InHand ER605 5G 边缘路由器

用户手册

资料版本：V1.0—2023.09

www.inhand.com.cn

北京映翰通网络技术股份有限公司

声明

首先非常感谢您选择本公司产品！在使用前，请您仔细阅读本用户手册。

非本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

由于不断更新，本公司不能承诺本资料与实际产品一致，同时也不承担由于实际技术参数与本资料不符所导致的任何争议，任何改动恕不提前通知。本公司保留最终更改权和解释权。

版权所有©2023北京映翰通网络技术股份有限公司及其许可者版权所有，保留一切权利。

本手册图形界面约定

格 式	意 义
【 】	表示功能模块或菜单，如：在【状态】菜单下。
“ ”	表示按钮名称，如：点击“添加”窗口。
〉	多级菜单用“〉”隔开。如“文件〉新建〉文件夹”多级菜单表示“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
说明	对操作内容的描述进行必要的补充和说明。

目 录

1 简介

Edge Router 605 是北京映翰通面向商业联网领域推出的新一代 5G 边缘路由器产品，该产品为各行业提供高速安全的网络接入。凭借 4G/5G 无线网络和多种宽带服务，提供随处可得的不间断的互联网接入，以其全面的安全性和无线服务等特性，实现设备联网，为真正意义上的设备信息化提供数据的高速通路。

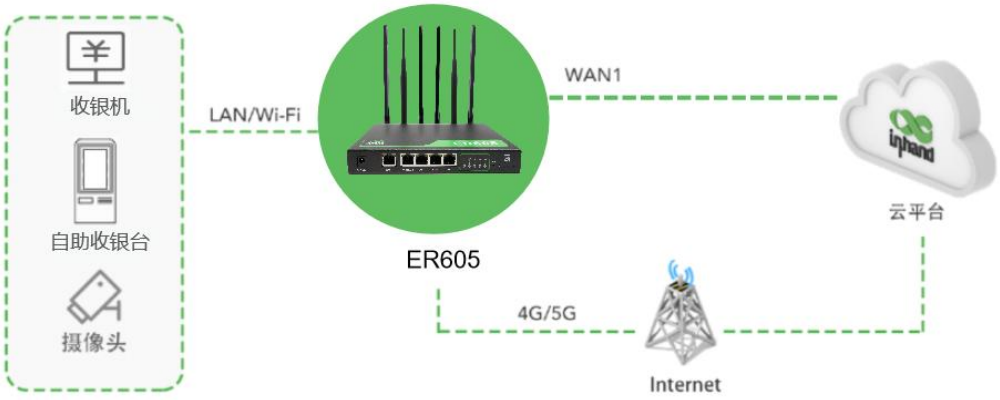


图 1 应用方案图

2 硬件部分

2.1 指示灯说明

ER605 指示灯	LED 灯状态和定义
系统状态灯	常灭 --- 设备未上电 红色常亮 --- 系统启动中 绿色闪烁 --- 系统正常运行 红色闪烁 --- 系统故障 黄色闪烁 --- 系统升级
联网状态灯	常灭 --- 网络未连接 红色闪烁 --- 蜂窝网连接中 绿色常亮 --- 蜂窝网连接成功 黄色闪烁 --- 有线网连接中 黄色常亮 --- 有线网连接成功
蜂窝信号灯	常灭 --- 处于关闭状态 红色常亮 --- 信号质量较差 黄色常亮 --- 信号质量良好 绿色常亮 --- 信号质量好
Wi-Fi 2.4G	常灭 --- 处于关闭状态 绿色闪烁 --- 2.4G 正常工作 绿色常亮 --- 2.4G WiFi 异常
Wi-Fi 5G	常灭 --- 处于关闭状态 黄色闪烁 --- 5G WiFi 正常工作 黄色常亮 --- 5G WiFi 异常

注：对于联网状态灯，如果两种网络均正常，则显示黄色有线指示灯；如果其中一种网络不正常，则显示当前正常网络的指示灯；若两种网络均不正常，则显示红色。

2.2 通过 Reset 按钮恢复出厂

通过 Reset 按钮恢复出厂默认值：

第一步：设备上电（10 秒）按住 reset 按键，直至 SYS 指示灯黄色常亮；

第二步：松开，SYS 指示灯变为黄色闪烁；

第三步：再次按 reset 键，直到 SYS 指示灯黄色常亮；

3 默认配置

序号	功能	默认配置
1	**蜂窝网络拨号**	- 启用双 SIM 卡，默认使用 SIM1
2	**Wi-Fi 默认配置**	- Wi-Fi 2.4G 接入点启用，SSID：以 ER605 - 为前缀，后面为无线 MAC 后 6 位数字 - Wi-Fi 5G 接入点启用，SSID：以 ER605-5G - 为前缀，后面为无线 MAC 后 6 位数字 - 认证方式为 WPA2-PSK - 密码均为 SN 序列号后 8 位
3	**以太网默认配置**	- 4 个 LAN 口启用 - IP 地址：192.168.2.1 - 子网掩码：255.255.255.0 - DHCP 服务器启用，地址池为 192.168.2.2 ~ 192.168.2.100，可为下端设备自动分配 IP 地址
4	**网络访问控制**	- 本地 HTTP 及 HTTPS 启用，端口号分别是 80 和 443 - 禁用来自蜂窝网络的访问
5	**用户名和密码**	- adm/123456（超级管理员）

4 路由器快速联网

4.1 环境准备

第一步：安装 4G/5G、Wi-Fi 天线并插入 SIM 卡。

第二步：连接电源线和网线，任意 LAN 口连接 PC。

第三步：设置 PC 与路由器设备 IP 处于同一网段。

设备 LAN 口默认开启 DHCP Server 功能，PC 和路由器需处于同一地址段。PC 侧需将 IP 地址配置为 192.168.2.2~192.168.2.254 中的任意地址，路由器设置为 192.168.2.1，子网掩码为 255.255.255.0，DNS 配置为 8.8.8.8/运营商 DNS 服务器地址。

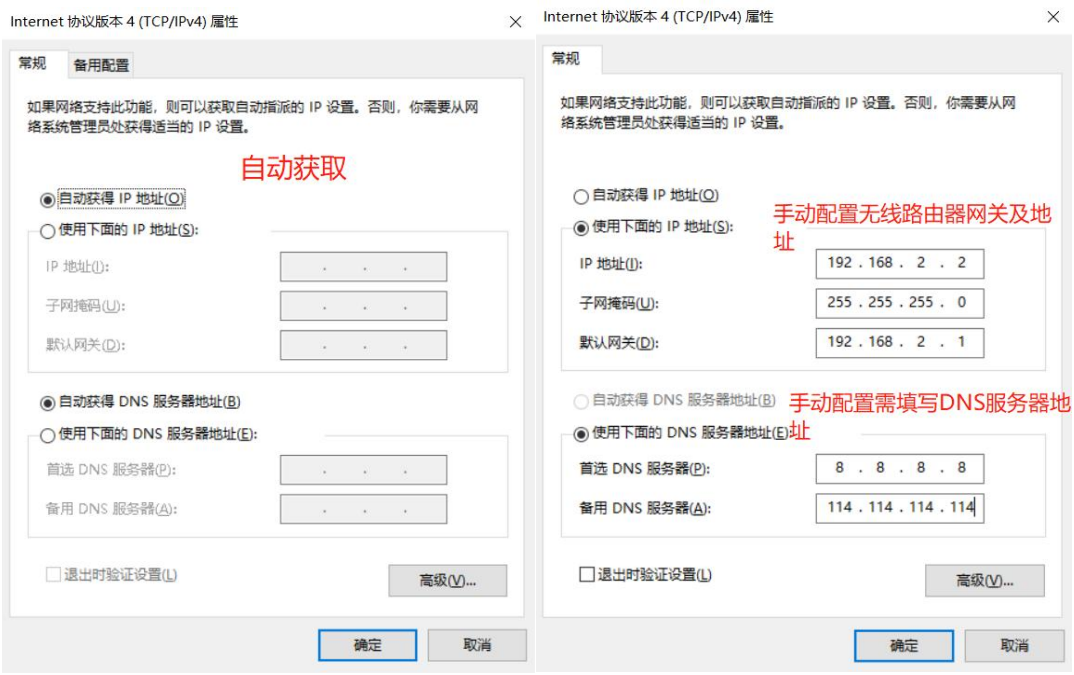


图 4-1-a/b 客户端动态获取/手动配置示意图

第四步：在浏览器地址栏中输入设备默认地址 192.168.2.1，输入用户名和密码后（默认为 adm/123456），进入设备 WEB 管理界面。如果页面提示网页不安全，打开隐藏或高级，选择继续前往。

图 4-1-2 设备WEB界面登录 示意图

4.2 设备联网

ER605 支持三种接入网络方式，每种类型下又支持多种配置方式。设备默认有 WAN1、Cellular 两条不可删除的上行链路，最多支持 WAN1、WAN2、Cellular、Wi-Fi(STA)四条链路。其中 WAN2、Wi-Fi(STA) 接口需要手动添加并支持删除。

4.2.1 有线接入网络

ER605 支持 DHCP、静态 IP、PPPoE 三种有线上网方式，点击【Internet】菜单里 WAN1 接口的“编辑”按钮

图 4-2-1-a WAN1 接口编辑入口 示意图

- DHCP：设备 WAN 接口默认开启 DHCP 服务，用网线将 WAN 接口与 Internet 连接即可实现路由器接入网络。
- 静态 IP：用户可以手动配置从运营商或上行设备分配的地址，配置完成后，路由器通过指定的静态 IP 接入网络。

图 4-2-1-b 路由器静态 IP 上网 示意图

- PPPoE：用户可以配置宽带拨号，配置完成后，路由器通过宽带拨号接入网络。

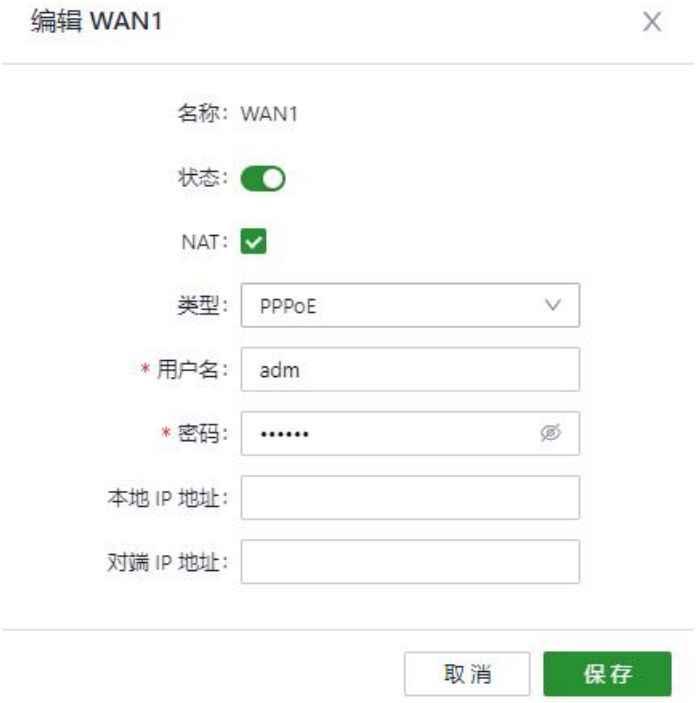


图 4-2-1-c 路由器 PPPoE 上网 示意图

对于需要用到第二条 WAN 接口的用户，可以点击【Internet】菜单里的“添加”按钮，添加 WAN2 接口，WAN2 接口支持配置的功能与 WAN1 接口相同。

图 4-2-1-d 路由器 PPPoE 上网 示意图

注意事项:

- 添加 WAN2 接口后，原 LAN1 接口角色将切换成 WAN2
- 删除 WAN2 接口后，WAN2 接口角色将会切换回 LAN1
- 删除 WAN2 后，与 WAN2 接口相关的静态路由、入站/出站规则、端口转发、策略路由、流量整形都将被删除。

4.2.2 蜂窝接入网络

通常情况下，ER605 按照说明，安装 SIM 卡、Wi-Fi 天线，上电后路由器会自动拨号接入网络。当用户需要配置 APN 参数时，点击【Internet】菜单里 Cellular 接口的“编辑”按钮。

图 4-2-2-a 蜂窝接口编辑入口 示意图

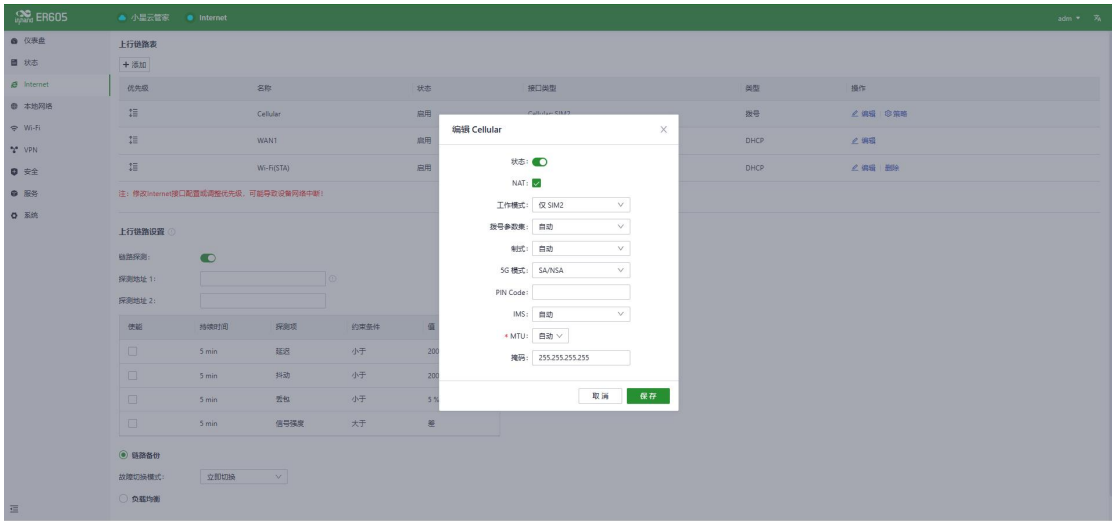


图 4-2-2-b 路由器蜂窝上网 示意图

ER605 在支持蜂窝上网的基础之上，增加了流量策略的设置功能。策略启用后，SIM 卡将在流量到达阈值后执行对应动作，流量统计将在次月起始日重置。

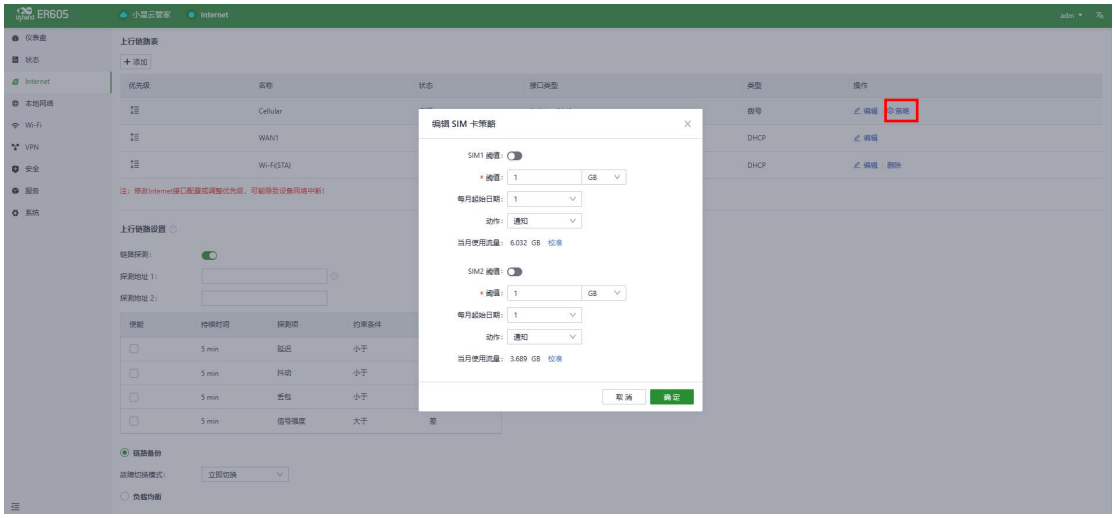


图 4-2-2-c 蜂窝策略配置 示意图

- 动作：SIM 卡流量到达阈值后触发的动作。
  - 通知：生成流量到达阈值的事件，但不会停用网络。
  - 仅保留云管理：生成流量到达阈值的事件，只支持云端管理流量，不转发访问 Internet 的业务流量。
  - 切换 SIM：生成流量到达阈值的事件，并切换到另一张 SIM 卡拨号上网。

注意事项：

- 部分专网情况下，需要手动关闭【Internet】菜单下的链路探测功能，避免因探测不通导致蜂窝不能正常工作。
- 部分情况下，需要手动配置蜂窝接口的子网掩码，保证 ARP 正常工作。

- 插拔 SIM 卡时，必须拔掉电源，以免造成数据丢失或设备损坏。

4.2.3 Wi-Fi(STA)接入网络

ER605 支持作为客户端接入现场 AP 的网络，点击【Internet】菜单里“添加”按钮，选择 Wi-Fi(STA)，填写 SSID 名称和密码等参数。

图 4-2-3 添加 Wi-Fi(STA)接口 示意图

注意事项：

- Wi-Fi(STA)添加后，ER605 在 Wi-Fi 功能中相同频段的 SSID 将被禁用且状态不可修改。
- Wi-Fi(STA)删除后，ER605 在 Wi-Fi 功能中相同频段的 SSID 状态可以修改
- Wi-Fi(STA)删除后，与 Wi-Fi(STA)接口相关的静态路由、入站/出站规则、端口转发、策略路由、流量整形都将被删除。

5 仪表盘

在左侧菜单中点击“仪表盘”，进入仪表盘界面查看设备的基本信息、接口状态、流量统计、蜂窝信号及 Wi-Fi 连接数等信息。

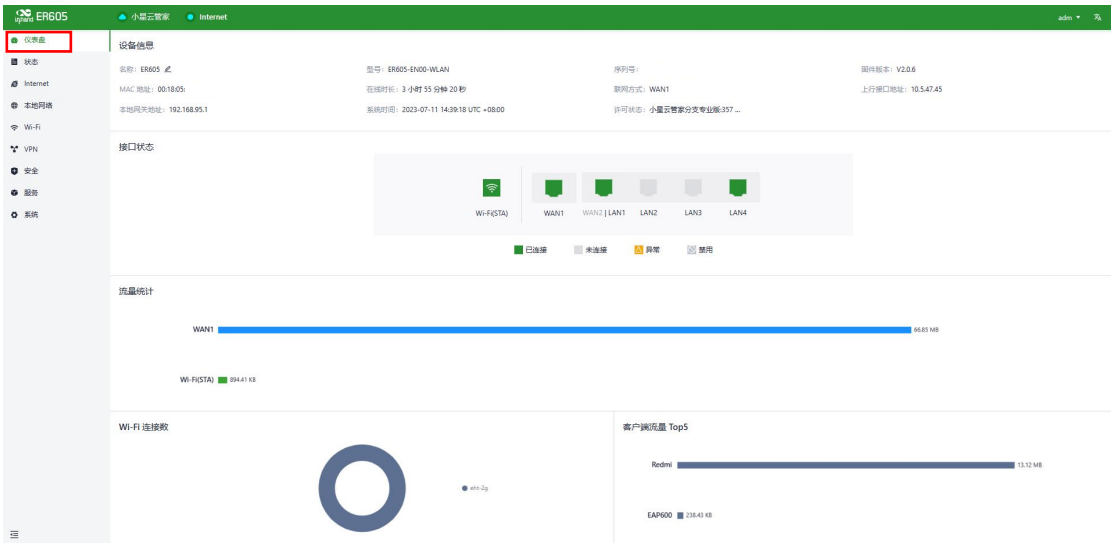


图 5 仪表盘示意图

5.1 设备信息

用户在仪表盘最上方可以查看设备基础信息。其中联网方式与上行接口地址将显示实际工作的链路及接口地址。

图 5-1 设备信息 示意图

5.2 接口状态

接口状态可以直观查看各接口的工作状态，点击“接口图标”，可以查看各接口的详细信息。

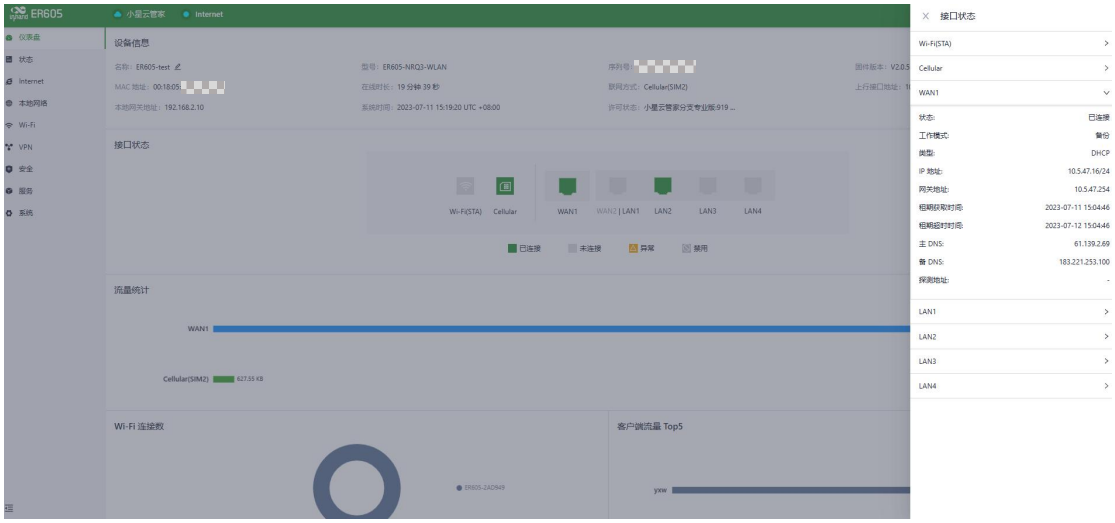


图 5-2 接口状态 示意图

5.3 流量统计

用户可在流量统计处查看路由器上电以来各上行接口流量的使用情况。流量统计会在设备重启之后重置，如果需要查看历史流量，可以在小星云管家对应设备的详情页面进行查看。

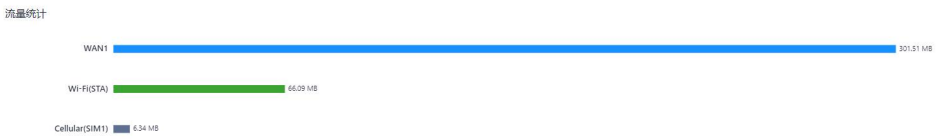


图 5-3 流量统计 示意图

5.4 Wi-Fi 连接数

通过此功能，用户可以查看 ER605 启用的 SSID 个数以及对应 SSID 下连接的客户端数量。

图 5-4 Wi-Fi 连接数 示意图

5.5 客户端流量 Top5

通过此功能，用户可以查看当前接入路由器的客户端流量使用排名。最多显示 5 条记录，当客户端断开连接后，统计将会清除。

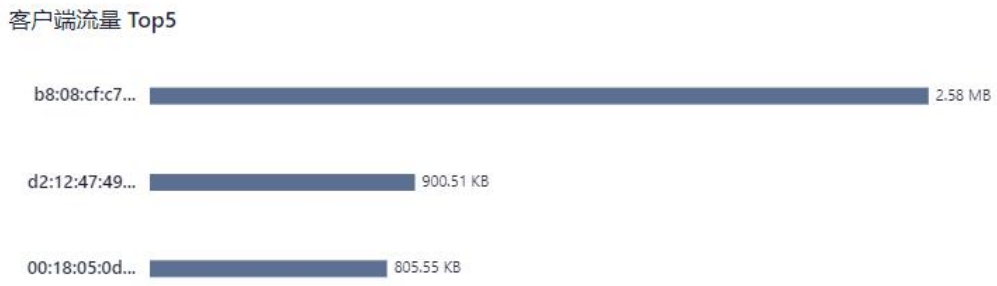


图 5-5 客户端流量 Top5 示意图

6 状态

单击左侧菜单中的【状态】进入状态界面，查看设备的上行链路、蜂窝信号、客户端、VPN、事件、日志等信息。

6.1 链路监控

在此功能下，用户可以查看各上行链路的健康状态以及各接口的吞吐率、延迟、丢包、信号强度等信息。

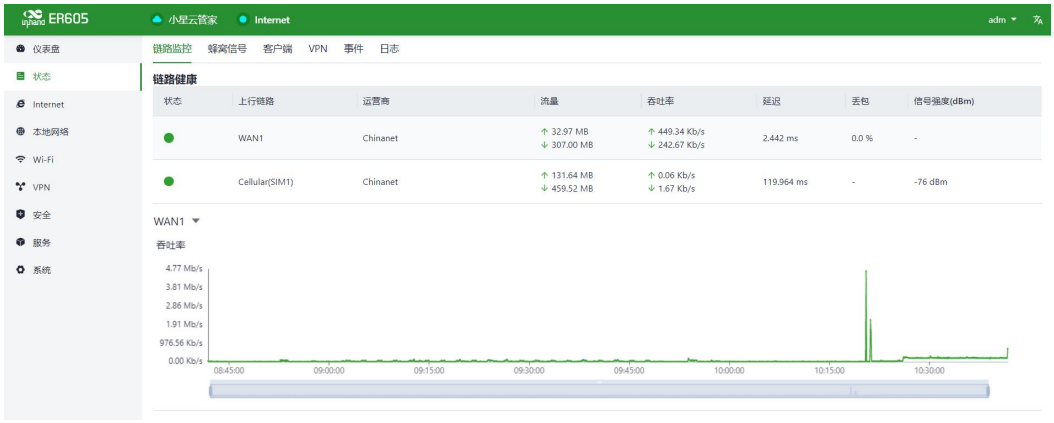


图 6-1 链路监控 示意图

6.2 蜂窝信号

在此功能下，用户可以查看蜂窝接口下 SIM 卡信号强度以及 RSSI、SINR、RSRP 等参数。

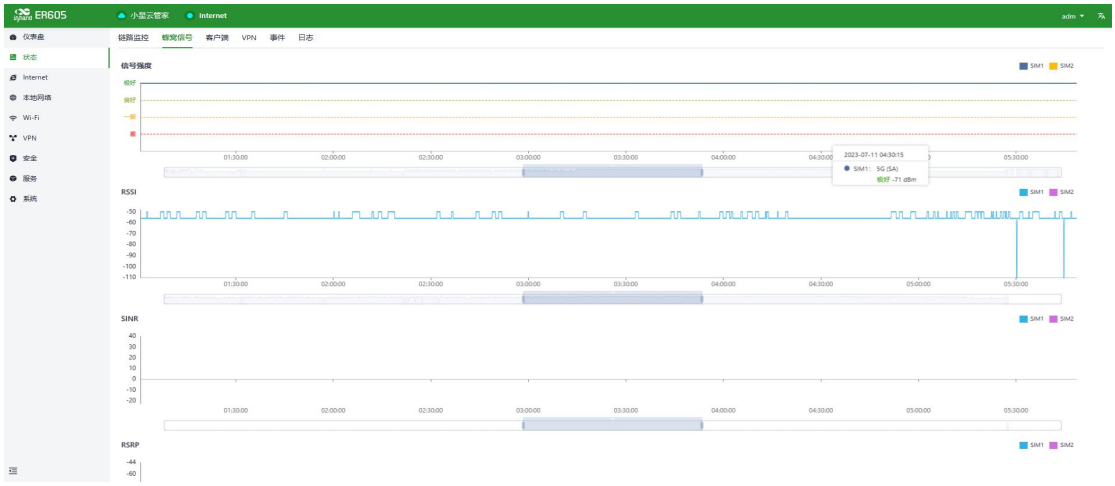


图 6-2 信号强度 示意图

6.3 客户端

在此功能下，用户可以查看连接到路由器的客户端详细信息，如名称、地址、MAC 地址、VLAN、连接的子网、流量使用、在线时长等信息。

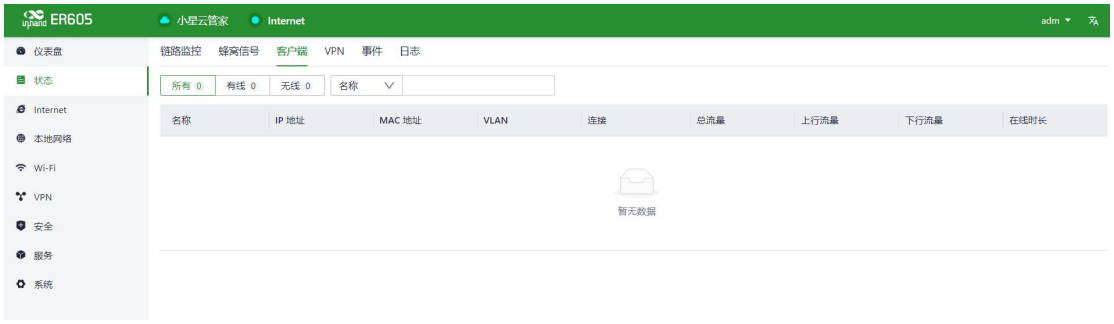


图 6-3 客户端 示意图

6.4 VPN

在此功能下，用户可以查看 IPSec VPN、L2TP VPN 的状态、名称、流量、最近一次连接时长等信息。

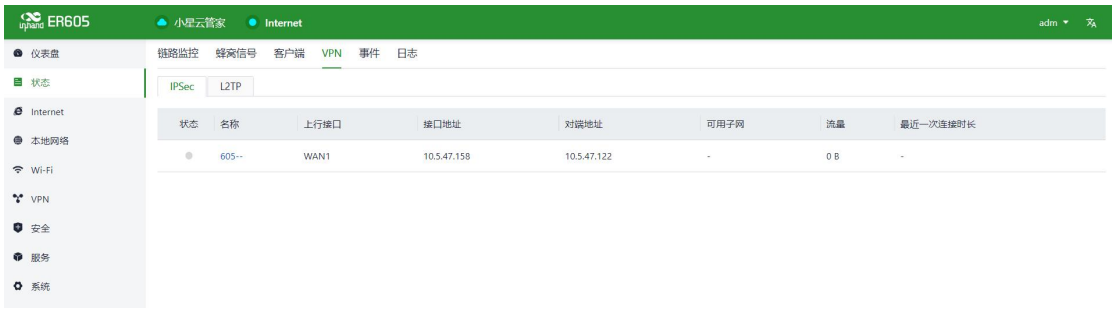


图 6-4 VPN 示意图

6.5 事件

在此功能下，用户可以查看设备运行的事件信息，帮助用户了解设备运行的状态。

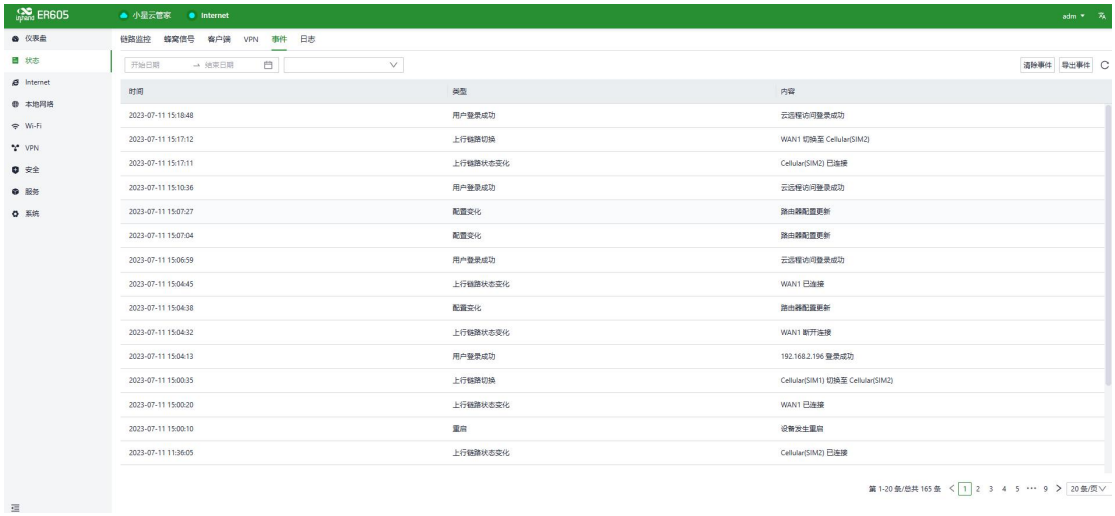


图 6-5 事件 示意图

当前支持事件类型：

- 用户登录成功/失败
- 配置变化
- 最近 5 分钟 CPU 利用率过高
- 最近 5 分钟内存利用率过高
- 蜂窝流量到达阈值
- VPN 状态变化
- 上行链路状态变化
- 上行链路切换
- WAN2/LAN1 切换
- 重启
- 升级

6.6 日志

此功能可查看设备系统运行的日志信息，当设备出现故障时，技术人员可根据系统日志进行问题排查，日志支持下载、清除操作。

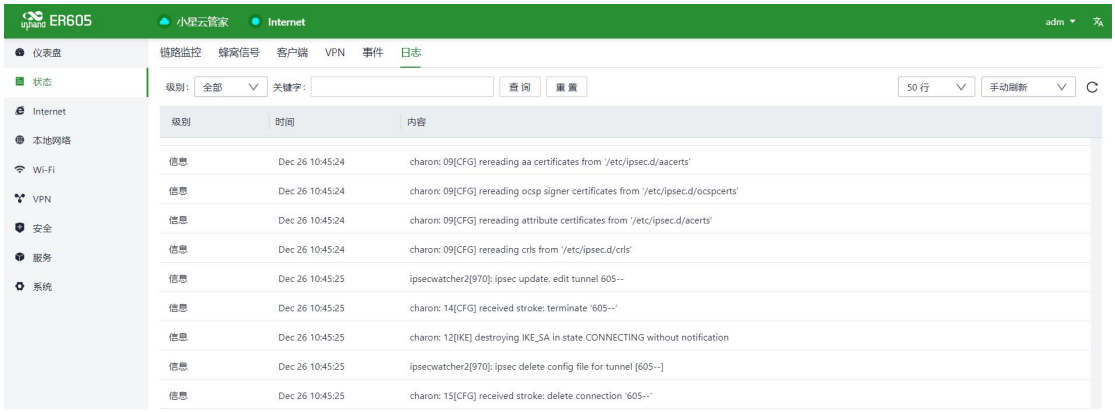


图 6-6 事件 示意图

- 下载日志：下载设备的运行日志。
- 下载诊断日志：诊断日志包含系统运行日志、设备信息、设备配置等。
- 清除日志：清除设备的运行日志。

7 Internet

在 Internet 模块下，用户可以配置各上行接口参数并设置工作方式。

注意事项：

- 对 Internet 菜单的修改可能导致设备联网中断，请谨慎操作！

7.1 上行链路表

在上行链路表中，用户可以编辑 WAN1、Cellular 接口，添加/编辑/删除 WAN2、Wi-Fi(STA）接口，详见 《4.2 设备联网》 。支持拖动“优先级”图标调整各接口的优先级。

图 7-1 上行链路表 示意图

7.2 上行链路设置

用户可在此设置链路探测相关的配置以及配置上行接口。

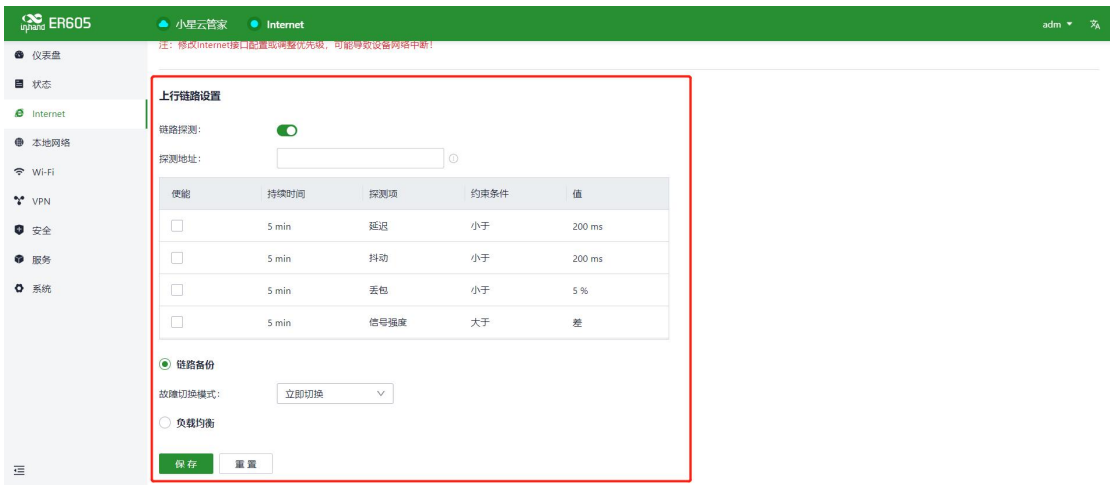


图 7-2 上行链路设置 示意图

- 链路探测开关：设备默认开启链路探测功能，部分无法与外网通信的专网环境下使用需要手动关闭链路探测功能。当链路探测功能关闭后，用户无法在【状态】菜单下查看各上行接口的延迟、抖动、丢包、信号强度图表。
- 当链路探测地址为空时，默认探测各接口获取的 DNS 地址。填写探测地址后，所有上行接口只会探测此地址。
- 当路由器处于链路备份模式时，用户可自定义探测参数，设备将根据使能的探测项进行链路切换。未使能探测项时，上行链路切换仅根据优先级和链路连通性触发切换。
- 当设备处于负载均衡模式时，所有可以正常工作的链路都会逐流转发。

8 本地网络

在此功能下，用户可以自定本地子网，添加后的子网可指定给通过 LAN 接口或 SSID 接入的客户端使用。

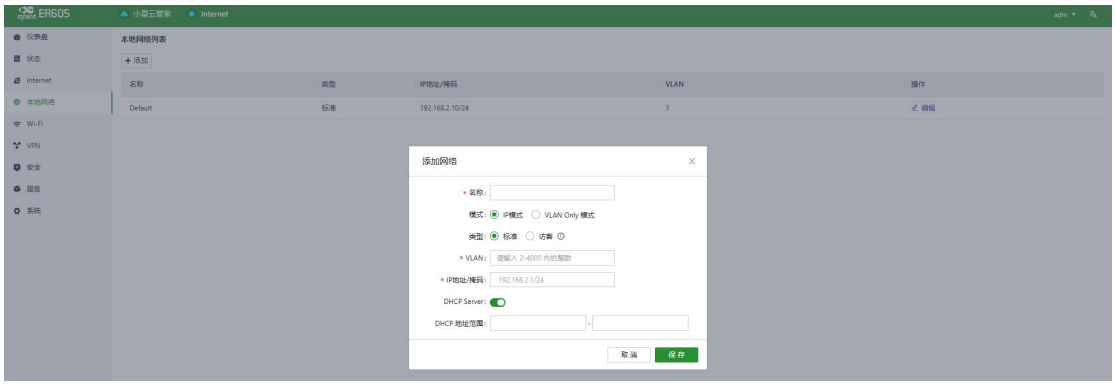


图 8-1 本地网络 示意图

点击“添加/编辑”按钮，添加新的本地网络或对已有本地网络进行编辑。

- 默认的本地网络不可删除且仅支持修改 IP 地址/掩码和 DHCP Server 配置。
- 已添加的本地网络模式不支持修改。
- VLAN Only 模式用于二层透传，无需配置 IP 地址/掩码、DHCP Server。

9 Wi-Fi

ER605 可以作为 AP 提供多 SSID 的无线网络接入功能，用户可以自定义不同 SSID 用途和配置。

图 9-1 Wi-Fi 列表 示意图

点击“添加/编辑”按钮，可添加新的 SSID 或对已有 SSID 进行编辑。

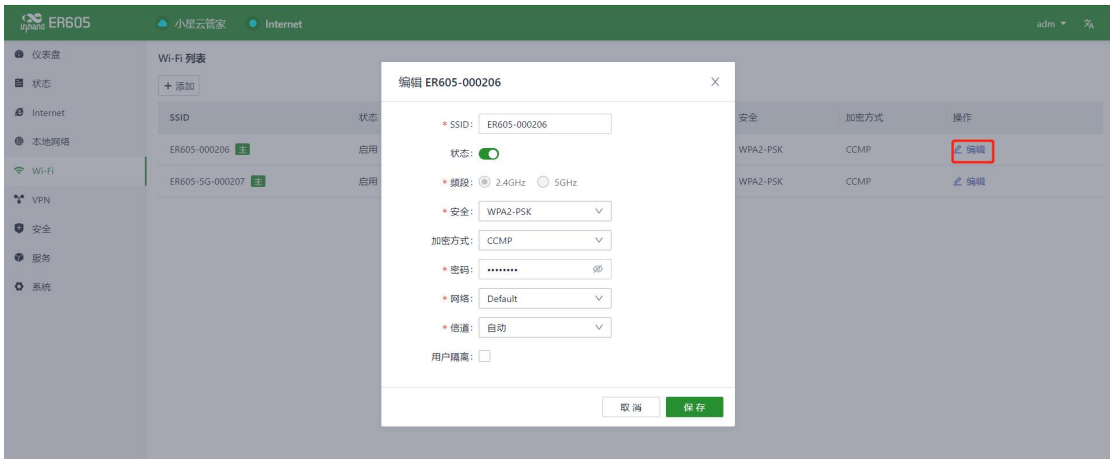


图 9-2 SSID 编辑 示意图

- 设备默认有 2.4G、5G 两个主 SSID，主 SSID 频段不支持修改且不支持删除。
- 已添加的 SSID 频段不支持修改，信道将自动与所属主 SSID 的信道保持一致。
- 若用户在【Internet】菜单创建 Wi-Fi(STA）接口，与 Wi-Fi(STA）接口相同频段的 SSID 都无法启用直到 Wi-Fi(STA）接口被删除。

10 VPN

VPN（虚拟专用网络）的功能是：在公用网络上建立专用网络，进行加密通讯。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 可通过服务器、硬件、软件等多种方式实现。相比传统 DDN 专线或帧中继的方法，VPN 提供了一种更加安全，方便的远程访问方案。

10.1 IPSec VPN

IPSec VPN 是 IETF 制定的一组开放的网络安全协议，在 IP 层通过数据来源认证、数据加密、数据完整性和抗重放功能来保证通信双方 Internet 上传输数据的安全性。减少泄漏和被窃听的风险，保证数据的完整性和机密性，保障了用户业务传输的安全。

点击【VPN】菜单里 IPSec VPN 页面下的“添加”按钮，添加 IPSec VPN。

图 10-1-1 IPSec VPN 添加入口 示意图

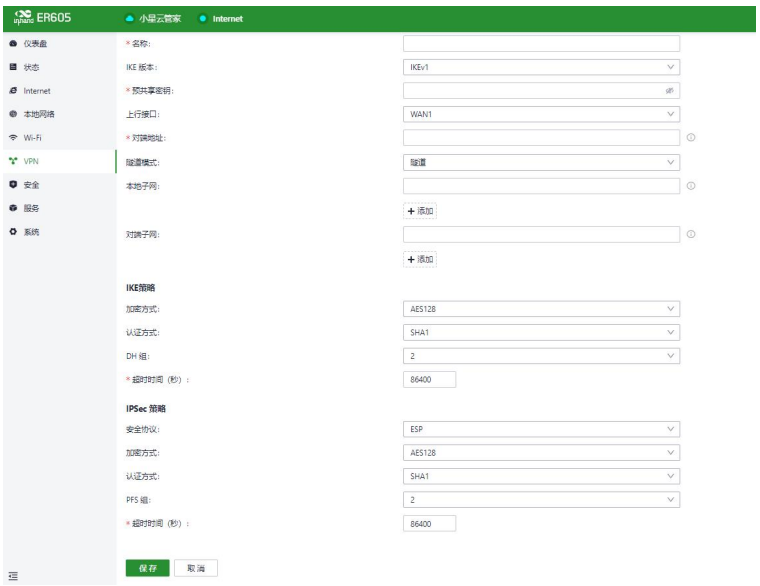


图 10-1-2 IPSec VPN 添加 示意图

两端配置完成后，隧道即可建立。用户可以在【状态>VPN】菜单中查看隧道建立状态。

下方仅列出部分必填项的说明。

- 名称：路由器创建的 IPSec VPN 名称标识，主要用于本地管理。
- IKE 版本：设置 IKE 协议使用的版本号，支持 IKEv1 和 IKEv2。
- 预共享密钥：在 IKE 协商的两端设备需要配置相同的认证密钥。
- Internet 接口：本地建立 IPSec VPN 使用的上行接口。
- 隧道模式：设置 IPSec 对 IP 报文的封装模式，支持隧道模式和传输模式。
- 对端地址：与 ER605 建立隧道的对端通信地址。

注意事项:

ER 系列设备在用 IPSec VPN 建立连接时，默认以使用公网地址的设备作为服务器，IPSec 服务器侧的对端地址需要配置为 0.0.0.0，IPSec 客户端侧的对端地址填写 IPSec 服务器侧的公网地址。

- 本地子网：填写需要通过 ER605 IPSec VPN 隧道通信的网段地址。
- 对端子网：填写隧道另一端需要通过 IPSec VPN 隧道通信的网段地址。
- IKE 策略：支持设置 IKE 协议的配置。
  - 加密方式：设置 IKE 使用的加密算法。
  - 认证方式：设置 IKE 使用的认证算法。
  - DH 组：设置 IKE 阶段密钥协商使用的 DH 交换参数。
  - 超时时间：设置 IKE SA 存活时间，默认 86400 秒。
- IPSec 策略：支持设置 IPSec 参数配置。
  - 安全协议：设置 ERP 协议使用的安全协议。
  - 加密方式：设置 ESP 协议的加密算法
  - 认证方式：设置 ESP 协议使用的认证算法。
  - PFS 组：IPSec 使用安全策略发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性参数。
  - 超时时间：设置 IPSec SA 老化时间，默认 86400 秒。

10.2 L2TP VPN

二层隧道协议 L2TP(Layer 2 Tunneling Protocol)是 VPDN 隧道协议的一种，通过拨号网络（PSTN/ISDN），基于点到点协议 PPP（Point-to-Point Protocol）的协商，建立远程用户到企业总部的隧道，使远程用户可以接入企业内联网。

10.2.1 客户端

ER605 可以作为 L2TP 客户端和位于远端的 L2TP 服务器建立隧道。点击【L2TP VPN-〉客户端】页面的“添加”按钮，添加 L2TP 客户端。

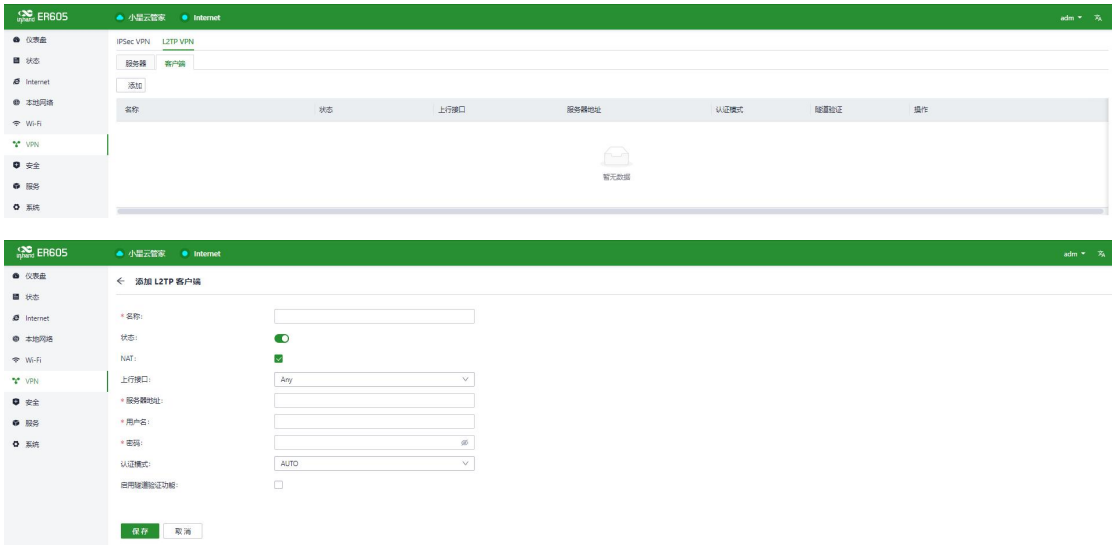


图 10-2-1-a/b L2TP 客户端添加 示意图

- 名称：L2TP 客户端的名称，用于本地标识。
- 状态：L2TP 客户端隧道开启/禁用开关。
- NAT：L2TP 客户端转发时的 NAT 功能开关。
- 上行接口：L2TP 客户端与服务器进行通信的上行接口。
- 服务器地址：对端 L2TP 服务器的通信地址。
- 用户名/密码：两端进行 L2TP 协商时需要配置相同的用户名/密码
- 认证模式：设置 L2TP 认证模式。
- 启用隧道验证功能：启用后，两端用于隧道验证的用户名/密码需要配置相同。

10.2.2 服务器

L2TP 服务器常常部署于企业总部，用于对移动办公或分支机构提供远程访问的服务器。点击【L2TP VPN > 服务器】 进入 L2TP 服务器的编辑页面。

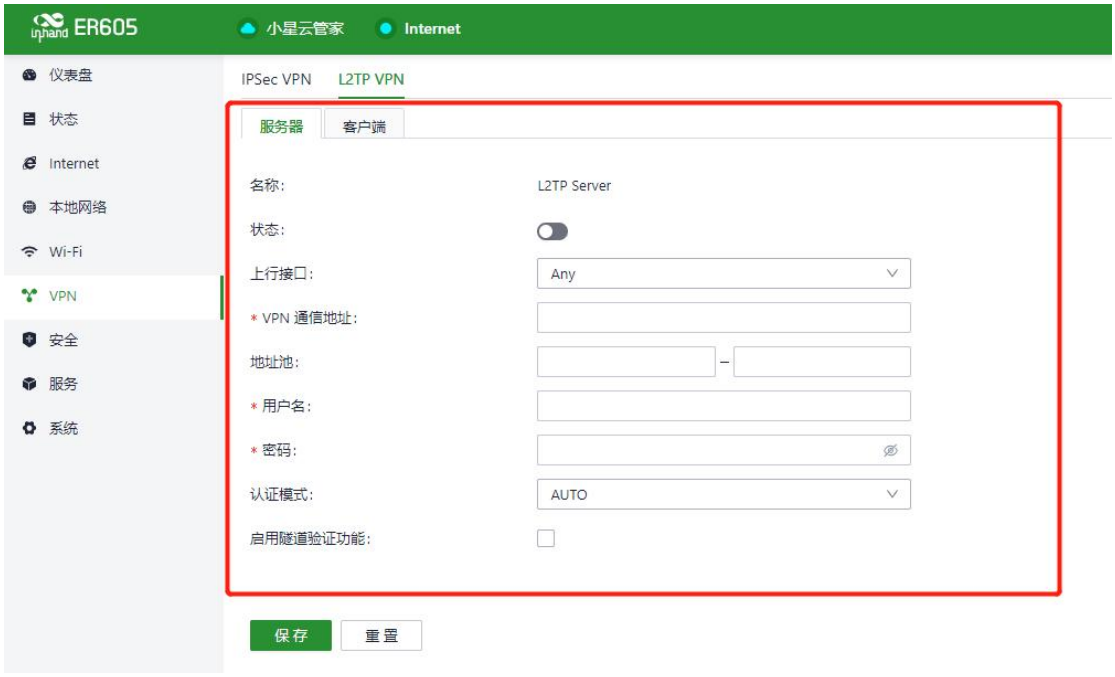


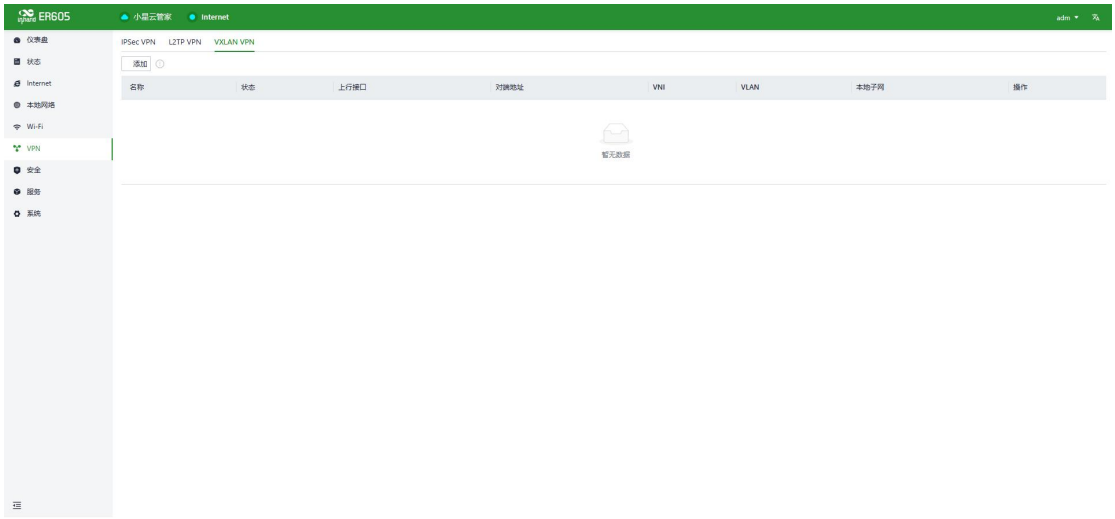
图 10-2-2 L2TP 服务器配置 示意图

- 名称：L2TP 服务器名称，不支持修改。
- 状态：L2TP 服务器的功能开关，默认禁用。
- 上行接口：L2TP 作为服务器时使用的上行接口。
- VPN 通信地址：作为 L2TP 客户端的网关地址，可为 L2TP 客户端设备分配地址池内的地址。
- 地址池：L2TP 客户端接入时用于通信的地址池。
- 用户名/密码：两端进行 L2TP 协商时需要配置相同的用户名/密码
- 认证模式：设置 L2TP 认证模式。
- 启用隧道验证功能：启用后，两端用于隧道验证的用户名/密码需要配置相同。

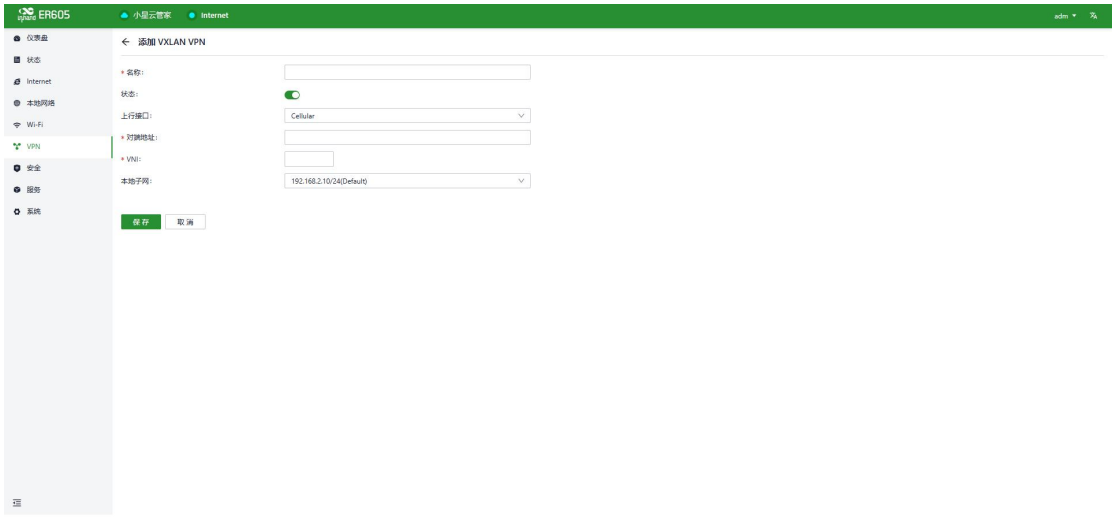
10.3 VXLAN VPN

VXLN VPN 能在源网络设备和目的网络设备之间的 IP 网络上创建逻辑隧道，经过特定封装后通过该隧道转发用户端数据包。

选择 VPN > VXLAN VPN，然后单击添加以添加【VXLAN VPN】。



10-3-1 新增 VXLAN VPN 配置入口



10-3-2 配置 VXLAN VPN

- 名称：设置该 VXLAN VPN 网路的名称。
- 对端地址：设置需要与该设备组建 VXLAN VPN 网络的对端设备的 IP 地址。
- VNI：VXLAN 的网络标识符，一个 VNI 就代表一个租户。

11 安全

在【安全】菜单下，用户可以设置防火墙、策略路由、流量整形相关的高级功能。

11.1 防火墙

防火墙当前包括：入站规则/出站规则、端口转发

11.1.1 入站规则/出站规则

用户可通过此功能实现基于接口的流量进出控制，例如：用户受到基于某 IP 地址为源的大量攻击行为，就可以通过防火墙入站规则限制此 IP 地址的流量数据。

IT 人员想要限制部分用户访问外网时，可以通过防火墙出站规则限制这个用户流量访问外网。入站规则和出站规则仅默认规则不同，可配置的内容相同，下方以添加入站规则为例：

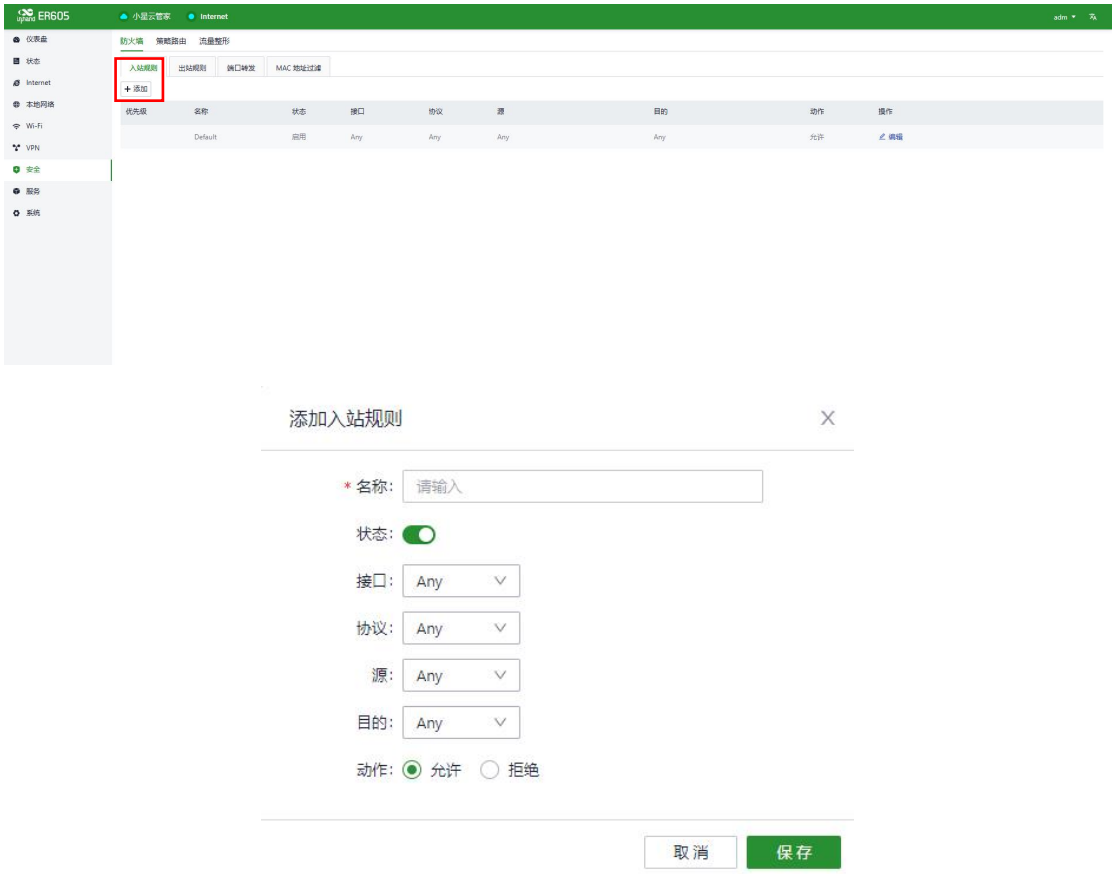


图 11-1-1-a/b 添加入站规则 示意图

- 名称：入站规则的名称，用于本地标识。
- 状态：规则的功能开关
- 接口：对于出站规则，指流量流出路由器的上行接口。对于入站规则，指流量进入路由器的上行接口。
- 协议：匹配流量的协议类型，支持 Any、TCP、UDP、ICMP、自定义
- 源：匹配流量的源地址，支持自定义，默认 Any。
- 目的：匹配流量的目的地址，支持自定义，默认 Any。
- 动作：入站规则/出站规则的对匹配流量的动作，支持允许和拒绝。
- 入站规则：外部网络访问路由器的流量管理规则，默认拒绝所有。
- 出站规则：通过路由器访问外部的流量管理规则，默认全部放行。
- 支持调整入站规则/出站规则的优先级。

11.1.2 端口转发

配置端口转发规则后，当外部流量访问路由器的特定端口时，设备会将数据转发至内部客户端的相应端口上，使部署在设备内的服务对外网也可用。此功能可将不同端口转发到不同的内部 IP 以及端口，实现使用同一公网 IP 地址访问多个服务器。例，当用户需要从外部访问内部 192.168.2.10 客户端的 1024 端口服务时，将此客户端的端口映射到 WAN1 接口下的 1024 端口，外部网络只需在浏览器输入 “https://WAN1 地址：1024”即可访问目标设备数据。

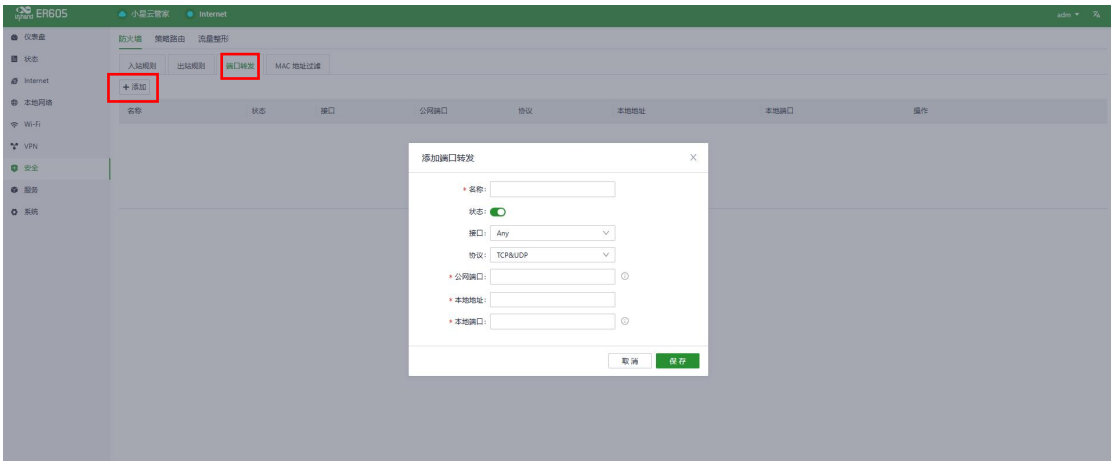


图 11-1-2 添加端口转发 示意图

- 名称：端口转发规则的名称，用于本地标识。
- 状态：端口转发规则的功能开关。
- 接口：对内部客户端提供映射功能的上行接口，上行接口需要公网地址支持。
- 协议：端口映射流量的协议类型，支持 TCP、UDP、TCP&UDP。
- 公网端口：对内部客户端提供映射功能的上行接口的端口号，需要与本地端口输入范围保持一致。
- 本地地址：外部网络需要访问的位于路由器下的目标设备地址。
- 本地端口：外部网络需要访问的目标设备的端口，需要与公网端口输入范围保持一致。

11.1.3 MAC 地址过滤

MAC 地址过滤是指禁止（允许）MAC 地址列表中的计算机上网，即通过路由器上的 MAC 地址控制局域网内计算机的上网请求。

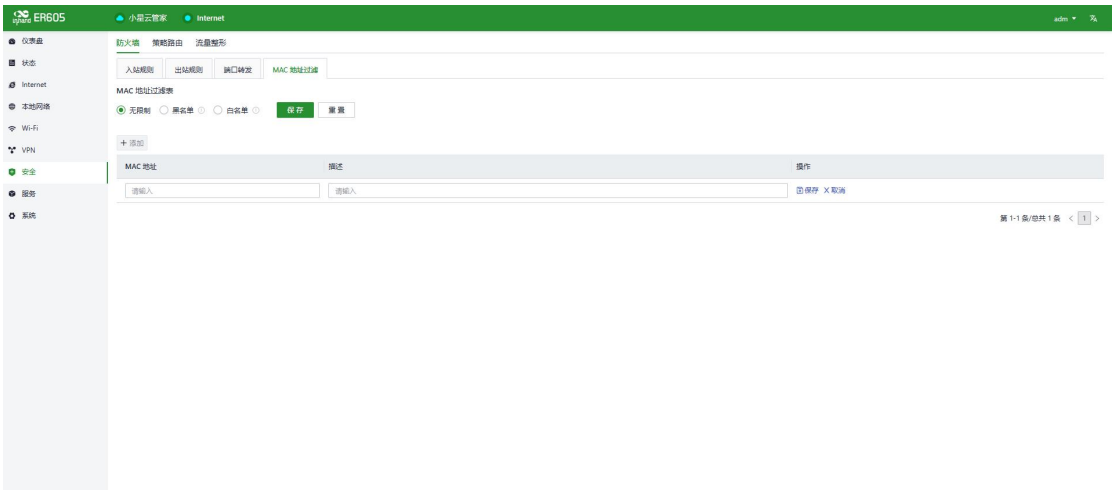


图 11-1-2　添加 MAC 地址过滤规则 示意图

您可以在列表中创建多个 MAC 地址，添加地址描述，并在列表中设置允许 MAC 地址访问网络（白名单），也可以禁用列表中的 MAC 地址访问网络（黑名单）。

11.2　策略路由

策略路由可以帮助用户根据实际需求制定策略，使不同的数据流通过不同链路进行转发，增强路由选择的灵活性和可控性，提高链路的利用效率和降低企业成本。点击【安全〉策略路由】页面的“添加”按钮。

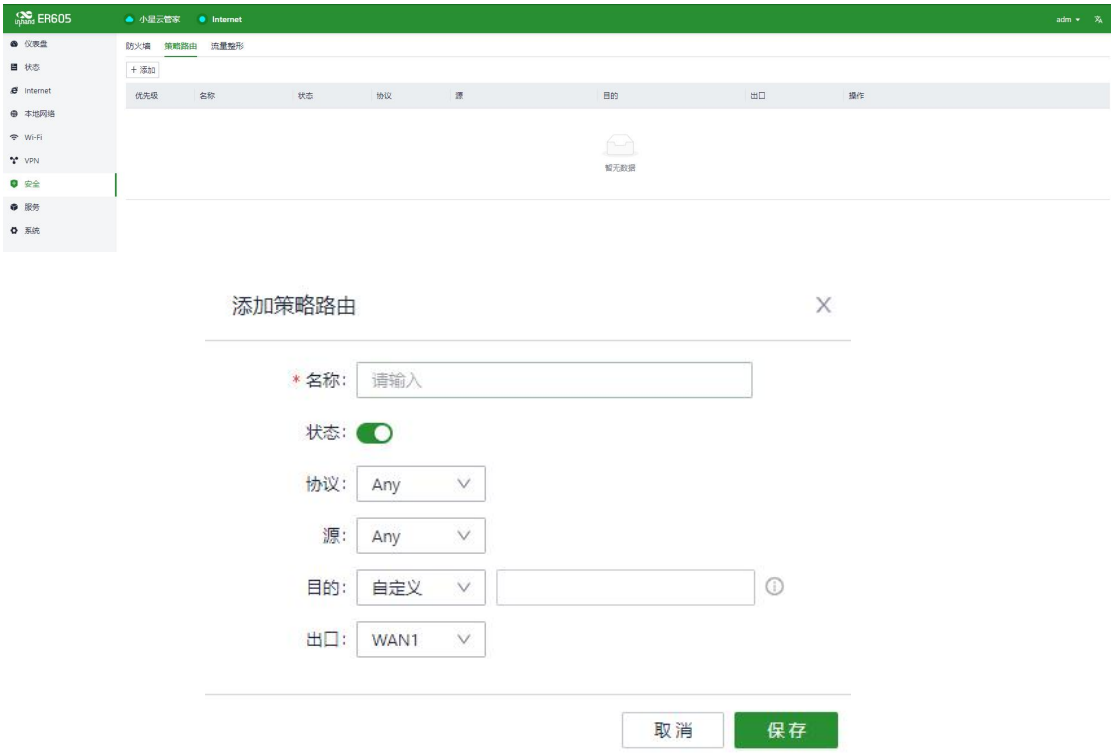


图 11-2-a/b 添加策略路由 示意图

注意事项:

- 策略路由的源地址和目的地址不能同时为 Any。

12 服务

12.1 接口管理

在此功能下，用户可以管理接口放行的本地网络以及接口的速率。

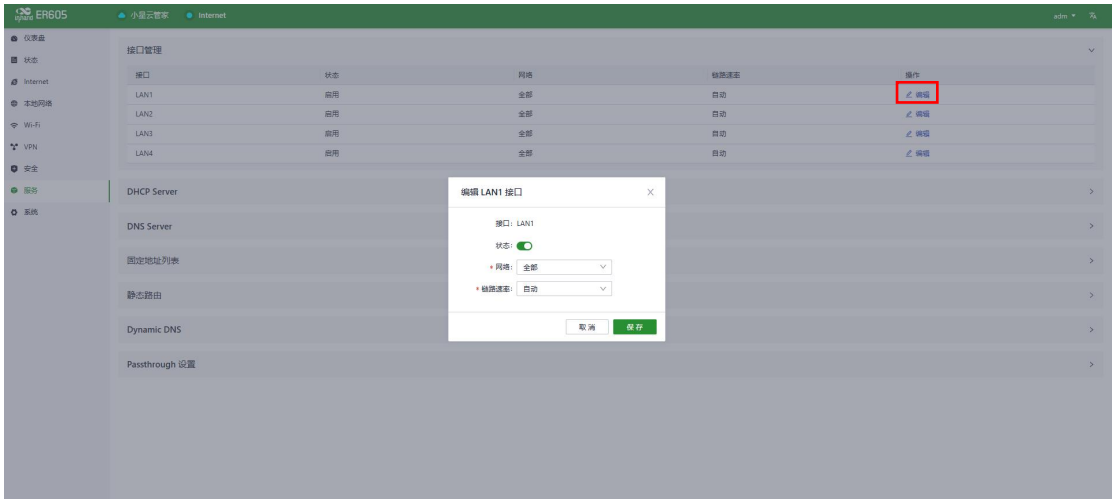


图 12-1 编辑 LAN 接口 示意图

12.2 DHCP Server

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出地址请求，服务器接到请并为客户端分配的 IP 地址，以实现 IP 地址的动态配置。

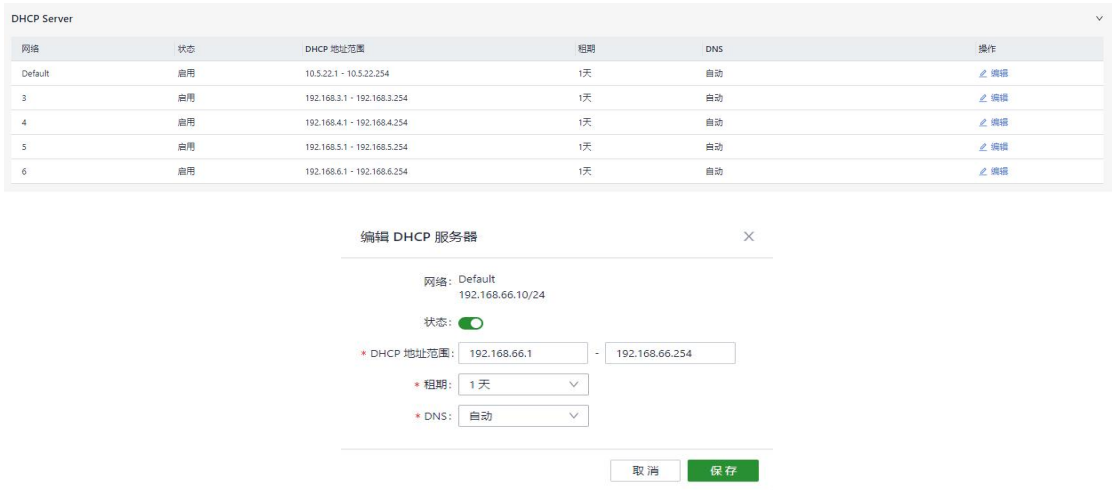
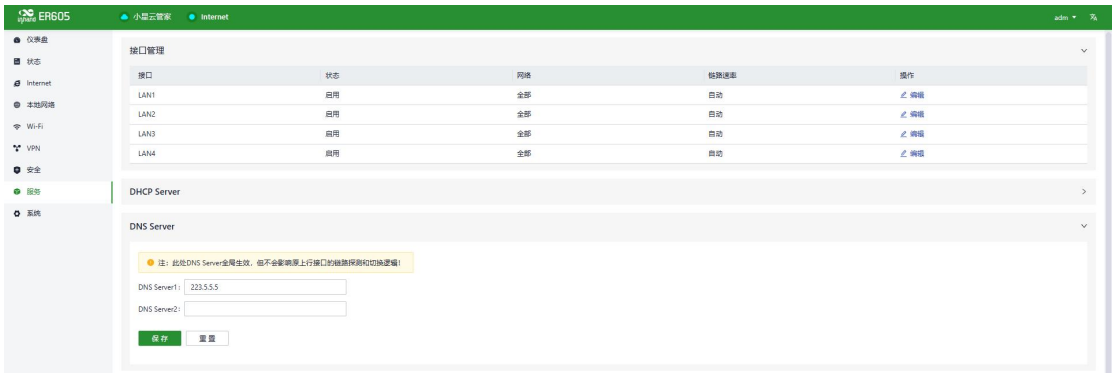


图 12-2-a/b 编辑 DHCP Server 示意图

- 设备的 DHCP 服务根据本地网络的网络信息生成，网络列表删除后，此网络的 DHCP Server 也删除。
- 本地网络对应条目需要处于 IP 模式下才有 DHCP Server 功能，VLAN Only 模式下的网络不在可选范围。

12.3 DNS Server

DNS 服务器将域名解析为 IP 地址，使用户更容易上网。



12-3 添加 DNS 服务器

12.4 固定地址列表

通过此功能可实现基于接入设备的 MAC 地址为该设备分配 IP 地址。

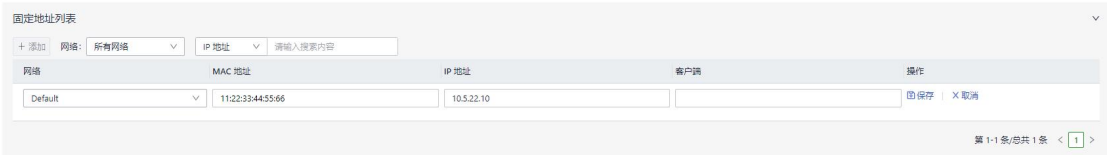


图 12-3 添加固定地址分配 示意图

- 可用于分配的地址必须在 IP 模式的本地网络的地址范围内。
- 当本地网络删除后，本地网络地址范围内的固定地址分配规则都将被删除。

12.5 静态路由

用户可自主配置静态路由，实现数据从指定的路径和接口转发。静态路由表中的内容均为用户手动创建，Internet 接口自动生成的路由不会在此表中显示。

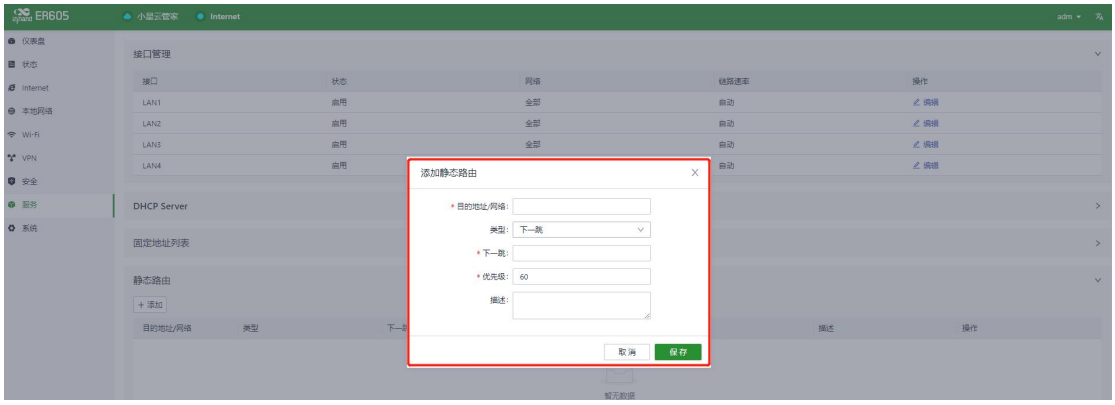
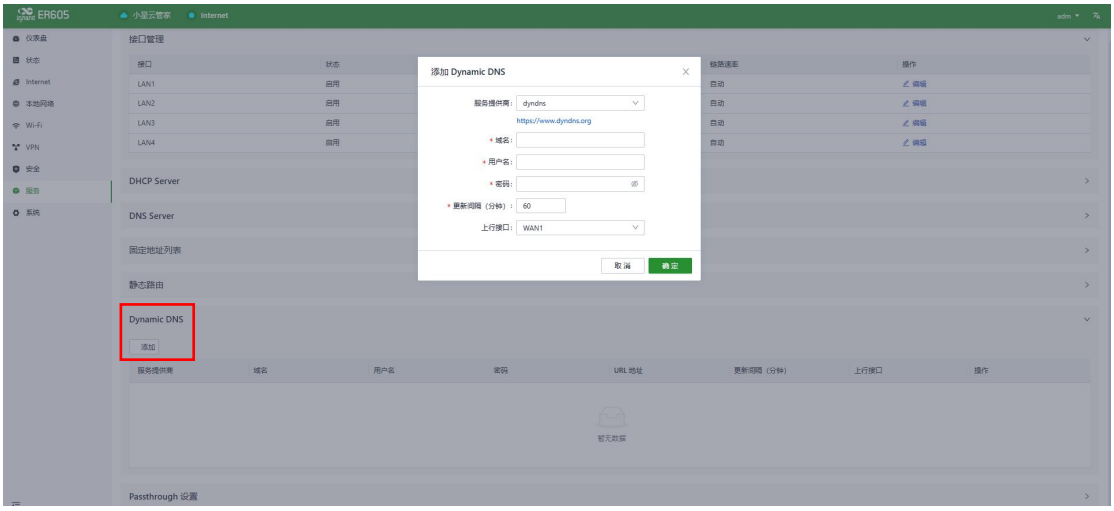


图 12-4 添加静态路由 示意图

- 相同目的地址/网络的静态路由，下一跳地址、接口或优先级不能相同。
- 当 WAN2、Wi-Fi(STA)、L2TP 客户端 VPN 删除后，使用对应接口的静态路由也将被删除。

12.6 Dynamic DNS

动态 DNS 是域名系统中自动更新名称服务器内容的一项技术，根据互联网的域名规则，域名必须遵循固定的 IP 地址。动态 DNS 为动态域提供固定的名称服务器，使外部用户能够通过及时更新连接到动态用户的 URL。



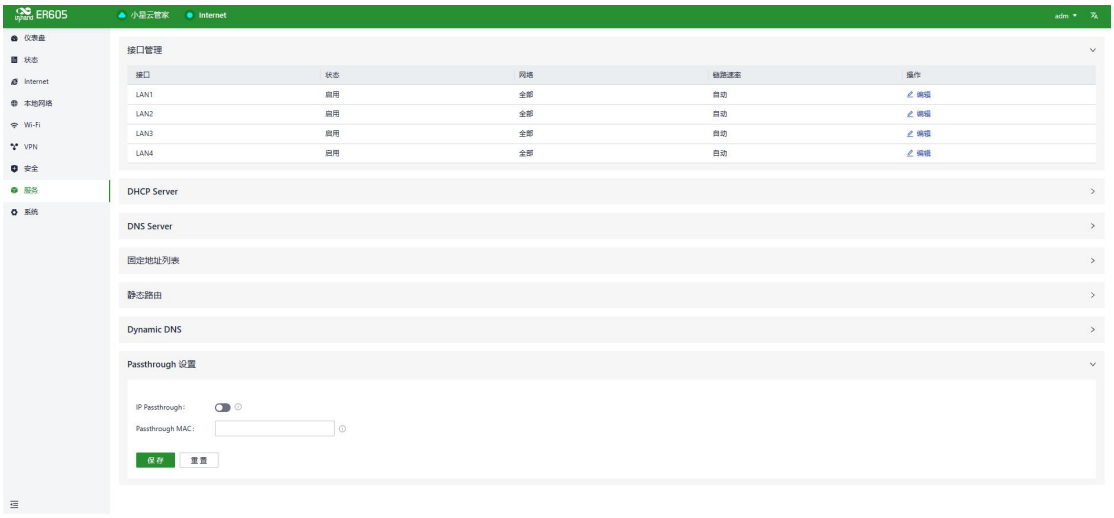
12-6 添加 Dynamic DNS 服务信息

- 服务提供商：由动态 DNS 运营商提供，您可以选择 dyndns，3322，oray，no-ip 或自定义（需要 URL）。
- 主机名：单击服务提供商下方的 URL 进行注册以获取主机名。

- 用户名：单击服务提供商下方的 URL 进行注册以获取用户名。
- 密码：用户在注册时设置的密码。

12.7 Passthrough

启用直通功能后，上行接口可以透明地传输到客户端设备。



12-7 开启 IP Passthrough 功能

Passthrough MAC：只有绑定到 MAC 的客户端才能获取直通地址。

注意：

- IP 直通模式开通后，只有一个客户端可以访问公网，禁用以下功能。

  静态路由、VPN、端口转发、基于策略的路由、SD-WAN Overlay、云连接。
- 访问客户端设备时，需要释放入站规则。
- 您仍然可以通过默认子网的 IP 地址访问路由器。

13 系统

在【系统】菜单下，用户可以完成云管理、远程访问控制、时钟、设备选项、配置管理、设备告警、工具、日志服务器等功能的设置。

13.1 adm 管理

设备的初始用户名和密码为 adm/123456，为了设备的使用安全，请修改设备的密码。点击页面右上的“adm”，在下拉菜单中点击“修改密码”进行修改。

图 13-1 修改 adm 密码 示意图

13.2 云管理

小星云管家(star.inhandcloud.cn)是映翰通针对企业网络当前面临的部署缓慢、运维困难、业务体验差的问题，打造的以用户为本的，集零接触部署、智能运维、安全

防护、良好的业务体验于一体的云平台。设备连接到云平台后，用户可通过平台对设备进行远程管理、批量配置、流量监控等操作。

可在此界面选择想要连接的云平台地址。当用户不希望使用云平台和服务时，可通过云管理功能禁止设备连接云平台。

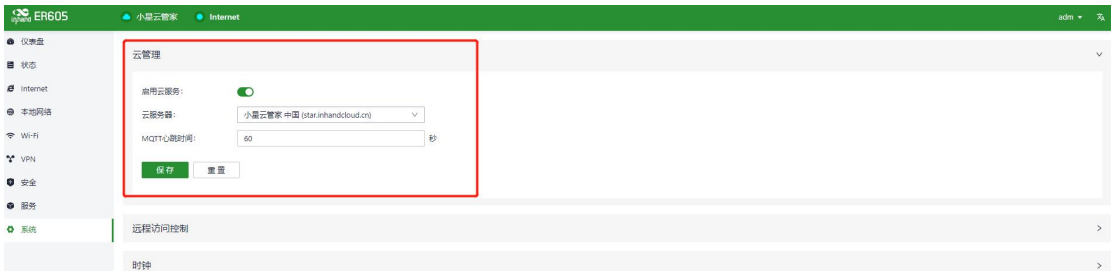


图 13-2 云管理 示意图

注意事项：

- ER605 默认联网自动接入小星云管家，若不希望使用云管理功能，请手动关闭。

13.3 远程访问控制

用户可通过此功能设置是否允许通过Internet地址从外部访问路由器的Web配置界面，支持设置访问的端口。

图 13-3 远程访问控制 示意图

- HTTPS：启用后，用户可以在浏览器输入上行接口的公网地址&端口，实现远程访问路由器的 Web 界面。
- SSH：启用后，用户可以在远程工具（如 CRT），输入设备上行接口的公网地址&端口、用户名及密码，实现远程登录路由器后台。
- Ping：启用后，上行接口地址允许外部网络发起 Ping 请求。

注意事项：

- LAN 接口不受此处配置影响。
- 防火墙规则不会限制远程访问。

13.4 时钟

在此功能下，用户可以选择时区作为设备系统时间，通过 NTP Server 与目标 NTP 服务器同步设备时间。

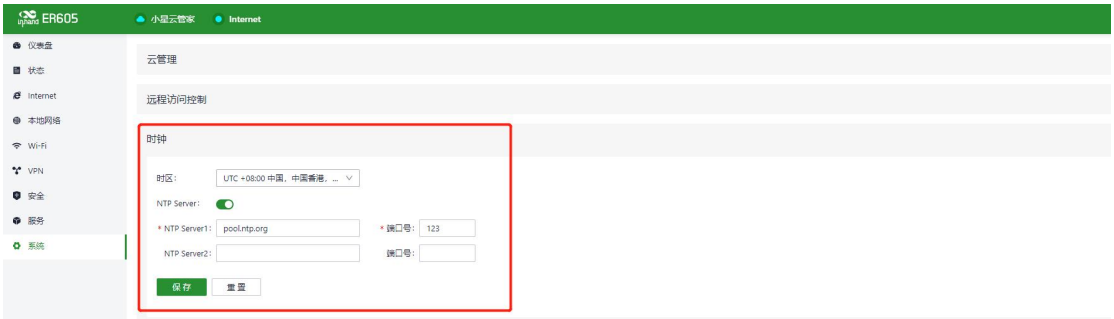


图 13-4 时钟 示意图

13.5 设备选项

在此界面中，可对设备进行重启、升级固件及恢复出厂操作。

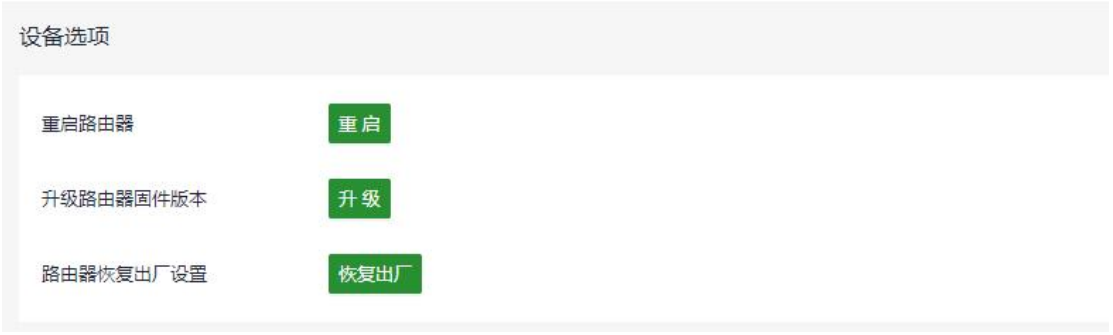


图 13-5 设备选项 示意图

注意事项：

- 本地升级固件时请确保固件从正规渠道获取，避免因为导入错误固件导致设备不可用。

- 当设备接入云平台后，由于云端配置同步机制，平台会将恢复出厂前的配置再次推到设备上，设备仅清除历史数据。

13.6 配置管理

用户可以导出设备配置存储在本地，当设备配置丢失时导入此设备以恢复配置。

图 13-6 配置管理 示意图

13.7 设备告警

当用户需要特别关注设备上可能发生的某些事件时，可勾选相应的告警事件并设置接收邮箱地址。当告警事件发生时设备会发送相应的邮件。当用户不勾选告警选项时，告警事件仍然会记录在设备本地日志中。

目前设备支持的告警事件如下：

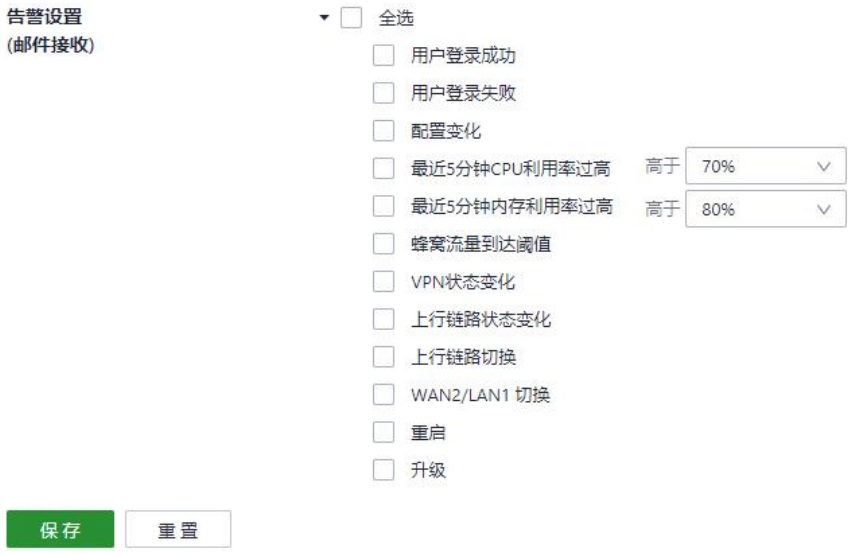


图 13-7-a 告警设置 示意图

配置发件邮箱的服务器地址、端口、用户名和密码后，设备将通过此邮箱发送告警邮件，可以通过发送测试邮件的选项检验发件邮箱的配置是否正确。

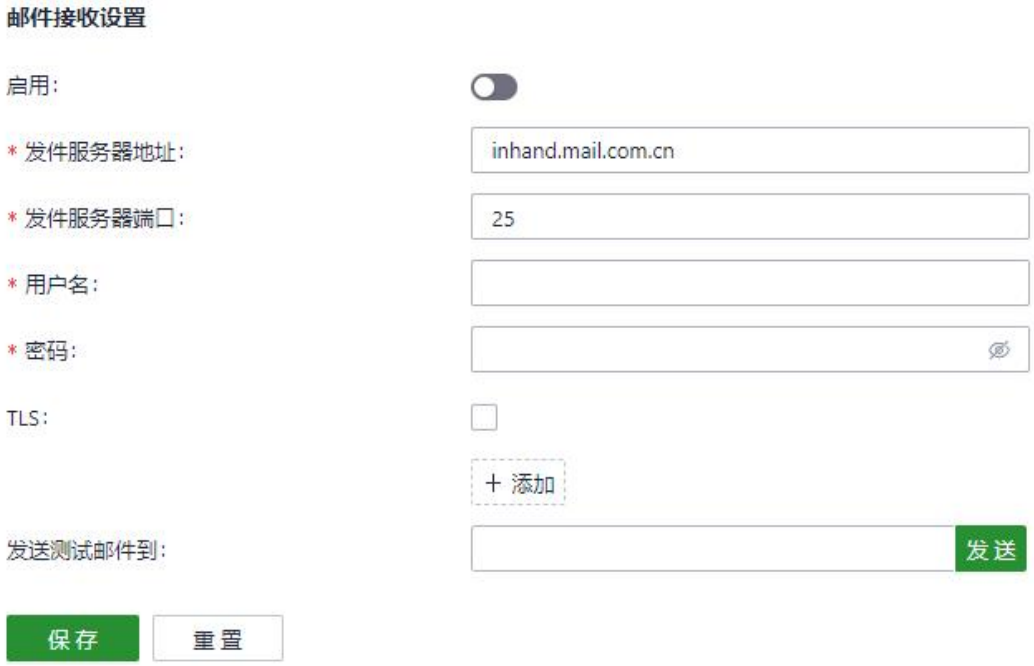
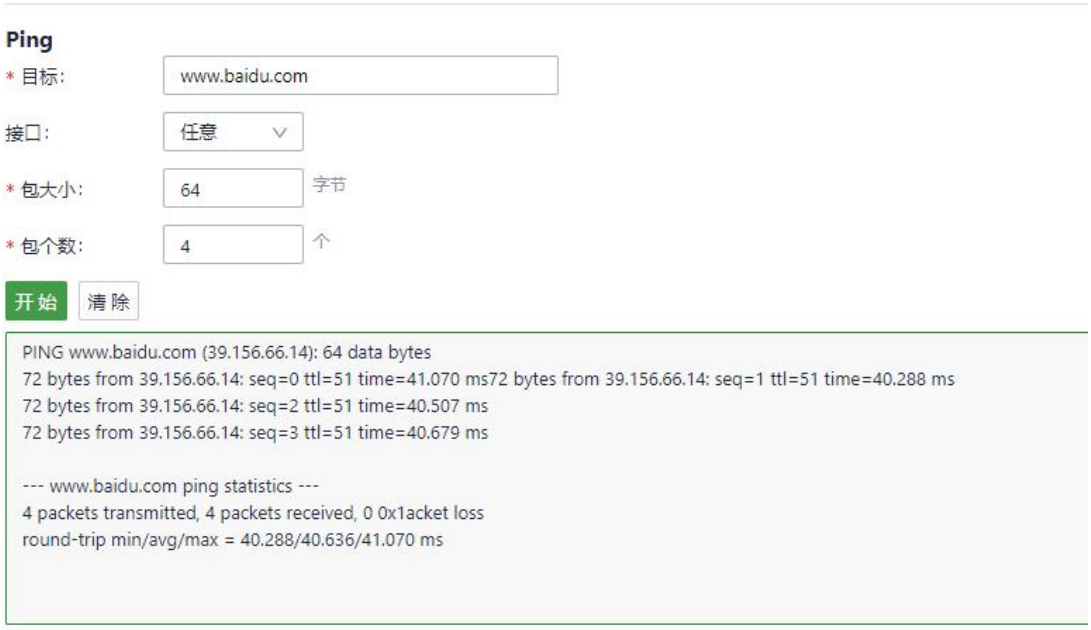


图 13-7-b 邮件接收 示意图

13.8 工具

13.8.1 Ping

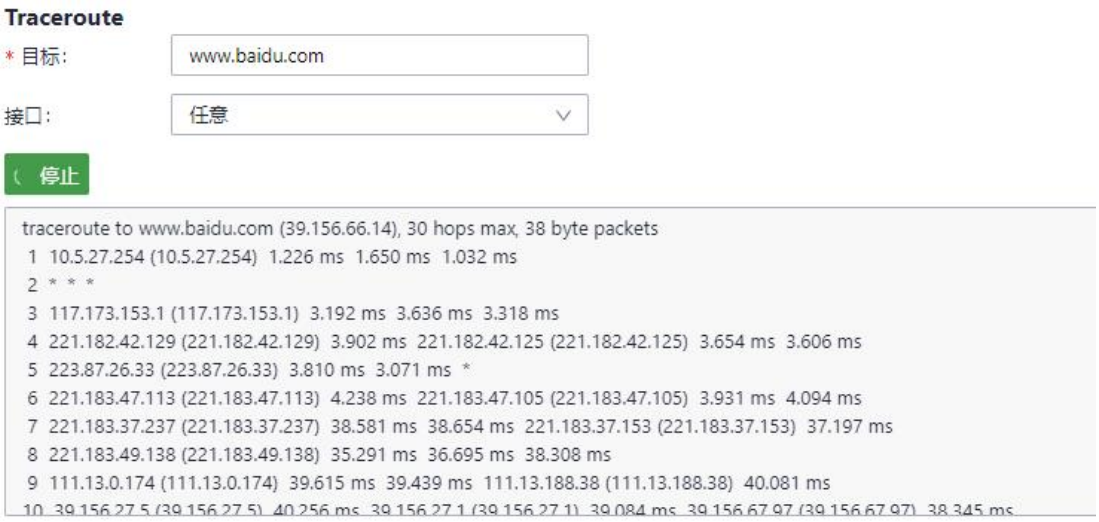
通过 ICMP 协议检测设备外网联通情况。在“目标”中填入任意域名或 IP 地址，点击开始即可检验设备与该目标的联通情况。



13-8-1 Ping 工具

13.8.2 Traceroute

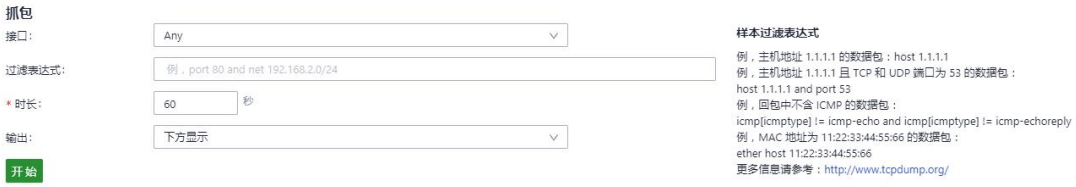
输入目标主机 IP 地址，选择接口，点击“开始”，检测设备到目标 IP 的路由连通情况。



13-8-2 路由追踪工具

13.8.3 抓包

通过此功能，用户可以抓取通过某一接口的数据包。通过选择“输出”选项，用户可以选择在界面中显示抓包数据或导出到本地。



13-8-3 抓包工具

13.9 日志服务器

启用日志文件服务器功能后，设备会定期将日志文件上传到指定的服务器。

13-9 设置日志服务器地址

13.10 其他设置

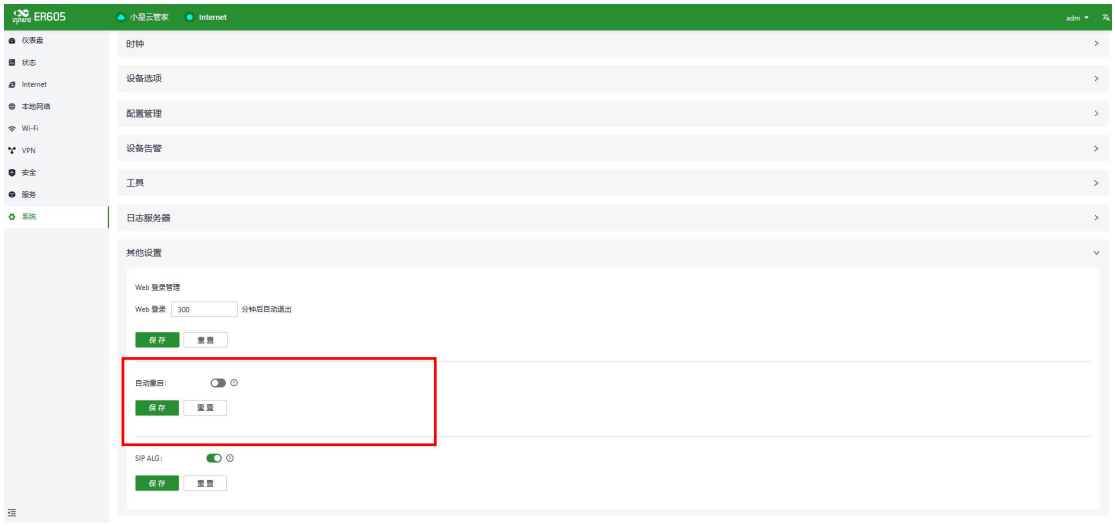
13.10.1 Web 登陆管理

设定登录 web 页面后间隔多长时间会自动登出

13-10-1 设置 web 页面自动登出时间

13.10.2 设备自动重启

开启此功能后，当设备无法联网且重试一小时后仍无法接入网络时，设备将会自动重启。



13-10-2 开启设备自动重启功能

13.10.3 SIP ALG

它通常用作防火墙，由两种技术组成，一种是会话发起协议（SIP），另一种是应用层网关（ALG）。

13-10-3 开启 SIP ALG 功能

注意:

开启此功能后 VoIP 电话通信将受到影响。