InHand VG710 车载网关用户手册 V1.1

InHand VG710 车载网关

用户手册

资料版本：V1.0—2022.02

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。

本手册图形界面约定

格 式	意 义
	表示按钮名，如“单击确定按钮”。
“”	表示窗口名、菜单名，如：弹出“新建用户”窗口。
>>	多级菜单用“>>”隔开。如“文件>>新建>>文件夹”多级菜单表示“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。
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。

技术支持联络信息

北京映翰通网络技术股份有限公司（总部）

电话：010-8417 0010

地址：北京市朝阳区紫月路 18 号院 3 号楼 5 层

成都办事处

电话：028-8679 8244

地址：四川省成都市高新区府城大道西段 399 号，天府新谷 10 栋 1406 室

广州办事处

电话：020-8562 9571

地址：广州市天河区棠东东路 5 号远洋新三板创意园 B-130 单元

武汉办事处

电话：027-8716 3566

地址：湖北省武汉市洪山区珞瑜东路 2 号巴黎豪庭 11 栋 2001 室

上海办事处

电话： 021-5480 8501

地址：上海市普陀区顺义路 18 号 1103 室

目 录

1 简介

InHand VG710 车载网关是面向车联网领域推出的新一代 4G 车载网关，该产品为汽车和运输服务车辆提供高速安全的网络，满足警用车辆，应急指挥车辆，工程车辆，医疗车辆以及物流车辆等移动高速网络需求，搭配基于云的远程车辆管理平台，为物流管理、资产跟踪、移动办公以及政府安全等工作提供随处可达的网络和不间断的运营监管。

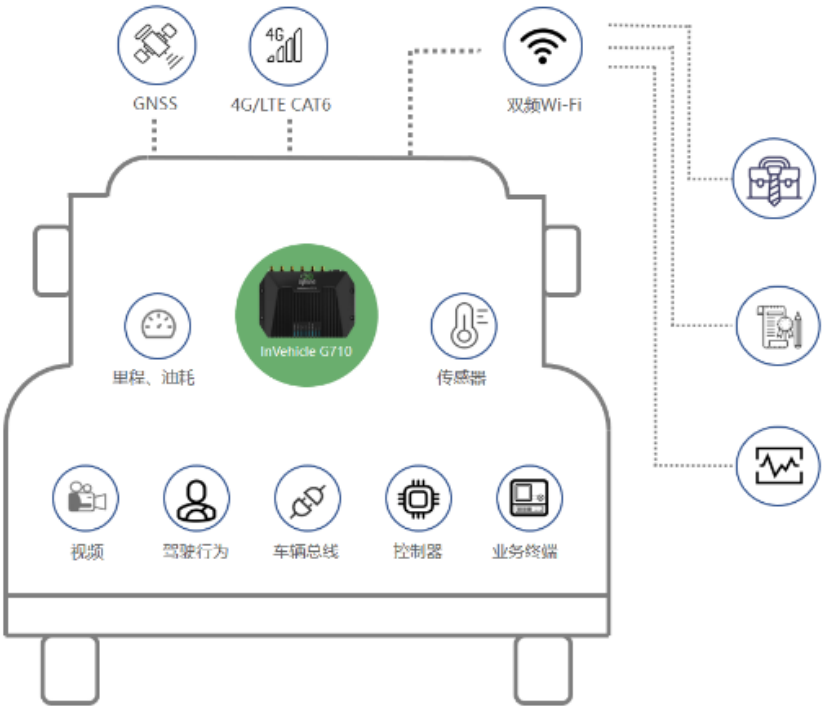


图 1 应用方案图

2 硬件部分

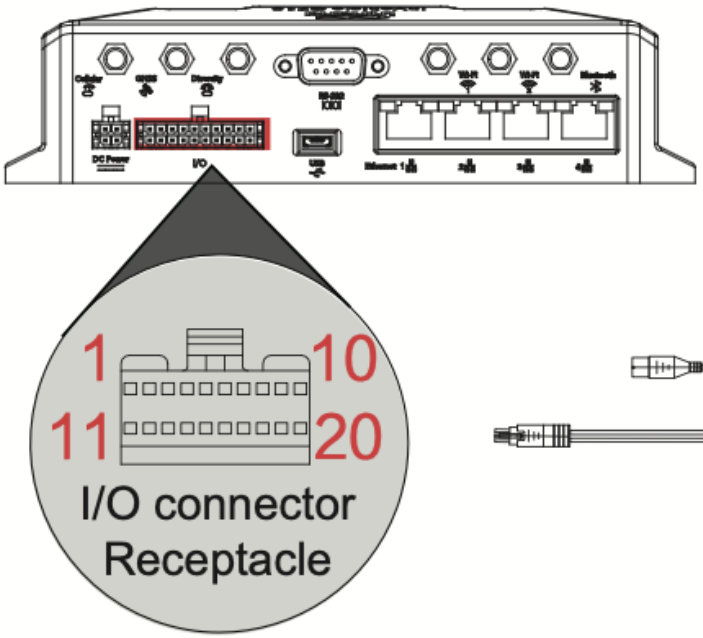
2.1 指示灯说明

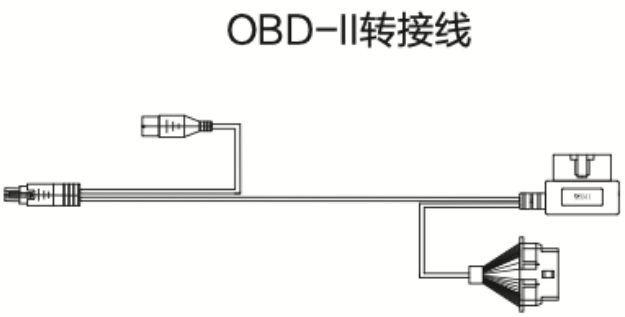
VG710 指示灯	LED 灯状态和定义
System	常灭 --- 设备未上电 红色常亮 --- 系统启动中 绿色闪烁 --- 系统正常运行 红色闪烁 --- 系统故障 蓝色闪烁 --- 系统升级
Cellular	常灭 --- 拨号功能处于关闭状态 绿色闪烁 --- 正在拨号 绿色常亮 --- 拨号成功 红色闪烁 --- 拨号故障【未探测到模块或 SIM 卡】
Signal	常灭 --- 当前拨号卡无信号 红色常亮 --- 当前拨号卡信号弱【信号值≤9asu】 蓝色常亮 --- 当前拨号卡 信号一般【信号值 10～19asu】 绿色常亮 --- 当前拨号卡信号强【信号值≥20asu】
GNSS	常灭 --- GNSS 处于关闭状态 绿色闪烁 --- 定位中 绿色常亮 --- 已定位
Wi-Fi 2.4G	作为 AP 使用：

	常灭 --- 处于关闭状态 绿色闪烁 --- 正常工作 作为 STA 使用： 常灭 --- 处于关闭状态或未关联上 AP 绿色常亮 --- 关联上 AP 后，因为密码错误无法连接 绿色闪烁 --- 已关联上 AP
Wi-Fi 5G	作为 AP 使用： 常灭 --- 处于关闭状态 蓝色闪烁 --- 正常工作 作为 STA 使用： 常灭 --- 处于关闭状态或未关联上 AP 蓝色常亮 --- 关联上 AP 后，因为密码错误无法连接 蓝色闪烁 --- 已关联上 AP
U1、U2	U1: 常灭 --- APP 处于关闭状态 绿色常亮 --- APP 为启用状态 U2: 常灭 --- VPN 处于关闭状态或 VPN 工作异常 绿色常亮 --- VPN 正常工作

2.2 接口面板说明

1. VG710 4G 版本 IO 接口接口介绍

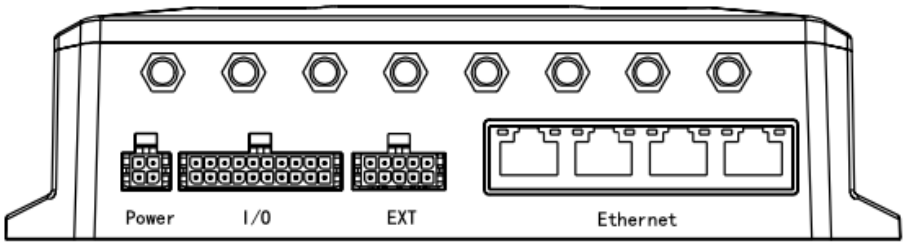




20PIN Definition			
PIN	Definition	PIN	Definition
1	-485	11	485
2	CANL	12	CANH
3	1-Wire	13	GND
4	DO4	14	DO3
5	DO2	15	DO1
6	GND	16	GND
7*	AI6/DI6	17*	AI5/DI5
8	AI4/DI4	18	AI3/DI3

9	AI2/DI2	19	AI1/DI1
10	GND	20	GND

1. VG710-H 5G 版本 IO 接口接口介绍



	ETX 10PIN Definition			
PIN	Definition	PIN	Definition	
1	J1708_A	6	J1708_B	
2	CAN_H	7	CAN_L	
3	GND	8	GND	
4	ODB_CAN_H	9	ODB_CAN_L	
5	K_LINE	10	L_LINE	
IO 20PIN Definition				
PIN	Definition	PIN	Definition	
1	AI1/DI1	11	AI2/DI2	

2	AI3/DI3	12	AI4/DI4
3	GND	13	GND
4	DO1	14	DO2
5	DO3	15	DO4
6	RS232_RX	16	1Wire
7	RS232_TX	17	GND
8	RS485_A_1	18	RS485_A_2
9	RS485_B_1	19	RS485_B_2
10	GND	20	GND

2.3 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，立即按下复位按钮（保持复位按钮按下状态）。大约 15 秒后，只有系统 System 灯红色常亮；

第二步：当 System 灯关闭然后再次变红，此时立即松开复位按钮；

第三步：当 System 灯关闭时，按下复位按钮（System 灯红色闪烁 2 次），然后松开复位按钮，设备即可恢复到出厂默认状态。

3 默认配置

序号	功能	默认配置
1	**蜂窝网络拨号**	• 启用【拨号成功则 Cellular 灯为绿色常亮】缺省状态下禁用双 SIM 卡，默认使用 SIM1
2	**卫星定位及惯性导航服务**	• 启用【定位成功则 GNSS 灯为绿色常亮】 • 惯性导航功能启用
3	**OBD 车辆诊断**	• 启用 • 自动探测 CANbus 波特率 • 自动探测车辆诊断协议 • 自动扫描车辆诊断数据
4	**Wi-FI 默认配置**	• Wi-Fi 2.4G AP 启用，SSID：以 VG710-为前缀，后面为 6 位数字 • Wi-Fi 5G AP 启用，SSID：以 VG710-5G-为前缀，后面为 6 位数字 • 认证方式为 WPA2-PSK • 密码为 SN 序列号后 8 位
5	**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
6	**网关的网络访问控制**	• HTTP 及 HTTPS 启用，端口号分别是 80 和 443 • Telnet 禁用 • SSH 禁用 • 来自蜂窝网络的访问仅允许 HTTPS 方式
7	**用户名和密码**	• **adm/123456**（超级管理员）
8	**电源管理**	• shutdown-delay 30 下电延时为 30 秒 • standby-mode 1 下电功能启用 • standby-check-interval 20 在待机模式下电源检查间隔 • standby-voltage 90 待机门限电压为 9V • standby-resume-voltage 105 待机状态下恢复正常工作的门限电压为 10.5V
9	**IO**	• 4 路数字输出默认输出低电平，上拉电阻禁用 • 6 路数字输入的上拉电阻禁用。

10	串口	• RS232 波特率：9600 数据位：8bits 检验位：无校验 停止位：1bit • RS485 波特率：9600 数据位：8bits 检验位：无校验 停止位：1bit

4 登录联网

4.1 设备通过拨号卡接入网络

1. 插入 SIM 卡、接好 GNSS 和 Cellular 天线，连接电源和 PC。拨号卡信号不好时请同时插入 Diversity 拨号天线。

电源

Cellular 天线

连接 PC

插入 SIM 卡

GNSS 天线

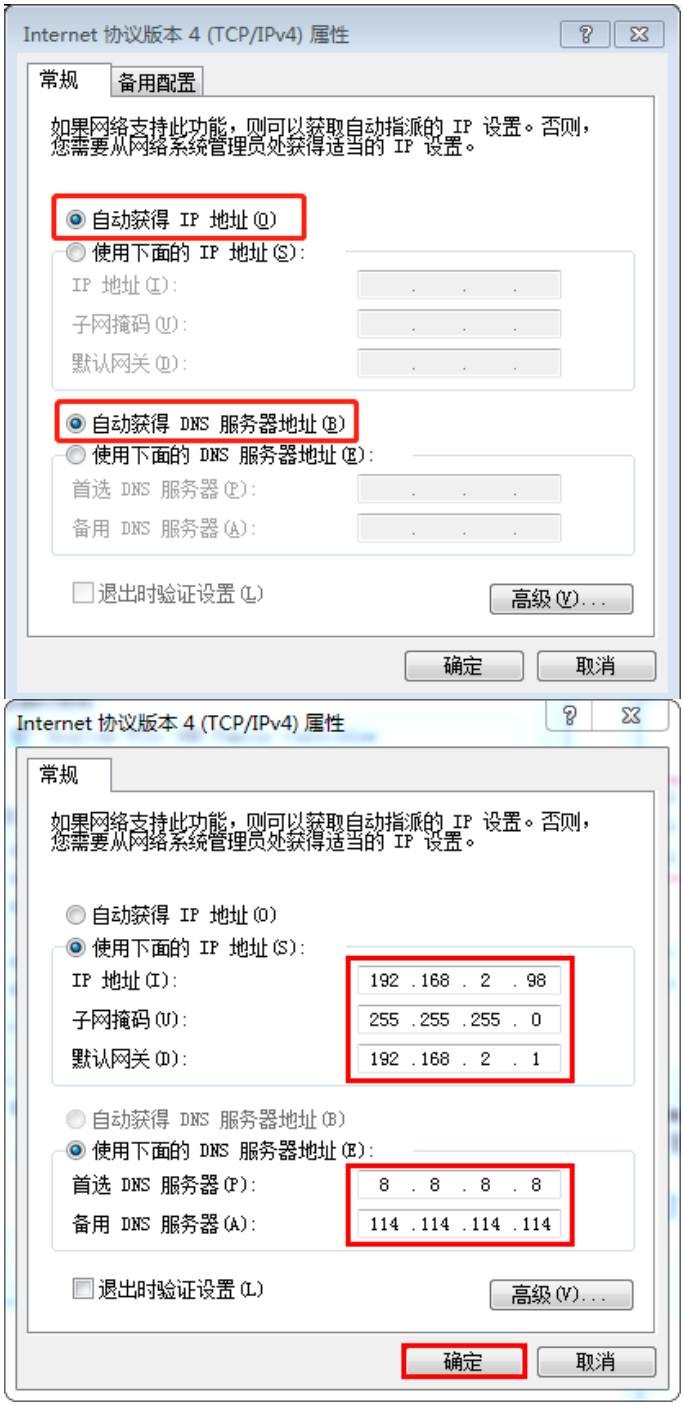
> 注意 注意：
>
> 插拔 SIM 卡操作时，必须拔掉电源，以免造成数据丢失或设备损坏。

1. 设置 PC 与网关的 IP 地址在同一网段。

方法一：自动获取 IP 地址（推荐）；

方法二：使用固定 IP 地址，设置 PC 和网关在同一网段。

步骤：选择“使用下面的 IP 地址”，输入 IP 地址（在 192.168.2.2~192.168.2.254 中任意值，避免与设备的初始 IP 地址 192.168.2.1 冲突），子网掩码（255.255.255.0），默认网关（192.168.2.1），配置 DNS 服务器地址，然后单击确定。



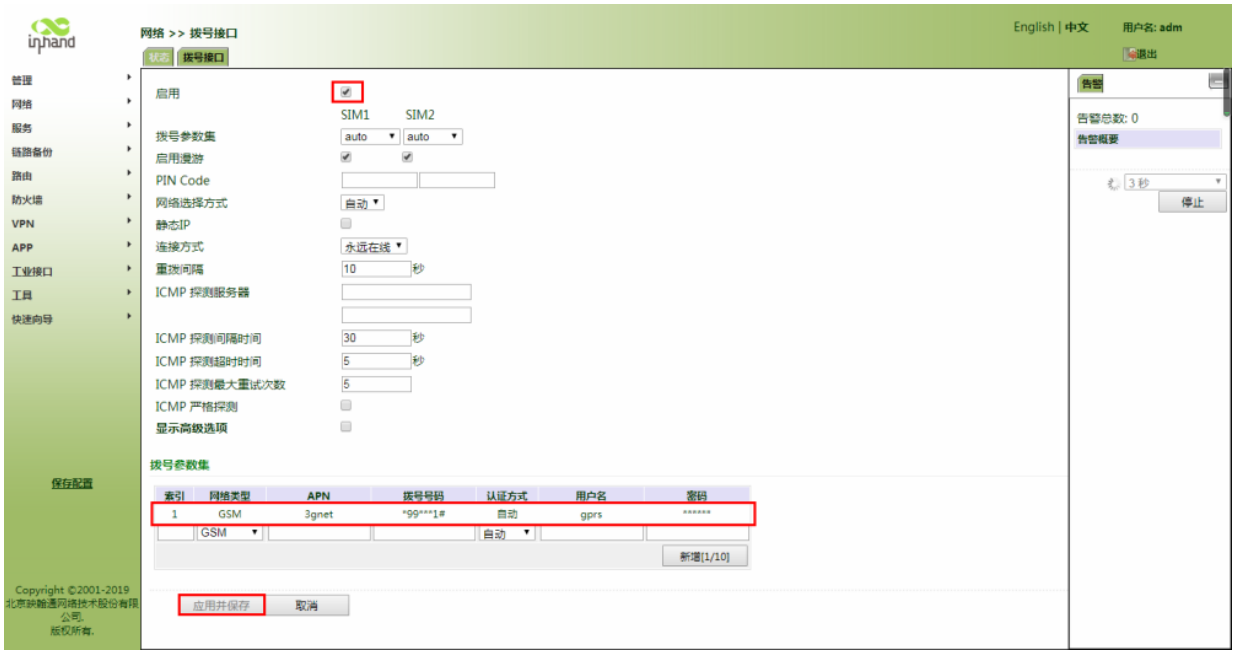
自动获取 IP 地址 使用固定 IP 地址

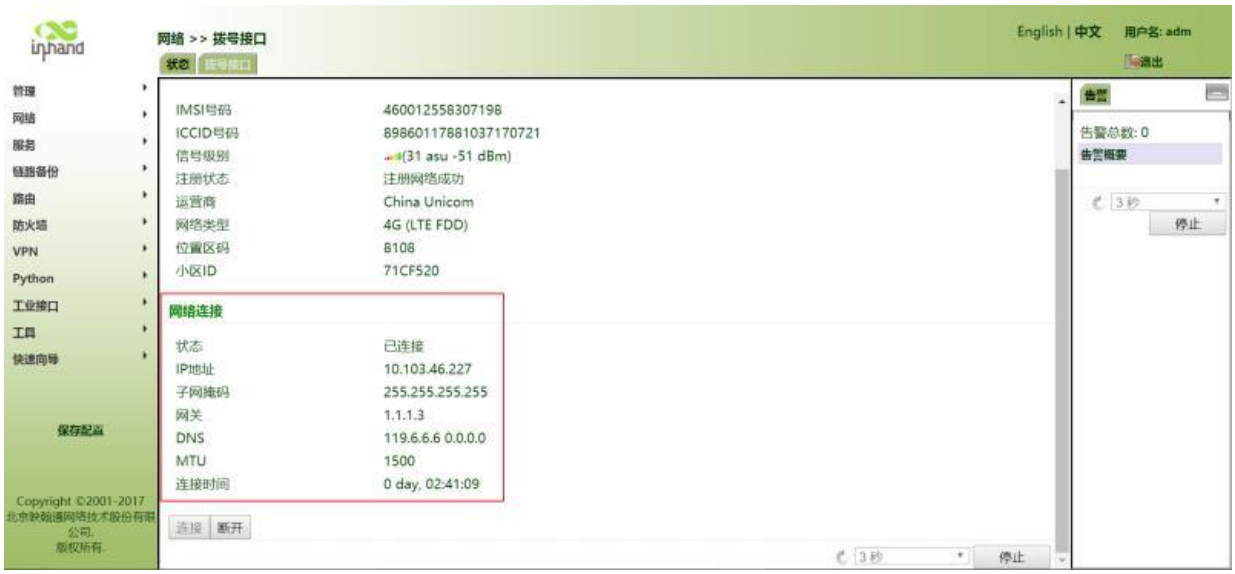
1. 打开浏览器，在地址栏中输入网关设备默认 IP 地址 192.168.2.1，回车。

1. 登录设备（如果提示拦截，点击高级>>继续前往）。

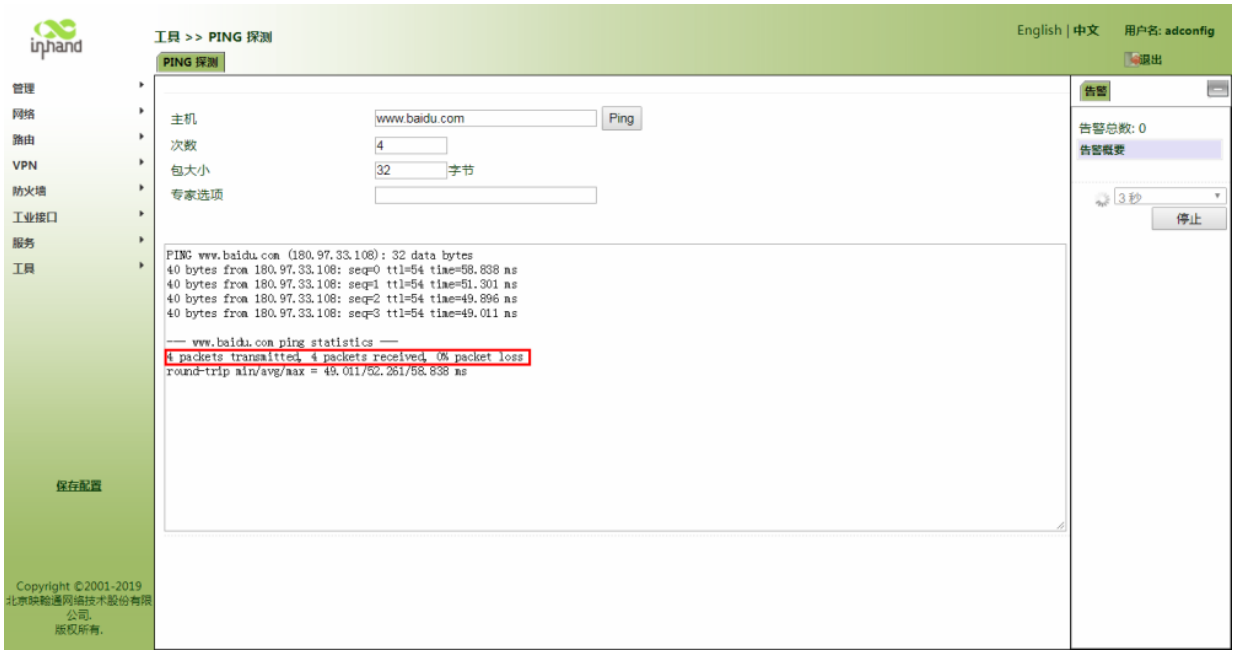
1. 点击“网络>>拨号接口”勾选启用，点击应用并保存。待网络连接状态显示为“已连接”并且显示已分配相应 IP 地址等状态时说明 SIM 卡已成功接入网络。

（专网卡还需要填写 APN 参数）

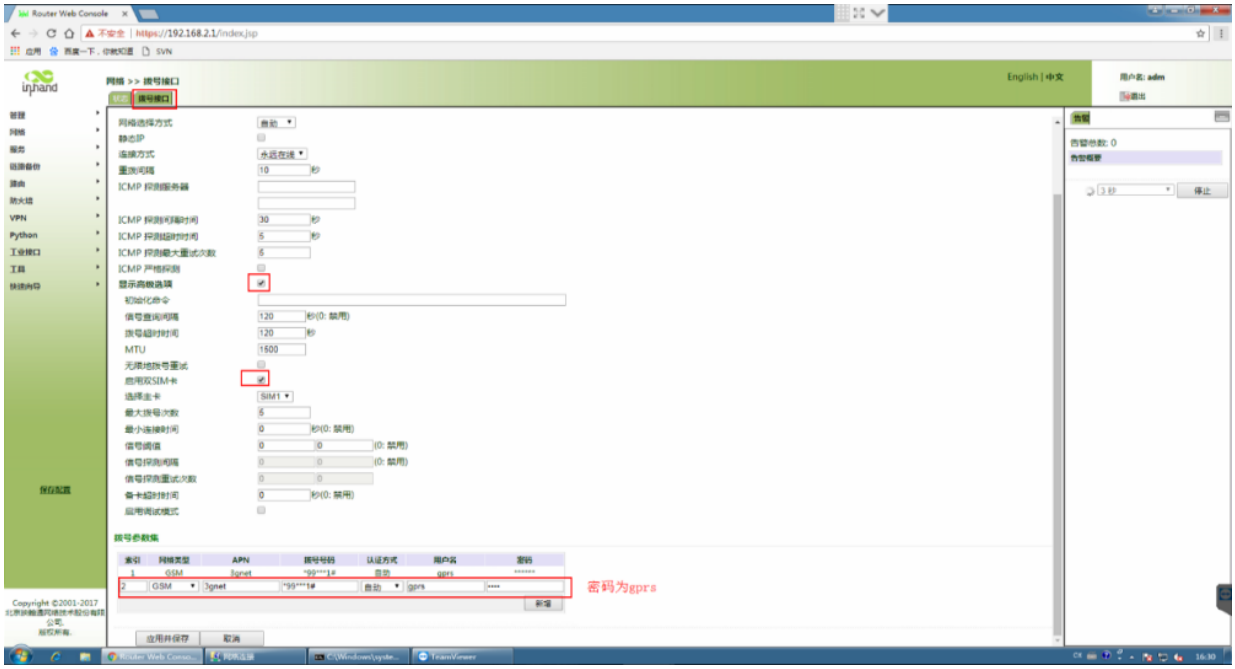




1. 使用 PING 探测工具 PING 国内常用网址，如果有数据传输表明设备已成功上网。



1. 当使用双卡时，需启用双 SIM 卡。



4.2 Wi-Fi 接入网络

1. 使用 Wi-Fi 上网的接线方法，如下图。

电源

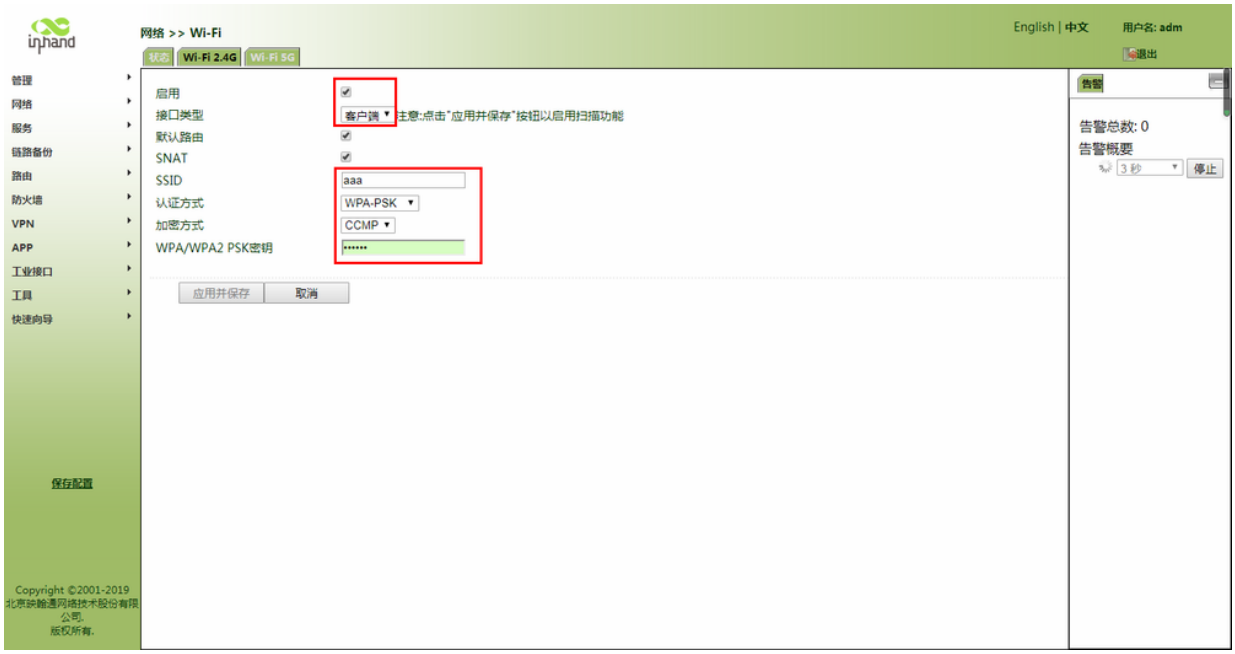
Wi-Fi 天线

连接 PC

GNSS 天线

1. 设置 PC 与网关设备的 IP 地址在同一网段，登录 WEB，参看 3.1 设备通过拨号卡接入网络。

2. 点击“网络>>Wi-Fi”，选择 2.4G 或 5G Wi-Fi 作为客户端使用，输入可用的无线接入点的名称、认证方式、密钥，点击应用并保存。



1. 点击“状态”栏，查看到当前网络状态为“已连接”，表示 Wi-Fi 已成功接入网络。

5 网络管理

在配置参数时，带绿色的填写框 表示必填写项，纯白色填写框 表示选填写项。

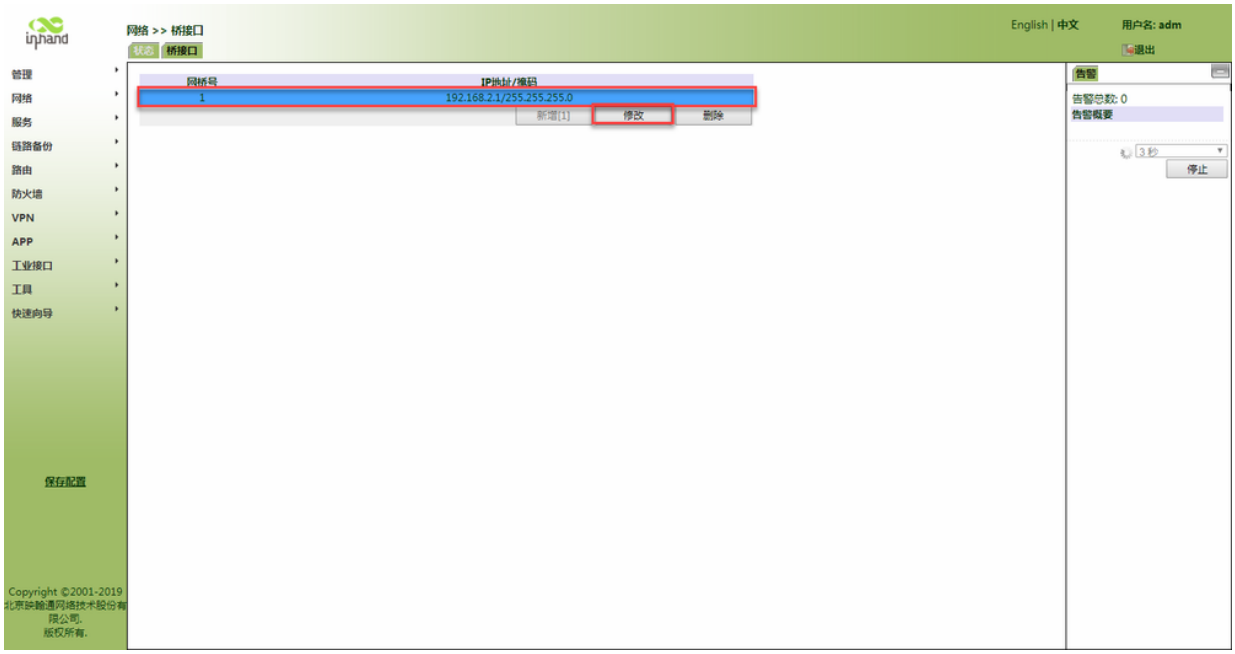
5.1 网络

5.1.1 桥接口

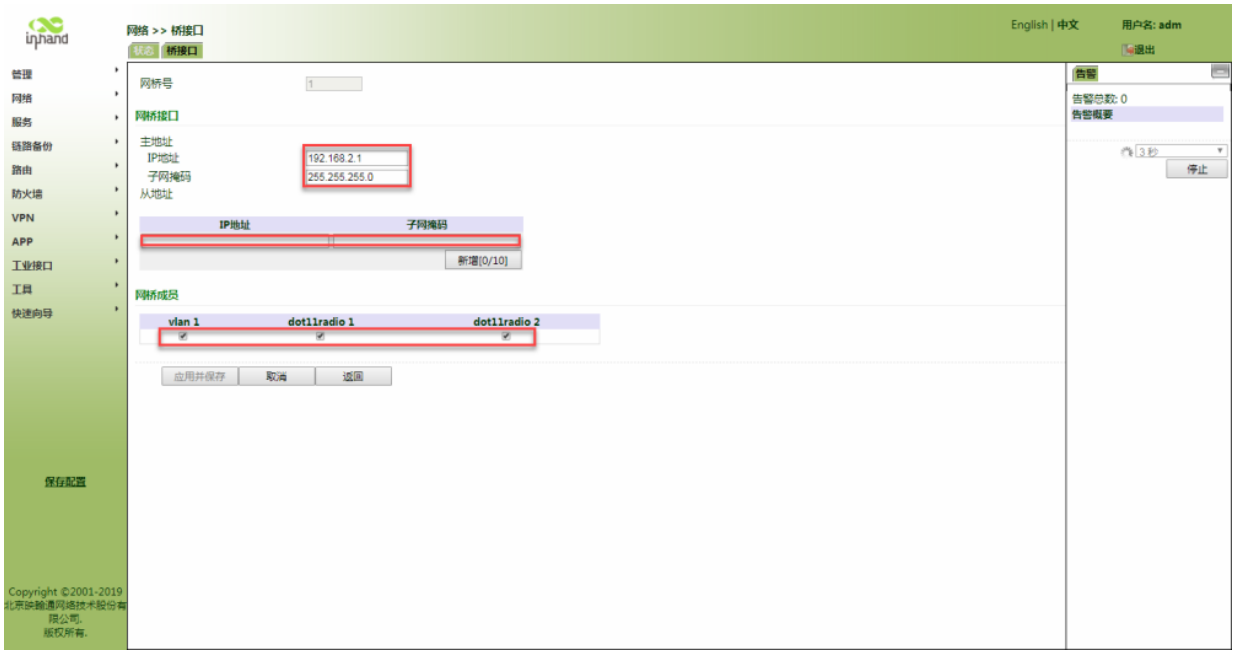
设置桥接口的目的是通过网桥把两个不同的物理局域网连接起来，是一种在链路层实现局域网互连的存储转发。

修改桥接口的 IP 地址和网桥成员的方法：

第一步：点击“网络>>桥接口，选中桥接口>>修改”。



第二步：修改桥接口的 IP 地址或者网桥成员。网桥成员中，dot11radio1 和 dot11radio2 分别为 Wi-Fi 2.4G 和 Wi-Fi 5G 接口。

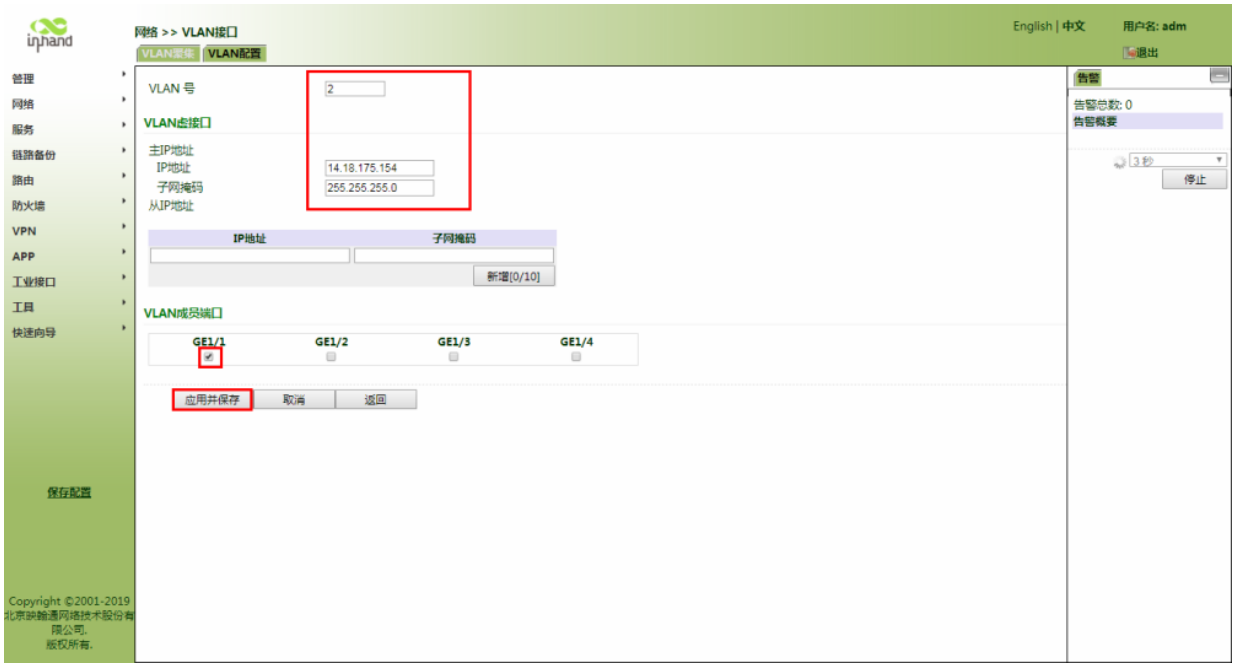


5.1.2 VLAN 接口

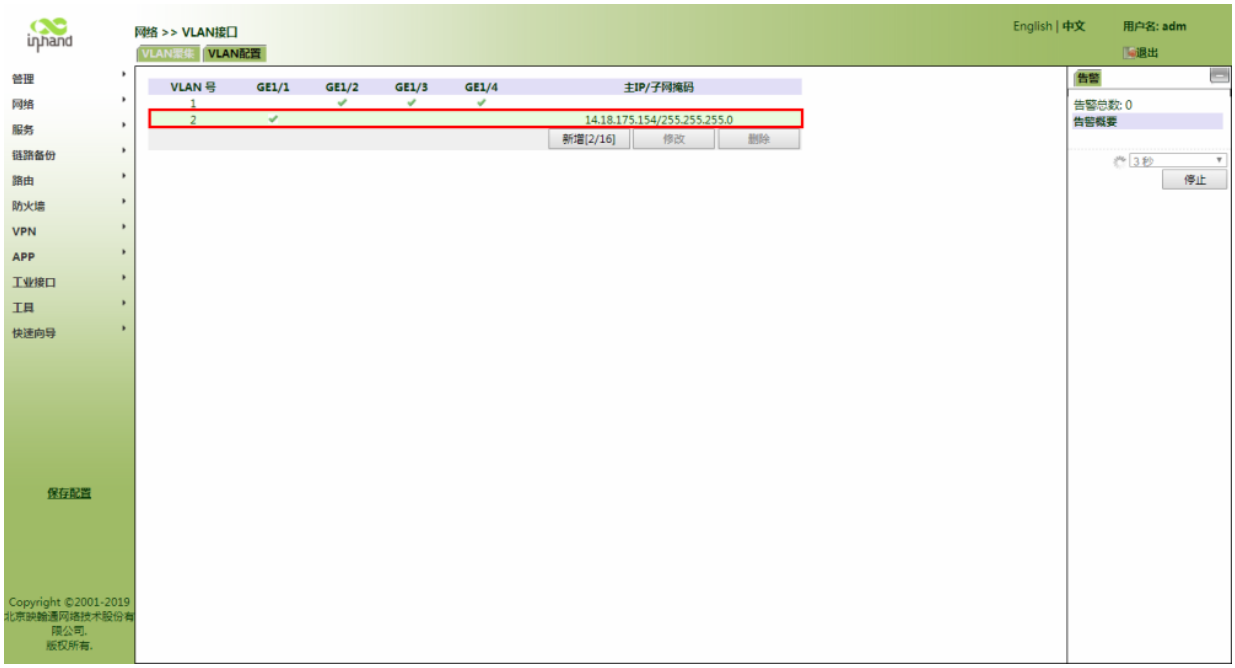
虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。

新增一个 VLAN2 接口的方法：

第一步：点击“网络>>VLAN 接口>>VLAN 配置>>新增”，按需求设置 VLAN2 接口的虚拟 IP 地址和选择 VLAN2 成员接口，点击应用并保存。



第二步：返回 VLAN 列表，VLAN2 接口已新增成功。



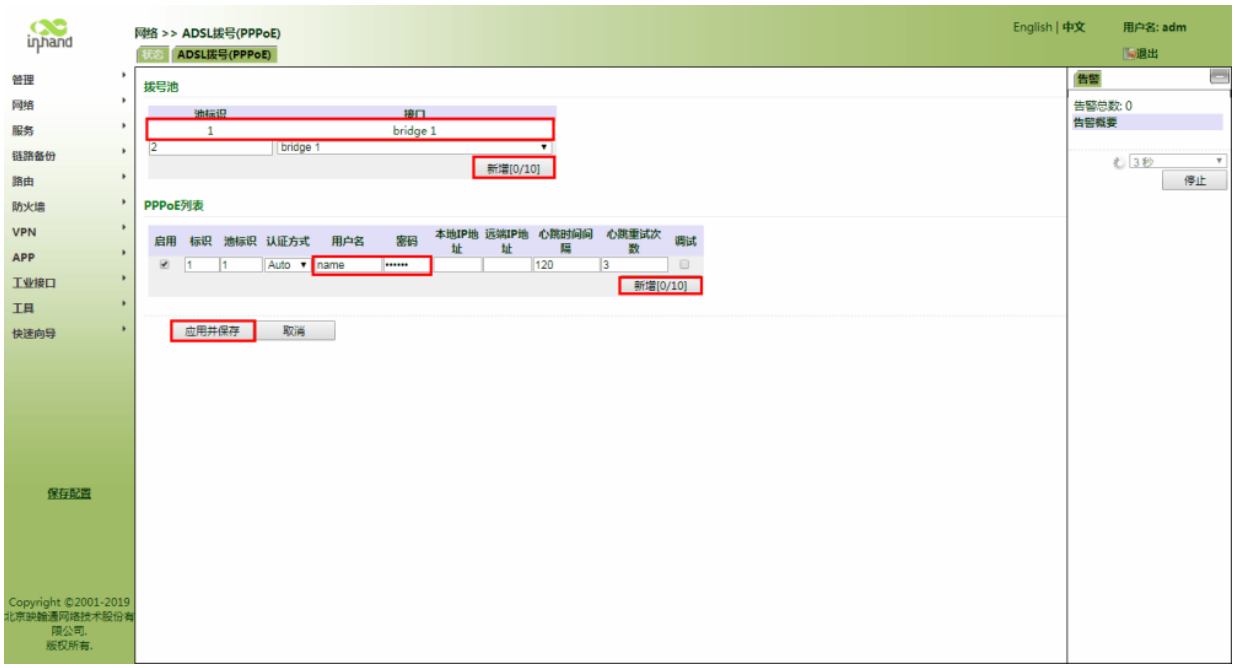
目前设备 VLAN 端口支持 Access 和 Trunk 两种链路类型。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 报文，可以用于交换机之间的连接，也可以用于连接用户的计算机。您可以通过 VLAN 聚集页面根据需要选择链路类型。

5.1.3 ADSL 拨号(PPPoE)

网关连接 PPPoE 服务器的设置方法：

第一步：点击“网络>> ADSL 拨号(PPPoE)”，在“拨号池”栏选择连接 PPPoE 服务器的 VG710 的接口，点击新增。

第二步：在“PPPoE 列表”栏填入 PPPoE 服务器的用户名、密码和池标识，池标识必须与“拨号池”中池标识相同，点击新增，然后点击应用并保存。

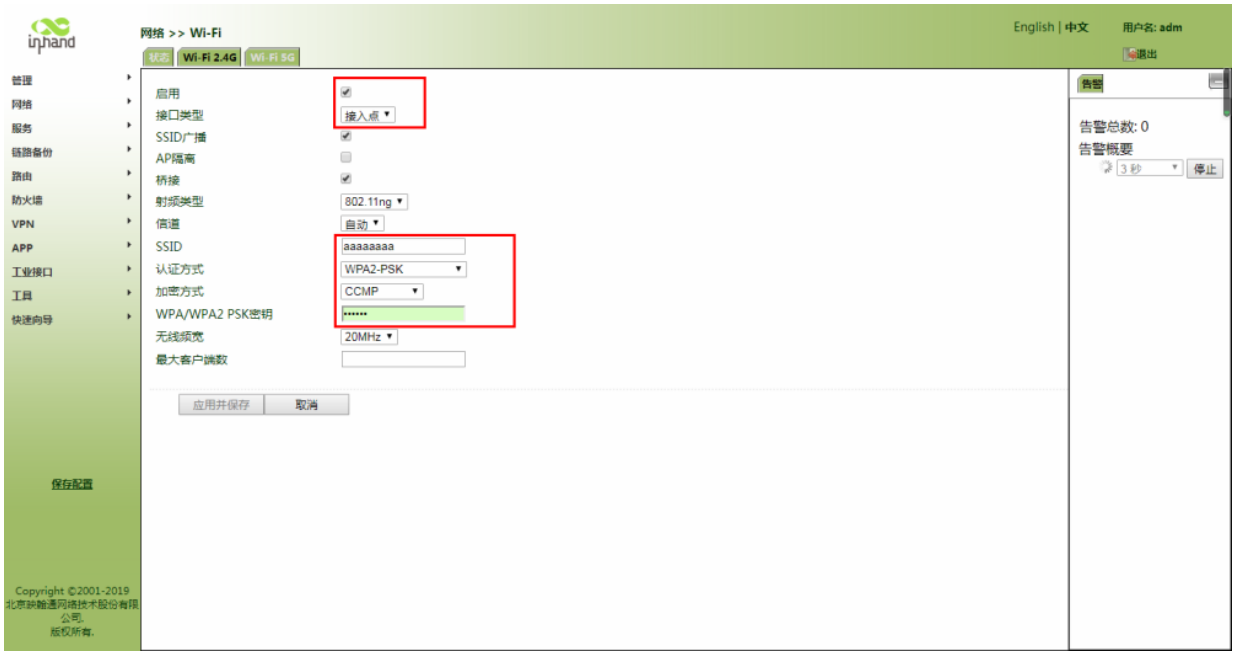


5.1.4 Wi-Fi

网关可作为接入点或者客户端使用，作为接入点使用时，其它用户可通过网关设备 Wi-Fi 上网；作为客户端使用时，设备连接接入点上网。状态栏显示设备当前的 Wi-Fi 网络情况。

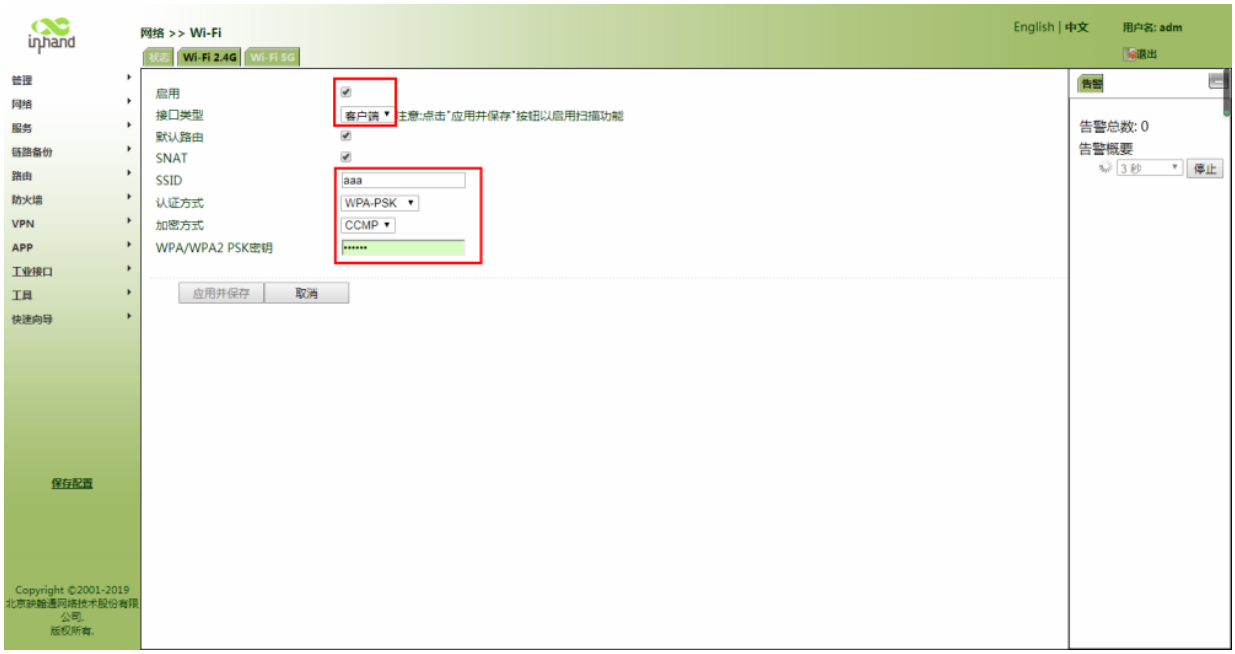
设备作为接入点使用，给无线终端提供网络访问服务的设置方法：

点击“Wi-Fi>>Wi-Fi2.4/5G”，“接口类型”选择接入点，填入 SSID、认证方式、加密方式和密钥，点击应用并保存。



VG710 作为客户端使用，连接接入点上网的设置方法：

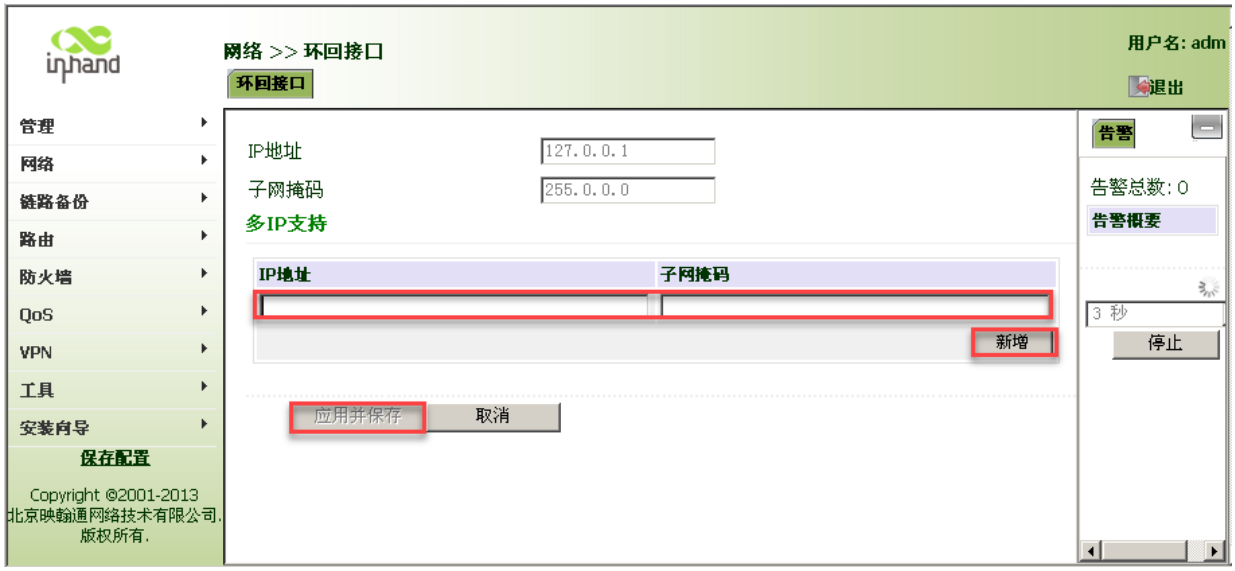
选择客户端，并填入 Wi-Fi 的 SSID 和密钥，点击应用保存。



5.1.5 环回接口

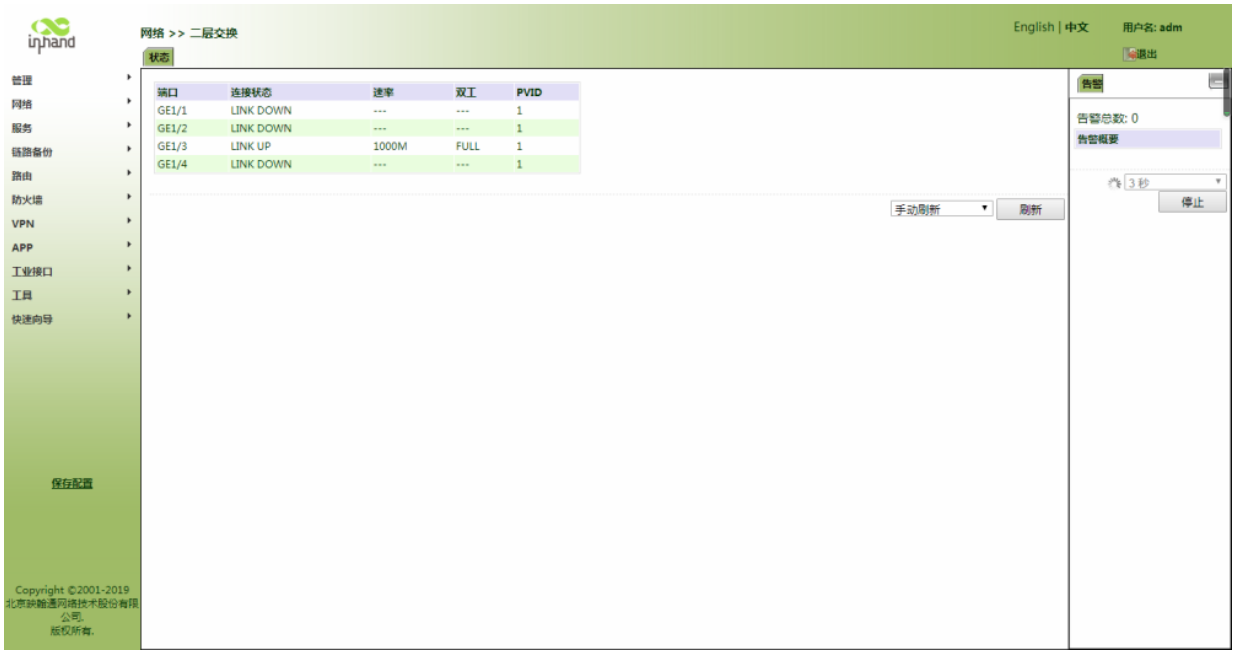
新增多个从 IP 的设置方法：

点击“网络>>环回接口>>多 IP 支持”为网关配置任意的 IP 地址，点击新增，然后点击应用并保存。



5.1.6 二层交换

查看 GE1~4 口的网络连接状态，LINK UP：连接；LINK DOWN：断开。



5.2 车辆诊断

车辆诊断服务用于实时的车况数据采集，排放的相关信息获取以及故障的诊断。车况数据包括油位，里程，行驶速度，发动机转速，发动机负荷，冷却液温度，制动压力等关键参数。排放信息包括车用尿素(AdBlue)容积，多种尾气后处理传感器(废气传感器，柴油颗粒过滤器等)和催化剂的工作情况和监测状态等信息。故障诊断可实时获取车辆标准的故障码及描述信息，便于车辆维护人员及时了解车辆的健康状况，帮助车辆维修人员进行故障的定位。

车辆数据采集，网关通过 **OBD-II** 或 **J1939 线缆**从网关的 I/O 端口接入到车辆的诊断接口，线缆配件可在购买时选配或定制，具体的接入方法可参考《VG710 快速入门指南》4.4 节。网关启动后自动启用车辆诊断服务，采集关键的车况数据和故障码信息。

> **注意** 注意：
>
> 应在车辆处于熄火状态下完成网关电源和 OBD 线缆的安装。

车辆诊断的状态页面，显示车辆诊断的状态信息。

OBD 状态信息显示：

CAN 接口状态【ERROR-ACTIVE：表示网关成功接入车辆的诊断接口，其他状态：表示连接异常或未能识别出车辆的诊断接口】

CAN 波特率 【在车辆诊断中，CAN 波特率自动适配，一般为 250kbps 或 500kbps】

CAN 接口的应用方式【车辆诊断|定制，默认为车辆诊断】

OBD 连接状态【未连接|正在连接|已连接】

OBD 协议类型【OBD-II|J1939】

手动扫描并查看报告：

通过点击扫描车辆诊断数据按钮可生成包含详细车况数据和诊断信息的车辆诊断数据报告文件，点击导出车辆诊断数据报告按钮可将生成的诊断数据报告保存到本地。

OBD 数据流： 显示实时的车况数据。

OBD数据流

参数名	值	单位
故障指示灯状态	off	---
故障码数量	0	---
燃油系统状态	CL	---
发动机负荷	87.45	%
发动机冷却液温度	100.00	C
燃油压力	48.00	kPa
进气歧管压力	32.00	kPa
发动机转速	928.00	RPM
车辆速度	73.00	km/h
进气歧管温度	17.00	C
节气门位置	11.76	%
车辆诊断标准	0x00000006	---
发动机启动时间	27272.00	sec
MIL激活后的行驶距离	4643.00	km
燃油轨压力	131240.00	kPa
油位	50.20	%
故障码被清除后的行驶距离	200.00	km
大气压力	101.00	kPa
电池电压	13.78	V
环境空气温度	-40.00	C
MIL激活后发动机的运行时间	257.00	sec
故障码被清除后的运行时间	771.00	sec
燃油类型	GAS	---
发动机机油温度	56.00	C
燃油消耗率	10.00	L/h

车辆诊断能力显示：

车辆诊断能力的版本号；

诊断协议类型；

车辆识别码；

网关可采集的有效变量和参考值。

车辆诊断能力

版本号	1.01
协议	OBD-II
车辆识别码	LFV3B28R8A3025310

有效变量	参考值
故障指示灯状态	0
故障码数量	0
发动机负荷	14.9
发动机冷却液温度	94
燃油压力	48
发动机转速	5089
车辆速度	110
节气门位置	36.08
发动机启动时间	8409
MIL激活后的行驶距离	4643
油位	50.2
故障码被清除后的行驶距离	200
电池电压	13.78

5.3 VPN 应用

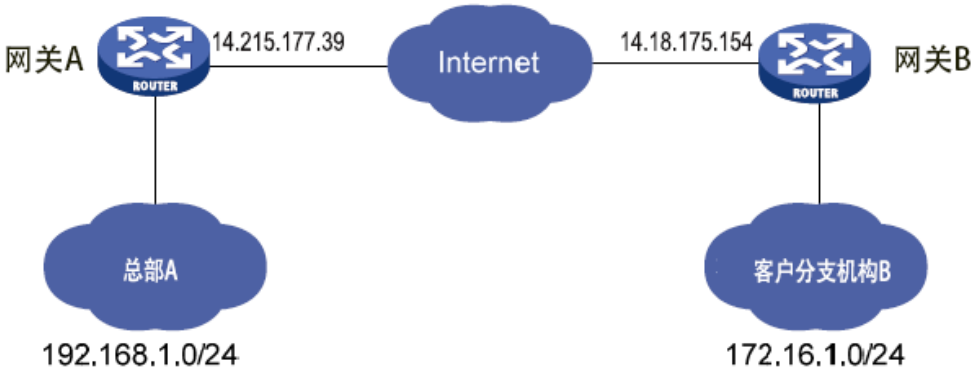
VPN（虚拟专用网络）的功能是：在公用网络上建立专用网络，进行加密通讯。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 可通过服务器、硬件、软件等多种方式实现。相比传统 DDN 专线或帧中继的方法，VPN 提供了一种更加安全，方便的远程访问方案。

最常见的 VPN 运用场景。例如为出差的老板提供企业内部网络的访问服务。老板连接到公司的 VPN 服务器，然后通过 VPN 服务器进入企业内网。VPN 服务器和客户端之间的通讯数据都进行了加密，可以看做是在一条专用的数据网络上传输。因此保证了数据的安全。

5.3.1 IPsec

IPSec 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。

情景：总部 A 所在的子网为（192.168.1.0/24）与客户分支机构 B 所在的子网为（172.16.1.0/24）通过网关 A 和网关 B 进行数据传输，我们为网关 A 和网关 B 传输通道进行 IPsec 加密，保护机构 A 和机构 B 之间数据传输的安全。



为网关 A 和网关 B 传输通道进行 IPsec 加密的设置方法：

配置参数表：

网关 A			**网关 B**	
配置 IKEv1/v2 参数			**配置 IKEv1/v2 参数**	
标识	自定义填写		标识	自定义填写
加密算法	AES128		加密算法	与网关 A 相同
哈希算法	SHA1		哈希算法	
Diffie-Hellman 秘钥交换	Group2		Diffie-Hellman 秘钥交换	
生命周期	86400		生命周期	
IPsec 策略			**IPsec 策略**	
名称	自定义填写		名称	自定义填写
封装	ESP		封装	与网关 A 相同
加密算法	AES128		加密算法	

认证方式	SHA1		认证方式	
IPsec 模式	隧道模式		IPsec 模式	
IPsec 隧道配置			**IPsec 隧道配置**	
对端地址	网关 B 建立 IPsec 服务的地址		对端地址	网关 A 建立 IPsec 服务的地址
接口	建立 IPsec 服务的接口		接口	建立 IPsec 服务的接口
IKE 版本	所使用的 IKE 版本		IKE 版本	与网关 A 相同
认证方式	共享秘钥		认证方式	
本地子网	网关 A 子网的 IP 地址		本地子网	网关 B 子网的 IP 地址
对端子网	网关 B 子网的 IP 地址		对端子网	网关 A 子网的 IP 地址

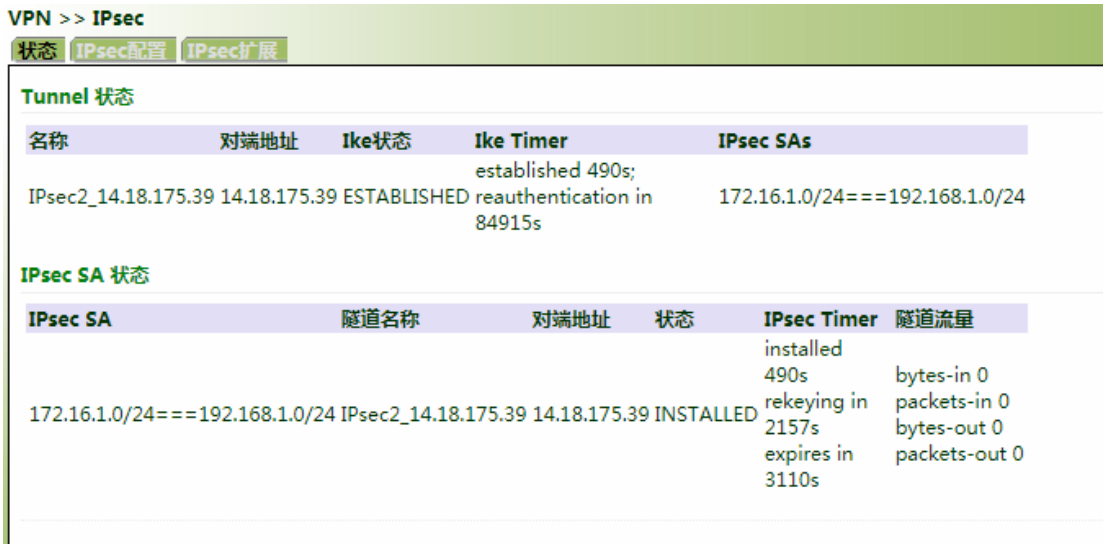
详细配置步骤：

第一步：分别设置网关 A 和网关 B。

1）新增 IKE 策略、IPsec 策略，点击应用并保存。

2）新增 IPsec 隧道，点击应用并保存。

第三步：网关 A、B 配置完成后，进入 IPsec“状态”页面，如下表示 IPSec 已成功建立。



注意 注意：

建立 IPsec VPN 时，IPsec Profile 不用配置，只有 DMVPN 时才用到 IPsec Profile。

5.3.2 GRE

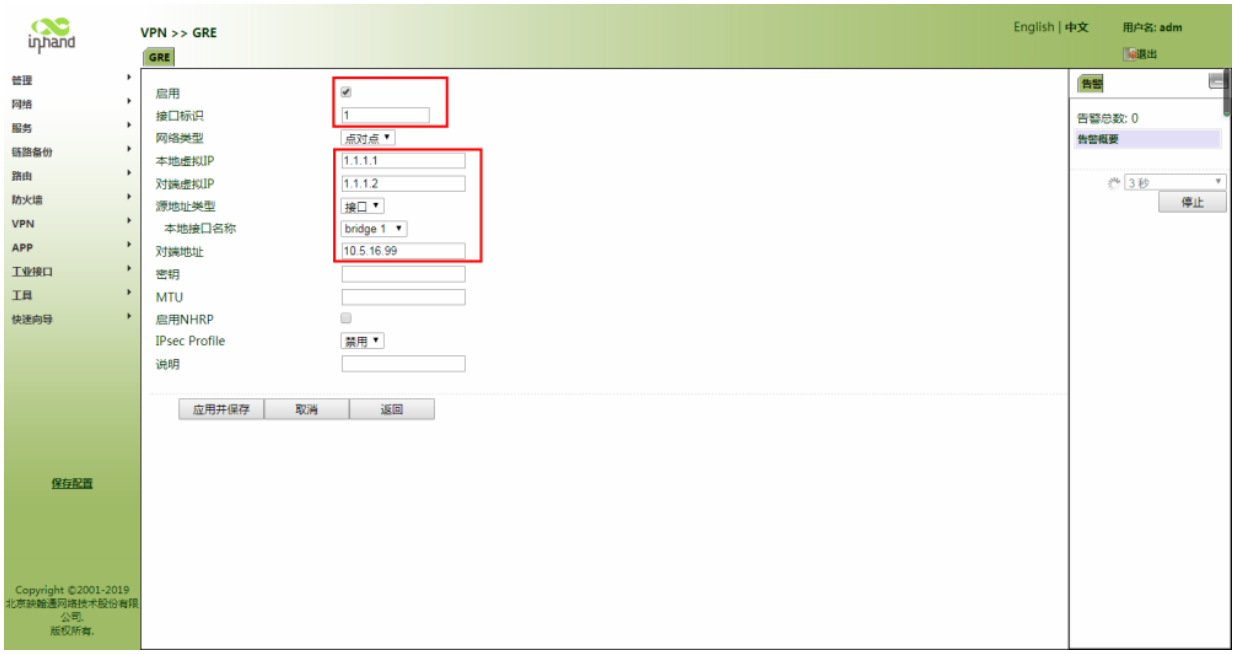
GRE 是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在 IPv4 网络中传输。

情景：VG710_A 和 VG710_B 通过公网建立 GRE 协议封装。

VG710_A 和 VG710_B 传输通道进行 GRE 封装的设置方法：

第一步：点击“VPN>>GRE”，点击新增。

第二步：“标识”自定义填写、“网络类型”支持“点对点”和“子网”类型，“本地和对端虚拟 IP”自定义填写但必须在同一网段，填写源和对端网络地址或者接口、密钥，点击应用并保存。



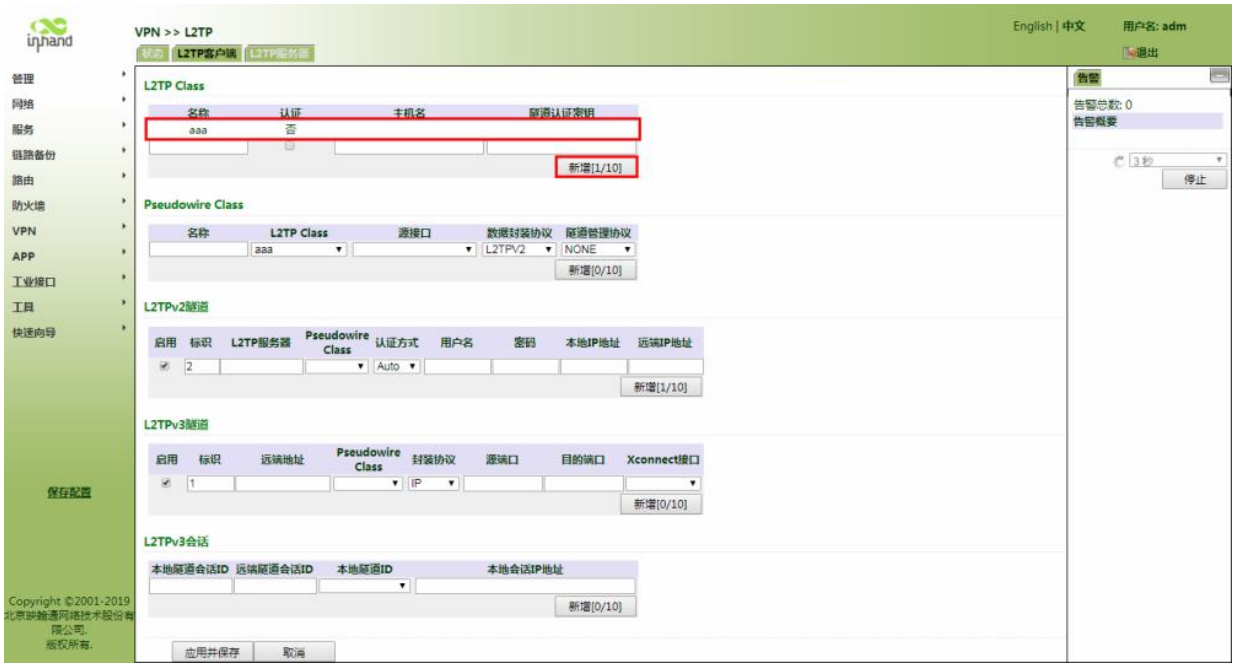
第三步：以相同方法设置 VG710_B，其中 VG710_B 的虚拟 IP、对端地址必须与 VG710_A 的对应，密钥与 VG710_A 的必须相同。

5.3.3 L2TP

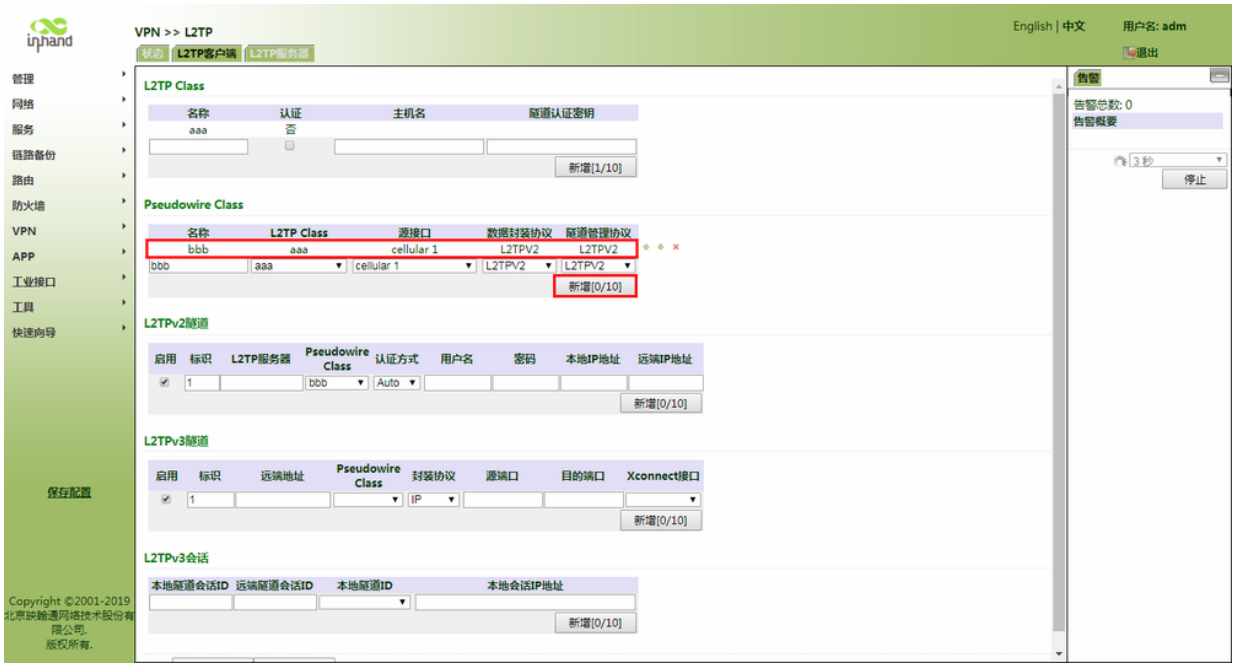
L2TP 是一种工业标准的 Internet 隧道协议，可以对网络数据流进行加密。

网关做 L2TP 客户端使用的设置方法：

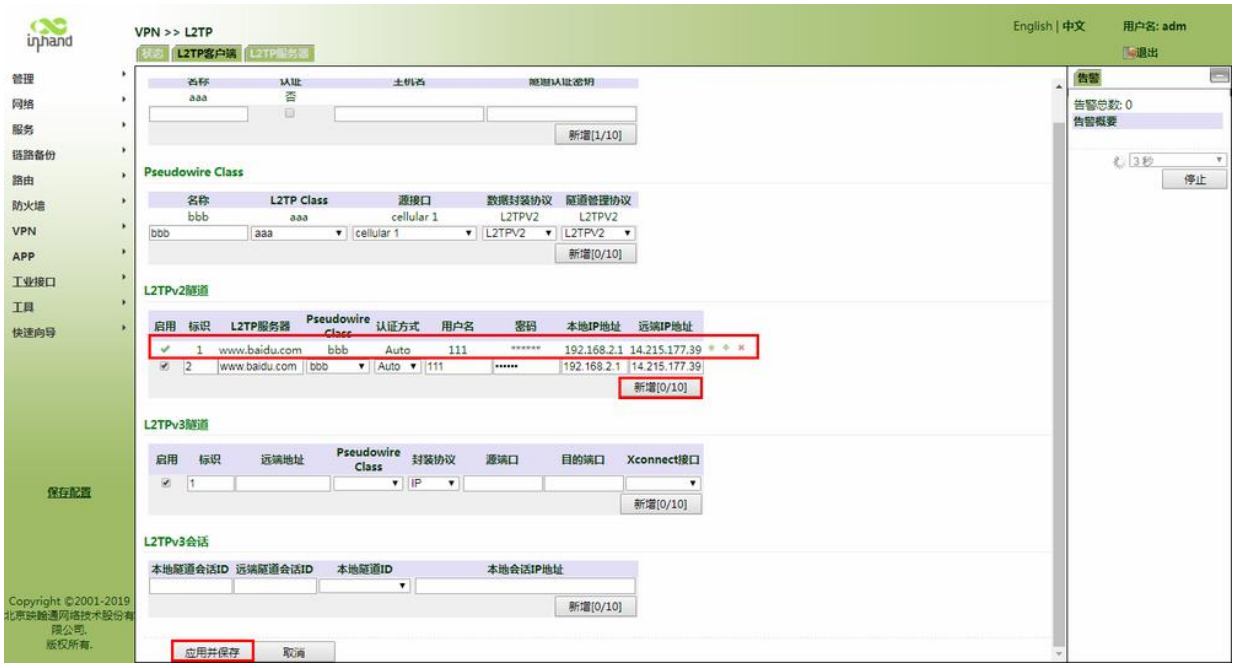
第一步：点击“VPN>>L2TP>>L2TP 客户端>>L2TP Class”填入一个 L2TP Class 名称，点击新增。



第二步：配置 Pseudowire Class，任意填写一个 Pseudowire Class 名称，“L2TP Class”与 L2TP Class 中名称相同，“源接口”填写与服务器建立连接的接口，“协议”选择 L2TPv2，点击新增；



第三步：配置 L2TPv2 隧道参数，“L2TP 服务器”填入服务器的域名或者 IP 地址，“Pseudowire Class”与 Pseudowire Class 中的名称相同，填写在服务器创建的用户名/密码，其它参数根据您的需求配置，点击应用并保存。



5.3.4 OpenVPN

OpenVPN 基于 OpenSSL 库的应用层 VPN 实现。它支持证书，秘钥或者用户名/密码等多种认证方式。和传统 VPN 相比，它的优点是简单易用。

认证列表：

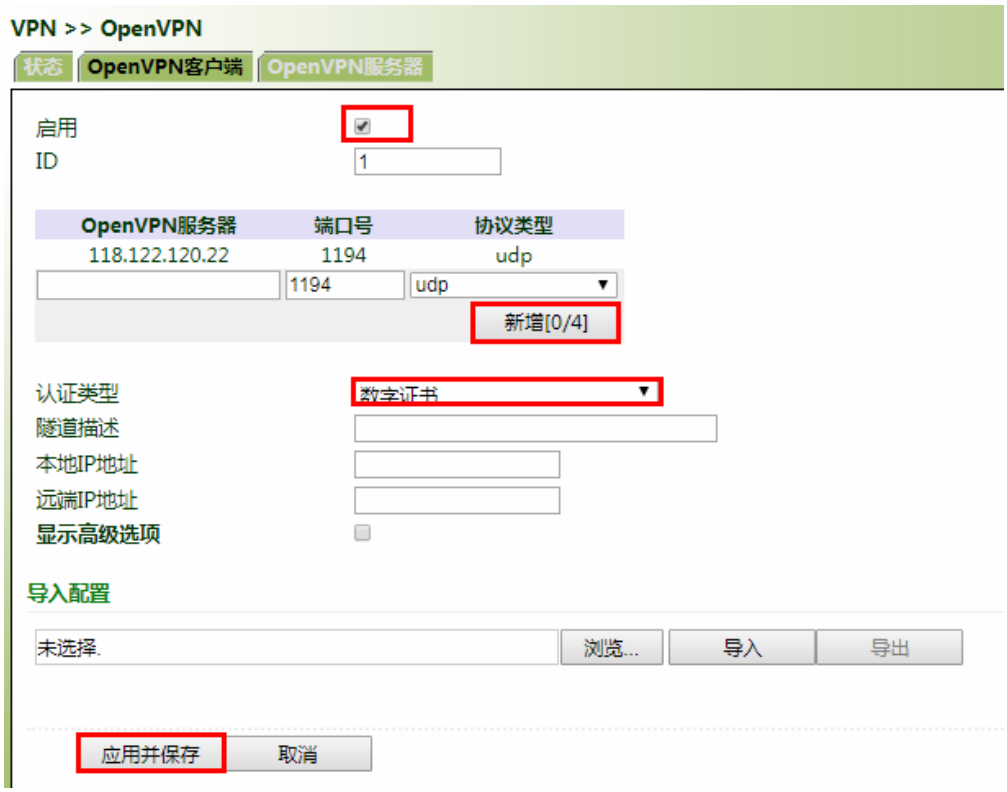
认证方式	Web 页面进行的操作
无	无需认证。
用户名/密码	需要输入 OpenVPN 服务器上设置的用户名和密码，并点击“VPN>>证书管理”导入 CA 证书、公钥、私钥进行认证。
预共享秘钥	需要输入 OpenVPN 服务器上设置的预共享秘钥。
数字证书	需要点击“VPN>>证书管理”导入 CA 证书、公钥、私钥。

数字证书/用户名/密码	需要输入 OpenVPN 服务器上设置的用户名和密码，并点击“VPN>>证书管理”导入 CA 证书、公钥、私钥进行认证。
数字证书/TLS 认证	需要输入 OpenVPN 服务器上设置的预共享秘钥，并点击“VPN>>证书管理”导入 CA 证书、公钥、私钥进行认证。
数字证书/TLS 认证/用户名/密码	需要输入 OpenVPN 服务器上设置的预共享秘钥，用户名和密码，并点击“VPN>>证书管理”导入 CA 证书、公钥、私钥进行认证。

网关作为客户端连接 OpenVPN 服务器的设置方法：

OpenVPN 支持手动配置和导入配置两种方式，以认证类型为数字证书为例：

第一步：按下图配置设备的 OpenVPN 参数，确保隧道两端网络参数保持一致，点击应用并保存。



第二步：“认证类型”选择**数字证书**，点击“VPN>>证书管理”导入 CA 证书、公钥、私钥。

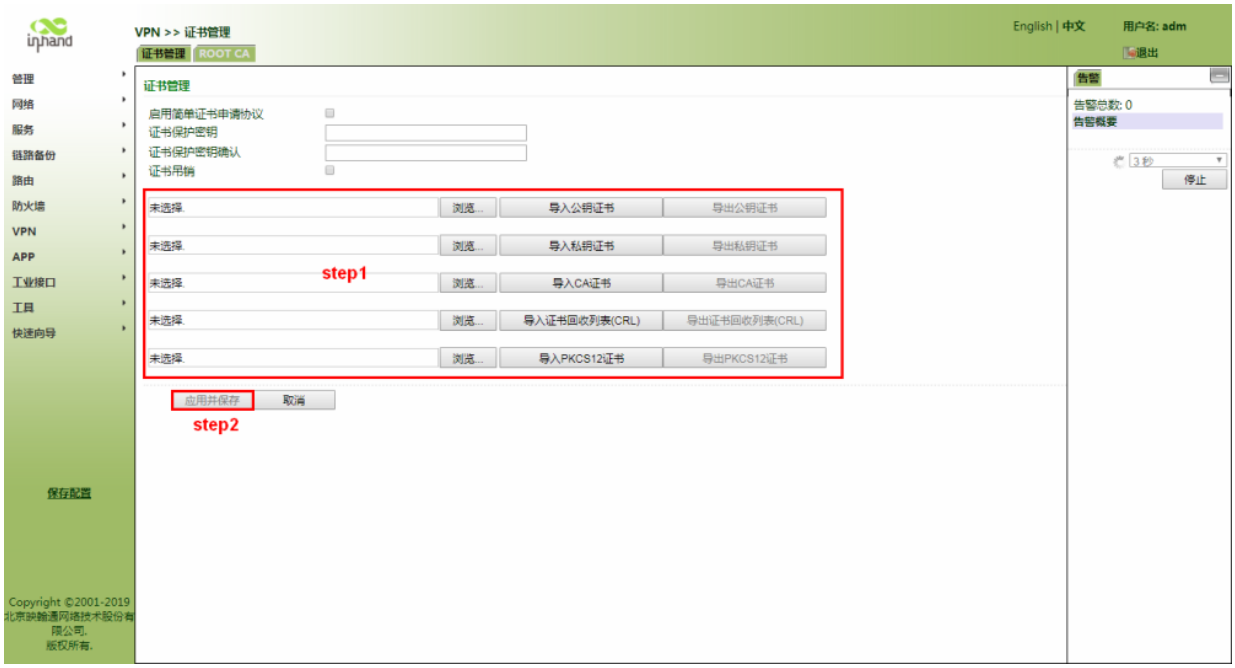
第三步：点击应用并保存。返回“状态”页面查看隧道建立状态。

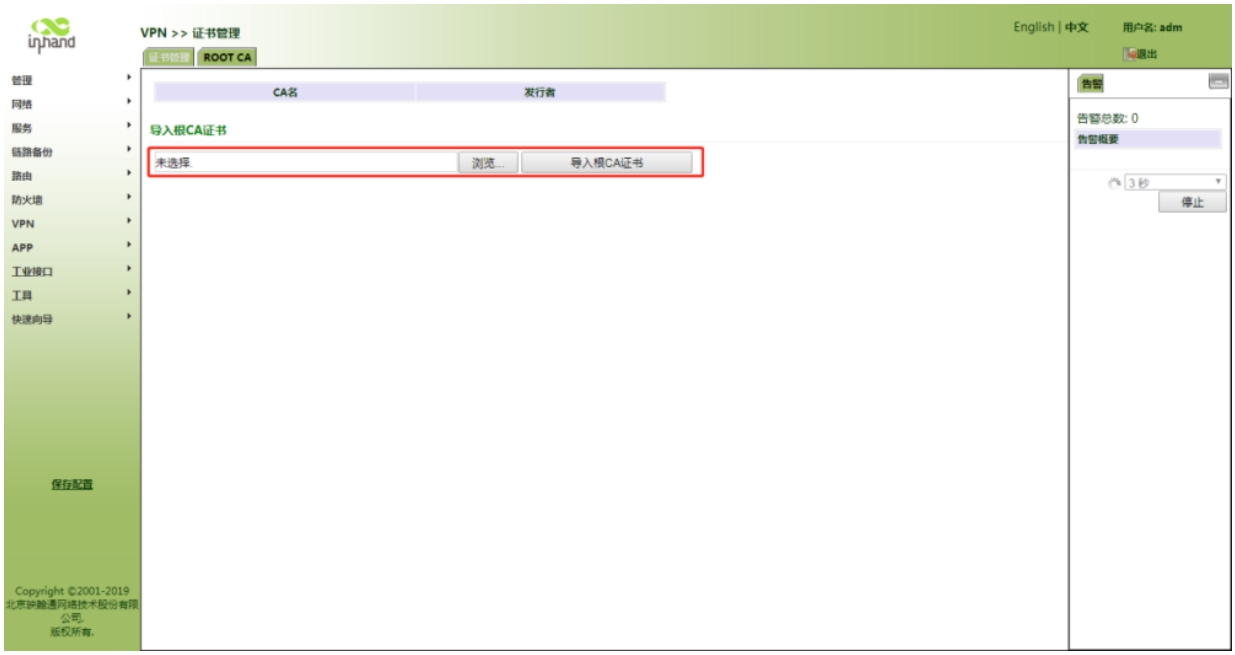
5.3.5 证书管理

可在本页面导入、导出证书。证书用于 IPsec、OpenVPN 服务。

导入证书的设置方法：

点击“VPN>>证书管理>>浏览”选择从证书服务器获得的证书文件，点击导入 XX 证书按钮，然后点击应用并保存。

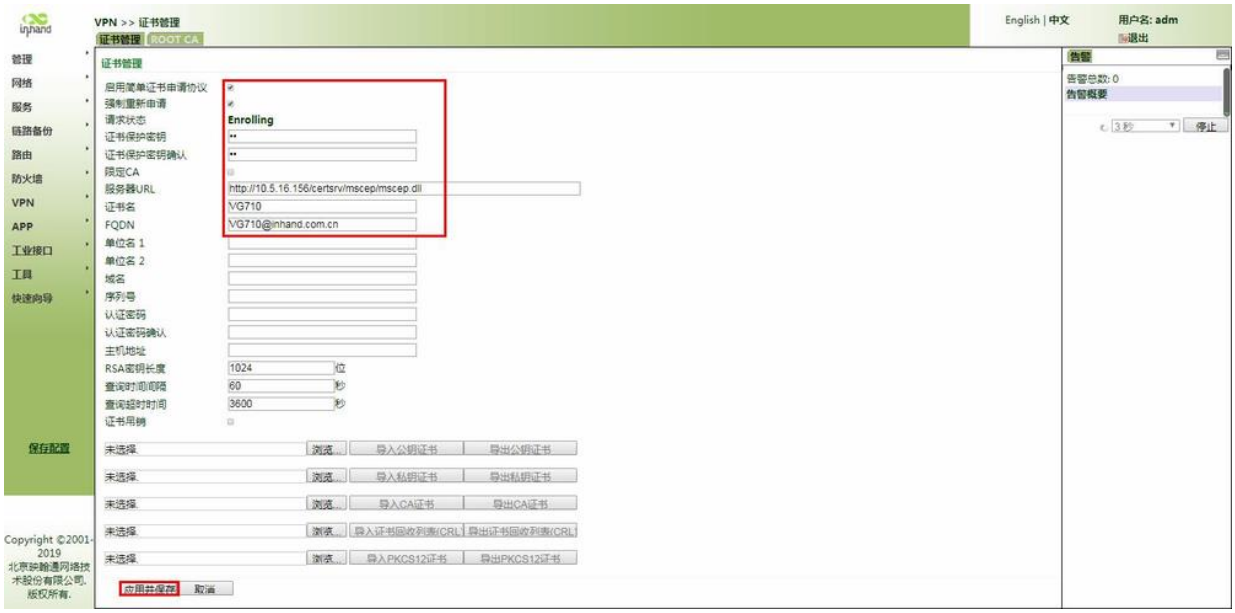




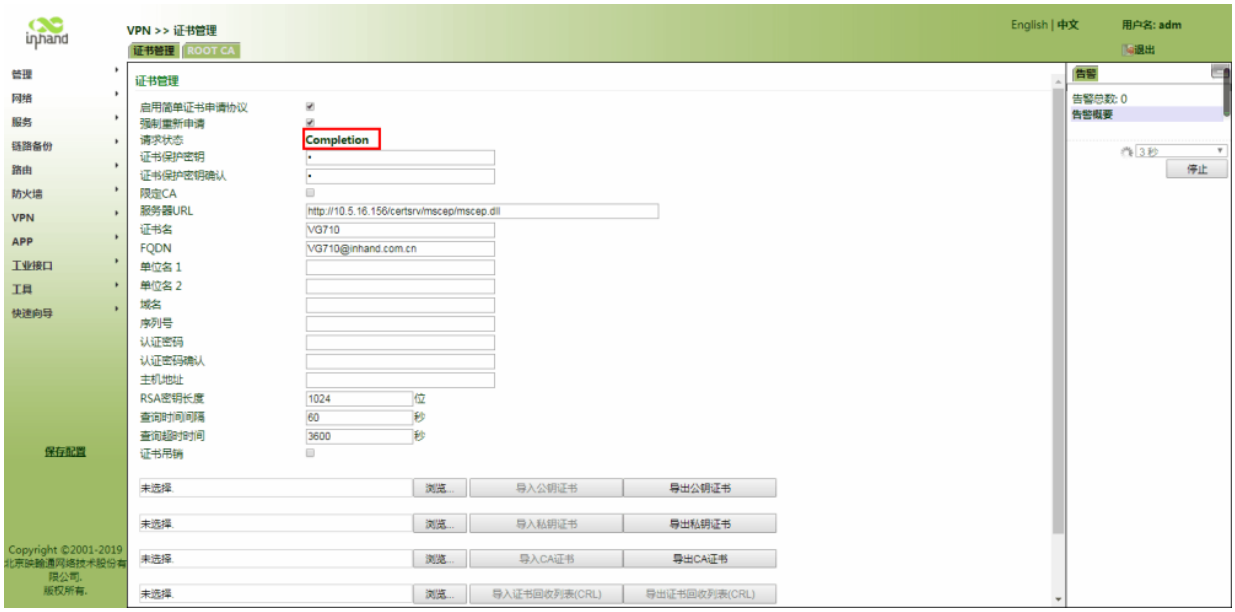
如果没有本地证书，可勾选“启用简单证书申请协议”在线申请证书。

网关在线申请证书的设置方法：

第一步：点击“VPN>>证书管理”勾选启用简单证书申请协议、强制重新申请，填入证书保护密钥及密钥确认，填入证书服务器 URL 地址、证书名和 FQDN，点击应用并保存。



第二步：待服务器颁发证书后，请求状态显示为“Completion”表示证书申请成功。



5.4 服务

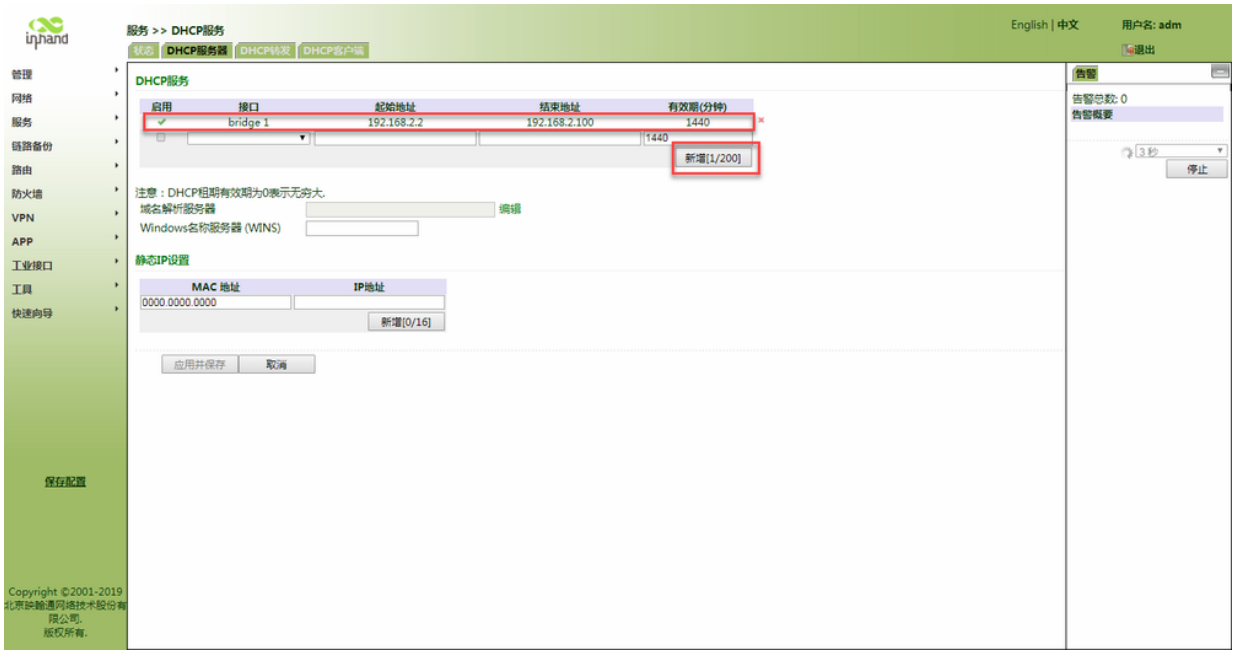
5.4.1 DHCP（自动获取 IP 地址）

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址，以实现 IP 地址的动态配置。

DHCP 服务器与 DHCP 转发功能互斥。

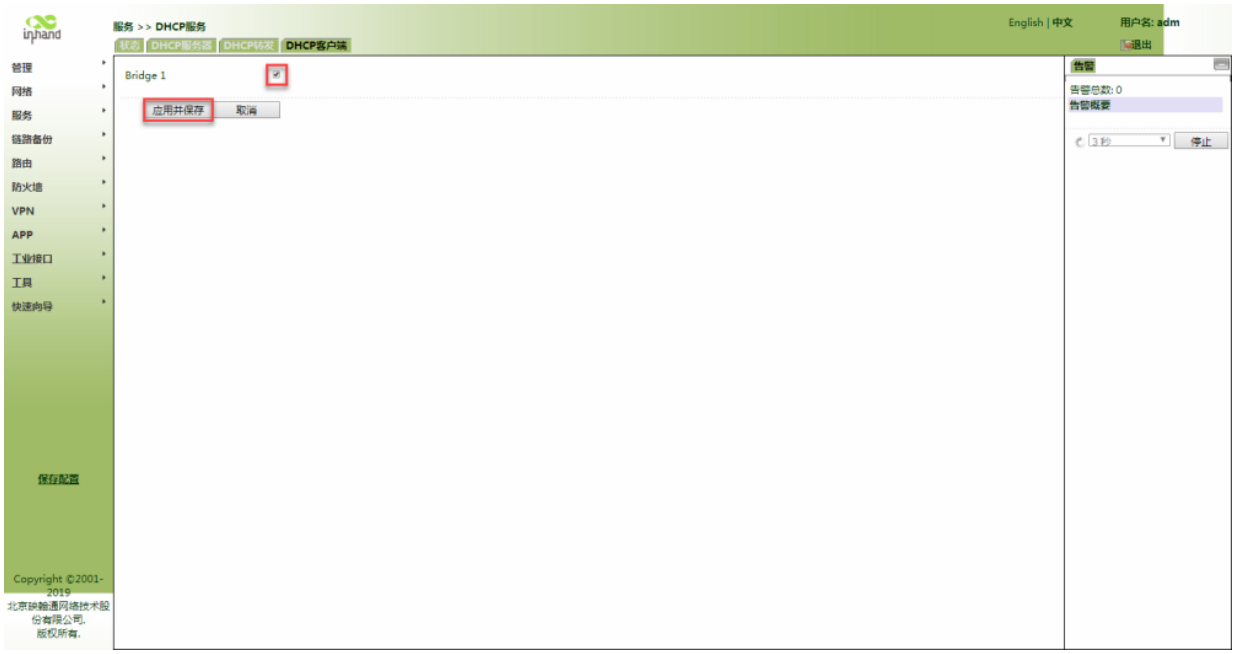
网关作为 DHCP 服务器使用的设置方法：

点击“服务>>DHCP 服务>>DHCP 服务器”在 DHCP 服务栏，勾选启用，选择接口，设置起始和结束 IP 地址，点击新增，然后点击应用并保存。



网关作为 DHCP 客户端使用的设置方法：

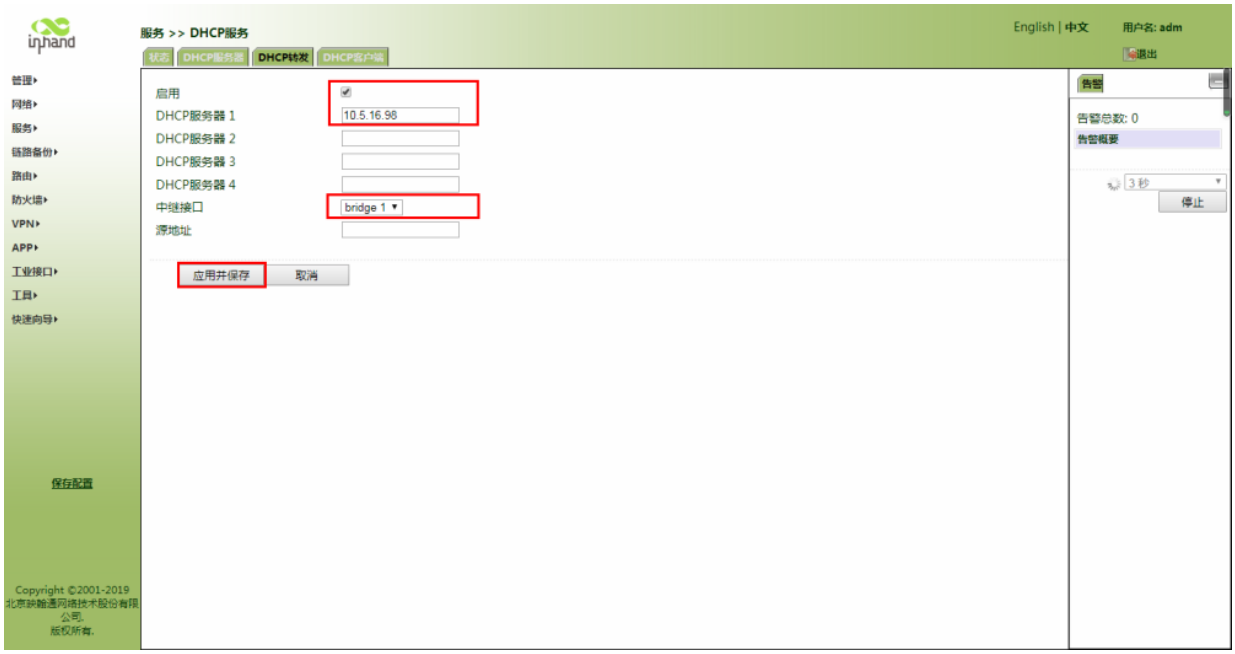
点击“服务>>DHCP 服务>>DHCP 客户端”勾选网关接口，点击应用并保存。



网关 DHCP 转发使用的设置方法：

DHCP 转发也叫做 DHCP 中继代理，它实现了在不同子网和物理网段之间处理和转发 DHCP 信息的功能。

点击“服务>>DHCP 服务>>DHCP 转发”勾选启用，填入服务器地址，选择网关接口，点击应用并保存。

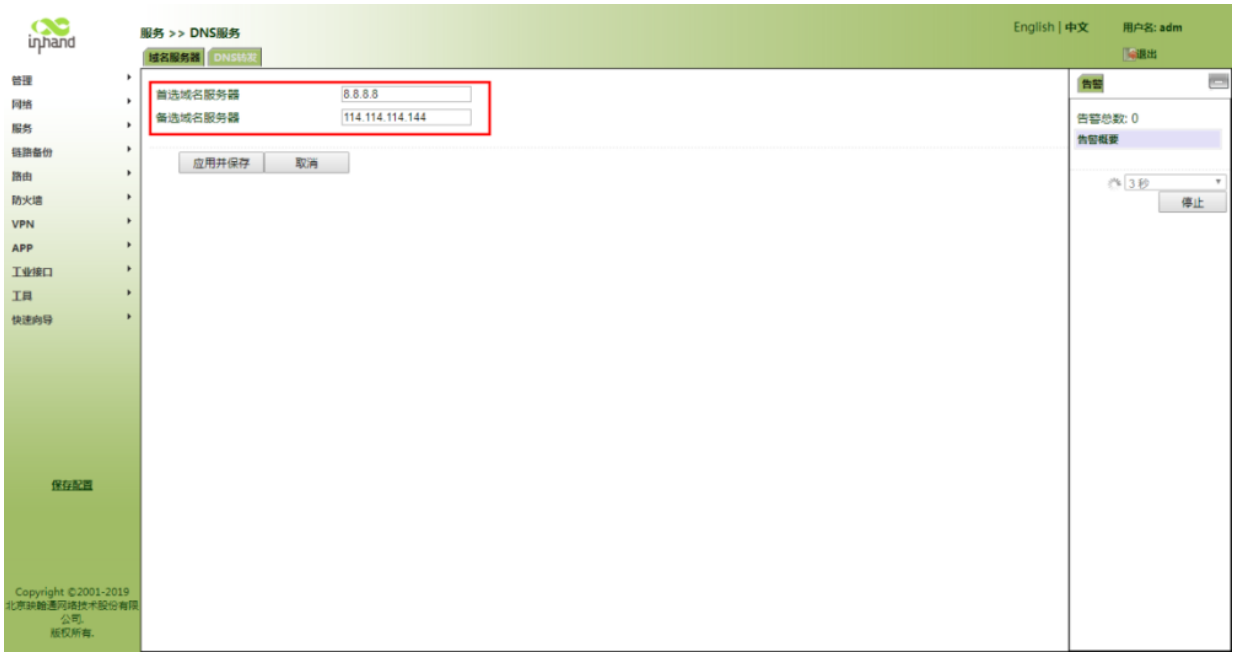


5.4.2 DNS（域名解析）

DNS 是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换。

网关使用 DNS 服务的设置方法：

点击“服务>>DNS 服务>>域名服务器”输入域名服务器地址，点击应用并保存。

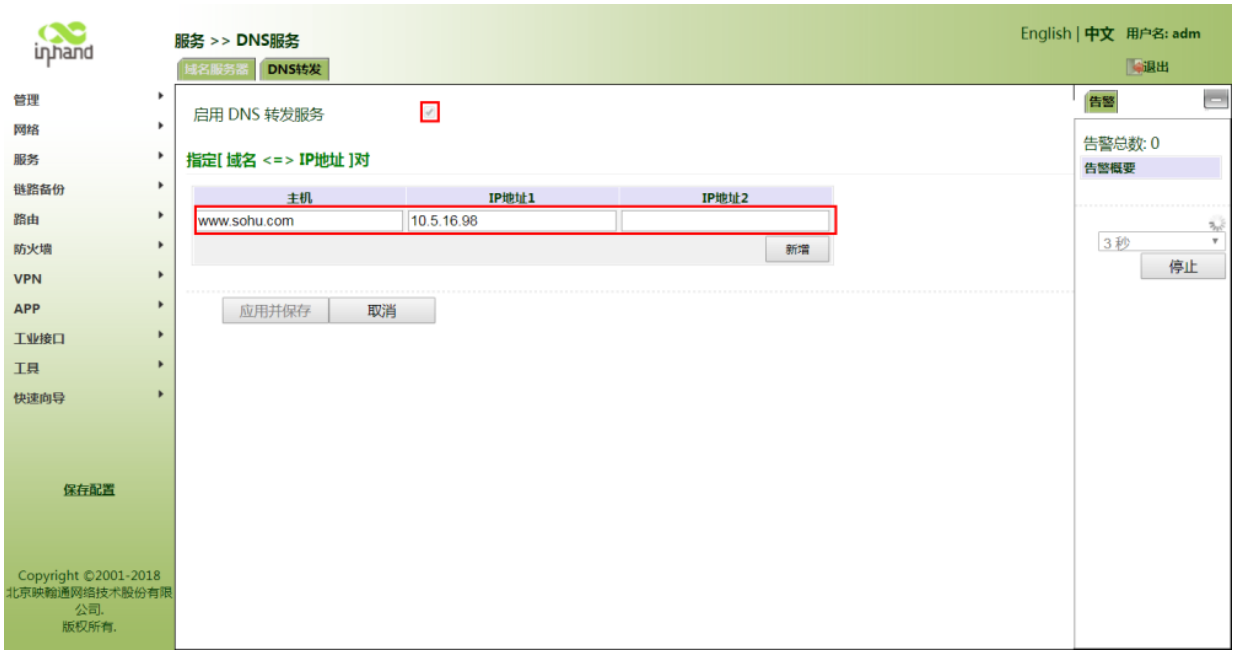


网关使用 DNS 转发服务的设置方法：

设备作为 DNS 代理，在 DNS 客户端和 DNS 服务器之间转发 DNS 请求和应答报文，代替 DNS 客户端进行域名解析。

如果网关开启了 DHCP 服务，会默认开启 DNS 转发功能并且不能关闭。

点击“服务>>DNS 服务>>域名服务器”,启用 DNS 转发服务，设置域名和 IP 地址对应关系，点击新增，然后点击应用并保存。设置完成后，当局域网内 DNS 客户端请求列表中的主机域名，DNS 代理服务器会将对应的 IP 地址应答给客服端。



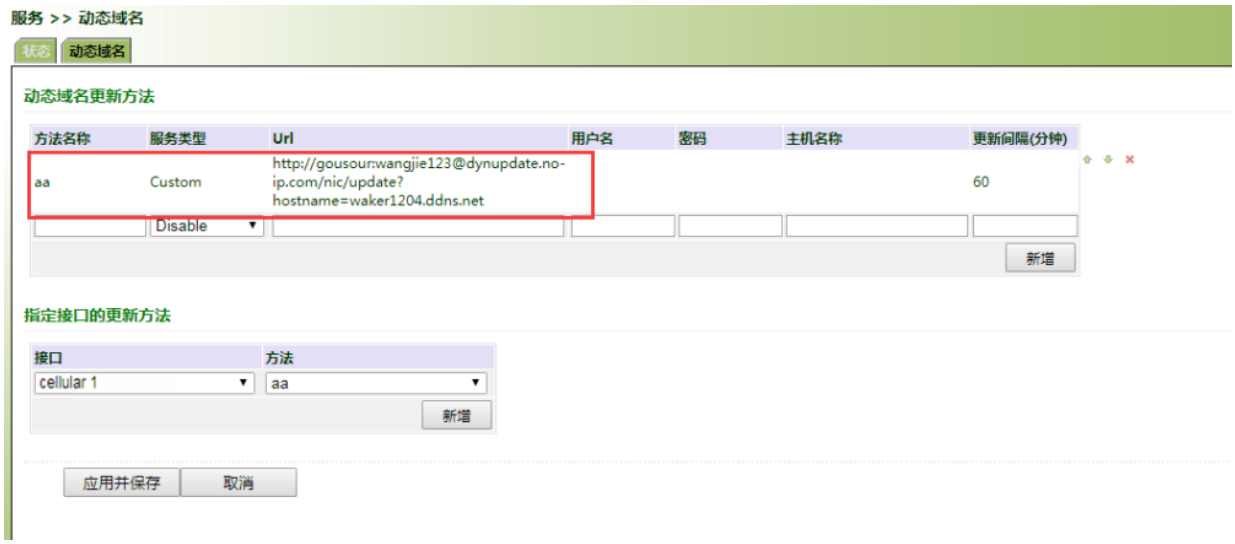
5.4.3 DDNS（动态域名）

DDNS 将设备动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候，客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，而服务器程序负责提供 DDNS 服务并实现动态域名解析。这样我们只要在外部输入我们的域名就可以访问了，即便 IP 换了也是一样的。

网关使用 DDNS 服务的设置方法：

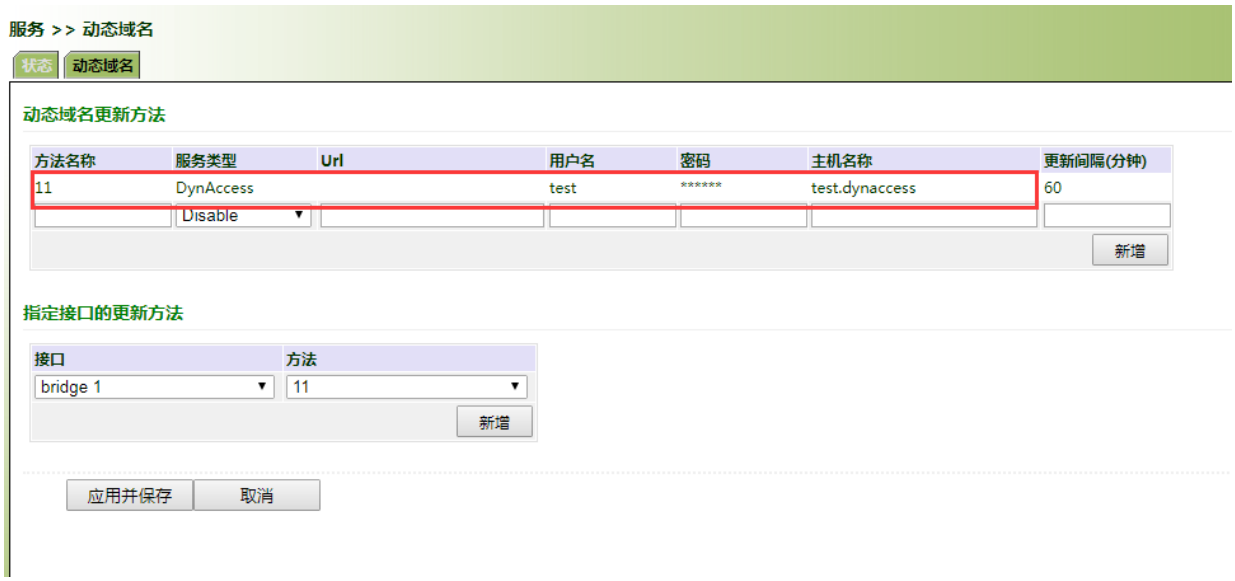
第一步：如果使用定制服务（Custom），“方法名称”自定义填写，“服务类型”选择 Custom，“Url”输入服务器 DDNS 表达式“http://用户名：密码@ddns.oray.com/ph/update?hostname=主机名称”，这个表达式只做参考，实际 Url 是由服务商提供（一般可以在服务商官网找到），点

击新增。

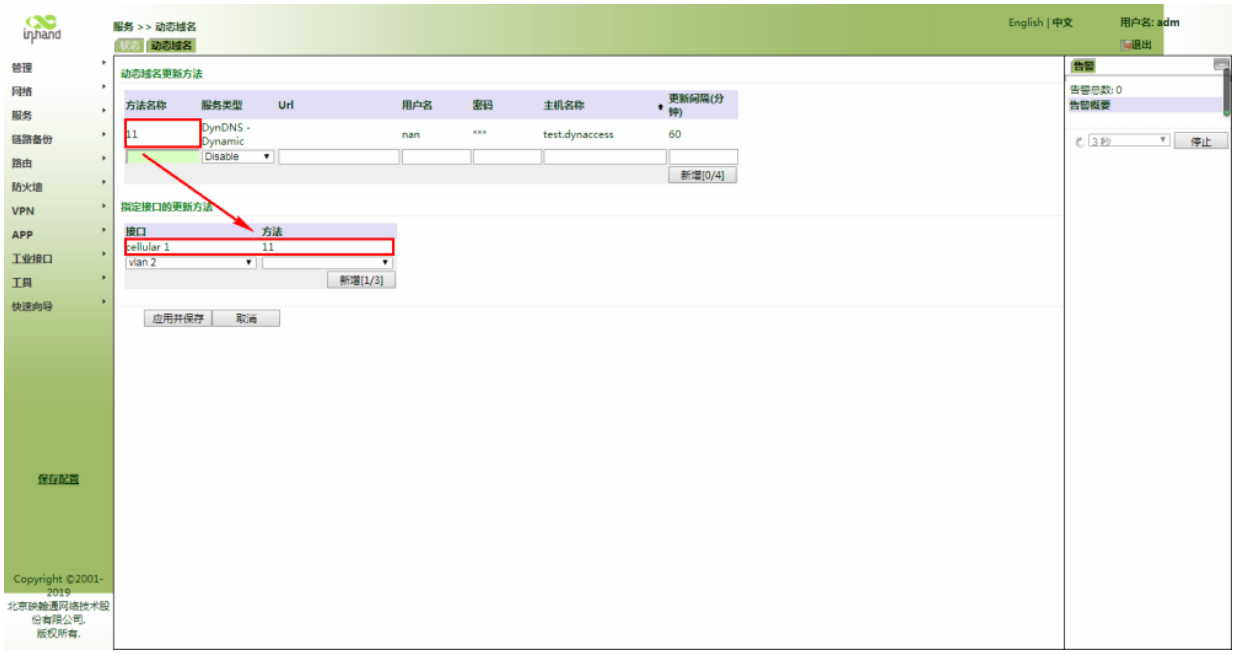


如果使用 Custom 之外的其它普通域名服务器，“方法名称”自定义填写，选择“服务类型”后，用户名、密码和主机名称从服务器获取并填入，点击新增。

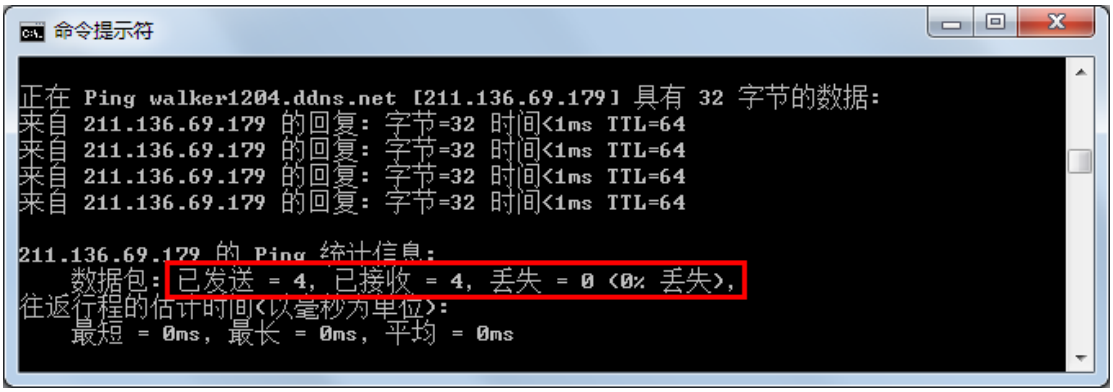
如果选择 Disable 表示不使用 DDNS 服务。



第二步：选择网关接口，填入“动态域名更新方法”中的方法名称，点击新增，然后点击应用并保存，将动态域名更新方法应用给网关接口。



第三步：配置好动态域名保存应用以后等待几分钟，然后 ping 域名服务器的主机名称（域名），确认动态域名服务功能成功应用。

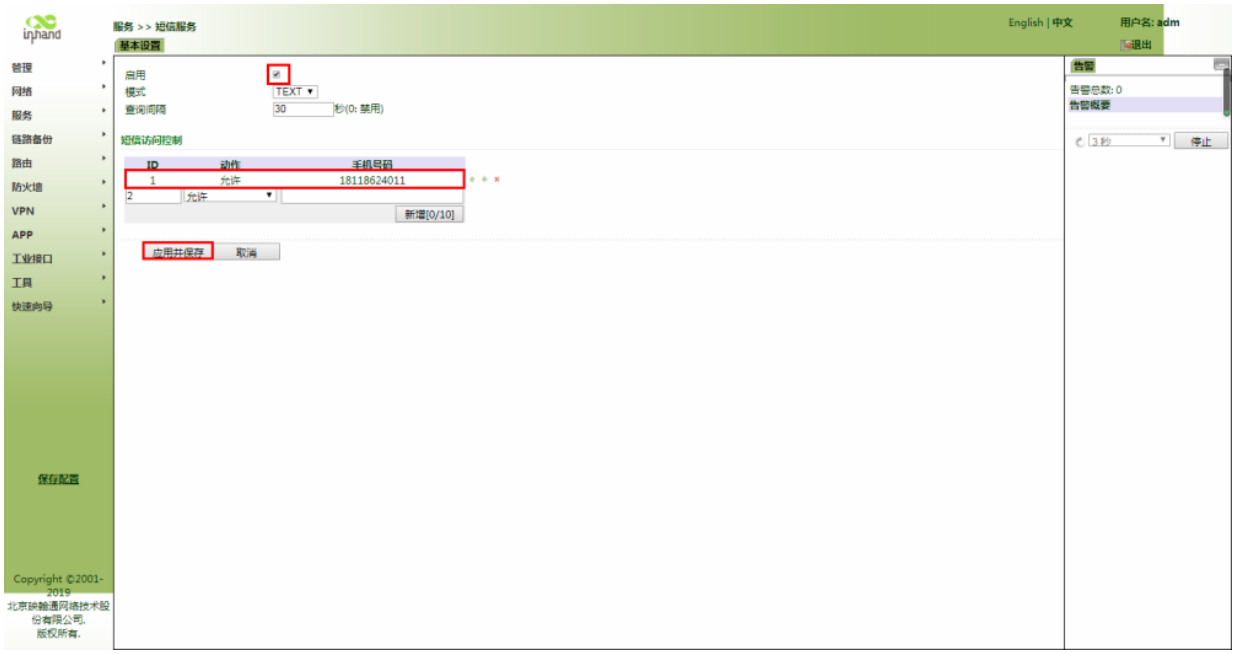


5.4.4 短信服务

启用短信服务，实现手机短信重启设备和手工拨号，部分设备还支持接收短信白名单里的告警信息。

使用手机短信控制网关重启和手工拨号的设置方法：

当拨号口选择短信激活方式时，点击“服务>>短信服务”勾选启用，短信访问控制列表中“ID”自定义填写，“动作”选择允许并输入手机号码，点击应用并保存。配置完成后就可以通过该手机号发送“reboot”指令重启设备，或者发送“cellular 1 ppp up/down”指令使网关重新拨号或断开拨号。

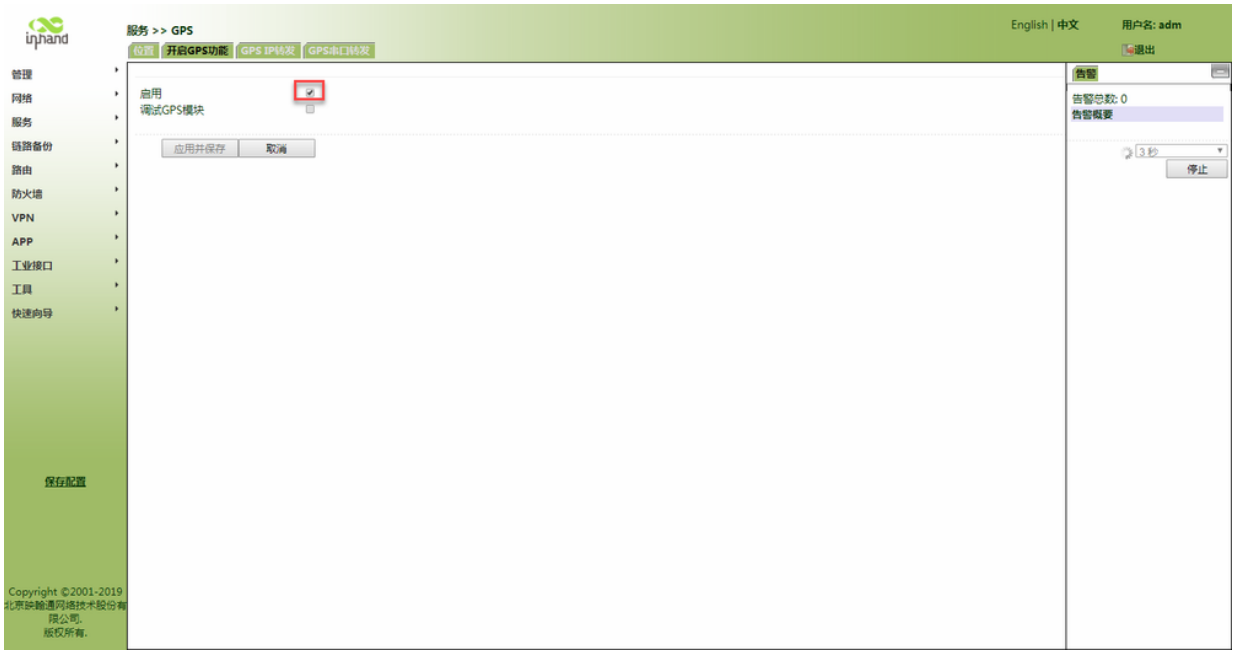


5.4.5 GPS

位置：用于查看简单的位置数据。

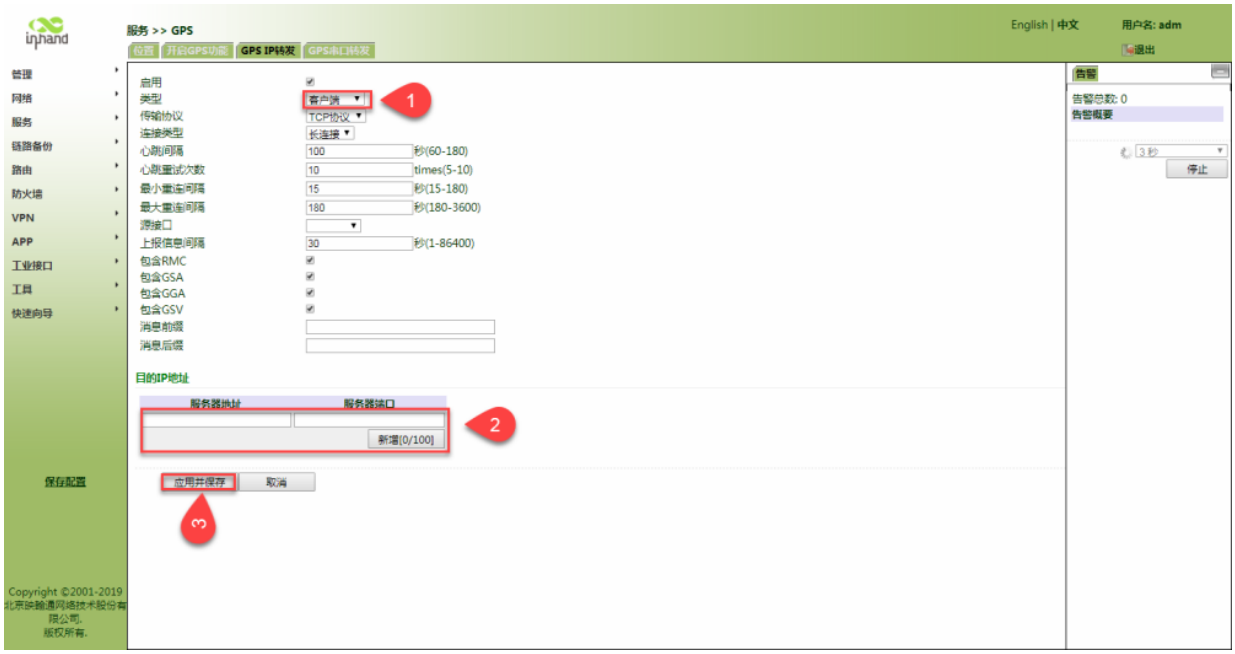
开启网关 GPS 功能的设置方法：

点击“服务>>开启 GPS 功能”勾选启用，点击应用并保存。缺省状态下，保持开启网关的 GPS 功能。



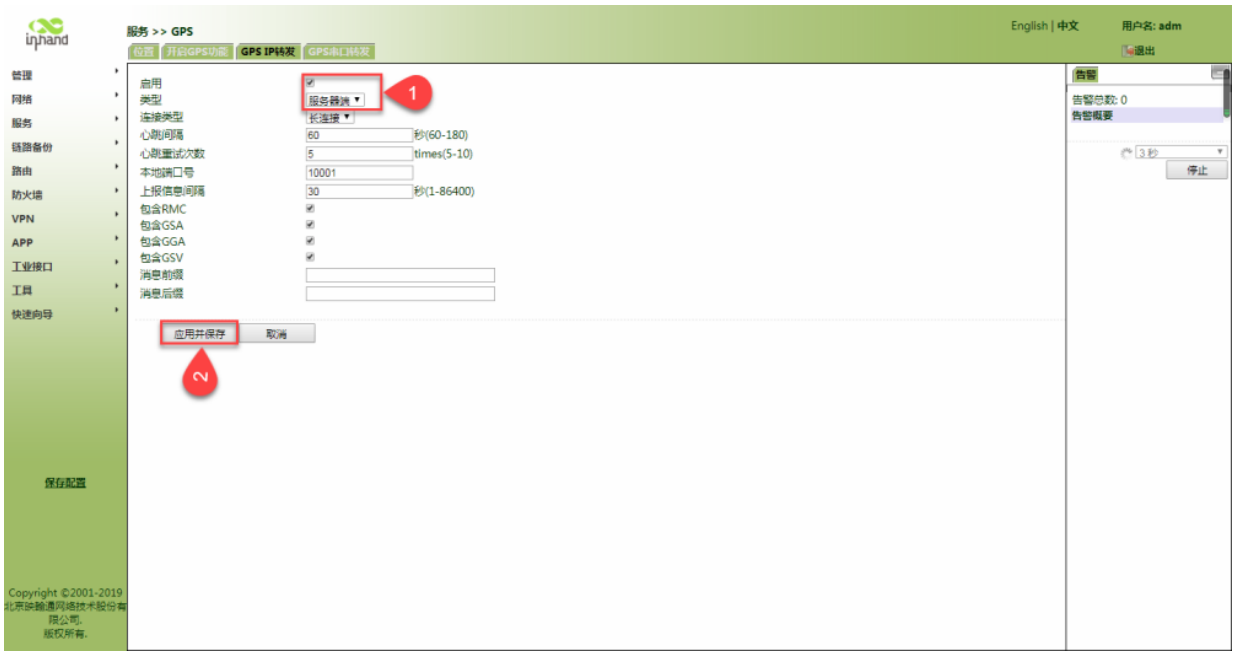
VG710 作为客户端使用 IP 转发 GPS 数据到服务器的设置方法：

点击“服务>>GPS IP 转发”勾选启用，“类型”选择客户端，并在目的 IP 栏输入服务器的地址和端口，点击新增，然后点击应用并保存。



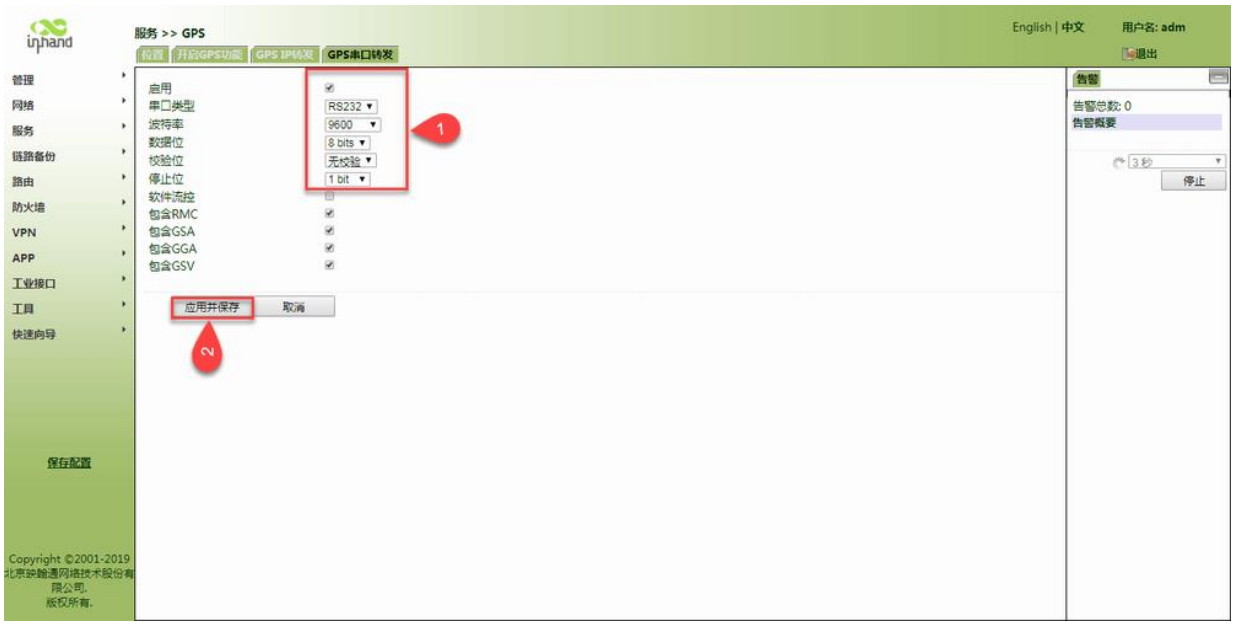
VG710 作为服务器使用 IP 转发 GPS 数据的设置方法：

点击“服务>>GPS IP 转发”勾选启用，“类型”选择服务器端，点击应用并保存。



VG710 使用串口转发 GPS 数据的设置方法:

点击“服务>>GPS 串口转发”勾选启用，根据使用的数据传输接口选择串口类型，波特率、数据位、校验位和停止位必须与当前串口相同，点击应用并保存。

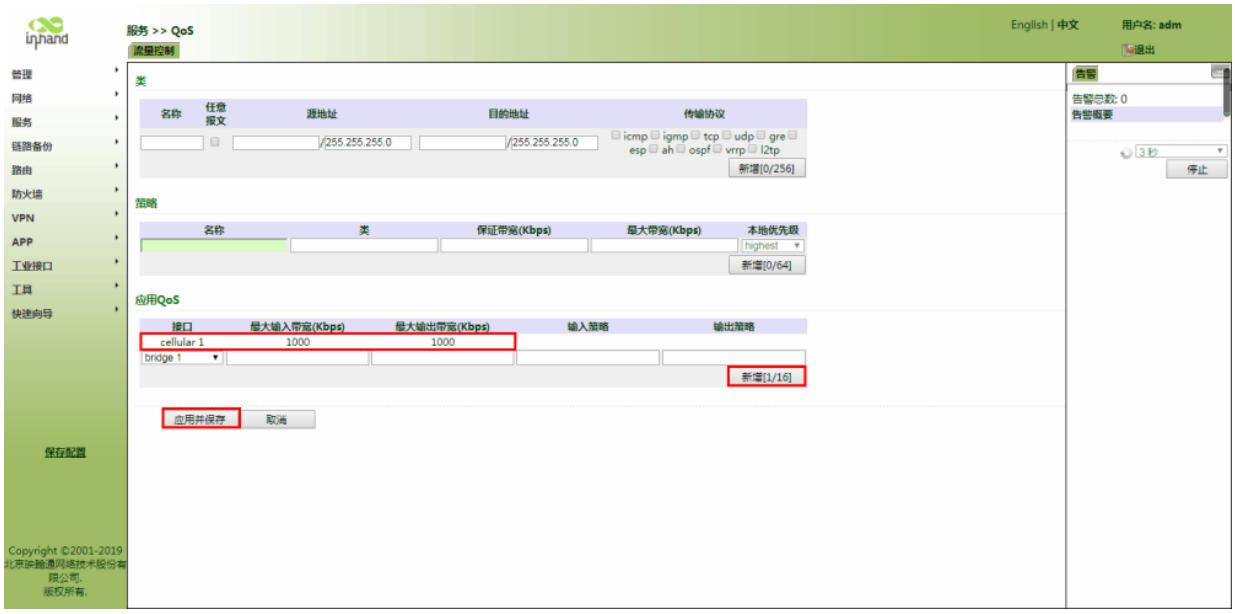


5.4.6 QoS

QoS 指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

网关使用 Qos 技术设置最大输出带宽的设置方法：

点击“QoS>>流量控制>>应用 QoS”选择网关接口，填入最大输出带宽，点击新增，然后点击应用并保存。



网关使用 Qos 技术应用输入、输出策略的设置方法：

第一步：新增网络链路分类。点击“QoS>>流量控制>>类”，勾选是否任意报文，设置好链路源、目的地址，勾选应用 QoS 技术的传输协议，点击新增。

第二步：设置传输策略。点击“QoS>>流量控制>>策略”输入自定义名称，“类”填入类的名称，设置保证带宽、最大带宽参数，并设置策略的优先级，点击新增。

第三步：点击“QoS>>流量控制>>应用 Qos”选择网关接口，“输出策略”填入策略的名称，点击新增，然后点击应用并保存。

5.4.7 流量控制

网关控制流量使用的设置方法：

点击“服务>>流量控制”启用流量控制，设置控制流量使用的参数，点击应用并保存。设置完成后，系统根据本页设置参数在流量超过限额后，进行告警、停止转发或者关闭接口等处理。

5.5 防火墙

5.5.1 访问控制（ACL）

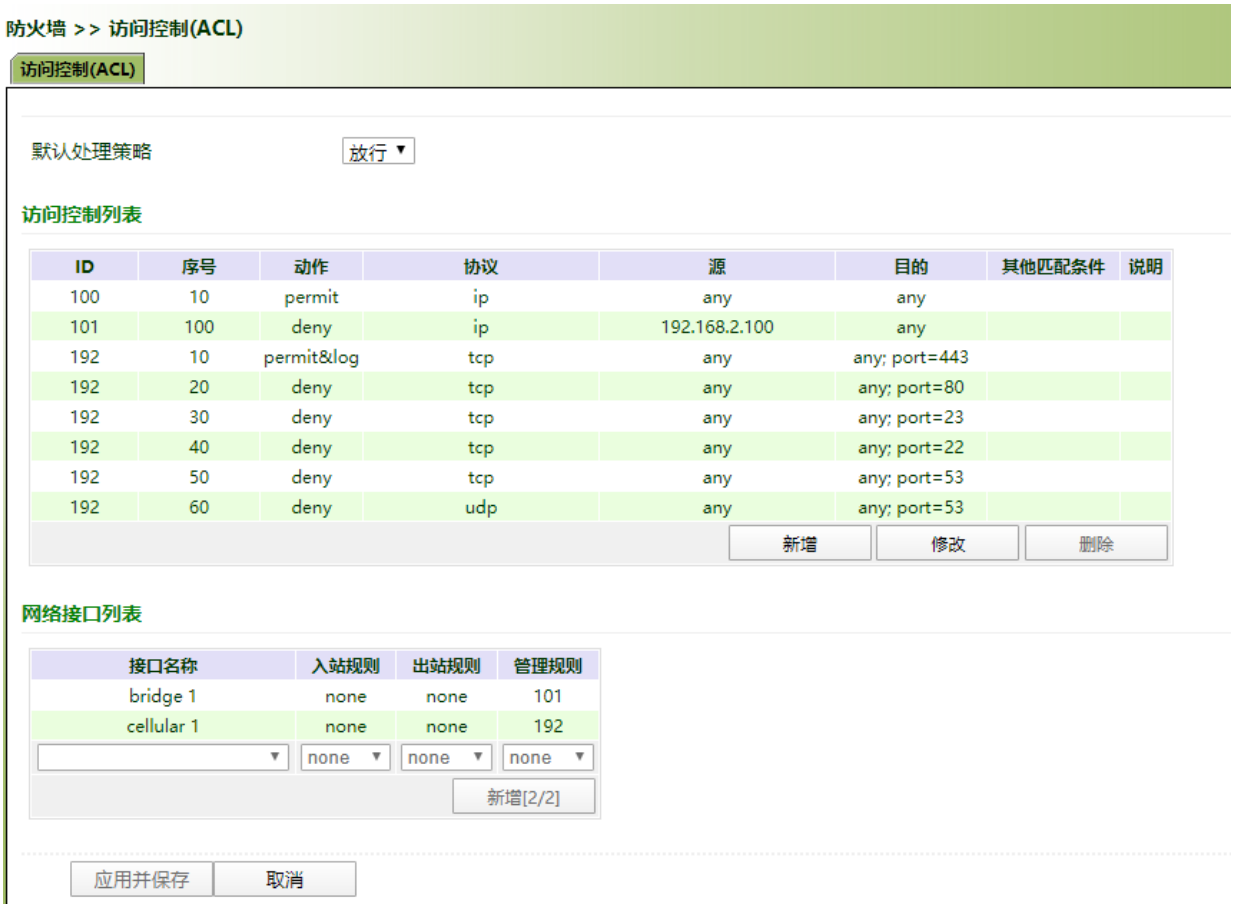
访问控制列表(ACL)是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。

常用情景：默认局域网内（Bridge 1）的设备都能访问外部网络，但是禁止 192.168.2.100 设备访问外部网络。

VG710 的设置方法：

第一步：点击新增访问控制列表。填入 ID 和序号。其中序号数值越小优先级越高。动作选择拒绝。填入源地址 192.168.2.100，源地址反掩码为 0.0.0.0。目的地址不填写代表 0.0.0.0/0 既所有地址。点击应用并保存。

第二步：回到访问控制页面将上述配置的 ID 为 101 规则加入到 Bridge 1 接口的管理规则中并点击新增。点击应用并保存。



5.5.2 网络地址转换(NAT)

当在专用网内部的一些主机本来已经分配到了本地 IP 地址（即仅在本专用网内使用的专用地址），但现在又想和因特网上的主机通信（并不需要加密）时，可使用 NAT 方法。

常用情景：用户想要通过公共网络访问设备局域网内的一个摄像头用于查看当前车辆行驶路况。摄像头地址为 192.168.2.100，开放端口 18000 提供视频服务。

第一步：点击新增“网络地址转换(NAT)规则”，选择动作为 DNAT，源网络为 Outside。转换类型可以选择 IP PORT to IP PORT 也可以选择 INTERFACE PORT to IP PORT。因为拨号上网获取到的公网地址不固定，所以选择 INTERFACE PORT to IP PORT 的方式比较方便。传输协议由于视频服务是 TCP 协议传输，这里选择 TCP。接口选择 cellular 1（蜂窝网络的拨号接口），端口配置为 20000。转换成的 IP 地址和端口则配置为 192.168.200 和 18000。点击应用并保存。

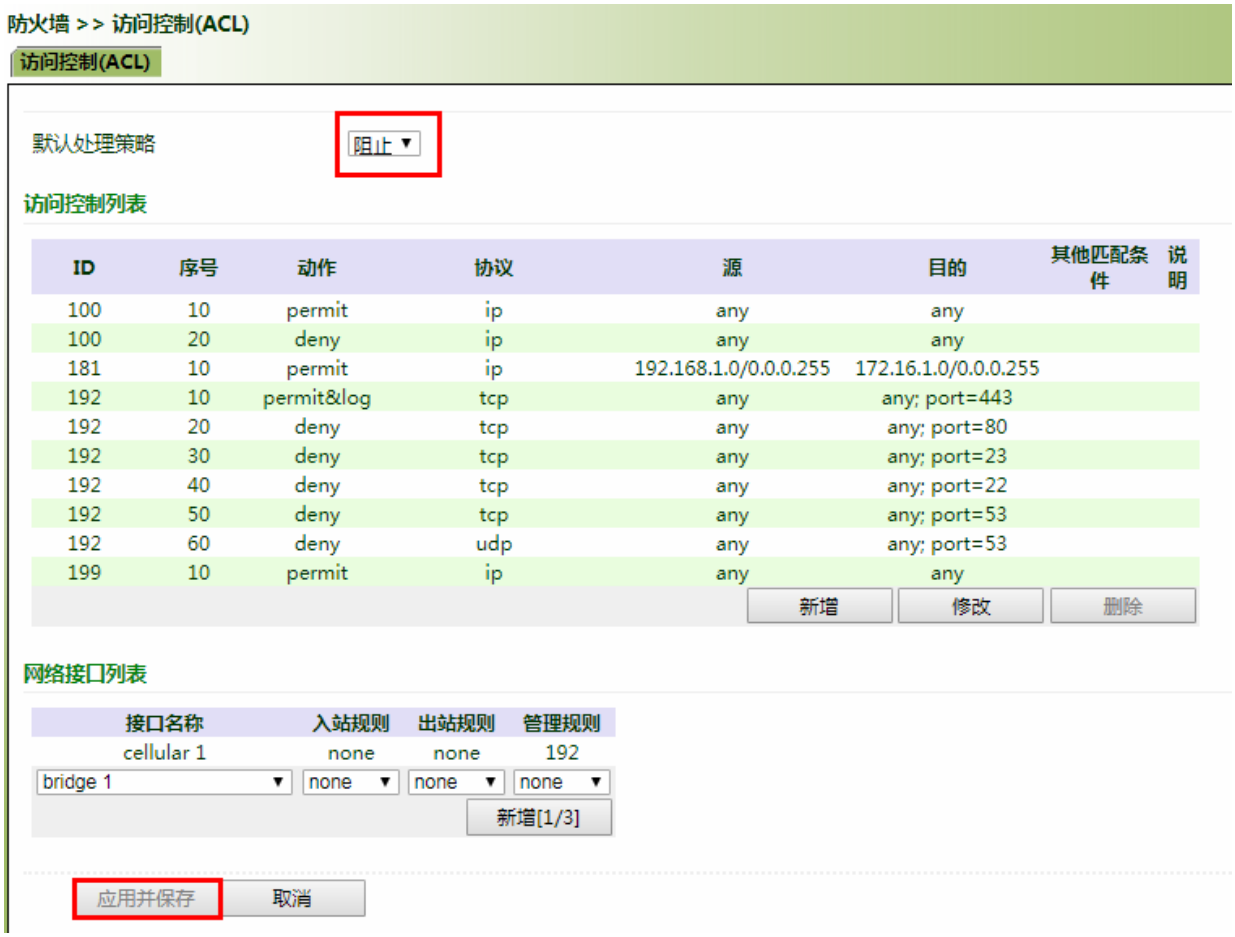
设备会将访问 cellular 1 接口 20000 端口的 TCP 服务，转换到内部 192.168.2.100 18000 端口上。实现访问内部服务的目的。

5.5.3 MAC-IP 绑定

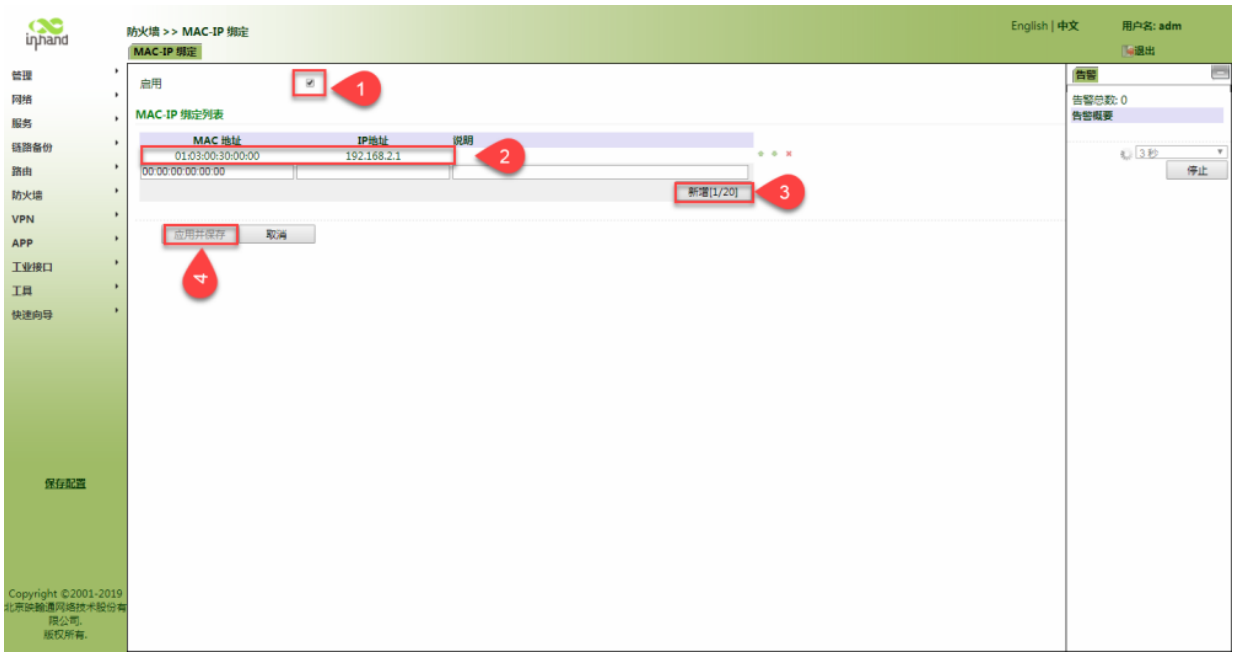
绑定 MAC-IP 后，PC 只有使用绑定 PC 本机 MAC 的 IP 才可以通过设备上公网；其他所有情况都上不了。

下接设备的 MAC 地址与 IP 地址绑定的设置方法：

第一步：进入防火墙控制把默认控制规则设置为阻止。



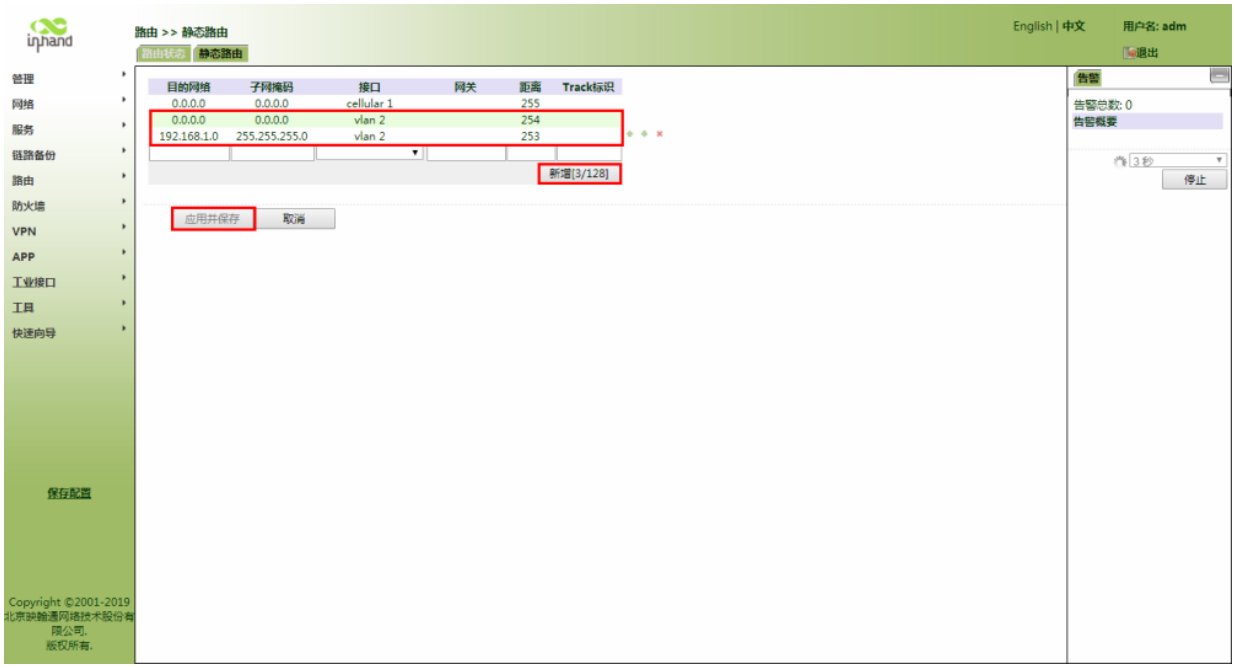
第二步：点击“防火墙>>MAC-IP 绑定”启用 MAC-IP 绑定，输入下接设备的 MAC 地址和 IP 地址，点击新增，应用并保存。



5.6 路由

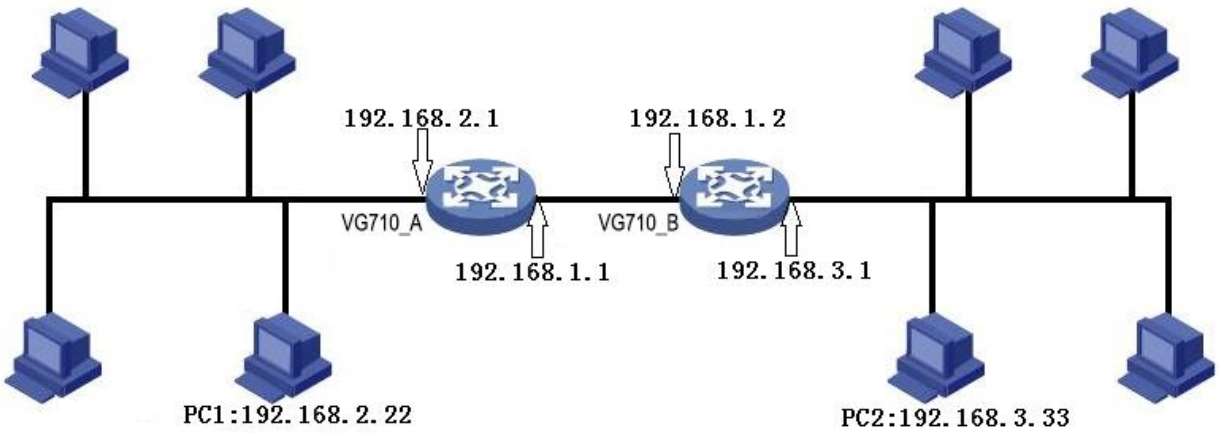
5.6.1 静态路由

根据您的需求填写目的网络、子网掩码、接口或者网关。



5.6.2 动态路由

情景：两个局域网之间建立动态路由，使其可以相互通信，拓扑图如下图所示。



5.6.2.1 RIP

RIP 是一种较为简单的内部动态路由协议，主要用于规模较小的网络中。

情景中 VG710_A 和 VG710_B 之间使用 RIP 协议的动态路由的设置方法：

第一步：配置 VG710_A 网关。点击“路由>>动态路由>>RIP”启用 RIP 协议，“网络”配置 VG710_A，宣告该 VG710_A 的路由条目。

第二步：配置网关 B。

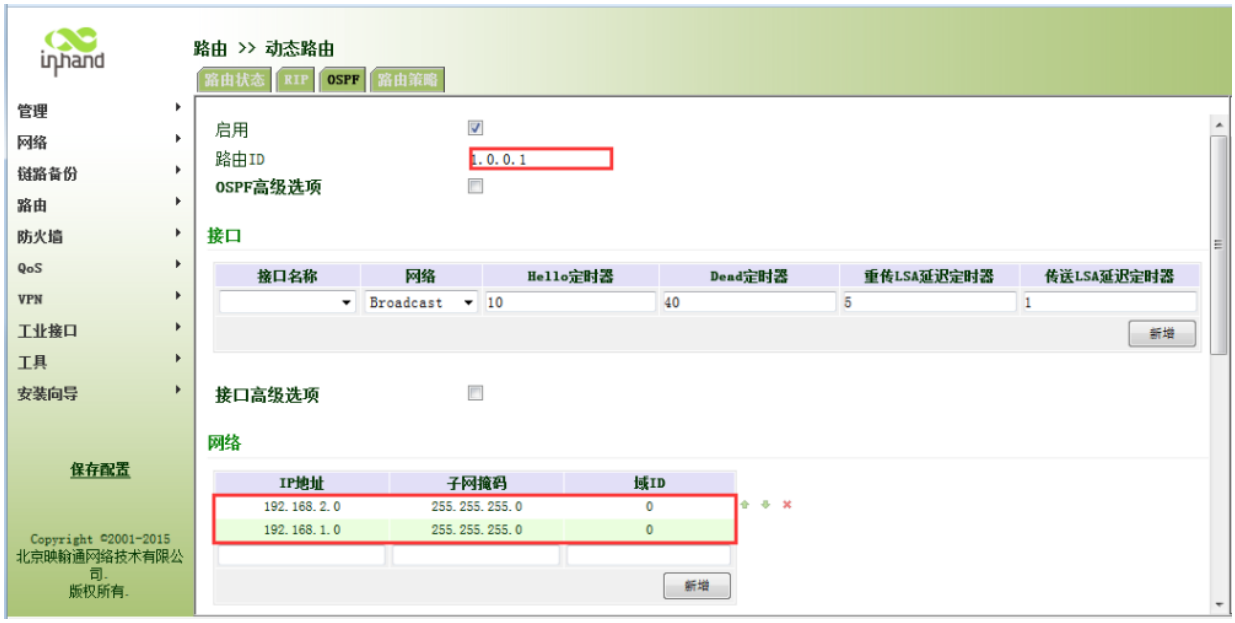
第三步：配置完成后，如果 PC1 和 PC2 可以相互通信，动态路由添加成功。

5.6.2.2 OSPF

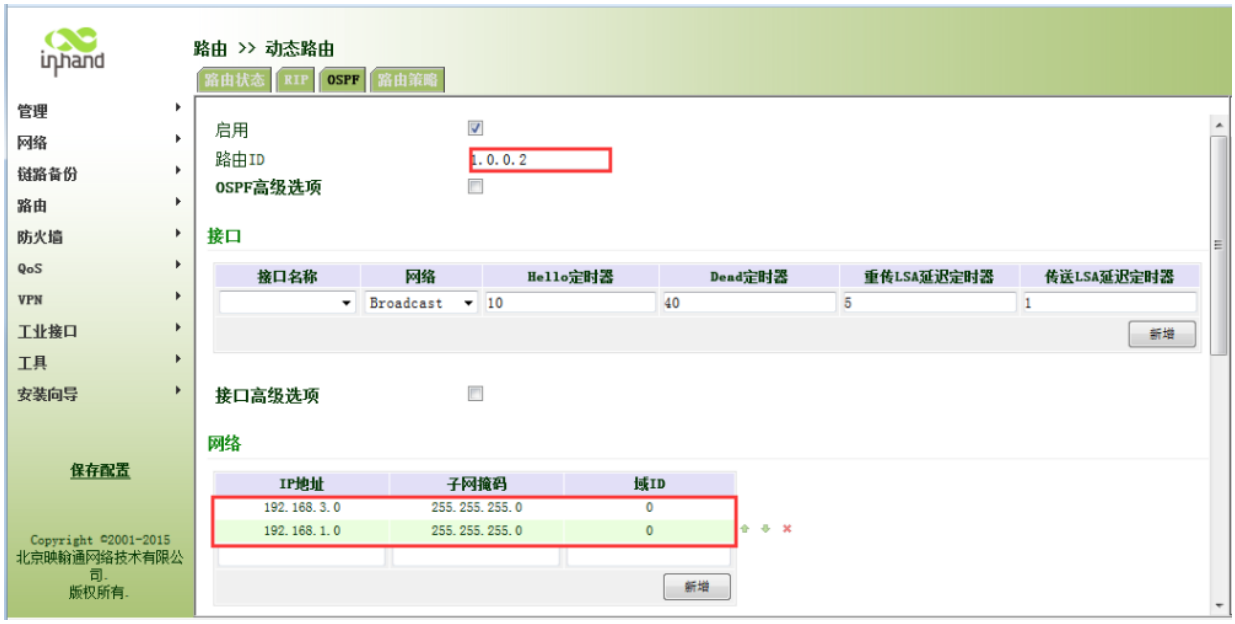
OSPF 开放最短路径优先协议是一个基于链路状态的内部网关协议,主要用于规模较大的网络中。

情景中 VG710_A 和 VG710_B 之间使用 OSPF 协议的动态路由的设置方法：

第一步：配置 VG710_A 网关。点击“路由>>动态路由>>OSPF”，“路由 ID”自定义填写但保证为一个 IP 号，“网络”表中配置 VG710_A，宣告该 VG710_A 的路由条目。



第二步：配置 VG710_B 参数。

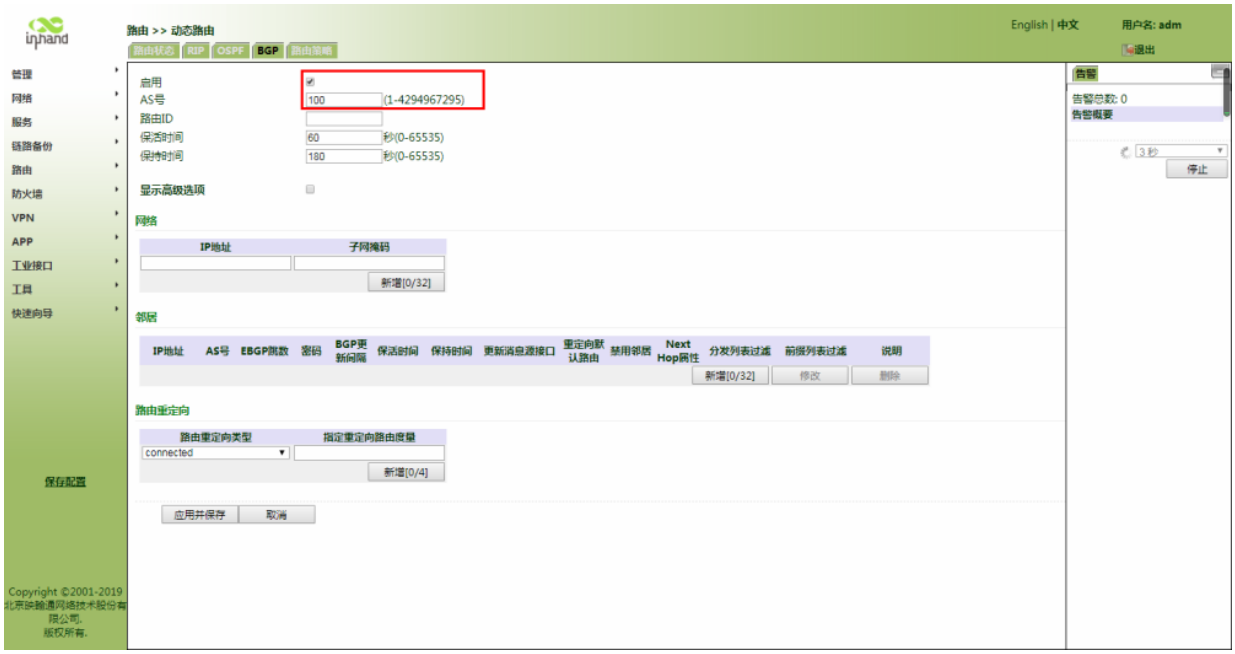


第三步：配置完成后，如果 PC1 和 PC2 可以相互通信，动态路由添加成功。

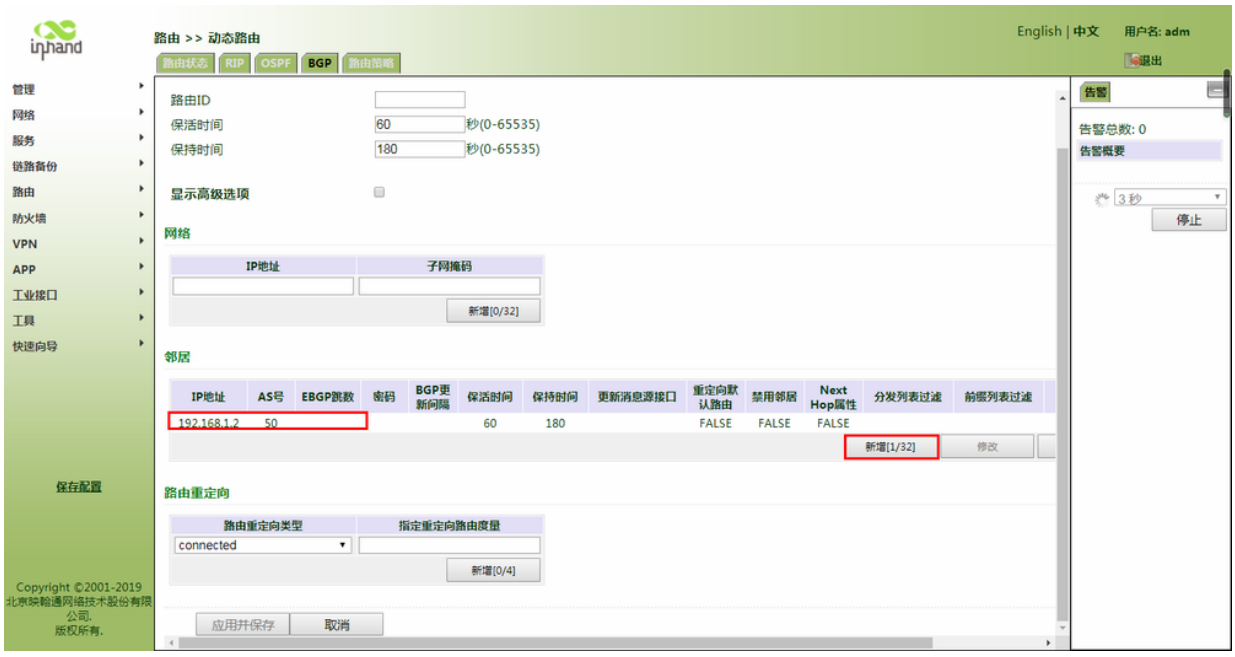
5.6.2.3 BGP

情景中 VG710_A 和 VG710_B 之间使用 BGP 协议的动态路由的设置方法：

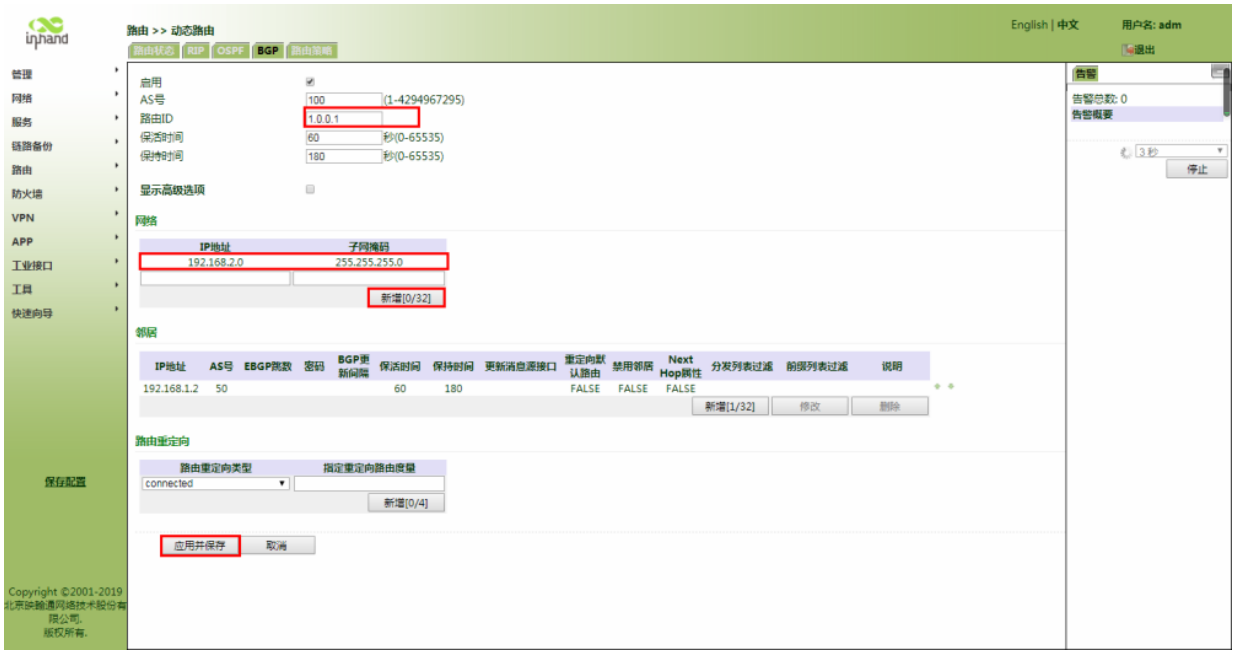
第一步：配置 VG710_A 网关。点击“路由>>动态路由>>BGP”，勾选启用，“AS”号自定义填写。



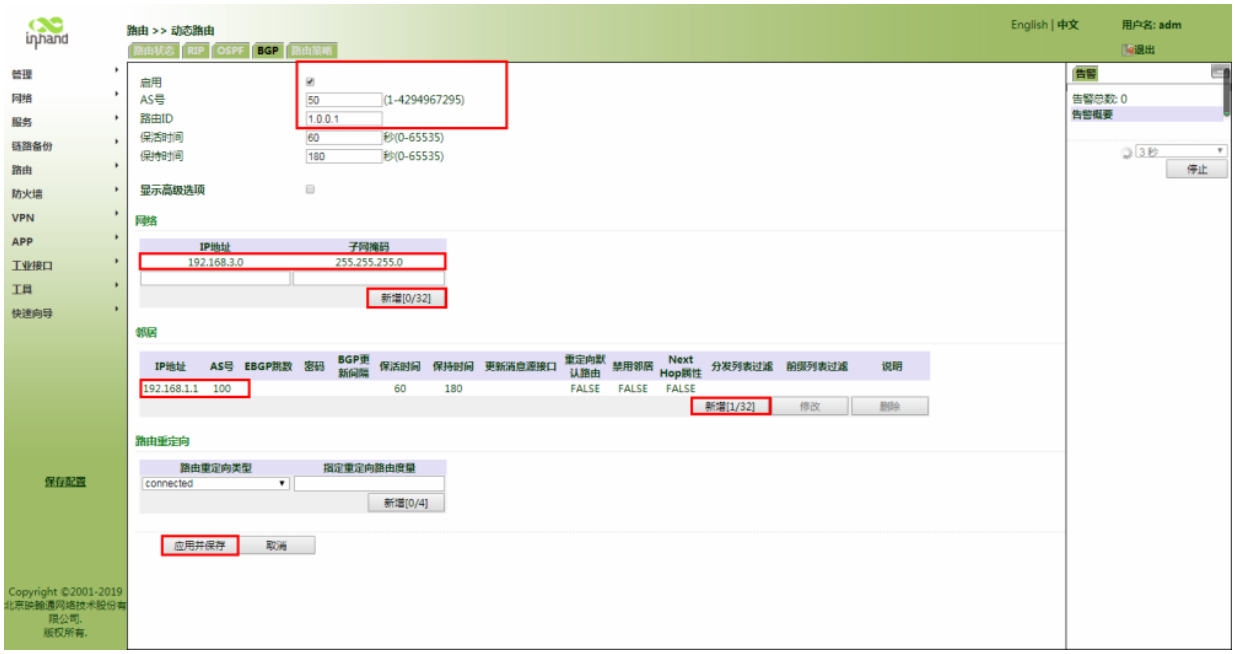
第二步：“邻居”栏，点击新增，配置 VG710_B 的 IP:192.168.1.2，“AS 号”自定义填写，点击应用并保存。



第三步：“路由 ID”自定义填写但必须是一个 IP 号，并在“网络”栏，配置 VG710_A，点击新增，宣告该 VG710_A 的路由条目。然后点击应用并保存。



第四步：配置 VG710_B 参数。与 VG710_A 参数相同或者对应。



第五步：配置完成后，如果 PC1 和 PC2 可以相互通信，动态路由添加成功。

5.7 链路备份

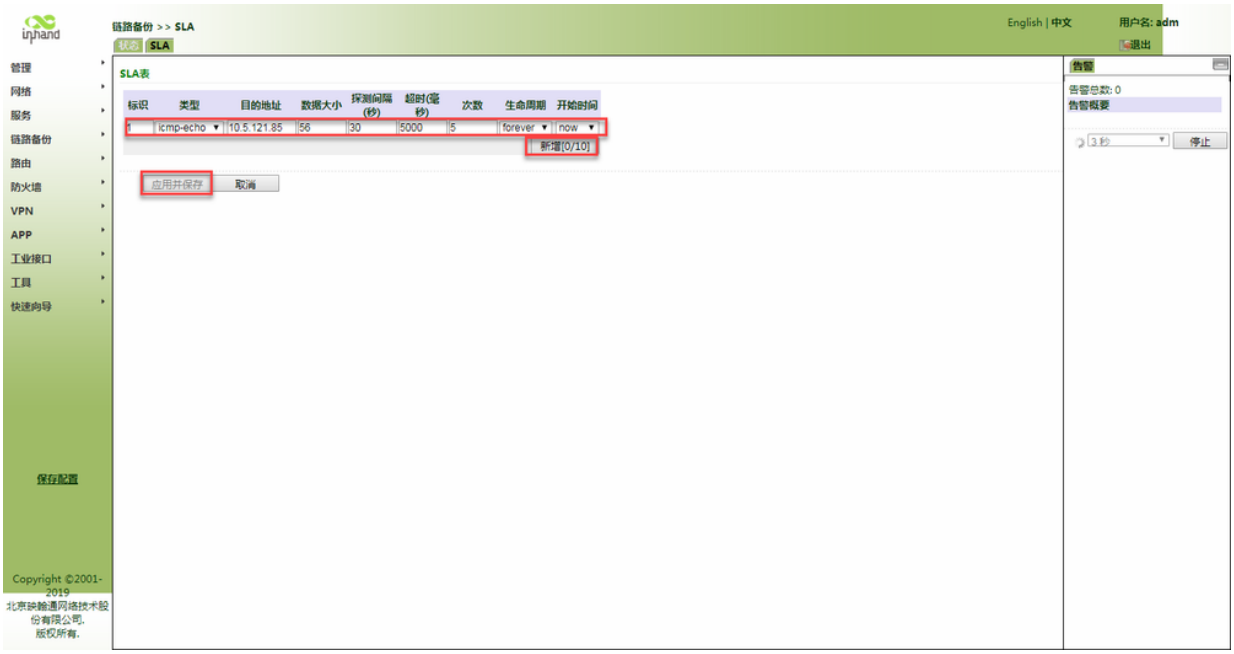
5.7.1 SLA

用于探测网关连接到 ISP 的链路是否出现故障。

网关新增一条 SLA 探测的设置方法：

点击“链路备份>>SLA>>新增”，“目的地址”输入被探测 IP 地址，其它参数自定义填写，点击新增，然后点击应用并保存。

超时（单位：毫秒）：即超时多长时间算一次探测失败；次数：即探测失败多少次为链路故障。



5.7.2 Track 模块

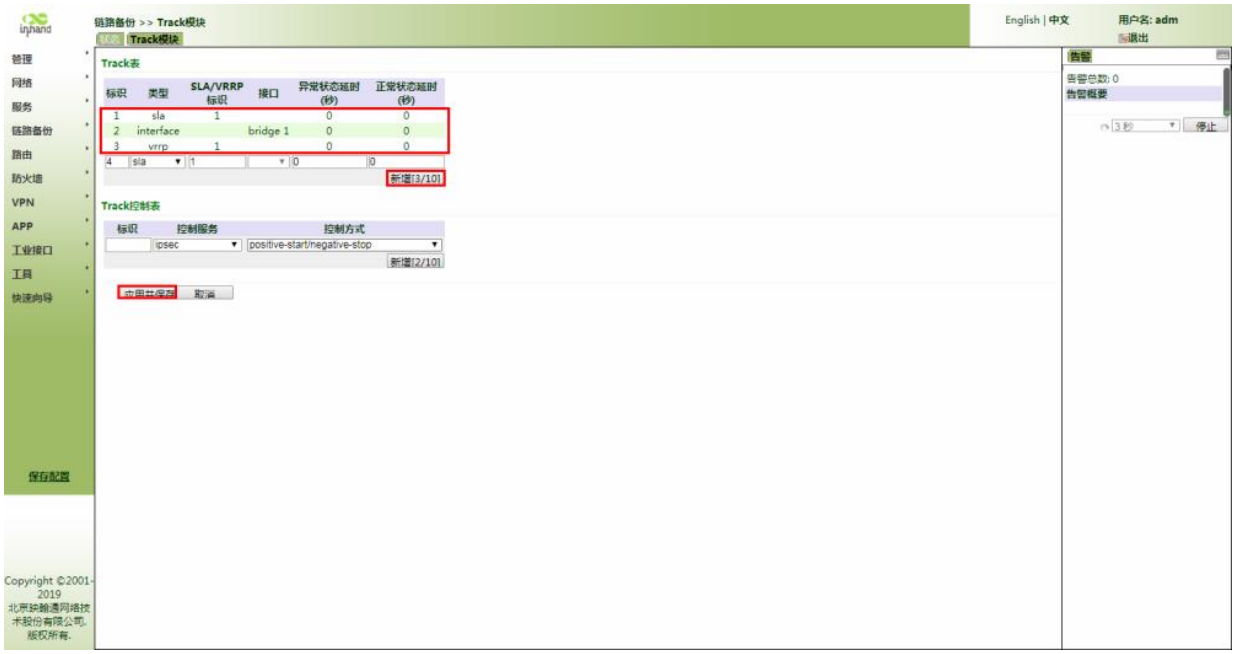
目前可以与 Track 模块实现联动功能的应用模块包括： VRRP、静态路由、接口备份。如果探测成功，对应 Track 项的状态为 Positive；失败为 Negative；

VG710 新增一条 Track 的设置方法：

点击“链路备份>>Track 模块>>Track 表”，“标识”自定义填写，“类型”选择 sla/interface/vrrp，“SLA/VRRP 标识”根据 SLA 表中的标识填写，“异常状态延时”和“正常状态延时”自定义填写，点击新增，点击应用并保存。

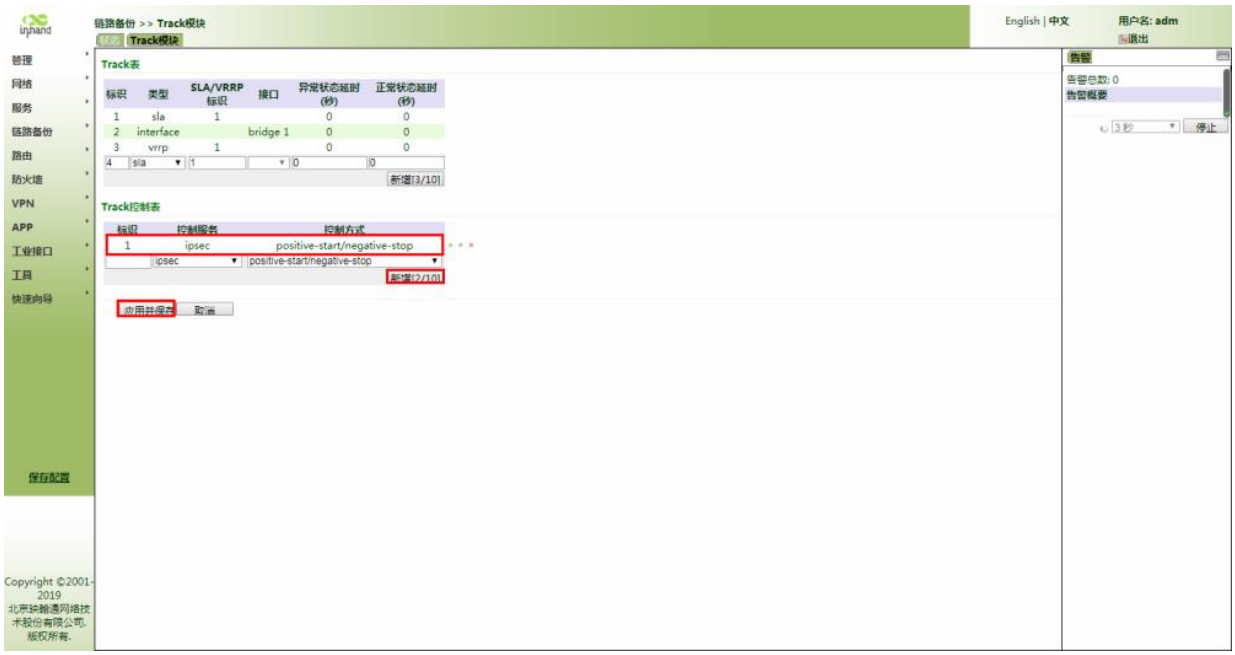
异常状态延时：当出现异常状态时，可根据设置的时间延迟切换(0 代表立即切换)；

正常状态延时：当故障恢复时，可根据设置的时间延迟切换(0 代表立即切换)。



VG710 新增一条 IPsec Track 的设置方法：

点击“链路备份>>Track 模块>>Track 表”，“标识”自定义填写，“positive-start/negative-stop”表示 track 探测状态为 positive 时，启动服务 IPsec 服务，track 探测状态为 negative 时停止 IPsec 服务。



5.7.3 VRRP

情景：若多个网关同时连接到一个网络中，其中 A 作为主机使用，为 A 网关做一个备份，当 A 网关出现故障时，B 网关可以代替 A 网关暂时作为主机使用。

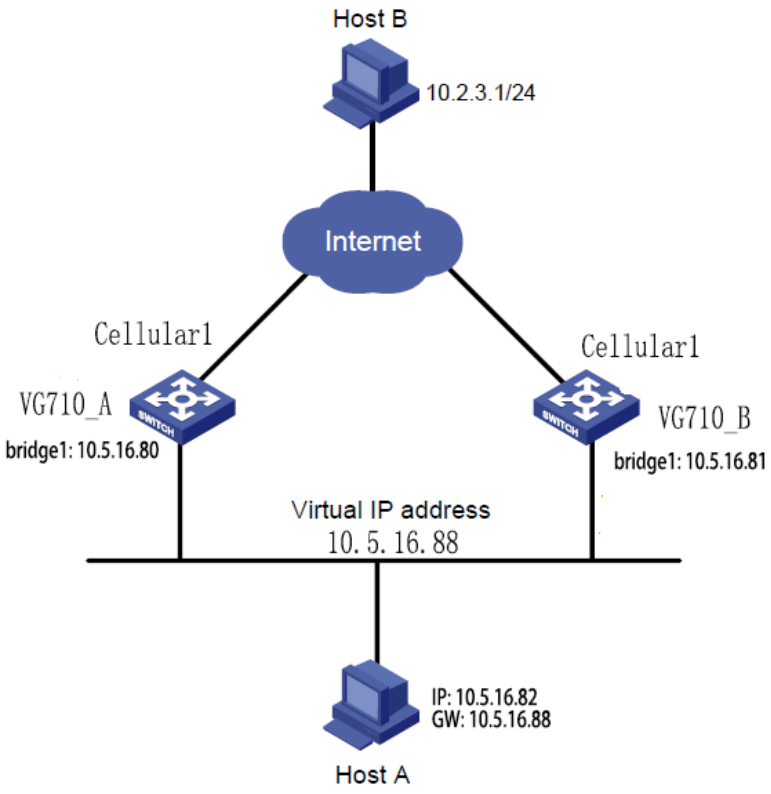
1. 组网需求

主机 A 把网关 A 和网关 B 组成的 VRRP 备份组作为自己的缺省网关，访问 Internet 上的主机 B。

VRRP 备份组构成：

- 备份组号为 1
- 备份组虚拟网关的 IP 地址为 192.168.2.254/24
- 网关 A 做 Master
- 网关 B 做备份路由，允许抢占

2. 组网图



网关	与 Host A 相连以太网接口	与 Host A 相连接口 IP 地址	优先级	工作模式
VG710_A	bridge1	10.5.16.80	110	抢占
VG710_B	bridge1	10.5.16.81	100	抢占

VG710_A 为主网关，VG710_B 为备份网关的设置方法：

第一步：配置 VG710_A。

点击“链路备份>>VRRP”，“虚拟路由 ID”自定义填写，选择 VG710_A 网关接口，输入虚拟 IP 地址，配置接口优先级为 110，点击新增。

单击导航树中的“链路备份>>VRRP”进入“VRRP 状态”界面，查看 VRRP 状态。

第二步：配置 VG710_B。

点击“链路备份>>VRRP”，配置接口优先级为 100，点击新增。

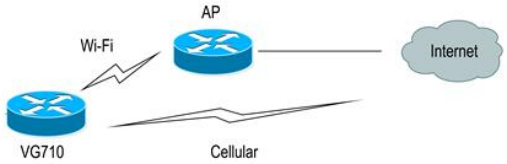
单击导航树中的“链路备份>>VRRP”进入“VRRP 状态”界面，查看 VRRP 状态。

虚拟路由器ID	接口	VRRP状态	优先级	Track状态
1	bridge 1	备份路由	100	-

正常情况下，VG710_A 行使网关的职能，当 VG710_A 关机或出现故障，VG710_B 将接替行使网关的职能。设置抢占方式的目的是当 VG710_A 恢复工作后，能够继续成为 Master 行使网关的职能。

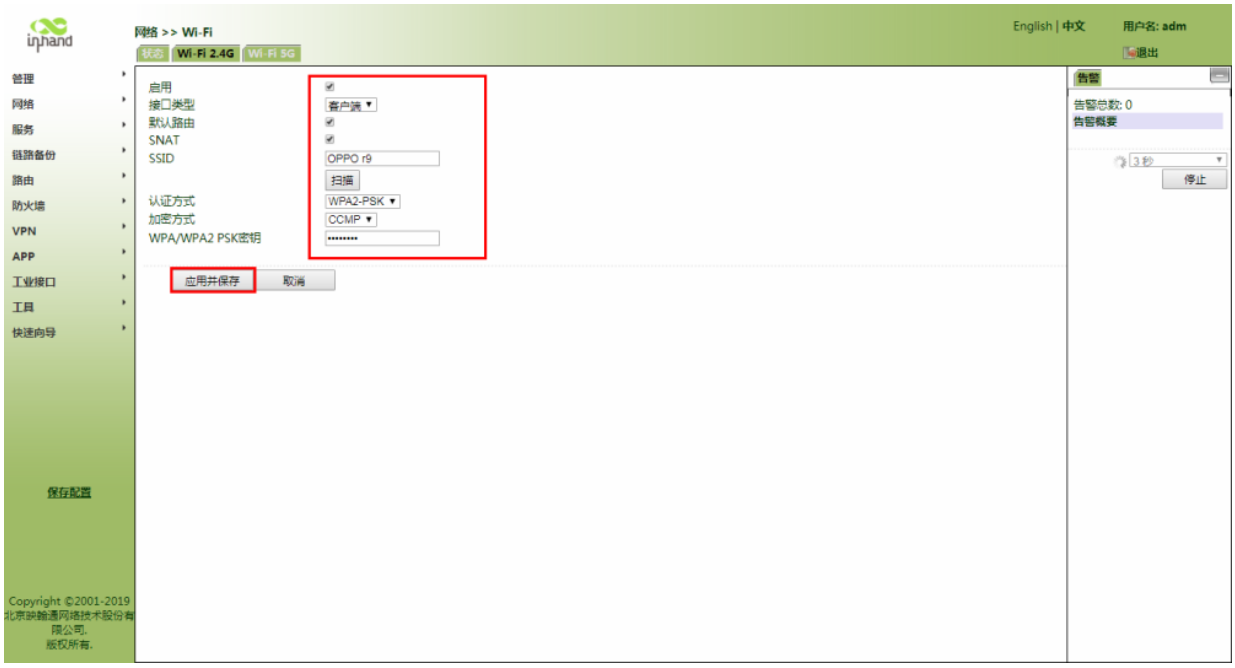
5.7.4 接口备份

情景：VG710 通过 Wi-Fi 上网，创建网关接口备份，使 VG710 在 Wi-Fi 故障时通过拨号上网，拓扑图如下所示。

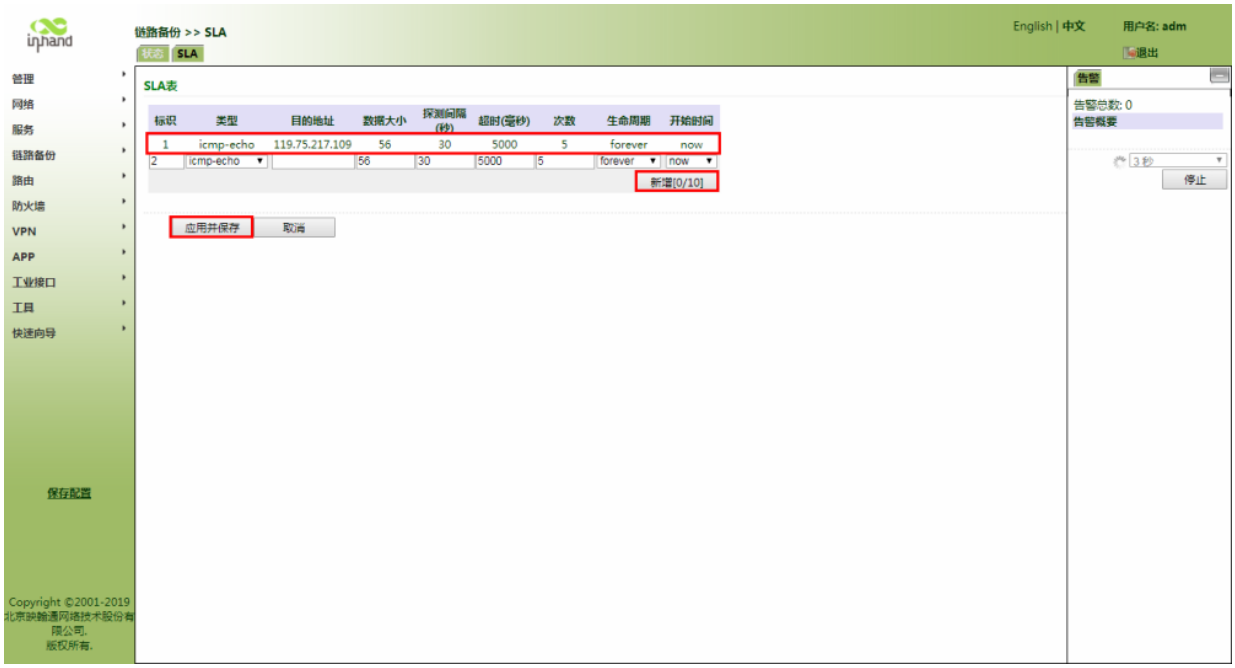


网关创建接口备份的设置方法：

第一步：使 VG710 通过 Wi-Fi 上网。

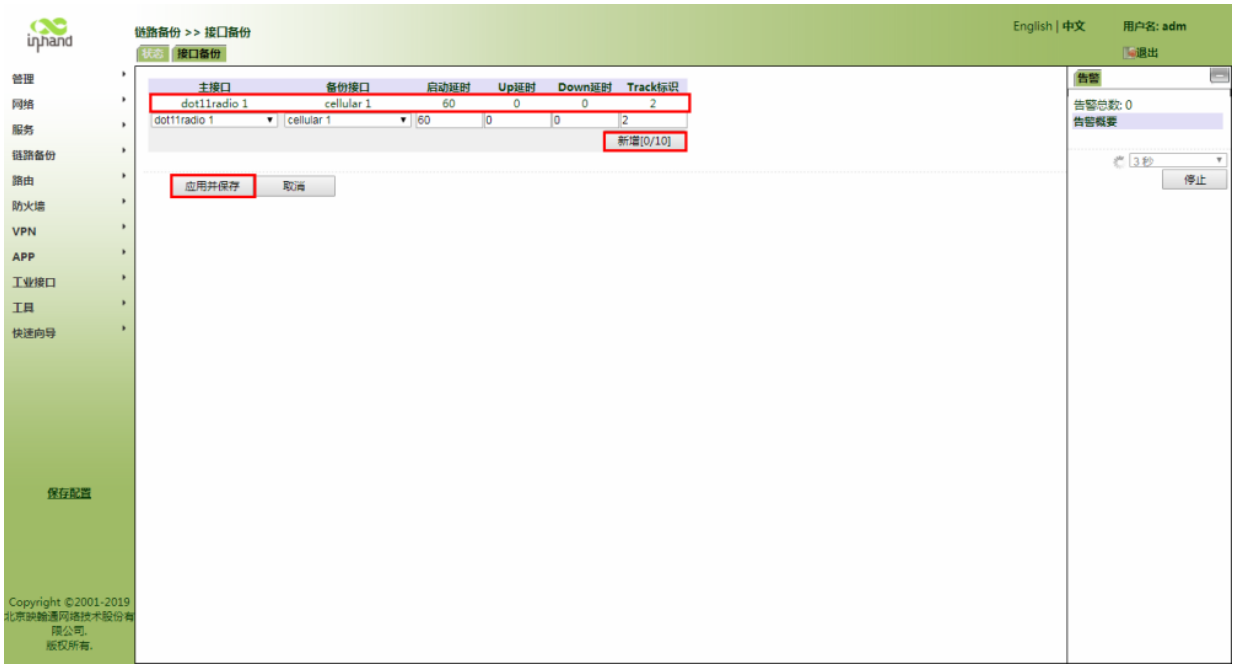


第二步：点击“链路备份>>SLA>>SLA 表>>新增”，新增一条 ICMP 探测，其中 IP 地址应设置为公网或专网内可 ICMP 探测的主机地址，例如百度首页网址 119.75.217.109，点击应用并保存。

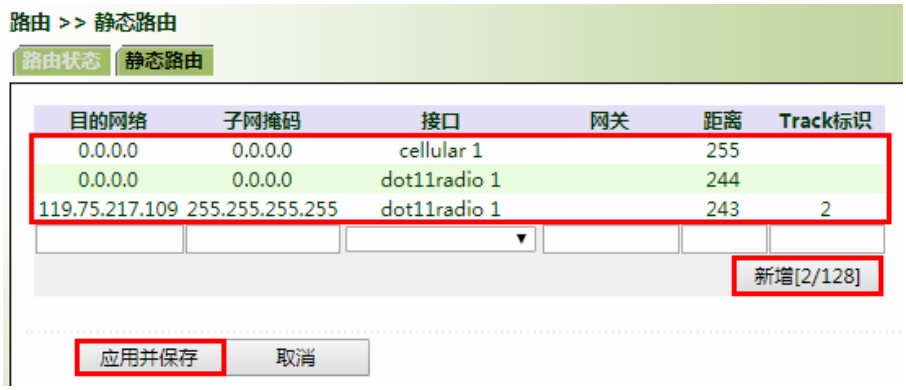


第三步：点击“链路备份>>Track 模块>>Track 表>>新增”新增一条 Track，“类型”选择 interface，“接口”选择 dot11radio1，点击新增，然后点击应用并保存。

第四步：点击“链路备份>>接口备份>>新增”，设置 dot11radio1 为主接口，cellular1 为备份接口，点击应用并保存。



第五步：点击“路由>>静态路由>>新增”，新增 2 条 dot11radio1、cellular1 接口访问网络的路由，其中“距离”数值越小越优先。



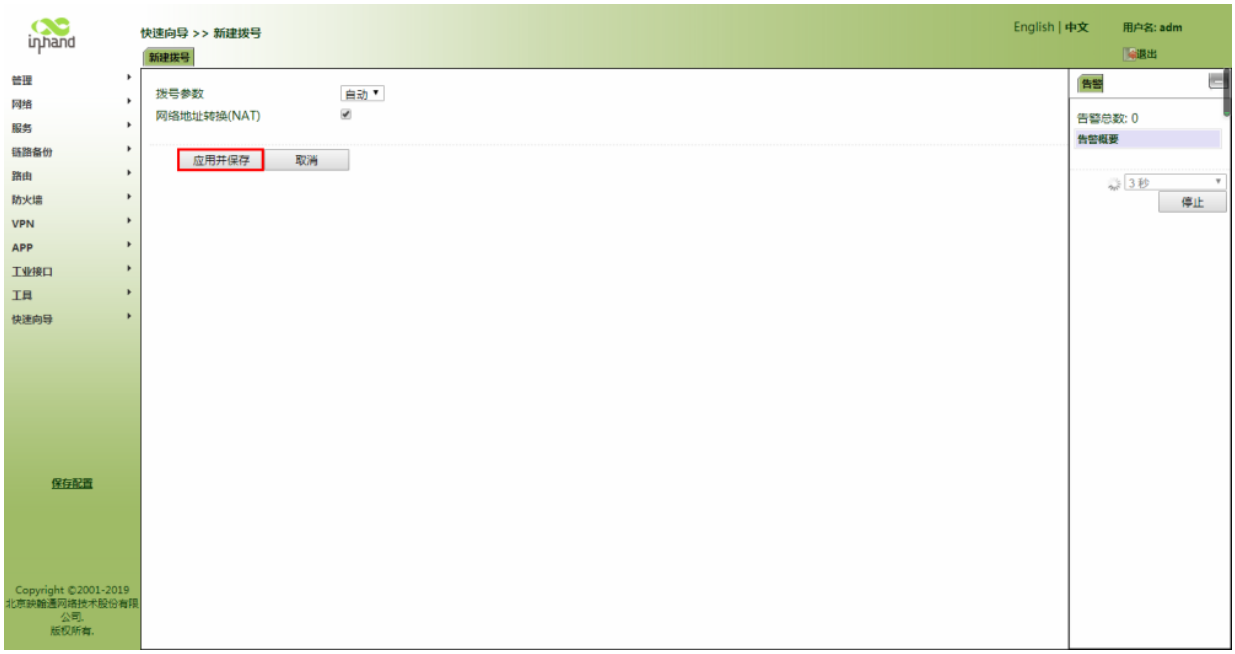
第六步：制造 Wi-Fi 上网故障，根据预设的链路探测策略， VG710 会立刻通过 cellular 口拨号上网；当 Wi-Fi 恢复正常后， VG710 又会立即切换到通过 Wi-Fi 上网。

5.8 快速向导

我们设计“快速向导”模块，将一些常用的通讯参数设置放置到本模块，使操作更加简便。

5.8.1 新建拨号

普通上网卡可以在插卡后，点击“快速向导>>新建拨号>>应用并保存”，完成后，进入系统状态栏，查看到设备网络状态为已连接。

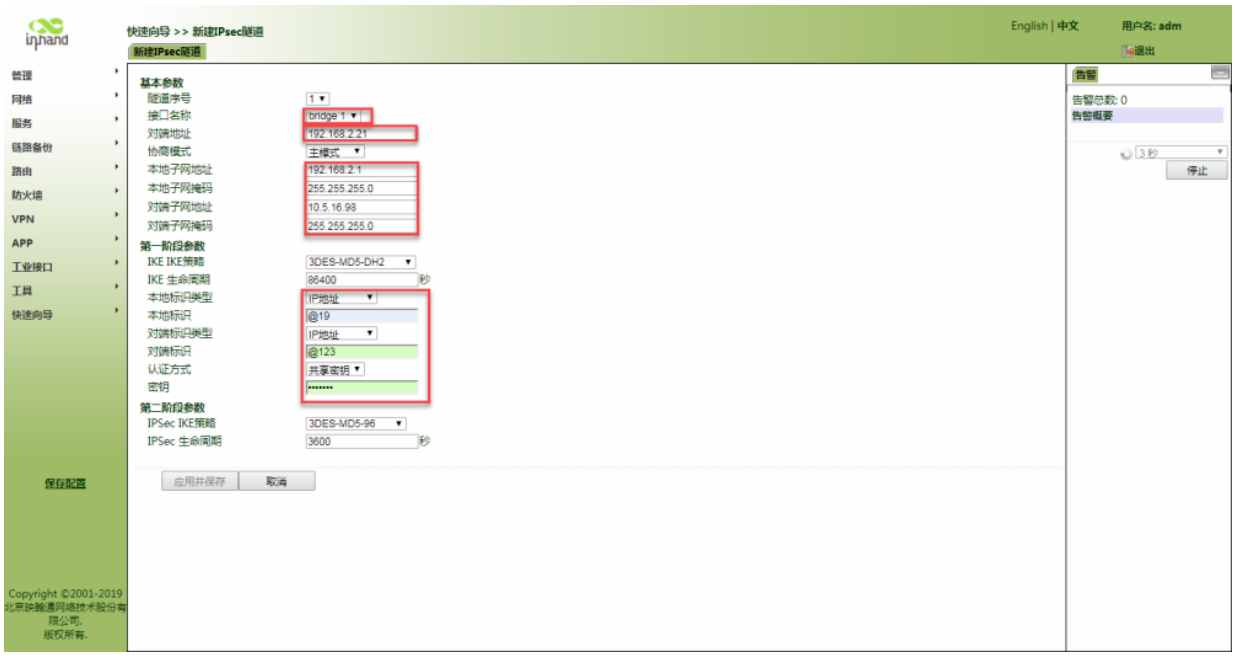


5.8.2 新建 IPsec 隧道

使网关和网络中的其它设备或云平台建立一个专用虚拟隧道。

网关建立 IPsec 隧道的设置方法：

点击“快速向导>>新建 IPsec 隧道”，“接口名称”选择要建立隧道的接口（bridge：桥接口；cellular：拨号口；dotllradio：Wi-Fi 接口），“对端地址”输入对端的 IP 地址，输入隧道两端的子网地址和掩码。在第一阶段，填写隧道两端的标识名和连接秘钥，点击应用并保存。



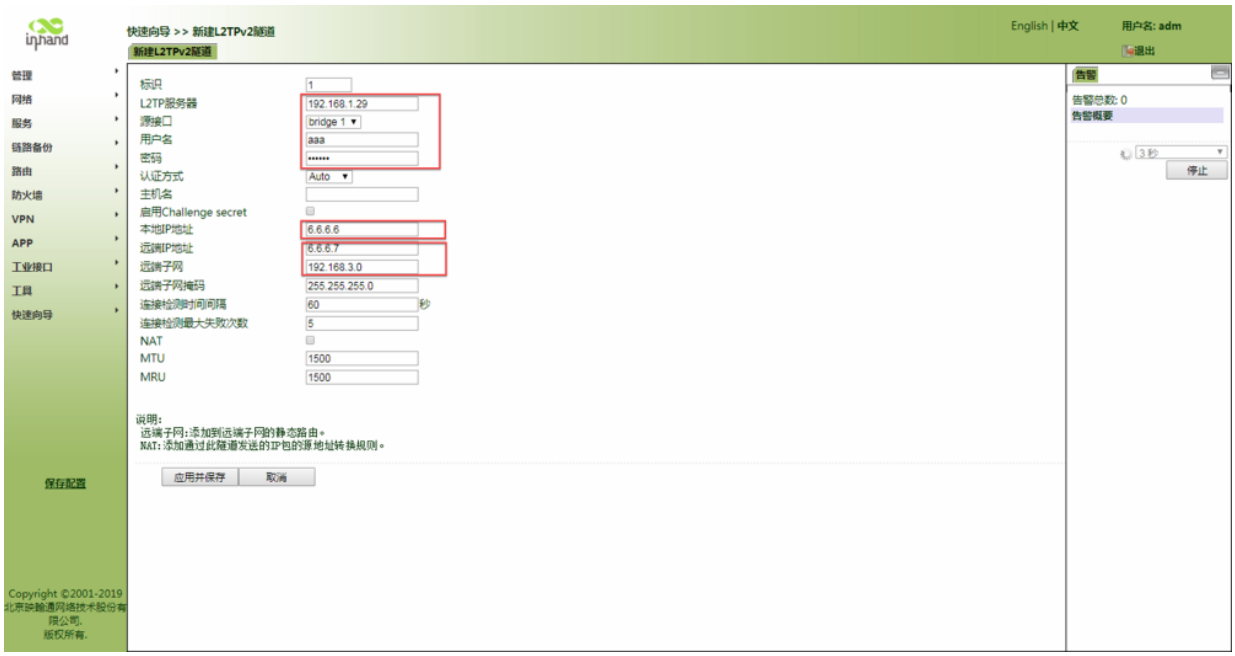
5.8.3 IPsec 专家配置

本功能仅供个别用户使用，如果需要使用此功能，请联系技术支持。

5.8.4 新建 L2TPv2 隧道

网关新建 L2TPv2 隧道的设置方法：

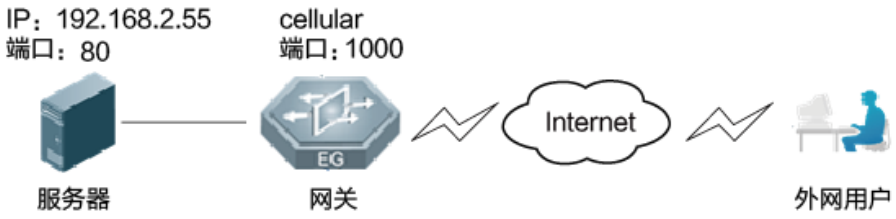
填写 L2TP 服务器参数、本地/远端地址等，点击应用并保存。



5.8.5 新建端口映射

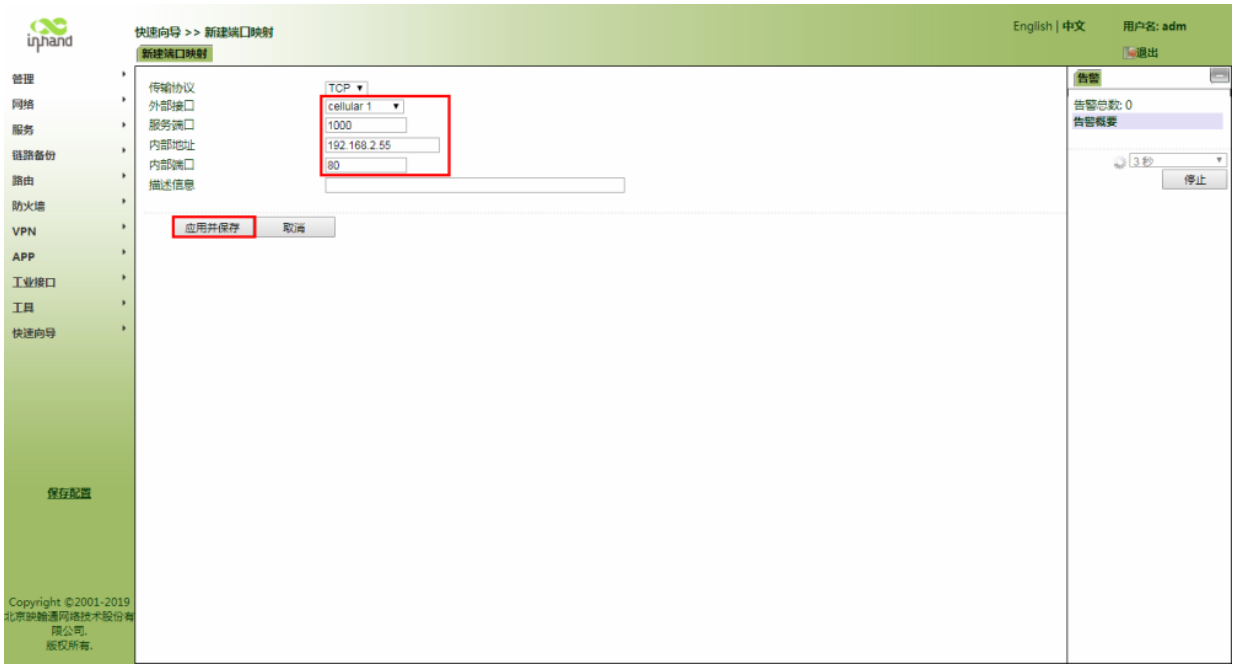
端口映射就是将内网中的主机的一个端口映射到外网主机的一个端口，提供相应的服务。当用户访问外网 IP 的这个端口时，服务器自动将请求映射到对应局域网内部的机器上。

情景：我们在内网中有一台 Web 服务器，但是外网中的用户是没有办法直接访问该服务器的。于是我们可以在网关上设置一个端口映射，只要外网用户从网关 cellular 接口访问 1000 端口，那么网关会自动把数据转到内网 Web 服务器的 80 端口上。



网关新建端口映射的设置方法：

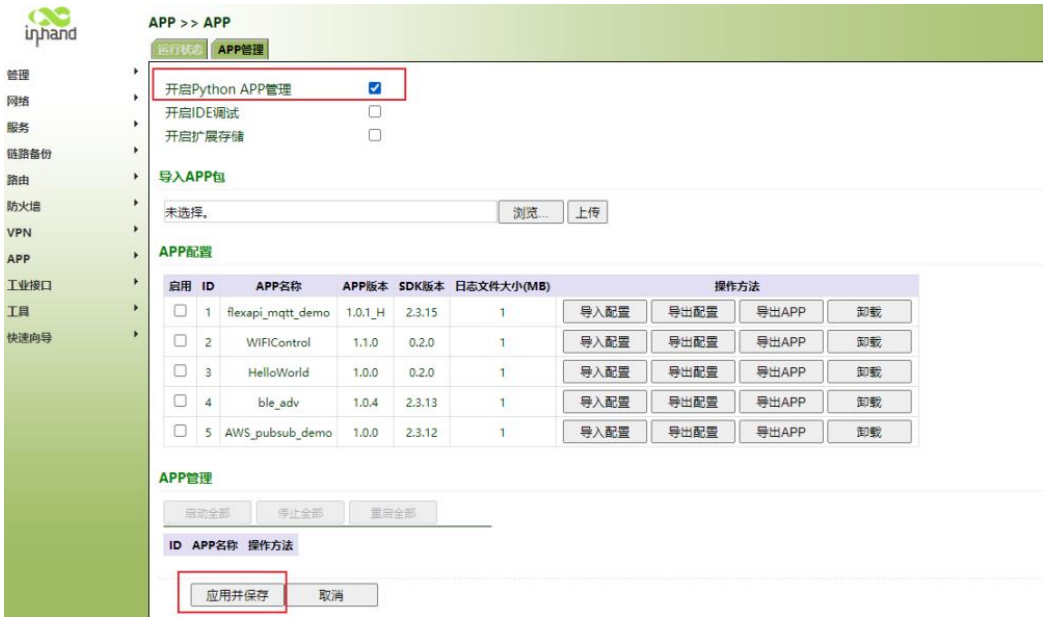
点击“快速向导>>新建端口映射”，“外部接口”填入网关的接口，“服务端口”填入网关的端口，“内端地址”填入内部主机的地址，“内部端口”填入内部主机的地址，点击应用并保存。



6 APP 管理

6.1 APP

第一步：点击 “APP>>APP>>APP 管理·>>开启 python APP 管理”，点击应用并保存。



第二步：点击运行状态,APP 管理运行状态在运行，则表示运行成功

6.2 Docker

第一步：点击“APP>>Docker>>启用”，在输入框中输入用户名、密码和端口号，点击应用并保存

6.3 第三方云平台

网关设备作为客户端的形式连接云平台实现通信，根据网关设备对应的配置来实时的获取数据，到达数据的交互的目的。

6.3.1 通过 MQTT 协议连接云平台

第一步：点击“APP>>第三方云平台>>MQTT>>启用”，选择云平台服务器的地址和端口，点击应用并保存。

第二步：点击“状态”连接状态为已连接，则表示连接成功。

注意：如果服务器需要认证和加密，需要对应开启即可，点击“APP>>第三方云平台>>MQTT>>启用”，选择云平台服务器的地址、端口、启用 MQTT 认证和 TLS 加密。

6.3.2 通过 TCP 协议连接云平台

第一步：点击“APP>>第三方云平台>>TCP>>启用”，选择云平台服务器的地址和端口，点击应用并保存

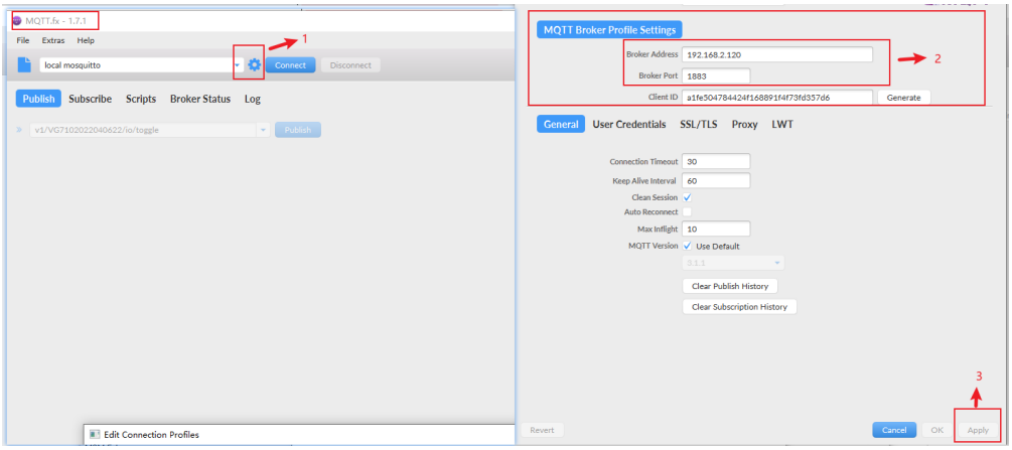
第二步：点击“状态”连接状态为已连接，则表示连接成功。

6.4 本地 MQTT 代理

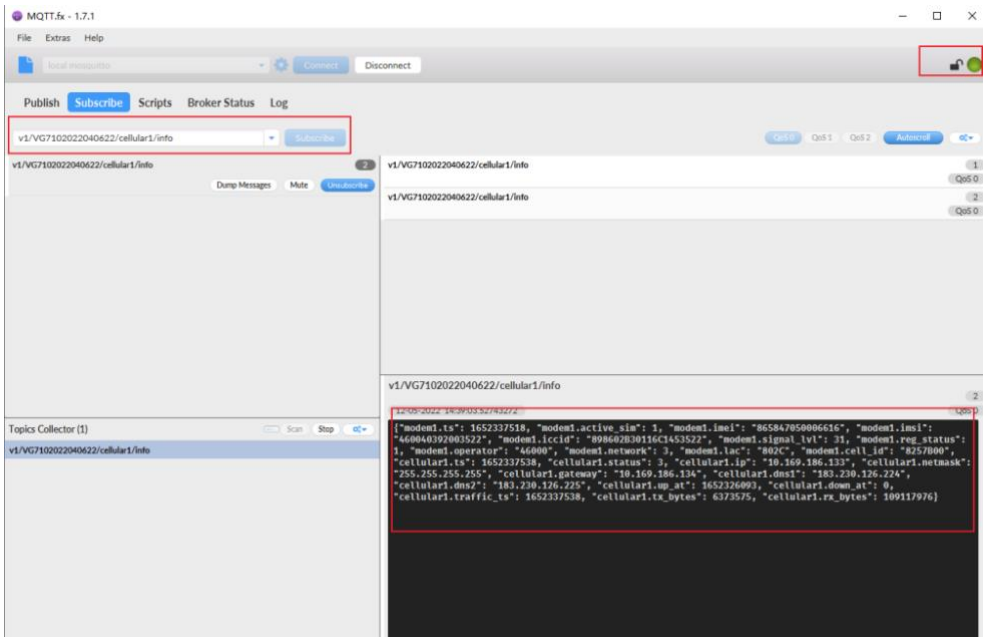
网关设备作为 MQTT 服务器去代理消息，用户需要消息时使用 MQTT 客户端去订阅信息

第一步：点击 “APP>>本地 MQTT 代理>>启用本机/本机 & LAN”，点击应用并保存

第二步：使用 MQTT 客户端信息：服务器地址，端口，认证等信息



第三步：点击 connect 连接，图标变绿则表示连接成功，然后去根据 topic 文档去订阅信息，网关将以 json 的格式返回数据例如：订阅蜂窝信息



6.5 REST API

除了使用 MQTT 和 TCP 去获取数据之外，用户也可以使用 REST API 根据接口文档调用数据

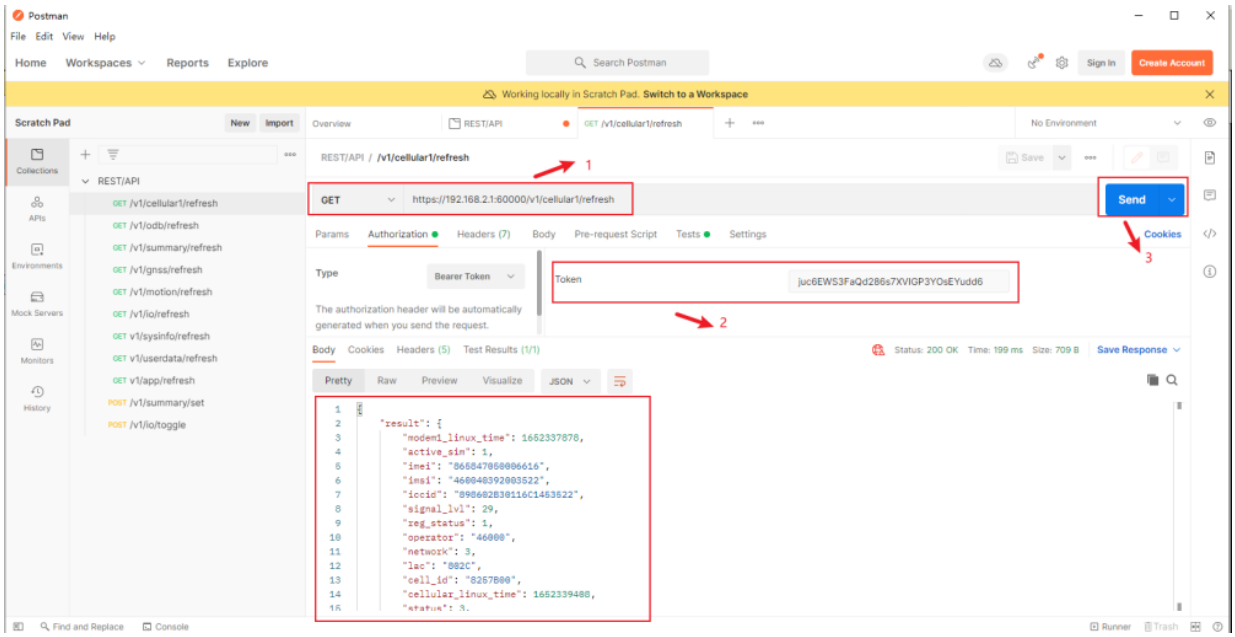
第一步：点击 “APP>>REST API>>启用本机 & LAN”，选择云平台服务器的地址和端口，点击应用并保存

第二步：根据接口文档使用工具比如：postman，去调用接口获取数据。

1、填写接口文档中的 URL，TOKEN 等，并注意是 get 还是 post 请求

2、点击发送

3、最终网关设备会以 json 的格式返回对应的数据结果



6.6 Azure IoT Edge

点击“APP>>Azure IoT Edge>>启用”，点击应用并保存

注意：此功能项依赖 Docker，开启前应打开 Docker 功能

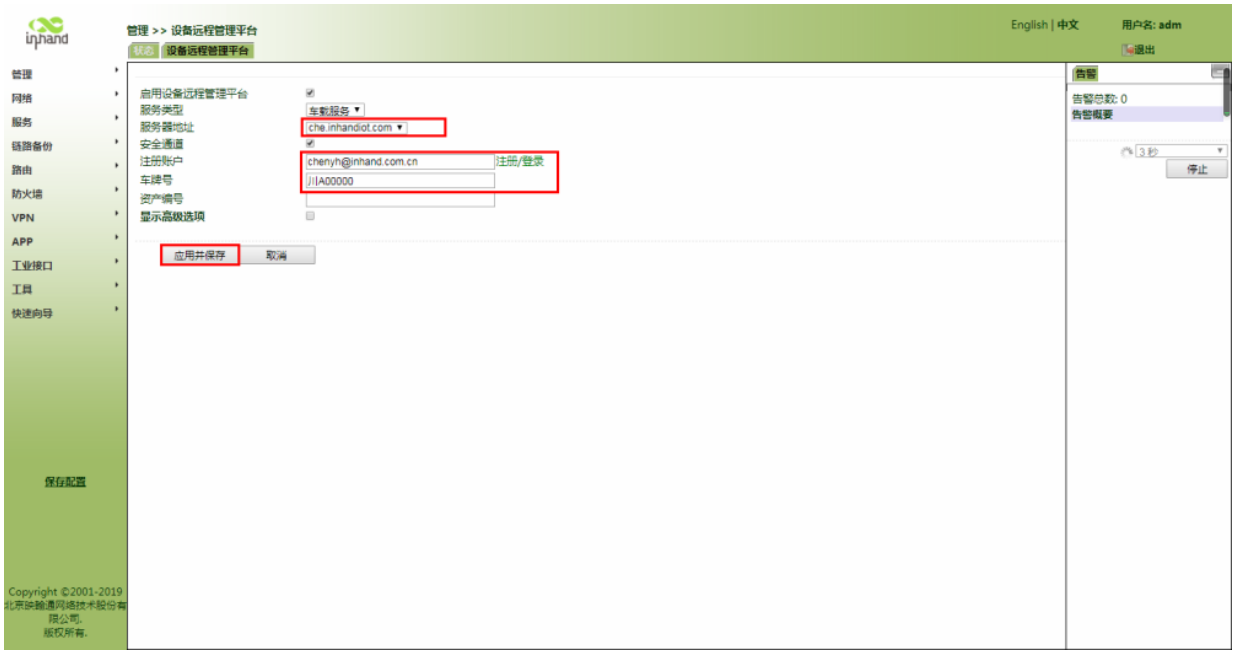
6.7 自定义数据

第一步：点击 “APP>>自定义数据>>自定义数据管理”，然后输入名称和对应的值，点击新增，最后点击应用并保存。

第二步：点击“状态”如果数据存在状态栏中，则表示添加成功。

7 网关连接到云平台

第一步：点击“管理>>设备远程监控平台>>设备远程监控平台>>启用”，选择云平台服务器地址并输入云平台注册账户及车牌号，点击应用并保存。



第二步：点击“状态”，Connected 表示连接云平台成功。

8 工业接口（串口）

VG710 工业接口包括 RS232 串口、RS485 串口和 IO 接口。

8.1 DTU

RS232 采用全串口通讯，支持硬件流控。

RS485 采用半双工通信，能远距离传输串行通信数据。

网关做 DTU 功能使用时 web 页面的设置方法：

第一步：启用 DTU1（RS232)或 DTU2(RS-485)。

第二步：配置网关接口与工业设备的连接参数，网络链路两端参数保持一致才能通信。

第三步：填入服务器的 IP 地址和传输协议（TCP 协议、UDP 协议）。

第四步：创建并启用服务器，网关通过 DTU 功能连接服务器，连接成功后网关会自动向服务器发送 DTU 标示（DTU 标示参数为空则不发送）。

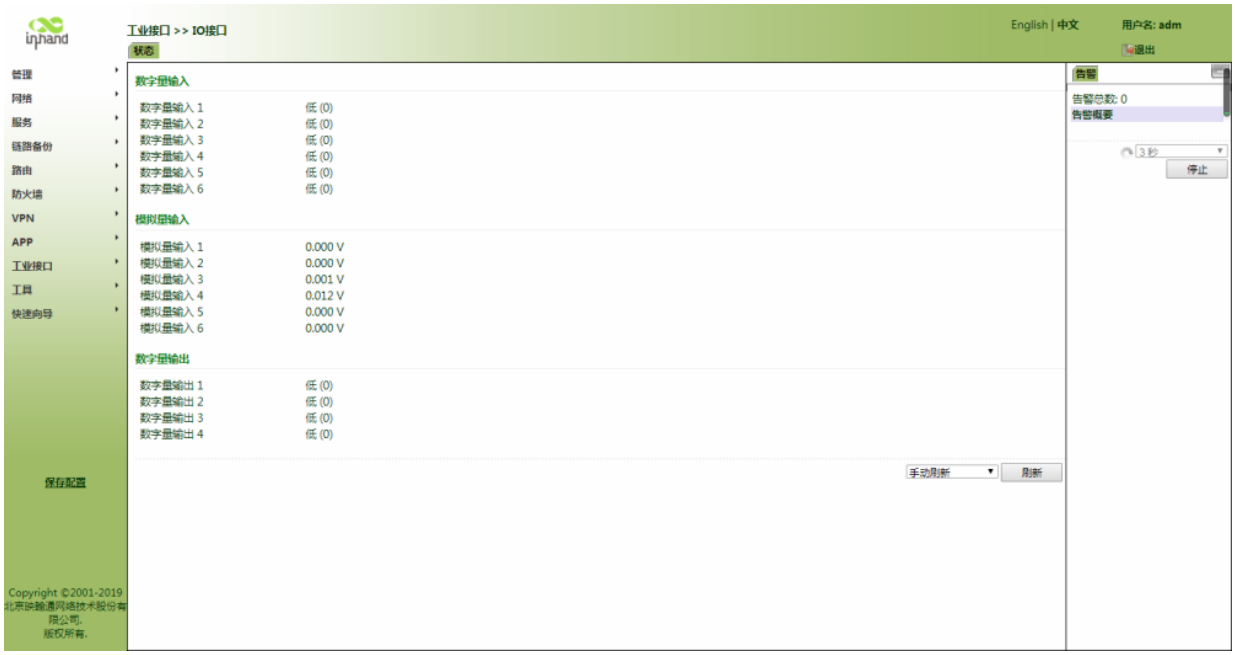
第五步：连接网关的 PC 通过 DTU 功能和服务器可以相互发送数据。


TCP&UDP测试工具 - [61.148.242.83:16504]
操作(O) 查看(V) 窗口(W) 帮助(H)
ZNE-200T全功能型快速以太网转串口模块
具有10/100M自适应以太网接口，串口通信最高
波特率高达1.15Mbps
NETCOM-10S标准型以太网转串口设备
具有TCP Server,TCP Client, UDP, Real
COM ,Group组播,TCP Auto等多种工作模式
更多.
创建连接 创建服务器 启动服务器 连接 全部断开 删除
属性栏
客户端模式
服务器模式
本机(172.17.23.62):22010
61.148.242.83:16504
61.148.242.83:16504
目标IP:
61.148.242.83
目标端口:
16504
指定本机端口:
22010
类型:
TCP
计数
发送:
1400
接收:
144
清空计数
发送区
自动发送: 间隔 2000 ms
发送
停止
按16进制 发送文件 发送接收到的数据
清空
选项
0123456789
接收区
暂停显示
清空
保存
选项
按16进制
保存到文件(实时)
0123456789
0123456789
0123456789
0123456789
0123456789
0123456789
0123456789
0123456789
发送时间: 00:03:58
发送速度(B/S): 5
接收速度(B/S): 6


SSCOM3.2 (作者:聂小猛(丁丁), 主页http://www.mcu51.com, Email: mc...
0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789
打开文件
文件名
发送文件
保存窗口
清除窗口
HEX显示
串口号 COM1
关闭串口
帮助
WWW.MCU51.COM
扩展
波特率 9600
数据位 8
停止位 1
校验位 None
流控制 None
DTR
RTS
定时发送 2000 ms/次
HEX发送
发送新行
字符串输入框:
发送
ESP8266WIFI转串口20元,QQ群120693138
欢迎访问大虾论坛！众多大虾等着你!
--------以下为广告--------
嘉立创PCB打样10*10cm只要50元.请找小万.
点这里进入http://www.sz-jlc.com.cn/
0123456789
www.mcu51.cor
S:144
R:120
COM1已打开 9600bps 8
CTS=0 DSR=0 RL

8.2 IO 接口

IO 支持 6 路模拟输入、6 路数字输入、4 路数字输出，模拟输入与数字输入共用接口。数字量对应两个状态：高（1）、低（0）。

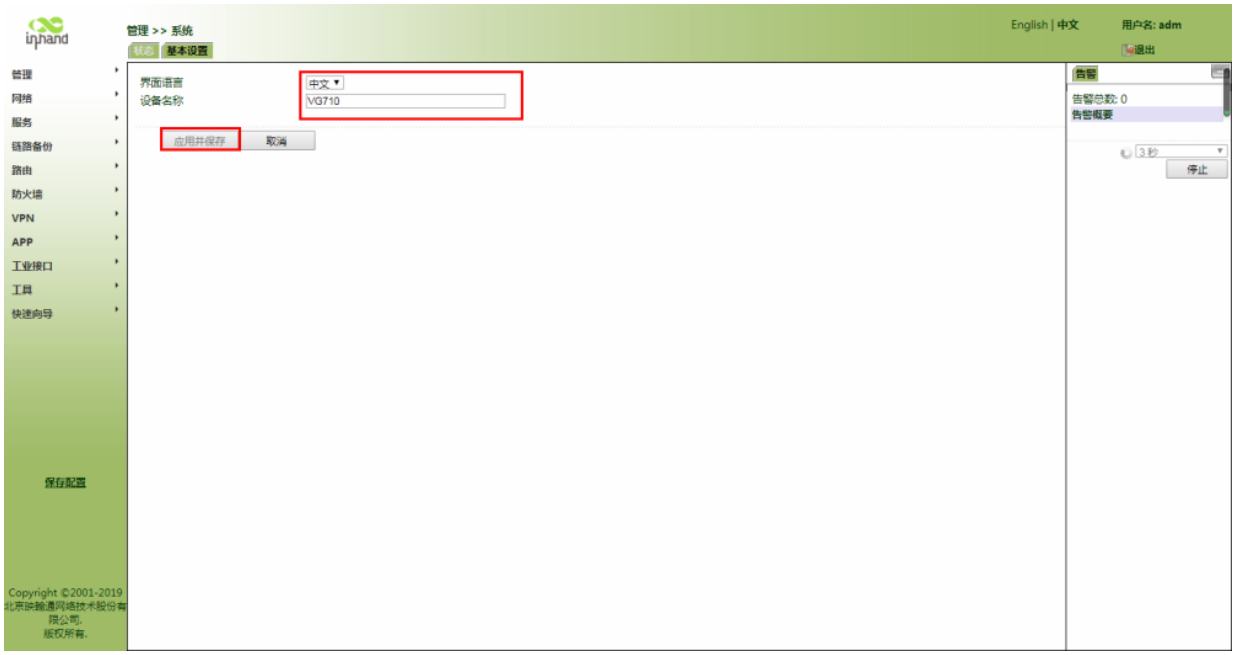


9 系统管理

9.1 系统

点击“管理>>系统>>状态”查看设备当前系统状态和网络状态。

点击“基本设置”修改系统语言和网关名称。



9.2 系统时间

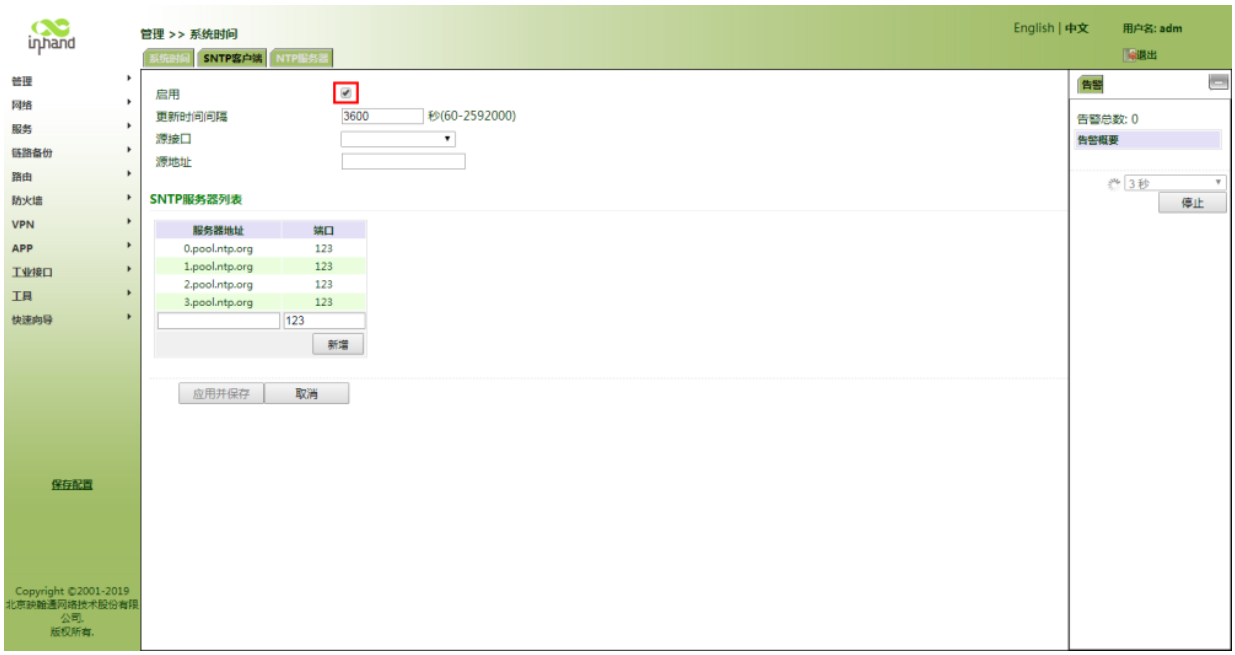
为了保证本设备与其它设备协调工作，用户需要将系统时间配置准确。

手动同步时间。点击“管理>>系统时间>>系统时间>>同步时间”，使网关和相连主机时间一致。

也可以点击“管理>>系统>>状态”同步时间。

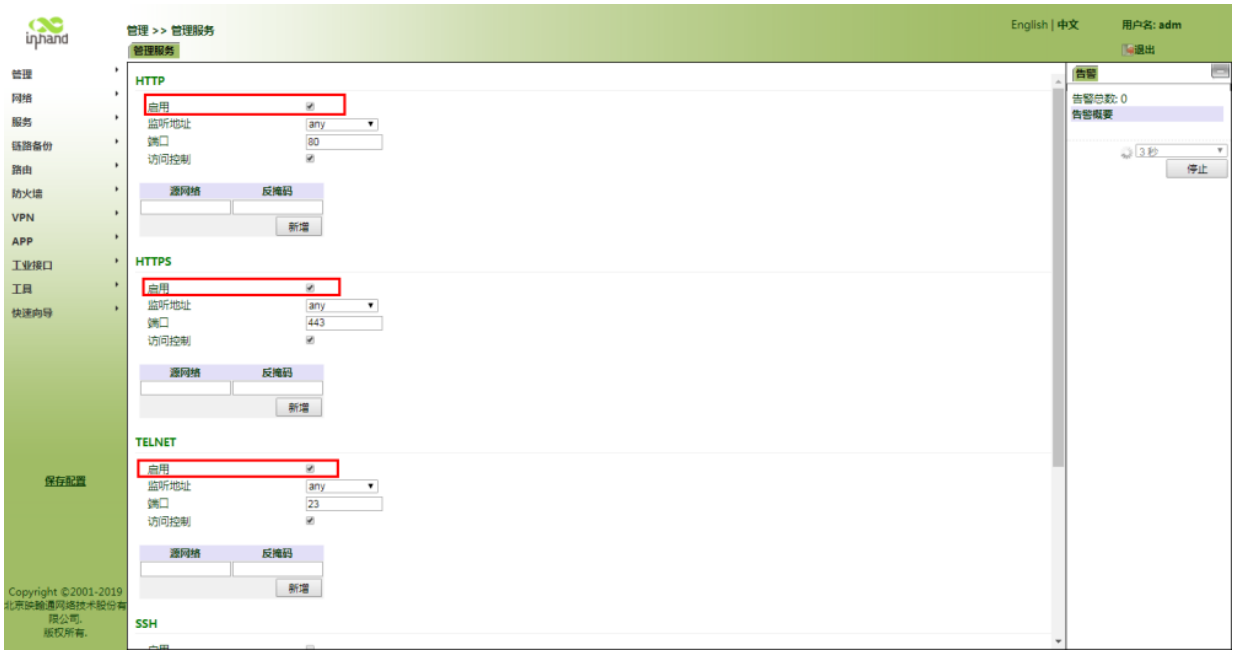
自动同步时间。点击“管理>>系统时间>>SNTP 或者 NTP>>启用”，同步设备和 SNTP 或者 ntp 服务器的时间。

启用 NTP，使网关对网络内所有设备进行时间同步。



9.3 管理服务

当网关要使用“HTTP、HTTPS、TELNET 和 SSH”功能时，点击“管理>>管理服务”启用并点击应用并保存后，才能使用该项功能。



9.4 用户管理

点击“管理>>用户管理”，在用户管理界面创建用户、修改密码和删除用户。

用户分为超级用户和普通用户：

- 超级用户：由系统自动创建且只有一个，用户名为 adm，默认密码为：123456，具有对网关的所有访问权限。
- 普通用户：由超级用户创建，查看网关的配置或者修改网关的配置。

说明：对于超级用户（adm），不能修改其用户名，也不能删除它，但可以修改超级用户的密码。

9.5 AAA

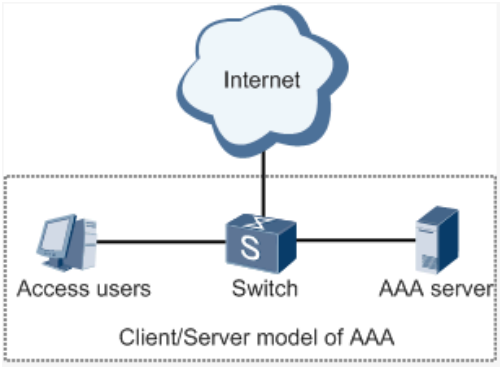
AAA 是认证（Authentication）、授权（Authorization）和计费（Accounting）的简称，是网络安全中进行访问控制的一种安全管理机制，提供认证、授权和计费三种安全服务。

它提供了完成下列服务的模块化方法：

- 认证：验证用户是否可以获得网络访问权。
- 授权：授权用户可以使用哪些服务。
- 计费：记录用户使用网络资源的情况。

可以只使用 AAA 提供的一种或两种安全服务。例如，公司仅仅想让员工在访问某些特定资源的时候进行身份认证，那么网络管理员只要配置认证服务器即可。但是若希望对员工使用网络的情况进行记录，那么还需要配置计费服务器。

AAA 通常采用“客户端—服务器”结构。这种结构既具有良好的可扩展性，又便于集中管理用户信息。如下图所示：



说明 说明：radius、tacacs+、ldap 指认证及授权服务器。local：网关本地用户名和密码。

9.5.1 Radius

远程认证拨号用户服务 Radius 是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

网关使用 Radius 服务器的设置方法：

点击“管理>>AAA>>Radius>>服务器列表”，填入服务器地址（域名/IP）、端口、认证密钥，点击新增，然后点击应用并保存。

9.5.2 Tacacs+

Tacacs+是终端访问控制器访问控制系统，与 Radius 协议相近，采用客户端/服务器模式实现 NAS 网络接入服务器与 Tacacs+服务器之间的通信。不过 Tacacs+用的是 TCP 协议，Radius 用的是 UDP。

Tacacs+协议主要用于点对点协议 PPP 和虚拟私有拨号网络 VPDN 接入用户及终端用户的认证、授权和计费。其典型应用是对需要登录到设备上进行操作的终端用户进行认证、授权、计费。设备作为 Tacacs+的客户端，将用户名和密码发给 Tacacs+服务器进行验证。用户验证通过并得到授权之后可以登录到设备上进行操作。

网关使用 Tacacs+服务器的设置方法：

点击“管理>>AAA>>Tacacs+>>服务器列表”，填入服务器地址（域名/IP）、端口、认证密钥，点击新增，完成后点击应用并保存。

9.5.3 LDAP

LDAP 主要的优点就在能够快速响应用户的查找需求。比如用户的认证，可能会有大量的并发。如果用数据库来实现，由于数据库结构分成了各个表，要满足认证这个非常简单的需求，每次都需要去搜索数据库，合成过滤，效率慢也没有好处。LDAP 就是一张表，只需要用户名和口令，加上一些其他的东西，非常简单。从效率和结构上都可以满足认证的需求。

网关使用 LDAP 服务器的设置方法：

点击“管理>>AAA>>LDAP>>服务器列表”，随便输入一个名称，填写服务器地址（域名/IP）和端口号、在服务器获取到基准 DN；设置访问服务器的用户名和密码；加密方式共 3 种选择：None、SSL 和 StartTLS；点击新增，然后点击应用并保存。

9.5.4 AAA 认证

AAA 支持以下认证方式：

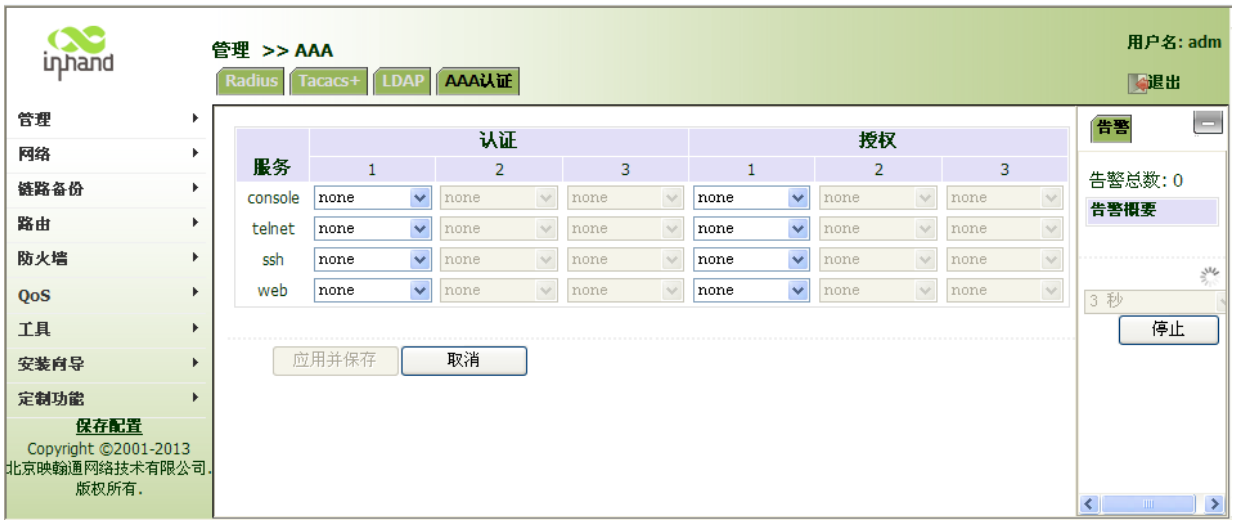
- 不认证(none)：不对其进行合法检查，一般情况下不采用此方式。
- 本地认证(local)：将用户信息配置在网络接入服务器上。本地认证的优点是速度快，可以为运营降低成本，缺点是存储信息量受设备硬件条件限制。
- 远端认证：将用户信息配置在认证服务器上。支持通过 Radius 协议、Tacacs+协议和 LDAP 进行远端认证。

AAA 支持以下授权方式：

- 不授权(none)：不对用户进行授权处理。
- 本地授权(local)：根据网络接入服务器为本地用户账号配置的相关属性进行授权。
- Tacacs+授权：由 Tacacs+服务器对用户进行授权。
- Radius 认证成功后授权：认证和授权绑定在一起，不能单独使用 Radius 进行授权。
- LDAP 授权。

网关进行认证和授权的设置方法：

点击“管理>>AAA>>AAA 认证”。1/2/3 分别对应 Radius/tacacs/ldap；认证 1/2/3 和授权 1/2/3 必须一一对应；当同时配置了 radius,tacacs+和 local 时，优先级顺序遵循：1>2>3。



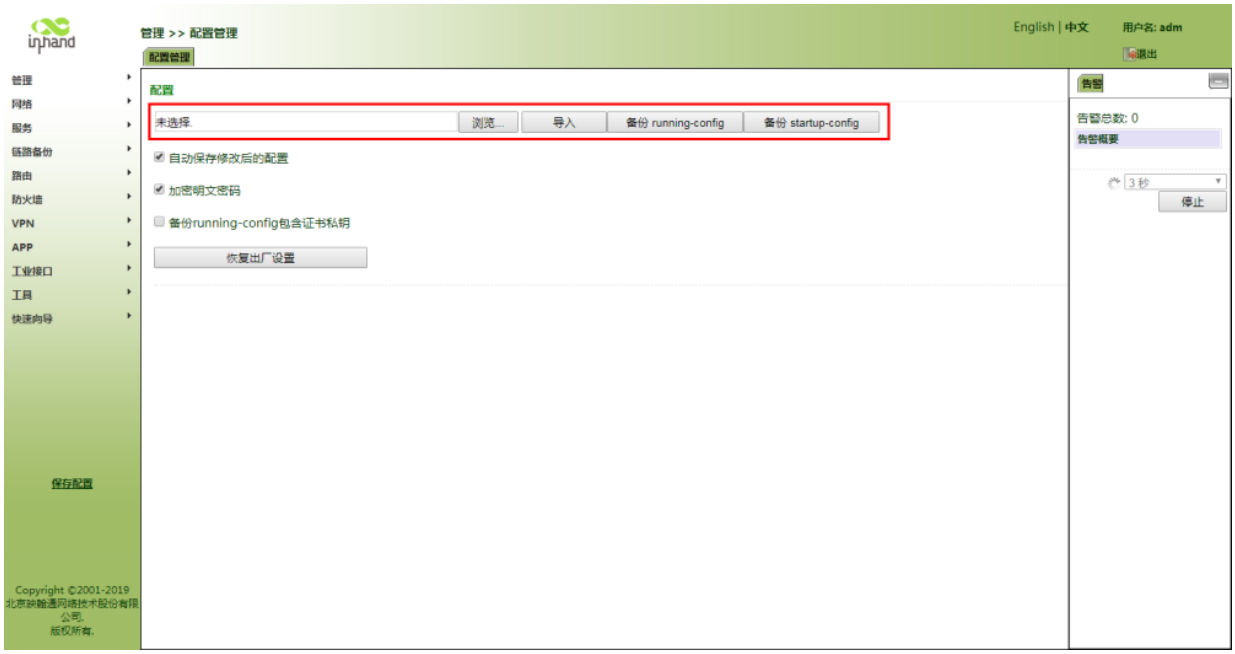
9.6 配置管理

导入配置的设置方法：点击“管理>>配置管理>>浏览，选择配置文件>>导入”把配置文件导入到网关；

备份当前运行的配置到 PC 的设置方法（常用）：点击备份 running-config 即可；

备份启动文件到 PC 的设置方法：点击备份 startup-config 即可。

恢复出厂的设置方法：点击恢复出厂设置，点击确认即可。



9.7 SNMP

9.7.1 SNMP

目前 VG710 设备的 SNMP Agent 支持 SNMPv1、SNMPv2c 和 SNMPv3 版本。

- SNMPv1 和 SNMPv2c 采用团体名认证。
- SNMPv3 采用用户名和密码认证加密方式。

VG710 启用 SNMP 的设置方法：

点击“管理>>SNMP>>SNMP”，勾选启用 SNMP 功能，选择 v1c 或 v2c 版本，点击应用并保存。

如果选择 v3c 版本，需要配置相应用户和用户组，用户组填入任意组名和选择安全级别后，点击新增。 用户填入任意用户名和刚用户组设置的组名，填写完认证/密码参数后，点击新增，最后点击应用并保存。

9.7.2 SnmpTrap（告警）

SNMP trap(SNMP 陷阱)：某种入口，到达该入口会使 SNMP 被管设备主动通知 SNMP 管理器，而不是等待 SNMP 管理器的再次轮询。在网管系统中，被管理设备中的代理可以在任何时候向网

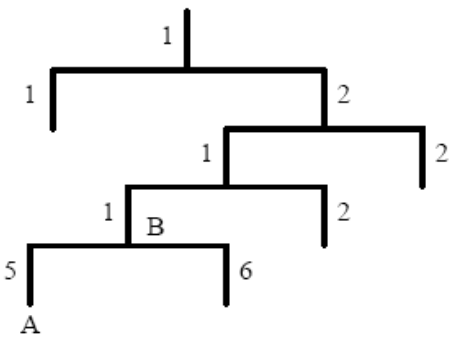
络管理工作站报告错误情况。代理并不需要等到管理工作站为获得这些错误情况而轮询他的时候才会报告。这些错误情况就是众所周知的 SNMP 自陷（trap）。

网关 SnmpTrap 的设置方法：

点击“管理>>SNMP>> SnmpTrap”，填入管理站(NMS)的 IP 地址；版本 v1 或 v2c 时填写相应的团体名，版本为 v3 时填写相应的用户名，长度 1-32 个字符；UDP 默认端口号范围 1-65535。

9.7.3 SnmpMibs

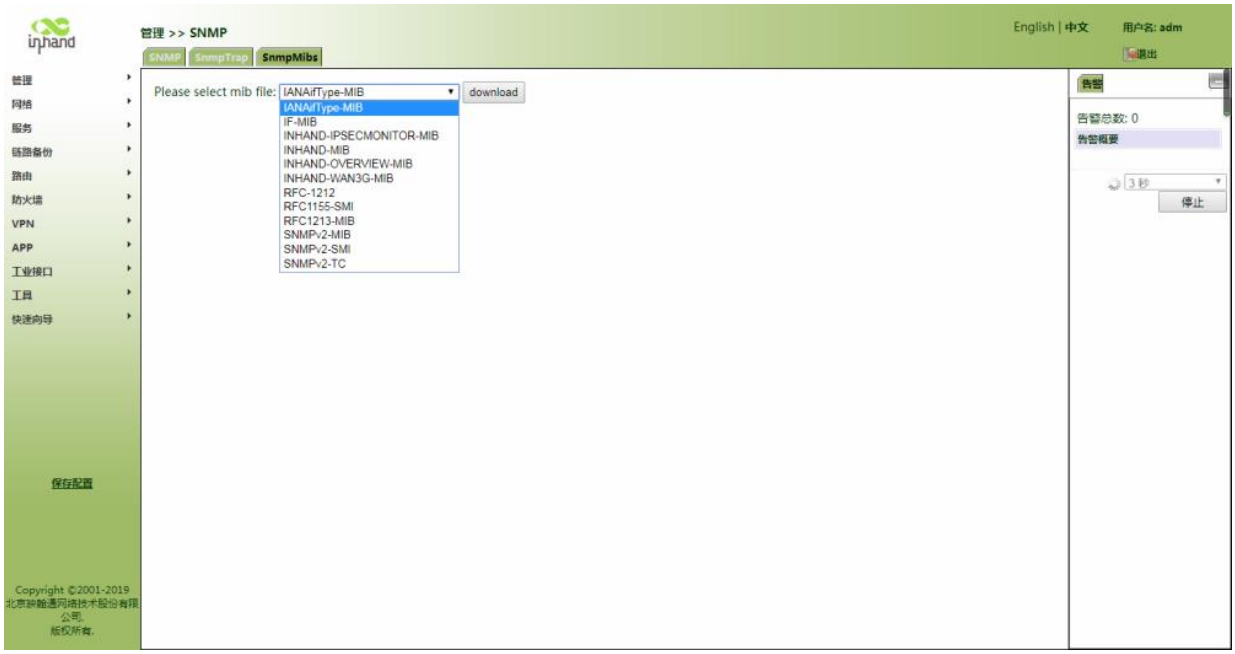
在 SNMP 报文中用管理变量来描述设备中的管理对象。为了唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象。整个层次结构就像一棵树，树的节点表示管理对象，如下图所示。每一个节点，都可以用从根开始的一条路径唯一地标识。



MIB（Management Information Base，管理信息库）的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。在上图中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的对象标识符（Object Identifier，OID）。

网关下载 SnmpMibs 文件到 PC 的设置方法：

点击“管理>>SNMP>>SnmpMibs”选择一个文件夹，点击 download 下载到 PC 打开，找到自己需要的文件夹，然后把这个文件夹导入到管理站使用。



9.8 告警

告警功能使用户及时获知网关异常。当异常产生时网关将发出告警，用户可以选择系统定义的多种异常并选择合适的通告方式来获知这些异常。所有告警都将被记录在告警日志中，使得用户能尽早的发现异常，供用户在需要时排查问题。

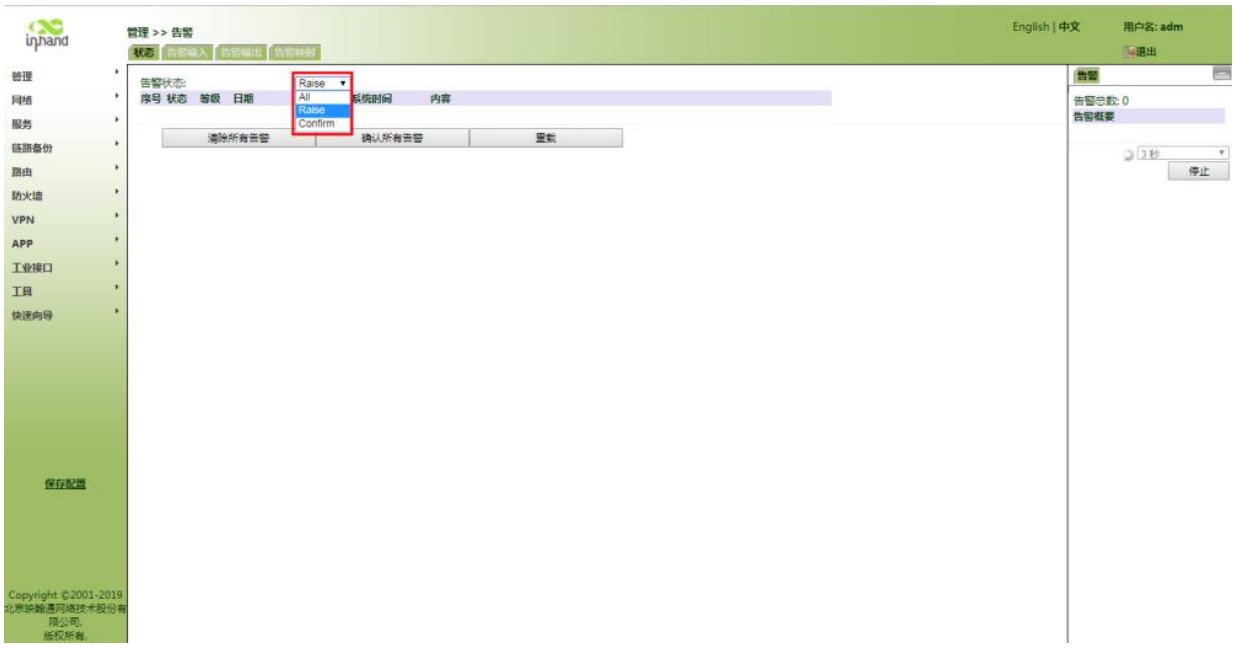
告警状态分为：

- 存在（Raise）：表示告警发生还没有被确认。
- 确认（Confirm）：表示发生的告警用户暂时不能解决。
- 全部（All）：表示发生的全部告警。

告警等级可分为：

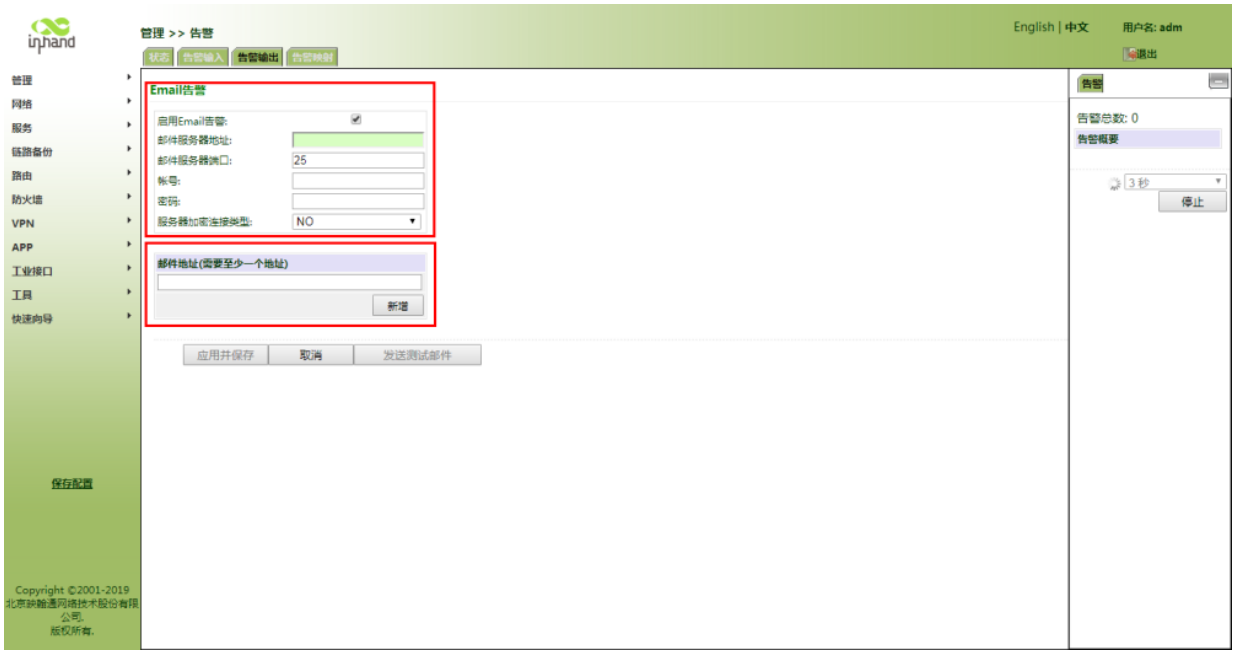
- EMERG：设备发生了某种严重的错误可能导致系统重启。
- CRIT：设备发生了某种不可恢复的错误。
- WARN：设备发生了某种影响系统功能的错误。
- NOTICE：设备发生了某种影响系统性能的错误。
- INFO：设备发生了某种正常的事件。

1）**查看告警：**点击“管理>>告警>>状态”，可以查看上电以来系统产生的所有告警。



2）**告警输入：**选择关心的告警类型，勾选后该项异常时产生报警。

3）**告警输出：**当有告警产生时，系统会自动以邮件的形式把告警内容发送到目的邮箱地址，普通用户不配置此项功能。“**Email 告警**”填写发送邮箱的信息，“**邮件地址**”填写接收告警的邮箱地址。其中，**邮件服务器地址**可以在浏览器上搜索到（例如：使用腾讯企业邮箱填 smtp.exmail.qq.com）。



4）**告警映射：**接收告警的方式有 CLI（console 口）和 Email（TH09 设备支持短信告警）。若要启用 Email 映射则要在告警输出部分启用并配置好邮箱地址。

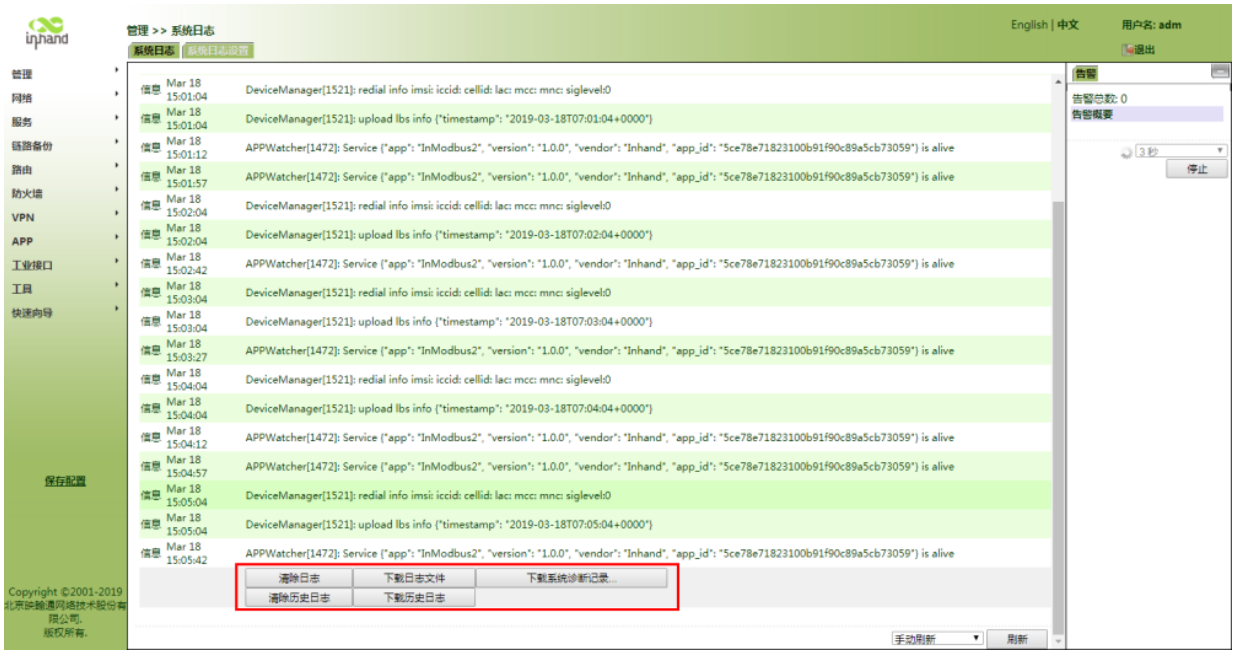
9.9 系统日志

查看系统日志的设置方法：

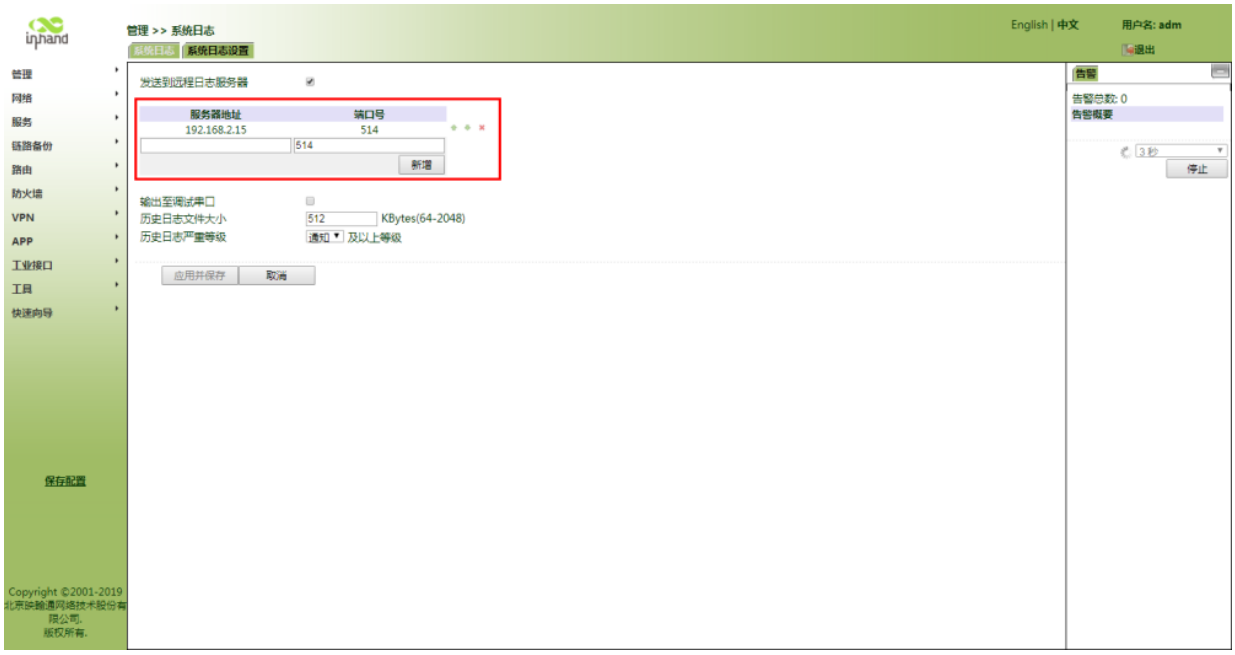
点击“管理>>系统日志”查看系统日志。

在此页面还可以“清除日志”、“下载日志”、“清除历史日志”、“下载历史日志”。历史日志指在“系统日志设置”界面规定保存更长久的日志。

“系统诊断记录”文件为加密文件，因为下载系统诊断记录时会把网关的配置信息也下载下来，所以需要使用我司的解密工具解密后才能查看。

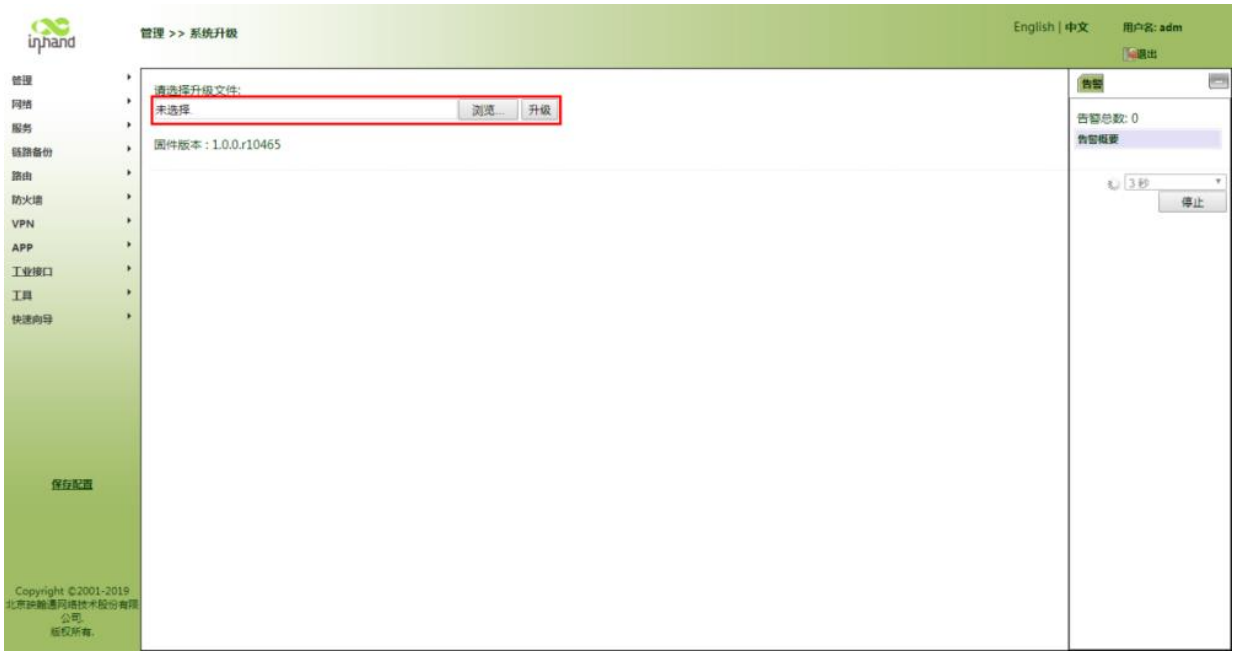


因为网关储存容量有限（默认为 512KB），如果想把日志信息全部保存下来，需要借助远程日志服务器（如:Kiwi Syslog Daemon 软件）的配合。在 WEB 设置好日志服务器的地址和端口，网关将会把所有的系统日志上传到远程日志服务器。



9.10 系统升级

点击“管理>>系统升级>>浏览，选择升级文件>>升级”,升级完成后重启系统。



注意 注意：

在软件升级的过程中，请不要在 WEB 上进行任何操作，否则可能会导致软件升级中断。

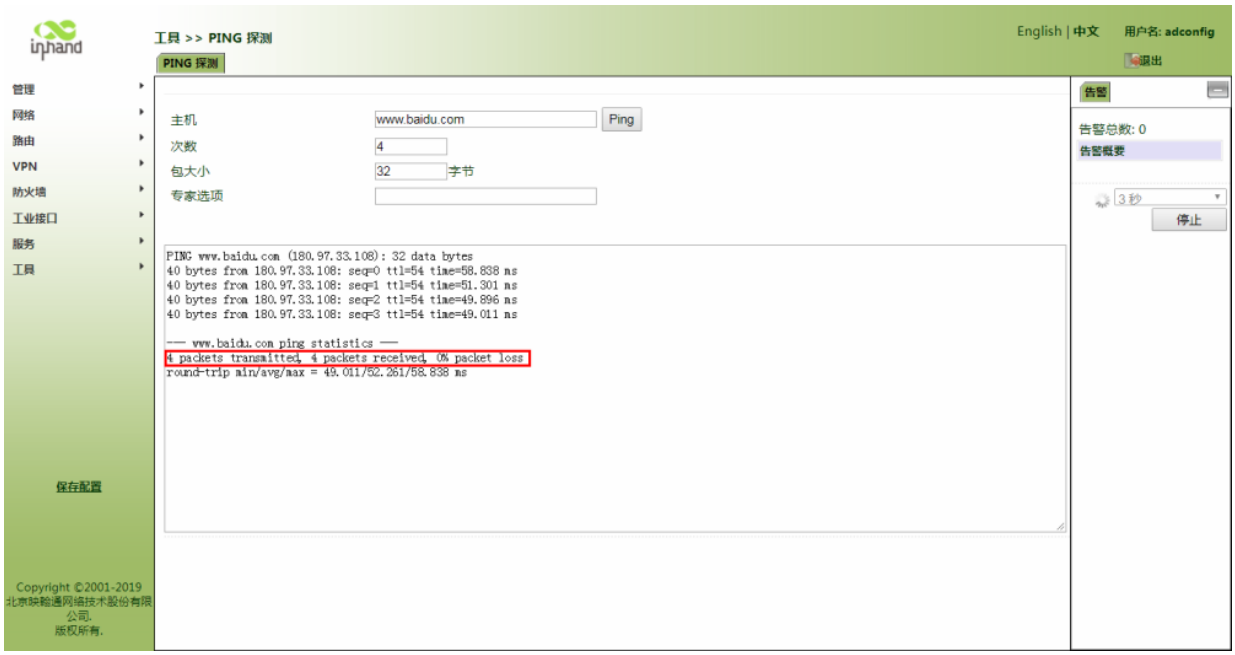
9.11 重启系统

点击“管理>>系统重启>>确定”即可重启系统。

10 诊断工具

用于探测网关网络连接情况：PING 探测、路由探测、网络抓包、网速测试。

PING 探测：用于检测设备外网联通情况。“主机”填入任意国内常用网站，点击 ping，有数据传输表示网络通畅。

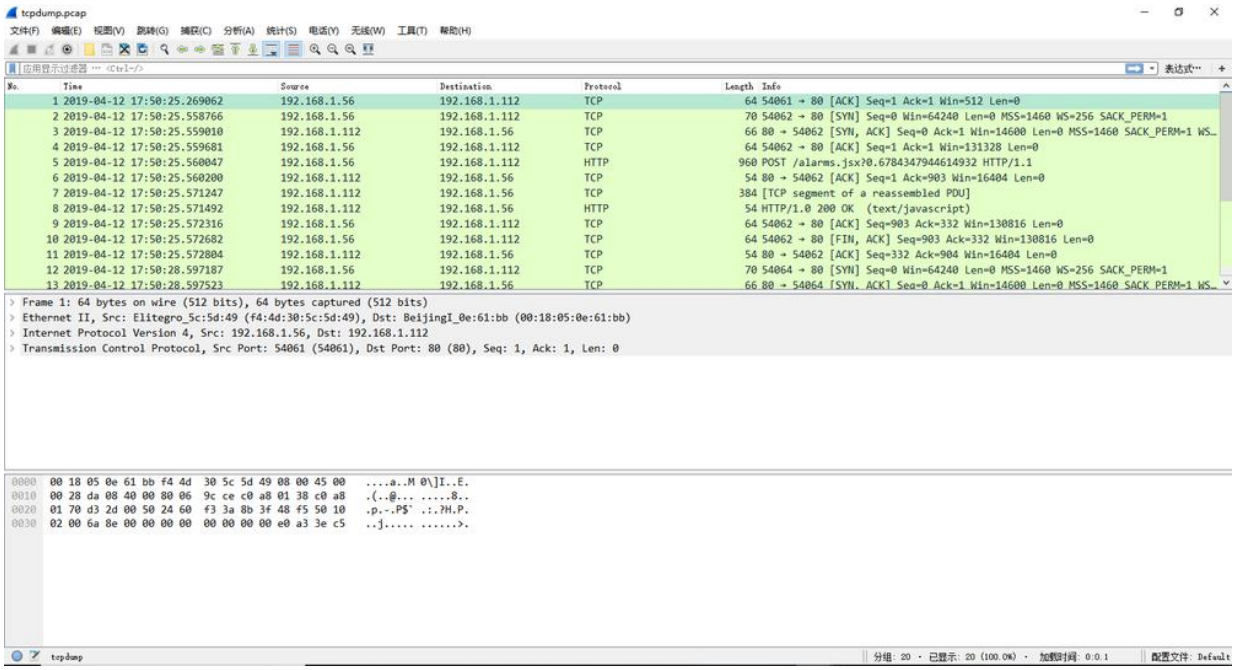


路由探测：输入对端主机 IP 地址，点击 Trace，检测路由连通情况。

网络抓包：

选择要抓包的接口（any/bridge1）和抓包个数，点击开始抓包>>停止装包>>下载抓包文件。

浏览器下载 **wireshark 软件来**打开抓包文件，并通过分析包，了解接口网络情况。



网速测试：通过上传或下载文件来测试网速。