



首科力通
SUPERONE

5G智能工业终端-SuperNet100

SuperNet 5G intelligent device



目录

用户重要须知.....	1
主机及组件.....	3
安装介绍.....	4
第一步：连接电源和 SIM 卡.....	4
第二步：连接天线和以太网接口.....	5
一、设备信息.....	7
1、进入配置页面.....	7
2、状态总览.....	8
3、端口信息.....	10
4、流量信息.....	11
5、流量检测.....	12
6、带宽检测.....	13
二、常规配置.....	14
1、端口设置：.....	14
2、VLAN 设置.....	18
3、公网设置.....	22
4、连接管理.....	26
5、路由管理.....	29
三、VPN 配置.....	32
四、高级配置.....	34
1、转发设定.....	34
2、DMZ 设定.....	36
3、本地 NAT.....	37
4、云端 NAT.....	39
5、DHCP 设定.....	43
五、系统配置.....	44
1、接入管理.....	44
2、时间同步.....	46
3、设备名称.....	48
4、备份管理.....	49
5、SNMP.....	50
6、系统日志.....	51
7、固件管理.....	52
六、安全配置.....	53
1、规则设定.....	53
七、系统工具.....	56
1、PING 工具.....	56
2、截取数据.....	57
3、追踪数据.....	58
4、日志数据.....	59
联系我们.....	60

用户重要须知

在安装、配置、操作或维护本产品之前，请阅读本文档“安装介绍”章节，了解关于安装、配置和操作该设备的信息。除了所有适用的条例、法律和标准的要求之外，用户还必须熟悉安装和接线。

包括安装、调整、投入运行、使用、装配、拆卸和维护等在内的操作必须由经过适当培训的人员根据适用的操作守则来执行。

如果未遵照制造商所指定的方式使用该设备，将可能导致该设备提供的保护失效。

任何情况下，对于因使用或操作本设备造成的任何间接或连带损失，北京首科力通机电设备有限责任公司概不负责。

本手册中包含的示例和图表仅用于说明。由于任何具体安装都涉及众多变数和要求，首科力通公司对于依据这些示例和图表所进行的实际应用不承担任何责任和义务。

对于因使用本手册中所述信息、电路、设备或软件而引起的专利问题，首科力通公司不承担任何责任。

未经首科力通公司的书面许可，不得复制本手册的全部或部分内容。

在整本手册中，我们在必要的地方使用了以下注释，来提醒您留意安全注意事项。

安全警示

为了保障您的个人安全以及产品和连接设备的安全，在安装模块产品之前请务必仔细阅读安全警示。本手册中的警示均用警示三角形标注并注明危险等级。



Danger

如果不采取合适的预防措施将会造成严重的人身伤亡以及财产损失。



Warning

如果不采取合适的预防措施可能会造成严重的人身伤亡以及财产损失。



Caution

如果不采取合适的预防措施将造成轻微的人身伤害以及财产损失。

一名合格的专业人员

只允许符合各项工作要求的合格的专业人员进行操作。合格的专业人员必须遵照安全规范及警示提示，并具备资质进行产品编程、接地、标记电路等操作。

Warning



正确使用本设备及其组件只允许用于产品目录或技术文件中已规定的应用情况，如果需要使用其他公司的产品和组件，必须得到我司专业人员推荐和允许。本产品必须在正确搬运、存放、组装、装配、安装、调试、操作和维护的前提下正确运行。

责任免除



我们已对手册中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证手册中所述内容与硬件和软件完全一致。手册中的数据都按规定经过检测，必要的修正值。

关于在下一版本中的更新。欢迎与我们联系并提出改进意见。

主机及组件

安装启动本产品您将具备以下配件。表 1-1 将列举主要组及功能。

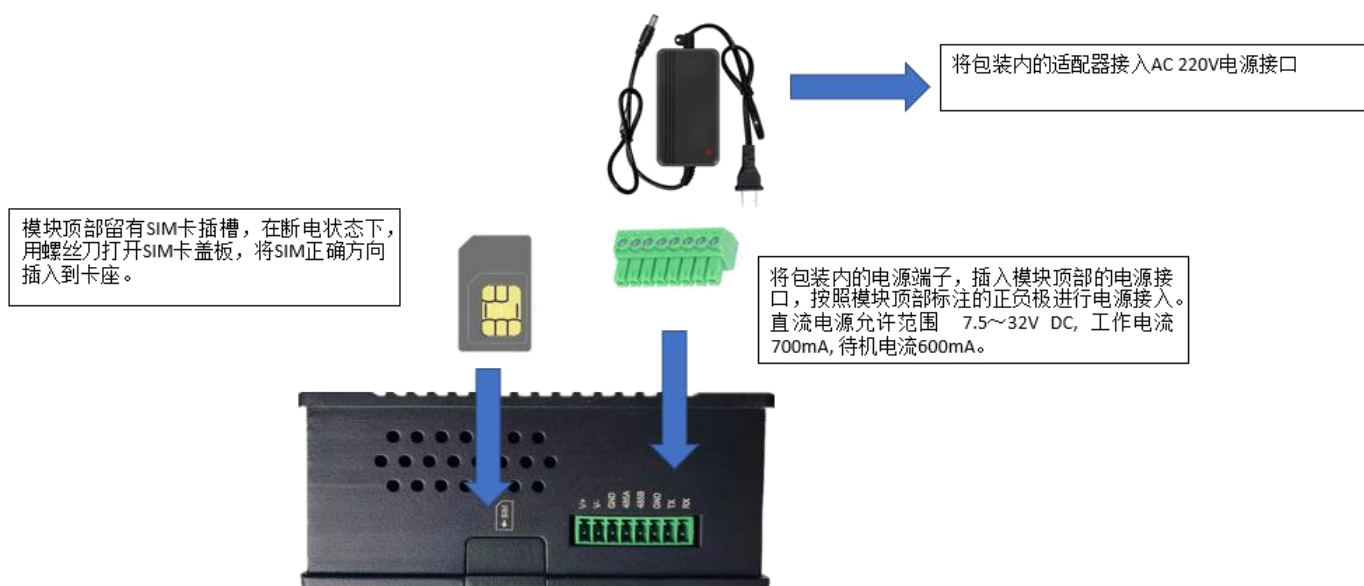
表 1-1 组件

<p>包装箱中包含 1 个主机</p>	
<p>包装箱中包含 1 个电源接线端子</p>	
<p>包装箱中包含 1 个适配器</p>	
<p>5G 天线（4 根）</p>	

安装介绍

本章将描述如何安装启动本模块产品。

第一步：连接电源和 SIM 卡



推荐采用模块包装内的电源适配器完成电源接入，如果违反该要求，超出该电源或者电压范围使用，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。



模块上部提供了一个标准尺寸 SIM 卡插槽，可以支持移动，联通，电信的 SIM 卡，如果是 Micro SIM 卡或者 Nano SIM 卡需要客户准备相应的卡托，之后再插入卡槽。

禁止将没有放入 Micro SIM 卡或者 Nano SIM 卡的空卡托直接插入卡槽，否则将会造成卡槽的损坏，如果违反该要求，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。



本产品支持 2 个 SIM 卡槽，可以选择任意一个插入 SIM 卡，均可以正常工作。



请在断电情况下插拔 SIM 卡，如果违反该要求，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。

第二步：连接天线和以太网接口



模块有 4 个千兆以太网端口。

默认使用 WAN/LAN1 端口作为宽带网络接入端口，同时该端口可配置成为普通 LAN 口接入常规以太网设备。

默认使用 LAN2-LAN4 端口作为常规以太网接口，接入常规以太网设备，包括各类控制系统、DCS、电脑、交换机等标准以太网设备。其中默认采用 LAN2 端口接入 PC 进行模块的组态和配置。

模块配有 4 根 5G 胶棒天线，天线增益为 3dBi。

可以通过 SMA 接头将天线和模块进行连接，为了获得最佳工作效果，需要同时接入所有天线。



模块通电之前，必须先完成天线连接，以免射频模组由于阻抗失配，导致信号受损而无法接入基站。如果违反该要求，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。



用户如果需要将天线放置于户外，需要对于延长线裸露在户外部分和室内部分的衔接处，进行必要的防水处理，以免水滴顺延长线进入模块天线或者电源部分造成模块损失。如果违反该要求，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。

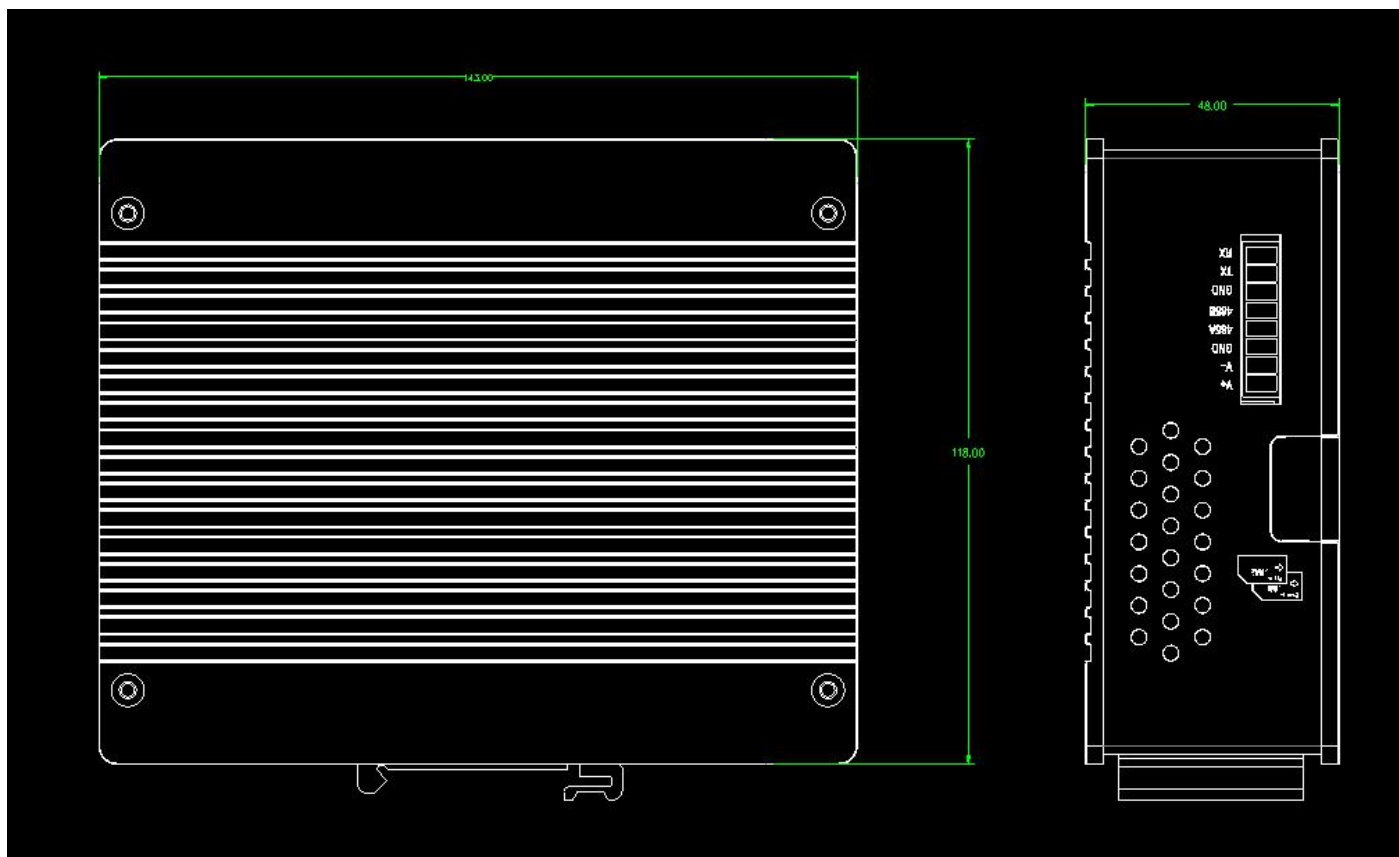


用户如果需要将天线放置于户外，推荐采用另外的馈线和避雷器等装置，如果未采取必要的避雷措施，由此造成的模块损坏，本司将不承担任何维修和赔偿责任。



除了包装内标准配置的天线和延长线之外，本司可为用户提供更远距离的延长线缆和馈线，和更强增益的全向、定向天线，该部分需要另外收费，详情请咨询本司销售人员。

以下为模块的外观尺寸，阅读相关信息有助于您完成模块的柜内设计安装。



一、设备信息

注意，插入和拔出 SIM 卡之前，请务必先对模块进行断电

PC 通过以太网接口连接 LAN2-LAN4 接口，该端口出厂 IP 地址为 **192.168.0.200**。

模块默认 LAN2、LAN3、LAN4 的 IP 地址为 192.168.0.200，默认 WAN\LAN1 位自动获取 IP 地址。

模块采用网页配置形式组态，无需安装其他多余的组态软件，推荐采用如下浏览器及以上版本（更好的支持HTML5的功能）对于模块进行配置：IE10、GOOGLE Chrome 35、FIREFOX 35、Safari 7 及以上的版本。

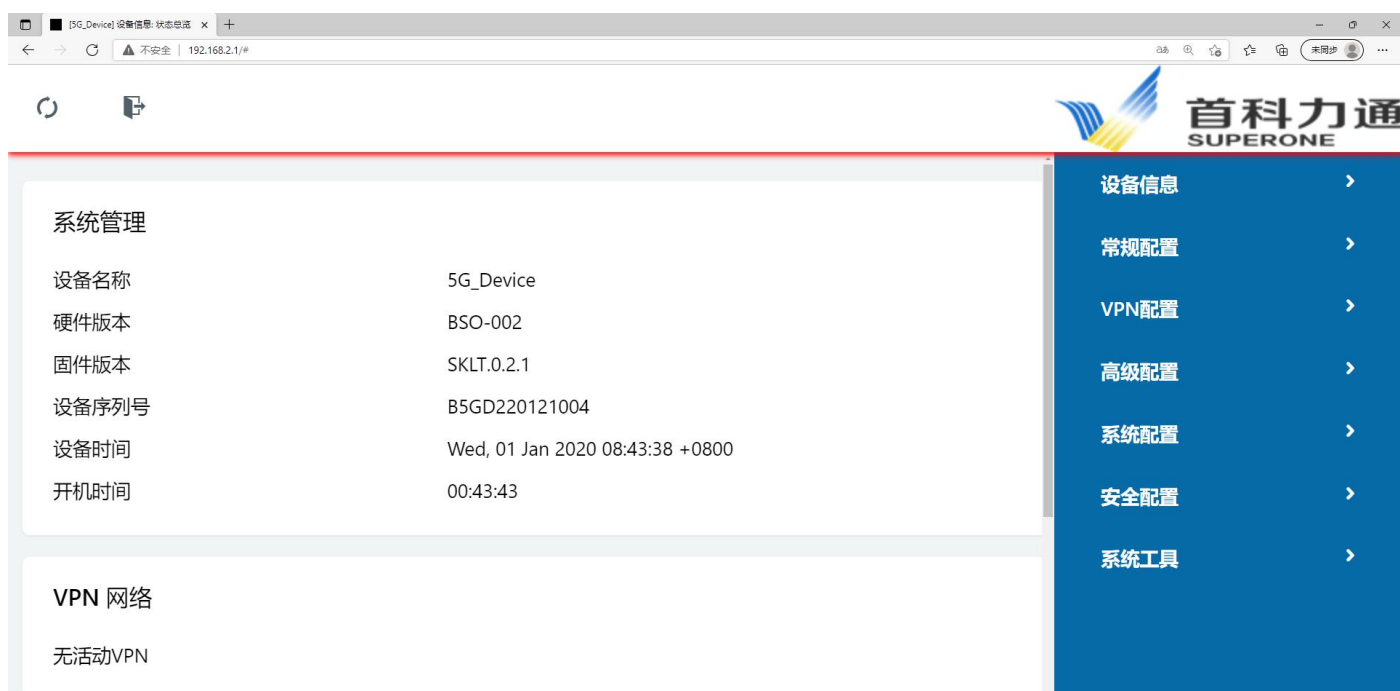
1、进入配置页面

把本地电脑的 IP 地址与所连接的模块端口配置成相同的 IP 网段，例如本案例中本地电脑配置成 192.168.0.123，然后在 GOOGLE Chrome 浏览器的地址框里面输入 192.168.0.200，点击回车键后，进入登录页面，默认的用户名为：**admin**，密码为：**123456**



The screenshot shows a web browser window displaying a login page for the device. The address bar shows the IP address 192.168.0.200. The page content includes the text "此网站要求您登录。" (This site requires you to log in.), a "用户名" (Username) field containing "admin", and a "密码" (Password) field with masked characters. There are "登录" (Login) and "取消" (Cancel) buttons at the bottom right.

填写用户名和密码后，进入到模块的配置页面如下图：



The screenshot shows the configuration page of the device. The browser address bar shows 192.168.2.1/#. The page features a navigation menu on the right with options: 设备信息 (Device Information), 常规配置 (General Configuration), VPN配置 (VPN Configuration), 高级配置 (Advanced Configuration), 系统配置 (System Configuration), 安全配置 (Security Configuration), and 系统工具 (System Tools). The main content area is divided into sections: "系统管理" (System Management) and "VPN 网络" (VPN Network). Under "系统管理", there is a table with device details:

设备名称	5G_Device
硬件版本	BSO-002
固件版本	SKLT.0.2.1
设备序列号	B5GD220121004
设备时间	Wed, 01 Jan 2020 08:43:38 +0800
开机时间	00:43:43

Under "VPN 网络", it shows "无活动VPN" (No active VPN).

2、状态总览

在配置页面的右侧导航条内，点击：**设备信息-状态总览**。

可以查看模块的各类运行状态，包括：

系统信息：

系统管理

设备名称	5G_Device
硬件版本	BSO-002
固件版本	SKLT.0.2.1
设备序列号	B5GD220121004
设备时间	Wed, 01 Jan 2020 08:46:02 +0800
开机时间	00:46:07

VPN状态和宽带WAN口状态：

VPN 网络

无活动VPN

联网方式	WAN网络
IP地址	192.168.10.10
子网掩码	255.255.255.0
网关	192.168.10.146
DNS服务器	192.168.10.146:53
连接状态	连接
已连接时间	00:46:18

移动网络状态：

移动网络

联网方式	ECM/QMI
Modem IMEI	863305040758483
Modem 状态	检测中...
运营商	
公网设置	
当前SIM卡	卡1工作中...
USIM 状态	失败
信号强度	0.0
IP地址	0.0.0.0
子网掩码	0.0.0.0
网关	0.0.0.0
DNS服务器	0.0.0.0
连接状态	断开
已连接时间	-

3、端口信息

在配置页面的右侧导航条内，点击：**设备信息-端口信息**。

可以查看模块 4 个千兆以太网端口（包括 WAN 口和 LAN 口）的各类状态信息，如下两图：

以太网端口状态



WAN网络

联网方式	DHCP
IP地址	192.168.10.10
子网掩码	255.255.255.0
网关	192.168.10.146
DNS服务器	192.168.10.146
连接状态	连接
已连接时间	00:50:40

局域网络

路由器 MAC 地址	34:0A:21:21:00:09
路由器 IP 地址	br0 - 192.168.2.1/24 br1 - 192.168.10.1/24
动态获取地址	br0 - Disabled br1 - Disabled

端口信息

网络接口	MAC 地址	IP地址 ^	名称	信号强度	信号质量	TX/RX 速率	剩余租约
br0	84:A9:38:7F:C9:6E	192.168.2.88			-		
br1	E4:90:69:A8:85:B4	192.168.10.82			-		
vlan2	90:2E:16:03:E9:70	192.168.10.142			-		
vlan2	74:59:09:08:C5:2A	192.168.10.146			-		

4、流量信息

在配置页面的右侧导航条内，点击：**设备信息-流量信息**。

可以查看网络接口的流量统计信息，如下图：

流量信息

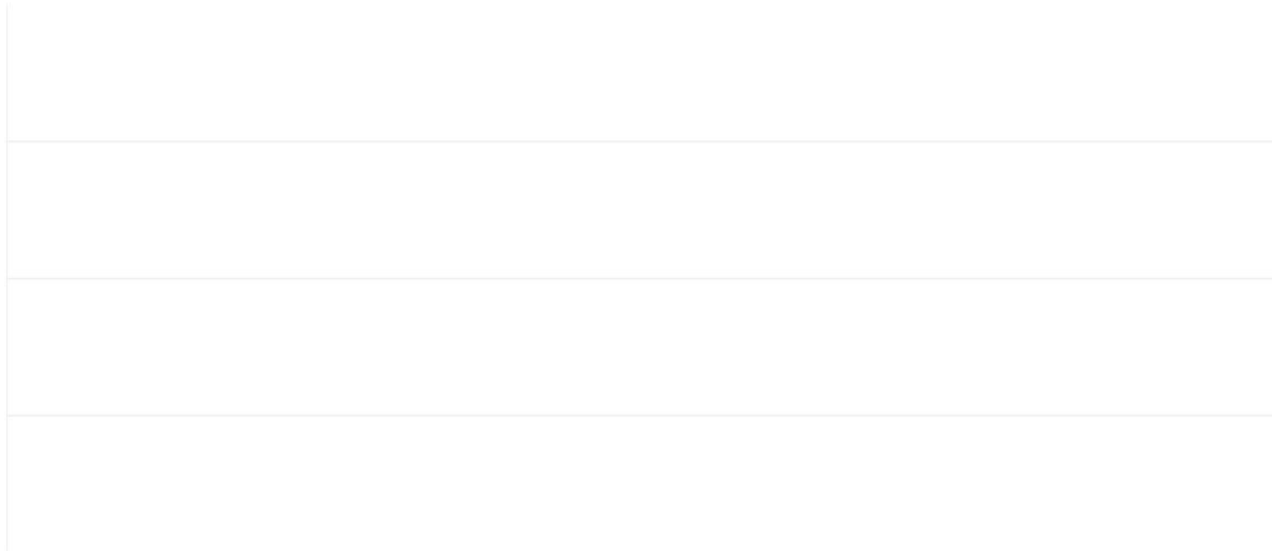
网络接口	发送流量	接收流量
WAN(vlan2)	10.32 MB	476.89 KB

5、流量检测

在配置页面的右侧导航条内，点击：**设备信息-流量检测**。

可以查看实时和历史流量信息，如下图：

实时 IP 流量监控



(分钟统计绘图窗口, 秒统计间隔)

接收
↓

平均
值

最大

总共

发送
↑

平均
值

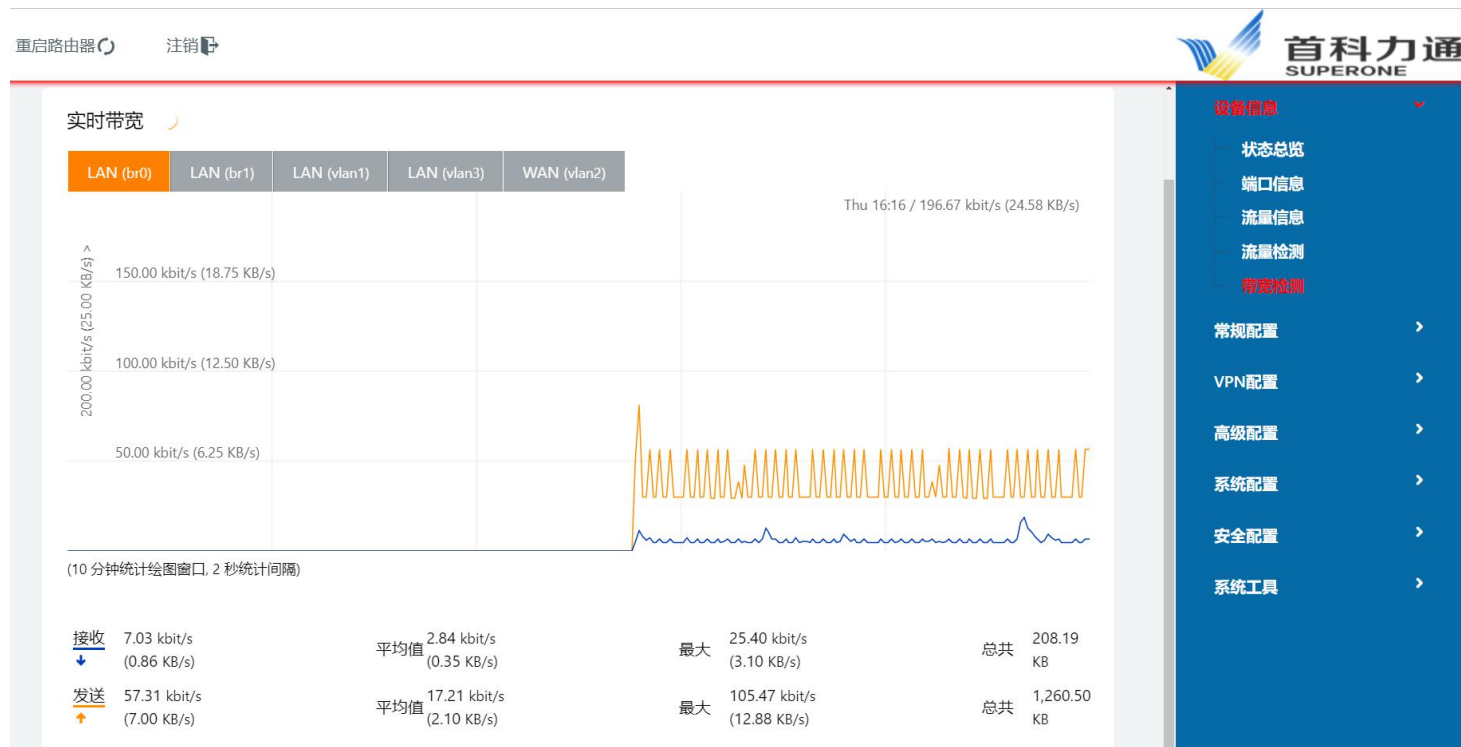
最大

总共

6、带宽检测

在配置页面的右侧导航条内，点击：**设备信息-带宽检测**。

可以查看不同通讯方式和端口的实时和历史带宽信息，如下图：



二、常规配置

1、端口设置：

在配置页面的右侧导航条内，点击：**常规配置-端口设置**。
可以修改配置 WAN\LAN 网络的相关参数。

1.1 WAN 口配置

其中 WAN 连接类型包括以下几种方式：动态获取地址、PPPoE、静态 IP 等接入方式。



1) 选择动态获取 IP 地址方式：则模块的 DHCP 客户端自动获取宽带服务器分配的 IP，通过 WAN 上网。

2) 选择 PPPoE 拨号获取 IP 方式，是通过 ADSL 拨号上网，需要填写相关服务信息，该部分填写内容请咨询您的 ISP 宽带服务提供方。

WAN / Internet

连接类型	PPPoE 拨号
用户名	<input type="text"/>
密码	<input type="password"/>
服务名称	<input type="text"/>
拨号模式	链路保持
检测间隔	10 (秒)
MTU	0 (0为系统默认)
多链路叠加	<input type="checkbox"/>

3) 选择静态 IP 地址，可手动填写需要的 IP 地址和网络信息。

WAN / Internet

连接类型	静态地址
IP地址	0.0.0.0
子网掩码	0.0.0.0
网关	0.0.0.0
MTU	0 (0为系统默认)

4) 如果需要关闭的话，则模块不再通过 WAN 口接入宽带网络。

1.2 LAN 口配置

可以修改配置局域网的相关参数。

WAN / Internet

连接类型	动态获取地址
MTU	0 (0为系统默认)

LAN

桥接 ^	IP地址	子网掩码	DHCP服务	IP地址范围	租约(分钟)
br0	192.168.2.1	255.255.255.0	×	-	
br1	192.168.10.1	255.255.255.0	×	-	

1) 桥接的接口默认为 br0 点击后可选择范围 0-3 来设定，一共 4 个选项；模块一共有 4 个千兆网口，都可以配置为 LAN 使用，所以此处最多可以填写 4 个桥接 (br)。桥接功能可以与后续介绍的 VLAN 功能一起使用，可以为不同的 LAN 口分配不同网段 IP 地址，或者将其中某几个 LAN 口绑定在一个 IP 网段上。

桥接 ^



A dropdown menu with a white background and a grey border. The top item is '0' with a downward arrow on the right. Below it, a list of items '0', '1', '2', and '3' is shown. The '0' item is highlighted with a grey background.

2) IP 地址和子网掩码，点击后都可以修改



Three input fields in a row. The first field contains '2' and has a dropdown arrow. The second field contains '192.168.0.200' and is highlighted with an orange border. The third field contains '255.255.255.0'.

删除 ×

取消 ⊙

确定 ✓

3) 也可以点击开启 DHCP 自动获取 IP 地址，并且指定地址范围以及有效时长。

DHCP服务	IP地址范围	租约(分钟)
<input checked="" type="checkbox"/>	192.168.0.2 192.168.0.51	1440

4) 举例，如下图设定了不同的 4 个 IP 网段对应 br0-br3, 每次填写完一个 br 之后，要点击“新增”对该填写部分进行保存。

LAN

桥接 ^	IP地址	子网掩码
br0	192.168.0.200	255.255.255.0
br1	192.168.1.150	255.255.255.0
br2	192.168.2.100	255.255.255.0
br3	192.168.3.50	255.255.255.0

1.3 设定 DNS 服务器

启用 DNS 服务器之后，可以填写主服务器和备用服务器的 IP 地址。

DNS

Use Custom DNS

主DNS服务器

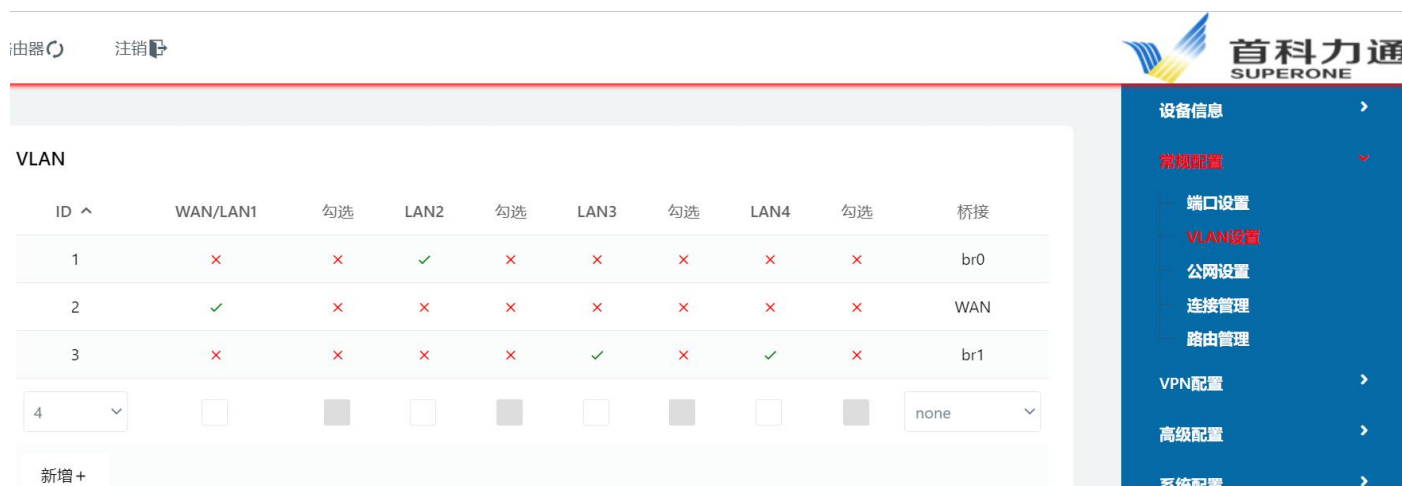
备用DNS服务器

该页面内容，配置完成后，单击页面右下角的“保存”按钮，此时设备会提示需要重启配置才会生效，可以点击立即重启，则设备会自动重启，以使相应配置生效。后续页面配置中也会采用同样方式保存配置内容。

2、VLAN 设置

在配置页面的右侧导航条内，点击：**常规配置-VLAN 设置**。

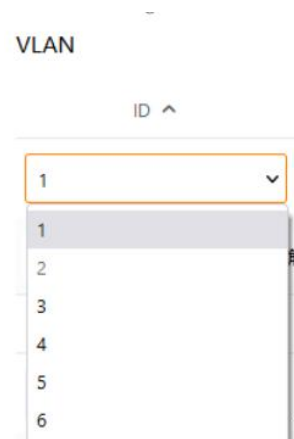
模块默认 LAN2、LAN3、LAN4 对应 br0 规则，上文中提到 br0 的 IP 地址为 192.168.0.200；默认 WAN/LAN1 对应 WAN 口规则，上文中提到 WAN 口默认配置为自动获取 IP 地址。



ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	×	×	✓	×	×	×	×	×	br0
2	✓	×	×	×	×	×	×	×	WAN
3	×	×	×	×	✓	×	✓	×	br1
4									none

2.1 VLAN 绑定 ID

每一个 VLAN 需要绑定一个 ID（ID 范围在 1-16），可以点击 ID 下拉菜单进行选择，也可以新增 VLAN 的 ID。每一个 ID 号代表一个不同的划分 VLAN 的规则，每一个 ID 号后面可以选择勾选不同的 LAN/WAN 口，选中后，该端口将会遵守这个 VLAN 的收发规则。



2.2 选择不同端口

选择了不同的 LAN 口之后，最后一列要对应刚才介绍的设定好的 br（0-3）桥接。

1) 选择 none, 表示该 ID 号内选中的 LAN 口，将不会生效，没有 IP 地址。

2) 选择 WAN, 表示该 ID 号内选中的 LAN 口，将会用作 WAN 口使用，WAN 口的具体设定规则，请参考前文中“1.1 WAN 口配置”相关内容。

3) 选择 br0-br3, 表示该 ID 号内选中的 LAN 口，IP 地址将会采用前文“1.2 LAN 口配置”中，已经设定好的 br 的 IP 地址。

2.3 举例说明：

1) 如下图配置，表示：

ID1: WAN/LAN1 端口勾选之后，分配为 WAN 口使用；

ID2: LAN2 端口勾选之后，分配 br0 的 IP 地址使用；

ID3: LAN3 端口勾选之后，分配 br1 的 IP 地址使用；

ID4: LAN4 端口勾选之后，分配 br2 的 IP 地址使用。

VLAN

ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	✓	✗	✗	✗	✗	✗	✗	✗	br3
2	✗	✗	✓	✗	✓	✗	✗	✗	br0
3	✗	✗	✗	✗	✗	✗	✗	✗	br1
4	✗	✗	✗	✗	✗	✗	✓	✗	br2

以下是前文中提到对于不同端口的配置内容。

WAN 口为自动获取，br0-br3 都分配了不同网段 IP 地址。

WAN / Internet

连接类型 动态获取地址 ▾

LAN

桥接 ^	IP地址	子网掩码
br0	192.168.0.200	255.255.255.0
br1	192.168.1.150	255.255.255.0
br2	192.168.2.100	255.255.255.0
br3	192.168.3.50	255.255.255.0

所以点击保存后，模块 4 个网口的配置信息对应关系如下：

接口	类型	IP	对应规则
WAN/LAN1	WAN 口	自动获取	WAN 口规则
LAN2	LAN 口	192.168.0.200	br0 规则
LAN3	LAN 口	192.168.1.150	br1 规则
LAN4	LAN 口	192.168.2.100	br2 规则

2) 如下图配置, 表示:

ID1: 把 WAN/LAN1 端口勾选之后, 分配 br3 的 IP 地址使用, 此时该端口不作为 WAN 口功能使用;

ID2: 把 LAN2 和 LAN3 端口勾选之后, 分配 br0 的 IP 地址使用;

ID3: 没有端口勾选;

ID4: 把 LAN4 端口勾选之后, 分配 br2 的 IP 地址使用。

VLAN

ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	✓	✗	✗	✗	✗	✗	✗	✗	br3
2	✗	✗	✓	✗	✓	✗	✗	✗	br0
3	✗	✗	✗	✗	✗	✗	✗	✗	br1
4	✗	✗	✗	✗	✗	✗	✓	✗	br2

所以点击保存后, 模块 4 个网口的配置信息对应关系如下:

接口	类型	IP	对应规则
WAN/LAN1	LAN 口	192.168.3.50	br3 规则
LAN2	LAN 口	192.168.0.200	br0 规则
LAN3	LAN 口	192.168.0.200	br0 规则
LAN4	LAN 口	192.168.2.100	br2 规则

根据该配置方式, 可以对于模块 4 个千兆网口, 分配各自的 IP 地址。



4 个网口中, 如果有一个以上的网口在同一个网段, 则这些网口的 IP 地址必须相同, 不支持分配相同网段中, 不同 IP 地址到不同的 LAN 网口。



建议保持一个 LAN 作为默认配置口的 IP 地址 192.168.0.200。

其他的 LAN1、LAN3、LAN4 可以根据应用要求进行不同网段 IP 地址的设定。

如果修改默认配置后, 且忘记网口 IP 地址, 可以采用 reset 按钮恢复出厂设置, 但是由此所造成的配置信息丢失, 本司将不承担任何赔偿责任。

2.4 勾选的应用：

每一个网口选中之后，后面还会出现“勾选”的选项（如下图）。

ID ^	WAN/LAN1	勾选
1	✓	✓

凡是被勾选的端口，都会被分配到同一个 VLAN 中，其发送和接收的数据包，都会被标注统一的 tag。

VLAN 网络划分的原则是，每一个 VLAN 中所有的网络端口，需要采用相同 ID 以及相同的 tag。

例如：

如下配置中，LAN2 和 LAN3 采用的是相同的 VALN ID，对应了相同的 IP 地址，同时勾选之后，2 个端口收发的数据包也会被标注相同的 tag，则这 2 个端口现在被划分到了一个相同的 VLAN 中。

而 LAN1 和 LAN4 都没有进行划分 VLAN。

VLAN

ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	×	×	×	×	×	×	×	×	
2	✓	×	×	×	×	×	×	×	WAN
3	×	×	✓	✓	✓	✓	×	×	br0

3、公网设置

配置页面的右侧导航条内，点击：**常规配置-公网设置**。

如果弹出如下，可以直接点击**不更新**。

要更新 http://192.168.0.200 的登录信息吗?

用户名

密码

显示密码(H)

在该页面配置运营商网络信息参数，如下图：

运营商网络配置

启用模块

SIM卡参数	SIM卡参数	其他参数	
启用PPP模式			<input type="checkbox"/>
ICMP检测			<input type="checkbox"/>
流量检查			<input type="checkbox"/>
MTU			<input type="text" value="0"/> (0为系统默认)
运营商锁定			<input type="text"/> 例如:46001
双卡模式			<input type="button" value="自动切换"/> v

3.1 启用模块

勾选启用或者关闭，如果关闭，将不能采用 5G 方式联网。

SIM 卡常规参数：

- 1) 启用 PPP 拨号方式，默认关闭，勾选后启用。
- 2) 启用 ICMP 检测，默认关闭，勾选后启用，并弹出如下配置内容：

ICMP检测	<input checked="" type="checkbox"/>
检测IP地址	8.8.8.8
检测IP地址 (可选)	4.4.4.4
间隔	60 (秒)
重试	3 (次)
异常处理	重启系统

可填写两个 IP 检测地址进行检测，默认采用第一个 IP 地址检测，若成功后，按照填写的间隔时长，进行下一次检测，若检测失败则会对第二个 IP 地址进行检测，若两个 IP 交替检测都失败，达到最大重试次数后，则会按照异常处理选项进行操作（重新拨号或者重启系统）。

- 3) 流量检测，默认关闭，勾选后启用，并弹出如下配置内容。

流量检查	<input checked="" type="checkbox"/>
检查模式	Rx
检测间隔	10 (分钟)范围: 1 ~ 1440
异常处理	重新拨号

检测模式，可选择收取流量，发送流量和收发流量的方式。

开启流量检测后，模块会按照设定间隔，检测运营商网络是否产生数据流量，如果在检测时间内没有流量产生，则会按照异常处理选项进行操作（重新拨号或者重启系统）。

- 4) 运行商锁定：可以锁定某个运行商的网络，需要咨询移动运营商。
- 5) 双卡模式：模块支持 2 张 SIM 卡同时插入，并且可以选择 4 种应用模式

双卡模式

自动切换

自动切换

仅卡1

仅卡2

备份

自动切换模式：2张SIM卡可以自动切换，卡1不能联网则切换到卡2上网，之后保持使用卡2上网，即使卡1可以恢复网络了也不切回卡1。

仅卡1 或者仅卡2：只选择一张SIM卡，不进行交换。

备份模式：2张SIM卡可以自动切换，卡1不能联网则切换到卡2上网，卡1恢复网络之后，自动从卡2切换回卡1继续工作。

SIM卡1、2参数，如下图：

SIM卡参数	SIM卡参数	其他参数
SIM 1 网络模式	Auto	
SIM 1 5G网络制式	SA & NSA	
SIM 1 PIN码		
SIM 1 APN接入点	3GNET	
SIM 1 用户名	CARD	
SIM 1 密码	••••	
SIM 1 拨号号码	*99#	
SIM 1 认证方式	Auto	
SIM 1 本地IP地址		

1) SIM1 的网络模式，可选择如下，默认为自动。

Auto

- Auto
- 5G NR
- LTE(FDD/TDD)
- 3G(WCDMA/TD-SCDMA/HSPA)
- 3G(CDMA 2000/CDMA 1x)

2) SIM 1 5G 网络制式，可选择如下，默认为 SA&NSA 兼容。



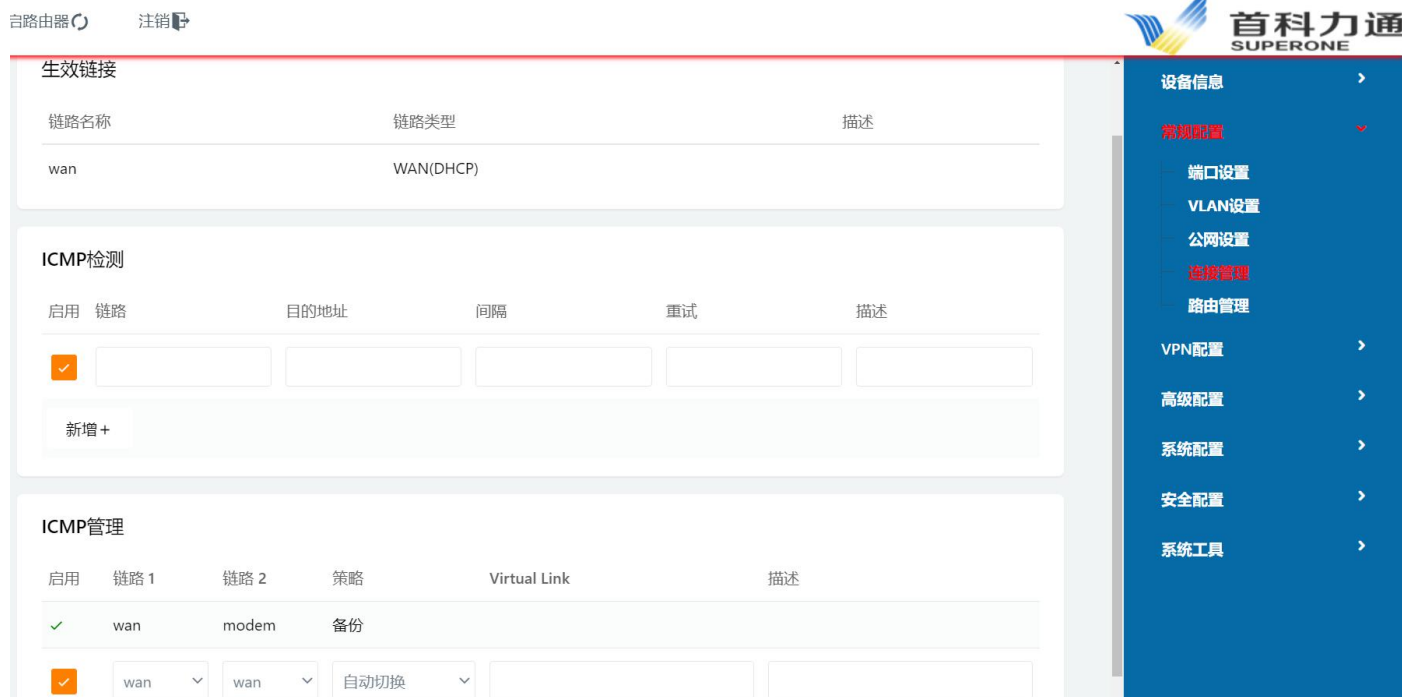
3) 以下内容需要咨询相关运营商进行填写。

SIM 1 PIN码	<input type="text"/>
SIM 1 APN接入点	3GNET
SIM 1 用户名	CARD
SIM 1 密码	••••
SIM 1 拨号号码	*99#
SIM 1 认证方式	Auto
SIM 1 本地IP地址	<input type="text"/>

4、连接管理

配置页面的右侧导航条内，点击：**常规配置-连接管理**。

进入连接管理页面，该功能主要应用于 5G 网络和有线网络相互备份链路的应用。



The screenshot shows the '连接管理' (Connection Management) page. It features three main sections:

- 生效链接 (Active Links):** A table with columns for '链路名称' (Link Name), '链路类型' (Link Type), and '描述' (Description). It lists a 'wan' link of type 'WAN(DHCP)'.
- ICMP检测 (ICMP Detection):** A table with columns for '启用' (Enabled), '链路' (Link), '目的地址' (Destination Address), '间隔' (Interval), '重试' (Retries), and '描述' (Description). The 'wan' link is checked for ICMP detection.
- ICMP管理 (ICMP Management):** A table with columns for '启用' (Enabled), '链路 1' (Link 1), '链路 2' (Link 2), '策略' (Strategy), 'Virtual Link', and '描述' (Description). It shows 'wan' as Link 1, 'modem' as Link 2, and '备份' (Backup) as the strategy.

The right sidebar contains a navigation menu with options: 设备信息, 常规配置 (highlighted), 端口设置, VLAN设置, 公网设置, 连接管理 (highlighted), 路由管理, VPN配置, 高级配置, 系统配置, 安全配置, 系统工具.

4.1 此处默认有 2 个生效链路

modem 代表 5G/4G/3G 的运行商网络，wan 代表有线宽带网络。

生效链接	
链路名称	链路类型
modem	ECM/QMI
wan	WAN(DHCP)

4.2 选择链路

在 ICMP 管理页面中，点击启用 ICMP 管理之后，可以选择 2 个链路，以及对应的策略。例如链路 1 选择 WAN 口宽带网络，链路 2 选择 modem 5G 网络，策略选择备份。



The screenshot shows the configuration form for ICMP Management. The '启用' (Enabled) checkbox is checked. The '链路 1' (Link 1) dropdown is set to 'wan', '链路 2' (Link 2) is set to 'modem', and '策略' (Strategy) is set to '备份' (Backup). A dropdown menu is open for '链路 1', showing options 'wan', 'modem', and 'wan'.

启用	链路 1	链路 2	策略
<input checked="" type="checkbox"/>	wan	modem	备份
删除 ×	取消	确定 ✓	

启用	链路 1	链路 2	策略
<input checked="" type="checkbox"/>	wan	modem	备份
删除 ×	取消	确定 ✓	自动切换 备份

按照如上设定之后，当链路 1（宽带）在线时，链路 1 保持数据通讯；当链路 1 经过 ICMP 检测失效后，会切换至链路 2（5G 网络）；而当链路 1 经过 ICMP 检测恢复生效后，又会重新采用链路 1 进行数据通讯。

如果策略选择自动切换模式，则当链路 1（宽带）在线时，链路 1 保持数据通讯；当链路 1 经过 ICMP 检测失效后会切换至链路 2（5G 网络）；而当链路 1 经过 ICMP 检测恢复生效后，不会进行切换，仍然采用链路 2 进行数据通讯，直到链路 2 经过 ICMP 检测失效后会切换至链路 1。

4.3 ICMP 检测参数配置

ICMP管理

启用	链路 1	链路 2	策略	Virtual Link	描述
<input checked="" type="checkbox"/>	wan	modem	备份		
<input checked="" type="checkbox"/>	wan	wan	自动切换		
新增 +					

此处填写内容为：

链路：模块采用 5G 网络或者宽带和外部通讯，所以此处只能填写：modem 或者 wan，不能添加新的链路名称。

目的地址：链路需要检测的 IP 地址或者域名，例如：内网 DNS 服务器地址 192.168.0.99，或者外网的域名 www.baidu.com。

检测该 IP 地址或者域名的时间间隔（s）

检测失败后重试次数。

4.4 如下图，举例：

生效链接

链路名称	链路类型
modem	ECM/QMI
wan	WAN(DHCP)

ICMP检测

启用	链路	目的地址	间隔	重试
✓	wan	www.baidu.com	3	5
✓	modem	www.baidu.com	3	5
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

新增 +

ICMP管理

启用	链路 1	链路 2	策略	Virtual Link
✓	wan	modem	备份	

1) 目前两个生效链路 modem 采用 5G 方式联网，wan 口自动获取 IP 方式通过宽带联网。

2) 两个链路之间采用备份策略，优先采用 WAN 口宽带方式连接外网，检测的目的域名为百度的网址，每隔 3 秒，模块会检测一次是否可以 PING 通百度域名，如果宽带网络出现问题，重试 5 次之后，未 PING 通百度网址，则会切换到 5G 方式联网。

3) 当 WAN 口恢复正常上网功能之后，可以 PING 通百度网址，则继续切换回 WAN 口宽带继续上网。



如果 5G 和 WAN 口连接内网的情况下，可以在“常规配置-端口设置”中设定 DNS 服务器地址，此时链路检测的目标地址可以采用服务器地址。



如果是设备确定只采用一种方式联网，需要将 ICMP 联络检测功能关闭，否则模块将会按照设定间隔和次数重复检测不同端口的状态。

例如：移动车辆设备，只采用 5G 移动网络方式联网，不采用 WAN 口联网时，如果 WAN 口没有关闭，且 ICMP 开启，当移动网络信号减弱，则模块会自动消耗时间去检测 WAN 口是否可以用于通讯，在这段时间内移动网络的通讯将会受到较为严重的影响。如果违反以上原则，由此操作所造成任何损失，本司将不承担任何责任。

5、路由管理

配置页面的右侧导航条内，点击：**常规配置-路由管理**。
 进入如下配置页面。

5.1 当前路由表

查看当前的路由路径。

当前路由表

目的地址	网关 / 下一跳	子网掩码	跃点数	网络接口
default	192.168.10.146	0.0.0.0	0	wan
127.0.0.0	*	255.0.0.0	0	lo
192.168.2.0	*	255.255.255.0	0	lan
192.168.10.0	*	255.255.255.0	0	lan1

5.2 静态路由表

需要在静态路由表中，手动添加相关信息，为转发数据包提供具体的转发路径。

静态路由表

目的地址	网关	子网掩码	跃点数	网络接口	描述
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="la"/> ▾	<input type="text"/>
<input type="button" value="新增 +"/>					

5.3 策略路由表

需要对前文中划分的不同 VLAN 网络，采取的上网方式进行策略设定。

策略路由表

Lan	modem	wan	sta	sta2
vlan1 ▾	Auto ▾	Auto ▾	Auto ▾	Auto ▾
新增 +				

举例：

1) 在端口设置中，对 br0-br2 做了设定。

LAN

桥接 ^	IP地址	子网掩码
br0	192.168.0.200	255.255.255.0
br1	192.168.1.200	255.255.255.0
br2	129.168.2.200	255.255.255.0

2) 在 VLAN 设置中，把 LAN1-LAN4 分配到了不同 VLAN ID 中，对应了不同的桥接，从而分配了不同的 IP 地址，

ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	×	×	✓	×	✓	×	×	×	br0
2	✓	×	×	×	×	×	×	×	br1
3	×	×	×	×	×	×	✓	×	br2

LAN1、VLAN ID 是 2，IP 地址是 192.168.1.200

LAN2 和 LAN3、VLAN ID 是 1，IP 地址是 192.168.0.200

LAN4、VLAN ID 是 3，IP 地址是 192.168.2.200

3) 在策略路由表中对不同 VLAN ID 进行上网策略配置。

Modem: 表示采用 5G 上网方式，wan 表示采用宽带上网方式，sta&sta2 缺省，无需配置。

Only: 表示只采用该方式。

Primary: 表示优先采用该方式，**Secondary:** 表示可以采用该方式，但是优先级较低。

Auto: 表示自动，但是不能同时 modem 和 wan 都选择自动方式。

策略路由表

Lan	modem	wan
vlan1	Only	
vlan2	Primary	Secondary
vlan3		Only

如上举例中：

VLAN ID 1: 代表 LAN2 和 LAN3 端口，IP 地址为 192.168.0.200，只能采用 5G 方式联网。

VLAN ID 2: 代表 LAN1 端口，IP 地址为 192.168.1.200，优先采用 5G 方式联网，WAN 口可用但是优先等级低。

VLAN ID 3: 代表 LAN4 端口，IP 地址为 192.168.2.200，只能采用 WAN 口方式联网。

5.4 OSPF

开放最短路径优先协议。

OSPF 使用短路径优先算法来构建和计算到所有已知目的地的最短路径。本手册中不做进一步详细的介绍，建议保持默认的配置。

5.5 “其他设置”

1) 网路模式，选择模块作为网关或者路由，默认采用网关方式，完成现场设备通过模块 LAN 口接入 5G 或者宽带网络，连接服务器。如果修改为路由方式，则会完成 IP 地址的路由映射，可能造成和服务器通讯配置失效。

请保持默认值。

2) RIPv1 & v2，是一种分布式的基于距离向量的路由选择协议。本手册中不做进一步详细的介绍，建议保持默认的配置。

3) DHCP 路由和生成树协议，本手册中不做进一步详细的介绍，建议保持默认的配置。



非网络专业人士，不建议修改该部分内容的默认值，如果违反以上原则，由此操作所造成任何损失，本司将不承担任何责任。

三、VPN 配置

模块默认支持 Open VPN 方式，且采用该方式和数据中心设备管理平台，或远程云端平台完成通讯。

客户如果需要选择采用其他 VPN 方式，可以咨询您的销售代表，以便获取进一步的详细信息，本手册中不再对其他 VPN 的应用进行介绍和举例。

点击右侧配置导航栏中 **VPN 配置-OPEN VPN 配置**。

进入如下配置页面，为了简化用户配置操作步骤，本产品已经固化了大部分基础配置内容，客户只需保持默认选项即可。该部分内容请参考《**管理平台启动手册**》中的相关内容。



需要用户手动填写的部分为，基本配置中，数据中心管理平台或者远程云平台的服务器 IP 地址和端口号。

服务器地址

需要用户手动添加的部分为，密钥设置中，为每一个 5G 终端分配的独立的密钥证书。

客户端

基本设置 高级设置 密钥设置 状态

VPN客户端 #1 (正在运行)

关于生成密钥, 请参考OpenVPN HOWTO.

客户端证书

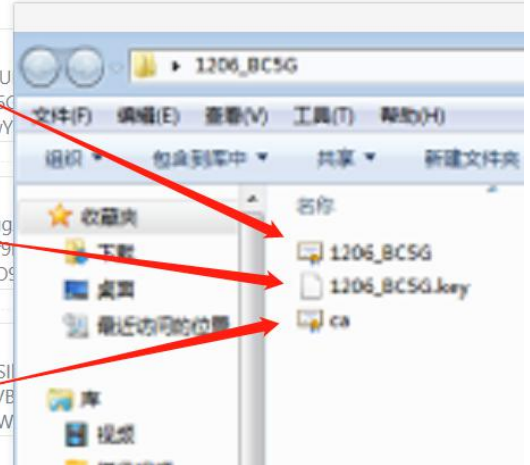
```
-----BEGIN CERTIFICATE-----  
MIID1DCCAz2gAwIBAgIBBTANBgkqhkiG9w0BAQU  
CzAJBgNVBAGTAKNBMRUwEwYDVoQHEwYDQwYwY  
YWNvbjEPMA0GA1UECzMGMQ8wDQYDVoQLEwZCZW
```

客户端密钥

```
-----BEGIN PRIVATE KEY-----  
MIICdglBADANBgkqhkiG9w0BAQEFAASCAmAwgg  
gKwfJotNQFFjYSwdnqWTMUMzQWjpJZ3Ck7Wrt9  
r3jF2rQzrp/O+7NEz2NfnPUkKeL1a1tRhI9yftNukO9
```

证书授权中心

```
-----BEGIN CERTIFICATE-----  
MIIDfjCCAuegAwIBAgIJAOvIRk11jip6MA0GCSqGSI  
VQQQEwJVUzELMAkGA1UECmQ0ExFTATBgNVB  
A1UEChMGQmVhY29uMQ8wDQYDVoQLEwZCZW
```



不建议修改该部分内容的其余参数默认值, 如果违反以上原则, 可能会造成无法和管理平台或者云平台正常通讯, 由此操作所造成任何损失, 本司将不承担任何责任。

四、高级配置

完成常规配置和 VPN 配置之后，模块即可和数据中心服务器或者远程远端平台进行通讯了。

本章节内容主要针对某些特殊应用，进行功能拓展，如果无其他特殊要求，请务必保持本章的各项内容，设定为默认值。

1、转发设定

在右侧配置导航栏中，点击：**高级配置—转发设定**。

进入如下配置页面：



端口转发功能主要是完成一个外部用户从外部经过一个被激活的 NAT 路由器，到达一个内网 IP 地址（局域网内部）。点击启用后，可填写相关参数。

1.1 协议部分

可从下拉菜单中选择。



1.2 外部 IP

外部 IP 可不用填写。

可填写特定 IP 地址，例如：188.188.188.188，

可以填写 IP 范围，例如：1.1.1.2 - 1.2.3.4”，

1.3 外部端口

从外部网络包括 WAN 口或者 5G 网络，进入模块的外部端口号。

1.4 内部端口

可不用填写，会自动认为是和外部端口保持一致。
若内部端口与外部端口不同时，须填入内部端口号。

1.5 内部 IP 地址

需要填写 LAN 口所连接内部局域网设备的 IP 地址。

举例，如下图：外部以太网设备通过 WAN 口或者 5G 网络，可以对于端口号为 1920 的 IP 地址 192.168.0.156 的设备进行通讯。

启用	协议	外部IP	外部端口	内部端口	内部 IP
<input checked="" type="checkbox"/>	TCP		1920		192.168.0.156



端口转发功能默认为关闭，启用后可能会造成外部设备对内网设备进行攻击，建议谨慎操作，由此造成的任何损失，本司将不承担赔偿责任。

2、DMZ 设定

在右侧配置导航栏中，点击：**高级配置—DMZ 设定**。

DMZ	
启用DMZ	<input type="checkbox"/>
内部地址	<input type="text" value="192.168.0.0"/>
外部IP限制	<input type="text"/>
允许CLI远程访问	<input checked="" type="checkbox"/>
允许WEB远程访问	<input checked="" type="checkbox"/>

DMZ 功能为了解决启用防火墙后，外部网络的用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。



DMZ 功能默认为关闭状态，启用后指定的内部 IP 的 PC 或者服务器，会完全暴露于公网，其所有端口都会向公网进行开放，可能会造成外部设备对该内网设备进行攻击，建议谨慎操作，由此造成的任何损失，本司将不承担赔偿责任。

2.1 勾选之后启用 DMZ 相关配置

2.2 填写内部地址

此处选择一个内部局域网 IP 进行填写，填写后该 IP 地址的设备将会暴露于外网。

2.3 可以选择特定 IP 地址

例如：192.168.77.77；或者 IP 地址范围，例如：192.168.77.77–192.168.88.88；或者特定 IP 地址/端口号，例如：192.168.77.77/345。

2.4 可选择是否允许 CLI 或者 WEB 对该暴露的 IP 地址设备进行远程访问

举例：将内网 IP 地址为 192.168.0.250 的设备设定为 DMZ 缓冲区，该设备所有端口均对外网开放。

允许外网中 IP 地址范围在 1.2.3.4–1.2.3.200 内的设备对该设备进行访问，同时允许采用 CLI 或者 WEB 方式远程访问。

DMZ	
启用DMZ	<input checked="" type="checkbox"/>
内部地址	<input type="text" value="192.168.0.250"/>
外部IP限制	<input type="text" value="1.2.3.4-1.2.3.200"/>
允许CLI远程访问	<input checked="" type="checkbox"/>
允许WEB远程访问	<input checked="" type="checkbox"/>

3、本地 NAT

在右侧配置导航栏中，点击：**高级配置—本地 NAT**。

进入如下页面，该部分功能主要介绍了如何完成 LAN 口所连接的相同网段 IP 地址的设备，通过 1:1 NAT 转换的规则，转化为 WAN 口所连接的不同网段（或相同网段）的 IP 地址。当现场设备 IP 地址冲突，IP 网段过多，或者 IP 地址资源不足的时候，可以利用该功能进行解决，最大转化数量为 50 条。

本地NAT		
启用	外网IP地址	内网IP地址
<input checked="" type="checkbox"/>	192.168.10.16	192.168.1.16
<input checked="" type="checkbox"/>	192.168.10.26	192.168.1.6
<input checked="" type="checkbox"/>	192.168.100.8	192.168.1.3
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="新增 +"/>		
可配置NAT链路数量: 47		

3.1 勾选 启用后，该条规则生效

3.2 外部 IP 地址

WAN 口所连接的设备的网段内的 IP 地址，可以根据现场设备实际情况填写，且无需设定和 WAN 口相同网段，IP 地址可以是相同网段或者不同网段。注意此时，在“常规配置-端口设置”中，一般建议对 WAN 口设定为静态 IP 地址，该固定 IP 地址无需和现场实际设备在相同网段内。

WAN / Internet

连接类型	静态地址
IP地址	<input type="text"/>
子网掩码	<input type="text"/>

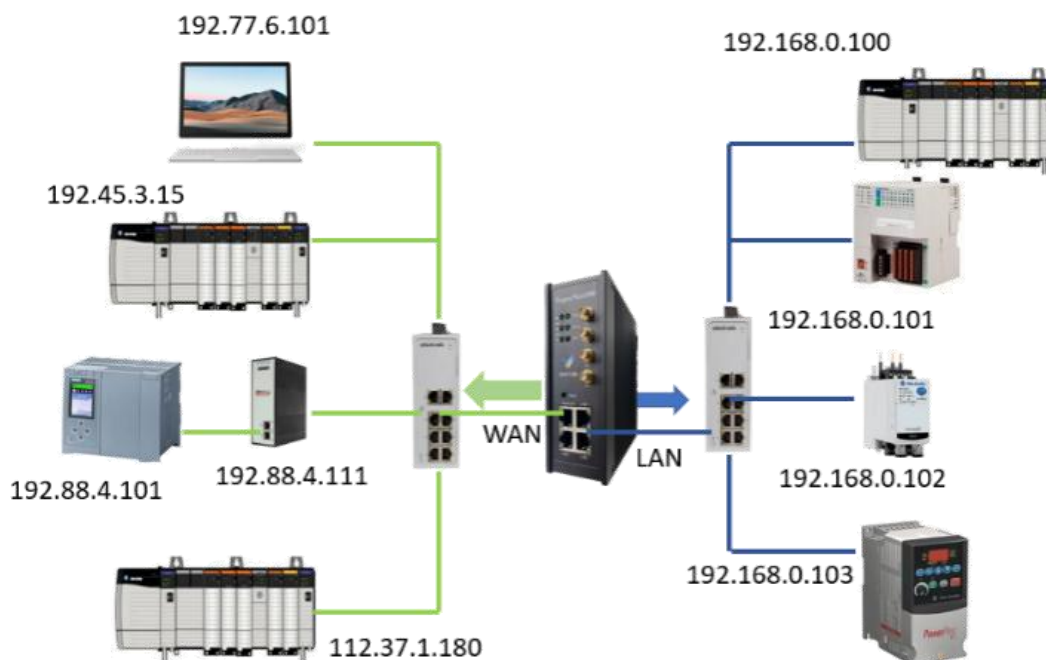
3.3 内部 IP 地址

LAN 所连接的设备的 IP 地址，注意通过 VLAN 功能，LAN2-LAN4 可以采用 3 个不同的 IP 网段，可参考前文中“常规配置”，端口设置以及 VLAN 设置”的相关内容，此处不做过多介绍。

3.4 举例

现场设备 IP 地址分布如下：

本地 NAT 配置内容如下，保存生效后：



本地NAT

启用	外网IP地址	内网IP地址
✓	192.77.6.100	192.168.0.100
✓	192.45.3.100	192.168.0.101
✓	192.88.4.100	192.168.0.102
☑	112.37.1.100	192.168.0.103

IP 地址为 192.77.6.101 的上位机，可以连接（原始 IP 为 192.168.0.100）PLC，其 IP 地址转换为 192.77.6.100；

IP 地址为 192.45.3.15 的 PLC，可以连接（原始 IP 为 192.168.0.101）PLC，其 IP 地址转换为 192.45.3.100；

IP 地址为 192.88.4.101 的西门子 PLC，可以通过协议转换网关，连接（原始 IP 为 192.168.0.102）E300 马达保护器，其 IP 地址转换为 192.88.4.100；

IP 地址为 112.37.1.180 的 PLC，可以连接（原始 IP 为 192.168.0.103）变频器，其 IP 地址转换为 112.37.1.100。



启用本地 NAT 功能之后，该功能可以良好的解决本地网络中 IP 地址冲突，IP 网段过多，或者 IP 地址资源不足的问题。但是开启本地 NAT 功能后不推荐同时开启云端 NAT 功能。不推荐同时开启 WAN/5G 之间的 ICMP 链路检测功能。如果违反以上原则，由此操作所造成网络风暴，数据丢失等任何损失，本司将不承担赔偿责任。

4、云端 NAT

在右侧配置导航栏中，点击：**高级配置—云端 NAT**。

进入到云端 NAT 配置页面，该页面主要解决现场不同网段设备，同时连接到管理平台或者远程云端平台的问题。因为模块通过 5G 网络或者宽带网络，连接管理平台或者远程云端平台时，需要所有 LAN 口连接的外部设备在同一个网段内，所以此处需要将不同网段的设备的 IP 地址，做 1:1 的转换。

云端 NAT

启用	IP地址	子网掩码	网关	虚拟IP地址	描述
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
新增 +					

可配置NAT链路数量：48

4.1 参数配置

- 1) 勾选 启用后该条规则生效
- 2) IP 地址：该地址为实际 LAN 口所连接现场设备的 IP 地址
- 3) 子网掩码和网关：为实际 LAN 口所连接现场设备的相关信息
- 4) 虚拟 IP 地址：此处填写模块转发到管理平台或者远程云端平台时采用的 IP 地址
- 5) 填写完成后点击新增，保存该条转换规则，点击保存-重启，生效所有的配置内容。
- 6) 可用于转换的 IP 地址最大为 50 条。

4.2 举例说明

模块有 4 个以太网口，默认情况下，LAN1 用于 WAN 口通讯，LAN2、LAN3、LAN4 负责连接现场实际设备。

首先通过前文中“**常规配置—端口配置—VLAN 配置**”中提到内容，将 LAN2、LAN3 和 LAN4 划分到不同网段。具体步骤如下：

在端口配置中，添加 **br0** 对应的 IP 地址 192.168.2.1，添加 **br2** 对应的 IP 地址 192.168.20.1，添加 **br3** 对应的 IP 地址 192.168.30.1，添加后，点击保存。

重启路由器  注销 

配置已修改，部分配置重启之后才能生效！ [立即重启](#)

WAN / Internet

连接类型:

MTU: (0为系统默认)

LAN

桥接 ^	IP地址	子网掩码	DHCP服务	IP地址范围	租约(分钟)
br0	192.168.2.1	255.255.255.0	✘	-	
br2	192.168.20.1	255.255.255.0	✘	-	
br3	192.168.30.1	255.255.255.0	✘	-	

设备信息 >

常规配置 >

端口设置

VLAN设置

公网设置

连接管理

路由管理

VPN配置 >

高级配置 >

系统配置 >

安全配置 >

系统工具 >

下一步，将刚才设定的 br0、br2、br3 的 IP 地址，分配给 LAN2、LAN3 和 LAN4，如下图：

配置已修改，部分配置重启之后才能生效！ [立即重启](#)

VLAN

ID ^	WAN/LAN1	勾选	LAN2	勾选	LAN3	勾选	LAN4	勾选	桥接
1	✘	✘	✔	✘	✘	✘	✘	✘	br0
2	✔	✘	✘	✘	✘	✘	✘	✘	WAN
3	✘	✘	✘	✘	✔	✘	✘	✘	br2
4	✘	✘	✘	✘	✘	✘	✔	✘	br3

5 none

新增 +

设备信息 >

常规配置 >

端口设置

VLAN设置

公网设置

连接管理

路由管理

VPN配置 >

高级配置 >

系统配置 >

安全配置 >

系统工具 >

取消 ✕ 保存 ✓

模块默认采用 LAN2 的 IP 网段连接管理平台或者远程云端平台，所以此时需要配置 LAN3、LAN4 以太网口连接的现场设备变成虚拟 LAN2 的 IP 地址。虚拟 IP 地址要与 LAN2 保持一个网段才可以添加到管理平台。配置完成，保存，**重启**。

此时的对应关系如下：

接口	类型	端口 IP	对应规则	连接设备实际 IP	连接设备上云 IP
WAN/LAN1	WAN 口	自动获取	WAN 口规则		
LAN2	LAN 口	192.168.2.1	br0 规则	192.168.2.5	192.168.2.5
LAN3	LAN 口	192.168.20.1	br2 规则	192.168.20.10	192.168.2.10
LAN3	LAN 口	192.168.20.1	br2 规则	192.168.20.11	192.168.2.11
LAN4	LAN 口	192.168.30.1	br3 规则	192.168.30.12	192.168.2.12
LAN4	LAN 口	192.168.30.1	br3 规则	192.168.30.13	192.168.2.13

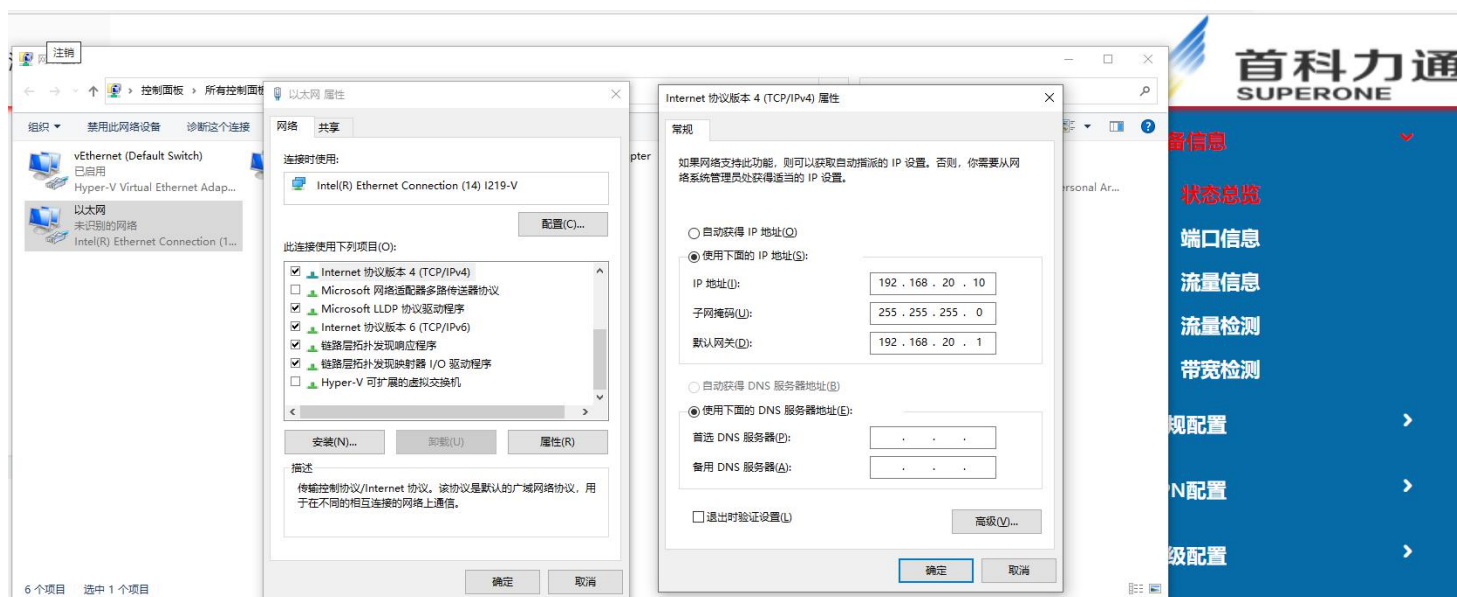
在管理平台添加对应的虚拟的 IP 地址, 正常通讯后, **Status** 会变成绿色。

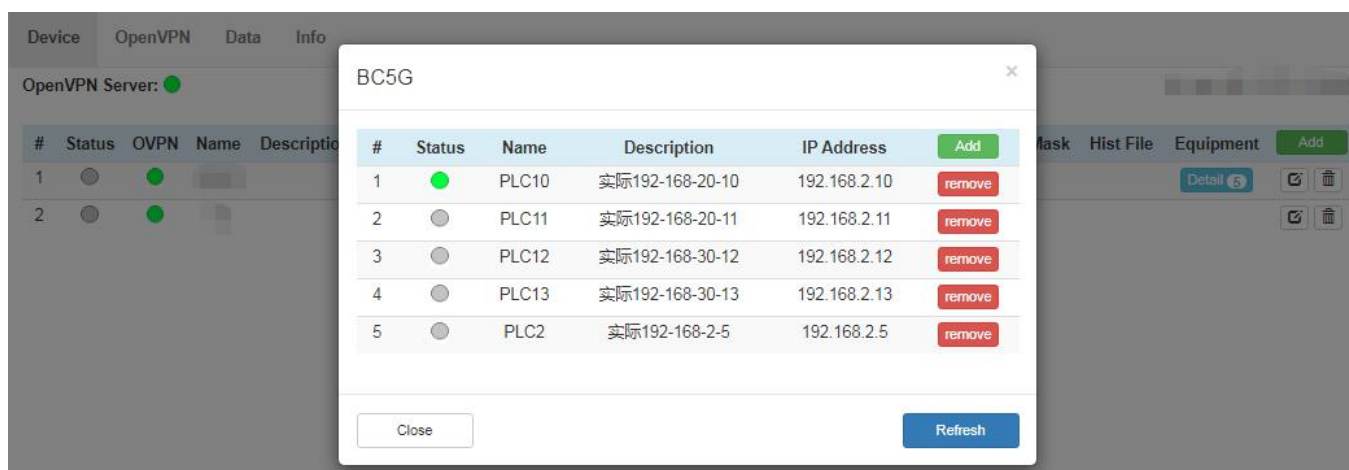
#	Status	Name	Description	IP Address	Add
1	●	PLC10	实际192-168-20-10	192.168.2.10	remove
2	●	PLC11	实际192-168-20-11	192.168.2.11	remove
3	●	PLC12	实际192-168-30-12	192.168.2.12	remove
4	●	PLC13	实际192-168-30-13	192.168.2.13	remove
5	●	PLC2	实际192-168-2-5	192.168.2.5	remove

Close Refresh

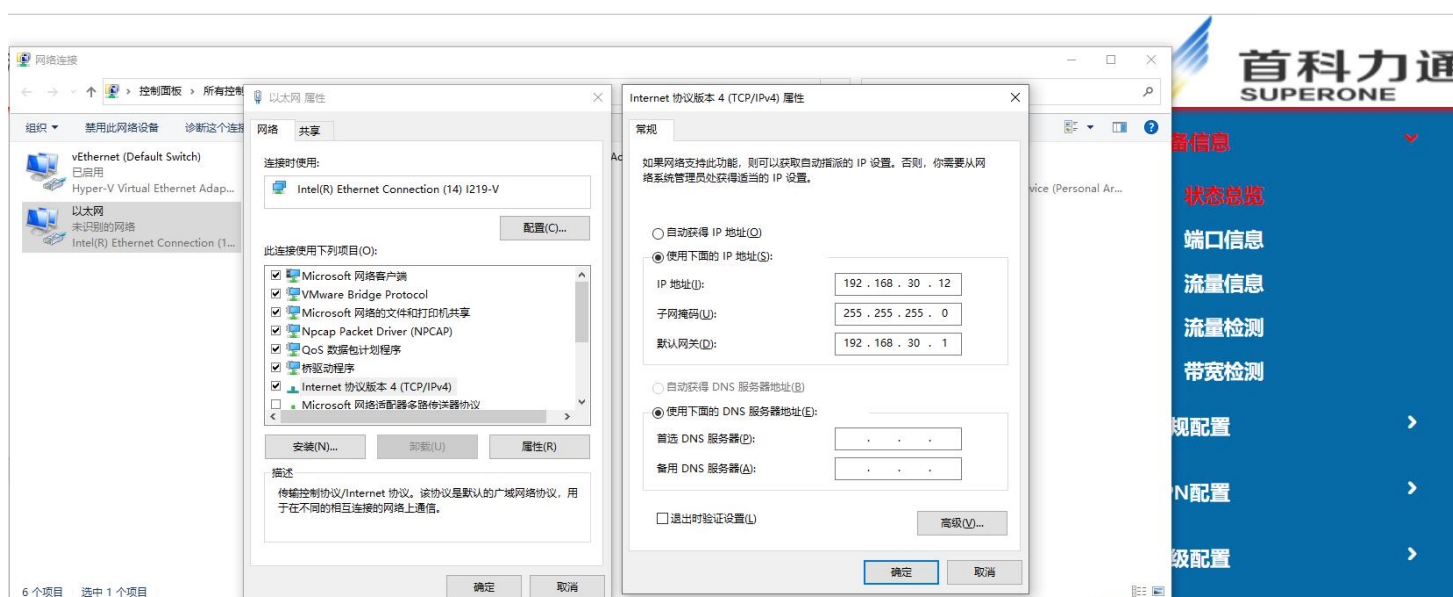
4.3 模拟测试

用电脑仿真一下, 本地电脑连接设置如下, 网线插在 LAN3 上。





用电脑仿真一下，本地电脑连接设置如下，网线插在 LAN4 上。



采用云端 NAT 功能，主要解决了现场最多 50 个工作在 4 个不同网段的设备，可以连接到管理平台或者远程云端的问题。不推荐同时开启本地 NAT 和云端 NAT 功能。如果违反以上原则，由此操作所造成网络风暴，数据丢失等任何损失，本司将不承担赔偿责任。

5、DHCP 设定

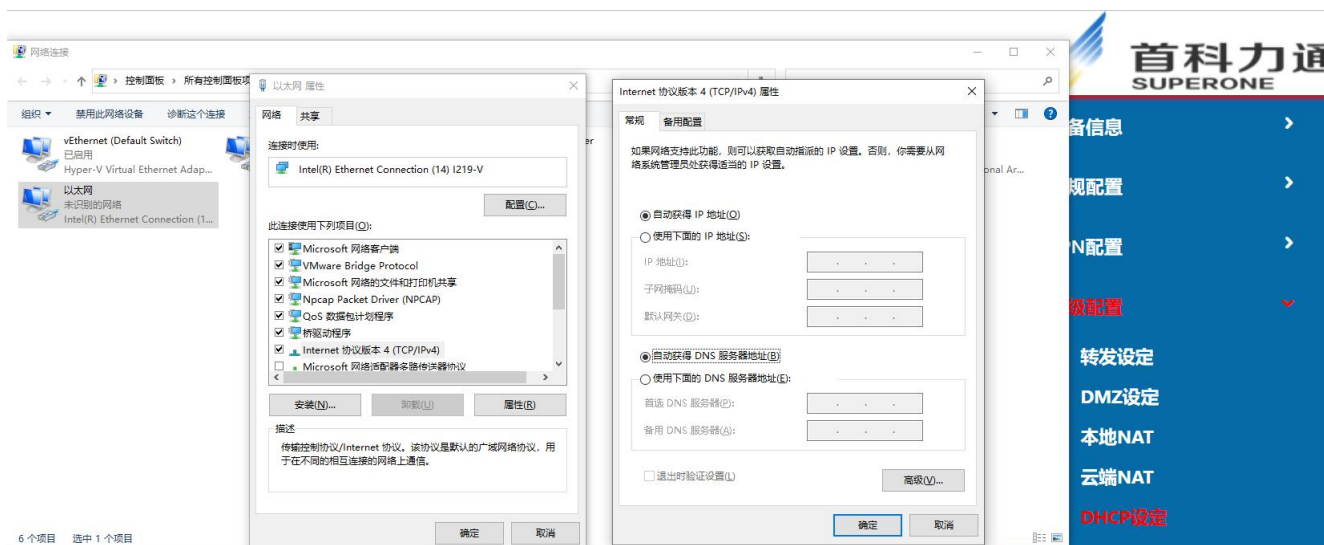
在右侧配置导航栏中，点击：**高级配置—DHCP 设定**。

进入如下配置页面，启用 DHCP 功能之后，模块 LAN 口所连接的现场设备能够自动获取到动态的 IP。



5.1 需要配置的参数：

- 1) MAC 地址：填写需要分配 IP 地址的设备的实际 MAC 地址，工业控制系统请查阅该设备说明书，PC 端可以使用管理员指令进行查询。
- 2) IP 地址：填写 5G 模块对该 MAC 地址设备，要分配的实际 IP 地址。
- 3) 主机名称和描述：可以空缺
- 4) 如果有多个外部设备，请依次填写相关 MAC 地址，和分配的 IP 地址
- 5) 需要获得 IP 地址的外部设备，必须要开启自动获取 IP 的选项，如果是 PC 请见下图，如果是其他设备，请查阅相关说明书。



- 6) 设置完成后，点击新增保存该配置，点击保存重启，使该配置生效。

五、系统配置

1、接入管理

在右侧配置导航栏中，点击：**系统配置—接入管理**。

进入如下界面，可以对访问配置页面的内容做相关修改

更改访问	
本地访问	HTTP
HTTP 访问端口	80
远程访问	关闭
WAN口禁PING	<input checked="" type="checkbox"/>
SSH开机启动	<input type="checkbox"/>
开启Telnet远程访问	<input type="checkbox"/>

密码设置	
修改密码 (admin)
(再次输入)

1.1 更改访问方式

1) 本地访问，在下拉菜单中进行不同登录配置页面方式的选择。

如果选择和 HTTPS 相关的方式，则需要证书才能进入模块的配置页面，一般情况下请保持 HTTP 方式以及默认值。

访问端口号建议保持默认值，否则仅通过 IP 地址，将无法正确进入配置页面。



本地访问

HTTP

HTTP 访问端口

80

2) 远程访问，默认关闭，如果需要未来远程接入模块，远程监控或者修改模块的配置参数，可以选择开启。同样请选择 HTTP 方式，同时保持默认端口号。

远程访问	HTTP
访问端口	8080
允许远程管理 IP地址	

3) 其余选项推荐保持默认值。

1.2 密码设置

初始密码为 123456，修改后点击**保存-重启**生效。

遗忘密码后无法进入本机设备，需要 reset 恢复出厂设置。如果造成配置内容丢失，本司不承担任何责任。

密码设置

修改密码 (admin)

●●●●●●●●

(再次输入)

●●●●●●●●



除了密码修改之外，建议用户保持默认参数值，如果违反以上原则，可能将无法正常进入配置页面。由此操作所造成损失，本司将不承担赔偿责任。

2、时间同步

在右侧配置导航栏中，点击：**系统配置—时间同步**。
进入如下界面，可以对同步时间的内容做相关修改

时间同步

设备时间 Wed, 01 Jan 2020 10:30:17 +0800 主机同步

时区 UTC+08:00 中国, 香港, 澳洲西部, 新加坡, 台湾

自动同步时间 每隔1小时

NTP服务器 默认

0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org

2.1 参数相关介绍

- 1) 点击主机同步，可以同步模块和 NTP 服务器的时间。
- 2) 可以选择不同时区。

UTC+08:00 中国, 香港, 澳洲西部, 新加坡, 台湾

UTC+00:00 冈比亚, 赖比瑞亚, 摩洛哥

UTC+00:00 英国

UTC+01:00 突尼斯

UTC+01:00 法国, 德国, 意大利, 波兰, 瑞典

UTC+02:00 爱沙尼亚, 芬兰, 拉脱维亚, 立陶宛

UTC+02:00 南非, 以色列

UTC+02:00 希腊, 乌克兰, 罗马尼亚, 土耳其, 拉脱维亚

UTC+03:00 伊拉克, 约旦, 科威特

UTC+03:00 莫斯科

UTC+04:00 阿曼, 阿联酋

UTC+04:00 亚美尼亚

UTC+04:30 喀布尔

UTC+05:00 巴基斯坦, 俄罗斯

UTC+05:00 俄罗斯, 叶卡捷琳堡

UTC+05:30 孟买, 加尔各答, 千奈, 新德里

可以选择自动同步的时间间隔。

每隔1小时

不同步

启动时更新

每隔1小时

每隔2小时

每隔4小时

每隔6小时

NTP 服务器可以选择默认或者自定义。

默认的服务器地址为：0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org。



时间同步功能非常重要，如果选择关闭自动同步时间的话，模块将无法和网络上其他设备通讯或者无法连接管理平台，由此操作所造成损失，本司将不承担赔偿责任。

3、设备名称

在右侧配置导航栏中，点击：**系统配置—设备名称**。

进入如下界面，可以对设备名称做相关修改。

设备名称	
设备名称	<input type="text" value="5G-Device"/>
主机名称	<input type="text" value="5G-Device"/>
域名	<input type="text"/>

4、备份管理

在右侧配置导航栏中，点击：**系统配置—备份管理**。


可以备份当前模块的配置内容，也可以恢复之前已经完成备份的模块配置，还能恢复出厂设置。



恢复出厂设置，将会造成当前所有配置内容和数据丢失，由此操作所造成损失，本司将不承担赔偿责任。

系统备份设置

.cfg


备份 

保存为默认配置

系统恢复设置

选择所要恢复的配置文件:

选择文件

恢复 

恢复出厂默认配置



确定

5、SNMP

在右侧配置导航栏中，点击：**系统配置—SNMP**。

启用该功能之后，可以使用 SNMP 管理工具对设备进行远程监测，查看设备的运行状态。

SNMP设置	
启用SNMP	<input type="checkbox"/>
端口	161
远程访问	<input checked="" type="checkbox"/>
允许远程管理 IP地址	
System Name	5G_Device
位置	5G_Device
联系	admin@5G_Device
只读Community	rocommunity
RW Community	rwcommunity
SNMPv3 Authentication Type	NONE ▼
SNMPv3 Privacy Type	NONE ▼

5.1 参数配置内容

- 1) 勾选 启用 SNMP 功能；
- 2) 端口号，建议保持默认值；
- 3) 远程访问：如果开启，需要填写状态上报的服务器 IP 地址；
- 4) 其余参数：保持默认值。

6、系统日志

在右侧配置导航栏中，点击：**系统配置—系统日志**。

系统日志	
记录到本地系统	<input checked="" type="checkbox"/>
记录到远端系统	<input type="checkbox"/>
生成间隔	每隔1小时 ▾
日志记录限制	60 (每分钟消息数 / 0 表示不限制)

6.1 系统日志

模块默认记录系统日志在本地内存，可在系统工具中进行查看。

生成间隔可以通过下拉菜单修改也可以关闭，记录限制可以做修改。

6.2 记录远端

如果开启记录到远端，则需要填写接收日志的 PC 或者服务器的 IP 地址和对应端口号。

记录到远端系统	<input checked="" type="checkbox"/>
主机或者IP地址 / 端口	192.168.1.2 : 514

7、固件管理

7.1 升级固件前准备

升级固件前，要先进入：“常规配置-公网设置”中，“运营商网络配置-启用模块”是使用中的（有对勾），如下图，则要禁用“启用模块”。修改后，“保存-重启”，再进行固件升级。



如果，进入“常规配置-公网设置”后，“运营商网络配置-启用模块”是禁用状态（没用对勾），则可以直接进行固件升级。

7.2 升级固件方法

在右侧配置导航栏中，点击：**系统配置—固件管理**。

通过该页面可以升级产品的固件，更新固件后，可以选择清除或者保留之前的产品配置。

更改固件

选择固件:

未选择任何文件

选择文件

升级

升级固件后清除所有配置数据



固件升级过程中不得对设备断电，插拔 SIM 卡，或者网线，如果违反该操作规定，由此操作所造成损失，本司将不承担赔偿责任。



固件升级前请确认是否清除之前的配置文件，如果勾选了清除所有数据后，由此操作所造成损失，本司将不承担赔偿责任。

六、安全配置

1、规则设定

在右侧配置导航栏中，点击：**安全配置—规则设定**。

1.1 IP/MAC/Port 过滤

通过该功能设定可以允许或者禁止，某个或者某几个 MAC 地址、IP 地址，通过模块访问服务器，或者服务器通过模块访问该设备。

IP/MAC/Port过滤

启用	来源MAC	来源IP	目的IP	协议	来源端口	目的端口	策略	描述
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	NONE	<input type="text"/>	<input type="text"/>	接收	<input type="text"/>
新增+								

1) 禁止某个 IP 地址通过模块接入服务器。

例如下图：该设备 IP 地址为 102.168.0.123 接入 LAN2 端口，服务器地址为 192.158.0.77，策略选择丢弃，则该设备将无法通过模块访问服务器，但是服务器仍然可以访问该模块。

启用	来源MAC	来源IP	目的IP	协议	来源端口	目的端口	策略
✓	-	192.168.0.123	192.168.0.77	-	-	-	丢弃

例如下图：该设备 IP 地址为 102.168.0.123 接入 LAN2 端口，服务器地址为 192.158.0.77，策略选择丢弃，则该设备将无法通过模块访问服务器，同时服务器也不能访问该模块。

启用	来源MAC	来源IP	目的IP	协议	来源端口	目的端口	策略
✓	-	192.168.0.123	192.168.0.77	-	-	-	丢弃
✓	-	192.168.0.77	192.168.0.123	-	-	-	丢弃

2) 禁止某个 MAC 地址通过模块访问 LAN2 端口所连接的某个设备。

例如下图，某个设备 MAC 地址为 B4:A9:FE:00:8E:09，LAN2 端口连接的设备 IP 地址为 102.168.0.123，此时该 MAC 地址的设备，无法对 LAN2 端口下连接的设备进行访问。

启用	来源MAC	来源IP	目的IP	协议	来源端口	目的端口	策略
✓	B4:A9:FE:00:8E:09	any/0	192.168.0.123	-	-	-	丢弃

3) 禁止某个 LAN2 端口连接的设备访问其他任何设备，同时允许其他所有联网设备访问它。

例如下图，某个 LAN2 端口连接的设备 IP 地址为 102.168.0.123，设定该地址为来源 IP，目的 IP 缺省，策略选择丢弃，则该设备无法访问网络上任何设备。设定该地址为目的 IP，来源 IP 缺省，策略选择接收，则网络上所有设备都可以访问这个地址上的设备。

IP/MAC/Port过滤							
启用	来源MAC	来源IP	目的IP	协议	来源端口	目的端口	策略
✓	-	192.168.0.123	any/0	-	-	-	丢弃
✓	-	any/0	192.168.0.123	-	-	-	接收



IP/MAC/Port 过滤的设定内容，可以根据现场情况进行调整，启用前需要详细规划策略，如果因为设定有误或者策略规划不当，由此操作所造成损失，本司将不承担赔偿责任。

1.2 URL 过滤设置

此处可以填写需要屏蔽的 URL 具体地址，填写后模块所连接的设备将不能被允许访问该 URL。

URL过滤设置

启用	域名URL	描述
<input checked="" type="checkbox"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
新增 +		

如下图，填写完成后，该 URL 地址将被屏蔽，关于 URL 和域名的填写规则请查询相关资料。

URL过滤设置

启用	域名URL ^
<input checked="" type="checkbox"/>	https://work.weixin.qq.com/mail/

1.3 域名过滤

启用后，可以选择创建白名单或者黑名单。

创建黑名单之后的域名将被屏蔽，关于 URL 和域名的填写规则请查询相关资料。

如下图：

域名过滤

启用

默认策略 黑名单 ▾

启用	域名
<input checked="" type="checkbox"/>	baidu.com

七、系统工具

1、PING 工具

在右侧配置导航栏中，点击：**系统工具—Ping 工具**。

可以选择某个在线的设备 IP 地址进行收发数据的 PING 测试。

地址、次数、数据包大小可以修改。

Ping工具

IP地址	<input type="text" value="192.168.0.123"/>	<input type="button" value="Ping"/>
Ping次数	<input type="text" value="10"/>	
包大小	<input type="text" value="128"/> (字节)	

序号	地址	接收字节	生存期限TTL	响应时间RTT(ms)	+/- (ms)
0	192.168.0.123 (192.168.0.123)	136	64	1.41	
1	192.168.0.123 (192.168.0.123)	136	64	1.11	-0.30
2	192.168.0.123 (192.168.0.123)	136	64	1.14	0.03
3	192.168.0.123 (192.168.0.123)	136	64	1.10	-0.04
4	192.168.0.123 (192.168.0.123)	136	64	1.10	-0.00
5	192.168.0.123 (192.168.0.123)	136	64	1.34	0.24
6	192.168.0.123 (192.168.0.123)	136	64	1.31	-0.03
7	192.168.0.123 (192.168.0.123)	136	64	1.49	0.18
8	192.168.0.123 (192.168.0.123)	136	64	1.16	-0.33
9	192.168.0.123 (192.168.0.123)	136	64	1.69	0.53

往返延迟: 1.097 最小, 1.284 平均, 1.694 最大
 数据包: 10 已发送, 10已接收, 0% 丢失率

2、截取数据

在右侧配置导航栏中，点击：**系统工具—截取数据**。

可以选择对于 WAN 口或者 LAN 口通讯数据进行一段时间的数据包截取，有助于分析网络通讯故障。点击“开始”进行截取，点击“停止”则停止截取。

截取的文件保存为 **pacp** 格式。采用 **HEX-Editor** 插件的 **Notepad++** 打开，能够以 16 进制数据的格式显示；或者使用 **Wireshark** 等抓包工具也可以正常打开这种文件。

截取数据

网络

LAN

开始

时长

1

分钟 (0 为时间不限)

3、追踪数据

在右侧配置导航栏中，点击：**系统工具—追踪数据**。

该功能可以有效的帮助找到某个可能联网的 IP 设备。

输入某个联网设备的 IP 地址，设定追踪的跳跃点数和每一跳的等待时间，然后点击追踪。

经过最大等待时间之后，会显示追踪该 IP 地址的各种信息，包括经过的 IP 地址、跳跃次数，以及时间间隔。

追踪数据

IP地址 追踪

最大跃点数

最大等待时间 (每跳秒数)

跃点	地址	最小 (ms)	最大 (ms)	平均 (ms)	+/- (ms)
1	192.168.0.123	1.03	1.63	1.24	

4、日志数据

在右侧配置导航栏中，点击：**系统工具—日志数据**。

日志数据

查看

下载日志文件

查找 🔍

4.1 如果在“系统配置—系统日志”中设定了记录到本地系统。

1) 点击查看，可以在线浏览系统日志数据。

```

Jan 23 19:14:39 5G_Device kern.info kernel: option 2-1:1.0: device disconne
Jan 23 19:14:39 5G_Device kern.info kernel: option1 ttyUSB1: GSM modem (1-p
Jan 23 19:14:39 5G_Device kern.info kernel: option 2-1:1.1: device disconne
Jan 23 19:14:39 5G_Device kern.info kernel: option1 ttyUSB2: GSM modem (1-p
Jan 23 19:14:39 5G_Device kern.info kernel: option 2-1:1.2: device disconne
Jan 23 19:14:39 5G_Device kern.info kernel: option1 ttyUSB3: GSM modem (1-p
Jan 23 19:14:39 5G_Device kern.info kernel: option 2-1:1.3: device disconne
Jan 23 19:14:39 5G_Device kern.info kernel: gmi_wwan_rm500 2-1:1.4: usb0: u
Jan 23 19:14:40 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:40 5G_Device user.notice modem_watchdog[682]: Modem 1 S15
Jan 23 19:14:41 5G_Device user.notice modem_watchdog[682]: Modem 1 S16
Jan 23 19:14:42 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:42 5G_Device user.notice modem_watchdog[682]: Modem 1 S17
Jan 23 19:14:43 5G_Device user.notice modem_watchdog[682]: Modem 1 S18
Jan 23 19:14:44 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:44 5G_Device user.notice modem_watchdog[682]: Modem 1 S19
Jan 23 19:14:44 5G_Device user.err modem_watchdog[681]: Start modem
Jan 23 19:14:45 5G_Device user.notice modem_watchdog[682]: Modem 1 S20
Jan 23 19:14:46 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:46 5G_Device user.notice modem_watchdog[682]: Modem 1 S21
Jan 23 19:14:47 5G_Device user.notice modem_watchdog[682]: Modem 1 S22
Jan 23 19:14:48 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:48 5G_Device user.notice modem_watchdog[682]: Modem 1 S23
Jan 23 19:14:49 5G_Device user.notice modem_watchdog[682]: Modem 1 S24
Jan 23 19:14:50 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:50 5G_Device user.notice modem_watchdog[682]: Check Modem 1 F
Jan 23 19:14:50 5G_Device kern.debug kernel: wlan1: no IPv6 routers present
Jan 23 19:14:50 5G_Device user.err modem_watchdog[681]: Start wan
Jan 23 19:14:50 5G_Device user.err modem_watchdog[681]: stop wan
Jan 23 19:14:51 5G_Device user.notice modem_watchdog[682]: Check Modem 1 U
Jan 23 19:14:52 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:52 5G_Device user.notice modem_watchdog[682]: Check Modem 1 U
Jan 23 19:14:52 5G_Device user.err modem_watchdog[681]: start wan
Jan 23 19:14:53 5G_Device user.notice modem_watchdog[682]: Check Modem 1 U
Jan 23 19:14:53 5G_Device user.notice modem_watchdog[6413]: Restart modem_
Jan 23 19:14:54 5G_Device daemon.info PL2303[1107]: waiting router online
Jan 23 19:14:54 5G_Device user.notice modem_watchdog[682]: Check Modem 1 U
    
```

2) 点击“下载日志文件”可以把日志文件保存成为 txt 类型文件，通过记事本方式打开。

联系我们

使用下列资源访问支持信息。

联系电话（总部）	(010) 82709788
技术资料文献库	https://bjsuperone.com/资料中心/技术资料/
查找您所在地区的技术支持热线	https://bjsuperone.com/关于我们/联系我们/
微信公众平台	微信扫一扫： 
首科力通网址	https://bjsuperone.com/

废弃电气和电子设备（WEEE）



使用寿命结束后，应将本设备与未分类的城市垃圾分开，单独进行收集。