查找具体功能的配置入口。

3.1.3 配置步骤

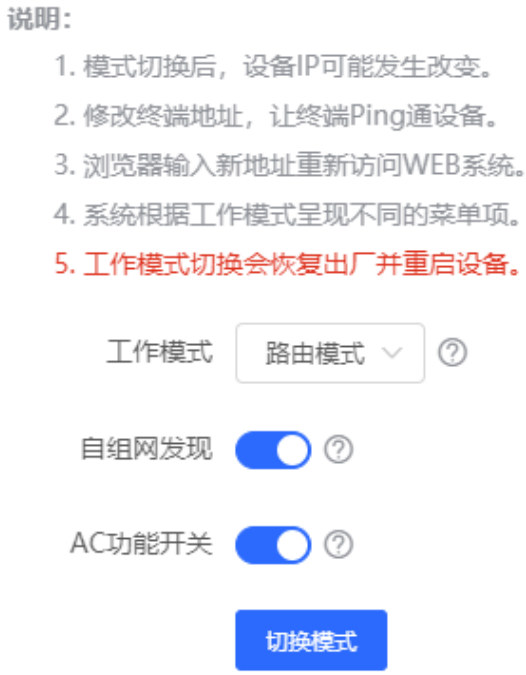
【本机管理-页面向导】设备概览>>设备详细信息

点击当前工作模式可进行修改。

注意

切换工作模式会恢复出厂并重启设备，请谨慎操作。

AC功能开关：若设备为路由模式并开启自组网发现功能，可设置AC功能开关。开启AC功能后，路由模式的设备具备虚拟AC功能，可以管理下联设备。关闭时，设备需通过自组网选举为AC才能管理下联设备。



3.1.4 查看自组网角色

【本机管理-页面向导】设备概览>>设备详细信息

开启自组网发现，可在设备信息页面查看设备的自组网角色。

主AP/AC：设备作为AC可管理下联设备。

从AP：设备已通过自组网接入AC管理。从AP受主AP/AC统一管理，部分无线网络设置不支持本地单独修改，由主AP/AC下发。

3.2 设置 WAN 口

【本机管理-页面向导】基本管理>> WAN设置

设备支持配置多线路接入，允许多条链路同时工作。切换到多线路后，除设置各WAN口的基本网络参数外，还可以设置线路的出口运营商和负载均衡模式。

注意

线路数量的支持情况在不同产品上存在差异，请以实际为准。

3.2.1 设置上网方式

【本机管理-页面向导】基本管理>> WAN设置>> 单线路/双线路/三线路/四线路

提供三种方式接入广域网：静态IP、动态IP和PPPoE拨号，请根据实际宽带线路类型进行选择，参考1.5 上网设置（路由模式）。

3.2.2 修改 MAC 地址

【本机管理-页面向导】基本管理>> WAN设置>> 单线路/双线路/三线路/四线路>> 高级设置

有时运营商出于安全性考虑，限制未知MAC地址的设备入网，此时可以将WAN口的MAC地址修改成有效的MAC地址。

点击展开高级设置，输入MAC地址，点击<保存>。无特殊情况不需要更改默认MAC地址。

3.2.3 修改 MTU

【本机管理-页面向导】基本管理>> WAN设置>> 单线路/双线路/三线路/四线路>> 高级设置

WAN口的MTU表示WAN口允许通过的最大传输单元，默认为1500字节。有时运营商网络会限制大数据包的速度或禁止大数据包通过，导致网络速度不理想甚至断网，此时可调小MTU值。

3.2.4 设置专用线路

【本机管理-页面向导】基本管理>> WAN设置>> 单线路/双线路/三线路/四线路>> 高级设置

点击<是否专线>按钮，设置当前WAN线路是否为专用网络线路。专线一般用于访问特定的内部网络，无法访问互联网，拥有更高的网络安全性。

3.2.5 设置 VLAN 标签

【本机管理-页面向导】基本管理>> WAN设置>> 单线路/双线路/三线路/四线路>> 高级设置

部分运营商会要求接入网络时需要携带VLAN ID，则可以开启本功能并为WAN口设置VLAN ID。默认关闭VLAN标签功能。无特殊情况建议保持关闭。

3.2.6 设置运营商地址库选路

【本机管理-页面向导】基本管理>>WAN设置>>双线路/三线路/四线路>>运营商/负载设置>>运营商设置

多线路情况下，开启地址库选路并设置各线路的出口运营商后，数据流将按运营商地址库自动选路，达到如“电信数据走电信、联通数据走联通”的效果，避免跨运营商访问，实现更快速的网络访问。

3.2.7 设置多链路负载模式

【本机管理-页面向导】基本管理>> WAN设置>> 双线路/三线路/四线路>> 运营商/负载设置>> 多链路负载模式设置

多线路情况下，在根据地址库选路后，剩余流量将根据负载模式进行分配。

表3-1 负载模式说明

负载模式	说明
均衡模式	流量按WAN口的权重值比例分配，权重值越高，所分配的流量越大。 选择本模式时需要同时指定各WAN口权重。 例如：双线路下WAN口和WAN1口的权重分别设置为3和2，则流量按照3:2比例分配，WAN分配60%，WAN1分配40%
主备模式	主接口工作正常时，流量全部走主接口；主接口发生故障时，流量自动切换到备接口 选择本模式时需要指定各WAN口为主/备接口，多个主/备接口时，需设置接口权重（同均衡模式说明）

指定负载模式为均衡模式后，可以配置链路负载均衡的策略。

表3-2 均衡策略说明

均衡策略	说明
基于连接进行均衡	启用后，多链路负载均衡基于连接进行分流。源IP、目的IP、源端口、目的端口和协议都相同的报文属于同一个连接
基于源IP进行均衡	启用后，多链路负载均衡使用源IP作为分流依据，同一个用户（相同源IP）的流会被分配到同一个出口。可避免同一个用户的流量被分流到不同的出口链路，降低网络访问异常风险
基于源IP和目的IP均衡	启用后，多链路负载均衡使用源IP和目的IP作为分流依据，相同源IP和目的IP的流会被分配到同一个出口

3.3 设置 LAN 口

3.3.1 修改 LAN 口地址

【本机管理-页面向导】基本管理>> LAN设置>> LAN设置

点击<修改>，输入IP和对应的掩码，点击<确定>。修改了设备LAN口的IP地址后，需要在浏览器中输入新的IP地址重新登录，才能对设备继续进行配置和管理。

3.3.2 修改 MAC 地址

【本机管理-页面向导】基本管理>> LAN设置>> LAN设置

若局域网内的终端设备为了防止ARP攻击而设置了网关的静态ARP表项（将网关的IP地址与MAC地址绑定），在替换网关设备时，网关IP地址保持不变而MAC地址发生变化，那么终端设备就无法学习到网关的MAC地址。此时除了修改终端的静态ARP表项，还可以将新设备的LAN口MAC地址设置为原设备的MAC地址，使局域网内的终端正常上网。

点击<修改>，输入MAC地址，点击<确定>。无特殊情况不需要更改LAN口的默认MAC地址。

3.4 设置 VLAN

3.4.1 VLAN 简介

VLAN（Virtual Local Area Network，虚拟局域网）是将一个物理的LAN在逻辑上划分为多个广播域的通信技术。每个VLAN具备独立广播域，VLAN内的主机间可以直接通信，而不同VLAN之间是二层隔离的，不能直接互通。与传统以太网相比，VLAN具有以下优点：

- 控制广播风暴：限制广播报文仅在VLAN内部转发，不会影响其它VLAN的性能，节省了带宽。
- 增强局域网的安全性：由于VLAN所划分的广播域，局域网内不同VLAN的报文相互隔离，不同VLAN的用户间不能直接通信，增强了网络的安全性。
- 简化网络的管理：在同一个物理网络下，可以利用VLAN技术划分不同的逻辑网络，当要改变网络拓扑结构时，只需修改VLAN配置。

3.4.2 创建 VLAN

【本机管理-页面向导】基本管理>> LAN设置>> LAN设置

局域网可以划分多个VLAN，点击<添加>按钮，创建VLAN。

表3-3 VLAN 配置信息描述表

参数	说明
IP地址	设置VLAN接口的IP地址。通过当前局域网上网的设备的默认网关应设置为该IP地址
子网掩码	设置VLAN接口的IP地址的子网掩码

参数	说明
VLAN ID	VLAN标识
备注	填写VLAN的描述信息
MAC地址	设置VLAN接口的MAC地址
DHCP服务	设置DHCP服务器功能，开启后局域网内的设备才能自动获取到IP。开启DHCP服务后，需要配置DHCP服务器分配IP的开始地址、分配IP数和地址租期，并支持配置DHCP服务器选项，配置详情请参考3.7.3 配置DHCP服务器。

⚠ 注意

VLAN配置与上联配置有关联，请注意配置。

3.4.3 设置端口 VLAN

【本机管理-页面向导】基本管理>> 端口VLAN

本页面展示了当前端口VLAN划分的情况。请先在LAN设置里创建VLAN（参考3.4.2 创建VLAN），然后在本页面中进行基于VLAN的端口配置。

点击端口下方对应的选项框，在下拉框中选择VLAN与端口的对应关系。

- UNTAG：设置VLAN为端口的Native VLAN，即端口接收到该VLAN的报文时将剥离VLAN标识后转发出去，并且当端口接收到未携带VLAN标识的报文，将为报文打上该VLAN标识，作为该VLAN的报文转发出去。每个端口只能设置一个VLAN为UNTAG。
- TAG：设置VLAN为端口允许通过的VLAN，但不为Native VLAN。即VLAN报文在端口转发时将携带原有VLAN标识。
- 不加入：设置端口不允许该VLAN的报文通过。例如VLAN 10和VLAN 20不加入端口2，则端口2不收发VLAN 10和VLAN 20的报文。

3.5 设置 DNS

3.5.1 本机 DNS

当WAN口使用DHCP协议或PPPoE协议时，设备将自动获取DNS服务器。如果上级设备未下发DNS服务器，或者需要修改DNS服务器，可以手动设置新的DNS服务器。

【本机管理-页面向导】高级管理>>本机DNS

本机DNS服务器：设置本机使用的DNS服务器地址，如果存在多个，中间使用空格隔开

3.5.2 DNS 代理

DNS服务器代理为可选配置，设备默认会从上级设备中获取域名服务器地址。

【本机管理-页面向导】基本管理>> LAN设置>> DNS代理

DNS代理开关：默认关闭，使用运营商下发的DNS。DNS若配置错误，可能出现设备域名解析失败，无法正常访问的情况。建议保持关闭。

DNS服务器：终端设备上网默认自动使用上级设备提供的DNS服务器地址。建议保持默认。开启DNS代理开关后，需要输入DNS服务器IP地址，各地区适用的DNS不同，可咨询当地运营商。

3.6 IPv6 设置

3.6.1 IPv6 简介

IPv6（Internet Protocol Version 6），全称为互联网协议第6版，是互联网工程任务组（IETF）设计的用于替代IPv4的下一代IP协议，用于解决IPv4存在的网络地址资源不足等问题。

3.6.2 IPv6 基础

1. IPv6 地址格式

IPv6的地址长度由IPv4的32位扩展到128位，相较于IPv4拥有更大的地址空间。

IPv6地址的基本格式为X:X:X:X:X:X:X:X，128位的IPv6地址用冒号（:）分隔为8组，每组的16位用4个十六进制字符（0~9，A~F）来表示。其中每个“X”代表一组的4个十六进制数值。

例如：2001:ABCD:1234:5678:AAAA:BBBB:1200:2100，800:0:0:0:0:0:0:1，1080:0:0:0:8:800:200C:417A

其中，对于IPv6地址中的数字“0”可以有如下的简写方式：

- 起始的0可以不必表示。例如2001:00CD:0034:0078:000A:000B:1200:2100可以写为2001:CD:34:78:A:B:1200:2100
- 某些IPv6地址中可能包含一长串的0，允许用“::”来表示这一长串的0。即地址800:0:0:0:0:0:0:1可以被表示为：800::1。只有当16位组全部为0时才允许被两个冒号取代，且两个冒号在整个地址中只能出现一次。

2. IPv6 前缀

IPv6地址由两个部分组成：

- 网络前缀：n比特，相当于IPv4地址中的网络ID。
- 接口标识符：128-n比特，相当于IPv4地址中的主机ID。

网络前缀的长度与IPv6地址间以斜杠（/）区分，例如：12AB::CD30:0:0:0:0/60，表示地址中用于选路的前缀长度为60位。IPv6 DHCP服务器分配IPv6地址时，就可以从IPv6前缀中去获取。前缀也可以自动的从上游DHCP服务器分配给下游DHCP服务器。

3. 特殊的 IPv6 地址

在IPv6中，也存在一些特殊的IPv6地址，如：

fe80::/8，链路本地地址，类似于IPv4的169.254.0.0/16；

fc00::/7，本地地址，类似于IPv4的10.0.0.0/8，172.16.0.0/16，192.168.0.0/16等；

ff00::/12，组播地址，类似于IPv4的224.0.0.0/8。

4. NAT66

NAT66（IPv6-to-IPv6 Network Address Translation，IPv6-to-IPv6网络地址转换）是将IPv6数据报文头中的IPv6地址转换为另一个IPv6地址的过程。NAT66前缀转换是NAT66的一种实现方式，其将报文头中的IPv6地址的前缀替换为另一个IPv6地址前缀，实现IPv6地址转换。NAT66可以实现内部网络与外部公共网络的互访。

3.6.3 IPv6 地址分配方式

- 手动配置。手动配置IPv6地址/前缀及其他网络配置参数。
- 无状态自动地址分配，即SLAAC方式。由接口ID生成链路本地地址，再根据路由通告报文包含的前缀信息自动配置本机地址。
- 有状态自动地址分配，即DHCPv6方式。DHCPv6又分为如下两种:

- DHCPv6自动分配。DHCPv6服务器自动配置IPv6地址/前缀及其他网络配置参数。
- DHCPv6 PD（Prefix Delegation，前缀代理）前缀自动分配。下层网络设备向上层网络设备提出前缀分配申请，上层网络设备分配合适的地址前缀给下层设备，下层设备把获得的前缀（前缀一般长度小于64）进一步自动细分成64位前缀长度的子网网段，把细分的地址前缀再通过路由通告至与IPv6主机直连的用户链路上，实现主机的地址自动配置。

3.6.4 开启 IPv6 功能

【本机管理-页面向导】基本管理>> IPv6设置

点击<是否开启>即可开启IPv6功能。

3.6.5 设置 WAN 口的 IPv6 地址

【本机管理-页面向导】基本管理>> IPv6设置>> WAN配置

开启IPv6开关后，显示WAN设置界面，WAN_V6的个数为当前设备WAN口的数量。

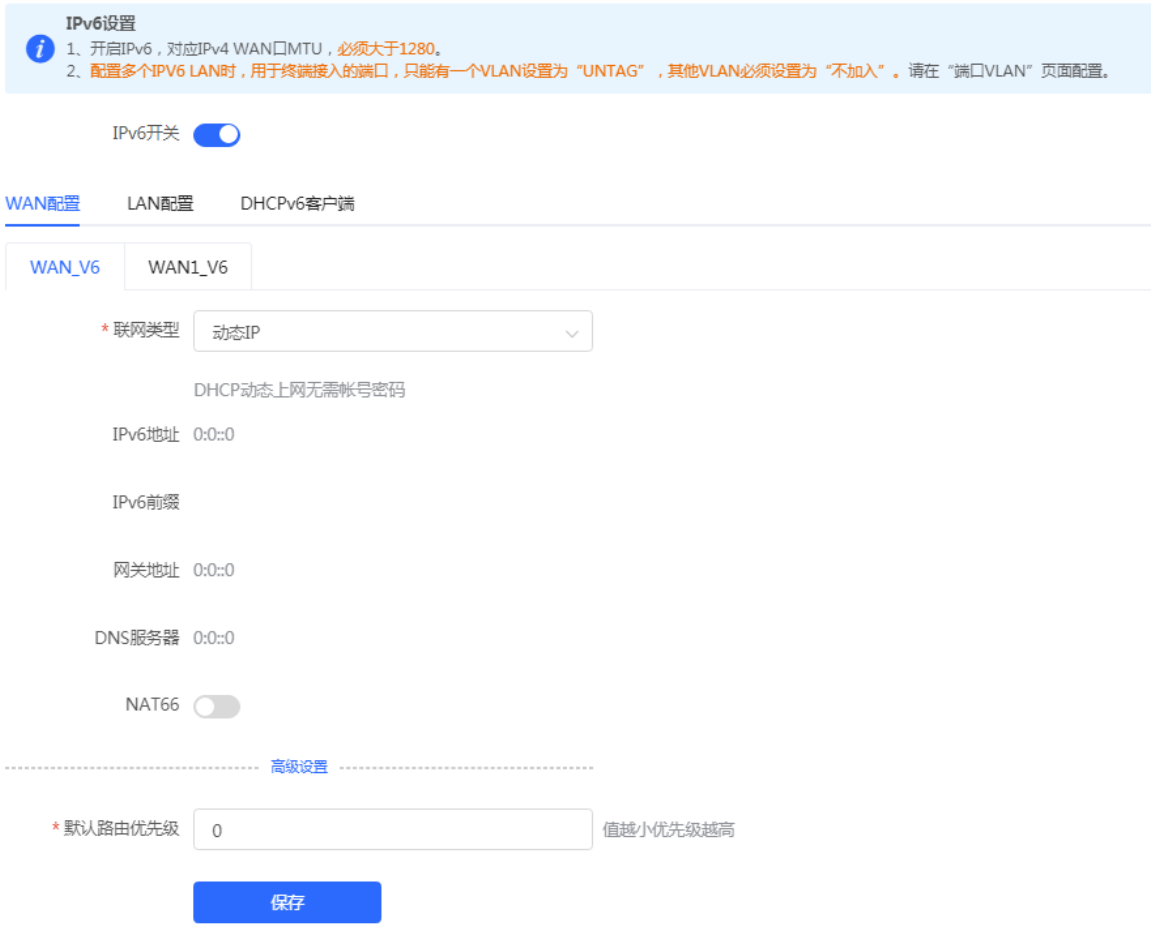


表3-4 WAN 口 IPv6 地址配置信息描述表

参数	说明
联网类型	设置WAN口获取IPv6地址的方式： ● 动态IP：当前设备将作为DHCPv6客户端，向上游网络设备申请IPv6地址/前缀 ● 静态IP：需要手动配置静态的IPv6地址、网关地址和DNS服务器 ● 无：当前WAN口将不开启IPv6功能
IPv6地址	当联网方式为动态IP方式时，将显示自动获取到的IPv6地址； 当联网方式为静态IP方式时，需要手动配置本参数
IPv6前缀	当联网方式为动态IP方式时，若当前设备获取到了上游设备下发的IPv6地址前缀，将显示自动获取到的IPv6前缀
网关地址	当联网方式为动态IP方式时，将显示自动获取到的网关地址； 当联网方式为静态IP方式时，需要手动配置本参数
DNS服务器	当联网方式为动态IP方式时，将显示自动获取到的DNS服务器地址； 当联网方式为静态IP方式时，需要手动配置本参数
NAT66	如果当前设备无法通过动态IP方式联网，或者无法获取到IPv6前缀，则需要通过开启NAT66功能来为内网终端分配IPv6地址
默认路由优先级	设置当前线路的默认路由的优先级，值越小，优先级越高。同一目的地址，在路由选路时会选择路由优先级高的作为最优路由

⚠ 注意

RG-EG105G和RG-EG105G-P不支持NAT66功能。

3.6.6 设置 LAN 口的 IPv6 地址

【本机管理-页面向导】基本管理>> IPv6设置>> LAN配置

当设备通过动态IP方式接入网络，可以由上游设备分配LAN口的IPv6地址，并通过IPv6地址前缀来为局域网中的终端分配IPv6地址；若上游设备无法为本设备分配IPv6地址前缀，则需要手动为LAN口配置一个IPv6地址前缀，并通过开启NAT66功能（参见3.6.5 设置WAN口的IPv6地址）来为局域网中的终端分配IPv6地址。

点击默认VLAN的<修改>按钮，在“IPv6地址/长度”一栏，填写一个长度不大于64的本地地址，该地址将同时作为IPv6地址前缀使用。

地址分配方式用来设置为终端分配IPv6地址的方式：

- 自动：将同时使用DHCPv6和SLAAC两种方式为终端分配IPv6地址
- DHCPv6：使用DHCPv6协议为终端分配IPv6地址
- SLAAC：使用SLAAC协议为终端分配IPv6地址
- 无：不为终端分配地址

选择哪一种协议分配地址，取决于内网终端支持哪种协议。如果不确定，选择“自动”方式即可。

点击展开高级设置，可以配置更多地址属性。

表3-5 LAN 口 IPv6 地址配置信息描述表

参数	说明
子网前缀名称	设置从哪个接口获取前缀，如“WAN_V6”、“WAN1_V6”等。默认为全部接口
子网前缀长度	设置子网前缀的长度，取值范围为48~64
子网ID	设置子网ID，十六进制格式，0表示自动递增
地址租期	设置IPv6地址租期，单位为分钟
DNS服务器	配置IPv6 DNS服务器地址

3.6.7 查看 DHCPv6 客户端

【本机管理-页面向导】基本管理>> IPv6设置>> DHCPv6客户端

当设备作为DHCPv6服务器为终端分配IPv6地址，可以在当前页面中查看从设备获取到IPv6地址的客户端信息，包括客户端的主机名、IPv6地址、剩余租期和DUID（DHCPv6 Unique Identifier，DHCPv6设备唯一标识符）。

在搜索栏中输入DUID，点击 ，可快速查找指定DHCPv6客户端的相关信息。

3.7 设置 DHCP 服务器

3.7.1 DHCP 服务器介绍

在局域网内开启DHCP服务器功能，能够实现自动为终端设备下发IP地址，让连接设备LAN口或连接Wi-Fi的终端设备获取到地址从而连接上网。

DHCPv6服务器功能相关介绍请参考3.6.6 设置LAN口的IPv6地址。

3.7.2 地址分配机制

DHCP服务器按照如下步骤为客户端选择IP地址：

(1) 设备接收到DHCP客户端申请IP地址的请求时，首先查找DHCP静态地址分配列表，如果这台DHCP客户端的MAC地址在DHCP静态地址分配列表中，则把对应的IP地址分配给该DHCP客户端。

(2) 如果申请IP地址的DHCP客户端的MAC地址不在DHCP静态地址分配列表中，或者DHCP客户端申请的IP地址与LAN口的IP地址不在同一网段，设备会从地址池中选择一个在局域网中未被使用的IP地址分配给该主机。

(3) 如果地址池中没有任何可分配的IP地址，则客户端获取不到IP地址。

3.7.3 配置 DHCP 服务器

1. 配置 DHCP 服务器基本参数

【本机管理-页面向导】基本管理>> LAN设置>> LAN设置

DHCP服务开关：开启后局域网内的设备才能自动获取到IP。

注意

若网络中的DHCP服务都被关闭，将导致终端设备无法自动获取到地址，需开启设备DHCP服务或每个终端设备手动配置固定IP上网。

开始地址：DHCP服务器自动分配的IP的开始地址，即DHCP地址池的起始地址。开始地址的范围需在由IP地址和子网掩码计算出的网段内。客户端从地址池中获取IP地址，若地址池被用完，客户端将获取不到IP地址。

分配IP数：地址池中的IP地址数量，默认254个地址。

地址租期：地址租约时间。终端设备在连接状态时一般会自动续租保持IP地址不变；若因终端设备断开连接或网络不稳定等情况，没有续租，过了租期时间，将收回IP地址。此时终端设备恢复连接将重新请求地址。默认租期为30分钟。

2. 配置 DHCP 服务器选项

【本机管理-页面向导】基本管理>> LAN设置>> DHCP选项

DHCP服务器选项为所有LAN口共用的配置，可根据实际情况选择配置。

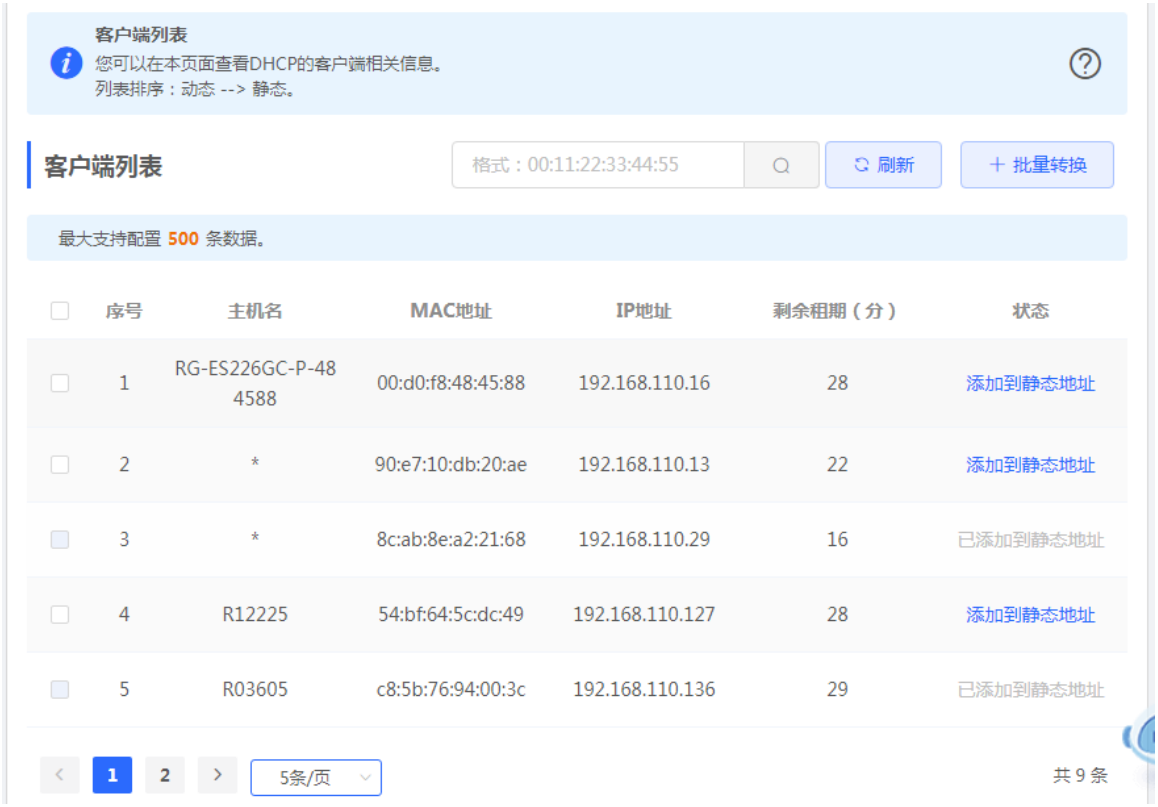
表3-6 DHCP 服务器选项配置信息描述表

参数	说明
DNS服务器	运营商提供的DNS服务器地址
Option 43	当AC（无线控制器）与AP不在同一局域网，AP通过DHCP服务器获取IP地址后，无法通过广播方式发现AC，因此需要在DHCP服务器上配置DHCP响应报文中携带的Option 43信息，通告AP使AP能够发现AC
Option 138	填入AC的IP地址。与Option 43类似，当AC与AP不在同一局域网时，可通过设置Option 138选项使AP获取AC的IPv4地址
Option 150	设置TFTP服务器地址选项。输入TFTP服务器IP地址，指定为客户端分配的TFTP服务器的地址

3.7.4 查看 DHCP 客户端

【本机管理-页面向导】基本管理>> LAN设置>> 客户端列表

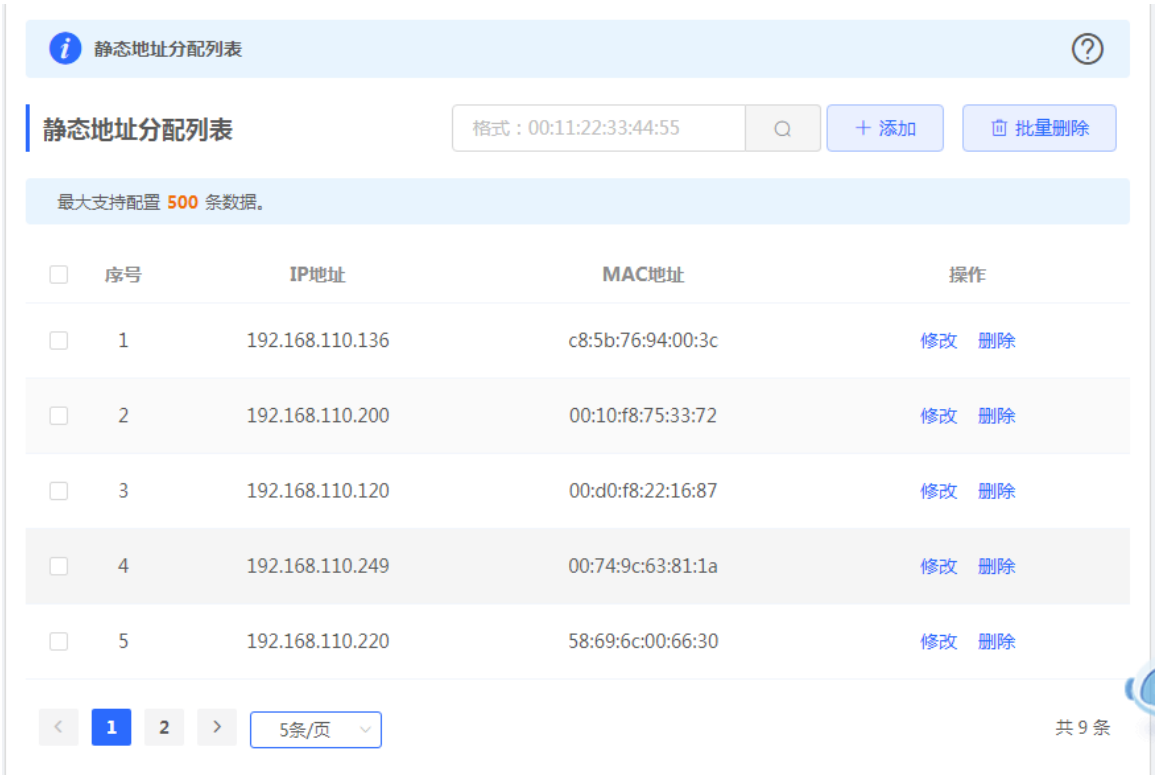
查看DHCP动态分配的客户端地址信息。点击状态栏中的<添加到静态地址>，或者勾选列表选择框后点击<批量转换>，将动态地址分配关系添加到静态地址分配列表中，使对应主机每次连接都将获取绑定的IP地址。静态地址分配列表的查看请参考3.7.5。



3.7.5 配置静态地址分配

【本机管理-页面向导】基本管理>> LAN设置>> 静态地址分配

显示已绑定的静态地址分配信息。



点击<添加>，在弹出的静态IP地址绑定对话框中，填写要绑定的设备MAC地址和IP地址，点击<确定>。绑定静态IP后，对应主机每次连接都将获取绑定的IP地址。

3.8 静态路由

【本机管理-页面向导】高级管理>> 路由设置>> 静态路由

静态路由由用户手工配置。当数据报文与静态路由匹配成功时，将按照指定的转发方式进行转发。

注意

静态路由不能自动适应网络拓扑结构的变化，当网络拓扑结构发生变化，需要手工重新配置。

点击<添加>，输入目的地址、子网掩码、出接口和下一跳IP地址，创建静态路由。

表3-7 静态路由配置信息描述表

参数	说明
目的地址	数据包要到达的目的网络。根据目的地址与掩码匹配数据报文的目的IP
子网掩码	目的网络的子网掩码。根据目的地址与掩码匹配数据报文的目的IP
出接口	数据包进行转发的接口
下一跳	数据包将发往的下一个路由点的IP地址。如果出接口通过PPPoE拨号上网，则无需配置下一跳地址

创建静态路由后，可在页面的静态路由列表中查看到相关配置信息及路由是否可达。“是否可达”用来指示下一跳是否可达，以此判断路由是否能够正常生效。若显示“不可达”，请检查当前路由的出接口是否能Ping通下一跳地址。

3.9 策略路由

3.9.1 功能简介

策略路由是一种根据用户指定的策略进行路由转发的机制。路由器转发数据报文时，首先根据配置的规则对报文进行过滤，匹配成功则按照一定的转发策略进行转发。设备提供的策略路由，可根据数据包中特定字段（源/目的IP，协议类型）制定规则，并从特定接口转发。

多线路场景中，若设备通过不同线路同时连接互联网和内部网络，在不做相应路由设置的情况下，流量默认均衡选路，可能出现访问内部网络的数据发往外网，而访问外网的数据发往内部网络的数据流向错误，进而导致网络异常。因此需要配置策略路由，控制内外网的数据隔离转发。

设备支持策略路由、地址库选路和静态路由三种策略作为报文转发的依据，在策略同时存在的情况下，优先级为：策略路由 > 静态路由 > 地址库选路。地址库选路的配置介绍请参考3.2.6。

3.9.2 配置步骤

【本机管理-页面向导】高级管理>> 路由设置>> 策略路由

点击<添加>，创建策略路由规则。

表3-8 策略路由配置信息描述表

参数	说明
规则名称	路由规则的名称，作为策略路由的标识，任意两条规则不允许重名
协议类型	策略路由生效的特定协议，可指定为IP、ICMP、UDP、TCP等协议或根据需要自定义协议类型
协议号	当指定协议类型为“自定义”时，需要输入协议号
源IP地址/范围	配置策略路由条目匹配的源IP地址/范围，默认为所有IP地址 ● 所有IP：匹配所有源IP地址 ● 自定义：匹配指定范围内的源IP地址
自定义源IP	当设置匹配的源IP地址/范围为“自定义”时，需要输入匹配的单个源IP地址或源IP地址范围
目的IP地址/范围	配置策略路由条目匹配的目的IP地址/范围，默认为所有IP地址 ● 所有IP：匹配所有目的IP地址 ● 自定义：匹配指定范围内的目的IP地址
自定义目的IP	当设置匹配的目的IP地址/范围为“自定义”时，需要输入匹配的单个目的IP地址或目的IP地址范围
源端口范围	当协议类型为“TCP”或“UDP”才有此配置项，配置策略路由匹配的报文源端口范围

参数	说明
目的端口范围	当协议类型为“TCP”或“UDP”才有此配置项，配置策略路由匹配的报文目的端口范围
出接口	对命中路由规则的数据包进行转发的接口
状态	点击按钮，设置是否启用本条路由规则。如果设置为“关闭”，本条策略将不生效

说明

如果希望限制接入设备只能访问特定的内部网络，可以将对应路由的出接口指定为专线网络的WAN口。关于如何设置专线网络，请参考3.2.4 设置专用线路。

策略路由列表显示已创建的策略路由，默认按照策略列表由上至下的顺序进行匹配，新增的策略排在最前面，优先匹配。可以在匹配顺序栏手动调整策略的匹配顺序，点击 上移策略，使策略优先匹配；点击 下移策略，使策略滞缓匹配。

3.9.3 典型配置案例

1. 组网需求

某企业接入两条不同带宽的线路，其中线路A（WAN1）用于访问外部互联网，线路B（WAN2）用于访问特定的内部网络（10.1.1.0/24）。通过设置策略路由，保障内外网数据流向正确，并将特定地址范围内（172.26.31.1~172.26.31.200）的设备隔离外部网路，只允许其访问特定的内部网络。

2. 配置要点

- 设置专用线路。
- 添加访问内部网络的策略路由。
- 添加访问非内部网络的策略路由。
- 添加策略路由限制指定设备只能访问内网。

3. 配置步骤

(1) 设置WAN2为内网专用线路

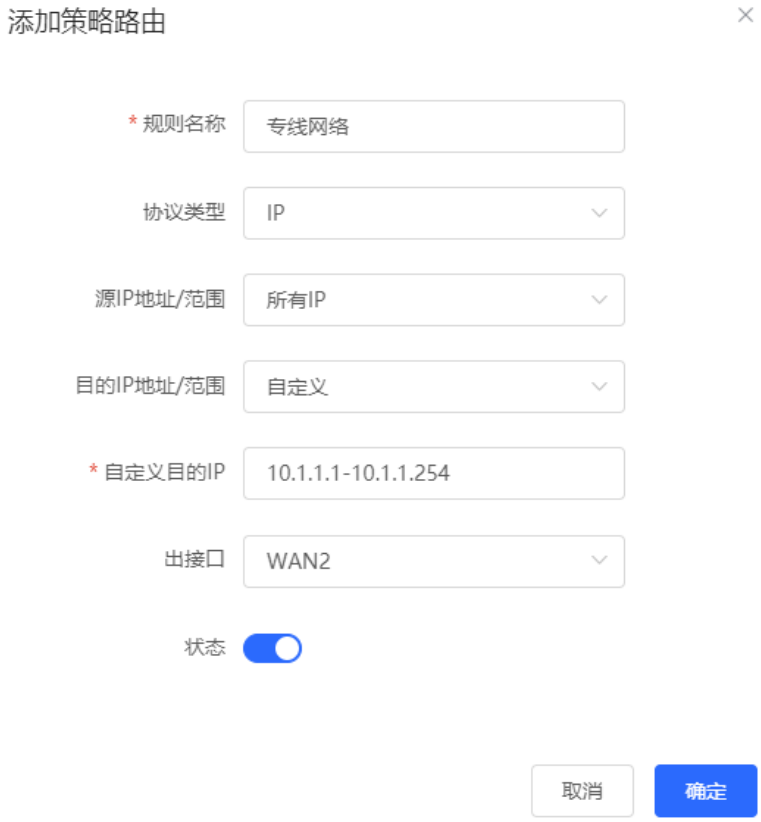
在设置WAN2口联网参数时，点击展开高级设置，开启“专线”开关，点击<保存>。参考3.2.4 。

(2) 添加策略路由，设置非内部网络的数据报文从WAN1口转发

点击 高级管理>>路由设置>>策略路由进入策略路由设置页面，点击<添加>，创建一条策略路由，指定出接口为WAN1。

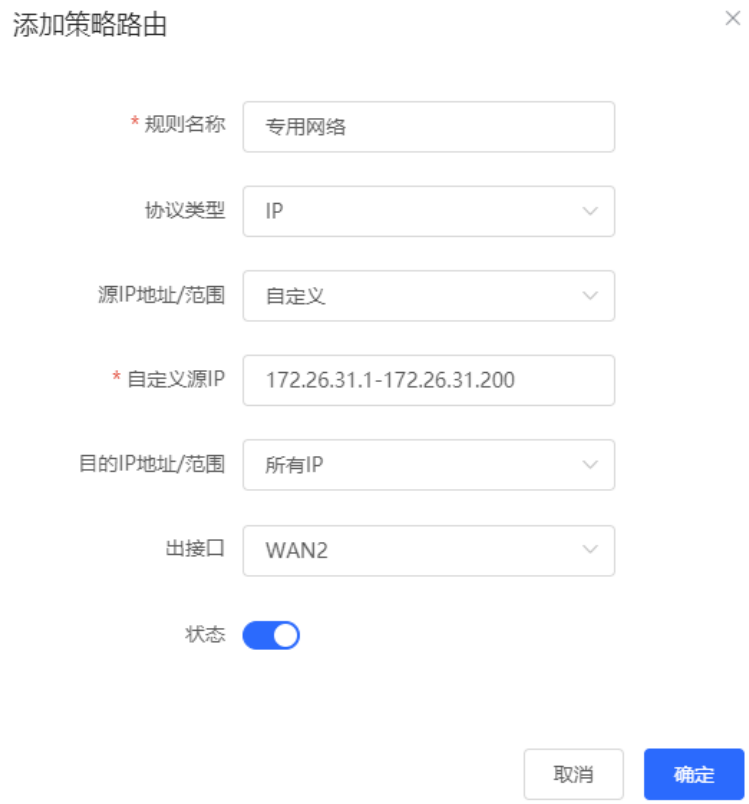
(3) 添加策略路由，设置访问内部网络的数据报文从WAN2口转发

创建一条策略路由，自定义目的IP地址范围为10.1.1.1~10.1.1.254，指定出接口为WAN2。



(4) 添加策略路由，限制172.26.31.1~172.26.31.200地址范围的设备只能访问内网专线

创建一条策略路由，自定义源IP，设置源IP地址范围为172.26.31.1~172.26.31.200，指定出接口为专线网络的WAN2口。



3.10 设置 ARP 绑定与防护

3.10.1 功能简介

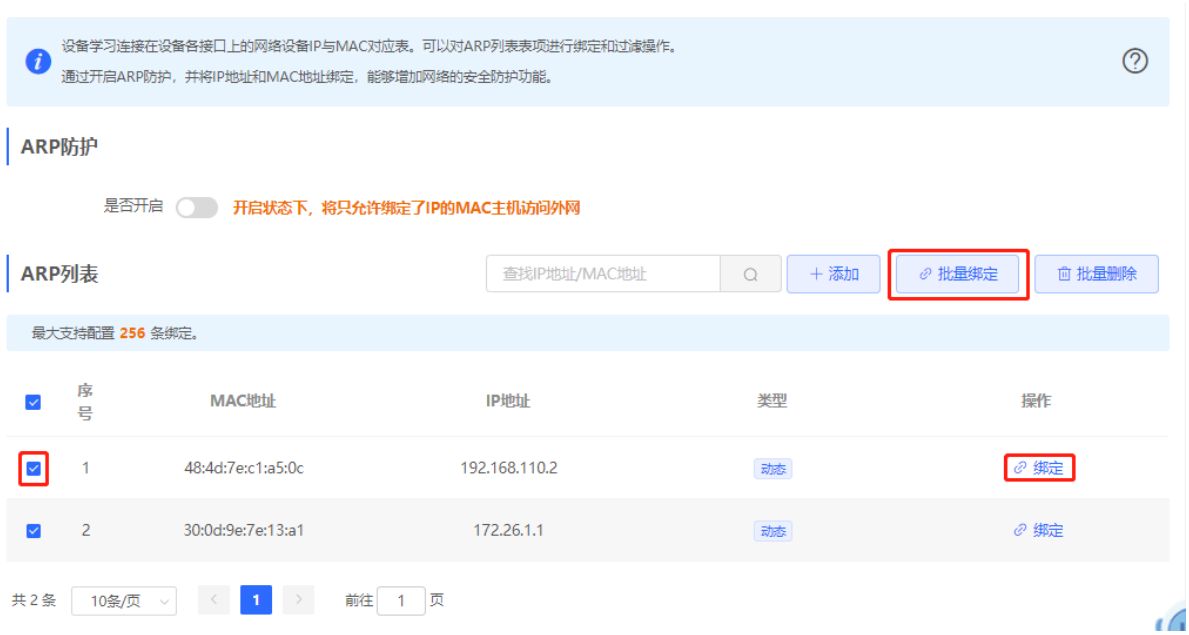
设备学习连接在设备各接口上的网络设备的IP地址与MAC地址，生成对应ARP表项。支持绑定ARP映射和开启ARP防护来限制局域网内主机访问外网，提高网络安全性。

3.10.2 设置 ARP 绑定

【本机管理-页面向导】安全管理>> ARP列表

在开启ARP防护功能前需要先设置IP地址与MAC地址的绑定关系。支持两种方式进行ARP映射绑定：

(1) 选中ARP列表中动态获取到的ARP映射表项，单击<绑定>按钮即可完成绑定。可以一次性勾选多条需要进行绑定的表项，点击<批量绑定>进行绑定。



(2) 点击<添加>按钮，输入绑定的IP地址和MAC地址。输入框将弹出ARP列表中已存在的地址映射信息，点击可自动填入。点击<确定>完成绑定。

若需要解除静态配置的IP地址和MAC地址绑定关系，点击操作栏中<删除>按钮。

3.10.3 设置 ARP 防护

点击按钮开启ARP防护功能。开启状态下，将只允许局域网内绑定了IP的MAC主机访问外网。ARP绑定的配置步骤请参考3.10.2 设置ARP绑定。

3.11 设置 MAC 地址过滤

3.11.1 功能介绍

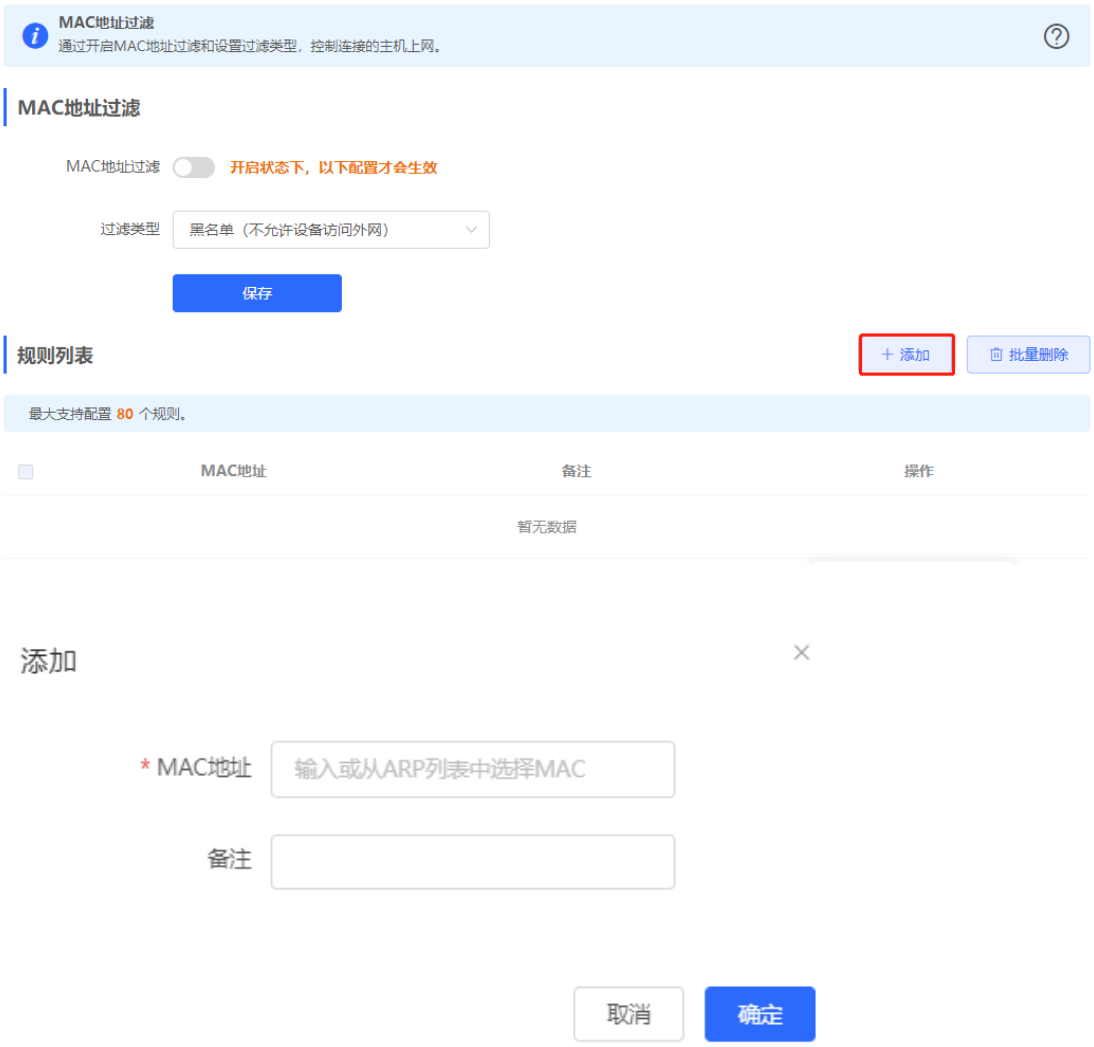
通过开启MAC地址过滤和设置过滤类型可以有效地控制局域网内的主机访问外网。支持两种过滤类型：

- 白名单：只允许过滤规则列表中的MAC地址所对应的主机访问外网。
- 黑名单：禁止过滤规则列表中的MAC地址所对应的主机访问外网。

3.11.2 配置步骤

【本机管理-页面向导】安全管理>> MAC过滤

(1) 点击<添加>按钮，输入MAC地址和备注信息。输入框将弹出ARP列表（安全管理>> ARP防护）中获取到的MAC地址，点击可自动填入。点击<确定>，创建过滤规则。



(2) 选择过滤类型，开启MAC地址过滤开关，并点击<保存配置>。

3.12 设置 PPPoE 服务器

3.12.1 功能简介

PPPoE（Point-to-Point Protocol over Ethernet），以太网上的点对点协议，是将点对点协议（PPP）封装在以太网（Ethernet）框架中的一种网络隧道协议。在路由器中，PPPoE服务器能够在局域网中向用户提供接入服务，并对用户提供带宽管理功能。

3.12.2 全局设置

【本机管理-页面向导】高级管理>> PPPoE服务器>> 全局设置

点击“启用”开启PPPoE服务器功能，并设置PPPoE服务器参数。

表3-9 PPPoE 服务器配置信息描述表

参数	说明
PPPoE服务器	PPPoE服务器开关，设置是否开启PPPoE服务器功能

参数	说明
强制PPPoE拨号	对局域网内的用户，是否强制其必须拨号才能上网
本地隧道地址	PPPoE服务器的点对点地址
地址池IP范围	PPPoE服务器分配给认证用户的地址范围
VLAN	当前PPPoE服务器作用的VLAN
首选/备选DNS服务器地址	下发给认证用户的DNS服务器地址
最大未应答LCP包数	当一条连接的未应答LCP包数超过这个数值时，PPPoE服务器会自动断开这条连接
认证方式	提供PAP、CHAP、MSCHAP和MSCHAP2共四种认证方式，需要至少选择一种

3.12.3 设置 PPPoE 用户账号

【本机管理-页面向导】高级管理>> PPPoE服务器>> 帐号管理

点击<添加>创建PPPoE认证用户账号。账号管理列表将显示当前已创建的PPPoE认证用户账号，点击<修改>，可以对配置信息进行修改；点击<删除>，可以删除已创建的账号。

表3-10 PPPoE 用户账号配置信息描述表

参数	说明
账号/密码	认证账号的账号名和密码，用于PPPoE拨号上网
到期时间	设置认证账号的有效截止日期，到期后账号失效，不能再用于PPPoE认证上网
备注	设置账号的描述信息
状态	设置是否启用该用户账号，不启用则账号无效，不能用于PPPoE认证上网
流控开关	设置是否对该账号进行流量控制。开启后需要为PPPoE认证用户设置流控策略。当智能流控功能处于关闭状态时，流控开关将处于禁用状态。若要配置账号的流控开关，需要先开启智能流控功能。智能流控功能的设置请参考6.7.2 智能流控。
账号套餐	开启流控后，需要为当前账号指定一个流控套餐，根据流控套餐限制用户带宽。流控套餐的配置与查看请参考3.12.4 设置用户流控。

3.12.4 设置用户流控

【本机管理-页面向导】高级管理>> PPPoE服务器>> 帐号套餐

当智能流控功能处于关闭状态时，账号套餐不生效。在配置账号套餐之前，需要先开启智能流控。智能流控功能的设置请参考6.7.2 智能流控。

点击<添加>创建账号套餐。账号套餐列表将显示当前已创建的账号流控套餐，可进行修改或删除。

表3-11 PPPoE 用户流控套餐配置信息描述表

参数	说明
套餐名称	流控套餐的名称，在配置认证账号时，根据该名称选择流控套餐
上行/下行保证带宽	带宽紧张时认证账号用户保证能够使用的上传和下载带宽
上行/下行最大带宽	带宽资源充足时，认证账号用户可使用的最大上传和下载带宽
上行/下行每用户最大带宽	每个用户所能占用的最大带宽，可选配置，默认不限速
应用接口	流控套餐所应用的接口

3.12.5 设置例外 IP

【本机管理-页面向导】高级管理>> PPPoE服务器>> 例外IP管理

在开启PPPoE服务器的情况下，如果想指定该VLAN某些IP地址不需认证账号密码即可上网，可以将对应IP地址配置为IP例外地址。

“例外IP管理列表”将显示当前已创建的例外IP地址表项。点击<修改>，可以修改表项的配置信息。点击<删除>，可以删除添加的例外IP地址表项。

起始IP地址/结束IP地址：例外IP的起止范围。

备注：例外IP范围的说明信息。

状态：例外IP是否生效。

3.12.6 查看在线用户

【本机管理-页面向导】高级管理>> PPPoE服务器>> 在线用户

查看当前通过PPPoE拨号上网的终端用户信息。点击<断开连接>可断开用户与PPPoE服务器的连接。

表3-12 PPPoE 在线用户信息描述表

参数	说明
在线用户数	当前通过PPPoE拨号上网的在线用户总数量
IP地址	终端的IP地址
MAC地址	终端的MAC地址
上线时间	用户接入上网的时间

3.13 端口映射

3.13.1 功能简介

1. 端口映射

端口映射功能可以将WAN口IP地址和端口号与局域网内服务器IP地址和端口号建立映射关系，使所有对WAN口某服务端口的访问将被重定向到指定的局域网内服务器的相应端口，从而实现外部网络用户能够通过WAN口IP和指定端口号主动访问局域网内的服务主机。

应用场景：通过设置端口映射，实现在公司或外地出差时访问家庭网络里的摄像头或计算机。

2. NAT-DMZ（Network Address Translation-Demilitarized Zone）

当外来的数据包没有命中任何端口映射时，DMZ规则可将该数据包重定向到内网服务器中，即所有从Internet主动发往设备的数据报文都将转发给指定的DMZ主机，从而实现外网用户访问内网服务器。既实现了外网访问服务，同时又确保局域网内其它主机的安全。

应用场景：当外部网络用户需要访问内部网络服务器，例如在家庭网络中搭建服务器以供在公司或外地出差时访问，则需要设置端口映射或DMZ。

3.13.2 配置前的准备

- 确认内网被映射设备的内网IP地址和服务所使用的端口号。
- 确认在内网能够正常使用所映射的服务。

3.13.3 配置步骤

【本机管理-页面向导】高级管理>> 端口映射>>端口映射

点击<添加>，输入规则名称、服务类型、协议类型、外部端口/范围，内部服务器IP地址和内部端口/范围。最多支持设置50条端口映射规则。

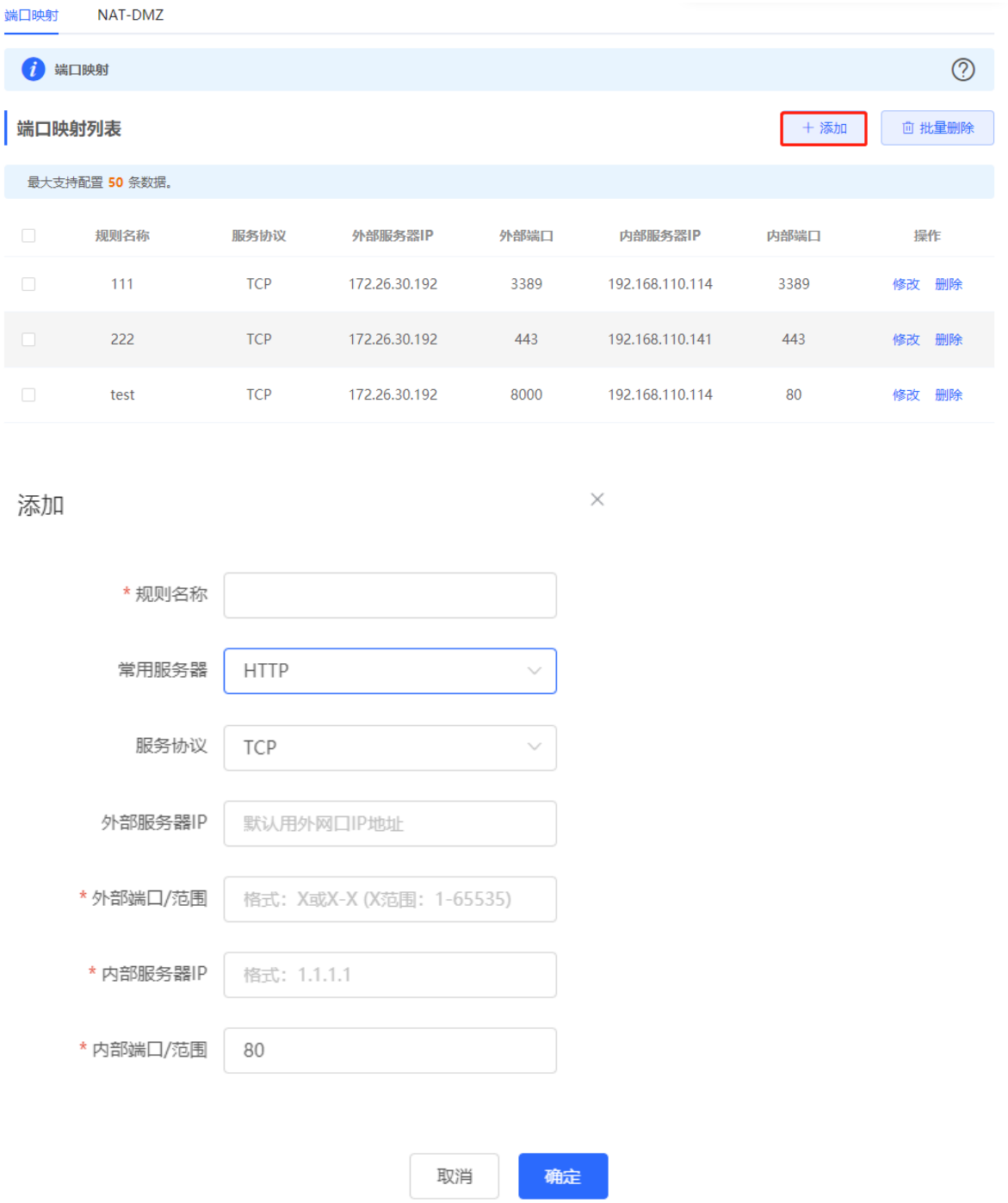


表3-13 端口映射配置信息描述表

参数	说明
规则名称	对端口映射规则进行描述，用于标识端口映射规则
常用服务器	选择要映射的服务类型，如HTTP，FTP等，将自动填入该服务对应的常用内部端口号。若服务类型不明确，可设置为自定义
服务协议	选择所选服务采用的传输层协议类型，TCP或UDP，ALL表示两种协议均生效。需符合对应服务的客户端配置
外部服务器地址	外网访问时使用的主机地址，默认为WAN口IP地址
外部端口/范围	外网访问时使用的端口号，需在客户端软件中确认，如摄像头监控软件。可输入单个端口号或端口号范围（如1050-1060），若输入端口号范围，则内部端口范围将与外部端口范围保持一致
内部服务器IP	需要映射到WAN口的内部服务器的IP地址，即供外网访问的内网设备的IP地址，如网络摄像头的IP地址
内部端口/范围	需要映射到WAN口的内部服务器的服务端口号，即供外网访问的应用所使用的端口号，如网页服务8080 可输入单个端口号或端口号范围（如1050-1060），若输入端口号范围，则内外部端口范围包含的端口个数应相同

3.13.4 验证与测试

使用外网设备，通过外部IP地址和外部端口号测试能否访问目的主机服务。

3.13.5 测试不成功的解决方案

(1) 修改外部端口号配置，用新的外部端口号再次测试。常见于使用了受防火墙阻挡的端口的情况。

(2) 开启服务器的远程访问权限。常见的原因是服务器默认禁止了远程访问，导致内网访问正常，跨网段后失败。

(3) 尝试设置DMZ规则，请参考DMZ配置步骤。常见的原因是设置的端口错误或不全。

3.13.6 DMZ 配置步骤

【本机管理-页面向导】高级管理>> 端口映射>>NAT-DMZ

点击<添加>，输入规则名称、内部服务器的IP地址，选择应用的接口与规则生效状态，点击<确定>。一个出接口能且只能配置一条DMZ映射规则。

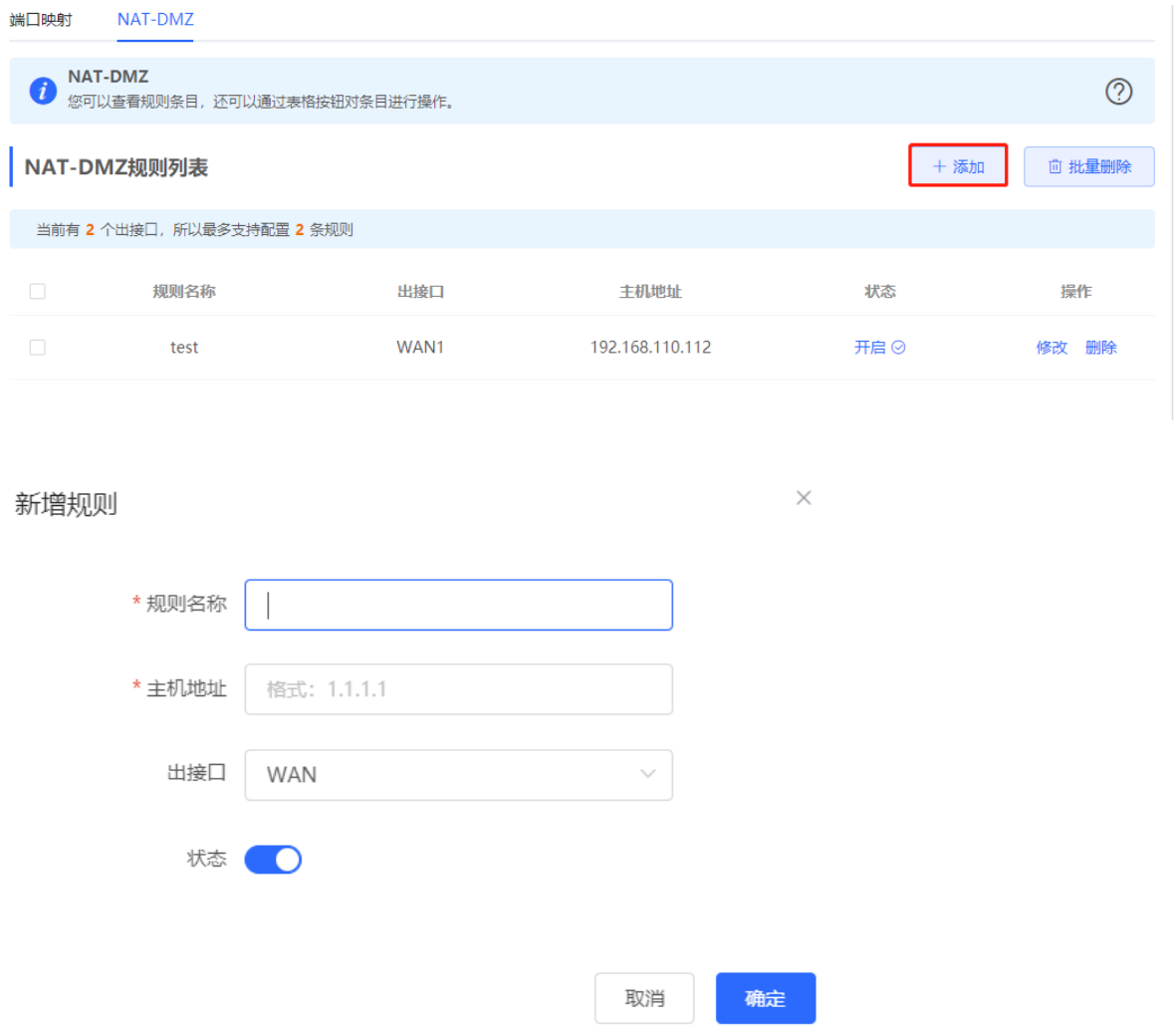


表3-14 DMZ 规则配置信息描述表

参数	说明
规则名称	对映射规则进行描述，用于标识DMZ规则
主机地址	报文重定向的DMZ主机的IP地址，即提供给外网访问的内网服务器的IP地址
出接口	规则匹配的WAN口。一个WAN口可配置一条规则
状态	设置规则是否生效，开启后规则才会生效

3.14 UPnP

3.14.1 功能简介

UPnP（Universal Plug and Play，通用即插即用）功能开启后，设备能够根据终端的请求转换终端上网服务所使用的端口，自动实现NAT转换。当互联网上的终端想要访问设备内网的资源时，设备就可以自动添加端口映射表项，实现一些业务的内外网穿越。常见支持UPnP协议的应用程序有MSN Messenger、迅雷、BT、PPLive。

在使用UPnP服务前，需要注意与UPnP功能配合使用的终端（PC、手机等）也要支持UPnP功能。

说明

通过UPnP实现端口自动映射需要满足以下条件：

- 本设备需启动UPnP功能；
- 内网主机的操作系统应支持并开启UPnP服务；
- 应用程序应支持并开启UPnP功能。

3.14.2 UPnP 设置

【本机管理-页面向导】高级管理>> UPnP设置

点击按钮，开启UPnP功能。在下拉框中设置默认接口。点击<保存>使配置生效。

若有相关应用程序自动转换了端口，将在下方列表显示。

表3-15 UPnP 配置信息描述表

参数	说明
是否开启	是否开启UPnP功能，UPnP功能默认处于关闭状态
默认接口	UPnP服务绑定的WAN口地址。默认为WAN口。多WAN环境下，可以手动选择绑定的WAN口，也可以配置为Auto，让设备自动选择WAN口进行绑定

3.14.3 效果验证

开启UPnP服务后，在与设备配合使用的终端上打开支持UPnP协议的应用程序（如迅雷、比特彗星），刷新设备Web页面，UPnP列表将会显示对应的UPnP表项，表示此时UPnP隧道已创建成功。

3.15 设置动态域名

3.15.1 功能简介

开启动态域名服务（DDNS，Dynamic Domain Name Server）后，外网用户能够随时在Internet用固定的域名访问设备的服务资源时不必再查WAN口的IP地址。该服务需要在第三方DDNS服务商注册账号和域名，设备支持花生壳和No-IP DNS。

3.15.2 配置前的准备

使用动态域名服务前，在花生壳或No-IP官网注册账号和域名。

3.15.3 设置动态域名

1. 配置步骤

设备支持花生壳动态域名和No-IP动态域名动态域名。其中花生壳不支持海外访问，而No-IP动态域名基于国内的花生壳，能够同时支持国内外用户使用动态域名服务。

【本机管理-页面向导】高级管理>> 动态域名>> 花生壳动态域名/No-IP动态域名

【本机管理-页面向导】Advanced >> Dynamic DNS >> No-IP DNS

输入注册的用户名和密码，点击<登录>，向服务器发起连接请求，使域名和设备WAN口IP地址的绑定关系生效。

点击<删除>，将清空输入的所有信息，并解除与服务器的连接关系。

连接状态用来指示是否与服务器成功建立连接。若在登录时未指定域名，则连接成功后将返回当前账号的域名列表，此时账号的所有域名都会解析成WAN口IP。

表3-16 动态域名登录信息描述表

参数	说明
服务接口	一个域名只能解析成一个IP地址，因此在多WAN环境下，需要用户设置域名所绑定的WAN口。默认为WAN
用户名/密码	在官网上注册的账号用户名和密码。如果当前无注册账号，可以点击“没有账户，注册一个”，跳转至官网来创建一个新账号
域名	设置服务接口IP绑定的域名 对于No-IP动态域名服务，该项为可选项。一个账号可以绑定多个域名，用户可以选择其中一个域名与当前服务接口IP进行绑定，即只有该域名会被解析为WAN口IP。如果未指定域名，则当前账号的所有域名都将被解析为当前WAN口IP

2. 效果验证

点击<登录>后，连接状态显示为“连接成功”，表示与服务器成功建立连接。配置完成后，在外网Ping域名，域名应该能够Ping通，并且被解析为设备WAN口的IP地址。

3.15.4 花生壳内网穿透

1. 功能介绍

花生壳内网穿透是DDNS的改进版，支持WAN口为内网IP的情况下使用。推荐使用花生壳内网穿透。开启花生壳内网穿透功能后，用户可以通过扫描二维码将花生壳账号与设备绑定，生成内网穿透的域名，从而使外网用户能够通过域名直接访问设备内网资源。

2. 配置步骤

【本机管理-页面向导】高级管理>>动态域名>>花生壳内网穿透

(1) 点击<开启>，并点击<保存>后，在下方将出现服务状态和二维码。请使用微信或花生壳APP扫码登录。用户扫码并在APP上绑定账号后，Web能够直接与花生壳服务器建立连接。

(2) 在花生壳管理APP上完成下一步配置。在花生壳管理APP的的内网穿透页面，点击添加映射，将当前账号下的域名与设备内网的IP和端口进行映射。

3. 效果验证

(1) 连接成功后，Web页面上会显示当前服务状态为在线，并且显示当前账号名。用户可以点击账号名跳转到花生壳管理界面。

点击<更换账号>，Web就会解除与服务器的连接，重新显示二维码。

(2) 绑定成功后，就可以通过域名直接访问设备内网的Web界面，如下图所示。

3.16 连接 IPTV

> 注意
>
> 仅在非中文环境支持，中文环境下如需设置请先切换系统语言，见9.11 。

IPTV是一种网络运营商提供的网络电视服务。

3.16.1 配置前的准备

- 确认是否开通了运营商的IPTV业务。
- 确认当地IPTV的类型是VLAN还是IGMP，VLAN类型需确认VLAN ID。若无法确认请联系当地运营商。

3.16.2 IPTV 配置步骤（VLAN 类型）

【本机管理-页面向导】Basics>> IPTV>>IPTV/VLAN

选择当地合适的模式，点击准备连接的接口后的下拉框，在下拉框中选择IPTV，输入运营商提供的VLAN ID。例如，IPTV电视盒子连接到设备LAN3接口，VLAN ID为20，配置如下图所示。

Internet VLAN：有时上网业务的网络也需要设置VLAN ID，则开启该功能输入VLAN ID。默认关闭VLAN标签功能。无特殊情况建议保持关闭。

配置好后请确认IPTV机顶盒连接到正确的接口，上例中应连接LAN3口。

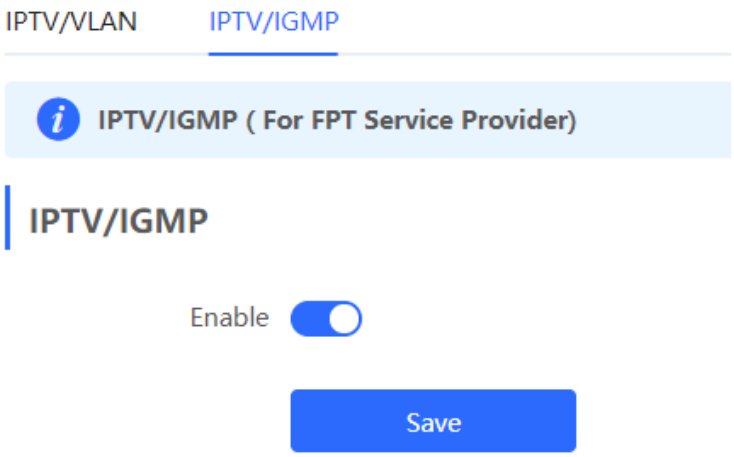
注意

开启该功能可能将导致断网，请谨慎操作。

3.16.3 IPTV 配置步骤（IGMP 类型）

【本机管理-页面向导】Basics>> IPTV>>IPTV/IGMP

适配FPT网络运营商。开启后将IPTV机顶盒连接路由器任意LAN口。



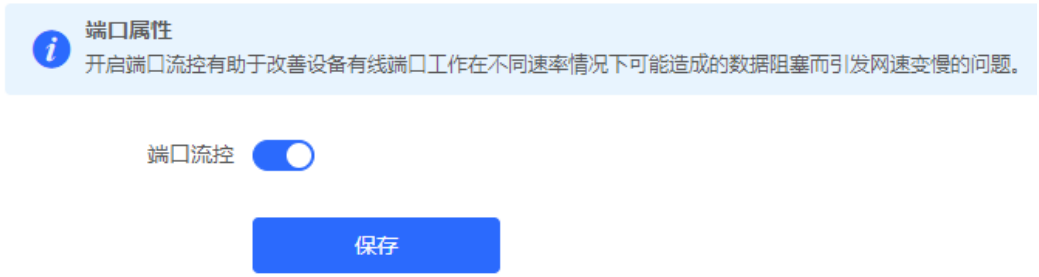
3.17 端口流控

注意

仅RG-EG105G-E和RG-EG210G-E支持本功能。

【本机管理-页面向导】高级管理>>端口属性

设备的有线端口工作在不同速率时可能发生数据阻塞，从而引发网速变慢，开启端口流控有助于改善这一问题。



3.18 连接数限制

【本机管理-页面向导】高级管理>>连接数限制

本功能用于控制每IP的最大连接数。

点击<添加>，可新增一条连接数限制规则。

表3-17 连接数限制规则配置信息描述表

参数	说明
规则名称	连接数限制规则的名称
开始地址	该规则匹配的IP地址范围的起始地址
结束地址	该规则匹配的IP地址范围的结束地址
最大连接数	对匹配该规则的IP，限制每IP的最大会话连接数量
状态	是否启用规则，启用后生效

3.19 其他设置

【本机管理-页面向导】高级管理>>其它设置

其他设置页面用于设置一些不常用的功能。默认都为关闭状态。

开启RIP&RIPng：开启后，LAN/WAN接口将支持RIP&RIPng动态路由协议，可自动与网络中其他开启了RIP的路由器同步路由信息。

开启高级防火墙：开启后，设备将加强的攻击防护，同时针对报文的协议等进行校验，但也会降低设备转发性能。

开启SIP ALG：部分语音通讯会使用SIP协议，如果服务器处于WAN口外，SIP报文经过NAT后，可能不可用。开启后，将对SIP协议进行ALG转换。请根据实际情况开启或关闭。

禁止ICMPv6发包：正常情况下，设备在收到ICMPv6异常报文时，将向报文来源发送ICMPv6差错报文。如果出于安全考虑，不希望设备发出这些报文，可开启该选项。

4 AP 管理

说明

- 若要对下联AP进行管理，需开启自组网发现功能（见3.1 ）。无线设置默认将同步到网络中所有无线设备上，可通过设置分组来限定配置的设备范围，详见4.1 。
- 设备本身不支持发射无线Wi-Fi信号，无线设置需下发至下联AP才能实际生效。

4.1 设置 AP 分组

4.1.1 功能介绍

开启自组网发现，设备可作为主AP/AC对下联AP以分组为单位进行批量配置和管理。在配置AP前，先对AP进行分组。

说明

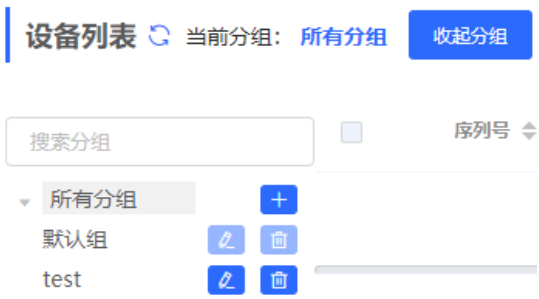
在设置无线网络时指定分组，则对应配置将在指定分组中的无线设备上生效。

4.1.2 配置步骤

【整网管理-页面向导】设备管理>> AP

(1) 查看当前网络中所有的AP设备的信息，包括基本信息、射频信息和型号信息。点击序列号可对单台设备进行设置。

(2) 点击<展开分组>，列表左侧会出现当前所有分组的信息。点击 创建新分组，最多支持添加8个分组。对于已创建的分组，可以点击 修改分组名称，点击 删除分组。默认组不可修改名称与删除。



(3) 点击左侧分组名称，将显示该分组下的所有设备。一台设备只能属于一个分组。默认所有设备都属于默认组。勾选列表中的表项，点击<迁移分组>，可将选中设备迁至指定分组。迁移分组后，设备将应用该分组下的配置。点击<删除离线设备>可将不在线的设备从列表中移除。

4.2 设置 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> 无线网络

输入Wi-Fi名称和Wi-Fi密码，选择Wi-Fi信号的使用频段，点击<保存>。

点击展开高级设置，可设置更多Wi-Fi特性。

注意

修改配置会重启无线配置，可能导致当前连接的终端掉线。请谨慎操作。

表4-1 无线网络配置信息描述表

参数	说明
Wi-Fi名称	无线终端搜索无线网络时显示的名称
应用频段	设置Wi-Fi信号的使用频段，支持2.4GHz和5GHz频段。5GHz频段相较于2.4GHz频段网络传输速率更快，受干扰更小，不过在信号覆盖范围和穿墙方面通常不如2.4GHz频段，可根据实际需求选择信号频段。默认Wi-Fi频段为2.4GHz+5GHz，同时在2.4GHz和5GHz频段放出Wi-Fi信号
加密类型	无线网络连接时的加密方式，有三种加密方式可选： 不加密：无需密码即可连接上Wi-Fi WPA-PSK/WPA2-PSK：使用WPA/WPA2加密方式 WPA_WPA2-PSK（推荐）：使用WPA2-PSK/WPA-PSK加密方式
Wi-Fi密码	连接无线网络的密码，由8~16个字符组成
选择时段	Wi-Fi开启的时段，设置后，其他时段用户无法接入Wi-Fi上网
VLAN	设置Wi-Fi信号所属VLAN

参数	说明
隐藏Wi-Fi	开启隐藏Wi-Fi功能能够防止Wi-Fi被非法用户接入，增强安全性。但手机或电脑将搜索不到Wi-Fi名称，必须手动输入正确的名称和密码进行连接。开启前需记录当前的Wi-Fi名称，防止隐藏后无法连接
用户隔离	开启后，接入该Wi-Fi的终端之间相互隔离，终端用户不能与同一AP下的其他用户（同一个网段）相互访问，以增强安全性
5G优先	开启后支持5G的终端设备优先选择5G Wi-Fi。Wi-Fi开启双频合一（即应用频段为“2.4G+5G”）才能开启本功能
竞速模式	开启后优先发送游戏报文，为游戏提供更稳定的无线网络
三层漫游	开启后终端在同一个Wi-Fi下IP保持不变，提升用户跨VLAN场景下的漫游体验
Wi-Fi6	开启后无线用户能够体验更快的上网速度，优化上网体验。 本配置只对支持802.11ax协议的AP和路由器生效。同时接入终端也需支持802.11ax协议，才能体验Wi-Fi 6带来的高速上网体验。若终端不支持Wi-Fi 6特性，可关闭本功能

4.3 设置访客 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> 访客Wi-Fi

访客Wi-Fi是为访客提供的无线网络，默认关闭。访客Wi-Fi默认开启“用户隔离”且不可关闭，即接入的用户之间相互隔离，只能连接Wi-Fi上网，无法互访，以此提高安全性。访客网络支持配置生效时段，时间到后，访客网络会变为关闭状态。

点击开启“访客Wi-Fi”开关，设置访客Wi-Fi的名称和密码。点击展开高级设置，可配置访客Wi-Fi的生效时段与更多Wi-Fi属性（配置项详情请参考4.2 ）。保存设置后，访客可通过Wi-Fi名称和密码连接无线网络上网。

4.4 添加 Wi-Fi

【整网管理-页面向导】整网管理>> 无线设置>> Wi-Fi列表

点击<添加>，输入Wi-Fi名称和密码，点击<确定>创建Wi-Fi。点击展开高级设置，可以配置更多Wi-Fi属性。可参考4.2 进行设置。添加Wi-Fi后，终端设备可以搜索到新建的Wi-Fi，Wi-Fi列表显示添加的Wi-Fi信息。

4.5 健康模式

【整网管理-页面向导】整网管理>> 无线设置>> 健康模式

点击开启健康模式，支持选择生效时段。

开启健康模式后，设备将在生效时段里降低无线发射功率，Wi-Fi覆盖面积减小。可能导致信号弱，网络卡顿问题。建议保持关闭或将生效时段设置为无人使用网络的时间段。

4.6 射频设置

【整网管理-页面向导】整网管理>> 射频设置

设备在开机时能够检测周围无线环境并选择合适的配置。但无法避免无线环境变化而引起的网络卡顿。用户可以分析AP和路由器周围的无线环境，手动选择合适的参数。

注意

修改配置会重启无线配置，可能导致当前连接的终端掉线。请谨慎操作。

表4-2 射频配置信息描述表

参数	说明
国家码	各国规定的Wi-Fi信道有可能不同。为防止终端搜索不到Wi-Fi，请选择实际所在的国家或地区

参数	说明
2.4G/5G频宽	频宽小网络较稳定，频宽大易受干扰。若干扰较严重，选择较低的频宽能够一定程度上避免网络卡顿。2.4GHz频段支持20MHz和40MHz的频宽，5GHz频段支持20MHz、40MHz和80MHz的频宽。 默认为“自动”，表示自动根据环境选择频宽
最大用户数	大量用户接入AP或路由器上，可能导致无线网络性能下降，影响用户上网体验。设置最大用户数后，当接入用户达到阈值，将禁止新用户接入。若接入终端带宽需求较高，可调低最大用户数。无特殊情况建议保持默认
踢下线阈值	在存在多个Wi-Fi信号的情况下，设置踢下线阈值可一定程度上改善无线信号质量。当终端距离无线设备较远，终端用户的无线信号强度低于踢下线阈值时，将断开Wi-Fi连接，迫使终端重新选择距离较近的无线信号。 但踢下线阈值越高，终端越容易被踢下线，为避免影响正常终端上网，建议保持关闭或小于-75dBm

说明

- 可选无线信道与国家码有关，请正确选择所在的国家或地区的国家码。
- 信道、功率和漫游灵敏度不支持全局设置，需要在对应设备上进行单独设置。

4.7 设置无线黑名单或白名单

4.7.1 功能简介

支持设置基于所有Wi-Fi的全局黑白名单或者基于SSID的无线黑白名单。黑白名单支持匹配终端设备的MAC地址前缀（OUI）。

无线黑名单：名单中的设备将被禁止上网，未加入名单的设备不限制。

无线白名单：只有名单中的设备能够上网，未加入名单的设备都禁止。

注意

白名单列表为空时，无线白名单不生效，即所有MAC均可接入。

4.7.2 全局黑白名单

【整网管理-页面向导】终端管理>>黑白名单>>全局黑白名单

选择黑/白名单模式，点击<添加>设置黑/白名单列表。在弹出的对话框中输入想要拉黑或加入白名单的设备的MAC地址和备注，点击<确定>保存。MAC地址输入框将弹出已连接的终端信息，点击可自动填入。黑名单模式下，将断开并禁止该终端设备的连接。全局黑白名单将在网络中所有设备的所有Wi-Fi上生效。

黑名单模式下点击<删除>，对应终端设备即可重新连接Wi-Fi；白名单模式下点击<删除>，且删除后白名单列表不为空，则会断开并禁止对应终端设备连接Wi-Fi。

4.7.3 基于 SSID 黑白名单

【整网管理-页面向导】终端管理>>黑白名单>>基于SSID黑白名单

在左侧列表选择设置的Wi-Fi，并选择黑/白名单模式，点击<添加>设置黑/白名单列表。基于SSID的黑白名单将限制指定Wi-Fi下的接入用户。

4.8 一键优化无线网络

【整网管理-页面向导】整网管理>>无线优化

在“无线优化”页签，勾选“我已阅读以上注意事项”，点击<无线优化>，将在组网环境下对无线网络进行自动优化。支持设置定时网优，在指定时间对网络进行优化。建议定时网优时间设置为凌晨或无人使用网络的时间段。

注意

优化期间可能造成终端掉线，且优化开始后无法回退配置至优化前，请谨慎操作。

优化开始后，请耐心等待优化完成。优化完成后，点击<取消优化>可以将优化的射频参数恢复为默认值。点击<查看详情>或点击<优化记录>页签，可查看最近一次的优化记录详情。

4.9 Wi-Fi 认证

4.9.1 功能简介

随着无线网络的普及，Wi-Fi成为商家的营销手段之一。顾客可以在观看广告，或者关注微信公众号后，连接商家提供的Wi-Fi上网。另外，为防止出现安全漏洞，无线办公网络通常要限制Wi-Fi只能由员工使用，因此需要对终端的身份进行验证。

设备的Wi-Fi认证功能使用了Portal认证技术来实现页面展示以及用户管理。用户在连接Wi-Fi后，流量不会被直接放行到互联网上。Wi-Fi使用者必须在Portal认证网站进行认证，只有认证通过后才可以使用网络资源。商家或企业还可以设置自定义的Portal页，实现身份验证，广告展示等功能。

4.9.2 配置前的准备

(1) 开启Wi-Fi认证前，请确保无线信号稳定，用户连上Wi-Fi可以正常上网。网络中用于认证的无线SSID应设置为不加密状态。加密容易导致微信连Wi-Fi认证异常。

(2) 若网络中的AP设备的IP在认证范围内，请将AP添加为免认证用户，参考4.9.9 免认证：

- 二层网络环境下，请将AP的MAC添加到免认证的MAC白名单中。
- 三层网络环境下，请将AP的IP添加到免认证的IP白名单中。

4.9.3 微信认证

1. 功能简介

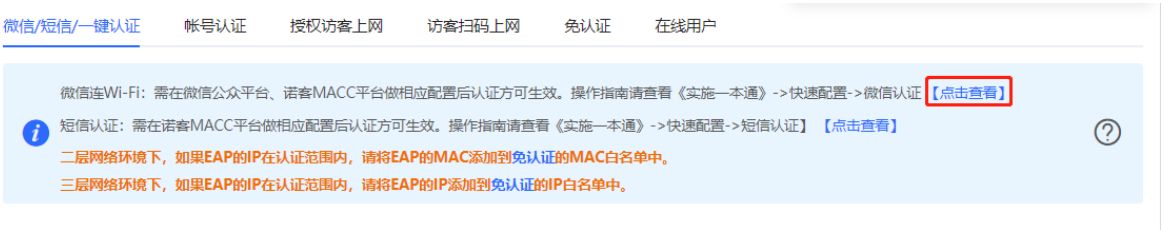
EG设备对接云端MACC认证服务器。Wi-Fi使用者在连接Wi-Fi后，弹出Portal页面，使用者需要跳转到微信，关注公众号后，才能上网。适用于商场环境，商家可以通过开启微信认证来引导用户关注公众号。

2. 配置前的准备

(1) 微信连Wi-Fi为二层协议，应确保认证设备能获取无线用户的MAC地址：

- 需要认证的无线用户的网关地址部署在认证设备上。
- 需要认证的无线用户的网关地址未部署在认证设备上，则要求设备作为DHCP服务器，通过为无线用户分配地址来获取终端的MAC地址信息。该场景下，需要同时设置网络类型为“三层网络”。

(2) 请先在微信公众平台、诺客MACC平台完成相应配置，再在设备上开启认证功能。具体操作指南请参考《MACC-auth诺客平台认证组件实施一本通》中的微信认证章节，点击页面“点击查看”可直接阅读在线文档。



3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置 >> 微信/短信/一键认证

(1) 开启微信认证上网

点击开启认证上网开关，选择服务器类型为“微信连Wi-Fi”，并设置网络类型、认证服务器地址、公众号重定向IP和是否开启用户逃生功能，点击<保存>。

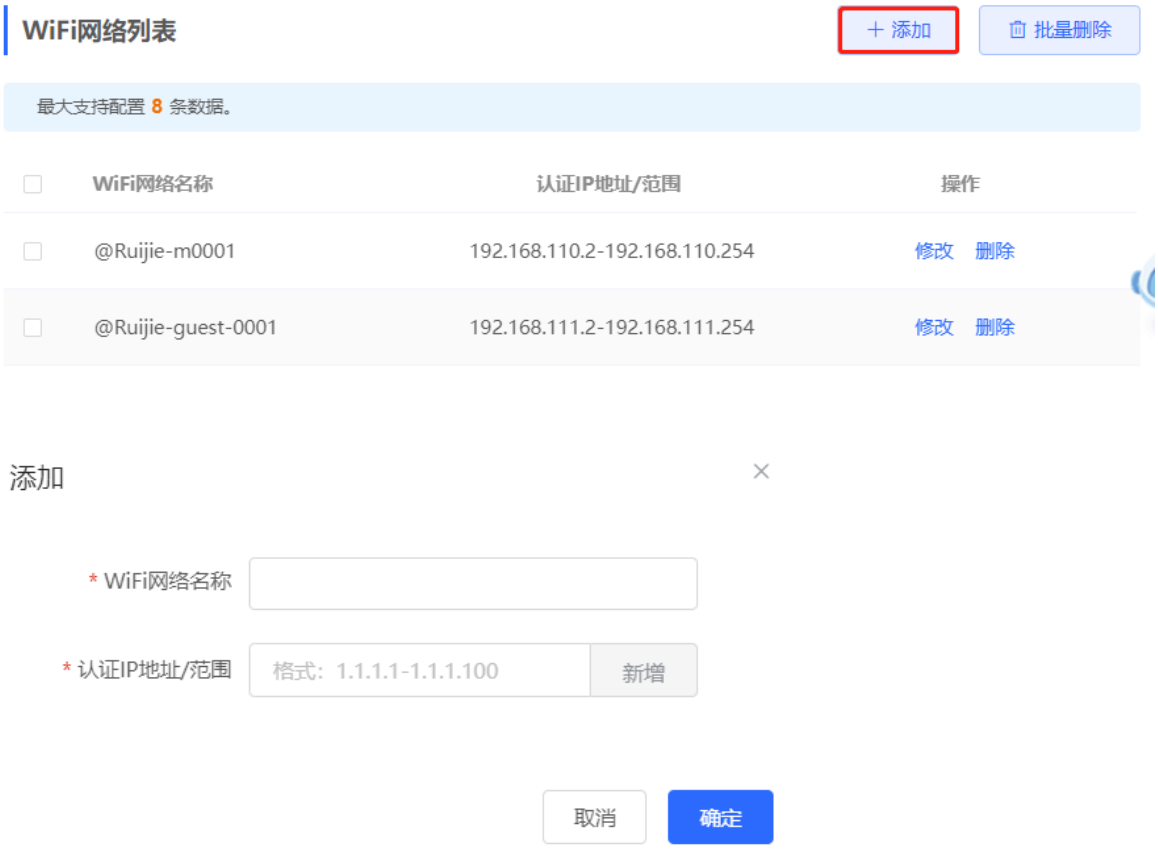
表4-3 微信认证配置信息描述表

参数	说明
网络类型	默认为二层网络，请根据实际网络环境进行选择。 由于微信连Wi-Fi为二层协议，三层网络环境下，应设置下联设备通过DHCP Relay指向当前认证设备，并将认证网段的DHCP地址池部署在认证设备上，使认证设备能够通过DHCP分配地址来获取无线用户的MAC地址。该场景下，应选择三层网络。
服务器类型	选择“微信连Wi-Fi”
认证服务器主页	在完成MACC服务器端配置后，MACC服务器会返回一个URL地址。在认证过程中，设备会向该URL发起认证请求
公众号重定向IP	与公众号设置的菜单/链接地址对应，默认为118.31.178.137，一般情况下无需修改。 用户在认证过程中重定向到微信公众号后，需要访问该IP地址，才能进行后续的认证步骤。 若需要修改，应设置为内网未使用网段的IP地址，具体配置请参考常见问题。
用户逃生功能	开启后，在认证服务器异常时，设备将关闭认证功能，使所有用户可直接上网；服务器恢复后，将自动重新开启认证功能

(2) 设置认证范围

在当前页面点击<添加>，填写Wi-Fi名称和需要认证的IP地址网段，点击<确定>。

对于无需认证的终端，如打印机、电脑或部分用户，可将IP地址配置为免认证，即可不用认证直接上网。配置详情请参见4.9.9 免认证。

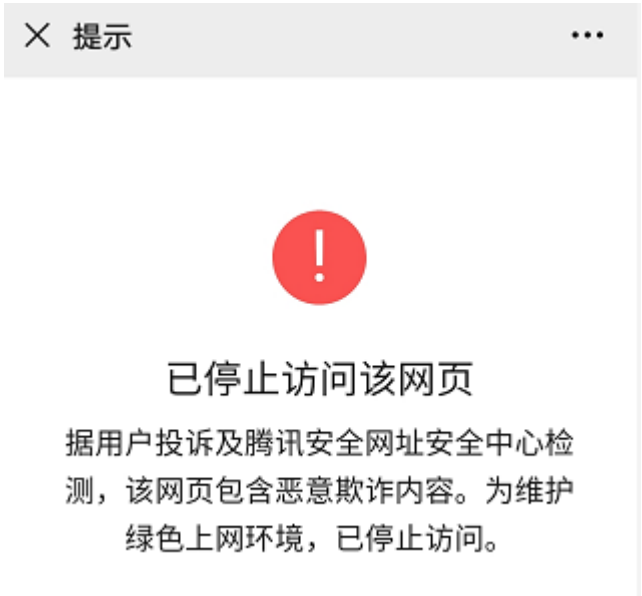


4. 效果验证

手机终端连接指定Wi-Fi，会自动弹出Portal认证页，用户在页面指引下进入微信页面，关注公众号后，点击菜单或自动回复链接可完成认证，正常上网。用户认证成功后，可在[高级管理]>>[认证设置]>>[在线用户]页面查看到该认证用户的信息，详见4.9.10 在线认证用户管理。

5. 常见问题

- 微信认证时在公众号点击认证菜单/认证链接时提示“已停止访问该网页”，造成认证失败。



问题原因：在公众号平台设置公众号的认证入口时，所设置的链接地址被微信客户端安全中心限制为非安全地址，终端在请求此地址后被微信拦截。

解决方案：修改设备的强制重定向地址和公众号的菜单/链接地址为内部局域网中未规划使用的某个IP地址。例如，内网未使用172.29.0.0网段，则可使用172.29.1.140作为公众号重定向IP，并将公众号里的链接地址也替换为172.29.1.140。

注意

如果设置公众号重定向IP为内网已使用的网段地址，会导致微信认证异常。

4.9.4 企业微信认证

1. 功能简介

与微信认证相似，Wi-Fi使用者在连接Wi-Fi后，需要跳转至企业微信，通过工作台-认证小程序认证后，才能上网。适用于企业环境，可用于管理公司员工终端和访客终端上网。

2. 配置前的准备

同4.9.3 微信认证。在开启企业微信认证功能前，应在企业微信控制台、诺客MACC平台完成相应配置。具体操作指南请参考《MACC-auth诺客平台认证组件实施一本通》中的企业微信认证章节，点击页面“点击查看”可直接阅读在线文档。

3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置 >> 微信/短信/一键认证

配置步骤与微信认证基本相同，主要区别为公众号重定向IP的不同，企业微信认证需要将公众号重定向IP设置为47.104.189.180:81。具体配置步骤请参考4.9.3 微信认证。

4. 员工认证上网

确保员工已加入企业微信组织中，员工使用手机连接Wi-Fi，会自动跳转到企业微信进行认证。员工打开企业微信后，需要进入企业微信的“工作台”，再点击由管理员创建的“认证应用”获取上网权限。提示认证成功后，员工可正常上网。

由于手机兼容性问题，部分手机可能存在Portal认证页面无法唤起企业微信的情况，此时用户可以手动打开企业微信并做后续操作。

5. 访客认证上网

访客来司，可由接待的员工为访客授权，使其能够连接公司Wi-Fi上网。访客连接访客Wi-Fi后会弹出认证二维码，此时由已经通过认证的企业员工使用手机版企业微信扫描该二维码，输入访客姓名，访客即可以通过认证正常上网。

需要注意的是，在使用访客认证方式时，需要在Wi-Fi网络列表下配置至少两个Wi-Fi以及对应关联的网段，分别用于员工连接和访客连接。

4.9.5 WiFidog 认证

1. 功能简介

EG设备对接云端MACC认证服务器。Wi-Fi使用者在连接Wi-Fi后，弹出Portal页面，需要账号密码验证通过后，才能上网。根据MACC端的认证配置，可设置认证方式为短信认证、固定账号认证或免账号一键登录。

2. 配置前的准备

(1) WiFidog协议为二层协议，应确保认证设备能获取无线用户的MAC地址：

- 需要认证的无线用户的网关地址部署在认证设备上。
- 需要认证的无线用户的网关地址未部署在认证设备上，则要求设备作为DHCP服务器，通过为无线用户分配地址来获取终端的MAC地址信息。该场景下，需要同时设置网络类型为“三层网络”。

(2) 请先在诺客MACC平台完成相应配置，再在设备上开启认证功能。若设置短信方式认证，还需要进行短信网关配置。具体操作指南请参考《MACC-auth诺客平台认证组件实施一本通》，点击页面“点击查看”可直接阅读在线文档。

3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置>> 微信/短信/一键认证

点击开启认证上网开关，选择服务器类型为“短信认证/一键认证”，并设置网络类型、认证服务器地址、是否开启用户逃生功能以及认证IP地址范围，点击<保存>。

表4-4 WiFidog 认证配置信息描述表

参数	说明
网络类型	默认为二层网络，请根据实际网络环境进行选择
服务器类型	选择“短信认证/一键认证”

参数	说明
认证服务器主页	在完成MACC服务器端配置后，MACC服务器会返回一个URL地址。在认证过程中，设备会向该URL发起认证请求
用户逃生功能	开启后，在认证服务器异常时，设备将关闭认证功能，使所有用户可直接上网；服务器恢复后，将自动重新开启认证功能
认证IP地址/范围	设置需要认证的IP地址范围，可以是单个IP地址（如192.168.112.2），也可以是IP地址范围（如192.168.112.2-192.168.112.254）。最多支持设置5个地址范围

4. 效果验证

手机终端连接指定Wi-Fi，会自动弹出Portal认证页。

若MACC服务器端设置认证方式为短信认证，则用户需要输入手机号来获取上网密码，输入密码后完成认证。

若MACC服务器端设置认证方式为免账号一键认证，则用户点击页面按钮后可直接上网。

若MACC服务器端设置认证方式为固定账号登录，则用户输入云端设置的账号和密码后，可以正常上网。

连接成功后，可在[高级管理]>>[认证设置]>>[在线用户]页面查看到认证用户的信息，详见4.9.10 在线认证用户管理。

4.9.6 本地账号认证

1. 功能简介

对接本地认证服务器，通过账号和密码验证用户身份。主要用于无线办公网络环境。

2. 配置前的准备

确保开启认证的设备已连接互联网，未联网状态下，终端连接Wi-Fi不会弹出认证页面。

3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置>> 账号认证

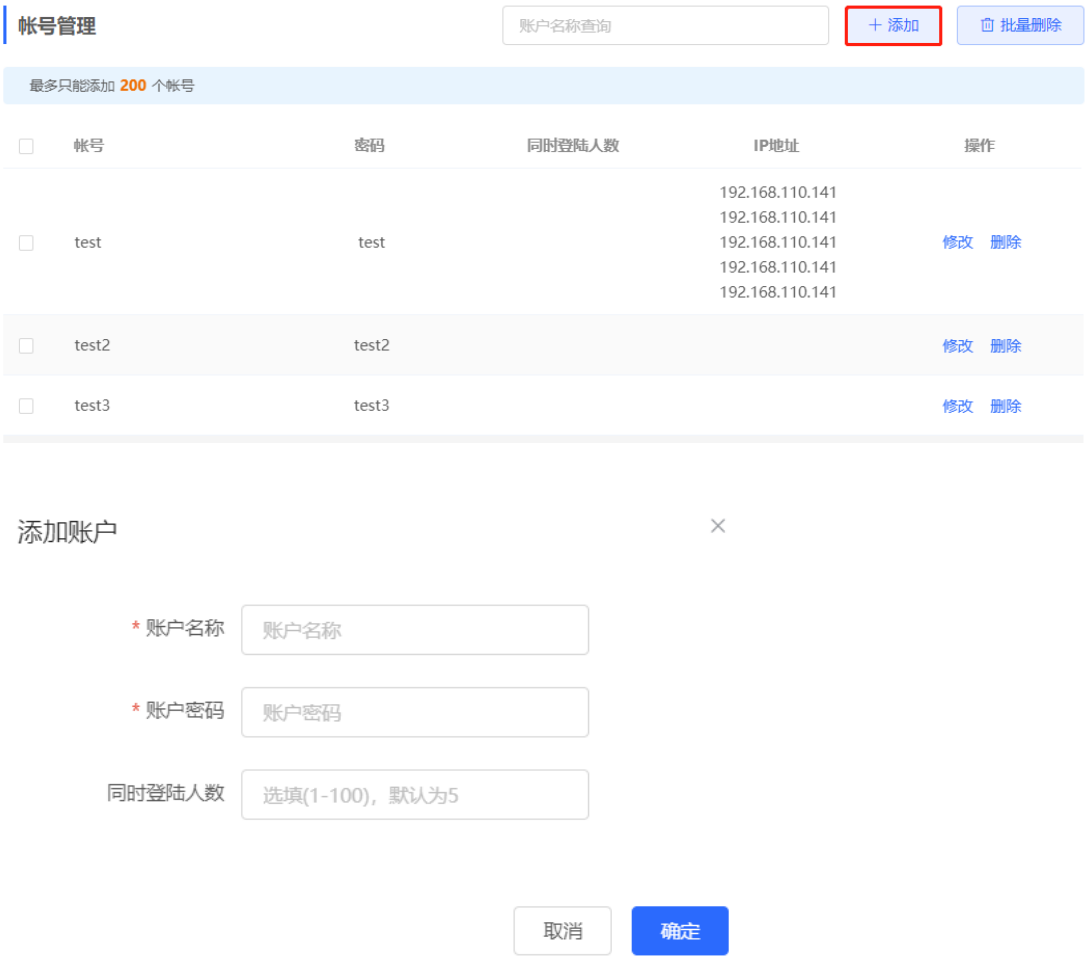
(1) 开启账号认证

点击开启账号认证，输入需要认证的终端IP地址范围，点击<保存>。开启后，认证IP地址范围内的终端需要通过认证才能上网。

(2) 设置认证账号

点击<添加>，创建可用于上网的认证账号。多个设备端可使用同一个账号密码认证上网，设置“同时登录人数”可限制同时使用该账号上网的最大用户数量。

当Wi-Fi使用者通过账号认证成功时，认证者的IP地址会显示在该账号后面的IP地址列表中。每个账号最多记录最新使用的5个设备的IP地址。



4. 效果验证

终端连接指定Wi-Fi，会自动弹出认证页面，在认证页面输入本地服务器所设置的账号密码，能够通过认证，正常上网。可在[高级管理]>>[认证设置]>>[在线用户]页面查看到连接成功的用户信息，详见4.9.10 在线认证用户管理。

4.9.7 授权访客上网

1. 功能简介

对接本地认证服务器，访客连接Wi-Fi后，由指定的授权IP用户或账号密码认证用户扫描对应访客认证弹出的二维码，访客即可上网。例如在无线办公网络下，员工网段的用户可以给访客网段的用户扫码授权。

2. 配置前的准备

确保开启认证的设备已连接互联网，未联网状态下，终端连接Wi-Fi不会弹出认证页面。

3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置>> 授权访客上网

点击开启“授权访客上网”，填写扫码信息提示、认证IP地址网段、授权IP地址范围以及是否限制访客的上网时长，点击<保存>。

表4-5 授权访客认证配置信息描述表

参数	说明
扫码信息提示	弹出的二维码页面上显示的文本信息
认证IP/范围	需要认证的用户的IP地址范围，可以输入单个IP（如192.168.110.2），或者是IP地址范围（如192.168.110.2-192.168.110.254），该IP范围内的用户需要通过认证才能上网
限制上网时长	是否限制访客用户的上网时长，开启后需设置“允许上网时长”，超过时长后访客需要重新授权才能继续上网。默认关闭，访客可以无期限地使用Wi-Fi
允许上网时长	被授权访客的可上网时长。用户授权上线后超过对应的时长会自动下线，需要重新授权
授权IP/范围	授权用户的IP地址范围。该IP地址范围内的用户拥有授权的功能，可通过扫码的方式给访客授权

4. 效果验证

访客连接Wi-Fi后，终端将弹出二维码认证页面，指定的授权用户扫描二维码后，访客即可上网。可在[高级管理]>>[认证设置]>>[在线用户]页面查看到连接成功的用户信息，详见4.9.10 在线认证用户管理。

4.9.8 访客扫码上网

1. 功能简介

访客扫描指定的二维码即可上网。例如在无线办公网络环境中，访客连接Wi-Fi后，通过扫描张贴的二维码上网。

2. 配置前的准备

确保开启认证的设备已连接互联网，未联网状态下，终端连接Wi-Fi不会弹出认证页面。

3. 配置步骤

【本机管理-页面向导】高级管理>> 认证设置>> 访客扫码上网

点击开启“扫描认证”，填写认证IP地址网段、二维码信息以及是否限制访客的上网时长，点击<保存>。

表4-6 访客扫码认证配置信息描述表

参数	说明
认证IP/范围	需要认证的用户的IP地址范围，可以输入单个IP（如192.168.110.2），或者是IP地址范围（如192.168.110.2-192.168.110.254），该IP范围内的用户需要通过认证才能上网
限制上网时长	是否限制访客用户的上网时长，开启后需设置“允许上网时长”，超过时长后访客需要扫码认证才能继续上网。默认关闭，访客可以无期限地使用Wi-Fi
允许上网时长	被授权访客的可上网时长。用户授权上线后超过对应的时长会自动下线，需要重新认证
二维码动态码	二维码动态码用于生成二维码图。更改动态码后，二维码图随之变化，之前的二维码图将失效 可将生成的二维码打印张贴，供访客扫码上网
二维码信息	访客在扫描二维码后，页面显示的二维码提示信息

4. 效果验证

终端连接Wi-Fi后，扫描访客二维码，即可通过认证，正常上网。可在[高级管理]>>[认证设置]>>[在线用户]页面查看到连接成功的用户信息，详见4.9.10 在线认证用户管理。

4.9.9 免认证

1. 功能简介

配置为免认证的用户IP或者MAC，可以直接上网不需要认证。黑名单用户的流量会被全部拦截。

2. 设置免认证用户

【本机管理-页面向导】高级管理>> 认证设置>> 免认证>>免认证用户

免认证用户：IP地址范围内的用户不需要认证，可直接上网。

点击<添加>，配置免认证用户的IP地址范围。可以输入单个IP（如192.168.110.2），或者是IP地址范围（如192.168.110.2-192.168.110.254）。支持配置50条表项。

3. 设置免认证外网 IP

【本机管理-页面向导】高级管理>> 认证设置>> 免认证>>免认证外网IP

免认证外网IP：所有用户包括未认证用户均可访问的IP地址。

点击<添加>，配置认证用户可以无需认证直接访问的外网IP。支持配置50条表项。

4. 设置 URL 白名单

【本机管理-页面向导】高级管理>> 认证设置>> 免认证>>URL白名单

URL白名单：用户在未认证情况下也可直接访问的网址。

点击<添加>，输入免认证的网址，点击<确定>。当用户的目的URL在URL白名单中时，无论用户是否完成认证，流量都会被直接放行。支持配置100条表项。

5. 设置用户 MAC 白名单

【本机管理-页面向导】高级管理>> 认证设置>> 免认证>>用户MAC白名单

用户MAC白名单：白名单中的MAC地址终端连接Wi-Fi，无需认证即可上网。

点击<添加>，输入免认证用户的MAC地址，点击<确定>。支持配置250条表项。

6. 设置用户 MAC 黑名单

【本机管理-页面向导】高级管理>> 认证设置>> 免认证>>用户MAC黑名单

用户MAC黑名单：禁止名单中的MAC地址终端上网。

点击<添加>，输入黑名单用户的MAC地址，点击<确定>。支持配置250条表项。

4.9.10 在线认证用户管理

1. 设置下线检测时长

【本机管理-页面向导】高级管理>> 认证设置>> 在线用户

配置在线用户无流量超时下线的时间。默认为15分钟。若在线用户在指定时长内均无流量通过设备，则将被强制下线，需重新认证后才能继续上网。

2. 踢用户下线

在线用户列表显示了当前所有在线用户的信息，包括用户IP地址、MAC地址、上线时间和认证方式等。可根据IP地址、MAC地址或用户名查找用户信息。点击在线用户表项操作栏的<删除>按钮，可以将用户踢下线，断开用户

的Wi-Fi连接。

4.10 开启易联功能

【整网管理-页面向导】整网管理>> 易联设置

开启易联功能后，支持易联的设备可以通过配对组成Mesh网络。设备间可以通过Mesh按键自动搜索周围的新路由器并自动配对，或登录路由器管理页面搜索选择新路由器进行配对。默认开启。

4.11 设置 AP 有线口

⚠ 注意

本配置仅对带有线LAN口的AP生效。

【整网管理-页面向导】整网管理>> AP有线口

输入VLAN ID，点击<保存>设置AP有线口所属的VLAN。VLAN ID为空表示有线口与WAN口同VLAN。

组网模式下，AP有线口配置将应用于当前网络中所有带有线LAN口的AP。其中，优先生效“AP有线口配置列表”中应用到AP的配置，点击<添加>可新增AP有线口配置；“AP有线口配置列表”中未应用到的AP，将生效AP有线口默认配置。


有线口设置
此配置仅对带有线LAN口的AP生效，以实际生效的设备为准，例如：EAP101面板AP。
有线口设置生效规则： 优先生效【AP有线口配置列表】中应用到AP的配置， 网络中未应用配置的AP，会生效AP有线口默认配置。
AP有线口默认配置
VLAN ID
去添加VLAN
(2-232,234-4090。为空表示与WAN口同VLAN)
应用到 【AP有线口配置列表】中未应用到的AP
保存
AP有线口配置列表
+ 添加
批量删除
最大支持8 条配置，或最多支持匹配32 台AP（当前已配置1 台）。
VLAN ID
应用到
操作
2
Ruijie
修改 删除

5 交换机管理

5.1 开启防环路

5.1.1 功能简介

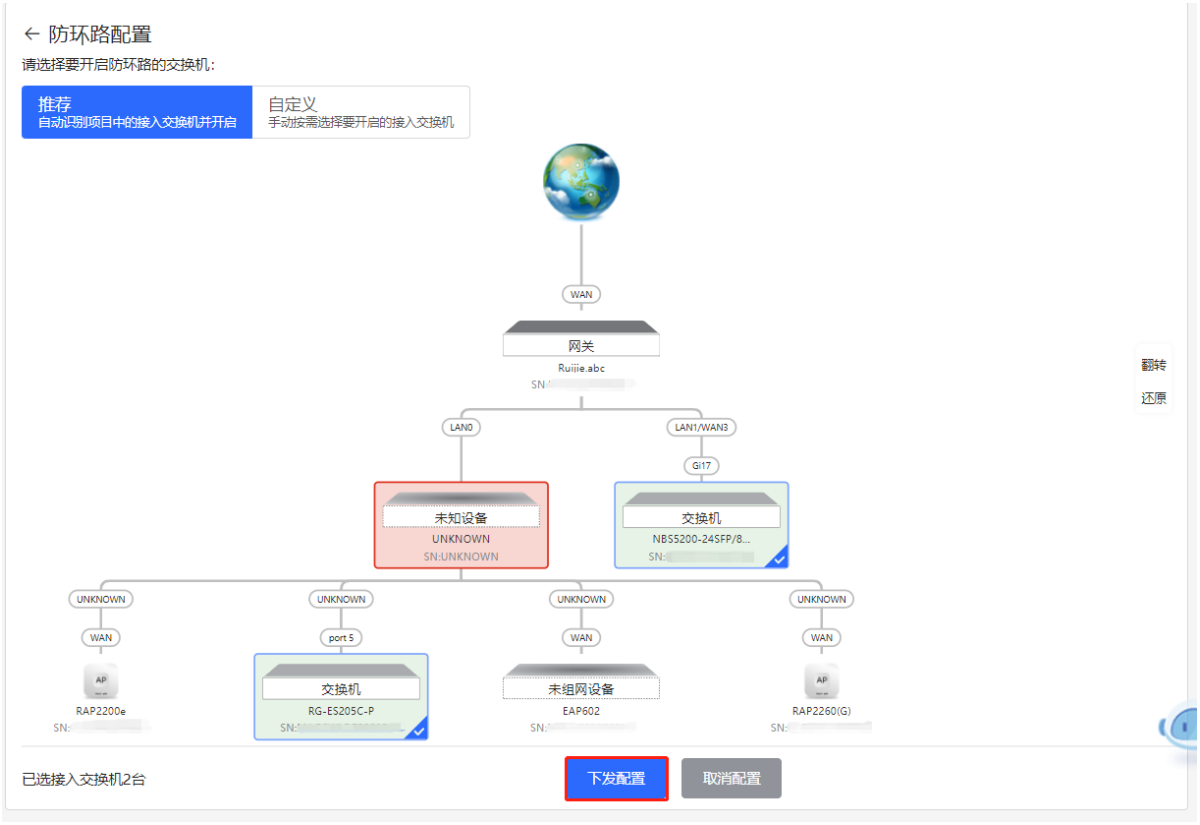
RLDP（Rapid Link Detection Protocol，快速链路检测协议）是一种以太网链路故障检测协议，用于快速检测链路故障和下联环路故障。开启防环路后，将避免出现环路导致的网络拥塞、连接中断等情况。发生环路后接入交换机环路的端口将被自动关闭。

5.1.2 配置步骤

【整网管理-页面向导】整网管理>>防环路

(1) 点击<开启>，进入防环路配置页面。

(2) 在组网拓扑中选择需要开启防环路功能的接入交换机，分为推荐和自定义两种方式：选择推荐，将自动选中网络中的全部接入交换机；选择自定义，可手动选择要开启防环路功能的交换机。点击<下发配置>，将在选中的交换机上开启防环路功能。



(3) 完成配置下发后，如需修改防环路功能的生效范围，点击<前往配置>，可在拓扑中重新选择开启防环路的交换机。点击防环路开关，可一键关闭网络中所有交换机上的防环路功能。

5.2 开启防私接

5.2.1 功能简介

防私接功能通过对客户端和服务器之间的DHCP交互报文进行窥探实现对用户IP地址使用情况的记录和监控，同时可以过滤非法DHCP报文，保证用户只能从控制范围内的DHCP服务器获取网络配置参数。开启防私接后，将避免出现“原网络中的上网终端获取到私自接入的路由器所分配的IP地址”，以保障网络的稳定性。

注意

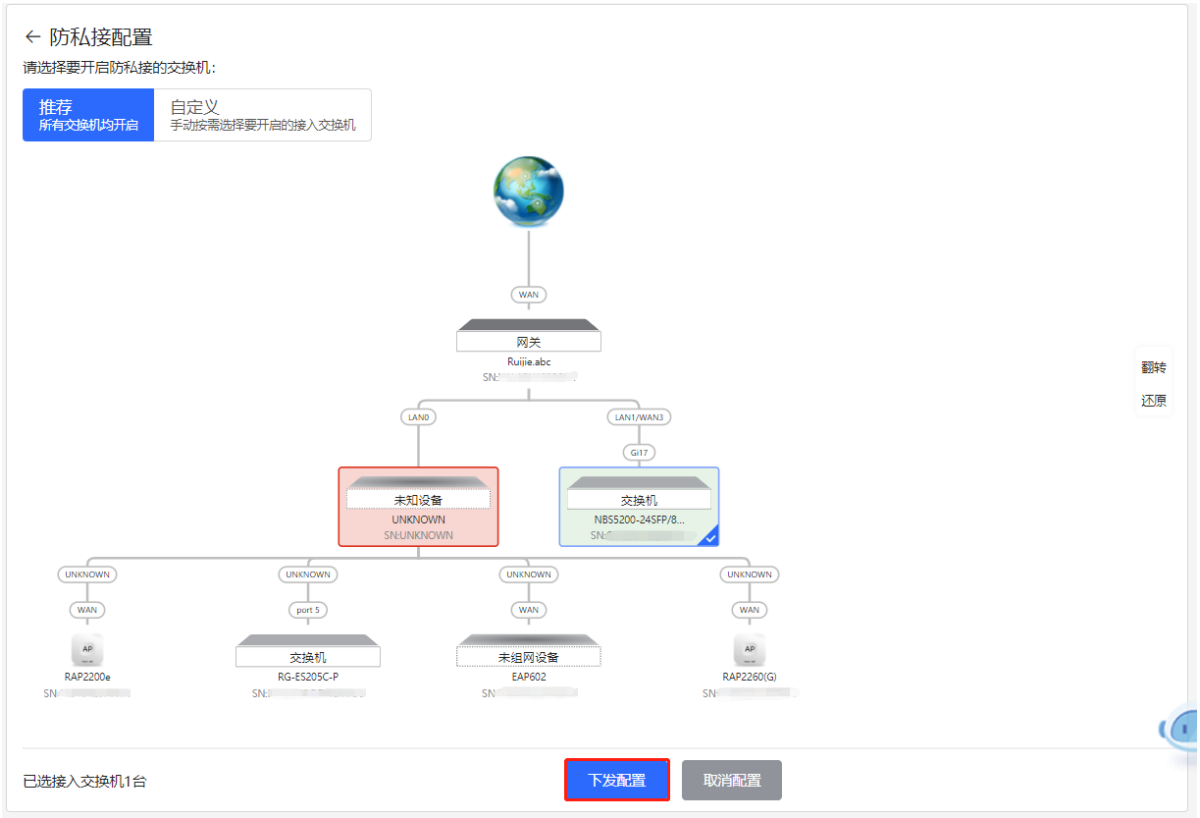
开启交换机的防私接功能，只能保证交换机不转发非法DHCP报文，但如果有用户直接连到私自接入的路由器，仍会获取到错误地址无法上网。此时需要找到私接的路由器关闭其DHCP或使用WAN口上联。

5.2.2 配置步骤

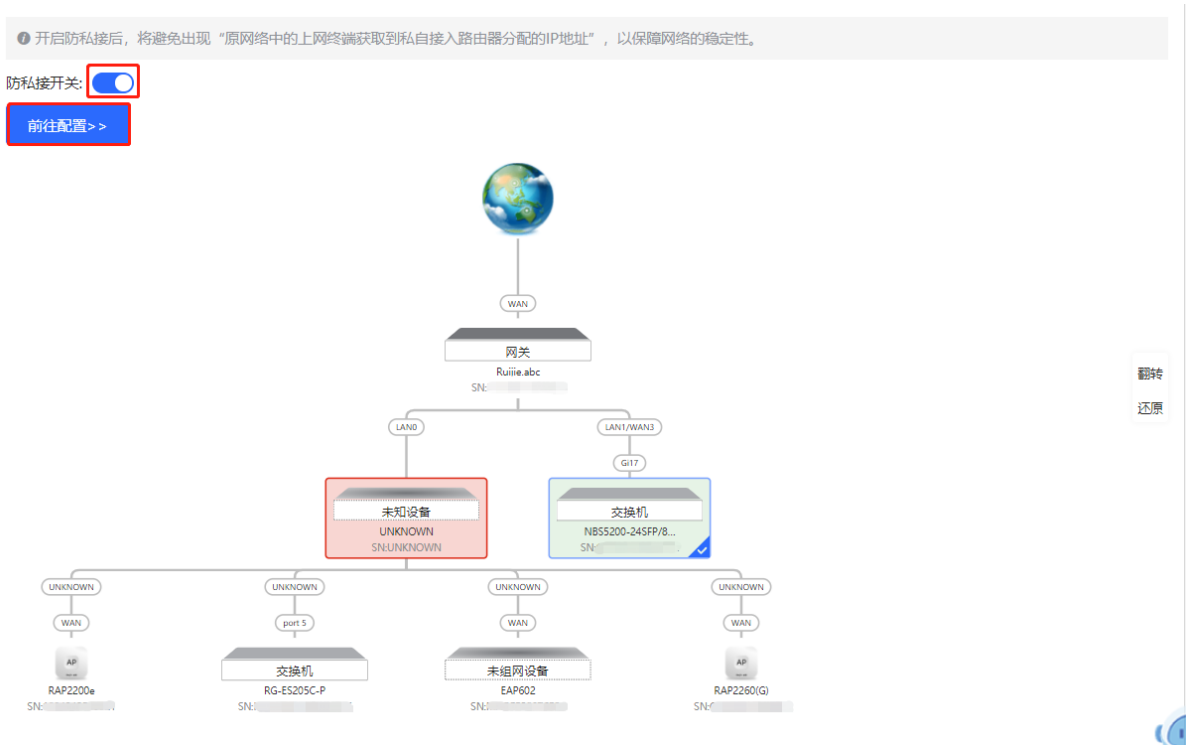
【整网管理-页面向导】整网管理>>防私接

(1) 点击<开启>，进入防私接配置页面。

(2) 在组网拓扑中选择需要开启防私接功能的接入交换机，分为推荐和自定义两种方式：选择推荐，将自动选中网络中的全部交换机；选择自定义，可手动选择要开启防私接功能的交换机。点击<下发配置>，将在选中的交换机上开启防私接功能。



(3) 完成配置下发后，如需修改防私接功能的生效范围，点击<前往配置>，可在拓扑中重新选择开启防私接的交换机。点击防私接开关，可一键关闭网络中所有交换机上的防接功能。



5.3 交换机批量设置

5.3.1 功能介绍

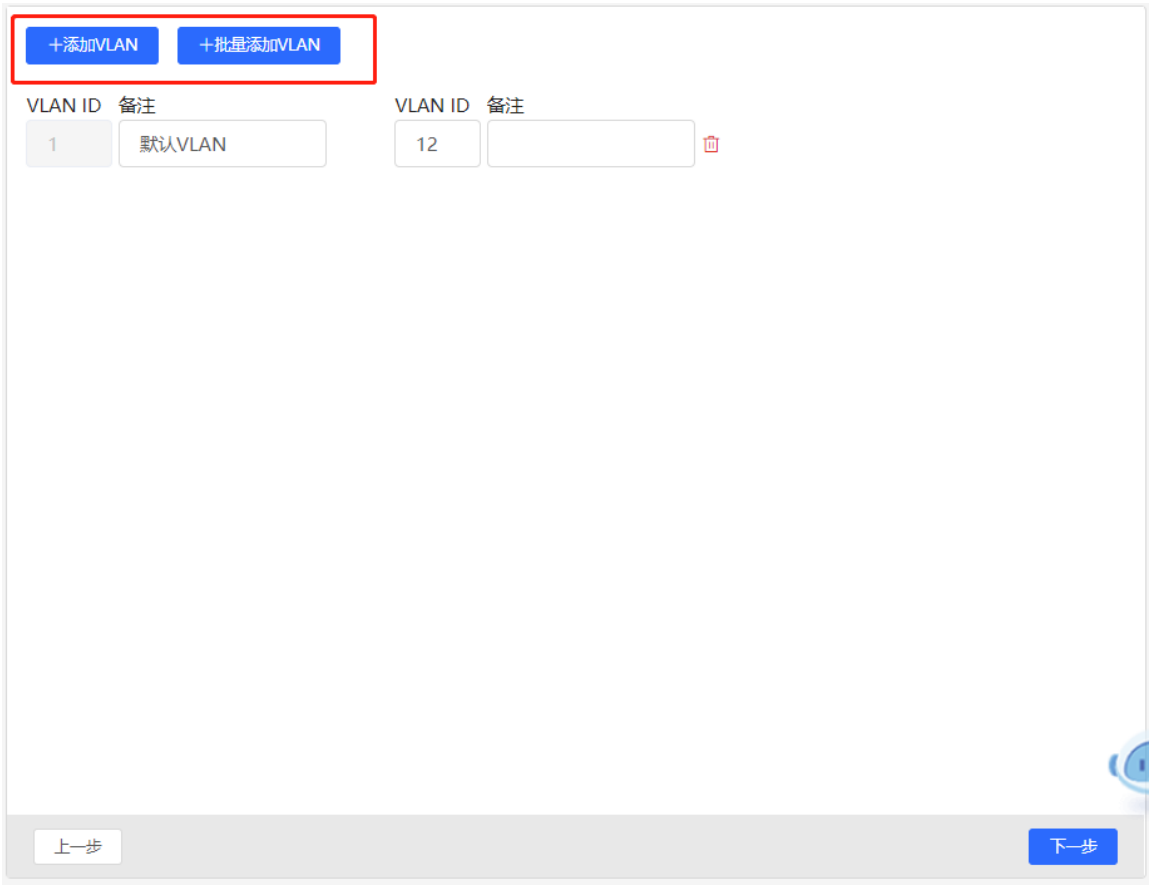
支持为组网中的交换机批量创建VLAN、设置端口属性以及划分端口VLAN。

5.3.2 配置步骤

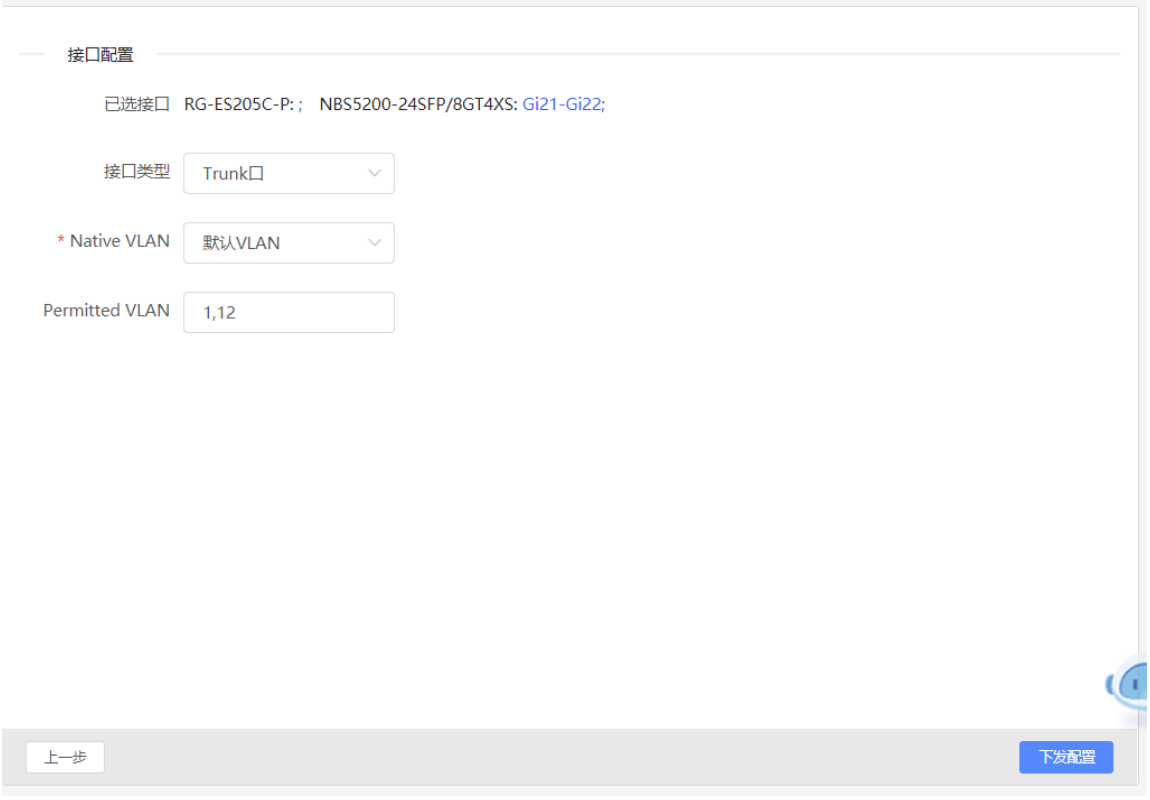
【整网管理-页面向导】整网管理>>交换机批量配置

(1) 页面将显示当前网络中所有的交换机，从中点击选择需要配置的设备，并在下方出现的设备端口视图中选择需要配置的端口。若当前网络中的设备较多，可在右上角下拉框中根据产品型号进行过滤。选择完毕后点击<下一步>。

(2) 点击<添加VLAN>即可为选中的设备批量创建VLAN。如需创建多个VLAN，点击<批量添加VLAN>并输入要创建的VLAN ID范围（如3-5,100）。完成VLAN设置后，点击<下一步>。

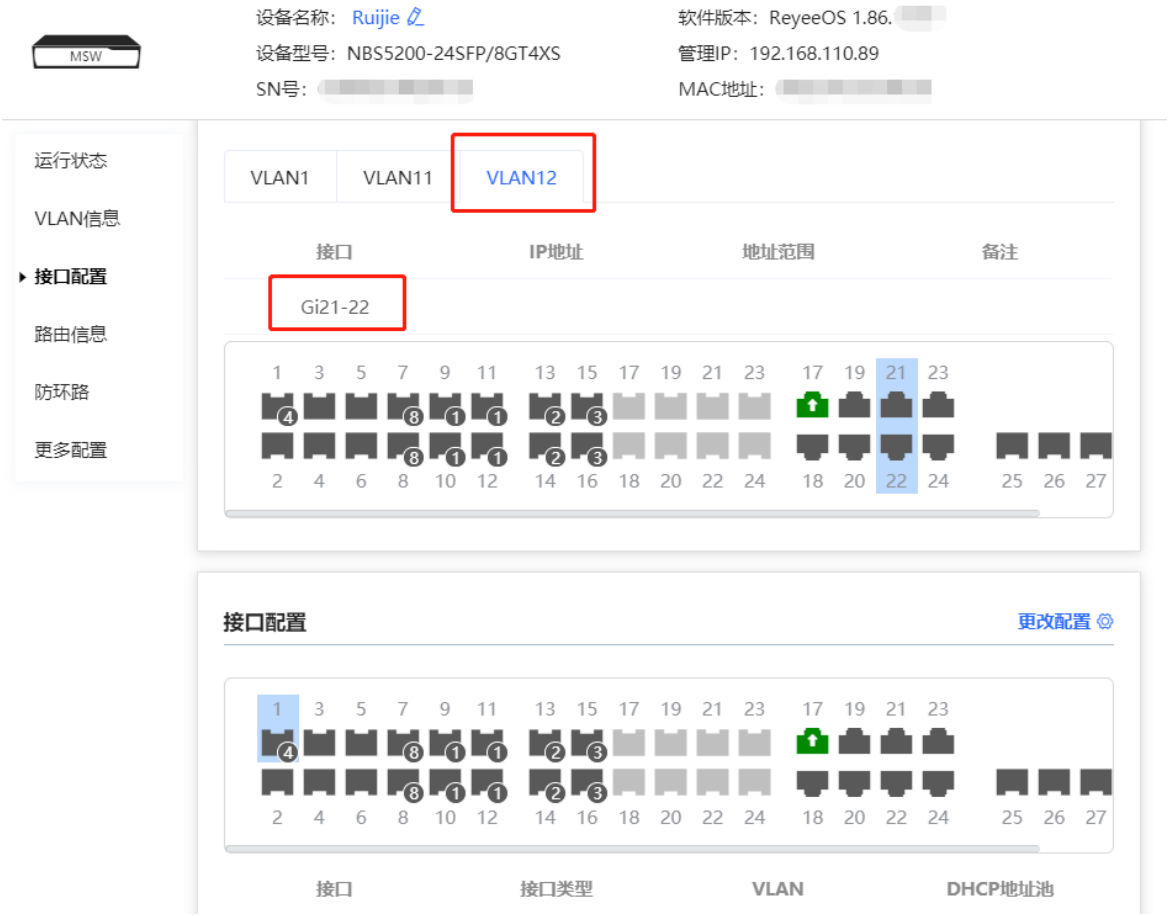


(3) 为第一步中选择的端口批量设置端口属性。选择端口类型，端口类型为“Access口”时需要设置端口的VLAN ID，端口类型为“Trunk口”时需要设置端口的Native VLAN和Permitted VLAN。完成端口属性设置后，点击<下发配置>，将批量配置下发至各设备。



5.3.3 效果验证

查看交换机的VLAN和接口信息，能查看到批量下发的配置。



6 上网行为管理

6.1 功能简介

行为管理即对内网用户上网行为的管理，表现为是否对用户的指定上网行为进行阻断或禁用。用户行为管理主要包含五大类，分别为应用控制、网站过滤、QQ管理、流量控制以及访问控制。其中，各行为管理策略均可通过指定用户IP及生效时间来灵活限制生效范围。

6.2 用户管理

6.2.1 功能简介

上网行为的管理策略往往需要灵活匹配具体的用户群体，在配置行为管理策略前先对用户进行管理、分类，能够有效提升配置效率，使管理更加高效。用户管理基于IP地址来维护用户信息，在进行上网行为管理时，可通过指定已创建或已认证的用户来限定应用阻断、流量审计、流控等业务的生效范围。

用户组包含两个默认根用户组：用户组和认证组。可在根用户组下创建和设置用户与用户组。

6.2.2 用户组

【本机管理-页面向导】行为管理>>用户管理

用户组下可以新增用户组或者用户，最多支持三级分组，而用户为叶节点，不可再下挂用户或用户组。所创建的用户分组可以在配置行为管理策略时作为配置选项，直接通过用户组名称进行引用。

用户组列表中默认存在“所有地址”组，包含地址段为1.1.1.1~255.255.255.255，不可修改或删除。

1. 创建用户组

点击用户组名称旁的 按钮或页面右上角的<添加>，在对话框中选择类型为“用户组”并输入组名称，点击<确定>，可在该用户组下创建子用户组。

表6-1 用户组配置信息描述表

参数	说明
父节点	设置所创建用户组所属的上级分组。目前用户组支持的最大层级数为三级（如：根节点/研发中心/研发1部），第三级分组下不允许创建用户组
组名称	用户组的名称

2. 创建用户

点击用户组名称，将显示当前分组下的用户信息。点击 按钮或页面右上角的<添加>，在对话框中选择类型为“用户”并输入用户名称和IP地址范围，点击<确定>，可在该用户组下创建用户。

表6-2 用户配置信息描述表

参数	说明
类型	可添加用户组或用户
父节点	设置所创建用户所属的分组，点击输入框将显示当前已创建的所有用户组，点击后自动填入
用户名称/类型	用户的名称，类型可选择IP或MAC
IP地址/范围	选择用户类型为IP类型时，用户的IP地址，可以是单个IP地址，也可以是IP地址范围。当某规则的生效用户范围包含该用户，则规则将在该IP地址范围内生效
MAC地址	选择用户类型为MAC类型时，输入用户的MAC地址。

3. 删除用户组或用户

点击用户组名称旁的按钮，可删除用户组及用户组下的用户；在用户列表中点击操作栏的<删除>，可删除指定用户。

4. 效果验证

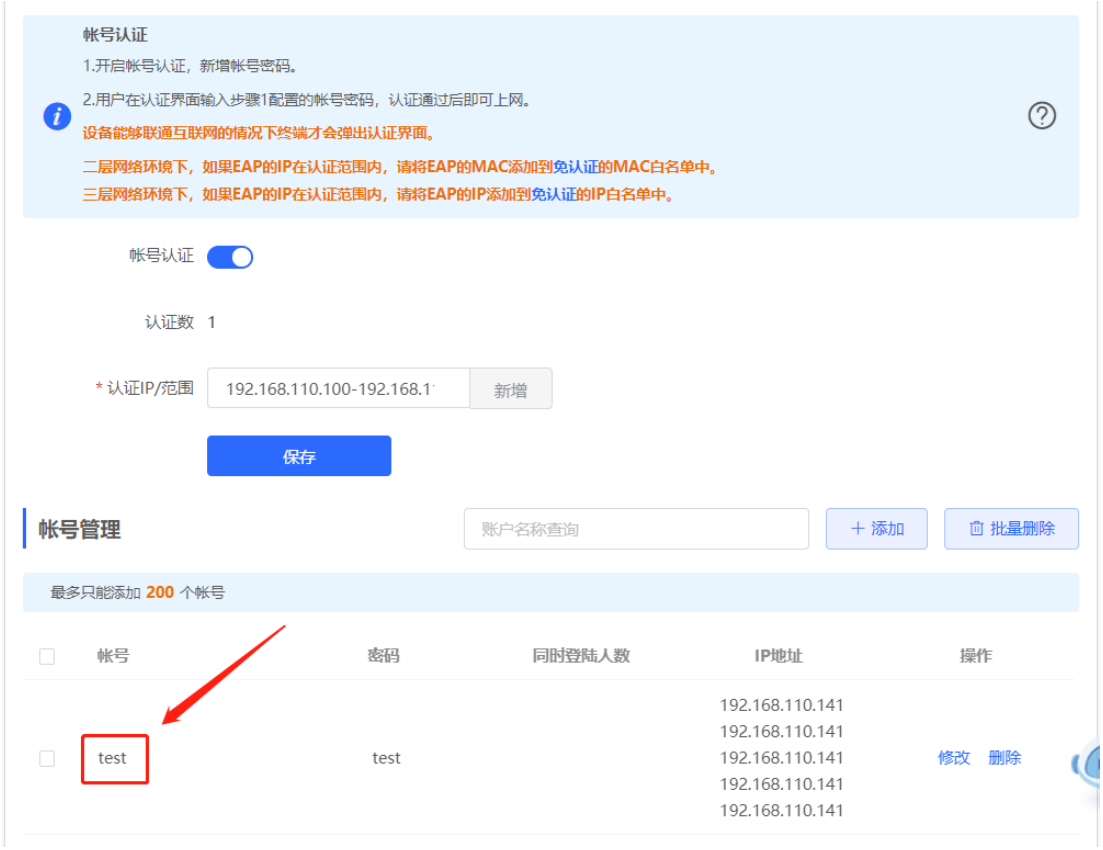
(1) 设置用户组和用户后，可以在页面左侧查看到创建的用户组；点击用户组，可查看该分组下的用户信息。

(2) 在设置行为管理策略（如添加应用控制规则）时，在用户组列表下能够查看并选择所创建的用户组以及用户成员。

6.2.3 认证组

【本机管理-页面向导】行为管理>>用户管理

认证组用户来源于认证服务器，能够从认证服务器上同步认证用户至认证组。其中，设备所设置的本地认证账号（参见4.9.6 本地账号认证）会自动同步到认证组的“本地认证组”下。



在设置行为管理策略（如添加应用控制规则）时，可设置策略在指定认证组上生效。认证用户上线后，将自动匹配认证组，并依此关联行为管理策略，实现对认证用户的上网行为控制。

6.3 时间管理

【本机管理-页面向导】行为管理>> 时间管理

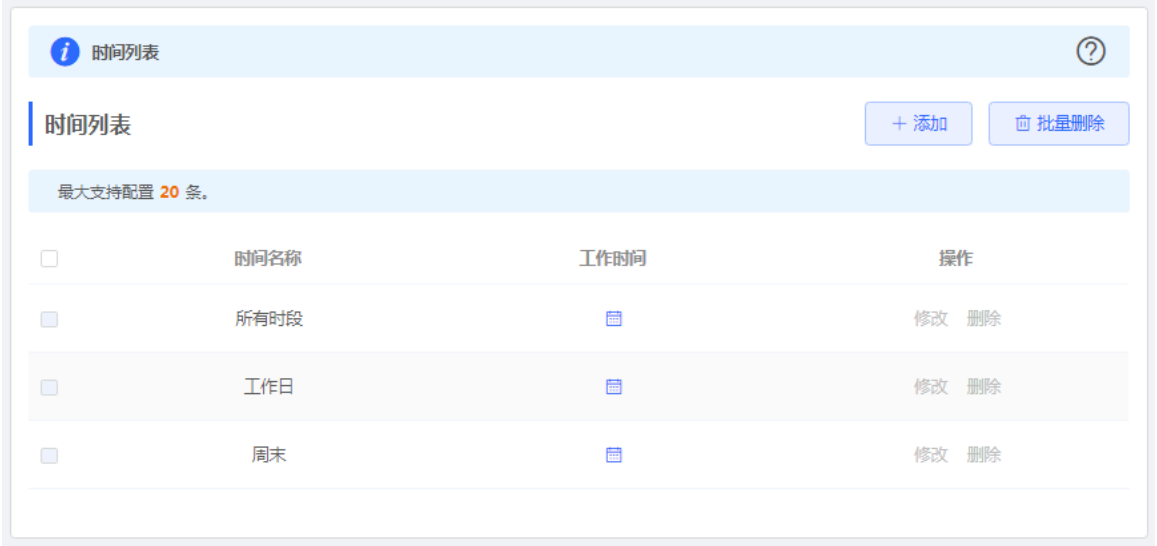
可以通过创建时间段，对时间进行分类。所创建的时间段可以在配置行为管理策略时作为配置选项，直接通过时间名称进行引用。

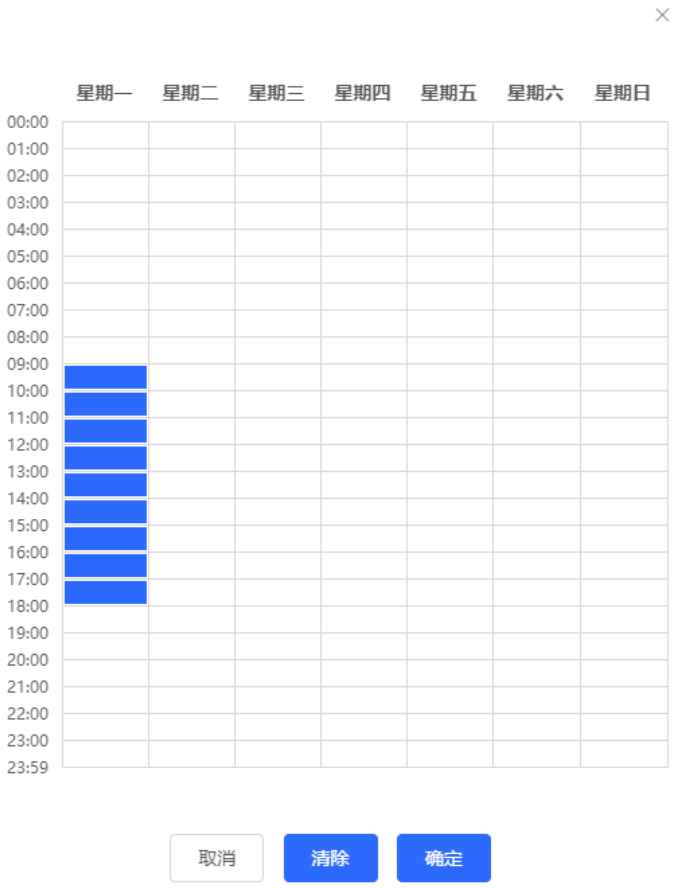
点击<添加>，输入时间名称并选择具体时间，可创建时间信息。

时间列表包含已创建的所有时段，点击<修改>，可以修改时间范围；点击<删除>，可以删除时段配置。默认存在“所有时段”、“工作日”和“周末”时段，不可修改或删除。

注意

创建的时间信息一旦在其他地方被引用（设置）则无法在“时间管理”页面直接删除，需要先解除引用。





6.4 应用控制

6.4.1 功能简介

应用控制，即控制用户所能访问的具体应用范围。默认不对用户访问的应用进行限制，用户可访问所有应用。设置应用控制策略后，用户在当前网络下无法访问被禁用的应用。可针对具体的用户群以及时间段设置禁用应用，如在办公网络下限制员工在工作时段访问娱乐游戏软件，以提高网络安全性。

6.4.2 配置步骤

【本机管理-页面向导】行为管理>>应用控制

1. 切换特征库

不同地区支持的应用列表不同，应用特征库版本分为中国版和国际版，请根据实际地区选择特征库版本。

点击选择特征库版本，在确认对话框中点击<确定>，稍等片刻后完成切换。

注意

- 切换特征库版本大概需要一分钟生效，请耐心等待片刻。
- 切换特征库版本后，原先的应用控制策略可能失效。请谨慎操作。

2. 设置应用控制

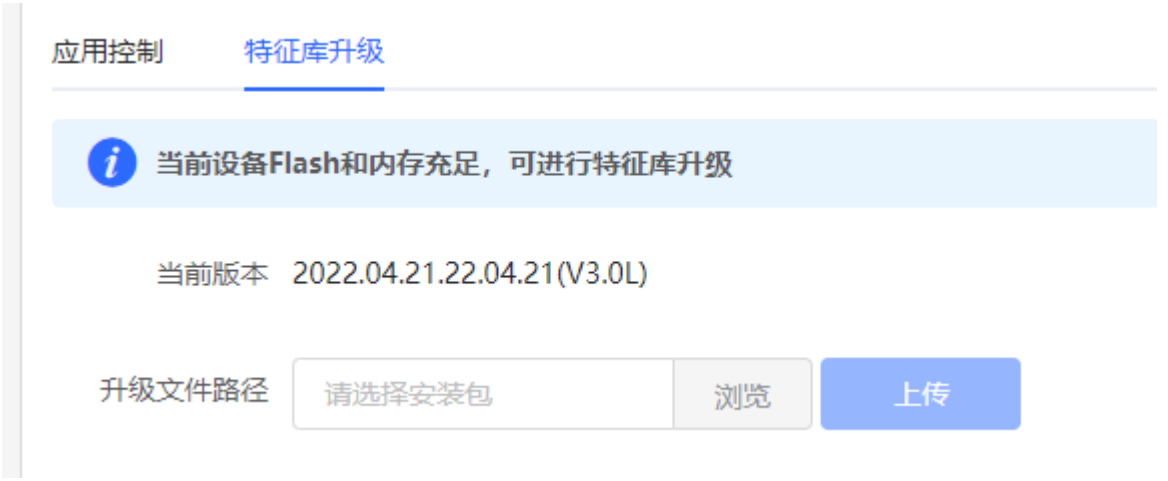
点击<添加>，创建应用控制策略。

表6-3 应用控制策略配置信息描述表

参数	说明
类型	应用控制策略的类型： ● 用户组：策略应用于指定用户组的用户。需要选择策略所应用的用户组。 ● 自定义：策略应用于指定IP地址段的用户。需要手动输入受管理的IP地址范围。
用户组	从用户组列表中选择策略所管理的用户，用户组列表在6.2 用户管理中设置。 若选中用户组下所有成员，则策略将对整个用户组生效（对后续添加到该用户组的成员也会生效）。
受管理IP地址组	受应用控制策略限制的IP地址范围，当策略类型为自定义时需要手动输入
受管理时间段	设置管控时间段，在受控时间内，受管理的终端无法访问禁用列表中勾选的应用。可在下拉框中选择6.3 时间管理里定义的时间段，或选择“自定义”，手动配置具体的时间段
禁用列表	需要禁止的应用或应用组
备注	策略的描述信息
状态	是否启用控制策略

3. 应用特征库升级

点击<浏览>，选择本地特征库文件，点击<上传>。



6.5 网站管理

6.5.1 功能简介

网站管理，包含网站分组和网站过滤两部分功能。网站分组指对具体的网站URL进行分类，可以对已有的分组进行修改，也可以新建网站分组；网站过滤则是对网站分组中已有的网站组群进行访问控制，禁止用户访问指定分组的网站。可以针对具体的用户群以及时间段进行网站过滤控制，如在办公网络下限制员工在工作时段访问游戏网站，以提高网络安全性。

6.5.2 配置步骤

【本机管理-页面向导】行为管理>> 网站管理

1. 设置网站分组

【本机管理-页面向导】行为管理>> 网站管理>>网站分组

点击“网站分组”页签跳转至对应设置页面，分组列表中包含已创建的网站分组。点击组成员列的“更多”，可查看分组下包含的所有网址；点击<修改>，可修改分组包含的成员网址；点击<删除>，可删除指定分组。

点击<添加>，可创建新的网站分组。

⚠ 注意

若网站分组在网站过滤规则中被引用，则无法在分组列表中被删除。若要删除该分组，则需要先修改网站过滤配置以解除引用。

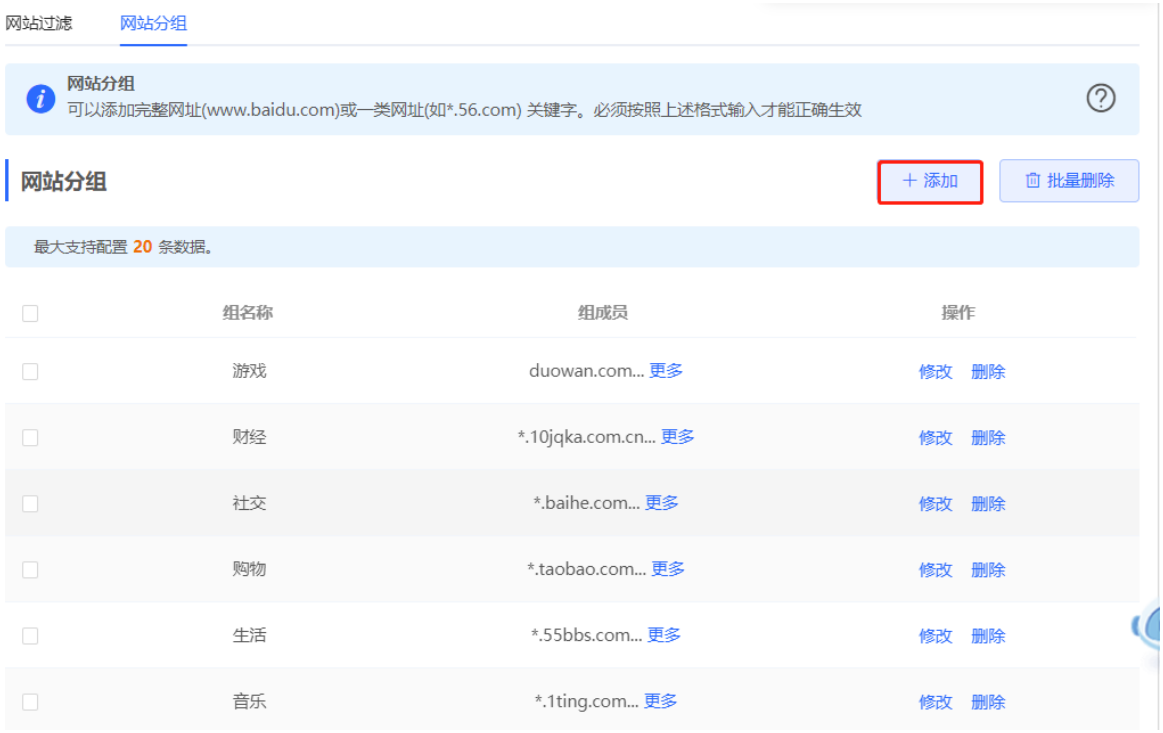


表6-4 网站分组配置信息描述表

参数	说明
组名称	为网站分组设置名称，1~64个字符，不同分组不能重名
组成员	网站分组成员，可以同时输入多个网站进行批量添加。组成员可以为完整网址（如www.baidu.com），也可以为网址关键字（在域名前面加通配符“*”，如*.baidu.com）。通配符“*”只允许在网址开头，而不能夹在域名中间或后面

2. 设置网站过滤

【本机管理-页面向导】行为管理>> 网站管理>> 网站过滤

点击“网站过滤”页签跳转至对应设置页面，过滤列表中包含已创建的网站过滤规则。点击<修改>，可修改规则信息；点击<删除>，可删除指定过滤规则。

点击<添加>，创建网站过滤规则。

表6-5 网站过滤配置信息描述表

参数	说明
类型	网站过滤规则的类型： ● 用户组：规则应用于指定用户组的用户。需要选择受管理的用户组。

参数	说明
	● 自定义：规则应用于指定IP地址段的用户。需要手动输入受管理的IP地址范围。
用户组	从用户组列表中选择规则所管理的用户，用户组列表在6.2 用户管理中设置。 若选中用户组下所有成员，则规则将对整个用户组生效（对后续添加到该用户组的成员也会生效）。
受管理IP地址组	受网站过滤规则限制的IP地址范围，当规则类型为自定义时需要手动输入
受管理时间段	设置管控时间段，在受控时间内，受管理的用户终端无法访问被禁用的网站。可在下拉框中选择6.3 时间管理里定义的时间段，或选择“自定义”，手动配置具体的时间段
禁用网站类型	设置需要禁止的网站类型，从已创建的网站分组中选择。选择某一分组后，则将禁止用户访问该分组下的所有网站。创建或修改网站分组请参考设置网站分组。
备注	规则的描述信息
状态	是否启用网站过滤规则

6.6 QQ 管理

6.6.1 功能简介

支持QQ黑名单和QQ白名单功能，可选择其中一种模式对QQ账号登录进行限制。

QQ黑名单模式：黑名单中的QQ账号将被禁止登录和收发消息，未加入黑名单的QQ账号不受限制。默认QQ黑名单为空，所有的QQ账号都能正常访问。

QQ白名单模式：白名单中的QQ账号能够正常访问，未加入白名单的QQ账号被禁止登录和收发消息。默认QQ白名单为空，即所有的QQ账号都被禁用。

6.6.2 配置步骤

【本机管理-页面向导】行为管理>> QQ管理

1. 切换 QQ 管理模式

默认为“关闭黑白名单模式”，所有QQ账号都能正常登录和访问外网。点击<黑名单模式>切换到黑名单模式，点击<白名单模式>切换到白名单模式。

2. 设置黑/白名单

【本机管理-页面向导】行为管理>> QQ管理>> 黑/白名单模式

切换到黑/白名单模式后，点击<添加>，创建黑/白名单表项。下面以QQ黑名单的配置步骤为例，白名单的配置步骤与之类似。

表6-6 QQ 黑/白名单配置信息描述表

参数	说明
类型	规则的生效用户类型： ● 用户组：规则应用于指定用户组的用户。需要选择受管理的用户组。

参数	说明
	● 自定义：规则应用于指定IP地址段的用户。需要手动输入受管理的IP地址范围。
用户组	从用户组列表中选择规则所管理的用户，用户组列表在6.2 用户管理中设置。 若选中用户组下所有成员，则策略将对整个用户组生效（对后续添加到该用户组的成员也会生效）。
受管理IP地址组	受QQ黑/白名单规则限制的IP地址范围，当规则类型为自定义时需要手动输入
受管理时间段	设置管控时间段，在受控时间内，受管理的用户终端无法登录被禁止的QQ账号。可在下拉框中选择6.3 时间管理里定义的时间段，或选择“自定义”，手动配置具体的时间段
禁止/允许的QQ号	黑名单模式下，设置需要禁止的QQ号；在受控时间内，受管理的用户终端无法登录被禁止的QQ号，其他QQ号可正常登录； 白名单模式下，设置允许正常登录的QQ号；在受控时间内，受管理的用户终端只能登录被允许的QQ号，其他QQ号都被禁用； 可输入多个QQ号码，不同QQ号间换行填写
备注	规则的描述信息
状态	是否启用该QQ管理规则

6.7 流量控制

6.7.1 功能简介

流量控制（Traffic Control）是将流量按照一定的规则进行分类，对不同类别的流量实施不同流量处理策略的机制。通过配置流量控制可以保障关键流量，并抑制恶意流量。用户可以在带宽不够充分或需要合理分配流量时启用流量控制。

6.7.2 智能流控

1. 功能简介

当用户需要对设备端口（如WAN、WAN1口）的上行流量和下行流量带宽进行限制时，可以选择开启智能流控功能。设置端口的线路带宽后，该端口下的流量将被限制在设置值范围内，同时将根据用户数量智能调整每个用户的带宽，保证每个用户公平分享带宽。

2. 配置步骤

【本机管理-页面向导】行为管理>> 流控设置>> 智能流控

点击按钮开启智能流控功能，根据运营商实际分配的带宽设定线路带宽。若设备存在多线路，支持对多个WAN口进行独立的带宽设置。多线路的相关配置请参考3.2 设置WAN口。

点击<保存>使配置生效。

⚠ 注意

开启流量控制后将影响测速，如需测试网速，请先关闭流控功能。

表6-7 智能流控配置信息描述表

参数	说明
是否开启	是否开启智能流控功能。智能流控功能默认处于关闭状态
WAN口线路带宽	设置端口上传（上行）和下载（下行）的限制带宽值，单位为Mbps

说明

智能流控功能支持对不同联网方式的线路进行流量控制，包括宽带上网、静态IP方式和动态IP方式。

6.7.3 自定义策略

1. 功能介绍

自定义策略用于在智能流控功能的基础上进一步实现对特定IP地址的流量的限制，从而满足特定的用户或服务器的带宽需要。在创建自定义流控策略时，用户可以灵活配置受限的用户范围、用户的限制带宽值、受限的应用流量以及限速模式。自定义策略处于启用状态时将优先于智能流控配置生效。

2. 配置前的准备

在配置自定义策略前，需要先开启智能流控功能。请参考6.7.2 智能流控进行设置。

3. 配置步骤

【本机管理-页面向导】行为管理>> 流控设置>> 自定义策略

(1) 切换特征库

不同地区支持的应用列表不同，应用特征库版本分为中国版和国际版，请根据实际地区选择特征库版本。

点击选择特征库版本，在确认对话框中点击<确定>，稍等片刻后完成切换。

注意

- 切换特征库版本大概需要一分钟生效，请耐心等待片刻。

- 切换特征库版本后，会重置应用优先级的模板内容（应用优先级的介绍请参考6.7.4 应用优先级），并且应用控制策略（应用控制策略的介绍请参考6.4 应用控制）可能失效。请谨慎操作。

(2) 设置自定义策略

点击<添加>，创建自定义流控策略。最多支持设置30条自定义策略。

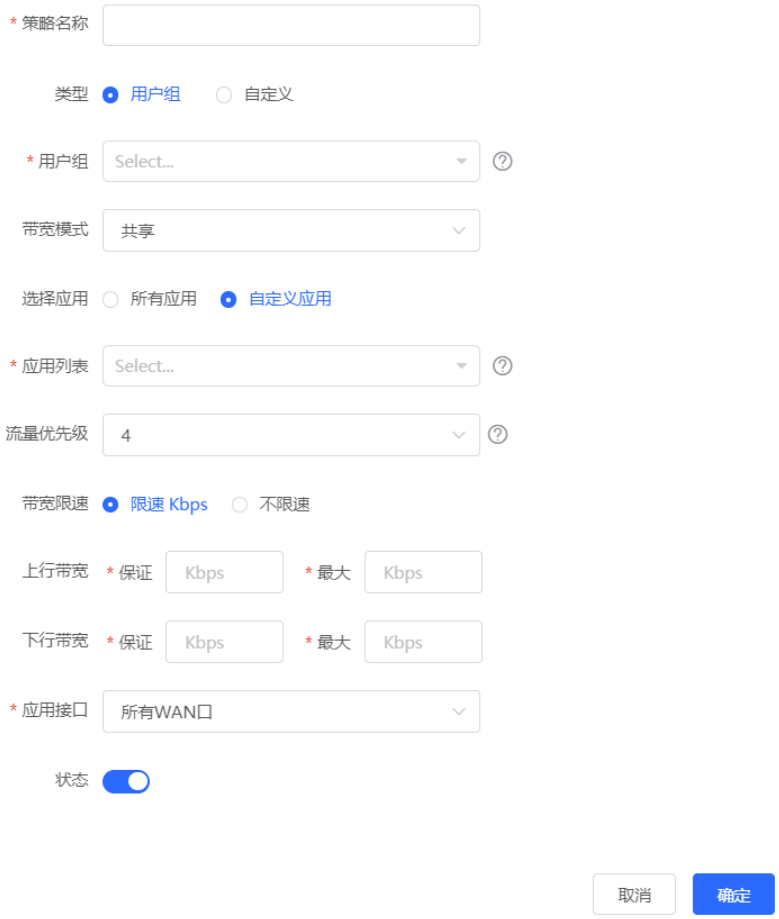
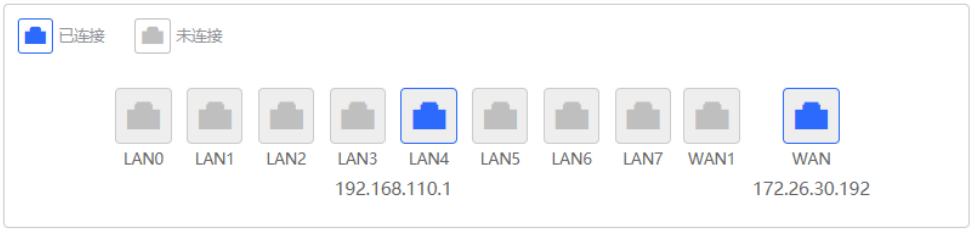


表6-8 自定义策略配置信息描述表

参数	说明
策略名称	自定义流控策略的唯一标识，不支持修改
类型	流控策略的类型： ● 用户组：策略应用于指定用户组的用户。需要选择受管理的用户组。 ● 自定义：策略应用于指定IP地址段的用户。需要手动输入受管理的IP地址范围。
用户组	从用户组列表中选择策略所管理的用户，用户组列表在6.2 用户管理中设置。 若选中用户组下所有成员，则策略将对整个用户组生效（对后续添加到该用户组的成员也会生效）。
IP地址/范围	配置流量控制策略生效的IP地址范围，当规则类型为自定义时需要手动输入，可配置为单个IP地址或者IP地址网段 IP地址范围必须处于LAN网段，用户可在[设备概览]>> [端口信息]中查看当前LAN口网段。例如，下图设备的LAN口网段为192.168.110.0/24。 
带宽模式	● 共享：用户组内所有用户（地址范围内所有IP）共用设定的上下行带宽，不对单个用户的带宽进行限制 ● 独立：用户组内所有用户（地址范围内所有IP）共用设定的上下行带宽，同时可对单个用户的最大带宽进行限制
选择应用	带宽模式为共享模式时，支持设置流控策略只对指定应用生效： ● 所有应用：流控策略对当前特征库中的所有应用生效 ● 自定义应用：流控策略只对“应用列表”中的指定应用生效 带宽模式为独立模式时，不支持选择应用，默认对当前特征库中的所有应用生效。
应用列表	“选择应用”为“自定义应用”时，设置策略对哪些应用生效。被选择的应用的流量将受到策略限制
流量优先级	流量的保障等级，取值范围为0~7，优先级值越小，优先级越高，0表示最高优先级。 流量优先级值与应用优先级模板的应用组相对应，2对应关键通道，4对应普通通道，6对应抑制通道，关于优先级模板的应用组的介绍，请参考6.7.4 。
带宽限速	是否限制带宽 ● 限速Kbps：用户可根据需要设置上下行带宽限速值 ● 不限速：带宽富余时，其使用的最大带宽不受到限制；带宽紧张时，最小带宽不得到保证

参数	说明
上/下行带宽	上传和下载的数据传输速率，分为保证带宽、最大带宽和每用户最大带宽，单位为Kbps ● 保证带宽：带宽紧张时保障所有用户可共享的最小带宽 ● 最大带宽：带宽宽松时所有用户一共所能占用的最大带宽 ● 每用户最大带宽：多用户共享带宽时，每个用户所能占用的最大带宽。可选配置，仅在带宽模式为独立模式时支持配置，默认不限速
应用接口	设置该策略在哪个WAN口上生效。配置为“所有WAN口”则各WAN口都将分别应用该策略
状态	设置是否启用该流控策略。若关闭，则策略不生效

注意

特征库版本切换后，可能需要重新配置应用列表。

(3) 查看自定义流控策略

当前配置的自定义策略可以在“策略列表”中查看。可对策略进行修改和删除；勾选需要删除的策略，并点击<批量删除>，可删除选中策略。

表6-9 策略列表信息描述表

参数	说明
应用列表	“应用列表”包含当前受策略管控的应用，若特征库版本与当前策略设置的”自定义应用”相匹配，则应用列表显示为绿色 自定义应用 ，若不匹配则显示灰色 自定义应用
状态	表示当前策略的启用状态，单击可修改状态，若特征库版本与当前策略所支持的“自定义应用”不匹配，则不允许直接修改状态，需用户点击操作栏的<修改>来编辑策略或切换至相应特征库版本
生效状态	表示这条策略规则在当前系统中是否已经生效。如果显示为“未生效”，请检查策略是否开启、策略对应的接口是否存在、接口是否在线以及“特征库版本”是否与当前策略所配置的应用匹配
匹配顺序	默认按照策略列表由上至下的顺序进行匹配，新增的策略排在最前面，优先匹配。可以手动调整策略的匹配顺序，点击 上移策略，使策略优先匹配；点击 下移策略，使策略滞缓匹配
操作	对自定义策略进行修改与删除操作

6.7.4 应用优先级

1. 功能介绍

在开启智能流控的基础上，可设置应用的优先级，使优先级高的应用的带宽能得到优先保证，优先级低的应用的带宽受到抑制。用户可根据需求，分别定义需要优先保证带宽和需要抑制带宽的的应用列表。

注意

若同一个应用同时存在于自定义策略和应用优先级的应用列表时，以自定义策略为准。

2. 配置前的准备

- 在配置应用优先级前，需要先开启智能流控功能。请参考6.7.2 智能流控进行设置。
- 在自定义策略（见6.7.3 ）页面确认已选择适当的特征库版本。

3. 配置步骤

【本机管理-页面向导】行为管理>> 流控设置>> 应用优先级

(1) 设置应用优先级模板

在“应用优先级”下拉框中选择使用的模板。

为满足不同的使用场景，“应用优先级”预置了4个模板，用户可根据需求进行切换。

4个“应用优先级”模板包括：

- 不使用模板：设备初始化时为此模板，不对任何应用的流量进行保证或抑制
- 办公模板：针对办公场景而设计，优先保证办公场景的应用流量
- 家庭模板：针对家庭场景而设计，优先保证家庭场景的应用流量
- 娱乐模板：针对娱乐场景而设计，优先保证娱乐场景的应用流量

(2) 设置应用组列表

每个默认模板存在3个应用组，分别为关键通道应用组、抑制通道应用组以及普通通道应用组。各应用组间的应用流量保障优先级为：关键通道>普通通道>抑制通道

- 关键通道：该通道的“应用列表”所包含的应用在使用时，流量得到优先保证。
- 抑制通道：该通道的“应用列表”所包含的应用在使用时，流量被抑制，以保障优先级更高的应用流量。
- 普通通道：该通道包含了特征库所有应用中，除“关键通道”和“抑制通道”以外的应用。该通道的应用流量在关键通道之后得到保证。

选择模板后，页面显示当前模板的三个应用组“关键通道”、“抑制通道”以及“普通通道”，及每个通道对应的应用列表，点击<更多>可查看每个“应用列表”的详细信息。

点击操作栏下的<修改>，可对关键通道应用组和抑制通道应用组的应用列表进行编辑，使应用流量得到优先保证或抑制。

注意

- 特征库版本的切换会导致“应用列表”中的应用得到相应变化。
- 切换应用优先级模板会重置应用列表。

6.8 访问控制

6.8.1 功能简介

访问控制功能通过对经过设备的数据包进行规则匹配，并设置在某一时间范围内，放行或丢弃数据包，从而控制内网用户是否能访问外网以及某条数据流是否被阻断。支持根据MAC地址或者IP地址进行报文匹配。

6.8.2 配置步骤

【本机管理-页面向导】行为管理>> 访问控制

访问控制规则列表包含已创建的访问控制规则。点击<添加>，可新增访问控制规则。

表6-10 访问控制规则信息描述表

参数	说明
生效状态	表示规则是否已经生效。如果显示为“未生效”，可能是当前系统时间不在生效时段内，鼠标移至 可查看具体原因
匹配顺序	默认按照列表由上至下的顺序进行规则匹配，新增的规则排在最前面，优先匹配。可以手动调整规则的匹配顺序，点击 上移规则，使规则优先匹配；点击 下移规则，使规则滞缓匹配
操作	对规则进行修改与删除操作

1. 设置基于 MAC 地址的控制规则

控制规则将对数据包的源MAC地址进行匹配，常用于控制在线用户或特定终端能否访问外网。

选择“基于MAC地址”，输入在线用户的MAC地址并选择规则类型和生效时段，点击<确定>。

说明

基于MAC地址的匹配规则，默认是对外网口生效。

表6-11 基于 MAC 地址的访问控制规则配置信息描述表

参数	说明
MAC地址	输入需要控制的用户的MAC地址。点击输入框将弹出当前在线用户信息，点击可自动填入对应MAC地址
规则类型	设置规则对符合匹配条件的数据包的处理方式 ● 允许：放行符合条件的数据包 ● 阻断：丢弃符合条件的数据包
生效时段	选择规则生效的时间段，可在下拉框中选择6.3 时间管理里定义的时间段，或选择“自定义”，手动设置具体的时间段
备注	输入规则的描述信息，可用于标识规则的用途

2. 设置基于 IP 地址的控制规则

控制规则将对数据流的源IP地址、目的IP地址和协议号进行匹配。

选择“基于IP地址”，输入数据流的源IP地址和端口和目的IP地址和端口，并选择协议类型、规则类型、生效时间以及生效接口域，点击<确定>。

注意

- 基于IP地址的访问控制规则仅单向生效。比如配置一条阻断的规则，源IP段是192.168.1.0/24，目的IP段是192.168.2.0/24。此时192.168.1.x的设备无法访问192.168.2.x的设备，但是192.168.2.x的设备是可以访问192.168.1.x的设备。如果要实现网段的双向禁止，需要再配置一条源IP段为192.168.2.0/24，目的IP段为192.168.1.0/24的阻断规则。
- L2TP/PPTP VPN只支持基于IP的访问控制，且生效接口域必须配置在内网。


添加访问规则
基于
MAC地址
IP地址
源IP地址:端口
网段：192.168.1.1/24
:
1-65535
目的IP地址:端口
网段：192.168.1.1/24
:
1-65535
协议类型
所有协议
规则类型
阻断（反向流不匹配）
生效时段
所有时段
生效接口域
访问外网
备注
标识规则用途
取消
确定

表6-12 基于 IP 地址的访问控制规则配置信息描述表

参数	说明
源IP地址:端口	匹配数据包的源地址和端口，为空表示所有地址/所有端口。源IP地址可以是单个IP地址（如192.168.1.1），也可以是一个网段（如192.168.1.1/24）
目的IP地址:端口	匹配数据包的目的地址和端口，为空表示所有地址/所有端口。目的IP地址可以是单个IP地址（如192.168.1.1），也可以是一个网段（如192.168.1.1/24）
协议类型	匹配数据包的协议类型，可选择TCP、UDP和ICMP协议
规则类型	设置规则对符合匹配条件的数据包的处理方式 ● 允许：放行符合条件的数据包 ● 阻断：丢弃符合条件的数据包，仅单向生效，反向流不阻断
生效时段	选择规则生效的时间段，可在下拉框中选择6.3 时间管理里定义的时间段，或选择“自定义”，手动设置具体的时间段
生效接口域	选择规则对应生效的接口 ● 内网互访：在LAN口上生效，对内网数据包进行访问控制 ● 访问外网：在WAN口上生效，对来自或发往外网的数据包进行控制
备注	输入规则的描述信息，可用于标识规则的用途

6.9 在线用户管理

【页面向导】（终端管理>>）在线用户

查看当前网络中的有线用户和无线用户。点击“访问控制”栏的“前往”，可创建一条针对该在线用户的访问控制规则，对终端的上网行为、联网时段等进行控制。访问控制规则的设置请参考6.8 。

表6-13 在线用户信息描述表

参数	说明
名称/接入类型	接入的终端名称和接入方式，分为无线接入和有线接入

参数	说明
接入位置	终端有线连接或通过无线信号关联的设备的SN号
IP地址/MAC地址	终端的IP地址和MAC地址
当前速率	当前上传和下载的数据传输速率
无线信息	接入类型为无线接入的用户会显示无线信号信息，包含信道、信号强度、用户在线时间和协商速率

7 VPN

7.1 设置 IPSec VPN

7.1.1 功能简介

1. IPSec 概述

IPsec（IP Security，IP安全）是Internet工程任务组（IETF）制定的三层隧道加密协议，用来提供网络的端对端加密和验证服务，为网络上传输的数据提供了高质量、可互操作和基于密码学的安全保证。特定的通信方之间在IP层通过加密与数据源认证等方式，可以获得以下的安全服务：

- 数据机密性（Confidentiality）：IPsec发送方在通过网络传输报文前，先加密报文。
- 数据完整性（Data Integrity）：IPSec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（Data Authentication）：IPSec接收方可以认证IPSec报文的发送方是否合法。
- 防重放（Anti-Replay）：IPSec接收方可检测并拒绝接收过时或重复的报文。

IPSec协议广泛应用于组织总部和分支机构之间的组网互联，当前设备支持部署IPSec服务器或客户端。基于IPSec协议建立总部与各个分支机构之间的安全隧道，能够保证传输数据的机密性，提高网络安全性。

2. IKE 概述

IPsec在两个端点之间提供安全通信，端点被称为IPsec对等体。SA（Security Association，安全联盟）是通信对等体间对某些要素的约定，例如对等体间使用何种安全协议、需要保护的数据流特征、对等体间传输的数据的封装模式、协议采用的加密和验证算法，以及用于数据安全转换、传输的密钥和SA的生存周期等。在配置IPsec的过程中，可以使用IKE（Internet Key Exchange，因特网密钥交换）协议来建立SA。IKE为IPSec提供自动协商交换密钥、建立和维护SA的服务，简化了IPSec的使用和管理。

3. IPSec 安全策略

IPSec安全策略规定了对什么样的数据流采用什么样的安全提议（相当于SA）。通过在通信两端设置相匹配的安全策略，IPSec客户端与IPSec服务端之间能够建立起IPSec安全隧道，实现对通信数据的保护。IPSec安全策略分为基础设置和高级设置两个部分，其中高级设置包含了具体的IKE策略与连接策略，为可选配置，无特殊需求可保持默认，如需配置请参考配置步骤说明。

7.1.2 设置 IPSec 服务端

【本机管理-页面向导】VPN管理>> IPSec设置>> IPSec安全策略

1. 基本配置

点击<添加>，选择“策略类型”为“服务端”，填写策略名称、本地子网范围并设置预共享密钥，点击<确定>。

表7-1 IPSec 服务端基本设置信息描述表

参数	说明
策略名称	设置IPSec安全策略的名称，1~28个字符
绑定接口	从下拉列表中指定本地使用的WAN口；通信对端（IPSec客户端）所设置的“对端网关地址”必须与该WAN口的IP地址相同 多线路情况下，推荐设置为“自动”
本地子网范围	设置受保护的数据流的本地子网范围，即服务器端的LAN口网段，由IP地址和子网掩码来确定
预共享密钥	通信双方必须指定相同的预共享密钥作为它们之间相互认证的凭证，并且为了安全起

参数	说明
	见，不同的对等体对之间应配置不同的密钥，即对于每对<IPSec服务端的绑定接口，IPSec客户端的对端网关>，都需要配置唯一且相同的预共享密钥
状态	是否启用该安全策略

2. 高级配置（阶段一）

点击“阶段一设置（IKE策略）”展开配置项。若无特殊需求可保持默认配置。

表7-2 IPSec 服务端 IKE 策略设置信息描述表

参数	说明
IKE策略	选择IKE协议使用的散列算法、参数加密算法和Diffie-Hellman组标识，IKE策略为三个参数的组合。支持设置5套IKE策略，参与IKE协商的双方至少拥有一套一致的IKE策略，这是IKE协商成功的必要条件。 ● 散列（HASH）算法： ○ sha1：SHA-1算法

参数	说明
	○ md5：MD5算法 ● 加密算法： ○ des：密钥长度为56比特的DES算法 ○ 3des：密钥长度为168比特的3DES算法 ○ aes-128：密钥长度为128比特的AES算法 ○ aes-192：密钥长度为192比特的AES算法 ○ aes-256：密钥长度为256比特的AES算法 ● Diffie-Hellman组标识： ○ dh1：768比特Diffie-Hellman组 ○ dh2：1024比特Diffie-Hellman组 ○ dh5：1536比特Diffie-Hellman组
协商模式	分为主模式和野蛮模式。IPSec要求服务器端和客户端的协商模式一致。 ● 主模式：一般情况下，主模式适用于两设备的公网IP固定、设备之间点对点通信的环境。主模式会对对端身份进行保护，安全性较高。 ● 野蛮模式：对于例如ADSL拨号用户，其获得的公网IP不是固定的，且可能存在NAT设备的情况下，则需要采用野蛮模式做NAT穿越；同时，由于IP不是固定的，还需要额外设置身份（ID）类型为“NAME”。野蛮模式不保护对端身份，安全性较低。
本地/对端ID类型	用于身份认证的ID类型。对端的“本地ID”必须与本端的“对端ID”保持一致。 ● IP地址：以IP地址作为身份ID，自动生成本端身份ID和对端身份ID ● NAME：以主机字符串作为身份ID，自动生成本端身份ID和对端身份ID。当IP地址不固定时，需设置本地ID类型为“NAME”，并在对端做相应兼容修改。ID类型为“NAME”时，需要同时设置作为身份ID的主机字符串。
本地/对端ID	ID类型为“NAME”时，作为身份ID的主机字符串。对端的“本地ID”必须与本端的“对端ID”保持一致。
生存时间	设置IKE SA存在的生命周期（IKE SA实际的生命周期以协商结果为准），建议采用默认值
DPD检测开启	DPD（Dead Peer Detection，对等体存活检测）用于IPsec邻居状态的检测。启用DPD功能后，当接收端在触发DPD的时间间隔内未接收到对端的IPSec加密报文时，会触发DPD查询，主动向对端发送请求报文，对IKE对等体是否存在进行检测。 当链路不稳定的情况下，建议配置DPD功能
DPD检测周期	指定对等体DPD检测周期，即触发DPD查询的间隔时间，建议保持默认

3. 高级配置（阶段二）

点击阶段二设置（建立连接策略）展开配置项。若无特殊需求可保持默认配置。

表7-3 IPSec 服务端连接策略设置信息描述表

参数	说明
转换集	特定安全协议和算法的组合。在IPSec安全联盟协商期间，两端使用同一个特定的变换集合来保护特定的数据流。IPSec服务器和客户端的转换集配置要保持一致 ● 安全协议：ESP（Encapsulating Security Payload，报文安全封装）协议为IPSec连接提供了数据源认证、数据完整性校验和防报文重放功能，并保证了数据的机密性 ● 验证算法： ○ sha1：SHA-1 HMAC验证算法 ○ md5：MD5 HMAC验证算法 ● 加密算法： ○ des：密钥长度为56比特的DES算法 ○ 3des：密钥长度为168比特的3DES算法 ○ aes-128：密钥长度为128比特的AES算法 ○ aes-192：密钥长度为192比特的AES算法 ○ aes-256：密钥长度为256比特的AES算法
完美向前加密	PFS（Perfect Forward Secrecy，完美向前加密）特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。IKE在使用安全策略发起一个协商时，可以进行一个PFS交换。如果本端设置了PFS特性，则发起协商的对端也必须设置PFS特性，且本端和对端指定的DH组必须一致，否则协商会失败 ● none：关闭PFS特性 ● d1：768位DH组 ● d2：1024位DH组 ● d5：1536位DH组 缺省情况下，PFS特性处于关闭状态.

7.1.3 设置 IPSec 客户端

【本机管理-页面向导】VPN管理>> IPSec设置>> IPSec安全策略

点击<添加>，选择“策略类型”为“客户端”，填写策略名称、对端网关、本地子网范围、对端子网范围并设置预共享密钥，点击<确定>。

表7-4 IPSec 客户端基本设置信息描述表

参数	说明
策略名称	设置IPSec安全策略的名称，1~28个字符
对端网关	填写对端的IP地址或域名
绑定接口	从下拉列表中指定本地使用的WAN口。多线路情况下，推荐设置为“自动”
本地子网范围	设置受保护的数据流的本地子网范围，即服务器端的LAN口网段，由IP地址和子网掩码来确定
对端子网范围	设置受保护的数据流的对端子网范围，即客户端的LAN口网段，由IP地址和子网掩码来确定
预共享密钥	设置与IPSec服务端相同的预共享密钥
状态	是否启用该安全策略

高级配置相关参数可参考服务器端的配置参数说明（见高级配置（阶段一）和高级配置（阶段二））。

7.1.4 查看 IPSec 连接状态

【本机管理-页面向导】VPN管理>> IPSec设置>> IPSec连接状态

在当前页面可查看IPSec隧道的连接状态。

表7-5 IPSec 连接状态信息描述表

参数	说明
名称	IPSec服务器/客户端的安全策略名称
SPI	IPSec连接的安全参数索引（Security Parameter Index），用于将收到的IPsec数据包与其对应的SA进行关联。每一个IPSec连接的SPI都不相同
方向	IPSec连接的方向，in表示入方向，out表示出方向
隧道两端	IPSec连接的两端的网关地址，箭头指示当前隧道保护的数据流方向
数据流	IPSec连接的两端的子网范围，箭头指示当前隧道保护的数据流方向

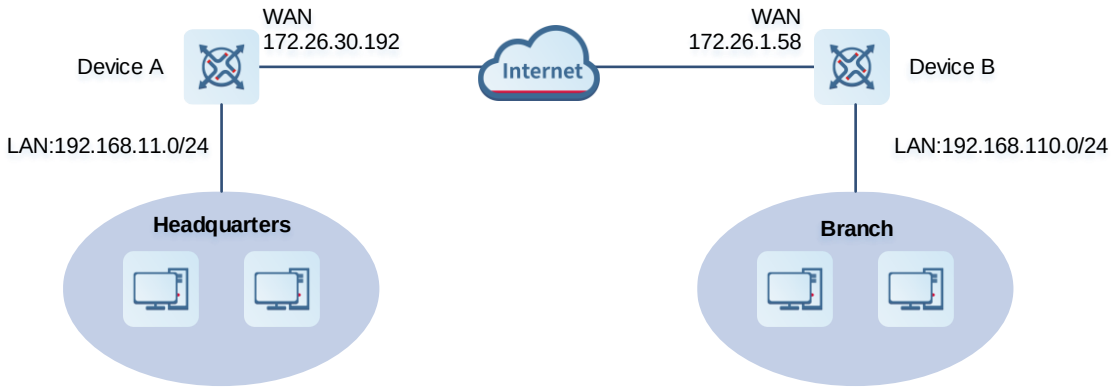
参数	说明
状态	当前IPSec隧道的连接状态
安全协议	IPSec连接使用的安全协议
算法	IPSec连接使用的加密算法和验证算法

7.1.5 典型配置案例

1. 组网需求

组织总部和分支机构之间的组网互联场景下，需要在总部网关和分支网关之间建立IPSec隧道来保证传输数据的机密性。

2. 组网图



3. 配置要点

- 在总部网关Device A上启用IPSec服务器端。
- 在分支网关Device B上启用IPSec客户端。

4. 配置步骤

(1) 配置总部网关

a 登录Web网管后，点击 VPN管理>> IPSec设置>> IPSec安全策略，进入IPSec安全策略设置界面。

b 点击<添加>，选择策略类型为“服务端”，输入策略名称、选择绑定接口并设置本地需要通过IPSec访问的网段以及预共享秘钥。

如果设备与易网络其他EG设备对接，建议阶段一和阶段二的设置保持默认即可；和其他厂商设备对接，参数保持一致即可。

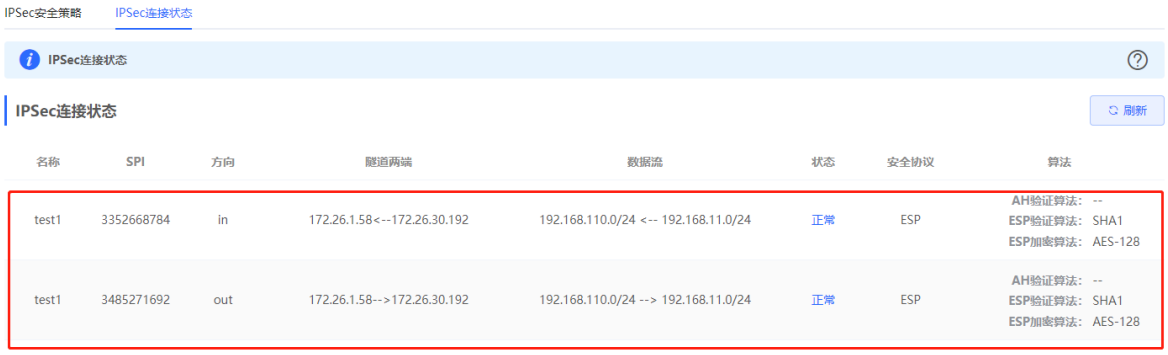
(2) 配置分支网关

a 登录Web网管后，进入IPSec安全策略设置界面。

b 点击<添加>，选择策略类型为“客户端”，输入策略名称、对端网关（写总部的外网口地址或者域名）、本地哪些网段要访问对端的哪些网段，以及与总部相同的预共享秘钥。其他的阶段一阶段二的参数与服务端保持一致即可。

5. 效果验证

(1) 登录总部/分支网关的Web页面，点击VPN管理>> IPSec设置>> IPSec连接状态，可以看到当前总部与分部的IPSec连接状态。



(2) 两端需要互访数据的终端进行互Ping测试，能够Ping通以及正常互相访问。

7.1.6 IPSec VPN 连接失败的解决方案

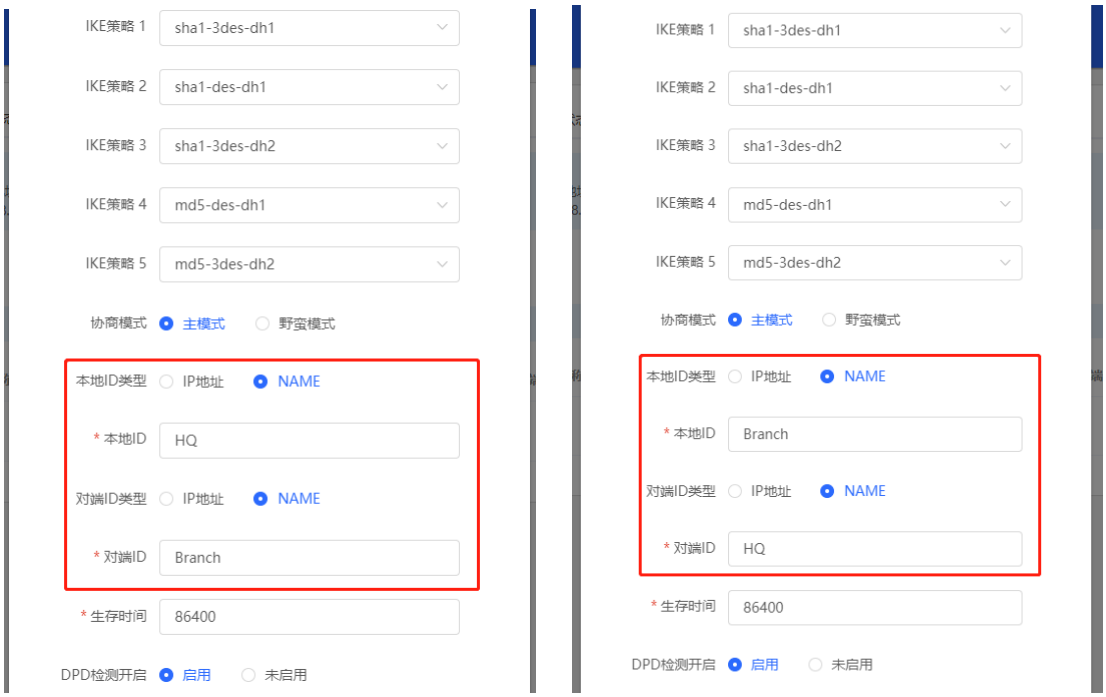
(1) 使用Ping命令检测客户端与服务器之间的连通性，详见9.9.3 。如果无法Ping通，请检查网络连接设置。
Check whether the branches' EG can ping to HQ EG. If it can't, please check the network connection between two EGs.

Click **Diagnostics->Network Tools**, then you can start the ping operation.详见9.9.3 。

(2) 确认IPSec服务端与客户端的配置是否正确。

点击 VPN管理>> IPSec设置>> IPSec安全策略，确认两端已设置匹配的安全策略。

(3) 确认服务器端设备的出口IP是否为公网IP。如果不为公网IP，需要在出口网关设备上设置DMZ或端口映射（IPSec VPN使用UDP端口500和4500），并在服务器端和客户端设置“本地ID类型”为“NAME”。
Check whether the WAN IP of your HQ EG is public IP. If it isn't, you need to configure DMZ or port mapping (IPsec VPN port are UDP 500 and 4500) on your external device and configure **Local ID Type** as **NAME** on HQ and Branches.



7.2 设置 L2TP VPN

7.2.1 功能简介

L2TP（Layer Two Tunneling Protocol，第二层隧道协议）是一种虚拟隧道协议，通常用于虚拟专用网。

L2TP协议自身不提供加密与可靠性验证的功能，但可以和安全协议搭配使用，从而实现数据的加密传输。L2TP协议常常与IPsec协议搭配使用，即先用L2TP封装报文再用IPSec封装，通过L2TP实现用户验证和地址分配，并利用IPSec保障通信的安全性。

L2TP VPN既可以用于构建企业分部与总部的安全隧道，也可以用于出差员工接入总部。当前设备支持部署L2TP服务器或客户端。

7.2.2 设置 L2TP 服务器

1. L2TP 服务端基本设置

【本机管理-页面向导】VPN管理>> L2TP>> L2TP设置

点击开关开启L2TP功能，选择L2TP类型为“服务器”，设置L2TP服务器端相关参数，点击<保存>。

表7-6 L2TP 服务端配置信息描述表

参数	说明
本地隧道地址	VPN隧道的服务器本地虚拟IP，客户端拨入之后可以通过该地址访问服务器
地址池IP范围	L2TP服务器用来给客户端分配IP地址的地址池
DNS服务器	L2TP服务器推送给客户端的DNS地址
隧道认证	设置是否启用L2TP隧道认证功能，若启用隧道认证需要设置隧道认证密钥。缺省情况下，不启用隧道认证。 隧道认证请求可由客户端侧发起。只要有一端启用了隧道认证，则只有在对端也启用了隧道认证，两端密钥完全一致且不为空的情况下，隧道才能建立；否则本端将自动断开隧道连接。若两端都关闭隧道认证，则隧道建立时无需认证密钥。 PC作为客户端拨号接入服务器端设备的场景下，建议不要启用L2TP服务器端的隧道认证功能。
IPSec加密	是否对隧道进行加密。若加密，则使用IPSec对L2TP隧道加密，为L2TP over IPSec模式。 若当前设备已启用IPSec安全策略，则不支持再对L2TP隧道开启IPSec加密；如需配置L2TP over IPSec，请先关闭IPSec安全策略 L2TP服务端与客户端的IPSec加密配置应保持一致，IPSec加密相关参数设置见设置

参数	说明
	L2TP over IPSec服务端
PPP链路维护时间间隔	L2TP VPN连通之后，发送PPP链路维护检测报文的时间间隔。建议保持默认

注意

本地隧道地址和地址池IP范围不能与设备本身的内网（LAN口）网段地址重叠。

2. 设置 L2TP over IPSec 服务端

【本机管理-页面向导】VPN管理>> L2TP>> L2TP设置

在完成L2TP服务端基本设置的基础上，在L2TP服务器端开启IPSec加密，保障通信的安全性。IPSec的相关介绍请参考7.1 设置IPSec VPN。

表7-7 L2TP over IPSec 服务端配置信息描述表

参数	说明
预共享密钥	必须指定相同且唯一的预共享密钥作为服务器和客户端之间相互认证的凭证

参数	说明
IKE策略	选择IKE协议使用的参数加密算法、散列算法和Diffie-Hellman组标识。参与IKE协商的双方至少拥有一套一致的IKE策略，这是IKE协商成功的必要条件。服务器和客户端的IKE策略必须一致 ● 散列（HASH）算法： ○ sha1：SHA-1算法 ○ md5：MD5算法 ● 加密算法： ○ des：密钥长度为56比特的DES算法 ○ 3des：密钥长度为168比特的3DES算法 ○ aes-128：密钥长度为128比特的AES算法 ○ aes-192：密钥长度为192比特的AES算法 ○ aes-256：密钥长度为256比特的AES算法 ● Diffie-Hellman组标识： ○ dh1：768比特Diffie-Hellman组 ○ dh2：1024比特Diffie-Hellman组 ○ dh5：1536比特Diffie-Hellman组
转换集	特定安全协议和算法的组合。在IPSec安全联盟协商期间，两端使用同一个特定的变换集合来保护特定的数据流。服务器和客户端的转换集配置要保持一致 ● 安全协议：ESP（Encapsulating Security Payload，报文安全封装）协议为IPSec连接提供了数据源认证、数据完整性校验和防报文重放功能，并保证了数据的机密性 ● 验证算法： ○ sha1：SHA-1 HMAC验证算法 ○ md5：MD5 HMAC验证算法 ● 加密算法： ○ des：密钥长度为56比特的DES算法 ○ 3des：密钥长度为168比特的3DES算法 ○ aes-128：密钥长度为128比特的AES算法 ○ aes-192：密钥长度为192比特的AES算法 ○ aes-256：密钥长度为256比特的AES算法
协商模式	协商模式 分为主模式和野蛮模式。服务器端和客户端的协商模式必须一致。 ● 主模式：适用于两设备的公网IP固定、设备之间点对点通信的环境。主模式会对对端身份进行保护，安全性较高。 ● 野蛮模式：对于例如ADSL拨号用户，其获得的公网IP不是固定的，且可能存在NAT设备的情况下，则需要采用野蛮模式做NAT穿越；同时，由于IP不是固定的，还需要额外设置身份（ID）类型为“NAME”。野蛮模式不保护对端身份，安全性较低。

参数	说明
本地ID类型	用于身份认证的ID类型。客户端的“对端ID”必须与服务端的“本地ID”保持一致。 ● IP地址：以IP地址作为身份ID，自动生成本端身份ID ● NAME：以主机字符串作为身份ID，自动生成本端身份ID。ID类型为“NAME”时，需要同时设置作为身份ID的主机字符串。 当服务器WAN口IP为私网地址时，需要设置本地ID类型为“NAME”并在外部设备上设置DMZ； 当IP地址不固定时，需设置本地ID类型为“NAME”，并在对端做相应兼容修改。
本地ID	本地ID类型为“NAME”时，作为身份ID的主机字符串。客户端的“对端ID”必须与服务端的“本地ID”保持一致。

3. 设置 L2TP 用户

【本机管理-页面向导】VPN管理>> 账号管理

L2TP服务器只允许VPN用户管理列表中已添加的用户账号拨入，因此需手动配置用于客户端接入的用户账号。

点击<添加>，选择服务类型为L2TP或ALL（ALL表示该账号可用于所有类型的VPN隧道建立），输入设置的用户名和密码以及对端子网范围，选择组网模式，点击<确定>。

表7-8 L2TP 用户配置信息描述表

参数	说明
用户名/密码	允许拨入的L2TP用户的名称和密码，用于客户端与服务器建立连接
组网模式	• 电脑拨入路由器：拨入的客户端是个人用户，往往由单个计算机拨入实现远端计算机与本地局域网的通信。 • 路由器对路由器：拨入的客户端是一个网段的用户，往往通过一个路由器拨入，实现隧道两端局域网的通信。
对端子网范围	L2TP隧道对端局域网使用的IP地址范围，一般填写客户端设备LAN口的IP地址网段。（服务器端和客户端的内网网段不能重叠） 例如：分支向总部拨号接入的场景下，填写分支（路由器）的内网网段
状态	是否启用该用户账号

7.2.3 设置 L2TP 客户端

1. L2TP 客户端基本设置

【本机管理-页面向导】VPN管理>> L2TP>> L2TP设置

点击开关开启L2TP功能，选择L2TP类型为“客户端”，设置L2TP客户端相关参数，点击<保存>。

表7-9 L2TP 客户端配置信息描述表

参数	说明
用户名/密码	L2TP隧道用户身份认证的用户名和密码，需与服务器端设置的L2TP用户的用户名和密码一致
绑定接口	客户端使用的WAN口
本地隧道IP	VPN隧道的客户端虚拟IP地址，选择“动态”表示从服务器地址池中获取IP地址，选择“静态”表示手动配置一个在服务器地址池范围内且不产生冲突的静态地址作为本端隧道IP地址
服务器地址	填写服务器的WAN口IP地址或者域名，服务端的出口IP必须是公网IP
对端子网	填写准备访问的服务器的内网网段，不能与客户端的内网网段重叠
隧道认证	设置是否启用L2TP隧道认证功能，若启用隧道认证则需要输入与服务端相同的隧道认证

参数	说明
	密钥。缺省情况下，不启用隧道认证，为了保证隧道安全，建议启用。
IPSec加密	是否对隧道进行加密。若启用，则使用IPSec对L2TP隧道加密，为L2TP over IPSec模式。客户端的IPSec加密配置应与服务器保持一致，详见设置L2TP over IPSec客户端。
工作模式	● NAT：对经过此L2TP隧道的数据包进行NAT转换（数据包的源IP替换为L2TP隧道的本地虚拟IP）。NAT模式下服务器无法访问客户端内网 ● 路由：对经过此L2TP隧道的数据包只进行路由转发。路由模式下，服务器能够访问客户端内网
PPP链路维护时间间隔	L2TP VPN连通之后，发送PPP链路维护检测报文的时间间隔。建议保持默认

2. 设置 L2TP over IPSec 客户端

【本机管理-页面向导】VPN管理>> L2TP>> L2TP设置

在完成L2TP客户端基本设置的基础上，在L2TP客户端开启IPSec加密，保障通信的安全性。客户端的IPSec加密配置应与服务器保持一致，请参考设置L2TP over IPSec服务端进行配置。

7.2.4 查看 L2TP 隧道信息

【本机管理-页面向导】VPN管理>> L2TP>> 隧道信息列表

服务器和客户端建立VPN连接需要些时间，完成服务器和客户端的设置之后，等待1~2分钟可以刷新页面查看L2TP隧道的建立状态。

表7-10 L2TP 隧道信息描述表

参数	说明
用户名	客户端用于身份认证的用户名
服务器/客户端	当前设备是属于客户端还是服务器
隧道名称	L2TP生成的虚拟网卡名称
虚拟本地IP	隧道的本端虚拟IP地址，L2TP客户端的虚拟IP地址由L2TP服务器分配
接入服务IP	隧道对端接入L2TP的实际IP地址
对端虚拟IP	隧道的对端虚拟IP地址，L2TP客户端的虚拟IP地址由L2TP服务器分配
DNS	L2TP服务器分配的DNS地址

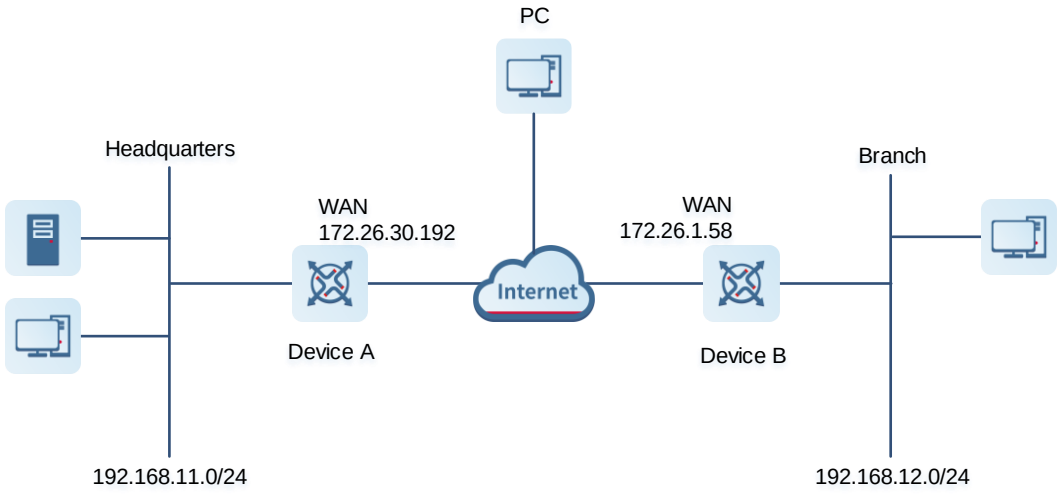
7.2.5 典型配置案例

1. 组网需求

创建L2TP隧道来实现出差员工和分部公司员工可以访问搭建在总部内网的服务器：

- 出差员工客户端（PC）能够通过L2TP VPN访问公司的服务器；
- 公司分部需要频繁访问总部的服务器资料，因此希望能由分部路由器（Device B）作为客户端进行拨号，实现分部员工访问总部资料时无需设置拨号，像访问分部内部服务器一样透明。

2. 组网图



3. 配置要点

- 配置总部网关Device A启用L2TP服务器端。
- 配置分部网关Device B启用L2TP客户端。
- 在出差员工PC上设置L2TP客户端。

4. 配置步骤

(1) 配置总部网关

> 说明
> 总部和分部的内网地址不能冲突，否则会出现无法访问资源的情况。

a 登录Web网管后，点击 VPN管理>> L2TP>>L2TP设置，进入L2TP设置界面。

b 点击开关开启L2TP，选择L2TP类型为服务器，输入本地隧道地址、地址池IP范围、DNS服务器地址并选择是否开启IPSec加密和隧道认证，点击<保存>完成参数配置。

表7-11 L2TP 服务端配置信息描述表

参数	说明
本地隧道地址	填写一个非内网网段的IP地址，PC拨入之后可以通过该地址访问服务器
地址池IP范围	填写非内网网段的IP地址范围，用于给客户端分配IP地址
DNS服务器	填写一个可用的DNS服务器地址
隧道认证	默认关闭隧道认证功能，开启后，客户端和服务器隧道密钥要一致才能对接。可保持关闭
IPSec加密	设置是否通过IPSec协议对L2TP隧道加密，建议选择加密以保证数据安全性 若当前设备已启用IPSec安全策略，则不支持再对L2TP隧道开启IPSec加密；如需配置L2TP over IPSec，请先关闭IPSec安全策略
预共享密钥	填写用于IPSec认证的密钥，客户端需设置相同的预共享密钥才能成功接入

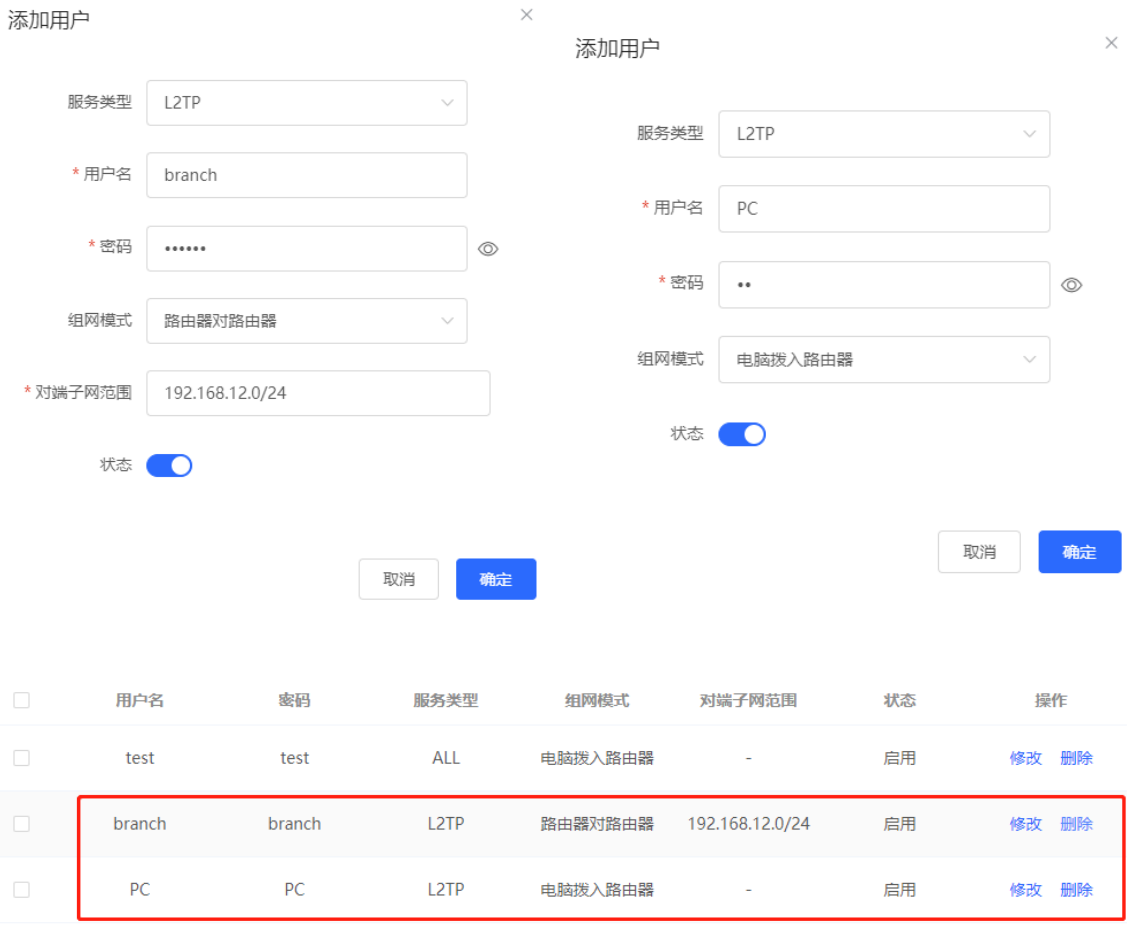
参数	说明
IKE策略、转换集、协商模式、本地ID类型	无特殊需求保持默认即可
PPP链路维护时间间隔	无特殊需求保持默认即可

c 点击 VPN管理>> 账号管理，分别添加供出差员工和分部访问总部的L2TP用户账号。

出差员工用户账号：组网模式选择“电脑拨入路由器”。

分部员工用户账号：组网模式选择“路由器对路由器”，对端子网范围设置为分支网关的内网网段，即192.168.12.0/24。

> 注意
> 服务器端和客户端的内网网段不能重叠。



用户名	密码	服务类型	组网模式	对端子网范围	状态	操作
test	test	ALL	电脑拨入路由器	-	启用	修改 删除
branch	branch	L2TP	路由器对路由器	192.168.12.0/24	启用	修改 删除
PC	PC	L2TP	电脑拨入路由器	-	启用	修改 删除

(2) 配置分支网关

a 登录Web网管后，进入L2TP设置界面。

b 点击开关开启L2TP，选择L2TP类型为客户端，输入服务端设置的用户名和密码、服务器地址、对端内网网段并设置和服务器相同的IPSec加密参数，点击<保存>完成参数配置。

表7-12 L2TP 客户端配置信息描述表

参数	说明
用户名和密码	填写服务器所设置的用户名和密码
绑定接口	客户端与服务器建立隧道的WAN口
本地隧道IP	选择动态方式获取即可。也可选择静态方式，输入一个服务器地址池范围内的IP地址
服务器地址	填写服务器的外网口（WAN口）地址，即172.26.30.192
对端子网	填写服务器端的内网网段（LAN口的IP地址范围），即192.168.11.0/24
隧道认证	与服务器端配置保持一致，本例中为关闭
IPSec加密	与服务器端配置保持一致，本例中为开启
预共享密钥	填写服务器端设置的预共享密钥，与服务器端配置保持一致
IKE策略、转换集、协商模式、对端ID类型	与服务器端配置保持一致，“对端ID类型”应与服务器的“本地ID类型”相同
工作模式	如果总部需要访问分公司的内网，应设置为“路由”
PPP链路维护时间间隔	L2TP VPN连通之后，发送PPP链路维护检测报文的时间间隔。保持默认即可

(3) 设置出差员工PC

说明

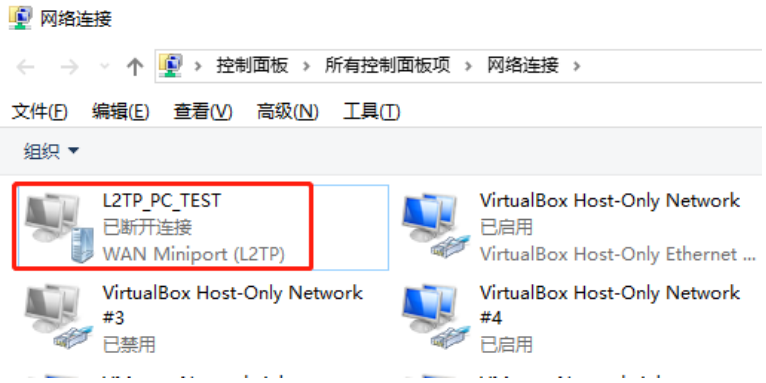
- 在出差员工PC上配置L2TP客户端，下文以装有Window 10系统的PC为例。

- Windows XP（简称XP）系统和Windows 7/Windows 10（简称Win7/10）系统对L2TP VPN的功能支持情况不同：XP系统如果要使用L2TP VPN，需要修改服务注册表项；Win7/10系统默认支持L2TP，不需要修改注册表项。
- Win7/Win10系统和XP系统不支持L2TP隧道认证功能，因此服务器端要关闭隧道认证。
- 苹果手机不支持无IPSec加密的L2TP拨入，只支持L2TP over IPSec。

a 点击[设置]>>[网络和Internet]>>[VPN]，进入VPN设置页面。

b 点击“添加VPN连接”，选择VPN提供商为Windows，填写连接名称和服务器的地址或者域名，点击保存即可。

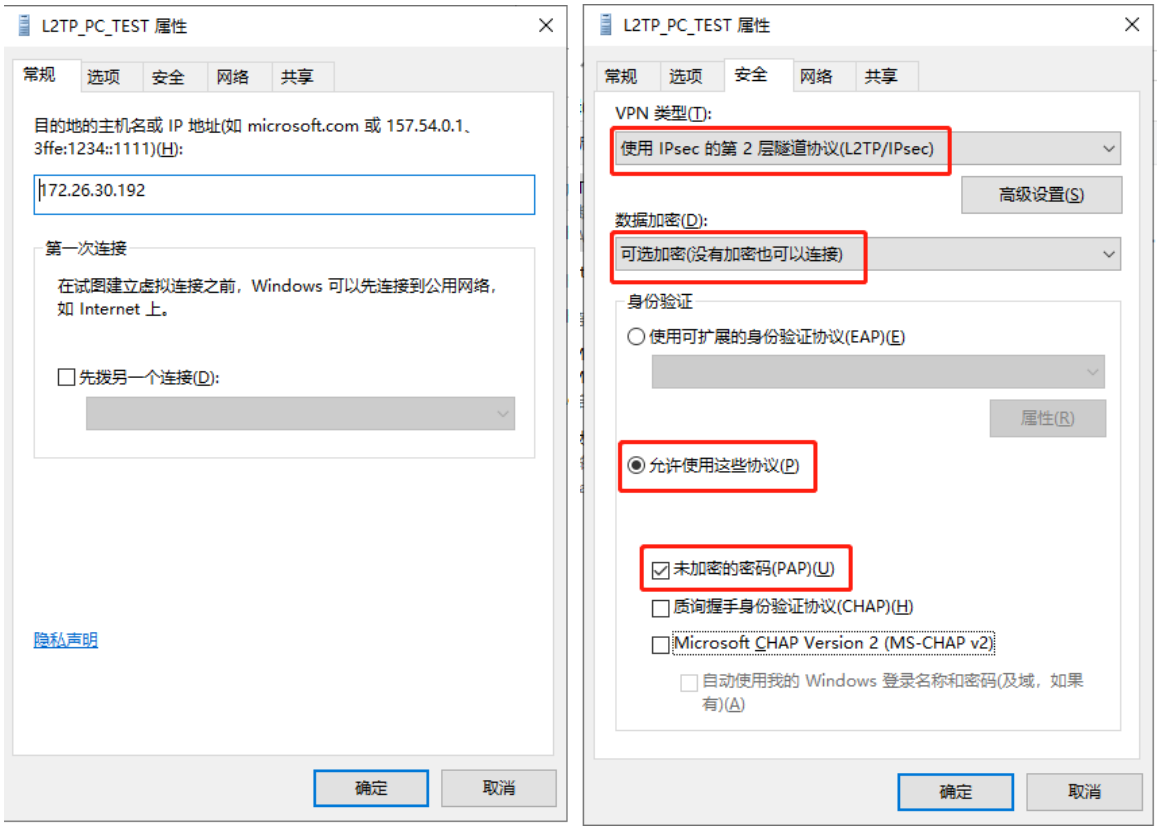
c 查看网络连接，右键点击创建的VPN连接“L2TP_PC_TEST”，查看属性。



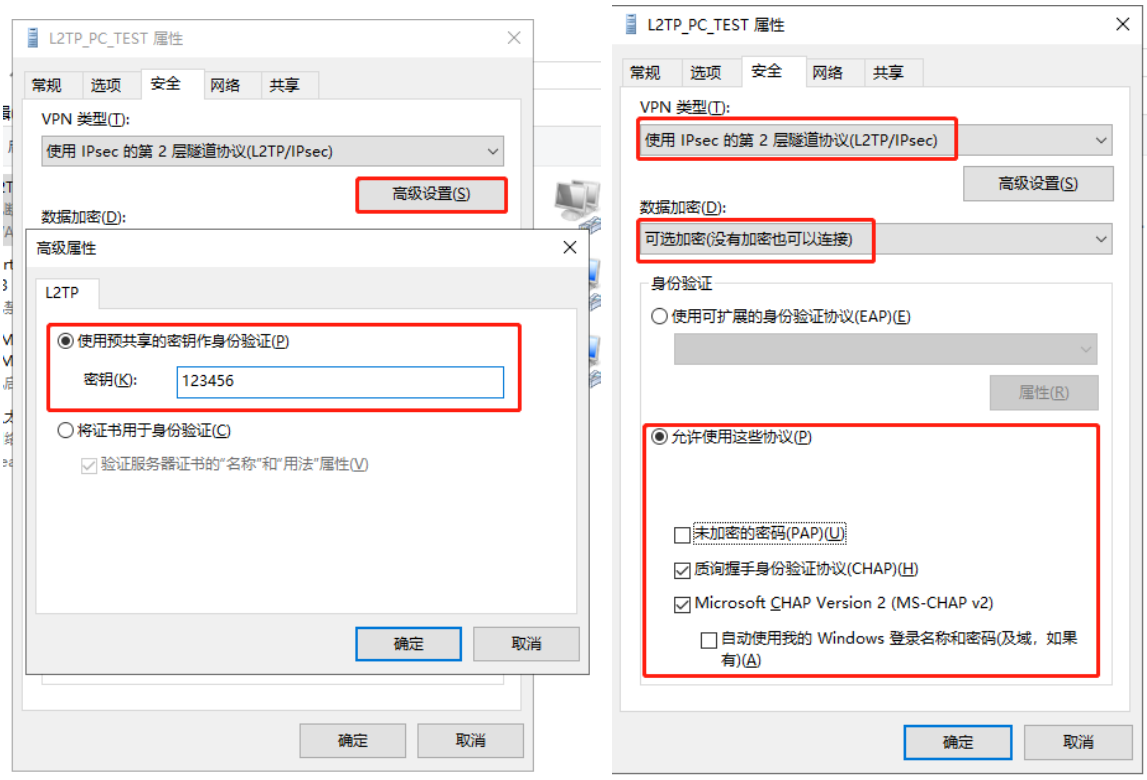
d 在弹出的属性对话框中，选择“安全”页签，在“VPN类型(T)”中选择“使用IPsec的第2层隧道协议(L2TP/IPsec)”，在“数据加密(D)”中选择“可选加密（没有加密也可以连接）”。

若L2TP服务器未启用IPSec加密，勾选“未加密的密码(PAP)”，点击<确定>。跳过步骤e。

若L2TP服务器启用了IPSec加密，按照步骤e 进行配置。



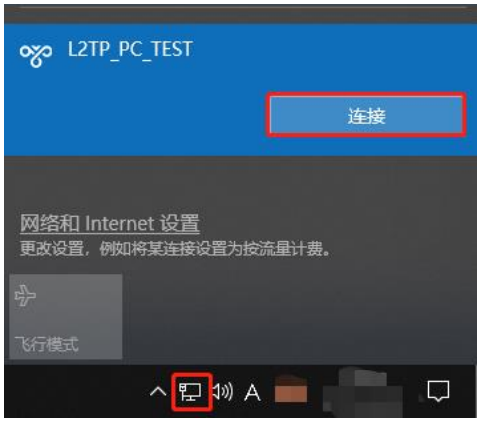
e 服务端启用了IPSec加密，需按照下图勾选CHAP和MS-CHAP v2作为身份验证的协议，并在“高级设置”中设置与服务端相同的预共享密钥。完成配置后，点击<确定>。



说明

设备不支持EAP身份验证协议，Windows系统客户端不能勾选EAP协议相关身份验证选项，否则将导致VPN连接失败。

f 上述步骤已完成PC的L2TP客户端设置，接下来可以在PC上发起VPN连接。点击任务栏的网络图标  ，选择L2TP VPN连接，点击<连接>。在弹框中输入服务端设置的用户名和密码，进行连接。



5. 效果验证

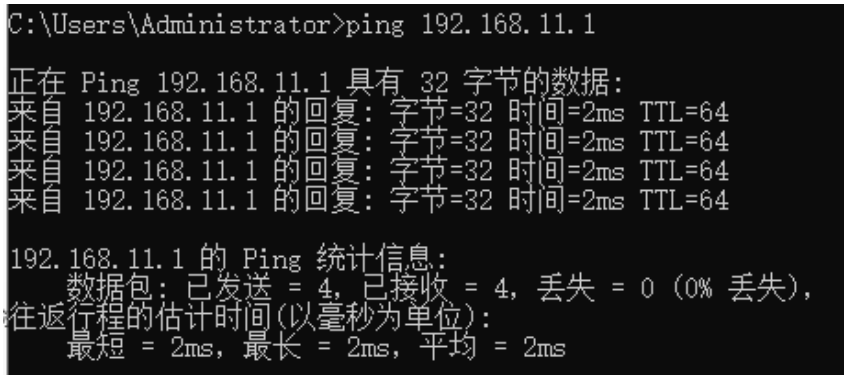
(1) 完成服务器和客户端的设置之后，等待1分钟左右可以在总部服务器端和分支客户端查看到L2TP隧道的连接信息，表示连接成功。

总部：

分支：

s

(2) 在总部或者分支Ping对端的内网地址，能正常通信。出差员工PC和分部员工PC都可以访问总部服务器。



7.2.6 L2TP VPN 连接失败的解决方案

(1) 使用Ping命令检测客户端与服务器之间的连通性，详见9.9.3 。如果无法Ping通，请检查网络连接设置。Check whether the branches' EG can ping to HQ EG. If it can't, please check the network connection between two EGs.

Click **Diagnostics->Network Tools**, then you can start the ping operation.详见9.9.3 。

(2) 检查客户端使用的用户名和密码是否与服务端所设置的账户匹配。Check whether the username and password on HQ VPN client settings are right or not.

(3) 确认服务器端设备的出口IP是否为公网IP。如果不为公网IP，需要在出口网关设备上设置DMZ。Check whether the WAN IP of your HQ EG is the public IP. If it isn't, you need to configure DMZ on your external device.

7.3 设置 PPTP VPN

7.3.1 功能简介

PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）是一种在PPP（Point-to-Point Protocol，点对点协议）的基础上开发的增强型安全协议，它允许企业通过私人“隧道”在公共网络上扩展自己的企业网络。PPTP

依靠PPP协议来实现加密和身份验证等安全性功能，通常可搭配PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，挑战握手认证协议）、MS-CHAPv1/v2（Microsoft Challenge Handshake Authentication Protocol，微软挑战握手认证协议）或EAP-TLS（Extensible Authentication Protocol-Transport Layer Security，可扩展认证协议-传输层安全协议）来进行身份验证；还可以MPPE（Microsoft Point-to-Point Encryption，微软点对点加密）实现连接时的加密，提高安全性。

当前设备支持部署PPTP服务器或客户端，支持设置MPPE加密配合MSCHAP-v2进行身份验证，暂不支持EAP认证。

7.3.2 设置 PPTP 服务器

1. 设置 PPTP 服务端

【本机管理-页面向导】VPN管理>> PPTP>> PPTP设置

点击开关开启PPTP功能，选择PPTP类型为“服务器”，设置PPTP服务器端相关参数，点击<保存>。

表7-13 PPTP 服务端配置信息描述表

参数	说明
本地隧道地址	VPN隧道的服务器本地虚拟IP，客户端拨入之后可以通过该地址访问服务器
地址池IP范围	PPTP服务器用来给客户端分配IP地址的地址池
DNS服务器	PPTP服务器推送给客户端的DNS地址
MPPE加密	是否使用MPPE对PPTP隧道加密。

参数	说明
	服务器启用加密后，如果客户端的数据加密类型配置为“可选加密”，则服务器和客户端可以正常连接，且不对报文信息加密；如果客户端配置为“启用加密”，则服务器和客户端可以正常连接，且报文信息是加密。如果客户端配置为“不加密”，则无法正常连接。 若服务器不启用加密，而客户端要求加密，也将连接失败。 默认情况下，服务器未启用加密。启用MPPE加密后，带宽性能会下降，若无特殊安全需求，建议保持关闭
PPP链路维护时间间隔	PPTP VPN连通之后，发送PPP链路维护检测报文的时间间隔

注意

本地隧道地址和地址池IP范围不能与设备本身的内网（LAN口）网段地址重叠。

2. 设置 PPTP 用户

【本机管理-页面向导】VPN管理>> 账号管理

PPTP服务器只允许VPN用户管理列表中已添加的用户账号拨入，因此需手动配置用于客户端接入的用户账号。

点击<添加>，选择服务类型为PPTP或ALL（ALL表示该账号可用于所有类型的VPN隧道建立），输入设置的用户名和密码以及对端子网范围，选择组网模式，点击<确定>。

表7-14 PPTP 用户配置信息描述表

参数	说明
用户名/密码	允许拨入的PPTP用户的名称和密码，用于客户端与服务器建立连接
组网模式	• 电脑拨入路由器：拨入的客户端是个人用户，往往由单个计算机拨入实现远端计算机与本地局域网的通信。 • 路由器对路由器：拨入的客户端是一个网段的用户，往往通过一个路由器拨入，实现隧道两端局域网的通信。
对端子网范围	PPTP隧道对端局域网使用的IP地址范围，一般填写客户端设备LAN口的IP地址网段。（服务器端和客户端的内网网段不能重叠） 例如：分支向总部拨号接入的场景下，填写分支（路由器）的内网网段
状态	是否启用该用户账号

7.3.3 设置 PPTP 客户端

【本机管理-页面向导】VPN管理>> PPTP>> PPTP设置

点击开关开启PPTP功能，选择PPTP类型为“客户端”，设置PPTP客户端相关参数，点击<保存>。

表7-15 PPTP 客户端配置信息描述表

参数	说明
用户名/密码	PPTP隧道用户身份认证的用户名和密码，需与服务器端设置的PPTP用户的用户名和密码一致
绑定接口	客户端使用的WAN口
本地隧道IP	VPN隧道的客户端虚拟IP地址，选择“动态”表示从服务器地址池中获取IP地址，选择“静态”表示手动配置一个在服务器地址池范围内且不产生冲突的静态地址作为本端隧道IP地址
服务器地址	填写服务器的WAN口IP地址或者域名，服务端的出口IP必须是公网IP
对端子网	填写准备访问的服务器的内网网段，不能与客户端的内网网段重叠
MPPE加密	是否使用MPPE对PPTP隧道加密。需与服务器端的配置保持一致

参数	说明
工作模式	NAT：仅允许客户端访问服务器网络，不允许服务器访问客户端网络 路由：允许服务器访问客户端网络
PPP链路维护时间间隔	PPTP隧道连通之后，发送PPP链路维护检测报文的时间间隔。建议保持默认

7.3.4 查看 PPTP 隧道信息

【本机管理-页面向导】VPN管理>> PPTP>> 隧道信息列表

服务器和客户端建立VPN连接需要些时间，完成服务器和客户端的设置之后，等待1~2分钟可以刷新页面查看PPTP隧道的建立状态。

表7-16 PPTP 隧道信息描述表

参数	说明
用户名	客户端用于身份认证的用户名
服务器/客户端	当前设备是属于客户端还是服务器
隧道名称	PPTP生成的虚拟网卡名称
虚拟本地IP	隧道的本端虚拟IP地址，客户端的虚拟IP地址由服务器分配
接入服务IP	隧道对端接入PPTP的实际IP地址
对端虚拟IP	隧道的对端虚拟IP地址，客户端的虚拟IP地址由服务器分配
DNS	PPTP服务器分配的DNS地址

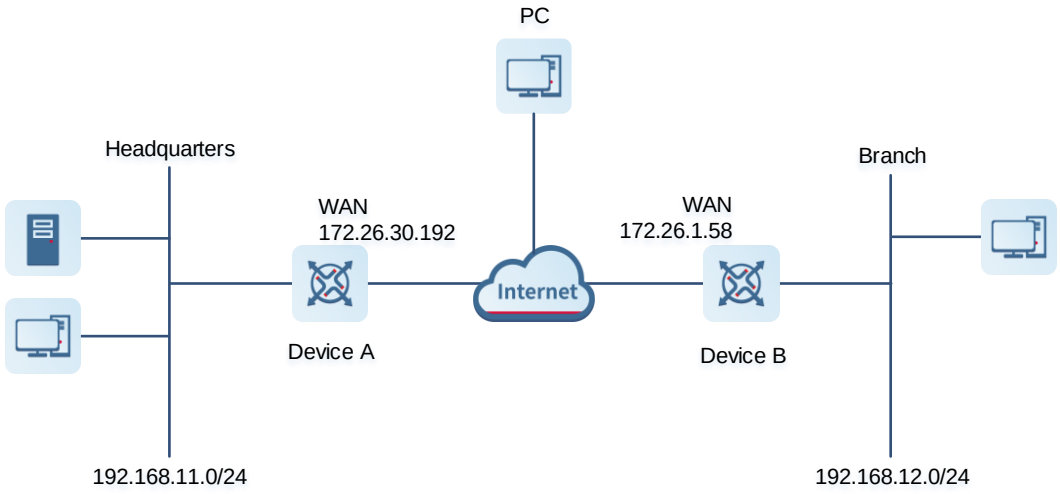
7.3.5 典型配置案例

1. 组网需求

创建PPTP隧道来实现出差员工和分部公司员工可以访问搭建在总部内网的服务器：

- 出差员工客户端（PC）能够通过PPTP拨号访问公司的服务器；
- 公司分部需要频繁访问总部的服务器资料，因此希望能由分部路由器（Device B）作为客户端进行拨号，实现分部员工访问总部资料时无需设置拨号，像访问分部内部服务器一样透明。

2. 组网图



3. 配置要点

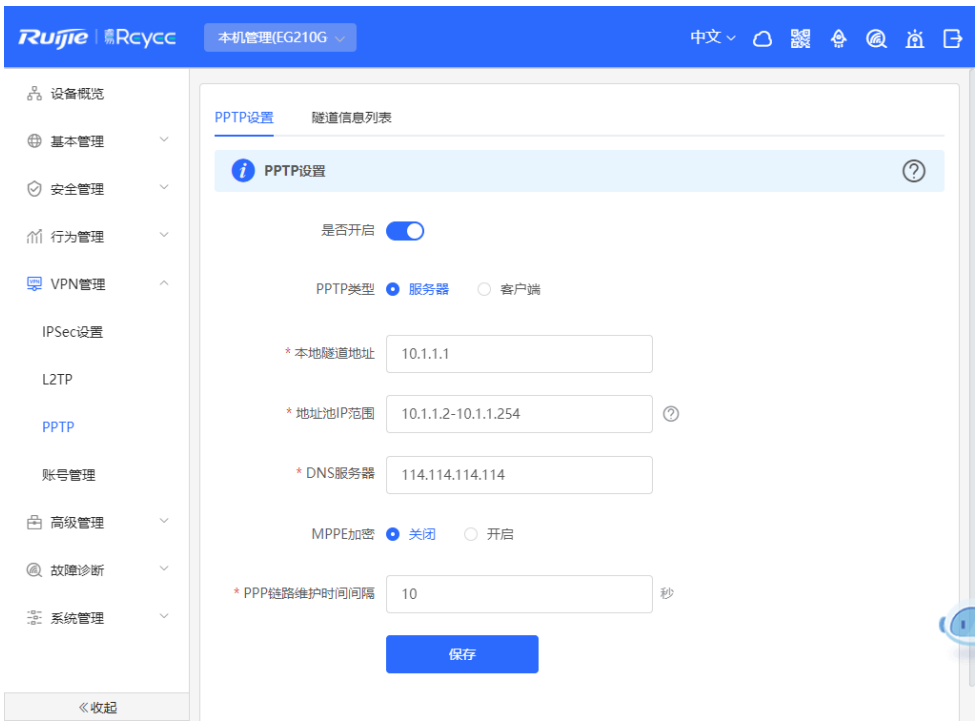
- 配置总部网关Device A启用PPTP服务器端。
- 配置分部网关Device B启用PPTP客户端。
- 在出差员工PC上设置PPTP客户端。

4. 配置步骤

(1) 配置总部网关

> 说明
> 总部和分部的内网地址不能冲突，否则会出现无法访问资源的情况。

a 登录Web网管后，点击 VPN管理>> PPTP>>PPTP设置，进入PPTP设置界面。



b 点击开关开启PPTP，选择PPTP类型为服务器，输入本地隧道地址、地址池IP范围、DNS服务器地址并选择是否开启MPPE加密，点击<保存>完成参数配置。

表7-17 PPTP 服务端配置信息描述表

参数	说明
本地隧道地址	填写一个非内网网段的IP地址，PC拨入之后可以通过该地址访问服务器
地址池IP范围	填写非内网网段的IP地址范围，用于给客户端分配IP地址
DNS服务器	填写一个可用的DNS服务器地址
MPPE加密	是否使用MPPE为PPTP隧道加密，需与客户端配置一致 启用MPPE加密后，安全性提升但带宽性能会下降，若无特殊安全需求，可保持关闭
PPP链路维护时间间隔	无特殊需求保持默认即可

c 点击 VPN管理>> 账号管理，分别添加供出差员工和分部访问总部的PPTP用户账号。

出差员工用户账号：组网模式选择“电脑拨入路由器”

分部员工用户账号：组网模式选择“路由器对路由器”，对端子网范围设置为分支网关的内网网段

> 注意
> 服务器端和客户端的内网网段不能重叠。

(2) 配置分支网关

a 登录Web网管后，进入PPTP设置界面。

b 点击开关开启PPTP，选择PPTP类型为客户端，输入服务端设置的用户名和密码、服务器地址、对端内网网段并设置和服务器相同的IPSec加密参数，点击<保存>完成参数配置。

表7-18 PPTP 客户端配置信息描述表

参数	说明
用户名和密码	填写服务器所设置的用户名和密码
绑定接口	客户端与服务器建立隧道的WAN口
本地隧道IP	选择动态方式获取即可。也可选择静态方式，输入一个服务器地址池范围内的IP地址
服务器地址	填写服务器的外网口（WAN口）地址
对端子网	填写服务器端的内网网段（LAN口的IP地址范围）
MPPE加密	与服务器端配置保持一致
工作模式	如果总部需要访问分公司的内网，应设置为“路由”
PPP链路维护时间间隔	PPTP VPN连通之后，发送PPP链路维护检测报文的时间间隔。保持默认即可

(3) 设置出差员工PC

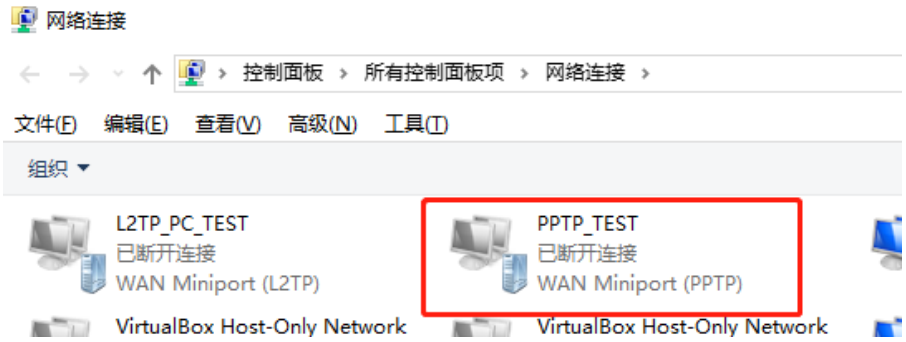
说明

- 在出差员工PC上配置PPTP客户端，下文以装有Window 10系统的PC为例。
- PC防火墙要开放端口号1723（PPTP）和47（GRE）。

a 点击[设置]>>[网络和Internet]>>[VPN]，进入VPN设置页面。

b 点击“添加VPN连接”，选择VPN提供商为Windows，VPN类型为“点对点隧道协议(PPTP)”填写连接名称和服务器的地址或者域名，点击保存即可。

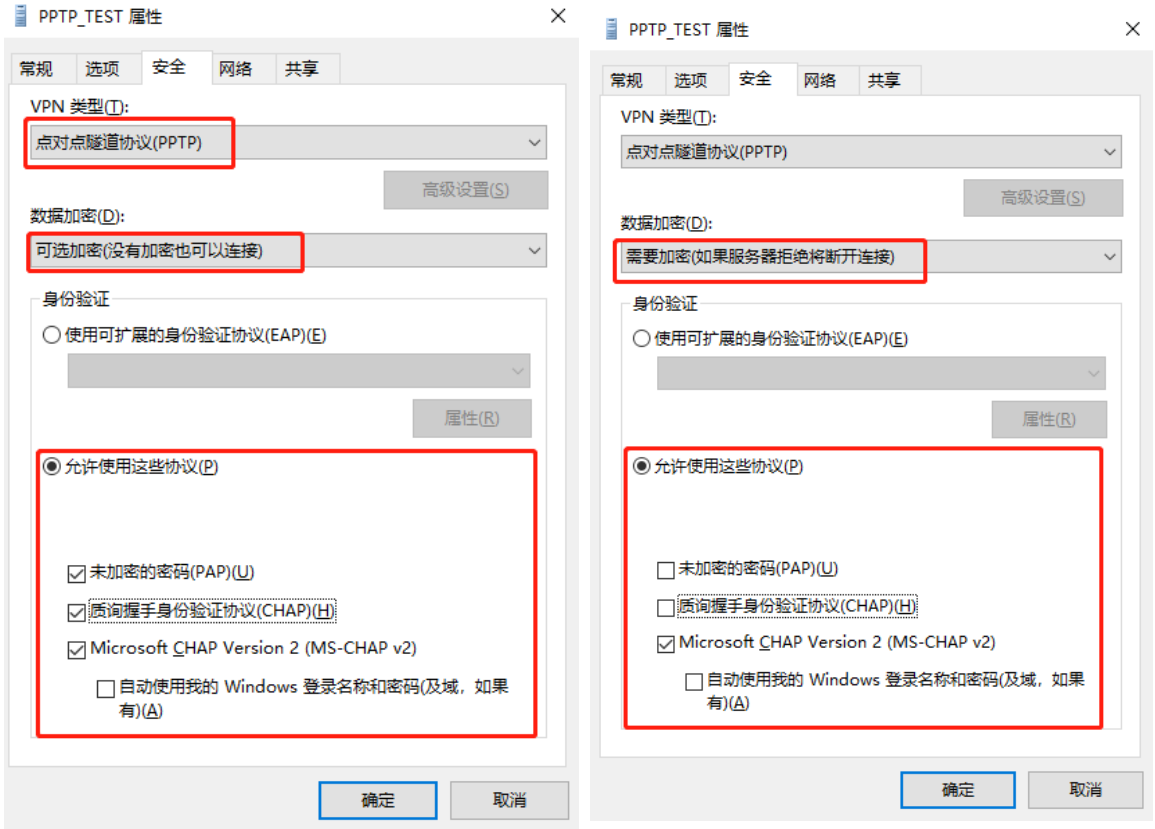
c 查看网络连接，右键点击创建的VPN连接“PPTP_TEST”，查看属性。



d 在弹出的属性对话框中，选择“安全”页签。

如果PPTP服务器未启用MPPE加密，“数据加密”可以选择“可选加密”或者“不允许加密”，同时可以使用PAP、CHAP、MS-CHAP v2进行身份验证，如下左图。

如果PPTP服务器启用了MPPE加密，“数据加密”可以选择“需要加密”或者“最大强度的加密”，同时身份验证只能使用MS-CHAP v2协议，如下右图。



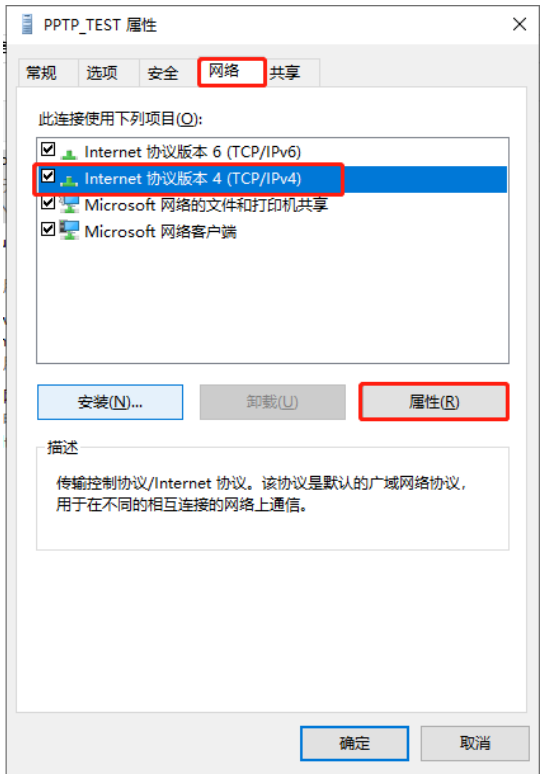
说明

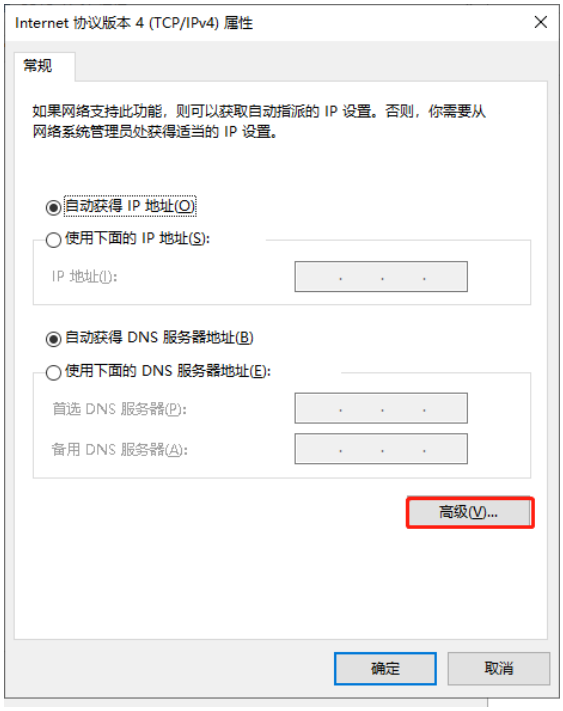
设备不支持EAP身份验证协议，Windows系统客户端不能勾选EAP协议相关身份验证选项，否则将导致VPN连接失败。

e PC作为客户端拨入时，还需要从以下两种操作中选择一种进行设置：

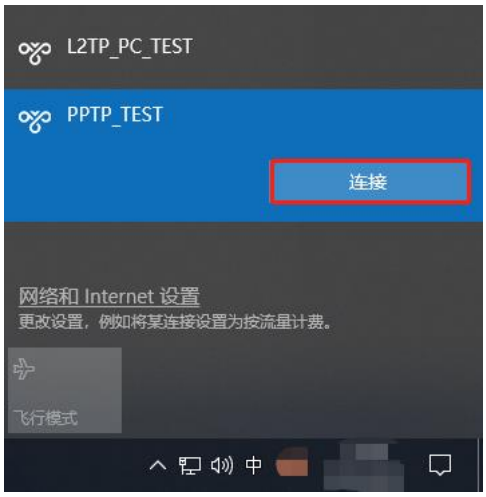
1） 在客户端PC上以管理员身份添加去往VPN对端网段的路由。

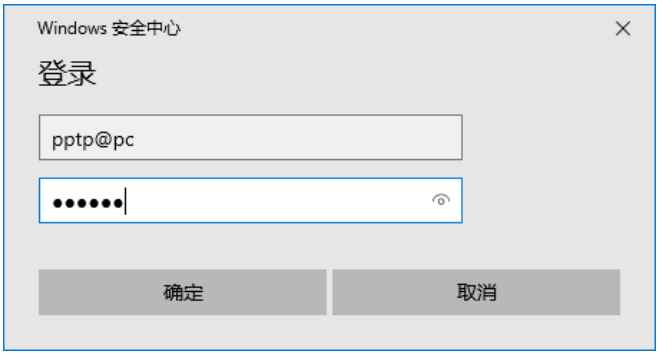
2） 在本地新建的VPN连接属性里勾选“在远程网络上使用默认网关”，当VPN连接成功后，客户端PC任何向外访问的数据流都会走VPN隧道。具体配置步骤如下图所示：





f 上述步骤已完成PC的PPTP客户端设置，接下来可以在PC上发起VPN连接。点击任务栏的网络图标  ，选择PPTP VPN连接，点击<连接>。在弹框中输入服务端设置的用户名和密码，进行连接。





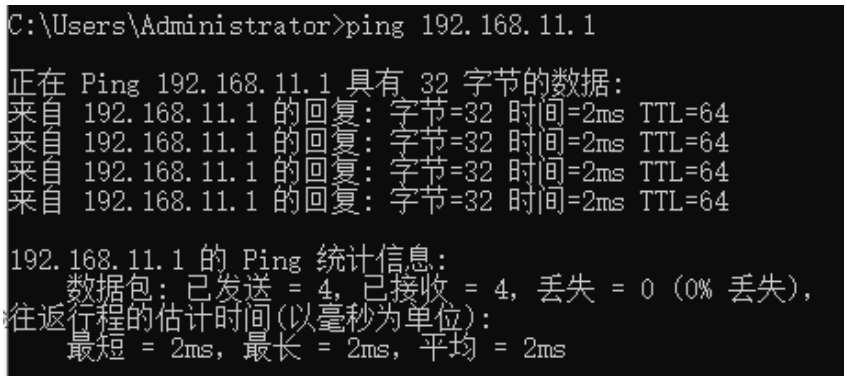
5. 效果验证

(1) 完成服务器和客户端的设置之后，等待1分钟左右可以在总部服务器端和分支客户端查看到PPTP隧道的连接信息，表示连接成功。

总部：

分支：

(2) 在总部或者分支Ping对端的内网地址，能正常通信。出差员工PC和分部员工PC都可以访问总部服务器。



7.3.6 PPTP VPN 连接失败的解决方案

(1) IPhone和其他IOS设备不支持PPTP，请使用L2TP VPN代替。IPhone and other IOS devices don't support PPTP. Please change to use L2TP instead.

(2) 使用Ping命令检测客户端与服务器之间的连通性，详见9.9.3 。如果无法Ping通，请检查网络连接设置。Check whether the branches' EG can ping to HQ EG. If it can't, please check the network connection between two EGs.

Click **Diagnostics->Network Tools**, then you can start the ping operation.详见9.9.3 。

(3) 检查客户端使用的用户名和密码是否与服务端所设置的账户匹配。Check whether the username and password on HQ VPN client settings are right or not.

(4) 确认服务器端设备的出口IP是否为公网IP。如果不为公网IP，需要在出口网关设备上设置DMZ。Check whether the WAN IP of your HQ EG is the public IP. If it isn't, you need to configure DMZ on your external device.

7.4 OpenVPN

⚠ 注意

- RG-EG105G不支持本功能。
- 仅在非中文环境支持，中文环境下如需设置请先切换系统语言，见9.11 。

7.4.1 功能简介

1. OpenVPN 概述

企业之间或个人和公司间由于安全性或跨NAT等原因，需要虚拟专用通道建立连接。OpenVPN是一种通过虚拟网卡实现二三层隧道的VPN。OpenVPN支持灵活的客户端授权方式，支持证书、用户名和密码，允许用户可以通过防火墙连接到VPN的虚拟接口，比其他VPN类型简单易用。OpenVPN能在Linux、xBSD、Mac OS X与Windows2000/XP上运行，本设备支持与PC、安卓/苹果系统手机、路由器和linux等设备建立VPN连接，能兼容市面上大多数oOpenVPN产品设备。

OpenVPN连接能通过大多数的代理服务器，并且能够在NAT的环境中很好地工作。服务端能够向客户端“推送”某些网络配置信息的功能，这些信息包括：IP地址、路由设置、DNS配置等。

2. 证书介绍

OpenVPN主要优势点在于自身的安全性，而OpenVPN安全性离不开证书的支持.

客户端证书有ca.crt、ca.key、client.crt、client.key，服务器端证书有ca.crt、ca.key、server.crt、server.key。

7.4.2 设置 OpenVPN 服务端

【本机管理-页面向导】VPN>> OpenVPN

1. 基本配置

点击Enable开启OpenVPN，选择OpenVPN Type为“Server”，设置其余参数后点击<Save>。完成基本配置后，可以在Tunnel List(隧道列表)查看服务器隧道信息。

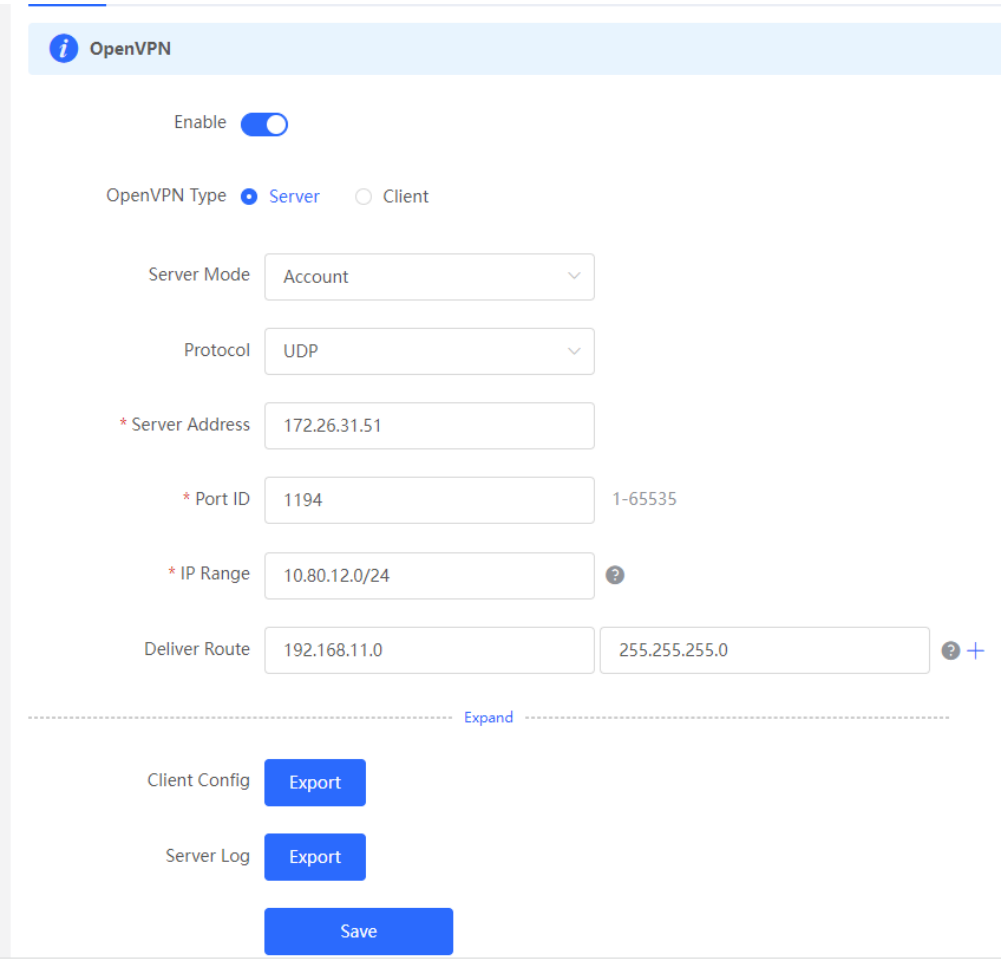


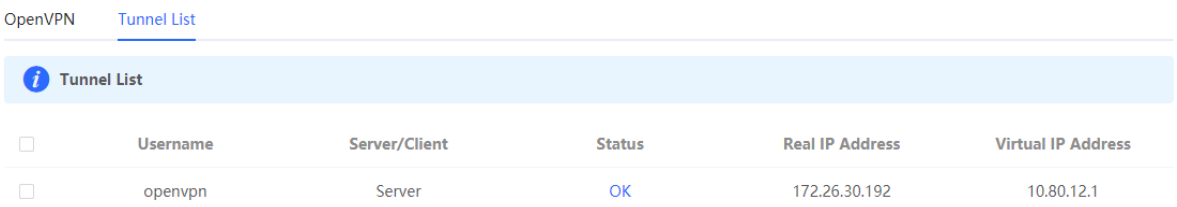
表7-19 OpenVPN 服务端基本配置信息描述表

参数	说明
Server Mode(服务器模式)	设备支持Account（账号密码）、Certificate（证书）和Account & Certificate（账号密码+证书）三种认证模式 ● 账号密码模式：客户端需要输入正确的账号密码和CA证书即可对接设备服务器，配置比较简单； ● 证书模式：客户端需要正确的CA证书、客户端证书和私钥即可对接设备服务器； ● 账号密码+证书认证模式：需要账号密码、CA证书、客户端证书和私钥，适用安全性要求高的场景。

参数	说明
Protocol(协议)	OpenVPN所有的通信都基于一个单一的IP端口，使用UDP或TCP协议通讯。 默认为UDP，推荐使用UDP协议通讯。在选择协议时候，需要注意2个加密隧道之间的网络状况，如有高延迟或者丢包较多的情况下，请选择TCP协议作为底层协议。
Server Address(服务器地址)	用于客户端对接的服务器地址，支持设置为域名
Port ID(端口号)	OpenVPN服务进程使用的端口。IANA（Internet Assigned Numbers Authority）指定给OpenVPN的官方端口为1194。若端口被占用或者在当地网络被禁用，则服务器日志会提示端口绑定失败的日志，需要更换端口号。
IP Range(地址范围)	OpenVPN地址池网段，地址池首个可用地址分配给服务器使用，其余地址分配给客户端，如设置地址范围为10.80.12.0/24，则服务器端VPN虚拟地址为10.80.12.1
Deliver Route(下发路由)	客户端访问服务器内网网段时需要走VPN拨号的线路。要实现客户端访问服务器内网，必须通过该设置来告知客户端路由信息。最多可配置3条路由
Client Config(客户端配置)	点击<Export>导出与该服务器对接的客户端的参数配置tar压缩包，解压后用于设置OpenVPN客户端 账号密码模式下压缩包包含配置文件client.ovpn、CA证书(ca.crt)、CA私钥(ca.key)； 若设置了证书认证，则压缩包包含配置文件client.ovpn、CA证书(ca.crt)、CA私钥(ca.key)，客户端证书(client.cart)和客户端私钥(client.key； 若开启TLS认证功能（见高级配置），除上述文件外，压缩包还会包含TLS身份验证密钥(tls.key)
Server Log(服务器日志)	点击<Export>导出服务端日志信息文件，包括服务端启动时间，客户端拨号日志等

注意

IP Range不能与设备本身的内网（LAN口）网段地址重叠。



2. 高级配置

点击扩展（Expand）可进行以下高级配置，若无特殊需求可保持默认。

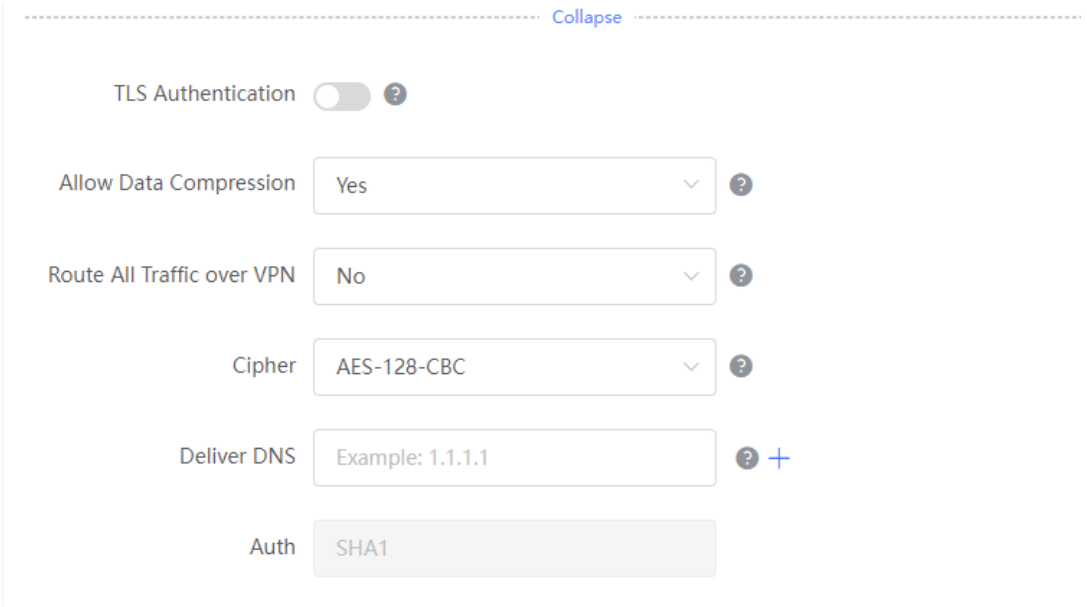


表7-20 OpenVPN 服务端高级配置信息描述表

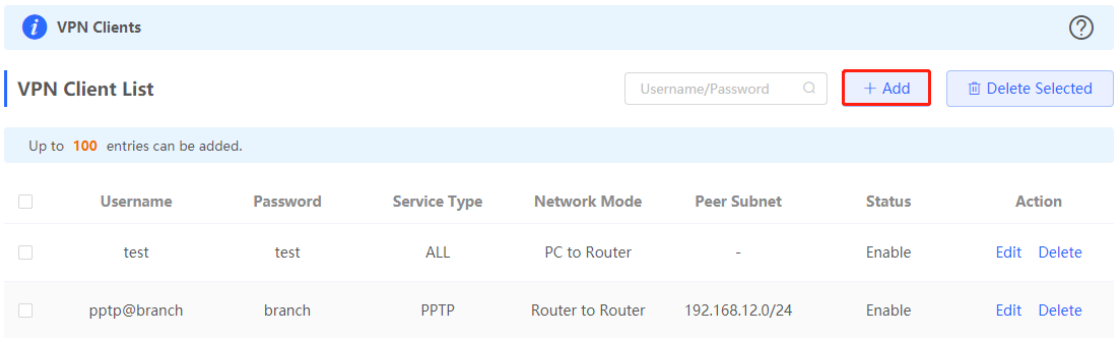
参数	说明
TLS Authentication(TLS校验)	TLS密钥用于通过要求双方在TLS握手之前拥有共享密钥来增强OpenVPN安全性。启用TLS身份验证后，客户端必须导入TLS密钥。（对端的OpenVPN客户端的版本必须高于2.40）
Allow Data Compression(允许数据压缩)	开启后，传送的数据可通过LZO算法压缩，压缩后节省带宽，但是会占用一定的CPU资源。要求客户端与服务器的该配置一致，否则连接无法成功
Route All Traffic over VPN(流量全部走VPN)	开启后，流量将全部走VPN路由通道，即配置VPN为默认路由
Cipher(数据加密方式)	在传输前对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读。 如果服务器配置为Auto模式，客户端可以配置任意数据加密算法； 如果服务器配置了具体的加密算法协议，则客户端必须配置相同的数据加密协议，否则无法连接成功
Deliver DNS	服务器推送给客户端的DNS地址，目前只支持向Window系统的客户端推送。
Auth	服务器使用的摘要算法，将告知客户端。默认为SHA1

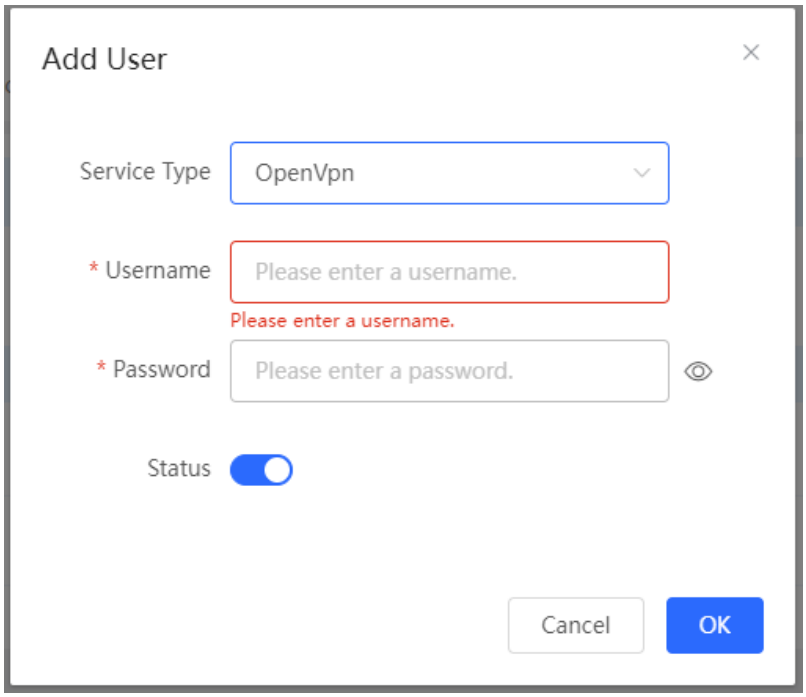
3. 设置 OpenVPN 用户

【本机管理-页面向导】VPN管理>> 账号管理

OpenVPN服务器只允许VPN用户管理列表中已添加的用户账号拨入，因此需手动配置用于客户端接入的用户账号。

点击<Add>，选择服务类型为OpenVpn，输入设置的用户名和密码点击<确定>。Status表示是否启用该账号。

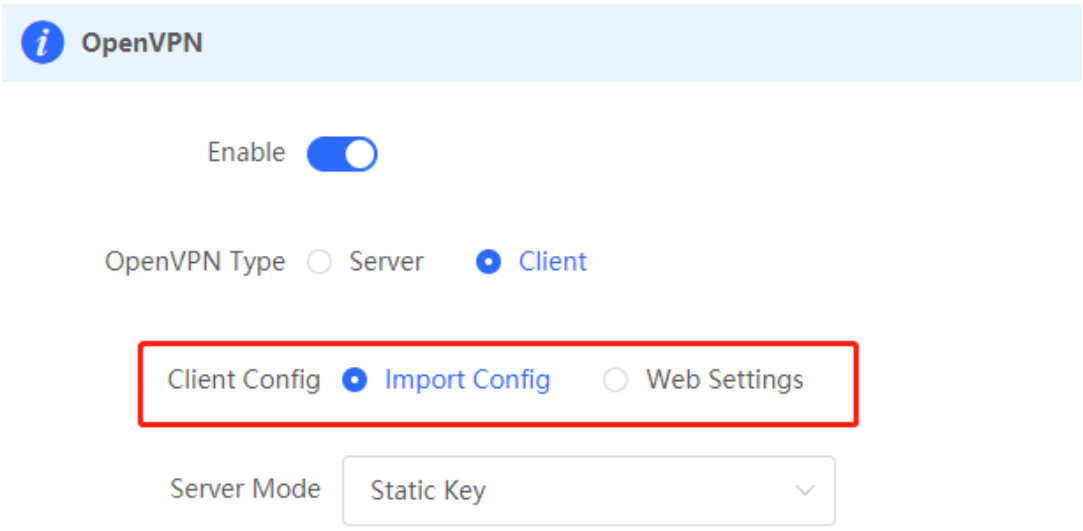




7.4.3 设置 OpenVPN 客户端

【本机管理-页面向导】VPN>> OpenVPN

目前本设备支持两种OpenVPN客户端配置模式：一种是Web Settings，即网页配置方式，一般用于对接非EG设备的服务器；另一种为Import Config，即手动导入配置文件的方式，用于对接类似本设备的服务器，客户端配置文件client.ovpn可直接由对接的OpenVPN服务器设备导出。



1. Import Config

点击Enable开启OpenVPN功能，选择OpenVPN Type为Client，并选择Client Config方式为Import Config，设置好服务器模式及对应参数后点击<Browse>导入客户端配置文件，点击<Save>使配置生效。

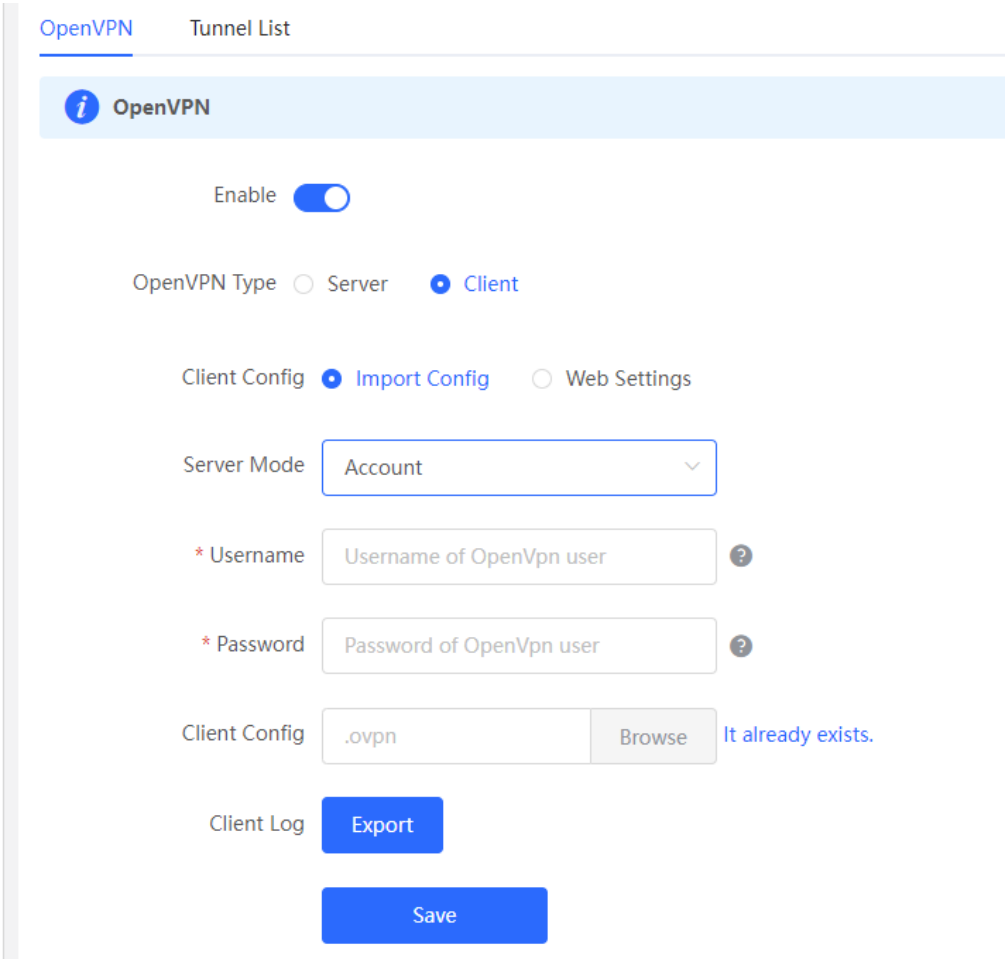


表7-21 OpenVPN 客户端 Import Config 方式配置信息描述表

参数	说明
Server Mode(服务器模式)	设备支持Account（账号密码）、Certificate（证书）、Account & Certificate（账号密码+证书）和Pre-Shared Key（静态共享密钥）四种认证模式 ● 账号密码模式：客户端需要输入正确的账号密码和CA证书，其中CA证书信息内嵌于客户端配置文件 ● 证书模式：客户端需要输入正确的CA证书、客户端证书和私钥，都内嵌于客户端配置文件 ● 账号密码+证书认证模式：客户端需要输入正确的账号密码、CA证书、客户端证书和私钥，其中CA证书信息、客户端证书和私钥内嵌于客户端配置文件 ● 静态共享密钥模式：除了上传客户端配置文件外，还需要上传静态密钥共享文件
Username & Password	输入服务器端配置的用户名和密码
Client Config	点击<Browse>，选取从服务器端导出的客户端配置文件进行上传
Pre-Shared Key	点击<Browse>，选取静态密钥共享文件进行上传
Workmode	仅在静态共享密钥模式下需要配置 NAT：仅允许客户端访问服务器网络，不允许服务器访问客户端网络 Router：允许服务器访问客户端网络
Client Log	点击<Export>，导出客户端的日志文件

2. Web Settings

点击Enable开启OpenVPN功能，选择OpenVPN Type为Client，并选择Client Config方式为Web Settings，设置好Device Mode、Server Mode等参数后点击<Save>使配置生效。

(1) 基本配置

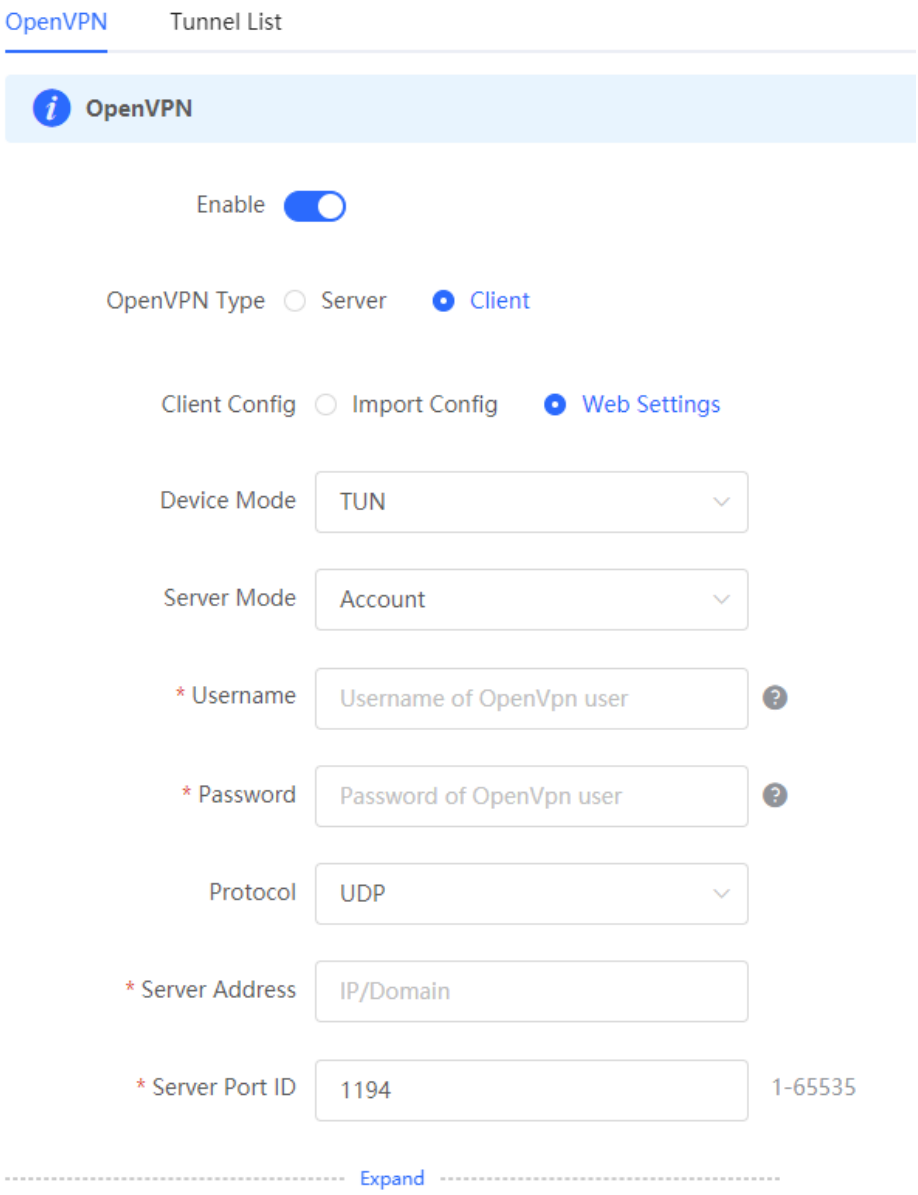


表7-22 OpenVPN 客户端 Web Setting 方式配置信息描述表

参数	说明
Device Mode(设备模式)	EG设备作为客户端支持设置为TUN或TAP模式，该配置要和服务器一致。 EG设备作为服务器仅支持TUN模式
Server Mode(服务器模式)	支持Account（账号密码）、Certificate（证书）和Account & Certificate（账号密码+证书）三种认证模式 ● 账号密码模式：客户端需要输入正确的账号密码和导入CA证书文件 ● 证书模式：客户端需要导入正确的CA证书、客户端证书和私钥文件 ● 账号密码+证书认证模式：客户端需要输入正确的账号密码并导入CA证书、客户端证书和私钥文件
Protocol(协议)	支持UDP和TCP模式，和服务器配置保持一致

参数	说明
Server Address(服务器地址)	填入要对接的服务器的地址或者域名
Server Port ID(服务器端口)	填入对接的服务器的端口号
CA Certificate	点击<Browse>，选取后缀为.ca的CA证书文件进行上传
Client Key	点击<Browse>，选取后缀为.key的客户端私钥文件进行上传
Client Certificate	点击<Browse>，选取后缀为.crt的客户端证书文件进行上传
Client Certificate Key	有些服务器（如Mikrotik服务器）提供的客户端证书是经过两次加密的，在客户端使用这种证书时需要本密钥
Client Log	点击<Export>，导出客户端的日志文件

(2) 高级配置

点击扩展（Expand）可进行更多配置，若无特殊需求可保持默认。

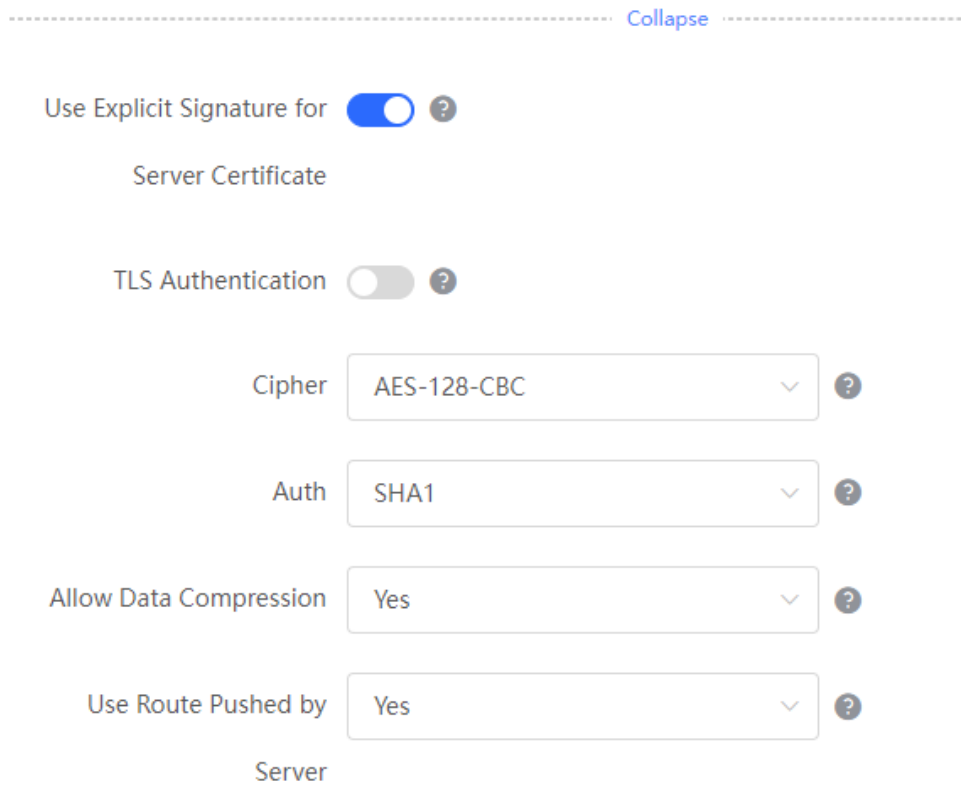


表7-23 OpenVPN 客户端 Web Setting 方式配置信息描述表

参数	说明
Use Explicit Signature for Server Certificate(对服务器证书使用显式	对服务器证书使用显式签名进行校验，默认开启 如果服务端证书不使用显式签名，如Mikrotik设备服务器，则需要关闭此功

参数	说明
签名)	能，否则会导致对接失败
TLS Authentication	开启后，要对服务器进行TLS身份验证。需要上传TLS证书文件
Cipher	数据压缩算法，该配置要和服务器一致，否则无法成功连接
Auth	用于验证数据包的摘要算法，目前支持SHA1、MD5、SHA256和NULL算法。该配置要和服务器一致，否则无法成功连接
Allow Data Compression	设置是否允许数据压缩，开启后，传送的数据可通过LZO算法压缩，该配置要和服务器一致
Use Route Pushed by Server	设置是否接受服务器端的路由推送。关闭后无法接受服务器的路由下发，若要访问服务器内网设备，需要设置为Yes。

7.4.4 查看 OpenVPN 隧道信息

【本机管理-页面向导】VPN管理>> OpenVPN>> Tunnel List

完成服务器和客户端的设置之后，可以查看到OpenVPN隧道的连接状态。若连接成功，服务端的隧道列表中将显示客户端的隧道信息。

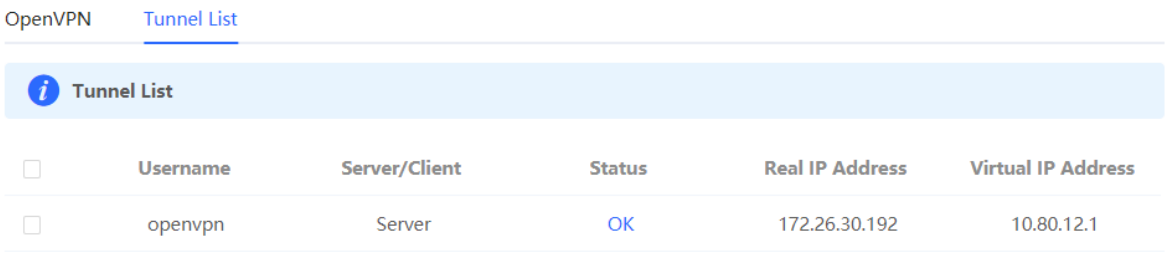


表7-24 OpenVPN 隧道信息描述表

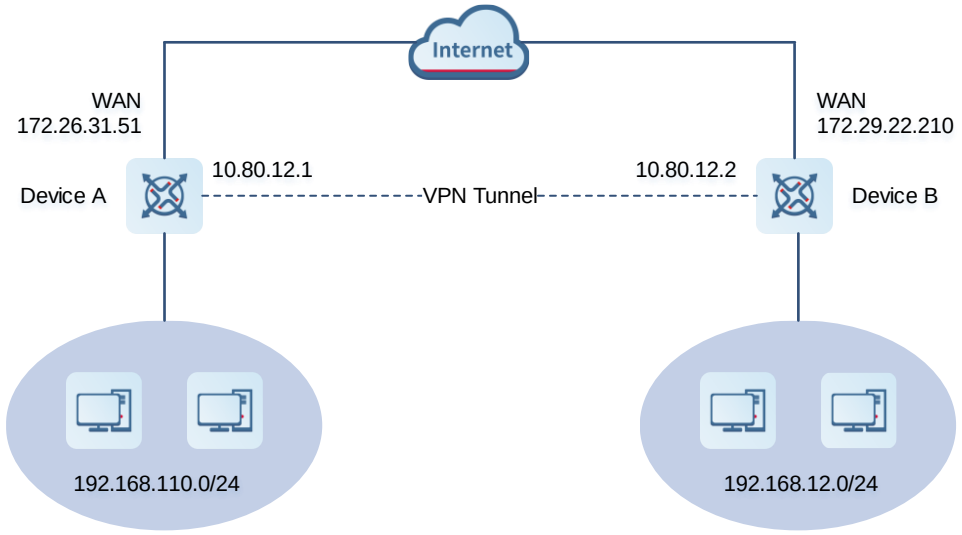
参数	说明
Username	客户端用于身份认证的用户名，服务端默认显示openvpn
Server/Client	隧道本端为客户端还是服务器
Status	隧道建立状态
Real IP Address	本端接入VPN的实际IP地址
Virtual IP Address	本端的虚拟IP地址，客户端的虚拟IP地址由服务器分配

7.4.5 典型配置案例

1. 组网需求

客户端网络通过OpenVPN的方式拨号到服务端，实现客户端和服务端能够互相访问内网。

2. 组网图



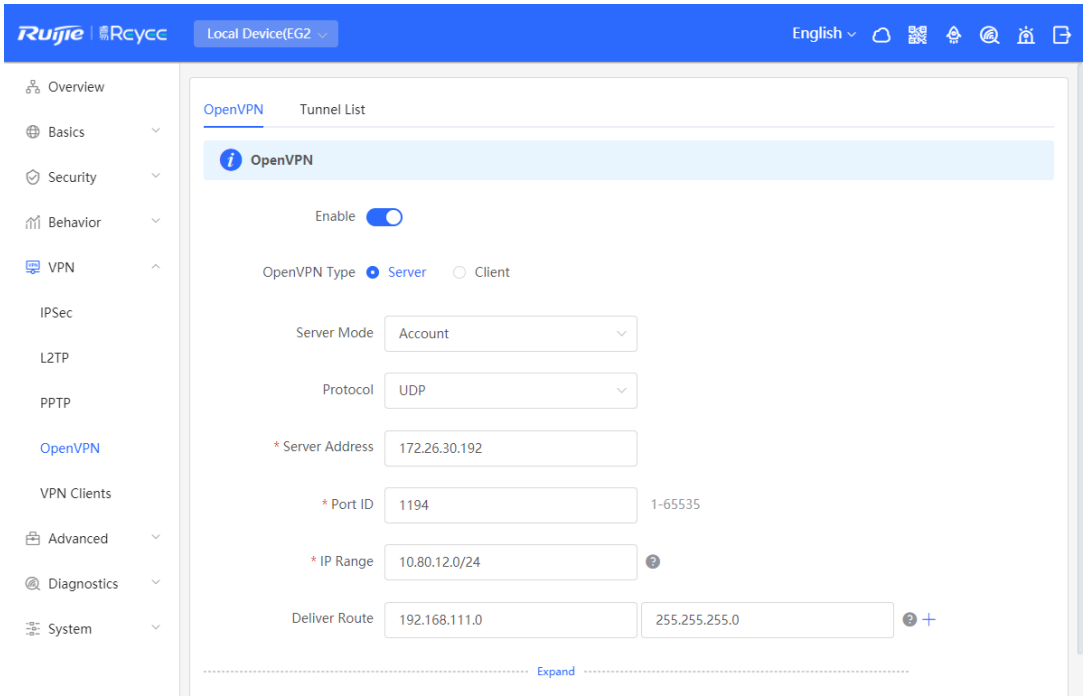
3. 配置要点

- 在Device A上部署OpenVPN服务器端。
- 在Device B上部署OpenVPN客户端。
- 服务端需将本端的内网网段推送给客户端，使客户端能够访问服务端内网。

4. 配置步骤

(1) 配置Device A

a 登录Web网管后，点击 VPN管理>> OpenVPN>> OpenVPN，进入OpenVPN设置界面。



b 点击开关开启OpenVPN，选择OpenVPN Type为Server，下拉选择服务器模式、协议，输入端口号（默认1194）、服务器地址（即本机的外网IP地址），点击<保存>完成参数配置。

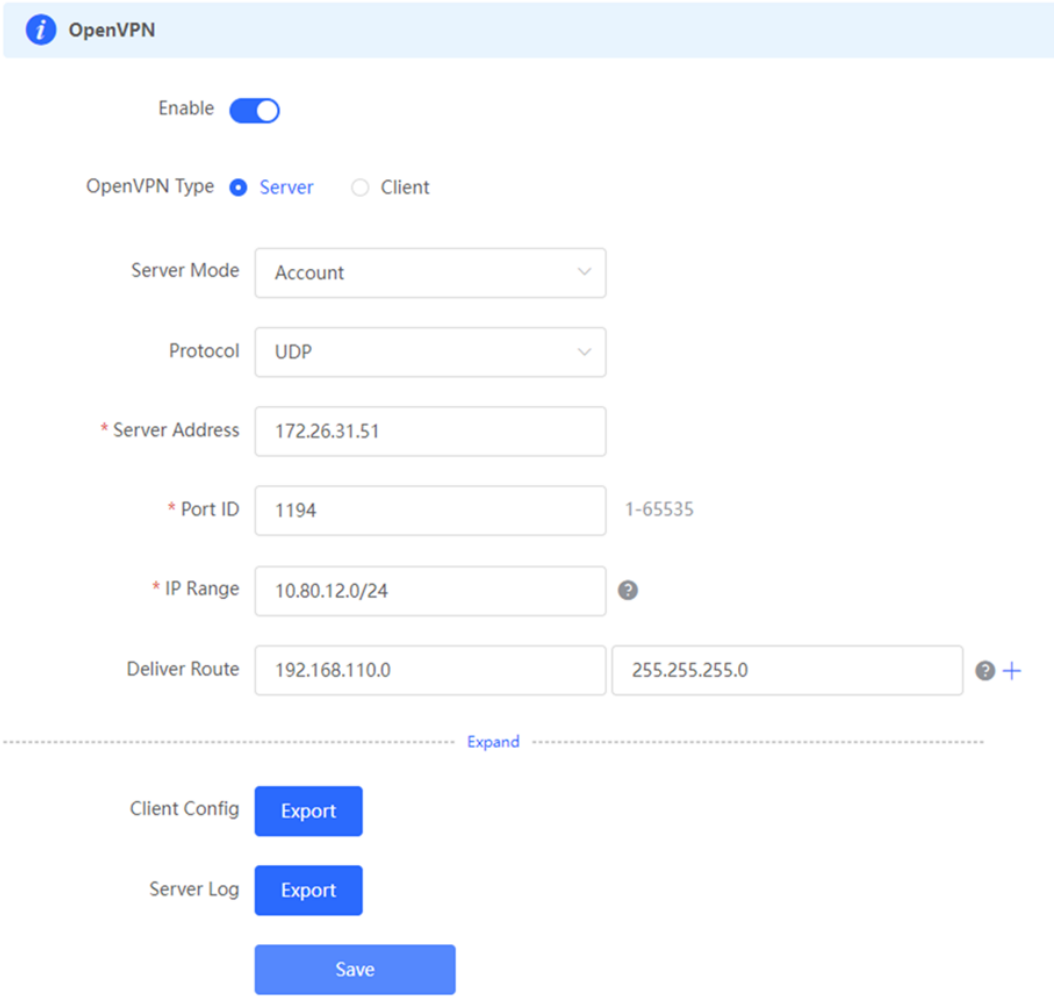
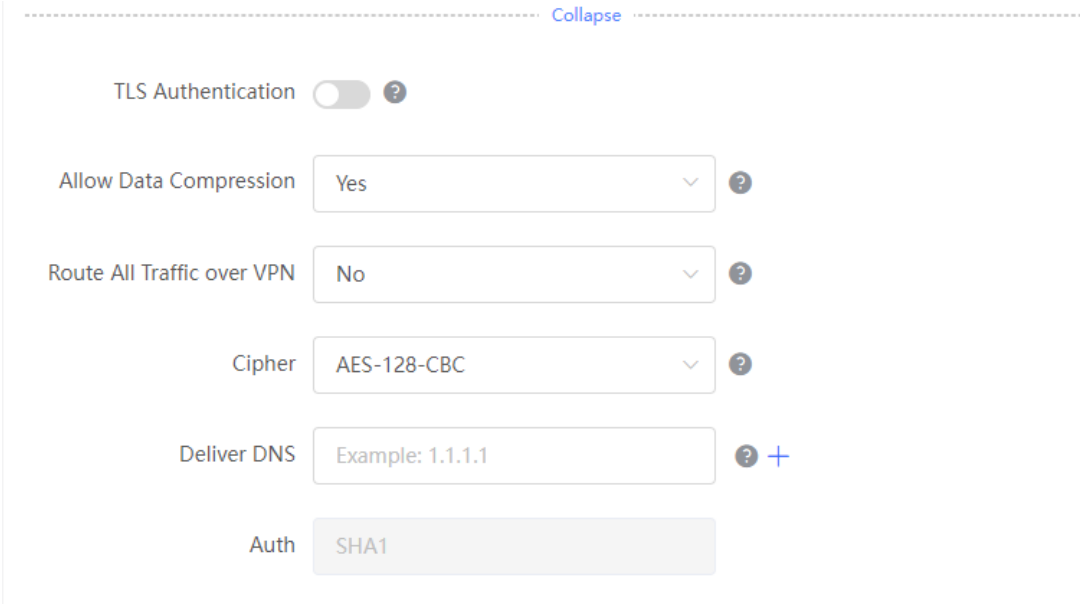


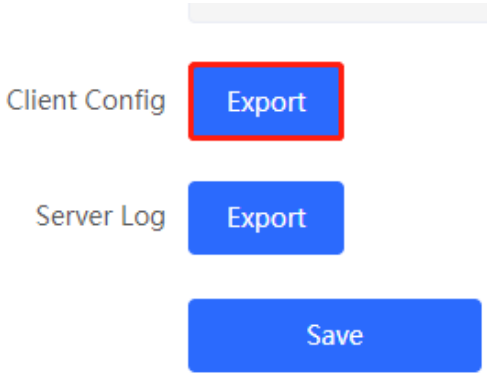
表7-25 OpenVPN 服务端配置信息描述表

参数	说明
Server Mode	选择认证模式，此处以Account模式为例 对于安全性要求高的场景，可选择Account & Certificate
Protocol	无特殊情况选择UDP即可。 若加密隧道之间的网络状况不加，例如有高延迟或者丢包较多的情况下，请选择TCP协议
Server Address	服务器的WAN口地址，即172.26.31.51
Port ID	默认为1194。无特殊情况保持默认即可，若端口被占用或者在当地网络被禁用，请更换为可用的端口号
IP Range	OpenVPN地址池网段，地址池首个可用地址分配给服务器使用，其余地址分配给客户端。设置地址范围为10.80.12.0/24，则服务器端VPN虚拟地址为10.80.12.1
Deliver Route	如果客户端想要访问服务器内网网段，则需添加对应网段的路由信息

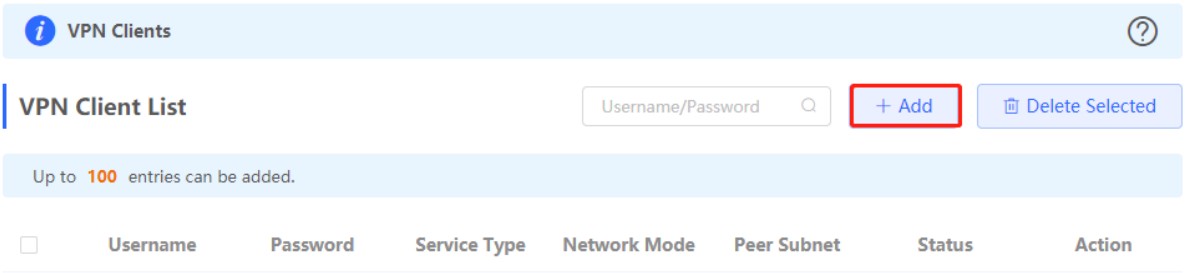
c 点击Expand展开更多设置。如果与易网络其他EG设备对接的话，建议高级配置保持默认即可；与其他厂商进行对接，参数保持一致即可。

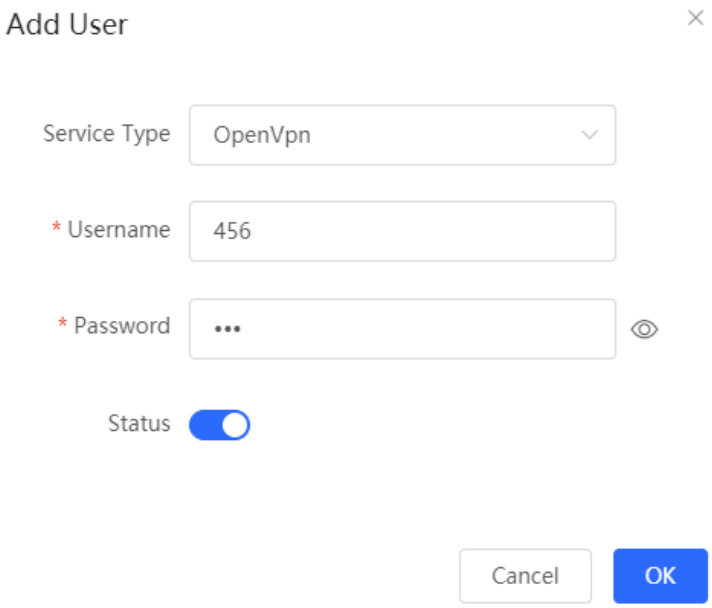


d 点击<Export>导出客户端参数配置压缩包，下载到本地并解压，用于后续步骤设置OpenVPN客户端。



e 点击 VPN >> VPN Clients，添加OpenVPN用户账号。





(2) 配置Device B

a 登录Web网管后，进入OpenVPN设置界面。

b 点击开关开启OpenVPN，选择OpenVPN类型为Client。有两种配置方式可供选择，请选择其中一种方式进行配置。推荐使用Import Config方式。

Import Config方式：

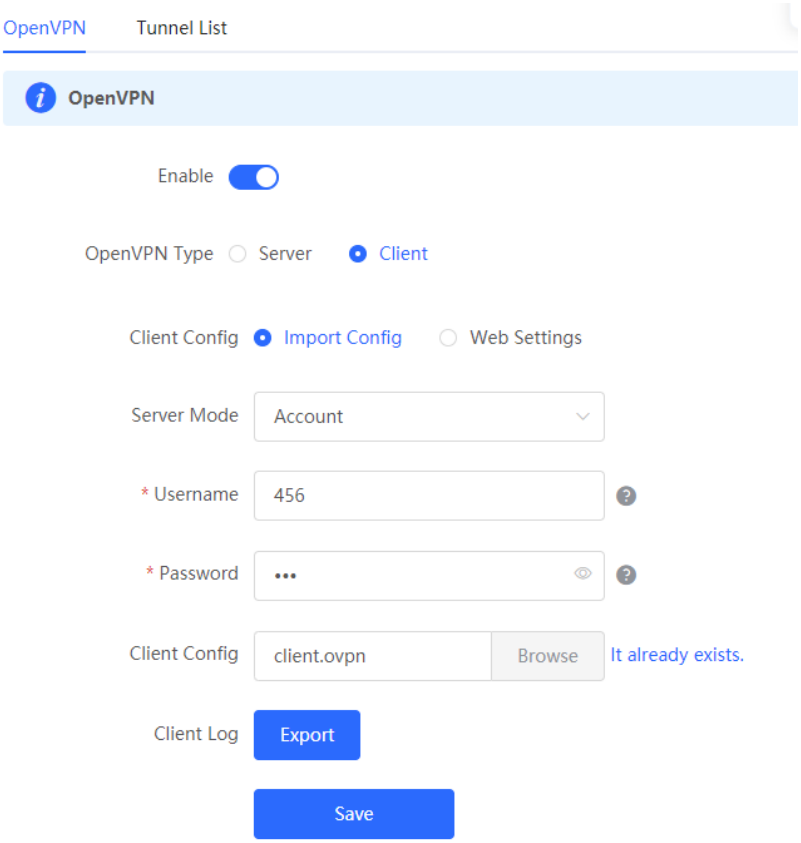


表7-26 OpenVPN 客户端 Import Config 配置示例描述表

参数	说明
Client Config	选择Import Config。
Server Mode	与服务端一致，本例中选择Account 模式
Username & Password	输入服务器端配置的用户名和密码
Client Config	点击<Browse>，选取从服务器端导出的客户端配置文件进行上传

Web Settings方式:

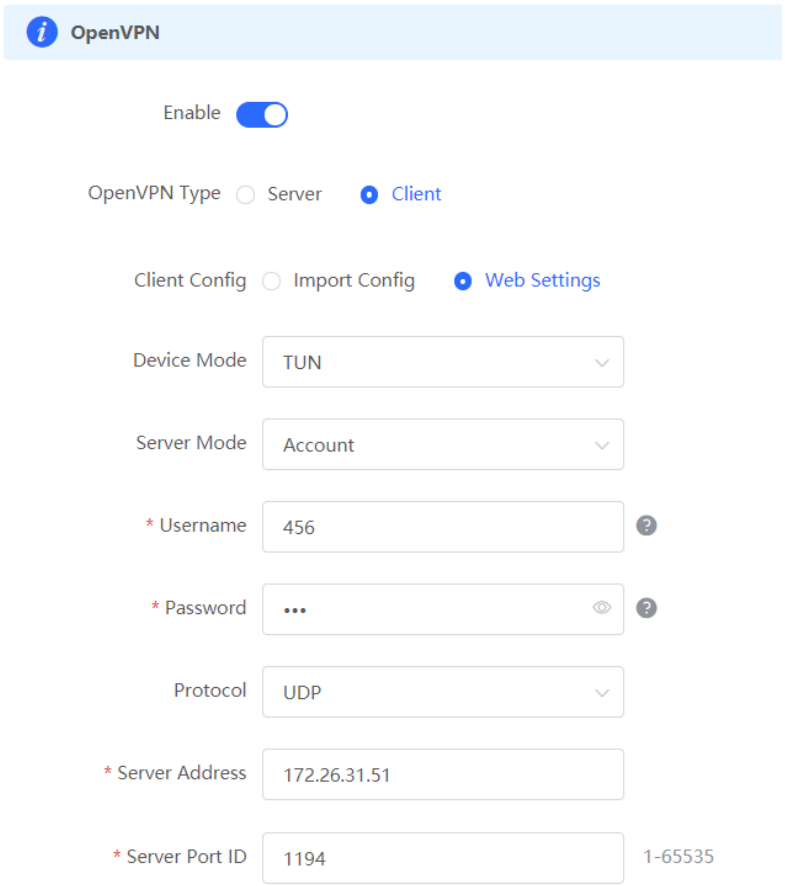


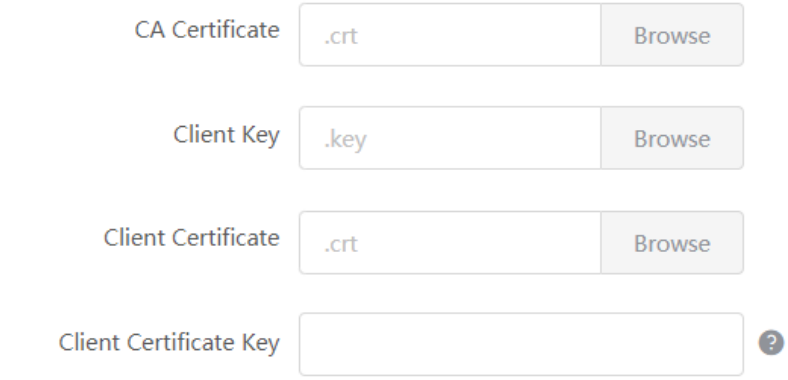
表7-27 OpenVPN 客户端 Web Settings 配置示例描述表

参数	说明
Client Config	选择Web Settings。
Device Mode	与服务端一致，本例中选择TUN模式
Server Mode	与服务端一致，本例中选择Account模式
Username & Password	输入服务器端配置的用户名和密码

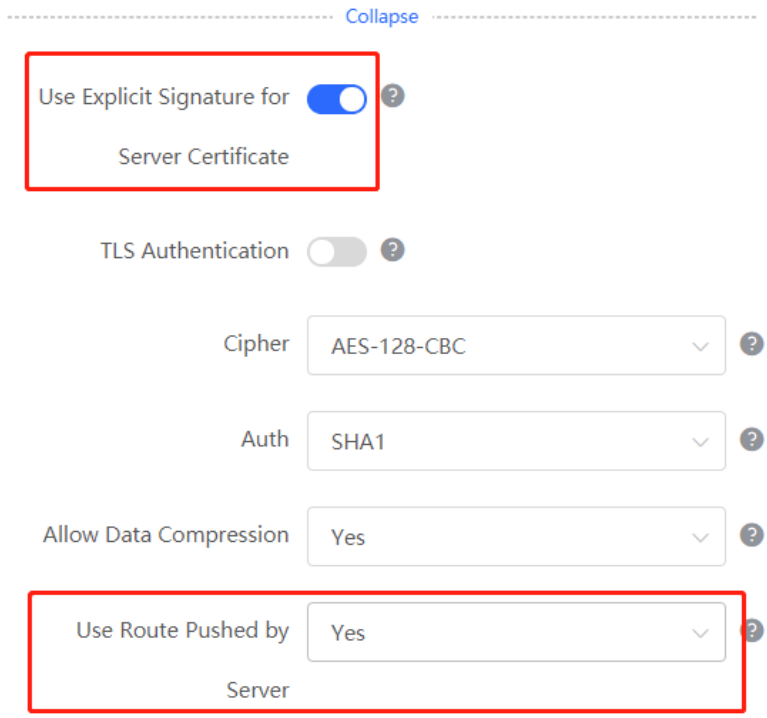
参数	说明
Protocol	与服务端一致，本例中选择UDP
Server Address	输入服务器的公网IP地址，即172.26.31.51
Server Port ID	填入服务器使用的端口号，如1194

根据Server Mode导入对应文件。

若设备模式包含证书（Certificate）模式，需要导入CA证书（CA Certificate）、客户端证书（Client Certificate）和客户端私钥（Client Key）文件；若设备模式为账号模式，导入CA证书文件即可。若客户端证书有加密，还需输入对应的共享密钥（Client Certificate Key）。



点击Expand展开更多设置，确认接受服务器推送路由（Use Route Pushed by Server）功能处于开启状态。配置与服务器端保持一致即可。如果客户端要对接非EG设备，如海外Mikrotik设备时，则需要关闭校验服务器使用显示签名（Use Explicit Signature for Server Certificate）功能。

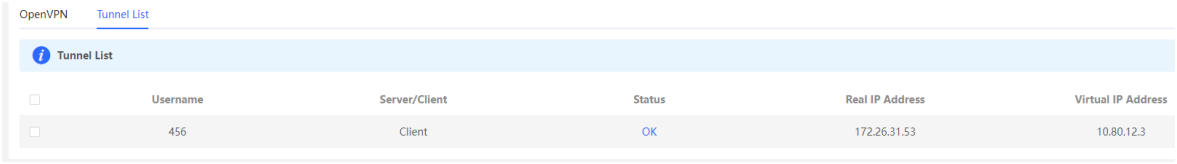


c 完成以上配置后，点击<Save>，使配置生效。

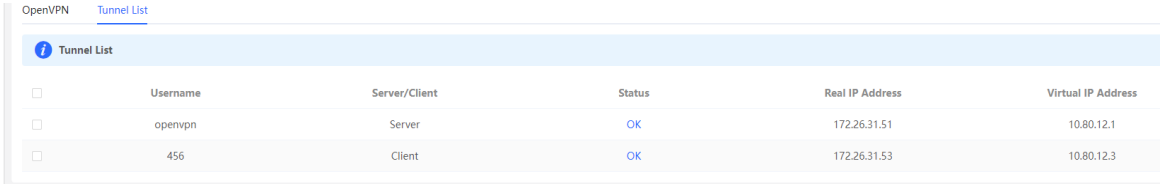
5. 效果验证

完成服务器和客户端的配置后，在Tunnel List里能查看到两端的隧道信息。

客户端：



服务器：



8 PoE 供电

注意

仅支持PoE供电的设备（一般设备型号后缀带-P标识）支持本功能。

例如：RG-EG105G-P和RG-EG210G-P。

【本机管理-页面向导】基本管理>> PoE供电

设备支持通过端口为PoE受电设备供电。可以查看供电总功率、当前已用功率（当前功耗）、剩余可供功率（剩余功耗），以及PoE供电状态是否异常。鼠标移至端口图标，出现供电开关，用来控制端口是否开启供电。

9 系统管理

9.1 设置 Web 登录密码

【关闭自组网发现-页面向导】系统管理>>登录管理>>登录密码

【开启自组网发现-整网管理-页面向导】系统管理>>登录密码

输入旧密码和新密码，保存后需使用新密码重新登录。

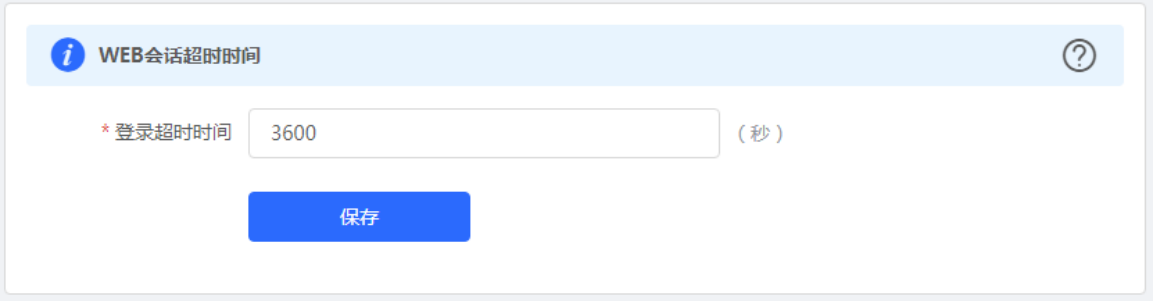
注意

当自组网发现处于开启状态，将同步修改网络中的所有设备的登录密码。

9.2 设置页面超时时间

【本机管理-页面向导】系统管理>> 登录管理>>登录超时时间

Web页面一段时间内没有操作，将自动断开会话，再次操作需要输入密码重新进入配置。默认超时时间为3600秒，即1小时。

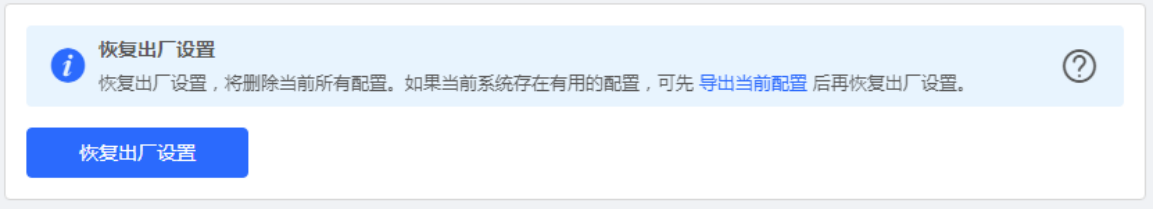


9.3 恢复出厂设置

9.3.1 本设备恢复出厂

【本机管理-页面向导】系统管理>> 配置管理>> 恢复出厂设置

点击<恢复出厂设置>按钮后确认，将恢复出厂的默认配置。



注意

该操作将清空现有设定，并重启设备。如果当前系统存在有用的配置，可先导出当前配置（请参考配置备份与导入）后再恢复出厂设置。请谨慎操作。

9.3.2 整网设备恢复出厂

【整网管理-页面向导】系统管理>> 配置管理>> 恢复出厂设置

选择<整网设备>，并选择是否“解除用户帐号绑定”，点击<整网恢复出厂设置>，当前网络的所有设备都将恢复出厂设置。

注意

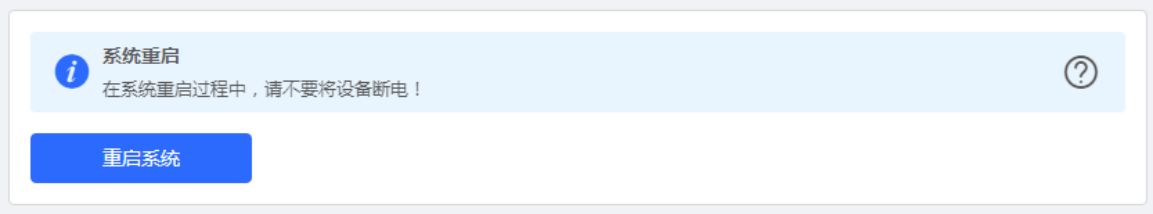
该操作将清空整网中所有设备的现有设定，并重启设备。请谨慎操作。

9.4 重启设备

9.4.1 重启本设备

【本机管理-页面向导】系统管理>> 设备重启>> 系统重启

点击<重启系统>，设备将重新启动。重启过程中，请勿刷新或关闭页面，当设备重启成功并且Web服务可用后，将自动跳转到登录页。



9.4.2 重启整网设备

【整网管理-页面向导】系统管理>> 设备重启>> 系统重启

选择<整网设备>，点击<整网重启系统>，重启当前网络中的所有设备。

注意

整网重启需花费一定时间，请耐心等待。整网操作将对整个网络造成影响，请谨慎操作。

9.4.3 重启网络中的指定设备

【整网管理-页面向导】系统管理>> 设备重启>> 系统重启

选择<指定设备>，从“可操作设备”列表中选择要操作的设备，点击<添加>到右侧“已选设备”列表。点击<重启系统>，将重启“已选设备”列表中所指定的设备。

9.5 设置定时重启

请确认系统时间准确，关于系统时间的配置介绍请参考9.6 设置和查看系统时间。防止在错误的时间重启导致断网。

【页面向导】系统管理>> 设备重启>> 定时重启

点击<开启>，选择每周定时重启的日期和时间。点击<保存>后，下次系统时间匹配到定时时间时设备将重启。

注意

在整网管理模式下开启定时重启，当系统时间匹配到定时时间，整网设备都将重启，请谨慎设置。

9.6 设置和查看系统时间

【页面向导】系统管理>> 系统时间

可查看当前系统时间，若时间错误，请检查并选择当地所在的时区。若时区正确时间仍有错误，可点击<修改>可手动设置。同时设备支持设置NTP服务器（Network Time Protocol，网络时间服务器），默认多个服务器互为备份，如有本地服务器需求可根据需要增加或删除。

点击“当前时间”，将自动填入当前登录设备的系统时间。

9.7 配置备份与导入

【页面向导】系统管理>> 配置管理>> 备份与导入

配置备份：点击<备份>，将生成备份配置并下载导出的配置文件到本地。

配置导入：点击<浏览>，在本地选择之前备份的配置文件，再点击<导入>，将文件所指定的配置应用到设备上。导入配置后设备将重启。

9.8 指示灯开关

【整网管理-页面向导】整网管理>> LED灯设置

点击开关按钮，控制下联设备的LED灯是否开启。点击<保存>使配置下发生效。

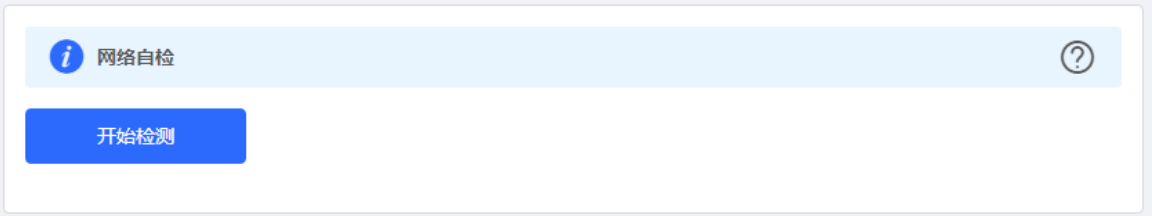
9.9 故障诊断

9.9.1 网络自检

当设备出现网络问题时，请执行“网络自检”功能，并根据检测结果配置设备。

【本机管理-页面向导】故障诊断>> 网络自检

点击<开始检测>按钮执行网络检测。检测完成后会显示检测结果。



如果检测到网络问题，将显示检测结果并给出修复建议。用户可参考建议修复故障。

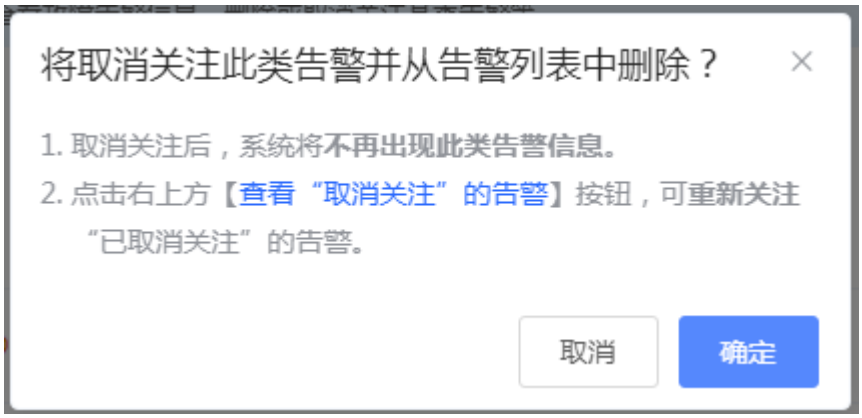
9.9.2 故障告警

【整网管理-页面向导】整网管理>> 故障告警

显示网络环境中可能存在的问题，以便于故障的预防与排查。默认关注所有类型的告警信息，点击告警列表右侧的<取消关注>按钮，可以不再关注指定告警。

注意

取消关注告警后，系统将不对该类故障进行告警提示，用户无法及时发现和处理故障，请谨慎操作。



点击<查看“取消关注”的告警>，可以查看和重新关注告警。

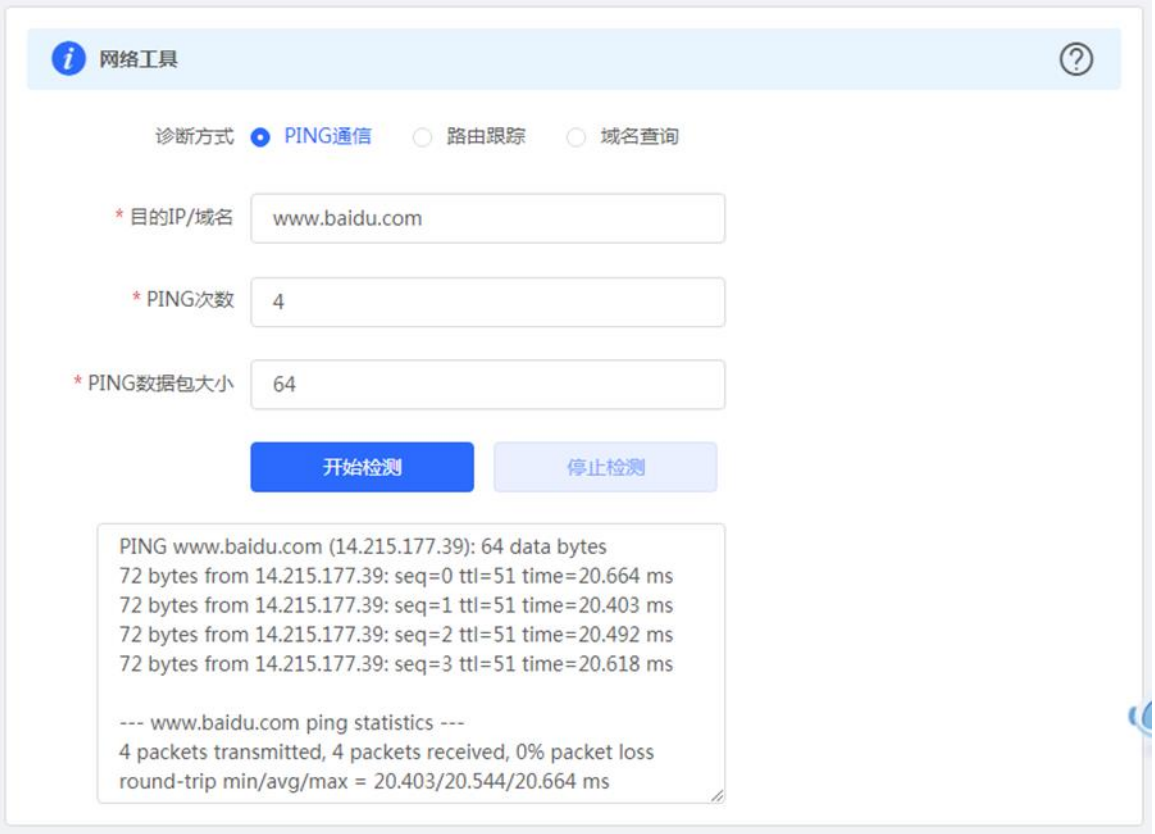
9.9.3 网络测试工具

【本机管理-页面向导】故障诊断>> 网络工具

选择诊断方式，输入IP地址或网址，点击<开始检测>。

PING通信用于测试设备与该IP或网址的网络连通性，显示Ping通信失败表示网络未与该IP或网址联通。

路由跟踪能够查看通向某IP或网址的网络路径，域名查询能够查看某网址解析所用的DNS服务器地址。



9.9.4 抓包诊断

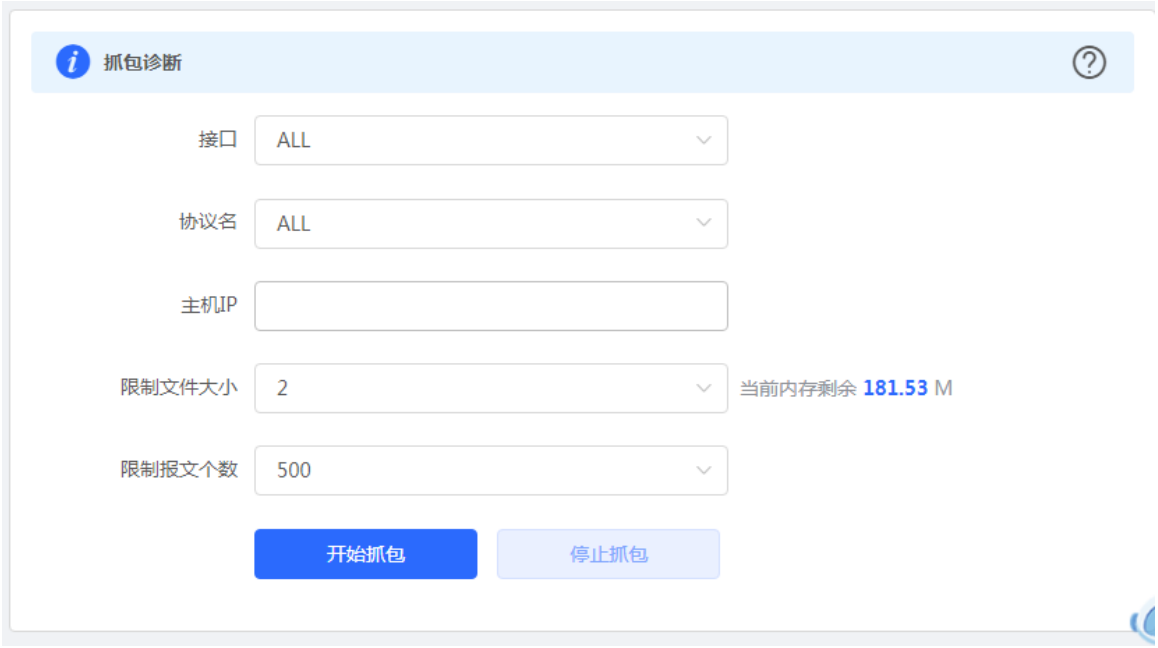
【本机管理-页面向导】故障诊断>> 抓包诊断

当设备出故障问题需要定位时，可以通过分析抓包结果来定位和排查问题。

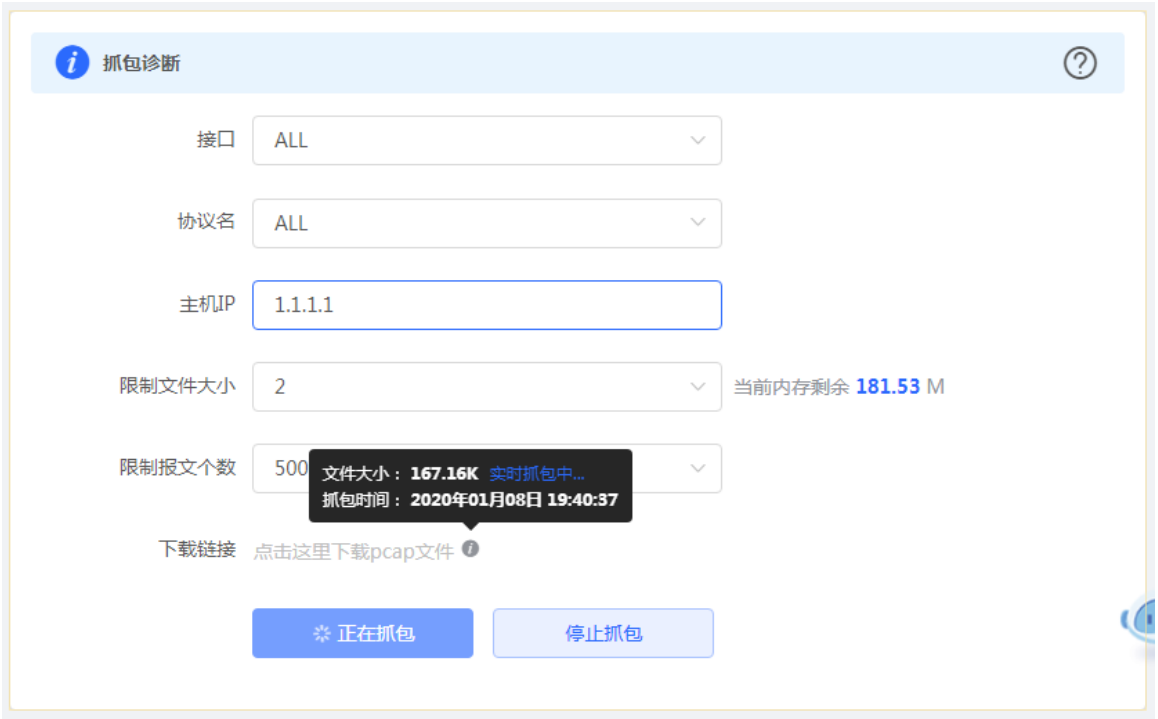
选择接口，通过指定协议和主机IP来指定抓取的数据包内容，并通过选择文件大小和报文数来确定抓包自动停止的条件（当抓取包大小或报文数达到设定值，将停止抓包并生成诊断包下载链接）。点击<开始抓包>，将执行抓包命令。

⚠ 注意：

抓包操作可能占用较多系统资源导致网络卡顿，请谨慎操作。



抓包过程中可随时停止，生成下载链接。点击链接可保存pcap格式的抓包结果到本地，用Wireshark等分析软件进行查看与分析。



9.9.5 故障收集

【本机管理-页面向导】故障诊断>> 故障收集

当设备出现故障时，需要收集故障信息。点击<一键收集>，将会打包设备配置文件为压缩文件，下载到本地后，可提供给开发人员定位故障。

9.10 系统升级和查看系统版本

注意

- 建议在进行软件升级前进行配置备份。
- 版本更新将重启设备，升级过程中请不要刷新或关闭浏览器。

9.10.1 在线升级

【本机管理-页面向导】系统管理>>系统升级>>在线升级

显示当前系统版本并检测是否存在可更新版本。如果检测到版本更新可以点击<马上升级>按钮进行在线更新。若不具备在线升级的网络环境，可先点击“下载升级包”将升级安装包保存至本地，再进行本地升级。

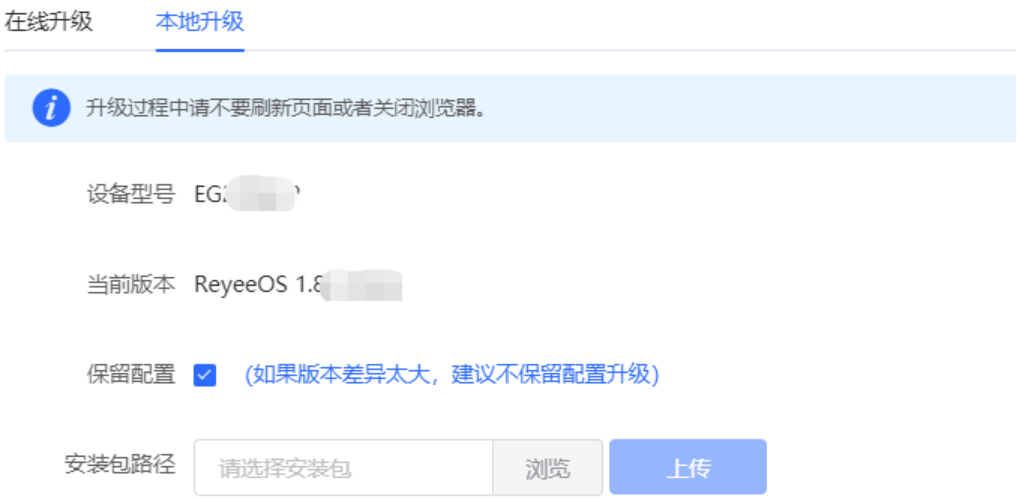
说明

- 在线升级会保留当前配置。
- 请不要在升级过程中刷新页面或关闭浏览器，升级成功后将自动跳转到登录页。

9.10.2 本地升级

【本机管理-页面向导】系统管理>>系统升级>>本地升级

显示设备型号及当前软件版本。可以选择是否保留配置升级，点击<浏览>选择本地软件版本安装包，点击<上传>上传安装包并进行升级。



9.11 切换语言

【页面向导】Web页面右上角 中文

在下拉框中点击选择语言，将切换系统界面的语言。

10 常见问题

10.1 登录 Web 失败怎么办

(1) 确认网线已正常连接到了设备的LAN口，对应的指示灯闪烁或者常亮。

(2) 访问Web管理系统前，建议将计算机设置成“自动获取IP地址”，由开启DHCP服务的设备自动给计算机分配IP地址。如果需要给计算机指定静态IP地址，请将计算机的IP与设备LAN口IP设置在一网段，如：默认LAN口IP地址为192.168.110.1，子网掩码为255.255.255.0，则计算机的IP地址应设置为192.168.110.X（X为2至254之间任意整数），子网掩码为255.255.255.0。

(3) 使用Ping命令检测计算机与设备之间的连通性，若Ping通信失败，请检查网络设置。

(4) 若完成上述步骤后仍无法登录到设备管理界面，请将设备恢复为出厂配置。

10.2 忘记设备密码/恢复出厂设置

在设备接通电源的情况下，长按面板上的reset键5秒，设备重启后将还原为出厂设置。恢复出厂设置后，可使用默认IP（192.168.110.1）登录设备Web。

10.3 宽带上网失败

(1) 确认宽带账号密码是否正确。如果忘记宽带账号密码，请参考忘记宽带账号密码的解决方案。Check whether the PPPoE account and password are correct.

(2) 确认运营商分配的IP地址是否与网络中的其他设备地址冲突。Check whether the IP address assigned by the ISP will conflict with the IP address existing on the router.

(3) 确认设备的MTU值配置满足运营商要求。Check whether the MTU setting of the device meets the requirements of the ISP.

默认MTU为1500，如需修改请参考3.2.3 修改MTU。

(4) 确认是否运营商是否要求接入网络时需要携带VLAN ID。Check whether it is needed to config Vlan tag for PPPoE.

默认不携带VLAN标签，请参考3.2.5 设置VLAN标签进行设置。There is no Vlan tag for PPPoE by default.