

边缘计算机用户手册 V2.0

用户手册

Version V2.0, 2024 年 12 月

本手册中描述的软件是根据许可协议提供的，只能按照该协议的条款使用

1 导言

边缘计算网关/边缘计算机该系列产品接口丰富，具备全球蜂窝接入能力。内置软件边缘计算引擎，支持上百种数据采集协议，轻松实现设备数据采集、处理及上云，同时支持设备云远程配置，帮助企业加快数字化进程。

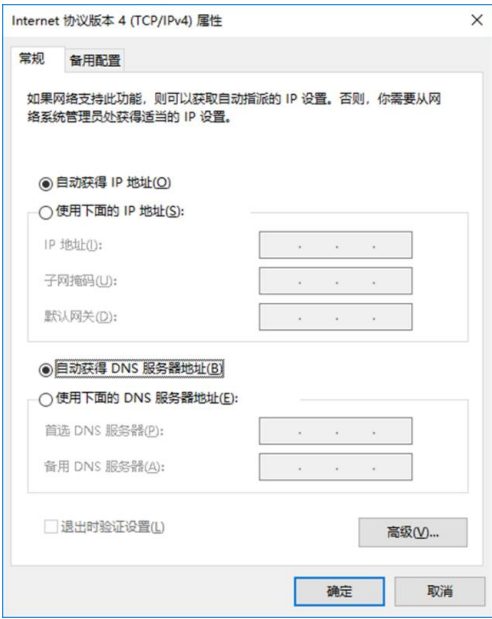
2 设备配置说明

2.1 访问网关

使用以下默认 IP 地址连接到网关（地址信息也可从设备背贴上查看到）

端口	默认 IP
ETH1	192.168.1.1

- 步骤 1：设置 PC 的 IP 地址与设备网口处于同一网段，以电脑网口插入到设备 ETH1 为例
 - 方法一：自动获取 IP 地址（推荐）



- 方法二：使用固定 IP 地址

选择“使用下面的 IP 地址”，输入 IP 地址（默认为 192.168.1.2~192.168.1.254 中任意值）；子网掩码（默认 255.255.255.0）；默认网关（默认为 192.168.1.1）以及 DNS 服务器地址，单击<确定>。



- 步骤 2：打开浏览器，访问网关的 ETH1 的 IP 地址并输入登录用户名和密码。设备出厂默认密码：**初始登录用户名：admin 初始登录密钥：admin**



- 步骤 3：登录成功后，可以看到如下图所示的概览页面。



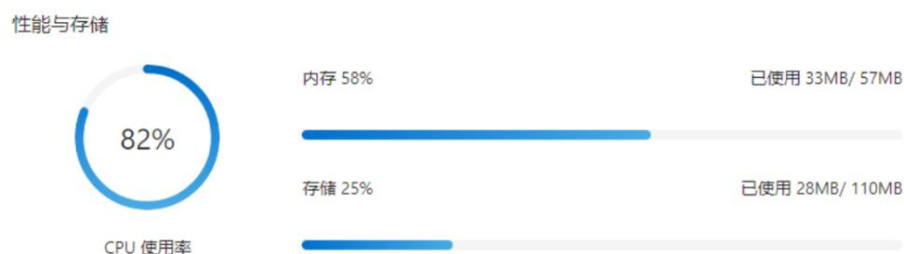
2.2 概览

此页面概述了网关的系统状态、系统性能、系统存储、网络连接、网络流量等信息。通过此页面您可以快速地对设备基本情况有所了解。

- **网络连接状态：**展示网关的网络连接情况以及网络配置
 - 外部网络状态：链接到设备云平台，具体配置可查看 [2.5.2 设备云网管](#)
 - 接口网络状态：若要对接口进行配置详细查看 [2.3.2 网络接口](#)



- **性能与存储：**展示设备当前 CPU、内存、Flash、MicroSD、USB 的使用情况



- **系统信息：**点击“编辑”按钮可修改网关设备的名称

系统信息	
名称:	pg-20421A582D27 🔗
型号:	X100
硬件版本:	Ver.V1
序列号:	202404081501
固件版本:	3.3.10.0076(91126e7)
设备时间:	2024-12-05 16:23:14
主机时间:	2024-12-05 16:23:17
系统运行时间:	1天 2小时 45分钟 48秒
边缘计算引擎:	禁用
边缘计算版本:	2.7.2.0005(b11b1b1)

2.3 网络

2.3.1 在线保持

蜂窝无线网络可能存在“假链接”（拨号成功并获得 IP，但是链路不通）等异常现象，通常通过 LCP 等方式进行维护，智能网关除了支持这种检测方式外还提供更为可靠的 ICMP 链路检测功能，它通过 ping 包检测方式检测通讯链路，当检测链路异常时则执行用户设置的动作，实现链路和系统的快速恢复。

此页面展示了网关当前的在线保持页面。您可以通过“启用”按钮对在线保持参数进行配置。



在线保持功能如下：

- 启用：启用/关闭在线保持功能。
- 连接检测类型：下拉可选 ICMP/TCP Connection

- 服务器 1~3：主/备用链路地址，检测网络状态的地址，可以是 IP 地址也可以是域名。
- 端口 1~2：主/备用端口，使用端口时检测连接用的端口。（在 TCP Connection 类型下可用）
- 超时时间：检测链路超时的时间，默认 60 秒。
- 心跳检测：是否开启心跳检测。
- 离线超时重启时间：网络异常超时时间，缺省 5 分钟。

2.3.2 网络接口

2.3.2.1 移动网络

选择“网络 > 网络接口 > 移动网络”，进入“移动网络”界面。

在线保持

网络接口

移动网络

WAN

LAN

WLAN

VLAN

接口配置

链路管理

网络服务

网络安全

转发配置

启用: ☒

拨号参数集

索引	APN	认证方式	用户名	密码	操作
无数据					

Modem 拨号号码:

* CID:

双SIM卡: ☐

SIM 1

拨号参数集:

PIN码:

> 在线检测

> 高级配置

提交 重置

移动网参数说明如下：

- 启用：启用/关闭移动网功能
- 拨号参数集：拨号参数集，用于专用网卡拨号时配置 APN，用户名，密码以及认证方式等信息。如果不是专网卡，通常不需要修改这里的配置。拨号参数集最多可以添加 10 条记录。

- APN: APN (Access Point Name) 用来标识 WCDMA/LTE 网络的业务种类, WCDMA/LTE 系统根据用户连接 WCDMA/LTE 网络的 APN 提供相应的服务。由运营商提供 (CDMA2000 系列不设置此项)
- 认证方式

自动: 自动选择一种认证方式。

PAP: 密码认证协议, 通过两次握手提供一种简单明文认证方式。

CHAP: 挑战握手认证协议, 通过三次握手确认摘要信息从而进行安全认证。

- 用户名: 指定接入外部 PDN 网络用户的用户名, 由运营商提供。
- 密码: 指定接入外部 PDN 网络用户的密码, 由运营商提供。
- Modem 拨号号码: 拨号使用的拨号串。拨号串由运营商提供, 请向运营商获取。
- CID: 下拉可选: Profile 0~16。

The screenshot shows a settings menu for '双SIM卡' (Dual SIM Card). At the top, there is a toggle switch labeled '双SIM卡:' which is turned on (blue). Below this, there are several configuration options, each with a red asterisk indicating it is required:

- * 主卡: A dropdown menu currently showing 'SIM 1'.
- * 最大重拨次数: A text input field containing the number '1'.
- * 最小连接时间: A text input field containing '10', followed by a '秒' (seconds) unit label.
- * 备卡超时时间: A text input field containing '0', followed by a '秒' (seconds) unit label.
- * 双卡最大切换次数: A text input field containing the number '10'.

- 双 SIM 卡: 是否启用双 SIM 卡 (仅限支持双 SIM 卡功能的设备)
 - 主卡: 可选 SIM1/SIM2
 - 最大拨号次数: 当 SIM1 在设置的最大拨号次数内一直没拨号成功, 设备将切换到 SIM2 拨号。
 - 最小连接时间: 当设备拨号连接成功时间小于设置的最小连接时间时, 设备的拨号次数会累计。当大于设置的最小连接时, 设备的拨号次数将清零。0 是禁用此功能。

- 备卡超时时间：若当前使用的为备卡，备卡拨号成功后，当达到设定的备卡超时时间后，设备会切换到主卡拨号。
- 双卡最大切换次数：在设置的双卡最大切换次数内可切换。
- 拨号参数集：拨号策略选择，对应于拨号参数集配置索引项，若不是专用网卡，选择默认即可。
- PIN 码：PIN 码即 SIM 卡的个人识别密码。如果启用 PIN 码，当不设置 PIN 码或设置错误的 PIN 码，设备拨号失败；设置正常的 PIN 码，设备可以正常拨号上网。

▼ 在线检测

主服务器：主/备用服务器都为空，即关闭探测

备用服务器：主/备用服务器都为空，即关闭探测

* 间隔时间：30 秒

* 超时时间：5 秒

* 最大重试次数：5

严格探测： ☐

离线强制重启： ☐

- 在线检测
 - 主/备用服务器：设备支持两个 ICMP 探测服务器：主服务器和备份服务器。当配置两个服务器后，首先检测第一个服务器，只有当第一个服务器达到最大重试次数后，系统才会检测第二个服务器。当两个服务器都检测失败的情况下，设备会重新拨号并进行下一轮 ICMP 探测。
 - 间隔时间：设备发送 ICMP 探测报文的时间间隔，默认 30 秒。
 - 超时时间：在设置的 ICMP 探测超时时间内，没有收到 ICMP 响应包认为本次 ICMP 探测超时，默认 5 秒。
 - 最大重试次数：设置 ICMP 探测失败时的最大重试次数（达到最大次数后会重新拨号），默认 5 秒。
 - 严格探测：当设备的拨号接口有数据流量时。设备不发送 ICMP 探测。当拨号接口没有数据流量时候才会发送 ICMP 探测，可以达到节省流量目的。
 - 离线强制重启：超过最大重试次数强制重启。

▼ 高级配置

优先注册网络: ☐

* 协议:

* 首选网络模式:

EHRPD: ☐

NAT: ☒

指定子网掩码:

添加默认路由: ☒

* 网关跃点:

MTU:

使用服务器指定DNS: ☒

PPP选项:

重拨时重启射频: ☐

配置APN重启射频: ☐

日志等级:

- 高级配置

- 优先注册网络：是否启用优先注册网络。
- 协议：下拉可选：auto/pppd
- 首选网络模式：用户根据所使用设备及 SIM 卡适用的情况，可选择特定的网络方式，或使用自动方式，设备可自行注册到适用当前网络状况的网络模式。
- EHRPD：该功能仅对 EVDO 部分网络生效。
- NAT：当私网电脑接入到 Internet 时，需要开启 NAT 功能。
- 指定子网掩码：可修改移动网络接口掩码地址。
- 添加默认路由：当私网电脑接入到 Internet 时，需要开启该功能。
- 网关跃点：设置接口优先级数值越低优先级越高。
- MTU：接口的最大传输单元。

- 使用服务器指定 DNS：设置首选的 DNS 服务器。
- PPP 选项：拨号方式。
- 重拨时重启射频：是否开启重拨时重启射频功能。
- 配置 APN 重启射频：是否开启配置 APN 重启射频。
- 日志等级：过滤详细日志。

2.3.2.2 WAN

选择“网络 > 网络接口 > WAN”，进入“WAN”界面。

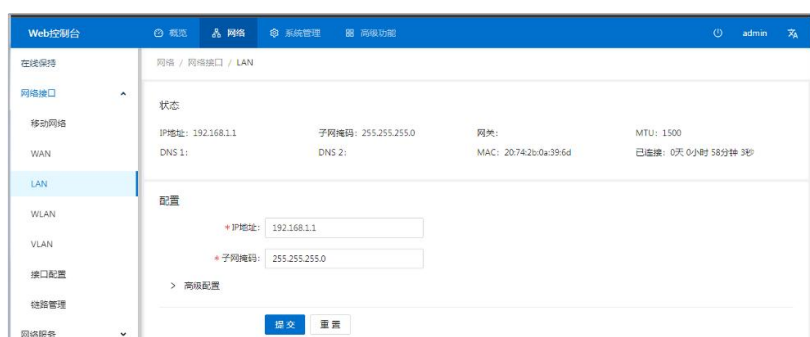
配置 WAN 为接入点时参数说明如下：

- 连接类型：广域网的连接类型。
 - 静态 IP：手动配置接口 IP
 - IP 地址：设置可以访问互联网的带子网掩码的 IP 地址
 - 子网掩码：WAN 口子网掩码
 - 网关：设置 WAN 口 IP 的网关

- DHCP:网关从 DHCP 服务器自动获取 IP
 - DHCP 客户端 ID: 配置 DHCP 客户端 ID, 用于客户端与服务端之间的身份识别与判断
- PPPoE:通过 PPPoE 拨号获取 IP
 - 服务名: 配置 PPPoE 服务名, 用于客户端与服务端之间的身份识别与判断
 - 用户名/密码: 输入由互联网服务提供商提供的用户名/密码
 - 启用 NAT: 当局域网内私网电脑接入到 Internet 时, 需要开启 NAT 功能
 - 添加默认路由: 设置 WAN 接口为默认路由出口
 - 使用服务器指定 DNS: 是否使用服务器的 DNS, 选择否时, 需手动输入 DNS
 - MAC 地址: 设置 WAN 口的 MAC 地址
 - MTU: 最大传输单元, 以字节为单位
 - 网关跃点: 设置接口优先级数值跃低优先级越高
 - DNS: 设置首选的 DNS 服务器

2.3.2.3 LAN

选择“网络 > 网络接口 > LAN”，进入“LAN”界面。



配置 LAN 为接入点时参数说明如下：

- IP 地址: 用户可以根据需要配置或更改主 IP 地址。

- 子网掩码：用户配置的以太网接口的子网掩码。
- MAC 地址：设置 LAN 口的 MAC 地址。
- 网关：设置 LAN 口 IP 的网关。
- DNS：设置首选的 DNS 服务器。
- MTU：最大传输单元，以字节为单位。

2.3.2.4 WLAN

选择“网络 > 网络接口 > WLAN”，进入“WLAN”界面。



编辑接口

×

配置：☒

* 网络制式：

802.11b/g/n mixed

* 通道：

自动

* 频宽：

40 MHZ(HT40)

* 无线电功率：

默认

禁用HT40+/-重叠扫描：

☐

取消

确定

接口列表参数说明如下：

- 配置：功能开关。
- 网络制式：WLAN 的网络模式，每种网络模式的最大区别是传输速率有较大差异，默认 bgn 混合模式。当工作模式选择 AP 时，需要手动。
 - 802.11b：工作在 2.4G 频段，最高速率 11Mbps
 - 802.11g：工作在 2.4G 频段，最高速率 54Mbps
 - 802.11n：工作在 2.4G 频段，也可以工作在 5G 频段，理论最高速率 300Mbps
 - 802.11b/g/n mixed：工作在 2.4G 频段，最高速率可以达到 600Mbps
 - 802.11 ac：工作在 5G 频段，根据所选频宽，理论最高速率可达几 Gbps

以上数据仅供参考，实际速率以设备兼容性和网络环境为主。

- 通道：信道是以无线信号作为传输媒体的数据信号传送通道，2.4G 频段共有 13 个信道，5G 频段共有 9 个信道，每个信道的载波频率不同。
- 2.4G/5G 频宽：下拉可选：20~80MHZ。
- 无线电功率：下拉列表选择 0~20dBm，通常选择默认。

点击操作“+”创建 WIFI_AP 模式、客户端模式、MESH 模式。

创建WIFI

配置: ☒

* 模式: AP模式

启用中继: ☐

MAC:

* SSID:

隐藏SSID: ☐

低应答断开: ☒

* 加密模式: WPA/WPA2

算法: 默认

密码:

取消 确定

• 当模式为 AP 模式参数说明如下：

- 配置：启用或禁用 WLAN 服务。启用 WLAN 服务后，可以配置无线网络的基本参数和安全认证选项，使得无线接入的用户可以实现接入 Internet。
- 模式：WLAN 的工作模式，支持 AP 模式/客户端模式。
- 启用中继：无线中继模式，即是无线 AP 在网络连接中起到中继的作用，能实现信号的中继和放大。
- MAC 地址：设置自定义 MAC 地址。
- SSID：设置自定义的 WiFi 名称
 - SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都要独立的身份认证，只有通过身份认证的用户才可以进入相应的子网络，防止未被授权的用户进入网络。
- 隐藏 SSID：选择 AP 模式时配置。用于配置 WLANSSID 是否广播以便客户端能搜索到该 SSID，通常在不希望其他人搜索并使用 WLAN 功能时禁用，禁用则表示在网络环境中隐藏 SSID 功能，用户若要连接，需手动添加该 SSID。
- 低应答断开：无数据交互 WIFI 自动断开。

- 加密模式：配置 WLAN 的加密模式，当不需要加密验证时可以不加密。WEP 加密相对容易被破解，建议使用 WPA 的加密方式。
- 加密模式可选：不加密、WEP 开放认证、WEP 共享密钥、WPA、WPA2、WPA/WPA2
 - 启用密码组：连接加密模式为 WEP 开放认证、WEP 共享密钥使用
 - 算法：加密采用的算法。可选：自动、强制使用 CCMP (AES) 加密、强制使用 TKIP 加密、TKIP 和 CCMP (AES) 混合加密
 - 密码：设置 WLAN_AP 密码

创建WIFI

配置: ☒

* 模式: 客户端模式

启用中继: ☐

MAC:

* SSID:

BSSID绑定: ☐

* 连接类型: 动态地址(DHCP)

* 网关跃点: 11

漫游: ☐

低应答断开: ☒

* 加密模式: WPA/WPA2

算法: 默认

密码:

• 当模式为客户端模式参数说明如下：

- 启用中继：无线中继模式，即是无线 AP 在网络连接中起到中继的作用，能实现信号的中继和放大。
- MAC 地址：设置自定义 MAC 地址。
- SSID：下拉选择所需要连接 WiFi 名称。
- BSSID 绑定：是否勾选 BSSID 绑定功能，若勾选需填写 BSSID 参数。

- 连接类型：下拉可选动态地址（DHCP）/静态 IP
 - 选择静态 IP 时需要填写 IP 地址、子网掩码、网关、DNS
- 网关跃点：填写网关跃点，默认 11。
- 漫游：是否开启漫游功能。
 - RSSI 阈值：填写 RSSI 阈值，默认-85。
 - 短间隔：填写短间隔时间，默认 120 秒。
 - 长间隔：填写长间隔时间，默认 600 秒。
- 低应答断开：是否开启低应答断开功能。
- 加密模式：根据连接的 WiFi 加密类型选择相应模式及算法，并填写正确的密码。

创建WIFI

×

配置：☒

* 模式：

MESH 模式

启用中继：☐

MAC：

* MESH ID：

低应答断开：☒

* 加密模式：

WPA/WPA2

算法：

默认

密码：

取消

确定

- 当模式为 MESH 模式参数说明如下（仅部分机型支持）：
 - 启用中继：无线中继模式，即是无线 AP 在网络连接中起到中继的作用，能实现信号的中继和放大。
 - MAC 地址：设置自定义 MAC 地址。

- MESH ID: 填写 MESH ID 号。
- 低应答断开: 是否开启低应答断开功能。
- 加密模式: 配置 WLAN 的加密模式, 当不需要加密验证时可以不加密。WEP 加密相对容易被破解, 建议使用 WPA 的加密方式。
 - 加密模式可选: 不加密、WEP 开放认证、WEP 共享密钥、WPA、WPA2、WPA/WPA2
 - 启用密码组: 连接加密模式为 WEP 开放认证、WEP 共享密钥使用
 - 算法: 加密采用的算法。可选: 自动、强制使用 CCMP (AES) 加密、强制使用 TKIP 加密、TKIP 和 CCMP (AES) 混合加密
 - 密码: 设置 WLAN_AP 密码

2.3.2.5 VLAN

选择“网络 > 网络接口 > VLAN”, 进入“VLAN”界面。

VLAN	VID	ETH0	ETH1	操作
1	1	Off	Untagged	编辑 删除
2	2	Untagged	Off	编辑 删除

- VLAN 列表参数说明如下:
 - VLAN: VLAN 端口
 - VID: VLAN 识别 ID
 - 端口: 各个端口的状态
 - 操作: 可对 WLAN“编辑”、“删除”操作
- “创建 VLAN”页面展示创建新 VLAN 的配置情况

- VLAN：选择 VLAN 端口。
- VID：VLAN 的识别 ID。下拉可选：OFF、Tagged、Untagged
- 端口：选择端口状态。下拉可选：OFF、Tagged、Untagged
- CPU 端口：选择 CPU 端口状态。下拉可选：OFF、Tagged、Untagged

2.3.2.6 接口配置

选择“网络>网络接口>接口配置”，打开“接口配置”界面。

接口	IP地址	子网掩码	网关	网关地址	应用时间	Up/Down
lan	192.168.1.1	255.255.255.0		0	0天 15小时 33分钟 30秒	Down
loopback	127.0.0.1	255.0.0.0		0	0天 15小时 33分钟 29秒	Down
wan	192.168.0.249	255.255.255.0	192.168.0.1	10	0天 15小时 33分钟 24秒	Down
wwan	10.93.115.102	255.255.255.252	10.93.115.101	12	0天 3小时 29分钟 14秒	Down

- 单击“创建”，创建一个新的接口。

创建接口 ✕

* 接口名称:

* 协议:

静态IP

IP地址:

+

网关:

NAT:

☐

使用服务器指定DNS:

☐

MAC:

20:15:05:14:15:1c

网关跃点:

* 接口类型:

桥接接口

动态ARP项检查:

☒

* 许可VLAN列表:

取消

确定

- 接口名称：接口配置的名称
- 协议：接口使用的协议，下拉可选：静态 IP/动态 DHCP
- NAT：是否开启 NAT，地址转换
- 使用服务器指定 DNS：是否使用服务器指定的 DNS
 - DNS 1：设置首选的 DNS 服务器
 - DNS 2：设置备用的 DNS 服务器
- MAC 地址：接口的物理地址
- 网关跃点：配置数据所需经过的节点数
- 接口类型：配置接口类型
- 许可 VLAN 列表：允许使用的 VLAN
- 当协议选择“静态 IP”时配置：

- IP 地址：当“协议”选择“静态 IP”时需配置
- 子网掩码：WAN 接口子网掩码，默认值 255.255.255.0
- 网关：指定 WAN 接口的下一跳地址，当需要 WAN 接口作为交换机时，可选配此项

2.3.2.7 链路管理

链路管理功能支持将网关多个联网端口进行充分利用，开启该功能可以实现多联网链路的冗余切换。另外还可实现带宽分流、带宽叠加等功能。“链路管理”页面展示了链路管理配置信息和参数信息，你可以在此页面配置链路管理或者查看详细的状态信息。

选择“网络 > 网络接口 > 链路管理”，进入“链路管理”界面。

Web控制台

🔍 筛选

🌐 网络

🔒 系统管理

📊 高级功能

admin

在线保持

网络接口

移动网络

WAN

LAN

WLAN

VLAN

接口配置

链路管理

网络服务

网络安全

转发配置

...

网络 / 网络接口 / 链路管理

状态

接口	状态	在线时长	离线时长
wan	未知	0天 0小时 0分钟 0秒	0天 0小时 0分钟 0秒
wwan	未知	0天 0小时 0分钟 0秒	0天 0小时 0分钟 0秒
wwlan	未知	0天 0小时 0分钟 0秒	0天 0小时 0分钟 0秒

第 1-3 条/总共 3 条 < 1 > 10 条/页

配置

接口 成员 策略 规则

接口	成员地址	成员超时	成员间隔	接口时延阈值	接口上链阈值	操作
wan	114.114.114.114	4	10	3	2	<a>编辑 <a>删除
wwan	114.114.114.114	4	10	3	2	<a>编辑 <a>删除
wwlan	114.114.114.114	4	10	3	2	<a>编辑 <a>删除

- 单击“编辑”，可编辑端口的链路管理详细参数。

编辑接口

配置: ☐ 关闭

接口名称: wan

探测地址: 114.114.114.114

添加探测路由: ☐ 关闭

* 探测超时: 4

* 探测间隔: 10

* 接口断线阈值: 3

* 接口上线阈值: 2

无缝切换: ☒ 开启

* 初始状态: 在线

自定义上线动作:

自定义断线动作:

取消 确定

- 编辑接口参数说明如下:

- 配置: 启用/关闭链路管理。
- 添加探测路由: 开启该功能会新增一条策略路由。
- 接口名称: 显示当前编辑的接口名称, 不可修改。
- 探测地址: 填写被探测的 IP 地址或域名, 用于判断端口链路是否正常联网, 默认为 114.114.114.114
- 探测超时: 根据接口断线阈值项的超时时间累积, 判断端口链路状态是否通信超时, 单位为/秒。默认值为 4, 取值范围在 1~255 之间。
- 探测间隔: 监测链路状态的间隔时间, 单位为/秒。默认值为 10, 取值范围在 5~255 之间
- 接口断线阈值: 通过 ping 探测地址次数判断链路是否超时响应, 单位为/次。默认值为 3, 取值范围为 1~255。
- 接口上线阈值: 通过 ping 探测地址次数判断链路是否恢复正常, 单位为/次。默认值为 2, 取值范围为 1~255。

- 优先级：指定端口的使用优先级。数值越低，优先级则越高。优先级高的端口链路将作为主链路联网使用。当主链路断开的情况下，网关将会自动切换至低优先级的链路。默认值为 1，取值范围为 1~255。
- 负载权重：通过设置数值进行端口的带宽分流，数值越大则通过该端口链路的流量越高。使用该参数需确保多个端口的优先级一致。默认值为 3，取值范围为 1~255。
- 无缝切换：是否启用无缝切换。

2.3.3 网络服务

2.3.3.1 DHCP

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分配申请，服务器返回为客户端分配的 IP 地址及相关联的信息（如：租期），以实现 IP 地址等信息的动态配置。你可以在“DHCP 服务器”页面设置和查看 DHCP 服务器的配置情况。

选择“网络 > 网络服务 > DHCP”，进入“DHCP”界面。

The screenshot shows the 'Web控制台' (Web Control Panel) interface. The left sidebar contains a menu with '网络服务' (Network Services) expanded, showing 'DHCP' selected. The main content area is titled '配置' (Configuration) and 'DHCP 绑定表' (DHCP Binding Table). The configuration options are:

- 启用 (Enable): ☒
- * 起始分配基址 (Start Allocation Base): 100
- * 客户数 (Number of Clients): 150
- 租用时间单位 (Lease Time Unit): 小时 (Hours)
- * 租用时间 (Lease Time): 12
- DNS服务 (DNS Service): 使用系统DNS设置 (Use System DNS Settings)

At the bottom, there are buttons for '提交' (Submit) and '重置' (Reset).

• 配置 DHCP 服务器参数说明如下：

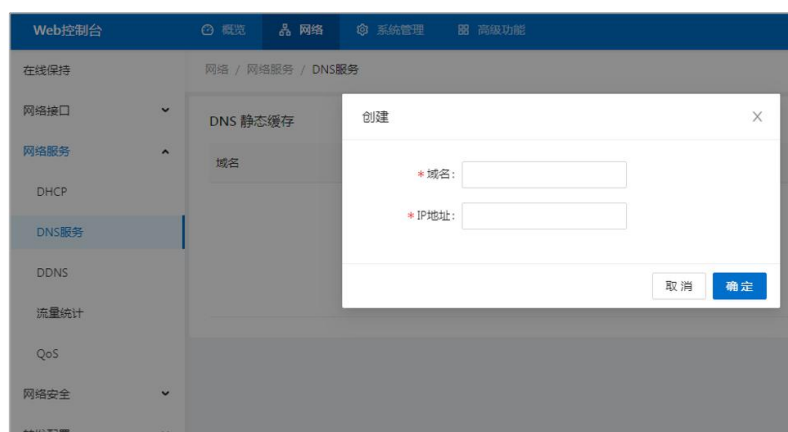
- 启用 DHCP 服务：启用/关闭 DHCP 服务。

- 起始分配基址：配置 DHCP 地址池的起始 IP 地址，默认 100。
 - 客户数：从起始地址 IP 开始，往后可分配的 IP 数量，默认 150。
 - 租用时间单位：时间单位。下拉可选：小时/分钟
 - 租用时间：DHCP 客户端获取 IP 后对 IP 租用时间，过期 DHCP 服务器将回收分配给客户端的 IP 地址并重新分配 IP 地址，默认 12 小时。
 - DNS 服务：使用系统 DNS 设置。
- **DHCP 绑定表配置的参数说明：**
 - 用户 IP 地址：设置一个静态指定的 IP 地址
 - 用户 MAC 地址：设置一个静态指定 DHCP 的 MAC 地址

2.3.3.2 DNS 服务

域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的 DNS 服务器将域名解析为正确的 IP 地址。你可以在“DNS 服务”页面设置和查看域名服务器及 DNS 中继服务。

选择“网络 > 网络服务 > DNS 服务”，进入“DNS 服务”界面。



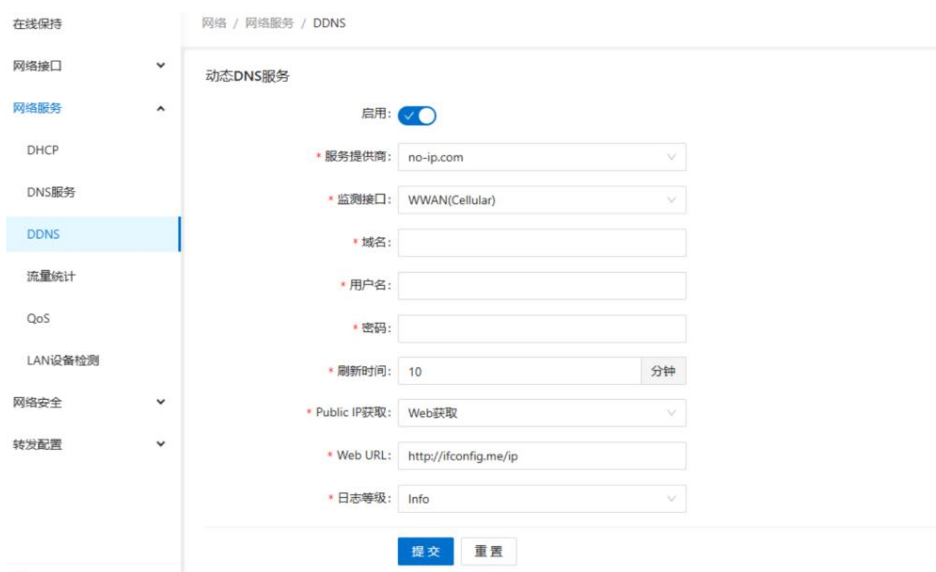
- **DNS 创建参数说明如下：**
 - 域名：自定义设置设备域名名称。

- IP 地址：自定义设置指定 IP 地址。

2.3.3.3 DDNS

DDNS 服务允许将一个动态 IP 地址映射到一个固定的域名解析服务商，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，服务器程序负责提供 DNS 服务并实现动态域名解析。

选择“网络 > 网络服务 > DDNS”，进入“DDNS”界面。



DDNS 参数说明如下：

- 启用：开启/关闭 DDNS 服务。
- 服务提供商：申请的域名对应的域名提供商选项，目前我司暂不支持列表之外的域名提供商的 DDNS 服务。
 - no-ip.com
 - duckdns.org
 - dynu.com
- 监测接口：下拉可选 WAN、WWAN、WLAN
- 用户名/密码：注册 DDNS 服务提供商域名的用户名/密码。

- 域名：DDNS 服务提供商提供的域名，它与网关的 IP 相对应，通常通过访问该域名来访问网关的 IP。
- 刷新时间（分钟）：网关与 DDNS 域名服务提供商更新 DDNS 相关信息的间隔时间，部分域名提供商的服务是 IP 发生变化后发送更新数据，更新间隔取决于您购买的 DDNS 服务，一般建议 4 分钟以上。
- Public IP 获取：Web 获取/网络接口
- Web URL：获取公网 IP 地址的网页链接
- 接口名称：WAN、WWAN、WLAN
- 日志等级：调整 DDNS 信息日志等级，None、Info、Notice、Warning、Error

2.3.3.4 流量统计

流量统计指的是对网络中数据传输量的测量、收集、分析和报告的过程。它涉及对网络流量的多个方面的监控，包括但不限于数据量、传输速度。网关会根据每月流量上限的设定对网关上线做管控，当网关超过每月流量上限时网关将断开网络，禁止用户访问外网达到限制 SIM 卡超流量的情况，每月初已经使用流量将会被清零。

选择“网络 > 网络服务 > 流量统计”，进入“流量统计”界面。

- 配置页面参数说明如下：
 - 启用：开启/关闭流量统计功能。
 - 保存统计数据：是否保存统计数据。

- 保存间隔：统计数据每隔 n 分钟保存一次数据。

点击“流量统计”页面，启用各接口



● 流量统计参数页面说明如下：

- 接口名称：显示需要启用流量统计功能的接口，对应接口如下：

- WAN（ETH0）
- LAN（ETH1-ETH4）
- WWAN（蜂窝网络）
- WLAN（WiFi）

- 上行流量：显示对应接口的上行流量统计。

- 下行流量：显示对应接口的下行流量统计。

- 总流量：显示对应接口的总流量统计，统计方式为上行流量和下行流量合计。

- 启用：启用/关闭对应接口的流量统计功能。

- 操作：可设置流量超标之后设备触发的动作，包括限速或限制拨号。该功能仅蜂窝网络接口生效。

- 限制拨号：设置阈值，当流量统计达到该阈值，则设备断开蜂窝网络

- 限速：设置阈值，当流量统计达到该阈值，则触发上行/下行流量的限速机制

2.3.3.5 QoS

QoS 功能主要针对带宽的控制，按需分配下载、上传的带宽。

选择“网络 > 网络服务 > QoS”，进入“QoS”界面。



- QoS 页面参数说明如下：

- 接口名称：显示需要启用 QoS 功能的接口，对应接口如下：

- WAN (ETH0)
 - WWAN (蜂窝网络)
 - WWLAN (WiFi)

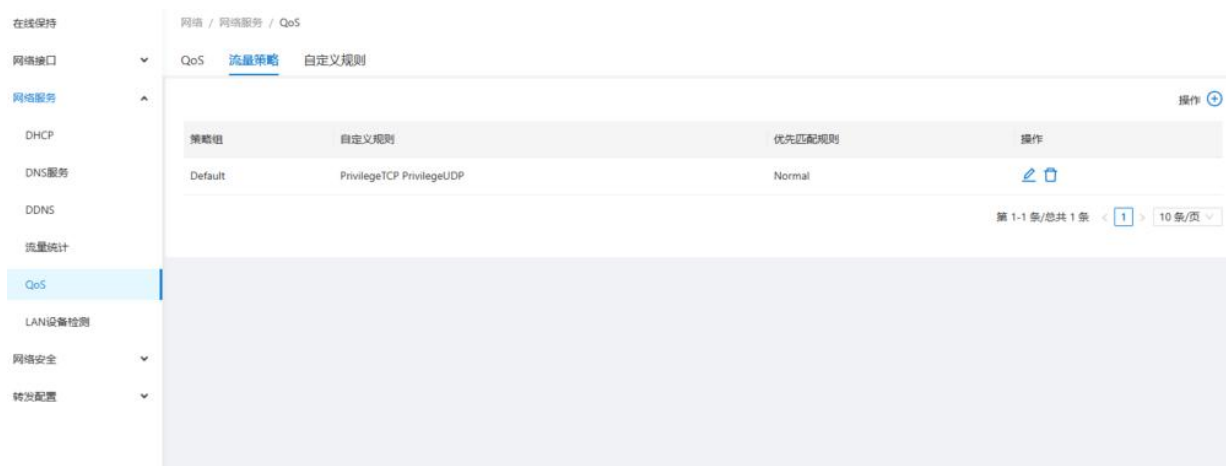
- 策略组：显示当前接口选用的策略组。

- 总下载 (KByte)：显示当前接口总下载的速度限制范围。

- 总上传 (KByte)：显示当前接口总上传的速度限制范围。

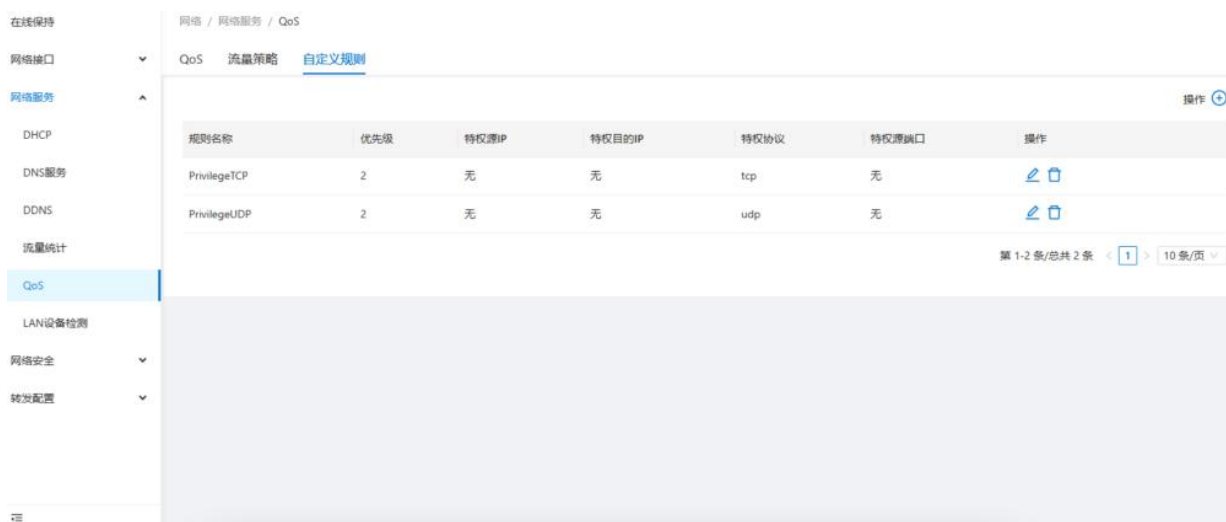
- 启用：启用/关闭当前接口的 QoS 功能。

- 操作：对应接口的 QoS 参数编辑或删除操作。



- 流量策略页面参数说明如下：

- 策略组：显示该策略组名称。
- 自定义规则成员：显示加入该策略组的自定义规则条目。
- 优先匹配规则：显示默认选择的优先使用规则。
- 操作：对应策略的编辑或删除操作。



- 自定义规则参数说明如下：

- 规则名称：显示当前规则名称。
- 优先级：显示当前规则优先级。
- 特权 IP：显示特权源 IP 地址

- 特权目的 IP：显示特权目的 IP 地址。
- 特权协议：显示特权协议。
- 特权源端口：显示特权源端口。
- 操作：对应规则的编辑或删除操作。

2.3.3.6 LAN 设备检测

选择“网络 > 网络服务 > LAN 设备检测”，进入“LAN 设备检测”界面。

在线保持

网络 / 网络服务 / LAN设备检测

网络接口

网络服务

DHCP

DNS服务

DDNS

流量统计

QoS

LAN设备检测

网络安全

转发配置

状态

状态检测: 禁用

配置

启用: ☒

IP地址: 192.168.10.1

+

* 间隔时间: 5 秒

* 超时时间: 1 秒

* 最大重试次数: 5

执行动作: 重置网口

* 重置网口: ETH1

提交 重置

- LAN 设备检测页面参数说明如下：
 - 启用：开启/关闭 LAN 设备检测功能。
 - IP 地址：设置检测 LAN 设备 IP 地址。
 - 间隔时间：发送检测报文的间隔时间，默认 5s。
 - 超时时间：设置的 LAN 设备检测超时时间内，没有收到响应包，认为本次探测超时。
 - 最大重试次数：检测设备的最大重试次数。
 - 执行动作：检测失败后执行的动作。下拉可选：重置网口/重置所有网口/软重启/重启

- 重置网口：设置重置的网口。下拉可选：ETH1/ETH2/...（备注：根据网关机型选择对应网口）

2.3.4 网络安全

2.3.4.1 防火墙

选择“网络 > 网络安全 > 防火墙”，进入“防火墙”界面。

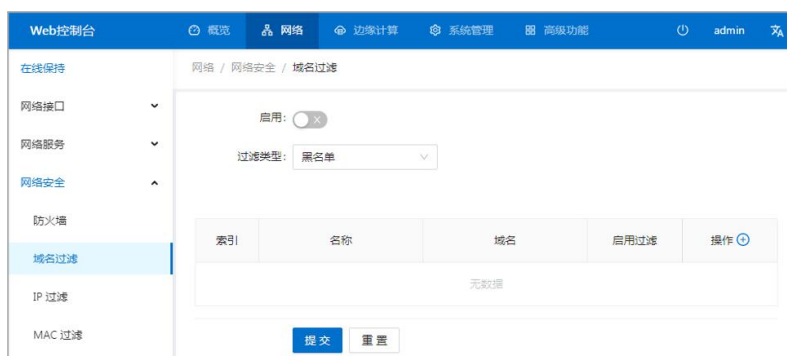


- 防火墙页面配置参数说明如下：
 - 启用：开启/关闭防火墙。
 - 动作：REJECT、DROP。
 - 桥接口防火墙：开启/关闭桥接口的防火墙功能。
 - 禁止 Traceroute 探测：开启/关闭禁止 Traceroute 探测功能。

2.3.4.2 域名过滤

域名过滤功能可设置对网站的访问限制，通过黑白名单功能设置特定的过滤规则，实现安全可靠的域名访问环境。可以在“域名过滤”页面手动设置过滤类型，如选择“黑名单”，则过滤规则的域名被禁止访问；如选择“白名单”，则仅有过滤规则的域名可以被访问，其余域名都被禁止访问。

选择“网络 > 网络安全 > 域名过滤”，进入“域名过滤”界面。



- 域名过滤页面参数说明如下：

- 启用：开启/关闭域名过滤。
- 过滤类型：选择过滤类型。下拉可选：黑名单/白名单
- 截流：是否启用截流功能，默认勾选。
- 索引：显示策略条目的序号。
- 名称：显示域名过滤配置项的名称。
- 域名：显示当前配置项被过滤的域名。
- 启用过滤：显示该配置项是否已启用。

- 操作：可对域名过滤规则“编辑”、“删除”操作。操作如下：

- a. 点击创建按钮可以创建规则
- b. 点击编辑按钮进行规则配置
- c. 点击删除按钮可删除该规则

2.3.4.3 IP 过滤

IP 过滤是指网关通过过滤规则来判定是否允许外部设备访问网关以及是否允许数据包经过网关转发，从而实现对网关设备的管理及局域网设备的上网行为管理。

选择“网络 > 网络安全 > IP 过滤”，进入“IP 过滤”界面。



- 配置 IP 过滤页面参数说明如下：

- 过滤类型：IP 过滤类型。下拉可选：白名单/黑名单/自定义

点击“IP 列表>操作+”创建并配置参数，如下：



创建

* 动作:

REJECT

▼

* 协议:

ALL

▼

* 源接口:

LAN

▼

源地址:

* 目的接口:

WAN

▼

目的IP:

▼ 高级配置

起始日期:

yyyy-mm-dd

结束日期:

yyyy-mm-dd

起始时间:

hh:mm:ss

结束时间:

hh:mm:ss

每月中的某天:

星期:

- 创建 IP 过滤参数信息如下：

- 动作：选择对访问的过滤规则。下拉可选：ACCEPT/REJECT/DROP
- 协议：选择访问所用的协议，如果不清楚当前的访问协议，建议选择“ALL”。下拉可选：TCP/UDP/TCPUDP/ALL
 - TCP 提供 IP 环境下的数据可靠传输，它提供的服务包括数据流传送、可靠性、有效流控、全双工操作和多路复用。通过面向连接、端到端和可靠的数据包发送。
 - UDP 提供的是非面向连接的、不可靠的数据流传输。UDP 不提供可靠性，也不提供报文到达确认、排序以及流量控制等功能。它只是把应用程序传给 IP 层的数据报发送出去，但是并不能保证它们能到达目的地。因此报文可能会丢失、重复以及乱序等。
- 源接口：指定访问源的接口。下拉可选：WAN/LAN
- 源地址：指定访问源的源地址。需手动输入 IP 地址、子网段或指定 IP 范围。
- 目的接口：指定 IP 数据包访问的网关接口。下拉可选：WAN/LAN
- 目的 IP：访问源所要访问的目标地址，可以是网关下接的 IP 设备。手动输入 IP 地址、子网段或指定 IP 范围。
- 高级配置：设置自定义生效时间。

2.3.4.4 MAC 过滤

MAC 过滤通常用来控制主机对网关的接入访问，白名单使得只有特定 MAC 的主机才能管理和访问网关。

选择“网络 > 网络安全 > MAC 过滤”，进入“MAC 过滤”界面。



创建

动作: REJECT

协议: ALL

过滤模式: 出站

* MAC: 1A:2B:3C:4D:5E:6F

高级配置

起始日期: yyyy-mm-dd

结束日期: yyyy-mm-dd

起始时间: hh:mm:ss

结束时间: hh:mm:ss

每月中的某天:

星期:

- 创建 MAC 过滤参数信息如下：

- 动作：选择对访问的过滤规则。下拉可选：ACCEPT/REJECT/DROR
- 协议：选择访问所用的协议，如果不清楚当前的访问协议，建议选择“ALL”。下拉可选：TCP/UDP/TCPUDP/ALL
- 过滤模式：该规则的过滤模式。下拉可选：出战/入站
- MAC 地址：MAC 需过滤的 MAC 地址。
- 高级配置：设置自定义生效时间。

2.3.5 转发配置

2.3.5.1 NAT

选择“网络 > 转发配置 > NAT”，进入“NAT”界面。



创建

* 名称:

模式:

协议:

外部区域:

* 外部端口:

内部区域:

* 内部IP:

* 内部端口:

- 创建 NAT 参数说明如下：

- 名称：设置 NAT 规则名称。
- 模式：选择相对应的端口映射模式。下拉可选：DNAT/SNAT/DNAT+SNAT
 - DNAT：目标地址转换模式
 - SNAT：源地址转换模式

- DNAT+SNAT：目的地址+源地址转换模式

注意：当下挂设备无法配置网关的情况下，请使用 DNAT+SNAT 模式

- 协议：针对哪种协议的数据包做目的地址转换。下拉可选：TCP/UDP/TCP+UDP
- 外部区域：外网。下拉可选：wan
- 外部端口：外网使用的端口。
- 内部区域：内网。下拉可选：lan
- 内部 IP：内网的 IP 地址。
- 内部端口：内网使用的端口。

2.3.5.2 路由配置

选择“网络 > 转发配置 > 路由配置”，进入“路由配置”界面。



点击操作列“+”创建新路由配置页面，你可以在此页面配置路由参数信息。

创建

×

接口名称: lan

* IP地址:

* 子网掩码: 255.255.255.0

网关:

* 网关跃点: 1

* MTU: 1500

取消

确定

● 配置路由模式规则参数说明如下：

- 接口名称：路由接口的名称。下拉可选：goconnect/ lan/ n2n/ open_vpn1/ open_vpn2/ wan
- IP 地址：输入目的主机或目的网络的 IP 地址。
- 子网掩码：输入目的主机或目的网络的子网掩码。
- 网关：输入该路由规则网关的 IP 地址，网关会把与该目的地址和子网掩码相匹配的全部数据转发给该网关。
- 网关跃点：设置网关跃点数。
- MTU：设置最大传输单元。

● 设备路由信息可点击“路由配置>路由表”查看

在线保持

网络接口

网络服务

网络安全

转发配置

NAT

路由配置

OSPF配置

网络 / 转发配置 / 路由配置

路由表

路由配置

IP地址	网关	子网掩码	网关跃点	接口名称
0.0.0.0	192.168.0.1	0.0.0.0	10	wan
192.168.0.0	0.0.0.0	255.255.255.0	10	wan
192.168.1.0	0.0.0.0	255.255.255.0	0	lan

第 1-3 条/总共 3 条 < 1 > 10 条/页

2.3.5.3 OSPF 配置

选择“网络 > 转发配置 > OSPF 配置”，进入“OSPF 配置”界面。



The screenshot shows the OSPF configuration page in a web interface. On the left is a sidebar menu with categories like '在线保持', '网络接口', '网络服务', '网络安全', '转发配置' (highlighted), 'NAT', and '路由配置'. Under '转发配置', 'OSPF配置' is selected. The main content area has a breadcrumb '网络 / 转发配置 / OSPF配置' and sub-tabs 'OSPF配置', '区域配置', '网络配置', and '接口配置'. The 'OSPF配置' tab is active, showing a '启用' (Enable) toggle switch which is turned on. Below it are input fields for '路由器ID:' and 'SPF计算间隔:'. At the bottom are '提交' (Submit) and '重置' (Reset) buttons.

- OSPF 配置页面参数说明如下：
 - 启用：开启或关闭 OSPF 配置功能。
 - 路由 ID：路由本端标识。
 - SPF 计算间隔：设置 SPF 计算的延时时间。
- 区域配置参数页面如下图



The screenshot shows the OSPF Area Configuration page. The sidebar is the same as the previous screenshot. The breadcrumb is '网络 / 转发配置 / OSPF配置'. The sub-tabs are 'OSPF配置', '区域配置' (highlighted), '网络配置', and '接口配置'. The '区域配置' tab is active, displaying a table with columns: '区域ID', '认证模式', '区域类型', '默认开销', and '操作:'. The table is currently empty, showing a '暂无数据' (No data) message with a folder icon.

- 设置 OSPF 区域 ID 号，0 为骨干区域其他为常规区域。
- 网络配置参数页面如下图

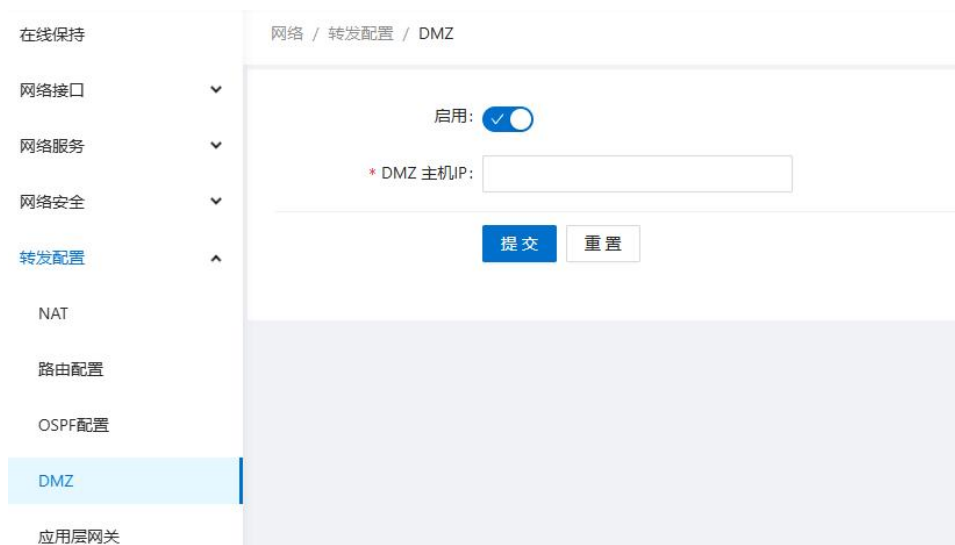


- 区域 ID：下拉选择已创建的 ID 号。
- 网段：配置对应设备网段地址。
- 反掩码：配置设备的反掩码。
- 配置参数后设备生成对应接口，页面如下图



2.3.5.4 DMZ

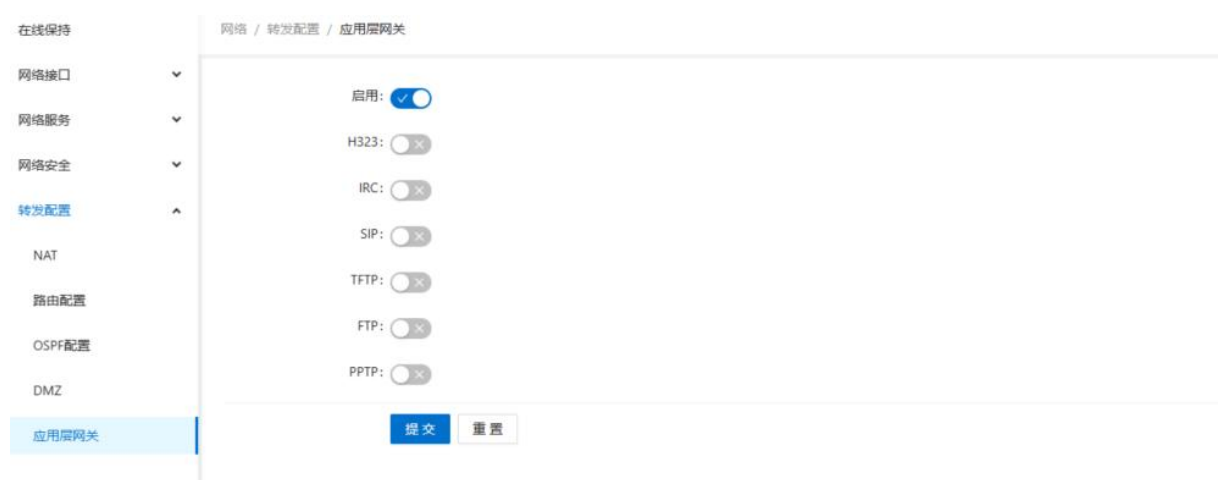
选择“网络 > 转发配置 > DMZ”，进入“DMZ”界面。



- 配置 DMZ 规则参数说明如下：
 - 启用：开启/关闭 DMZ 功能。
 - DMZ 主机 IP：DMZ 主机的 IP 地址。

2.3.5.5 应用层网关

选择“网络 > 转发配置 > 应用层网关”，进入“应用层网关”界面。



- 应用层网关页面参数说明如下：
 - 启用：开启/关闭应用层网关功能。
 - H323：是否开启 H323 功能。
 - IRC：是否开启 IRC 功能。
 - SIP：是否开启 SIP 功能。
 - TFTP：是否开启 TFTP 功能。
 - FTP：是否开启 FTP 功能。
 - PPTP：是否开启 PPTP 功能。

2.4 边缘计算

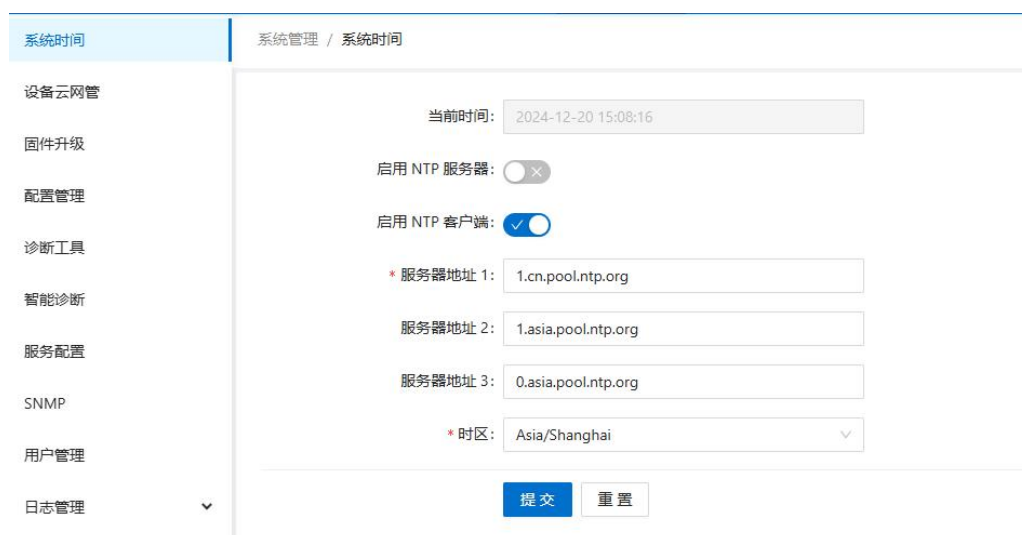
边缘计算功能可参考 [《GoEdge 边缘计算用户手册》](#)。

2.5 系统管理

2.5.1 系统时间

为了让网关与其他设备更好的协同，需精准配置系统时间。

选择“系统管理 > 系统时间”，进入“系统时间”界面。



系统时间

系统管理 / 系统时间

当前时间: 2024-12-20 15:08:16

启用 NTP 服务器: ☐

启用 NTP 客户端: ☒

* 服务器地址 1: 1.cn.pool.ntp.org

服务器地址 2: 1.asia.pool.ntp.org

服务器地址 3: 0.asia.pool.ntp.org

* 时区: Asia/Shanghai

提交 重置

- 配置方式及步骤如下：

- 选择“系统管理 > 系统时间”，进入“系统时间”界面。
- 在“系统时间”中选择启用 NTP 服务器/客户端模式。
 - 关闭 NTP 客户端模式
 - 时间：手动设置时间，格式：YYYY-MM-DD
 - 启用 NTP 客户端模式
 - 服务器地址 1~3：默认公共时间服务器池，提供同步时间服务

- 时区：下拉可选对应时区，当前所在时区为 Asia/Shanghai

c. 选择后点击“提交”即可

2.5.2 设备云网管

智能网关系统内置通过 WMMP 协议与 M2M 平台通信功能，可通过平台实现对设备的远程维护管理和现场网络状态的监控管理。

选择“系统管理>设备云网管”，进入“设备云网管”界面。

系统时间

系统管理 / 设备云网管

设备云网管

启用: ☒

* 云服务器地址: c.rigo.io

* 云服务器端口: 10883

注册账号:

现场名称:

* 设备ID: 202409121536

> 高级配置

提交 重置

- 配置设备云网管参数说明如下：
 - 启用：开启/关闭设备云网管服务。该功能需要配合我司网管管理平台使用。
 - 云服务器地址：网管平台服务器的 IP 地址或域名。
 - 云服务器端口：网管平台服务器使用的端口号。
 - 设备 ID：连接网管平台的识别 ID。从管理平台上分配
 - 注册账号：管理设备的平台账号。
 - 现场名称：多台设备时用于识别设备点位。

- 设备 ID：设备系统 ID，不可自定义。
- 高级设置
 - 状态上报间隔：按配置的间隔上报设备状态信息。
 - 定位上报间隔：按配置的间隔上报设备位置信息。

2.5.3 固件升级

网关支持本地网络方式升级系统文件，在升级之前请您确定您已获得系统更新的目标文件，并将更新文件已经存放置局域网的计算机上。

选择“系统配置>固件升级”，进入“固件升级”界面。



- 升级固件操作如下：
 - 点击上传文件>选择已经下载固件包>上传完成后>选择是否保留配置>点击升级。
- 保留配置：升级后保留用户在页面配置的参数。
- 不保留配置：升级后不保留用户在页面配置的参数。

升级注意事项：

升级过程，请勿对设备进行断电操作，以防升级失败。在升级时，不建议关闭页面；在升级完成后，页面会自动跳转。

2.5.4 配置管理

选择“系统配置 > 配置管理”，进入“配置管理”界面。



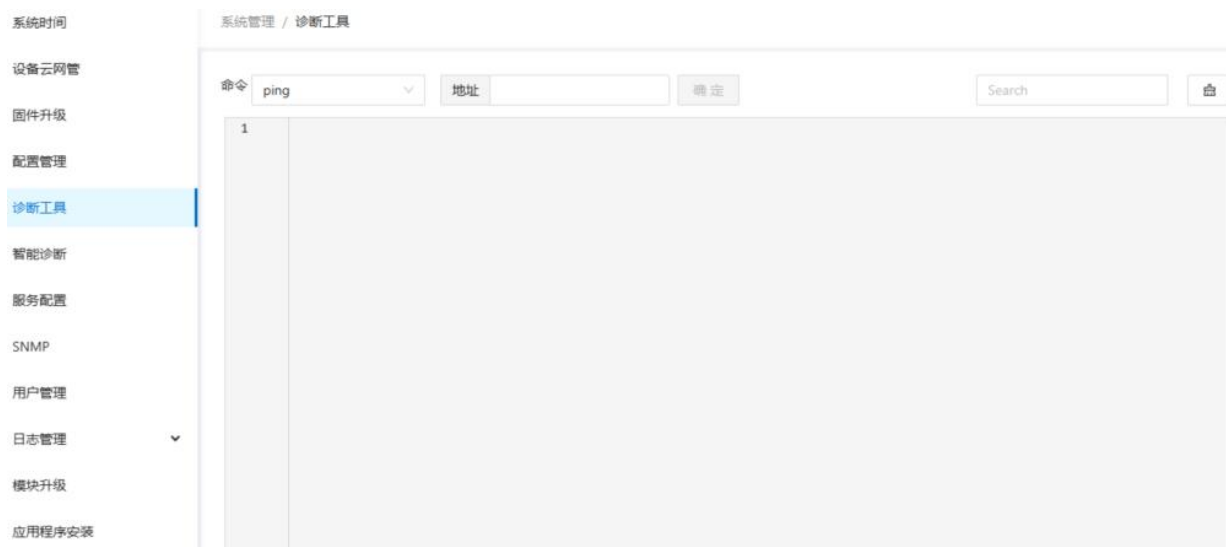
- 配置文件操作

- 导出配置：导出当前系统配置文件到本地，实现文件/参数的备份功能。
- 恢复出厂默认：恢复出厂配置，清除当前所有配置，网关所有的配置被恢复到默认参数。
- 上传文件：浏览本地需要导入的配置文件，需单击“导入”完成文件的导入。（**注意：**导入备份文件后，系统自动重启，在重启系统之后才能生效。）

2.5.5 诊断工具

网络测试，包括常用的 Ping 功能、Traceroute 功能和 Tcpdump 工具。

选择“系统管理 > 诊断工具”，进入“诊断工具”界面。



- 诊断工具参数说明如下：

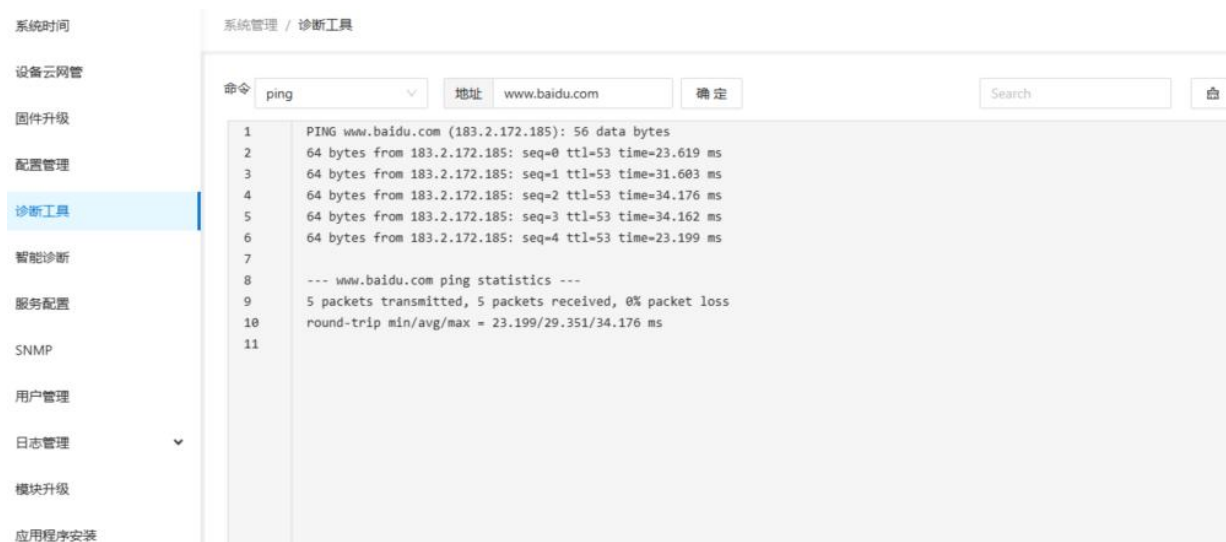
- 命令：选择测试命令。下拉可选：

- ping：测试网络连通性
 - tracert：测试网关到达目的地址的跳数
 - tcpdump：进行抓包动作，可导出抓包数据进行分析网络情况

- 地址：设置用于测试的目的 IP 地址或域名。

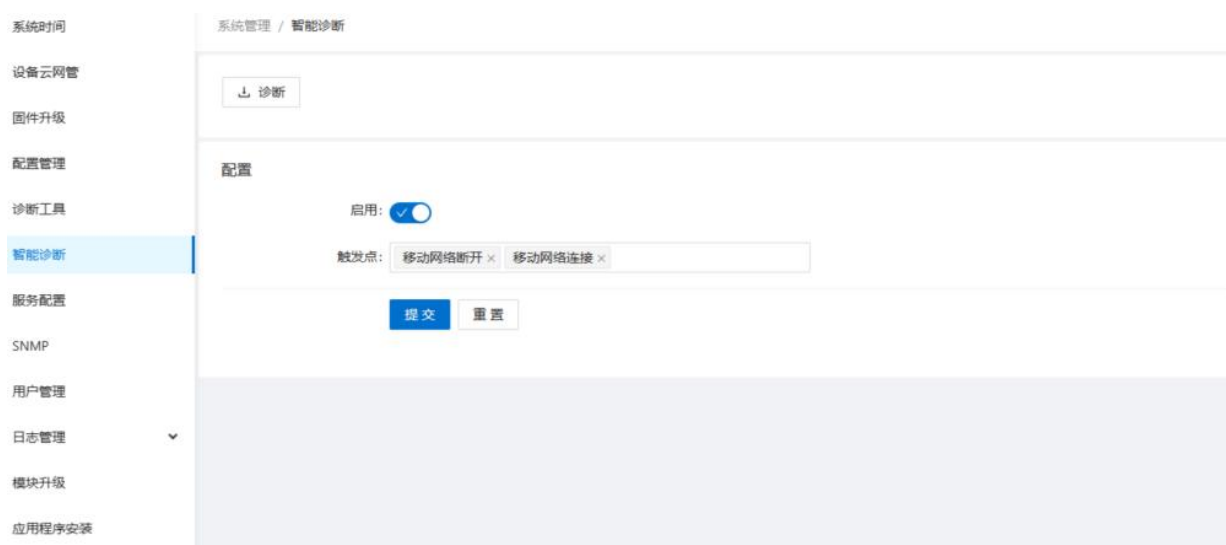
- 指定接口：使用 tcpdump 功能时选择对应的网络接口进行抓包。下拉可选：
lan/wan/goconnect/...

- 单击“确定”，可在下方框中查看结果如下图：



2.5.6 智能诊断

选择“系统管理>智能诊断”，进入“智能诊断”界面。



- 配置智能诊断工具页面参数说明如下：

- 启用：开启/关闭智能诊断功能。
- 触发点：智能诊断的触发点。下拉可选：移动网络断开/移动网络连接

2.5.7 服务配置

服务配置可对设备 WEB 管理端口号进行自定义修改，对 RFC1918 过滤、Telnet、SSH 功能进行打开或关闭设置。

选择“系统管理>服务配置”，进入“服务配置”界面。

系统管理 / 服务配置

* WEB http 端口: 80

RFC1918 过滤: ☒

Referer 检查: ☐

密码加密: ☐

启用 Telnet: ☒

启用 SSH: ☐

启用控制台: ☒

在线灯控制: 在线保持

提交 重置

- 服务配置参数说明如下：

- WEB http 端口：自定义修改设备 WEB 登陆端口号，默认 80。
- RFC1918 过滤：启用后，设备专用局域网地址将拒绝被外部访问。
- Referer 检查：是否启用 Referer 检查功能。
- 密码加密：选择是否启用密码加密。
- 启用 Telnet：选择是否启用 Telnet 功能。
- 启用 SSH：选择是否启用 SSH 功能。
- 启用控制台：是否启用控制台关闭该功能串口无法进入控制台。
- 在线灯控制：通过两种方式判断 online 灯。

1、在线保持：4G 联网成功且能正常 ping 通对应地址 online 常亮

2、移动网络：4G 网络联网成功 online 常亮

2.5.8 SNMP

选择“系统管理>SNMP”，进入“SNMP”界面。

系统时间

设备云网管

固件升级

配置管理

诊断工具

智能诊断

服务配置

SNMP

系统管理 / SNMP

启用: ☒

版本: V1

* Trap 地址:

* Trap 端口: 162

* 团体名称: public

提交 重置

- 配置 SNMP 参数说明如下：

- 版本：用户可选择 SNMP 版本。下拉可选：V1/V2/V3
- Trap 地址：用户可设置 Trap 地址。
- Trap 端口：用户可设置 Trap 端口。
- 团体名称：用户可设置团体名称。

2.5.9 用户管理

你可以在“用户管理”页面新添加一个用户或者管理用户的账号密码及访问权限，实现多用户访问和管理。

选择“系统管理>用户管理”，进入“用户管理”界面。



- 用户列表页面参数说明如下：

- 用户名：用户自定义用户名。
- 会话超时时间：设置会话超时时间。
- 角色：设置用户角色。

2.5.10 日志管理

日志管理包含网络和网关的大量信息，包括运行状态、配置变化等。

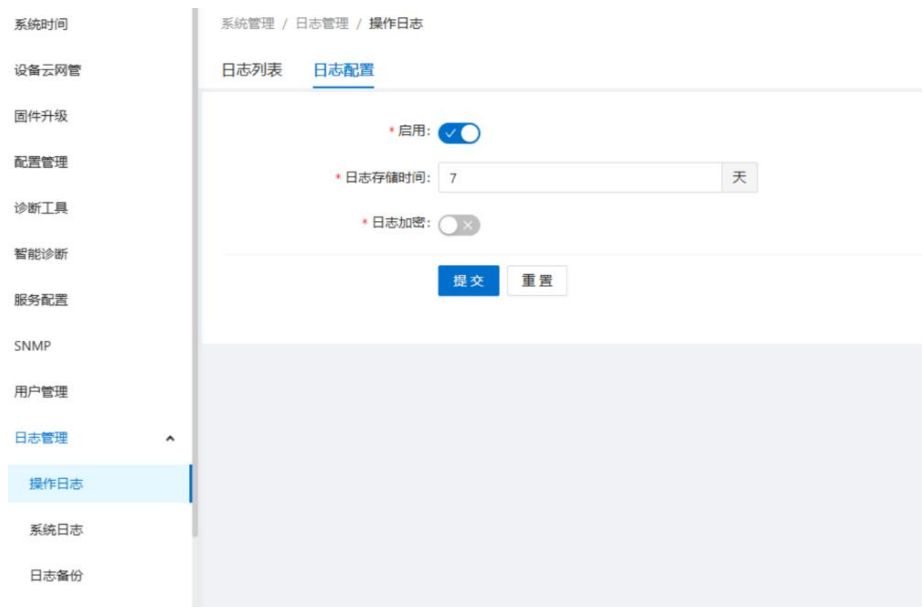
2.5.10.1 操作日志

选择“系统配置>日志管理>操作日志”，进入“操作日志”界面。

点击“日志列表”可查看操作日志信息。

时间	用户	操作	描述
2023-11-04 06:10:37	admin	用户登录	登录成功
2023-11-03 06:18:21	admin	用户登录	登录成功
2023-11-02 06:23:10	admin	用户登录	登录成功
2023-11-01 10:44:09	admin	用户登录	登录成功
2023-10-30 10:35:20	admin	用户登录	登录成功

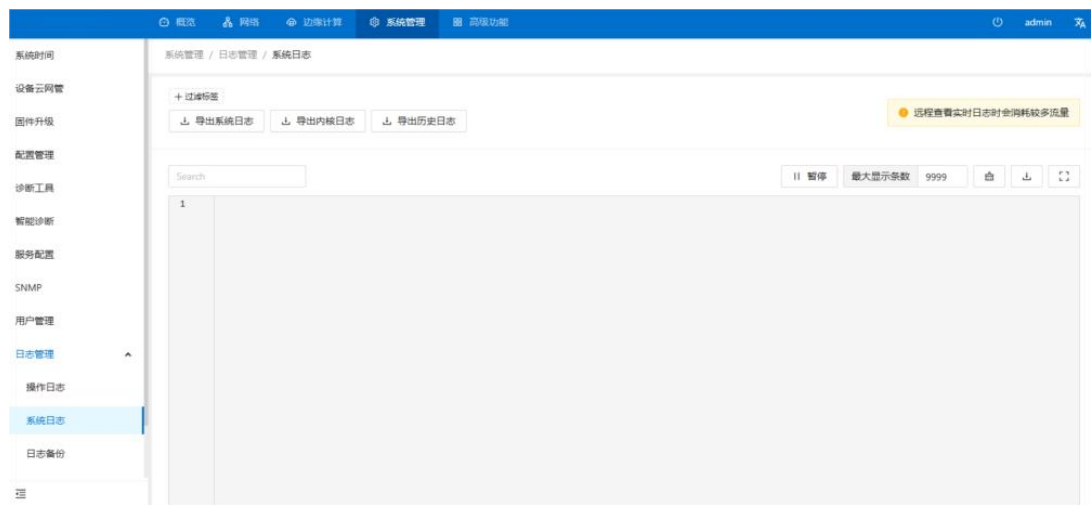
点击“日志配置”可配置日志参数信息。



- 日志配置页面参数信息说明如下：
 - 启用：开启/关闭日志配置功能。
 - 日志存储时间：日志存储的时间，默认 7 天。
 - 日志加密：是否开启日志加密功能。

2.5.10.2 系统日志

选择“系统配置>日志管理>系统日志”，进入“系统日志”页面。



此页面可以查看系统日志，能够导出系统日志/内核日志/历史日志。

2.5.10.3 日志备份

选择“系统配置>日志管理>日志备份”，进入“日志备份”页面。

系统管理 / 日志管理 / 日志备份

* 启用: ☐

备份路径:
备份路径和备份文件不能同时为空

备份文件:
备份路径和备份文件不能同时为空

* 保存路径:

* 备份周期:

* 日志存储时间: 天

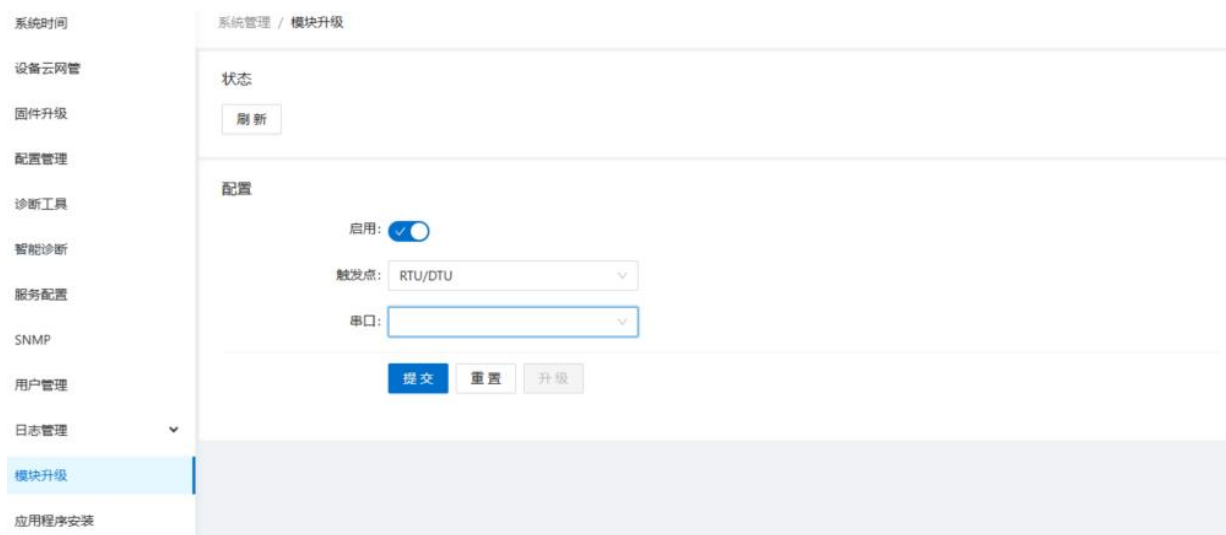
* 日志加密: ☐

- 日志备份页面参数说明如下：

- 启用：开启/关闭日志备份功能。
- 备份路径：填写备份路径，备份路径和备份文件不能同时为空。
- 备份文件：填写备份文件，备份路径和备份文件不能同时为空。
- 保存路径：填写日志备份保存路径。
- 备份周期：填写日志备份周期。
- 日志存储时间：设置日志存储时间，默认 7 天。
- 日志加密：选择是否开启日志加密。

2.5.11 模块升级

选择“系统配置>模块升级”，进入“模块升级”页面。



• 配置模块升级页面说明如下：

- 启用：开启/关闭模块升级功能。
- 触发点：配置模块升级的触发点。下拉可选：RTU/DTU、移动网络模块
- 串口：配置模块升级的串口。下拉可选：CONSOLE/COM1 (RX1/TX1) / COM2 (A1/B1) / COM3 (EX2/TX2) / COM4 (A2/B2)
- 移动网络模块：支持升级的模块：ME3630

2.5.12 应用程序安装

选择“系统配置>应用程序安装”，进入“应用程序安装”页面。



点击操作“+”上传安装包文件



2.6 导航栏操作

2.6.1 返回首页

你可以在网关的任意 WEB 界面点击左上角的“**Web控制台**”以快速跳转至“概览”页面。



2.6.2 重启

你可以点击右上角的“**🔌**”重启页面。



2.6.3 退出登录

你可以点击“**admin**”退出登录。



2.6.4 切换语言

你可以点击右上角的“**🌐**”以切换 WEB 界面的语言显示，网关支持简体中文和 English 两种语言。



3 高级功能

3.1 应用配置

3.1.1 串口应用

系统内置与注册中心和数据中心通信功能，可提供类似 DTU 功能。

选择“高级功能>应用配置>串口应用”，进入“串口应用”界面。



- 如果要在 DTU 服务器工作模式下工作，请配置 DTU 在服务器工作模式下的参数，配置的参数说明如下：
 - 启用：开启/关闭 DTU 功能。
 - 串口选择：DTU 使用的串口选择。下拉可选：Console/UART 端子
 - 协议：DTU 使用的协议。下拉列表选择：自定义/ DTU/ MQTT/ HJ212/ DC/ Modbus-Net-bridge/ 3H
 - 主中心 IP：DTU 中心服务器的地址。
 - 主中心端口：DTU 中心服务器端口。
 - 绑定端口：DTU 中心服务器绑定端口。
 - 波特率：选择串口波特率。

- 数据位：串口数据传输位。下拉可选：5~8
- 校验位：串口校验位。下拉可选：None/Odd/Even
- 停止位：串口停止位。下拉可选：1-2
- 设备 ID：连接上数据中的注册的识别 ID。
- SIM 卡号：连接上数据中的注册的 SIM 卡号码。
- 日志等级：过滤日志信息。

3.1.2 DTU 应用

DTU(Data Terminal Unit)是一种用于远程数据采集、传输和控制的设备，广泛应用于工业自动化、能源监测、环境监测等领域。

3.1.2.1 配置

选择“高级功能>应用配置>DTU 应用>配置”，进入“配置”界面。

- 配置 DTU 应用参数说明如下：

- 全局启用：开启/关闭 DTU 应用服务。
- 设备类型：选择对应的下挂设备接口类型。下拉可选：串口/网口

- 多中心轮询模式：选择多中心通信连接方式。下拉可选：轮询/并发
 - 轮询：当第一路中心通信中断，则连接第二路中心
 - 并发：同时连接多路中心
- 设备 ID：连接上数据中的注册的识别 ID。
- SIM 卡号：连接上数据中的注册的 SIM 卡号码。
- 转义：转义心跳数据。
- 自定义帧配置：配置自定义帧上报格式。下拉可选：关闭/GDP/自定义
- 心跳间隔：发送心跳包的时间间隔。

高级配置

调试等级：部分调试信息

* 调试信息接口：COM2(A1/B1)

串口缓存：☒

TCP连接在线保持：☒

* TCP在线保持空闲间隔：30000 毫秒

* TCP在线保持探测间隔：10000 毫秒

* 在线保持探测失败次数：5

* 在线保持用户超时时间：30000 毫秒

● 高级配置信息说明如下：

- 调试等级：调试日志等级信息。下拉可选：无调试信息/部分调试信息/全部调试信息
- 调试信息接口：调试信息输出串口，UART 端子。
- 串口缓存：当出现网络中断的情况下，串口数据将进行缓存，网络恢复则上报缓存数据。
- TCP 连接在线保持：通过检测 TCP 连接状态，判断链路是否存活。

- TCP 在线保持空闲间隔(毫秒)：设置空闲时间，此时间内无数据交互发送探测包。
- TCP 在线保持探测间隔(毫秒)：设置发送探测包的时间间隔。
- 在线保持探测失败次数：用于限定在线保持探测失败次数阈值。
- 在线保持用户超时时间(毫秒)：设置在线保持用户超时时间。

3.1.2.2 本地串口

选择“高级功能>应用配置>DTU 应用>本地串口”，进入“本地串口”界面。

应用配置

高级功能 / 应用配置 / DTU应用

串口应用

配置本地串口网口子设备数据中心HJ212 配置监测因子配置MQTT 配置MPPT 配置RGCC 配置通道配置

DTU应用

操作

串口	应用	波特率	数据位	校验位	停止位	封装间隔	设备功能	操作
COM1	禁用	115200	8	NONE	1	200ms	所有数据中心	编辑
COM2	禁用	115200	8	NONE	1	200ms	所有数据中心	编辑
COM3	禁用	115200	8	NONE	1	200ms	所有数据中心	编辑
COM4	禁用	115200	8	NONE	1	200ms	所有数据中心	编辑

第 1-4 条/总共 4 条 < 1 > 10 条/页

3.1.2.3 网口子设备

选择“高级功能>应用配置>DTU 应用>网口子设备”，进入“网口子设备”界面。

应用配置

高级功能 / 应用配置 / DTU应用

串口应用

配置本地串口网口子设备数据中心HJ212 配置监测因子配置MQTT 配置MPPT 配置RGCC 配置通道配置

DTU应用

操作

序号	应用	从设备地址	对端端口	工作模式	网口功能	操作
1	禁用	无	5002	TCP客户端	关闭	编辑
2	禁用	无	5002	TCP客户端	关闭	编辑
3	禁用	无	5002	TCP客户端	关闭	编辑
4	禁用	无	5002	TCP客户端	关闭	编辑

第 1-4 条/总共 4 条 < 1 > 10 条/页

3.1.2.4 数据中心

选择“高级功能>应用配置>DTU 应用>数据中心”，进入“数据中心”界面。



- 点击操作列的“编辑”对数据中心进行参数配置，数据中心配置参数页面如下图。

The screenshot shows a modal dialog box titled '编辑' (Edit) with a close button (X). It contains four configuration fields: '工作模式' (Work Mode) is a dropdown menu currently set to 'TCP'; '使用自定义帧' (Use Custom Frame) is an unchecked checkbox; '数据中心地址' (Data Center Address) is an empty text input field; and '数据中心端口' (Data Center Port) is a text input field containing the value '23'. At the bottom right of the dialog are two buttons: '取消' (Cancel) and '确定' (Confirm).

- 数据中心配置参数说明如下：
 - 工作模式：设置与数据中心相对应的工作模式。下拉可选：HJ212_2005/ HJ212_2017/ HTTP/.../ HJ212_TRANS（注意：数据中心的工作模式若选择 HJ212_2005、HJ212_2017、HJ212_TRANS、MQTT 等中其一，需进行下一步的参数配置，数据才可正常上报。）
 - 数据中心地址：填写数据中心域名或 IP 地址。
 - 数据中心端口：填写数据中心开放的数据接收端口号。

3.1.2.5 HJ212 配置

选择“高级功能>应用配置>DTU 应用>HJ212 配置”，进入“HJ212 配置”界面。

配置 本地串口 网口子设备 数据中心 HJ212 配置 监测

实时上报使能: ☒

* 实时数据上报间隔: 30 秒

* 分钟上报间隔: 10 分钟

小时上报: ☒

日上报: ☒

FLAG: ☒

QN: 发送

* 系统编码: 31

拓展中心ST1:

拓展中心ST2:

拓展中心ST3:

拓展中心ST4:

* 命令编码: 2011

* 访问密码: 123456

* 设备唯一标识: 88888888

HJ212转发串口: 关闭

* HJ212透传上行MN: 88888888

* HJ212透传下行MN: 88888888

> 字段配置

> 加密配置

> 高级配置

- HJ212 配置参数说明如下:

- 实时上报使能: 是否实时上报数据报文。
- 实时数据上报间隔: 设置实时数据上报的时间间隔。
- 分钟上报间隔: 设置分钟上报的时间间隔。
- 小时/日上报: 是否上报小时/日报文。
- FLAG: 是否上报 FLAG。
- QN: 是否发送 QN。
- 系统编码: 主中心系统编码。
- 拓展中心 ST1~ST4: 多中心并发模式下拓展中心 1~4 系统编码, 为空时使用主中心系统编码。

- 命令编码：设置命令编码。
- 访问密码：设置访问密码。
- 设备唯一标识：设置设备唯一标识符。
- HJ212 转发串口：选择转发报文的串口。下拉可选：关闭/UART 端子
- HJ212 透传上行 MN：透传模式下，上行数据 MN。
- HJ212 透传下行 MN：透传模式下，下行数据 MN。



√ 字段配置

上报字段 MIN: ☒

上报字段 AVG: ☒

上报字段 MAX: ☒

上报字段 COU: ☒

- “字段配置”页面配置上报字段信息配置：

- 上报字段 MIN/AVG/ MAX/COU：是否配置上报字段限制。



√ 加密配置

加密模式: 不加密

* 加密次数: 2

加密密钥: D780D0D4

iv偏移量: 83202380

填充方式: PKCS5Padding

* 数据块大小: 256

- 加密配置参数说明如下：

- 加密模式：设置是否对上报的数据进行加密。下拉可选：不加密/DES 不加密/DES 加密/AES 加密
- 加密次数：对数据进行 X 次加密，需手动输入。

- 加密密钥：设置数据加密密钥，需手动输入。
- iv 偏移量：设置 iv 偏移量，需手动输入。
- 填充方式：设置填充方式。下拉可选：ZeroPadding/ PKCS5Padding/ PKCS7Padding
- 数据块大小：设置数据块大小。



高级配置

CRC大小写: 大写

* 报文重发间隔: 3 秒

* 报文重发次数: 3

中心1应答标志: 不应答

中心2应答标志: 不应答

中心3应答标志: 不应答

中心4应答标志: 不应答

中心5应答标志: 不应答

- 高级配置参数信息说明如下：

- CRC 大小写：配置 CRC 校验码大小写。下拉可选：大写/小写
- 报文重发间隔：设置报文重发间隔。
- 报文重发次数：设置报文重发次数。
- 中心 1/2/3/4/5 应答标志：设置中心 1/2/3/4/5 应答标志。下拉可选：应答/不应答

3.1.2.6 监测因子配置

选择“高级功能>应用配置>DTU 应用>检测因子配置”，进入“检测因子配置”界面。

应用配置

高级功能 / 应用配置 / DTU应用

配置本地串口网口子设备数据中心HJ212 配置监测因子配置MQTT 配置MPPT 配置RGCC 配置通道配置

DTU应用

定时任务位置服务LoRa应用短信服务探针应用VPN 服务

序号	监测因子编码	折算值	采集通道	操作
0	a24087	禁用	禁用	✎
1	a24088	禁用	禁用	✎
2	a24089	禁用	禁用	✎
3	a24090	禁用	禁用	✎
4	a24091	禁用	禁用	✎
5	a24092	禁用	禁用	✎
6	a24093	禁用	禁用	✎

操作

- 点击操作列表编辑检测因子参数配置

编辑

×

序号:	0
* 监测因子编码:	a24087
折算值:	☐
COU统计方式:	累加
* 小时上报间隔:	1 小时
采集通道:	☐
硬件类型:	串口
硬件编号:	COM1(RX1/TX1)
* 从站号:	1
* 寄存器地址:	0
* 寄存器个数:	2
Modbus功能码:	3
写寄存器函数码:	10H
* 数据类型:	float
* 数据格式:	ABCD
默认实时数据:	<NONE>
* 采集间隔时间:	1000 秒
数据上报方式:	按时上报
* 缩放因子:	1
* 基值:	0.0
* 因子上报精度:	2
* 下量程:	0
* 上量程:	0
* 最小值:	0
* 最大值:	0
* 比特位置:	0
* 丢弃初始数据包:	0 个
Modbus累计使能:	☐
采集失败上报值:	当前值

- 监测因子配置参数说明如下:

- 监测因子编码：设置监测因子命名编码，需手动输入。
- 折算值：选择是否启用折算值。
- COU 统计方式：分钟报、小时报、日报中上报 COU 方式。下拉可选：累加/区间累计
- 小时上报间隔：小时包数据时间，取值范围在 0~23。
- 硬件类型：选择数据接入类型，可选择串口数据或运算数据。下拉可选：串口/运算
- 硬件编号：当使用串口接入数据方式，需要指定使用设备对应的串口号。下拉可选：关闭/UART 端子
- 从站号：配置从设备 ID 号，取值范围在 1~254。
- 寄存器地址：配置寄存器地址。
- 寄存器个数：配置寄存器个数，可配置寄存器数为 1~4。
- Modbus 功能码：选择对应的 Modbus 通信协议功能码。下拉可选：1/2/3/4
- 写寄存器函数码：选择对应的 Modbus 通信协议的写寄存器函数码，下拉可选：05H/06H/0FH/10H
- 数据类型：选择对应的数据类型，下拉可选：int/float/.../int32
- 数据上报方式：上报数据方式，下拉可选：按时上报/变更上报
 - 按时上报：按照实时上报间隔上报数据
 - 变更上报：当采集到的数据发送变化时上报一包报文。
- 缩放因子：对采集的数据进行缩放设置。
- 基值：在采集的数据基础上赋值。
- 因子上报精度：上报的数据小数点位数，取值范围在 0~6。
- 上/下量程：设置上/下量程限值。
- 丢弃初始数据包：某些场景下，需要设置过滤初始数据包，以保数据准确性。

- Modbus 累计使能：选择启用或者关闭 Modbus 累计功能。
- 采集失败上报值：采集数据失败时上报，下拉可选：当前值/默认值

3.1.2.7 MQTT 配置

选择“高级功能>应用配置>DTU 应用>MQTT 配置”，进入“MQTT 配置”界面。

The screenshot displays the 'MQTT 配置' (MQTT Configuration) page. The left sidebar shows the navigation menu with 'DTU应用' (DTU Application) selected. The main content area contains the following fields:

- * ClientID: 123456789000
- 发布主题: /up
- 用户名: username
- 密码: password
- 服务质量: 1 (dropdown)
- MQTT 版本: MQTT 3.1 (dropdown)
- 连接清空标志: ☐
- 订阅主题: /down
- 拓展订阅主题2: (empty field)
- 拓展订阅主题3: (empty field)
- 拓展订阅主题4: (empty field)

At the bottom right, there are two buttons: '提交' (Submit) and '重置' (Reset).

- MQTT 配置参数说明如下：

- ClientID：客户端 ID，需手动输入。
- 发布主题：配置 MQTT 发布消息的主题，需手动输入。
- 服务质量：配置 MQTT 订阅服务器使用的服务质量等级。下拉可选：0/1/2
- MQTT 版本：设置 MQTT 版本。下拉可选：MQTT3.1/ MQTT3.1.1
- 连接清空标志：选择是否启用连接清空标志功能。
- 订阅主题：配置 MQTT 订阅消息主题，需手动输入。

3.1.2.8 MPPT 配置

The screenshot shows the 'MPPT 配置' (MPPT Configuration) page within the 'DTU应用' (DTU Application) settings. The page has a breadcrumb trail: '高级功能 / 应用配置 / DTU应用'. The left sidebar lists various application settings, with 'DTU应用' selected. The main content area contains four input fields: 'PK:', 'DN:', 'SECRET:', and '上报间隔:' (Report Interval). The '上报间隔' field is set to '30' seconds. At the bottom, there are '提交' (Submit) and '重置' (Reset) buttons.

- MPPT 配置页面参数说明如下：
 - PK：最大功率点的功率值。
 - DN：最大功率点位置
 - SECRET：最大功率点追踪。
 - 上报间隔：设置上报间隔时间。

3.1.2.9 RGCC 配置

选择“高级功能>应用配置>DTU 应用>RGCC 配置”，进入“RGCC 配置”界面。

The screenshot shows the 'RGCC 配置' (RGCC Configuration) page within the 'DTU应用' (DTU Application) settings. The breadcrumb trail is '高级功能 / 应用配置 / DTU应用'. The left sidebar shows 'DTU应用' selected. The main content area contains several input fields and dropdown menus: '采集超时时间:' (Collection Timeout) set to '1000' seconds, '轮询重试次数:' (Polling Retry Count) set to '0', '定时上报时间:' (Scheduled Report Time) set to '60' seconds, '自定义轮询时间间隔:' (Custom Polling Time Interval) set to '30' seconds, '指令间隔时间:' (Command Interval Time) set to '1000' milliseconds, 'CRPC上报方式:' (CRPC Report Method) set to '变化上报' (Report Change), and '注册包模式:' (Registration Packet Mode) set to '仅首次连接时' (Only at first connection). At the bottom, there are '提交' (Submit) and '重置' (Reset) buttons.

- RGCC 配置页面参数信息说明如下：
 - 采集超时时间：设置采集超时时间限制，默认设置 1000 秒。
 - 轮询重试次数：设置采集轮询重试次数。

- 定时上报时间：设置数据定时上报时间，默认 60 秒。
- 自定义轮询时间间隔：设置采集轮询间隔时间，默认 30 秒。
- 指令间隔时间：每条指令间隔时间，默认 1000 毫秒。
- CR 电脑上报方式：设置 CR 电脑上报方式。下拉可选：变化上报/按时上报
 - 按时上报：按照实时上报间隔上报数据
 - 变化上报：当采集到的数据发送变化时上报一包报文。
- 注册包模式：设置注册包模式。下拉可选：仅首次连接时/仅数据上传时/同时

3.1.2.10 通道配置

选择“高级功能>应用配置>DTU 应用>通道配置”，进入“通道配置”界面。

应用配置

高级功能 / 应用配置 / DTU应用

配置 本地串口 网口子设备 数据中心 HJ212 配置 监测因子配置 MQTT 配置 MPPT 配置 RGCC 配置 通道配置

DTU应用

定时任务

位置服务

LoRa应用

短信服务

探针应用

序号	启用	串口	自定义轮询时间指令	自定义包头	操作
0	禁用	COM1		<NONE>	✎
1	禁用	COM1		<NONE>	✎
2	禁用	COM1		<NONE>	✎
3	禁用	COM1		<NONE>	✎

- 点击操作可编辑通道配置参数

编辑

✕

序号: 0

启用: ☐

串口: COM1(RX1/TX1)

自定义轮询时间指令:

自定义包头格式: ASCII

自定义包头: <NONE>

取消 确定

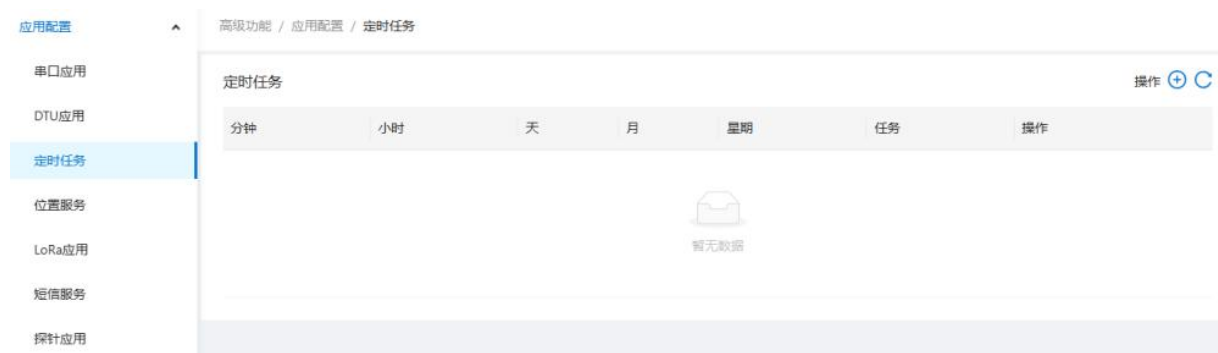
- **配置 RGCC 通道参数说明如下：**

- 启用：开启/关闭 RGCC 通道功能。
- 串口：选择需使用的串口号。下拉可选：UART 端子
- 自定义轮询指令：设置自定义轮询指令，需手动输入。
- 自定义包头格式：设置自定义包头格式。下拉可选：HEX/ASCII
- 自定义包头：设置自定义包头内容，需手动输入。

3.1.3 定时任务

作为一个无线业务网关路由产品，很多客户在使用时希望能控制网关的在线时长，以便能对网络业务和 3G/4G/5G 资费进行更好的管理。工业级网关任务管理可以满足客户此类需求，客户可以根据需求配置多个在线时间（如某天的某几个小时），除此之外它还能实现时间点的任务执行（如每天凌晨零点重新拨号或重启系统）。

选择“高级功能>应用配置>定时任务”，进入“定时任务”界面。



点击操作“+”创建定时任务。

创建

×

分钟:

小时:

天:

月:

星期:

任务:

重启

ⓘ *: 每分钟 (小时, 天, 月, 周) 执行

ⓘ a-b: 第a到b分钟 (小时, 天, 月, 周) 内执行

ⓘ */n: 每隔n分钟 (小时, 天, 月, 周) 执行

ⓘ a,b,c,...: 第a, b, c, ...分钟 (小时, 天, 月, 周) 执行

取消

确定

- 配置定时任务通道参数说明如下：

- 分钟：组合使用时为时间点，独立使用时为每 X 分钟
- 小时：组合使用时为时间点，独立使用时为每 X 小时。
- 天：某月的某天
- 月：具体月份
- 星期：具体星期
- 任务：下拉选择：重启、关闭 LAN、开启 LAN、重播移动网络、开启移动网络、关闭移动网络、开启设备云网管、关闭设备云网管、自定义等定时任务。

3.1.4 位置服务

3.1.4.1 定位服务

选择“高级功能>应用配置>位置服务>定位服务”，进入“定位服务”界面。

应用配置

高级功能 / 应用配置 / 位置服务

串口应用

DTU应用

定时任务

位置服务

LoRa应用

短信服务

VPN 服务

状态

禁用

配置

定位服务 IP转发 串口转发 Modbus JT/T 808 百度鹰眼

启用: ☒

搜星模式: GPS/北斗混合定位

* 更新间隔: 3 秒

A-GNSS: ☐

基站定位: ☐

提交 重置

- 定位服务参数说明如下：

- 启用：开启/关闭定位服务功能。
- 搜星模式：下拉可选：GPS 定位、北斗定位、GPS/北斗混合定位
- 更新时间：设置定位服务更新时间，默认 3s。
- A-GNSS：开启 A-GNSS 功能。
- 基站定位：开启基站定位服务。

3.1.4.2 IP 转发

选择“高级功能>应用配置>位置服务>IP 转发”，进入“IP 转发”界面。

配置

定位服务 IP转发 串口转发 Modbus JT/T 808 百度鹰眼

启用: ☒

* 主中心IP: 192.168.1.2

* 主中心端口: 5001

包头增加设备ID: ☐

设备ID:

数据类型: 原始数据

* 上报间隔: 60 秒

提交 重置

- IP 转发参数说明如下：

- 启用：开启/关闭位置服务 IP 功能。
- 主中心 IP：中心服务器的地址。
- 主中心端口：中心服务器端口。
- 包头增加设备 ID：选择是否开启该功能。
- 设备 ID：填写设备 ID 号。
- 数据类型：位置数据类型。下拉列表选择：原始数据/位置数据/GPGGA/GPRMC/IEC101
- 上报间隔：设置上报间隔时间，默认 60 秒。

3.1.4.3 串口转发

选择“高级功能>应用配置>位置服务>串口转发”，进入“串口转发”界面。

- 串口转发参数说明如下：

- 启用：开启/关闭位置服务串口转发功能。

- 串口选择：提供多串口选择（部分机型只支持 console 串口接口）。下拉可选：console/COM1/COM2/COM3/COM4
- 波特率：选择串口波特率。
- 校验位：串口校验位。下拉可选：None/Odd/Even
- 停止位：串口停止位。
- 数据类型：位置数据类型。下拉可选：原始数据/位置数据/GPGGA/GPRMC/IEC101
- 上报间隔：设置上报间隔时间，默认 60 秒。

3.1.4.4 Modbus

选择“高级功能>应用配置>位置服务>Modbus”，进入“Modbus”界面。



配置

定位服务 IP转发 串口转发 **Modbus** JT/T 808 百度鹰眼

启用: ☒

工作模式: ModbusTCP

* 从站号: 1

* 端口: 5001

提交 重置

- **Modbus 参数说明如下：**

- 启用：开启/关闭位置服务 Modbus 功能。
- 工作模式：Modbus 工作模式。可选 ModbusTCP/ModbusRTU
- 从站号：从站号为 1 字节，取值范围为 0~FFH。
- 端口：0-65535 范围内的端口号。

3.1.4.5 JT/T 808

选择“高级功能>应用配置>位置服务>JT/T 808”，进入“JT/T 808”界面。



- JT/T 808 参数说明如下：

- 启用：开启/关闭 JT/T 808 功能。
- 协议版本：运输车辆卫星地位系统协议。下拉可选：2019/2013
- 主中心 IP：中心服务器的地址。
- 主中心端口：中心服务器端口。
- 心跳周期：间隔 N 秒发送一次心跳，默认 30。
- 超时时间：检测链路超时的时间，默认 5 秒。
- 位置汇报间隔：位置间隔上报周期，默认 60 秒。

- 终端手机号：设置终端手机号。
- 省域/市县 ID：填写省域/市县 ID 号，默认 0。
- 制造商 ID：填写制造商 ID 号。
- 终端型号：填写终端型号。
- 终端 ID：填写终端 ID 号。
- 车牌颜色：填写车牌颜色，默认 0。
- 车牌号：填写车牌号码。
- 状态：可查看注册状态。

3.1.4.6 百度鹰眼

百度鹰眼相关配置信息需通过百度平台获取填入相关配置内。

选择“高级功能>应用配置>位置服务>百度鹰眼”，进入“百度鹰眼”界面。

配置

定位服务 IP转发 串口转发 Modbus JT/T 808 百度鹰眼

启用: ☒

* 服务ID:

名称:

* 服务Token:

* 更新间隔: 秒

提交 重置

- 百度鹰眼参数说明如下：

- 启用：开启/关闭百度鹰眼功能。
- 服务 ID：设置服务 ID。

- 名称：设置名称。
- 服务 Token：设置 Token。
- 更新间隔：数据更新时间，默认 10 秒。

3.1.5 LoRa 应用

3.1.6.1 LoRa 应用

选择“高级功能>应用配置>LoRa 应用”，进入“LoRa 应用”界面。



- 创建一个新的 LoRa 应用配置页面。

创建

✕

* 名称:

启用:

☒

* 串口:

工作模式:

透传

接收方地址:

☐

波特率:

115200

数据位:

8

校验位:

NONE

停止位:

1

* 超时时间:

3000

毫秒

日志等级:

INFO

- LoRa 应用配置参数说明如下:

- 启用: 开启/关闭 Lora 应用。
- 串口: 中心服务器端口。下拉可选: Console/COM
- 工作模式: Lora 应用工作模式。下拉可选: 透传/定向/自定义
- 接收方地址: 是否开启接收方地址。

高级配置

空中速率:

2.4K

* 模块信道:

23

* 模块地址:

4660

模块调试等级:

部分调试信息

- 高级配置参数说明如下:

- 空中速率: 配置无线空中速率频段, 两端需保持一致。下拉可选: 0.3K/1.2K/...2.4K

- 模块信道：设置通信模块信道。下拉可选：1~32
- 模块地址：设置通信模块地址。
- 模块调试等级：模块调试日志信息等级。下拉可选：无调试信息/部分调试信息/模块调试信息

3.1.6.2 LoRa 通道

选择“高级功能>应用配置>LoRa 通道”，进入“LoRa 通道”界面。

通道名称	接收方信道	接收方地址	虚拟串口名	操作
1	23	4560		
2	24	4561		

第 1-2 条/总共 2 条 < 1 >

- 创建一个新的 LoRa 通道

创建

×

* 通道名称:

波特率: 115200

数据位: 8

校验位: NONE

停止位: 1

* 接收方信道:

* 接收方地址:

取消

确定

- LoRa 通道参数说明如下：
 - 通道名称：自定义通道名称。
 - 接收方信道：设置接收方信道。
 - 接收方地址：设置接收方地址。

3.1.6 短信服务

选择“高级功能>应用配置>短信服务”，进入“短信服务”界面。

应用配置

高级功能 / 应用配置 / 短信服务

串口应用

DTU应用

定时任务

位置服务

LoRa应用

短信服务

探针应用

VPN 服务

启用: ☒

* 端口:

目的号码:

分隔符:

PIN码:

Modem设备:

提交 重置

- 短信服务参数说明如下：

- 启用：开启/关闭短信服务功能。
- 端口：设置需要开放的端口号。
- 目的号码：设备发往的目的号码。
- 分隔符：填写分隔符。
- PIN 码：设备卡的 PIN 码。
- Modem 设备：设备端口，开启移动网络时可能会影响短信发送占用设备端口。

3.1.7 探针应用

选择“高级功能>应用配置>探针应用”，进入“探针应用”界面。

应用配置

高级功能 / 应用配置 / 探针应用

串口应用

DTU应用

定时任务

位置服务

LoRa应用

短信服务

探针应用

VPN 服务

启用: ☒

* 服务器地址:

* 端口:

IMEI:

IMSI:

* 平台登录验证标识:

* 文件存储路径:

* 日志等级:

提交 重置

- 探针应用页面参数说明如下：

- 启用：开启/关闭探针应用功能。
- 服务器地址：填写服务器地址。
- 端口：填写应用端口。
- IMEI：标识移动设备，用于设备管理。
- IMSI：标识移动网络中的用户，提供网络服务。
- 平台登录验证标识：用于确认用户或设备合法登录平台的凭证
- 文件存储路径：文件存储路径，默认不可改。
- 日志等级：配置日志等级。

3.2 VPN 服务

VPN 是在公共网络（如互联网）基础上构建的“虚拟”私人专用通信网络。所谓“虚拟”，是指它并非像传统的专用网络那样拥有独立的物理链路和基础设施，而是通过网络技

术在公共网络上建立起一个逻辑上隔离且专用的通信通道，实现类似于专用网络的功能和安全性。

通过隧道技术、加密技术等手段，使得用户在使用 VPN 时感觉像是在一个独立、安全的专用网络中进行通信，但实际上数据是在公共网络的基础上传输的，只是在逻辑上实现了专用性和私密性。

3.2.1 L2TP/PPTP

L2TP 服务器部署在企业总部，通常作为企业总部的网关。L2TP 服务器接收 L2TP 客户端所传递的用户信息，对接入的用户身份进行验证，响应 L2TP 客户端发起的 L2TP 隧道连接请求，和 L2TP 客户端共同建立 L2TP 连接。

3.2.1.1 客户端

选择“高级功能>VPN 服务> L2TP/PPTP>客户端”，进入“客户端”页面。



3.2.1.2 服务端

选择“高级功能>VPN 服务> L2TP/PPTP>服务端”，进入“服务端”页面。



- 创建一个新的 L2TP 服务器页面。

创建

×

* 接口名称:

vpn4CNrA

* 协议:

L2TP

▼

地址分配:

10.0.0.1/24

添加默认路由:

☐

×

MTU:

1500

> 高级配置

取消

确定

- L2TP 服务器配置参数说明如下：
 - 启用：开启/关闭 L2TP 服务器功能。
 - 接口名称：该条 VPDN 规则的名称。
 - 地址分配：设置 L2TP 服务器的私网 IP 地址及地址池。网关 IP”作为 L2TP 客户端的网关地址，“子网掩码”确定动态分配给 L2TP 客户端的 IP 地址资源。
 - MTU：设置最大传输单元, 手动输入数值，默认值为 1500。
- 单击“高级配置”展开高级配置内容，对 L2TP 高级配置

▼ 高级配置

禁用 EAP: ☐

禁用 CHAP: ☐

禁用 PAP: ☐

禁用 MS-CHAP: ☐

禁用 MS2-CHAP: ☐

* LCP 间隔时间: 秒

* LCP 重试次数:

启用 MPPE: ☐

• L2TP 服务器高级配置参数说明如下：

- 禁用 EAP：是否禁用 EAP。
- 禁用 CHAP：是否禁用 CHAP。
- 禁用 PAP：是否禁用 PAP。
- 禁用 MS-CHAP：是否禁用 MS-CHAP。
- 禁用 MS2-CHAP：是否禁用 MS2-CHAP。
- LCP 间隔时间：设置 LCP 间隔时间，默认 30 秒。
- LCP 重试次数：设置 LCP 重试次数，默认 5 次。
- 启用 MPPE：是否启用 MPPE。

3.2.2 IPsec

IPSec VPN 即指采用 IPSec 协议来实现远程接入的一种 VPN 技术。

选择“高级功能> VPN 服务> IPsec”，进入“IPsec”页签。

启用: ☒

* 运行模式: ☒ 客户端模式 ☐ 服务端模式

协商模式: 主动模式

启动模式: 默认

* 对端地址: 192.168.0.227

IKE 认证模式: IKE-PSK

* 共享密钥: admin

封装模式: 隧道模式

本地子网: 192.168.1.0/24

本地协议端口:

对端子网: 192.168.13.0/24

对端协议端口:

本端标识: abc

对端标识: 123

启用DPD检测: ☒

DPD动作: 默认

* 检测间隔: 30 秒

* 超时时间: 150

关闭动作: 无

第一阶段

加密方式: 3des

哈希算法: md5

DH 组: group 2(1024)

* IKE 生命周期: 86200

第二阶段

加密方式: 3des

认证算法: md5

PFS 组: group 2(1024)

* KEY 生命周期: 28800

提交 重置

- IPsec 配置参数说明如下:

- 启用: 开启/关闭 IPsec 功能。
- 运行模式: 选择运行模式。下拉可选: 客户端模式/服务端模式
- 协商模式: 选择 IKE 的协商模式。如果 IPSEC 隧道一端的 IP 地址是自动获取的。下拉可选: 主动模式/野蛮模式

- 主动模式：主动模式将密钥交换信息与身份认证信息相分离。这种分离保护了身份信息，从而提供了更高的安全性。
- 野蛮模式：野蛮模式缺少身份认证，但可以满足某些特定的网络环境需求。如果无法预先知道发起者的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥认证方法来创建 IKE SA，就可以用野蛮模式。
- 启动模式：设置 IPsec 启动阶段的默认模式。下拉可选：自动/触发/添加
 - 自动：启动 IPsec 则自动发起连接。
 - 触发：当设备产生 IPsec 数据流，则发起连接。数据流，则发起连接。
 - 添加：作为服务端模式下，用于等待客户端接入的状态。
- 对端地址：设置对端 IP 地址或域名。
- IKE 认证模式：选择 IKE 协商的认证模式。下拉可选：IKE-PSK/IKE-PSK-XAUTH
- 封装模式：选择数据报文封装格式。下拉可选：隧道模式/传输模式
 - 隧道模式：在原始 IP 报文头外封装一个 IPSec 报文头（AH 或 ESP），然后在最外层封装新的 IP 报文头，原 IP 报文被当作有效载荷的一部分受到 IPSec 的保护。隧道模式一般用在两个安全网关之间。在一个安全网关被加密的报文，只有到达另一个安全网关才能够被解密。
 - 传输模式：在 IP 报文头和上层协议报文头之间插入一个 IPSec 报文头（AH 或 ESP）。在这种模式下，原 IP 报文头不变，只是 IP 协议字段被改为 AH 或 ESP，并重新计算 IP 报文头校验和。传输模式适用于两台主机，或者是一台主机和一个安全网关之间的通讯。
- 共享密钥：使用的密钥。
- 本地子网：IPsec 定义的感兴趣流中的源网络。
- 对端子网：IPsec 定义的感兴趣流中的目的网络。
- 本端/对端标识：本端/对端地址标识。

- 启用 PDP 检测：是否使用 PDP 检测。
 - DPD 超时时间：当接收端触发 DPD 查询，主动向对端发送请求报文进行检测，超过超时时间仍没有收到对端的 DPD 回应报文时，将删除此 IPsec SA。合法值：10-3600 单位：秒
 - DPD 重试间隔：用于 IPsec 邻居状态的检测时间间隔。启动 DPD 功能后，当接收端在触发 DPD 的时间间隔内收不到对端的 IPsec 加密报文时，能够触发 DPD 查询，主动向对端发送请求报文，对 IKE 对等体是否存在进行检测。合法值：1-60，单位：秒
- PDP 动作：PDP 心跳选择。下拉可选：清除/保持/重连
- 加密方式：选择第一阶段的加密方式。下拉可选：aes128/aes192/aes256/3des/des
 - 3des：使用三个 64bit 的 des 密钥对明文进行加密
 - des：使用 64bit 的密钥对一个 64bit 的明文块进行加密
 - aes：使用 128bit、192bit 或 256bit 密钥长度的 aes 算法对明文进行加密
- 哈希算法：可选择 md5/sha1/sha256/sha384/sha512/不使用
 - md5：通过输入任意长度消息，产生 128bit 的消息摘要
 - sha1：输入长度小于 128bit 消息，产生 160bit 消息摘要
 - sha256：输出 256bit
 - sha384：输出 384bit
 - sha512：输出 512bit
- 认证算法：可选择 md5/sha1/sha256/sha384/sha512/不使用
- DH 组：选择 DH 分组应用于 IKE 协商。下拉可选：group 1(768)/group 2(1024)/group 5(1536)/group 14(2048)/group 15(3072)/group 16(4096)
- PFS 组：选择 PFS 分组应用于 IKE 协商。

- IKE 生命周期：设置在 IKE 协商中的生存时间。在 SA 过期前，IKE 协商出新的 SA；新的 SA 一建立，立即生效；旧的一个过期后会立即清除。
- 单击“高级配置”展开高级配置内容，对 IPSEC 高级配置



说明：

- 加密算法的安全性由高到低依次是：aes、3des、des，安全性高的加密算法实现机制复杂，但运算速度慢。对于普通的安全要求，des 算法就可以满足需要
- 当网关作为 IPsec server 时，对端地址请配置成 0.0.0.0，一般用于一端公网地址，一端拨号上网地址不固定场景
- IPsec 扩展一般和 GRE 结合使用，用于组建 DMVP 或 GRE OVER IPsec 网络

3.2.3 GRE

通用路由封装（GRE）定义了在任何一种网络层协议上封装任意一个其它网络层协议的协议。GRE 可以作为 VPN 的三层隧道协议，为 VPN 数据提供透明传输通道。简单来说，GRE 是一种隧道技术，提供了一条通路使封装的数据报文能够在这个通路上传输，在隧道的两端分别对数据报进行封装及解封装。



点击操作“+”创建 GRE 页面。

创建

×

协议：

GRE

* 对端WAN IP：

* 对端子网地址：

* 对端子网掩码：

本端WAN IP：

添加HOST路由：

×

NAT：

✓

MTU：

1280

* 本端隧道IP：

* 本端隧道掩码：

取消

确定

- 配置 GRE 参数说明如下：

- 协议：设置 GRE 类型，Ethernet over GRE 为二层 GRE。下拉可选：GRE/Ethernet over GRE
- 当协议为 GRE 时：
 - 对端 WAN IP：设置 GRE 隧道的对端 IP 地址。

- 对端子网地址：设置 GRE 隧道的对端 IP 的子网地址。
 - 对端子网掩码：设置 GRE 隧道的对端子网掩码。
 - 本端 WAN IP：设置 GRE 隧道的本端 IP 地址。
 - 添加 HOST 路由：是否使用 HOST 路由。
 - NAT：是否开启 NAT 功能。
 - MTU：设置 GRE 隧道的最大传输单元，以字节为单位，默认值为 1500。
 - 本端隧道 IP：设置 GRE 隧道的本端 IP 的子网地址。
 - 本端隧道掩码：设置 GRE 隧道的本端子网掩码。
- 当协议为 Ethernet over GRE 时：
- 对端 WAN IP：设置 Ethernet over GRE 隧道的对端 IP 地址。
 - 本端 WAN IP：设置 Ethernet over GRE 隧道的本端 IP 地址。
 - 添加 HOST 路由：是否使用 HOST 路由。
 - NAT：是否开启 NAT 功能。
 - MTU：设置 Ethernet over GRE 隧道的最大传输单元，以字节为单位，默认值为 1500。
 - 桥接接口：选择 Ethernet over GRE 隧道桥接接口，默认为 lan。

3.2.4 OpenVPN

在 OpenVPN 中，如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN 模式）或数据帧（TAP 模式）发送到虚拟网卡上，服务程序接收该数据并进行相应的处理后，通过 SOCKET 从外网上发送出去，远程服务程序通过 SOCKET 从外网上接收数据，并进行相应的处理后，发送给虚拟网卡，则应用软件可以接收到，完成了一个单向传输的过程，反之亦然。

选择“高级功能> VPN 服务>OpenVPN”，进入“OpenVPN”界面。

状态

状态: 未连接

接口名称:

IP地址:

子网掩码:

网关:

配置

接口

证书管理

配置: ☒

* 服务器地址:

my_server_1

* 端口:

1194

* 设备类型:

TUN

* 通道协议:

UDP

- 配置 OpenVPN 接口参数说明如下：
 - 配置：开启/禁用 OpenVPN 连接。
 - 服务器地址：对端 IP 地址或远端 OPENVPN 服务器的域名。
 - 接口名称：服务器的端口。
 - 设备类型：通道设备类型。下拉可选：TUP/TAP
 - 通道协议：通道协议，根据应用需求选择。下拉可选：UDP/TCP
 - 路由策略：当前使用的路由策略。
 - 压缩算法：是否使用压缩算法。下拉可选：不压缩/LZO/LZ4

▼ 高级配置

* 加密方式: BF-CBC

* 认证算法: SHA1

路由策略:

* 压缩算法: LZO

禁止选项一致性检查: ☐

不绑定本地地址和端口: ☒

自定义配置选项:

- 高级配置参数说明如下:

- 加密方式: OpenVPN 传输数据时使用的加密协议, 必须与服务器保持一致。
 - 下拉可选: BF-CBC/RC2-40-CBC/CACT5-CBC/RC2-64-CBC/...
- 认证算法: OpenVPN 传输数据时采用的校验方式, 校验不通过数据传输失败, 必须与服务器一致
 - 下拉可选: SHA1/RSA-MD5/MD5/...
- 禁止选项一致性检查: 不使用选项一致性检查。

- 配置证书管理配页面如下, 你可在此页面上传/更新/删除证书。

配置

接口 证书管理

认证CA证书:

用户/密码:

TA证书:

TLS密钥:

本地证书:

本地私人密钥:

密码:

3.2.5 VXLAN

VXLAN 是一种网络虚拟化技术，可以改进大型云计算在部署时的扩展问题，是对 vlan 的一种扩展。VXLAN 是一种功能强大的工具，可以穿透三层网络对二层进行扩展。它可通过封装流量并将其扩展到第三层网关，以此来解决 VMS（虚拟内存系统）的可移植性限制，使其可以访问在外部 IP 子网上的服务器。

选择“高级功能> VPN 服务>VXLAN”，进入“VXLAN”界面。



点击操作“+”创建 VXLAN 页面。

创建

×

* 名称:

* 对端地址:

* 端口:

4789

* VID:

MTU:

1280

NAT:

☒

* 桥接接口:

lan

取消

确定

- VXLAN 配置参数说明如下：

- 接口名称：该条 VXLAN 规则的名称
- 对端地址：设置对端 IP 地址或域名。
- 端口：连接端口，缺省情况下 4789。
- VID：显示该配置项的 ID 号。
- MTU：设置 VXLAN 最大传输数据单元。
- NAT：是否开启 NAT 地址转换功能。
- 接口类型：配置需要接口类型。

3.2.6 N2N

N2N 旨在提供去中心化、无需管理、安全、稳定的网络连接，而和用户的位置、IP 地址和网络类型无关。通俗地说就是不需要公网 IP、不需要配置 NAT、穿透防火墙。

选择“高级功能> VPN 服务>N2N”，进入“N2N”界面。

The screenshot shows the '配置' (Configuration) window for N2N. It includes a toggle for '启用' (Enable) which is turned on. Below it are input fields for '本机 IP' (Local IP) set to 10.10.10.1, '超级节点 IP' (Super node IP), '超级节点端口' (Super node port), '通讯组' (Communication group), '通讯组密码' (Communication group password), 'MAC' set to 20:28:36:0a:55:40, and 'MTU' set to 1400. At the bottom, there is a checkbox for '添加默认路由' (Add default route) which is also checked.

- **配置 N2N 参数说明如下：**

- 启用：开启/关闭 N2N_v2 连接。
- 本机 IP：设置一个内网 IP 地址。

- 超级节点 IP/端口：连接超级节点的 IP/端口。
- 通讯组：N2N 通讯组织机构的名字。
- 通讯组密码：所在通讯组使用的合法访问密码。
- MAC 地址：N2N 节点的接口物理地址。
- MTU：设置 N2N 最大数据传输单元，默认值为 1500。
- 添加默认路由：添加一条 N2N 接口的默认路由。

3.2.7 EoIP

EoIP（Ethernet over IP）隧道是一个建立在两个网关的 IP 传输层之间的以太网隧道协议。EoIP 接口表现的类似以太网传输，当网关的桥接功能被启用后，所有的以太网数据流量（所有的以太网协议）将被桥接，即同一局域网跨越 IP 层，实现远端二层网络互连。

选择“高级功能> VPN 服务> EoIP”，进入“EoIP”界面。



配置							操作:  
隧道ID	桥接接口	远端地址	本端地址	MTU	启用	操作	
1	br-lan	192.168.0.123	192.168.0.85	1500		 	

第 1-1 条/总共 1 条 < 1 > 10 条/页

- 点击操作“+”创建 EoIP 隧道页面。

创建

* 隧道ID:

* 远端地址:

* 本端地址:

* MTU:

自动 TCPMSS: ☐

* 接口类型:

取消 确定

- 隧道 ID: 设置 EoIP 隧道 ID 号，两端隧道 ID 号必须一致。
- 远端地址: 设置 EoIP 隧道的对端 WAN IP 地址。
- 本端地址: 设置 EoIP 隧道的本端 WAN IP 地址。
- MTU: 设置 EoIP 隧道最大传输单元，默认值为 1500。
- 自动 TCPMSS: 设置最大数据段长度。
- 接口类型: 配置需要桥接的接口类型，默认设置为 br-lan。

3.2.8 MPLS

MPLS (Multi-Protocol Label Switching) 即多协议标记交换，是一种标记 (label) 机制的包交换技术，通过简单的 2 层交换来集成 IP Routing 的控制。当分组进入网络时，要为其分配固定长度的短的标记，并将标记与分组封装在一起，在整个转发过程中，交换节点仅根据标记进行转发。

选择“高级功能> VPN 服务> MPLS”，进入“MPLS”界面。

- 配置参数说明如下：

- 启用：开启/关闭 MPLS 接口。
- 网关 ID：网关 IP 地址。
- 外出接口：设置外出接口，下拉可选：NULL/wan
- DEBUG：是否开启调试日志。
- MPLS 应用接口：添加 MPLS 应用接口。

- 配置 VPLS 参数说明如下：

- 邻居 LSRID：填写邻居 LSRID，需手动填写。

- 对端地址：填写对端 ip 地址，需手动填写。
- 虚链路类型：选择虚链路类型. 下拉可选：ethernet-tagged/ethernet
- 控制字选择：设置控制字. 下拉可选：exclude/include
- 虚链路 ID：设置虚链路 ID，需手动填写。
- 桥接接口：选择需要进行桥接的接口，默认接口 br-lan。
- VID：填写 VID，需手动填写。

3.2.9 Wireguard

选择“高级功能> VPN 服务> Wireguard”，进入“Wireguard”界面。



- 点击操作“+”创建新 Wireguard 页面。

创建

×

* 接口名称:

取消

确定

- 接口名称：填写接口名称。

配置

对端

启用：☒

开机自动运行：☒

* 私钥：

* 公钥：

生成新密钥对

监听端口：

随机

IP地址：

+

MTU：

1420

NAT：

☐

×

添加默认路由：

☐

使用服务器指定DNS：

☐

链路监测：

☐

×

无主机路由：

☐

×

网关跃点：

0

- 配置接口页面参数说明如下：

- 启用：开启/关闭接口。
- 开启自运行：开启/关闭开启自动运行功能。
- 点击生成新密钥对生成公钥私钥。
 - 私钥：需保密。
 - 公钥：可以公开分享。
- 监听端口：设置监听端口。
- IP 地址：设置网络接口 IP 地址。
- MTU：最大传输单元。
- NAT：是否开启 NAT 功能。
- 添加默认路由：是否开启添加默认路由功能。

- 使用服务器指定 DNS：是否开启使用服务器指定 DNS 功能。
- 链路检测：是否开启链路检测功能。
- 无主机路由：是否开启无主机路由功能。
- 网关跃点：设置网关跃点，默认 0。

选择“对端”页面如下

配置		对端								
										操作 
描述	公钥	私钥	预共享密钥	允许IP	对端地址	对端端口	心跳间隔	启用	操作	
										暂无数据

点击操作“+”创建对端页面。

创建

✕

启用：☒

描述：

* 公钥：

私钥：

生成新密钥对

预共享密钥：

生成预共享密钥

允许IP：

+

路由允许的IP：☐

对端地址：

对端端口：

心跳间隔：

- 配置对端页面参数说明如下：
 - 启用：开启/关闭该功能。
 - 描述：填写对端描述信息。
 - 点击生成新密钥对生成公钥私钥。
 - 私钥：需保密。
 - 公钥：可以公开分享。
 - 点击生成预共享密钥生成预共享密钥。
 - 允许 IP：添加允许 IP 地址。
 - 路由允许 IP：是否开启路由允许 IP。
 - 对端地址：填写对端地址。

- 对端端口：填写对端端口。
- 心态间隔：填写心跳间隔时间。