

无线AC控制网关 操作手册

V1.1

2023年4月20日

目录

无线AC控制器.....	1
1. 产品概述.....	4
2. 登录WEB界面.....	4
3. 熟悉WEB页面的各个功能.....	4
3.1. 系统状态.....	4
设备信息.....	5
接口状态.....	6
内网IP流量.....	6
应用流量.....	7
3.2. 网络配置.....	7
接口配置-外网配置.....	8
接口配置-内网/DHCP.....	8
接口配置-物理口划分.....	10
路由规则-多线路分流规则.....	11
路由规则-静态路由.....	12
动态域名.....	12
NAT/端口映射.....	13
3.3. 流控策略.....	14
智能流控.....	14
策略限速.....	14
免流控.....	15
3.4. AC管理.....	15
AP设备列表.....	15
AP配置模板.....	17
AP升级.....	18
无线漫游.....	18
自动信道.....	19
审计配置、定位服务器.....	20
3.5. 认证上网.....	21
认证配置.....	21
PPPoE认证.....	21
Portal认证.....	22
Radius计费.....	23
认证用户.....	23
认证用户状态.....	25
部门/级别定义.....	25
3.6. 行为控制.....	26
应用防火墙.....	26
网址跳转.....	26
域名跳转.....	27
3.7. 对象管理.....	28
基本对象—时间对象.....	28
基本对象—源IP对象.....	28

基本对象—端口对象	29
基本对象—目的IP对象	29
应用对象—内置应用对象	30
应用对象—自定义应用对象	31
3. 8. 安全防护	32
IP-MAC绑定	32
连接数控制	32
内网异常检测	32
内网攻击防护	34
外网禁PING/外网登录	34
3. 9. 日志记录	35
用户认证日志	35
在线人数日志	35
接口流量日志	36
系统日志	36
3. 10. VPN应用	36
PPTP	36
L2TP	38
VTUNS	38
3. 11. 设备维护	40
设备升级	40
密码修改	40
Ping检测	41
配置文件维护	41
重启设备	43
定时任务	43
时间同步	44
云平台配置	44

1. 产品概述

本产品为无线控制AC网关，拥有多线分流，多线叠加负载均衡功能，提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务，具有组网灵活、绿色节能等优势。

2. 登录WEB界面

- 2.1. 网关上电正常开机后，机身上Run状态灯会规律闪烁，网线连接LAN口，保证登录的客户机到网关的网络正常连接。
 - 2.2. 浏览器输入172.16.0.1:2011，默认账号和密码都为admin
- 登陆成功后进入首页



图1 - 首页

3. 熟悉WEB页面的各个功能

3.1. 系统状态

显示网关的一个综合信息，包括各个接口状态、内网客户端的信息和上行下行、各个应用实时上行下行速度和总流量

设备信息



设备信息：显示的是网关的综合信息

序号1：显示接口的物理连接情况，彩色图标代表已连接

序号2：显示接口对应的IP地址

序号3：设备唯一的ID号，可用于远程连接

序号4：当前连接网关的终端数，AP除外。

序号5：显示设备型号

点击在线用户，可根据用户、IP、MAC地址3种类型筛选AP、终端，查看IP和MAC对应。



接口状态

可查看当前各个接口的综合信息。可查看接口详细和WAN口测速



内网IP流量

可查看内网各个终端独立使用的流量信息，还有链路跟踪表。

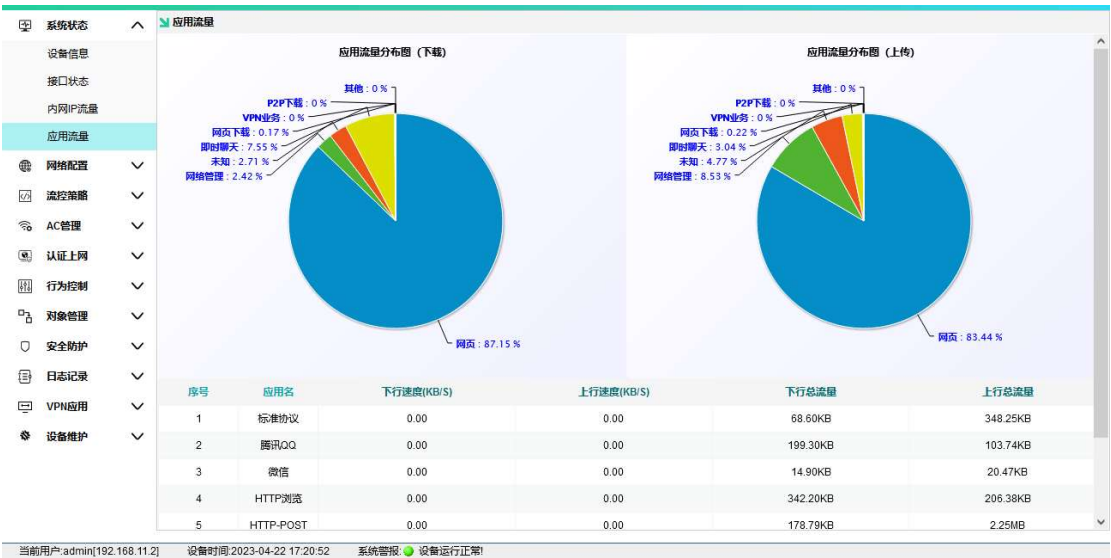


查看该用户的流量类型、速度、协议连接数



应用流量

查看下载和上传各个流量的占比。



3.2. 网络配置

用于设置外网和内网的配置信息，内网的路由

接口配置-外网配置



上网方式——根据实际情况，选择上网方式

- ADSL/PPPOE: 填入宽带账号和密码
- 固定IP: 填入运营商提供的IP、掩码、网关及DNS
- DHCP: 直接插入运营商提供的线路，获取IP

线路中断检测——Ping检测（114DNS, 腾讯官网, 阿里DNS, 百度DNS），如果连续ping不通，高延迟，并且没有数据互通，将视为线路异常。当质量为差的时候，拨号尝试重拨，DHCP 尝试重新获取，固定IP则离线处理。离线的线路，不参与负载。多线路环境，建议启用线路中断检测，个别线路离线了才能自动切换。

备注：成都和重庆专网线路不能勾选（无法进行检测）；个别专线，如果运营商禁ping，也不能启用线路检测。

PING检测IP：默认0.0.0.0，表示使用内置的IP（114DNS, 腾讯官网, 阿里DNS, 百度DNS）进行检测。如当地DNS能ping通，或者有其他延迟更低的公网IP能ping，可填写，作为检测依据。

提示：此项建议由专业的技术人员评估后再填入检测IP。

接口配置-内网/DHCP

序号1：LAN1口地址，默认出厂为LAN1~4为同一个LAN，即用于访问AC的地址。

序号2：IP地址池分配的IP段的配置信息，不能和WAN口获取的IP段相同。

序号3：DHCP静态分配，可管理绑定IP和MAC。

系统状态

网络配置

外网配置

内网/DHCP

物理口划分

多线路分流规则

静态路由

动态域名

NAT/端口映射

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

内网/DHCP

内网DHCP配置

DHCP分配状态

LAN1

LAN1口配置

DHCP配置

基本参数

IP地址池

DHCP静态分配

IP地址: 192.168.11.1

子网掩码: 255.255.255.0

自定义MAC: ☐

内网MAC广播: 禁用

工作模式: 自协商

功能启用: ☒ 已启用 点击禁用

主DNS: 192.168.11.1

备用DNS: 192.168.11.1

地址租期: 3600 秒 默认值 3600

AP的IP分配策略: ☐ 只对AP分配IP ☐ 不对AP分配IP

开始IP: 192.168.11.1

结束IP: 192.168.11.255

添加

删除

☐	序号	MAC地址	IP地址	备注	操作
☐	1	90-ZE-16-FC-F4-2D	192.168.11.2		

保存

当前用户: admin(192.168.11.2)

设备时间: 2023-04-23 09:12:12

系统告警: 设备运行正常

查看DHCP分配状态记录

序号	接口	IP地址	MAC地址	终端名称
1	LAN1	192.168.11.2	90-2E-16-FC-F4-2D	13
2	LAN1	192.168.11.3	1-FC-60	

说明：如AC当旁路由连接时，则勾选“只对AP分配IP”

DHCP配置

功能启用: 已启用, 点击禁用

基本参数

主DNS: 192.168.22.1

备用DNS: 192.168.22.1

地址租期: 3600 秒 默认值: 3600

AP的IP分配策略: ☒ 只对AP分配IP ☐ 不对AP分配IP

接口配置-物理口划分

用于根据需求划分多个WAN口和划分LAN口

序号1：如果需要划分多个局域网，可以取消勾选，则LAN1~4为不同地址

序号2：开启硬件NAT转发，数据转发不经过CPU, 直接转发出去，提高网络速度。

物理口划分

☒ 4LAN + 1WAN

☐ 3LAN + 2WAN

☐ 2LAN + 3WAN

☐ 1LAN + 4WAN

高级

☒ 合并所有LAN口为一个内网口(LAN1)

☒ 启用硬件NAT

保存 注意：物理口功能定义修改后，需要重新配置路由。

路由规则-多线路分流规则



单线路可以不配置分流规则；有2个或以上WAN口接入外网的时候，可选择不同的源地址和分流模式进行设置，模式分成3种：

- 会话分流：把所有上网的连接，分到每条线上。比如张三开迅雷下载，迅雷并发的很多链接，会话分流到三条线路，每个线路均有连接产生流量回来，汇总到迅雷，达到了带宽叠加的效果。
- 源+目的地址分流：在会话分流的基础上，判断源地址和目的地址再负载到每个线路上。比如张三同时的打开了工商银行，京东商城，淘宝三个网站（这里为了讲解说明，视这三个网站的IP只有 A，B，C）。使用源+目的地址分流，分流所有人走三条外网。最终的效果为：张三的工商银行固定走线路1；京东商城固定走线路2，淘宝固定走线路3。
- IP分流：按照源地址始终分流在一个线路上。以3条外网9个人上网的环境为例，IP分流所有人到3条外网上，结果为：张三固定走线路一；李四固定走线路二；王五固定走线路三；赵六固定走线路一，依次将这9个人分摊在3条线上固定走。由于每个人固定在一个线路上，上网的速度，受限于该线路的带宽。

权重：权重可理解为“比例”，只用于IP分流有效。以3条外网12个人上网的环境为例，IP分流所有人分流到3条外网上，线路一权重3、线路二权重2、线路三权重1。结果为，线路一分得6人，线路二分得4人，线路三分得2人。

（权重就是比例，比如三条线路配置权重为 4 ， 2， 1，效果就是 4：2：1）

总结：IP分流适用于线路非常多的条件下，尽量减少WAN口的IP同时被多人开销，提高IP的利用率。多用于做小区宽带里的一些需要做淘宝，亚马逊的电商用户，也多见于一些游戏工作室用到（因为太多人从一个WAN口出去访问，可能会被电商会视为刷单，挂机）。

会话分流适用于需要**非常极致**的分流多线程下载业务，比如分流P2P下载，游戏更新服务器。

源+目的地址分流，是在会话分流的基础上，做到更好的兼容性，默认推荐使用

路由规则-静态路由

一般指定走专网的时候需要在此设置终端访问对应IP段时转发到对应的网关。



查看静态路由表

序号	目的地址	网关	接口	路由类型
1	127.0.0.0/255.0.0.0	--	LAN3	网段本地
2	127.0.0.0/255.0.0.0	--	LAN2	网段本地
3	127.0.0.0/255.0.0.0	--	LAN3	网段本地
4	127.0.0.0/255.0.0.0	--	WAN2	网段本地
5	172.16.0.0/255.255.254.0	--	WAN1	网段本地
6	192.168.11.0/255.255.255.0	--	LAN1	网段本地

动态域名

从外网来管理路由，即通过该动态域名来访问动态域名，主要是由动态域名服务商来提供。



备注：

- 1，路由只是做IP上报，对于解析的正确性，解析的速度，取决于3322的服务商。
- 2，某些运营商，运营商分配上网IP，是分配为一个局域网IP，比如为10. 10. 99. 99，这是个局域网IP，外网是无法访问的。如果是局域网IP，配置了动态域名也是徒劳。

NAT/端口映射

用于把局域网的端口映射到公网

系统状态

网络配置

外网配置

内网/DHCP

物理口划分

多线路分流规则

静态路由

动态域名

NAT/端口映射

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

NAT/端口映射

端口映射

DMZ主机

源地址转换

目的地址转换

添加

删除

序号	协议	内网地址	内网端口	外网端口	外网线路	备注
前还没有定义端口映射规则,请 添加						

端口映射

协议: TCP

内网地址: 192.168.1.100

内网端口范围: 80 ~ 80

外网端口范围: 8080 ~ 8080

外网线路接口选择: ☐ WAN2 ☒ WAN1

备注

确定

取消

例子中是映射的电脑IP是: 192.168.1.100
内部端口是80 外部端口是8080
这是HTTP的映射
这样确定后就能通过外网IP: 8008直接访问电脑的HTTP80端口

DMZ主机

是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，点击开启 DMZ 主机，手动填写地址和外网口确定生效此功能。

系统状态

网络配置

外网配置

内网/DHCP

物理口划分

多线路分流规则

静态路由

动态域名

NAT/端口映射

流控策略

AC管理

NAT/端口映射

端口映射

DMZ主机

源地址转换

目的地址转换

添加

删除

序号	外网线路	主机地址	备注	操作
1	WAN1	192.168.1.2	pc	编辑 删除

DMZ主机

外网线路: WAN1

主机地址: 192.168.1.2

备注: pd

确定

取消

源地址转换

目的地址转换

源地址转换

源地址: 192.168.1.0

掩码: 255.255.255.0

目的地址: 192.168.1.0

掩码: 255.255.255.0

转换地址: 192.168.1.200

备注:

确定 取消

目的地址转换

源地址:

掩码: 255.255.255.0

目的地址:

掩码: 255.255.255.0

转换地址:

备注:

确定 取消

3.3. 流控策略

管理终端的网速，实行平均分配带宽或者限制终端带宽。

智能流控

系统状态

网络配置

流控策略

智能流控

策略限速

免流控

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

智能流控

WAN1

WAN2

一键智能流控

功能启用: ☒ 已启用, 点击禁用

上行带宽: 100000

下行带宽: 100000

KB 512Kbps 1Mbps 2Mbps 4Mbps 5Mbps 6Mbps 10Mbps

KB 4Mbps 5Mbps 10Mbps 20Mbps 50Mbps 100Mbps 200Mbps

为了保证良好的流控效果，外网线路的上行和下行带宽要配置正确

运营商给的线路带宽通常是以比特 (bit/s) 为速率单位: bps，路由转发速率以字节 (BYTE/s) 为速率单位: Bps，注意转换，建议用运营商给的bit速率除以10得到。

比如上行 20M 下行 100M 的拨号光纤，可以配置上行为2000KB，下行 10000KB。配置线路带宽非常重要，智能流控根据所配的带宽自动限速。（需要勾选“启用智能流控”的勾选项，配置带宽的值才生效）

策略限速

根据不同源地址规则来进行限速



免流控

设置不受智能流控整体网速控制的约束，需要单独在策略限速单独限制其最大带宽。

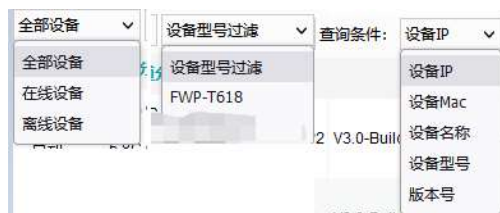


3.4. AC管理

AP设备列表

显示所有连接AC网关上的AP，快速查看和管理。





序号1：查看上线的AP数，绿色代表已经上线的AP，红色是连接过的总AP数。

序号2：筛选只显示在线或离线的AP。

序号3：筛选只显示单型号的AP。

序号4：可选择根据AP设备的IP/MAC/名字/型号/版本号来进行搜索。

序号5：WIFI分析仪，用于扫描该AP的2.4G或5.8G频段下所有信道的WIFI。

序号6：编辑单个AP的参数和配置。

序号7：显示AP的2.4G、5.8G、5.8G2的SSID（无线WIFI名称）和信道。点击绿色小人实现连接该AP的终端。

序号8：AP 服务器登录地址。



点击AP列表右侧  编辑单个AP的配置



主要编辑栏目：

序号1：选择编辑当前频段的参数。

序号2：编辑AP发射的WIFI名字。

序号3：加密方式，一般选择WPA2PSK。

序号4：编辑WIFI密码，点击右侧的钥匙按键可查看密码。

序号5：可选择当前频段不同的协议模式。



次要栏目：

设备名称、设备备注：用于区分该AP所有位置，一般可备注设为安装位置或覆盖位置。

定时重启：设定该AP可根据每天某个整点、或者隔1~10天自动重启。

AP管理密码：该AP的管理页面的登录密码。

无线状态：选择该频段是启用或者关闭状态。

信道：可选择自动信道，AP会自动搜寻最优信道，或者手动选择指定信道。

广播SSID：启动即终端可以搜索出来，关闭则为隐藏SSID。

用户隔离：使该AP下的终端能否互相访问。

发射功率：默认100%，可选择为75%、50%、25%、12%。

AP覆盖阈值：检测终端连接强度弱于阈值则AP选择剔除该终端。

接入用户数：接入该AP的最大终端数。

虚拟无线：每频段最多可创建3个虚拟WIFI，设置不同的SSID和密码。

虚拟无线1		虚拟无线2		虚拟无线3	
状态	关闭	状态	关闭	状态	关闭
SSID	VAP_Wireless1	SSID	VAP_Wireless2	SSID	VAP_Wireless3
安全模式	OPEN	安全模式	OPEN	安全模式	OPEN
广播SSID	启用	广播SSID	启用	广播SSID	启用
VLANID	0 (0,2~4095)	VLANID	0 (0,2~4095)	VLANID	0 (0,2~4095)
密钥		密钥		密钥	

确定 取消

AP配置模板

选择型号添加模板，一个型号对应一个模板。配置好SSID和密码，然后在AP里面里全选同一个型号的AP选择应用配置对应模板。



AP升级

可选择在线升级，或者上传固件进行本地升级。



无线漫游

默认打开自动漫游功能。



信号表：可查看已经连接AP的无线终端的分配信息

系统状态

网络配置

流控策略

AC管理

AP设备列表

AP配置模板

AP升级

无线漫游

自动信道

审计配置

定位服务器

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

无线漫游

参数配置

信号表

终端MAC

AP_MAC

AP_IP

AP名称

信号强度

级别

无线类型

接入AP

接入时间

FML-2G-4A-1E-99-86-F8-2D

5-94

172.16.100.4

My WTP 1

-84dBm

--

2G

--

2023-04-23 10:39:43

51-78

172.16.100.28

My WTP 1

-81dBm

--

2G

--

2023-04-23 10:59:50

60-E4

172.16.100.3

My WTP 1

-80dBm

--

2G

--

2023-04-23 10:59:51

55-74

172.16.100.34

My WTP 1

-72dBm

良

2G

接入

2023-04-23 10:59:49

FML-2G-7C-A1-77-DC-15-27

5-74

172.16.100.34

My WTP 1

-75dBm

--

2G

接入

2023-04-23 10:57:54

5-B0

172.16.100.6

My WTP 1

-66dBm

良

2G

--

2023-04-23 10:59:54

0-14

172.16.100.9

My WTP 1

-60dBm

良

2G

接入

2023-04-23 10:59:54

FML-2G-C2-7E-7E-A1-3E-D3

55-94

172.16.100.4

My WTP 1

-71dBm

--

2G

--

2023-04-23 10:49:47

4F-F0

172.16.100.33

My WTP 1

-81dBm

--

2G

--

2023-04-23 10:31:59

55-B0

172.16.100.6

My WTP 1

-47dBm

优

2G

接入

2023-04-23 10:21:10

0-14

172.16.100.9

My WTP 1

-57dBm

良

2G

--

2023-04-23 10:21:10

FML-2G-F8-9E-4A-A5-63-56

1F-F0

172.16.100.33

My WTP 1

-69dBm

良

2G

--

2023-04-23 10:21:12

60-E4

172.16.100.3

My WTP 1

-79dBm

--

2G

--

2023-04-23 10:21:12

上一页

1

下一页

跳转到

页

确定

当前用户:admin[2.2.2.2]

设备时间:2023-04-23 11:01:50

系统警报: 设备运行正常!

自动信道

配置重新定时重新信道配合的时间

系统状态	网络配置	自动信道	参数配置		KVR参数配置		信道表	
			审计参数					
			自动信道分配: 已启用, 点击禁用					
			密集部署无线信道可分配时, 请开启此功能					
			密集部署智能网优: ☐					
			定时对AP进行信道重新分配					
			定时重分配: ☒ 周日 ☒ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六					
			开始时间: 04:00 时间格式: 24小时制 (HH:mm), 如 13:10					
			保存					
			当前用户:admin[192.168.11.4] 设备时间:2023-04-23 11:03:29 系统警报: 设备运行正常!					

KVR切换阈值配置

系统状态	网络配置	自动信道	参数配置		KVR参数配置		信道表	
			KVR参数					
			2G切换阈值: -85					
			5G切换阈值: -65					
			开启漫游: ☒					
			开启5G优先: ☒					
			保存					
			当前用户:admin[192.168.11.4] 设备时间:2023-04-23 11:03:29 系统警报: 设备运行正常!					

信道表，查看每个AP的其他WIFI的信道和信号强度。

系统状态

网络配置

流控策略

AC管理

AP设备列表

AP配置模板

AP升级

无线漫游

自动信道

审计配置

定位服务器

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

自动信道

信道表

AP地址

搜索

一键网优

最新数据

AP_MAC	无线类型	自动信道	周围AP_MAC	AP名称	信道	信号强度
192.168.11.3 My WTP 1	2G	4 已分配	3C-C5	--	2	强(-39dBm)
			51-6A	--	6	中(-49dBm)
			4-00	--	6	中(-55dBm)
			E-65	--	7	中(-54dBm)
			1-56	--	9	中(-50dBm)
			7-52	--	9	强(-38dBm)
			3-A0	--	10	中(-54dBm)
			3-D0	--	13	强(-36dBm)
			52	--	36	中(-50dBm)
			6A	--	40	强(-43dBm)
5G	64 已分配	66	--	149	中(-55dBm)	
		3C-C6	--	153	中(-61dBm)	
		3C-C6	--	157	中(-46dBm)	

上一页

1

下一页

跳转到

页

确定

当前用户: admin(192.168.11.1)

设备时间: 2023-04-23 11:06:27

系统语言: 设备运行正常

审计配置、定位服务器

用于定制开发对接审计系统

审计配置

审计参数

安全厂家编码:

数据采集地编码:

数据发送地编码:

FTP IP: 0.0.0.0

FTP PORT: 0

FTP 用户名:

FTP 密码:

保存

序号	设备名称	MAC	设备场所编码	场所名称备注	操作
1	AA				

定位服务器

功能启用: ☒ 已启用, 点击禁用

IP地址:

端口:

3.5. 认证上网

通常情况下，上网用户，通过配置网卡的IP地址，或者通过路由DHCP分配地址，得到IP，即可直接上网

认证上网，意思是需要有“用户”的身份，才允许上网。

认证配置

控制对应LAN口的认证开关。

注意：只要开启其中任意一个开关，即表示对LAN2的口，进行拦截。必须通过认证的用户，才允许上网



PPPoE认证

PPPoE认证——用于小区宽带，内网用户通过PPPoE拨号上网。拨号的帐号密码在路由上创建（对接radius计费的，需radius计费系统上创建）。

地址池的分配，建议用局域网地址，且不能和LAN口的IP 同网段。比如LAN口的IP 是192.168.1.1。此处地址池不能为192.168.1.xxx

DNS建议分配当地运营商的DNS。

系统状态

网络配置

流控策略

AC管理

认证上网

认证配置

PPPoE认证

Portal认证

Radius计费

认证用户

认证用户状态

部门级别定义

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

PPPoE服务

PPPoE高级选项

接入状态

所有内网口

LAN1

功能启用: 已启用, 点击禁用

服务名称:

分配IP地址范围

网关IP: 10.1.0.1

开始地址: 10.1.0.2

结束地址: 10.1.200.254

根据MAC地址分配IP:

请在右边的文本框输入IP与MAC的分配规则, 格式为IP地址 空格 MAC地址 每行一个
例如:
10.10.1.2 AA:BB:CC:DD:EE:FF
10.10.1.3 BB:CC:DD:EE:FF:00
10.10.1.4 DD:EE:FF:00:11:22

DNS配置

主DNS: 114.114.114.114

辅DNS: 8.8.8.8

检测在线间隔: 5分钟

MTU: ☐ 启用自定义MTU

MRU: ☐ 启用自定义MRU

提示: 1. 修改PPPoE拨号配置之后, 已经拨号上的用户会断开网络, 需要重新拨号;
2. PPPoE的拨号用户, 统一在《用户管理》认证用户

保存

系统状态

网络配置

流控策略

AC管理

认证上网

认证配置

PPPoE认证

Portal认证

Radius计费

认证用户

认证用户状态

部门级别定义

行为控制

PPPoE服务

PPPoE高级选项

接入状态

隔离内网拨号用户: 已禁用, 点击启用

过期用户不能拨号: 已启用, 点击禁用

禁止相同MAC地址拨号: 已禁用, 点击启用

免密码认证: 已禁用, 点击启用

根据“部门级别”分配DNS(为实现对不同用户分配不同的DNS, 当用户所属的“部门级别”在这里配置了DNS, PPPoE服务将直接采用这里配置的DNS单独给用户进行DNS分配)

添加 删除

规则由上而下执行, 所以越靠上越优先得到DNS分配。可以通过上下移动 箭头调整顺序 置顶 置底

序号	类型	名称	主DNS	辅DNS	操作
当前还没有添加PPPoE高级配置, 请 添加					

Portal认证

系统状态

网络配置

流控策略

AC管理

认证上网

认证配置

PPPoE认证

Portal认证

Radius计费

认证用户

认证用户状态

部门级别定义

行为控制

Portal认证配置

认证选项

认证页面定制

Portal认证用户超时时间: 30 分钟

认证选项

一键认证: ☐ 启用 ☒ 禁用

WEB密码认证: ☒ 启用 ☐ 禁用

手机短信密码认证: ☐ 启用 ☒ 禁用

认证成功跳转网址:

认证失败跳转网址:

保存

一键认证: 用于酒店, 宾馆防止有针孔摄像头链接WIFI联网。需要多一个人工点击步骤。相当于自助点击放行使用。

WEB密码认证: 连上路由的用户（比如手机），通过弹出的认证窗口，输入用户名密码上网。WEB密码的帐号密码在路由上创建（对接radius计费的，需radius计费系统上创建）

短信认证（付费功能）: 通过输入手机号码，短信平台发送随机密码认证上网。

认证页面定制：可自定义上传图片素材



Radius计费



认证用户

下图添加的为四种类型的用户。

系统状态	认证用户	共有用户 5							
网络配置	添加	批量添加	全部应用	导出用户	删除	用户部门过滤	用户级别过滤	用户类型过滤	状态
策略策略	精确	查找							
AC管理	序号	名称	部门	用户级别	用户类型	备注	创建时间	到期时间	操作
认证上网	1	vpn	default	default	VPN拨号		2023-05-17 13:35	无限制	 
认证配置	2	web	default	default	WEB密码认证		2023-05-17 13:35	无限制	  
PPPoE认证	3	mac101	default	default	MAC地址认证		2023-05-17 13:35	无限制	 
Portal认证	4	ip101	default	default	IP地址认证		2023-05-17 13:34	无限制	 
Radius计费	5	pppoe	default	default	PPPoE拨号		1970-01-01 08:06	无限制	  
认证用户									
认证用户状态									
部门级别定义									

用户对象

账号: 李四

MAC地址: 00-7E-12-2A-10-33

部门: 默认部门

级别: 默认级别

用户类型: MAC地址认证

账号状态: 启用

创建时间: 2018-03-14 10:20

过期时间: 无限制

姓名:

联系电话:

备注:

+

用户对象

账号: 张三

IP地址: 192.168.0.214

部门: 默认部门

级别: 默认级别

用户类型: IP地址认证

账号状态: 启用

创建时间: 2018-03-14 10:19

过期时间: 无限制

姓名:

联系电话:

备注:

+

用户对象

账号: bytevalue

密码: 88888888

部门: 默认部门

级别: 默认级别

用户类型: WEB密码认证

账号状态: 启用

创建时间: 2018-03-14 10:19

过期时间: 无限制

姓名:

联系电话:

备注:

+

用户对象

账号: sz075588888888

密码: 8888888

部门: 默认部门

级别: 默认级别

用户类型: PPPoE拨号

账号状态: 启用

创建时间: 2018-03-14 10:19

过期时间: 无限制

姓名:

身份证号:

联系电话:

地址:

备注:

确定

取消

认证用户状态

可看到用户上线，图中的绿色的图标代表已上线的用户。

系统状态

网络配置

流控策略

AC管理

认证上网

认证配置

PPPoE认证

Portal认证

Radius计费

认证用户

认证用户状态

部门级别定义

认证用户状态

匿名用户 ☐ 在线

总用户数:1/5

▼ default [1/5]

ip101

mac101

pppoe

vpn

web

用户级别过滤

用户类型过滤

到期时间过滤

状态

账号

查找

序号	用户	级别	电话	地址/备注	到期时间	IP	在线状态	认证状态
1	ip101	default			无限制	--	未上线	-
2	mac101	default			无限制	192.168.22.2	在线8秒	-
3	0000a	default			无限制	--	未上线	-
4	yn	default			无限制	--	未上线	-
5	web	default			无限制	--	未上线	-

部门/级别定义

部门划分 管理部门和级别，用于绑定上网用户所属

部门划分用途：用户对象必须选择所属的部门，所以，在定义用户前需要划分部门，对公司而言通常根据行政部门来划分部门，例如：销售部、生产部等;对小区而言通常根据接入用户的地点来划分部门，例如：东35栋，西88栋。划分了部门后，用户可以根据划分的部门做各种控制规则

系统状态

网络配置

流控策略

AC管理

认证上网

认证配置

PPPoE认证

Portal认证

Radius计费

认证用户

认证用户状态

部门级别定义

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

部门划分

级别划分

部门划分用途：用户对象必须选择所属的部门，所以，在定义用户前需要划分部门，对公司而言通常根据行政部门来划分部门，例如：销售部、生产部等;对小区而言通常根据接入用户的地点来划分部门，例如：东35栋，西88栋。划分了部门后，用户可以根据划分的部门做各种控制规则；

添加

序号	部门名称	操作
1	default	

| 2 | 销售部 | |

| 3 | 客服部 | |

级别划分用途：用户对象必须选择所属的级别，所以，在定义用户前需要划分级别；对公司而言通常根据用户的权限和职位划分级别，例如：高级主管、普通员工等。对小区而言通常根据用户购买的带宽来划分级别，例如：2M，4M。划分级别后，可以根据划分的级别做各种控制或者限速规则；



3.6. 行为控制

应用防火墙

根据源和时间配置需要的放行和直接阻止的目的IP、端口、应用。



网址跳转

设置当终端访问原网址，自动跳转到目的网址。（清理浏览器缓存后生效）



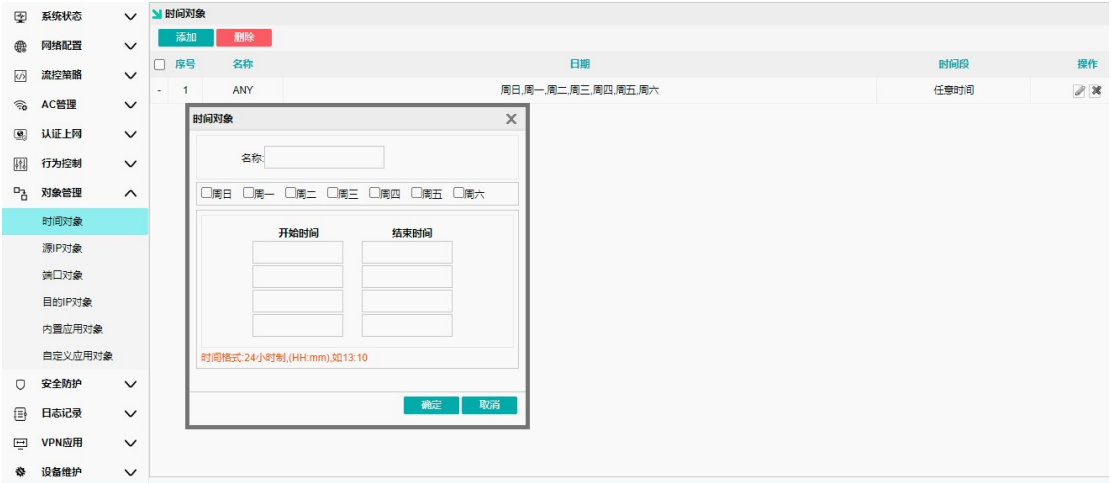
域名跳转

设置当终端访问域名，自动解析到指定IP（清理浏览器缓存后生效）

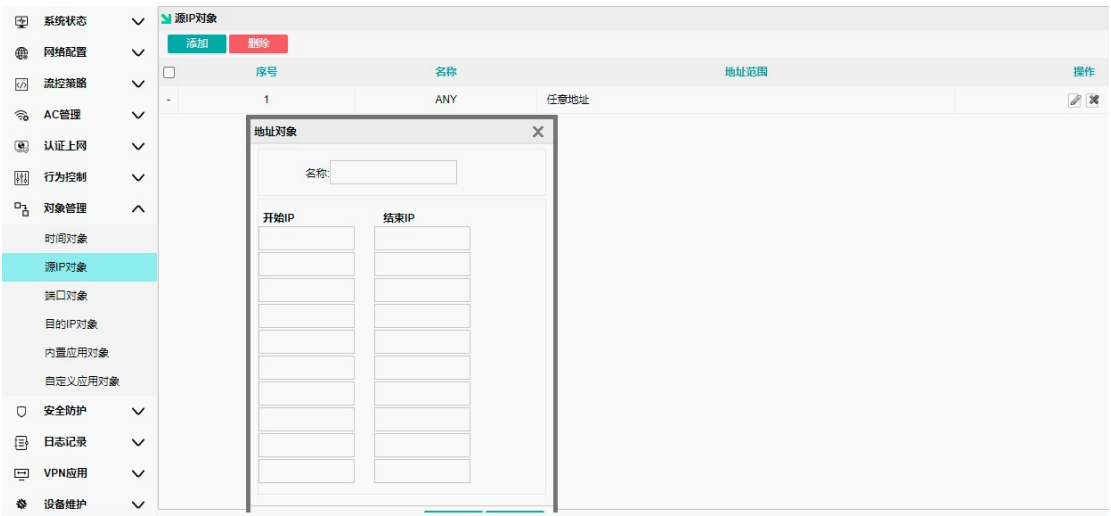


3.7. 对象管理

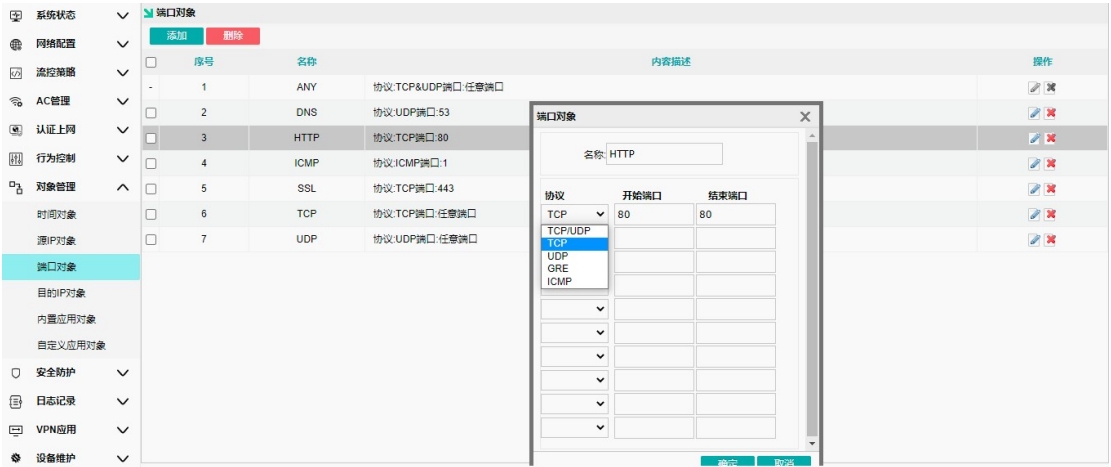
基本对象--时间对象



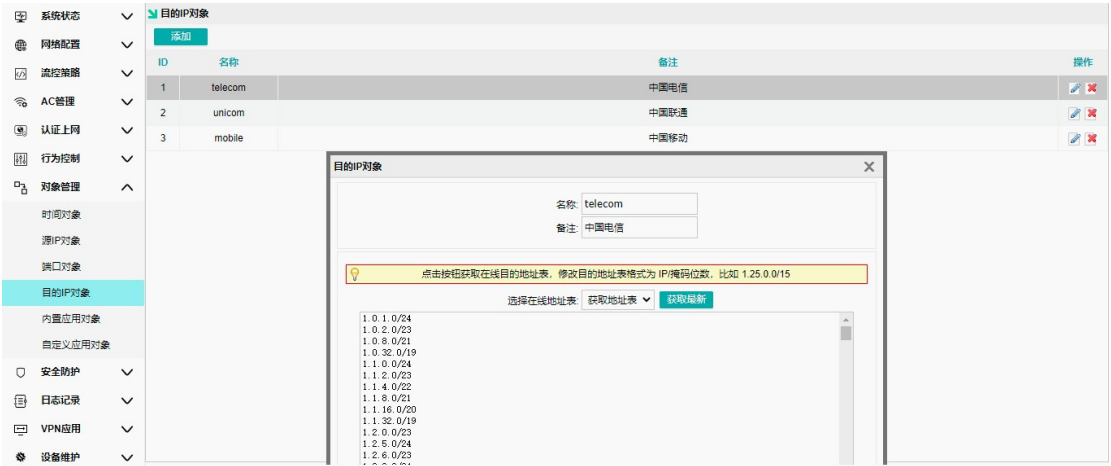
基本对象--源IP对象



基本对象--端口对象



基本对象--目的IP对象



应用对象--内置应用对象

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

时间对象

源IP对象

端口对象

目的IP对象

内置应用对象

自定义应用对象

安全防护

日志记录

VPN应用

设备维护

内置应用对象

内置应用对象升级

内置应用对象

内置应用对象库

当前内置应用对象库版本V1-20230515已经是最新!

设置自动更新

自动更新内置应用对象库: 已启用自动更新

系统状态	内置应用对象	内置应用对象升级	内置应用对象
网络配置	应用名称	查找	
流控策略	其他分类	序号	应用名称
AC管理	网络游戏	应用分类	描述
认证上网	网络游戏	1	11平台刀塔
行为控制	游戏加速器	2	175平台
对象管理	网络管理	3	300英雄
时间对象	远程管理	4	360测速
源IP对象	电子邮件	5	360安全卫士
端口对象	文件传输	6	起凡三国争霸
目的IP对象	即时聊天	7	三国争霸2
内置应用对象	网页	8	六间房
自定义应用对象	网页视频	9	起凡游戏
安全防护	网页下载	10	AcFun
日志记录	云服务	11	永恒之塔
VPN应用	VPN业务	12	阿里云CDN
设备维护	宽带测速		
	影音P2P加速		
	P2P下载		
	苹果传输服务		
	无盘更新		

应用对象--自定义应用对象

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

时间对象

源IP对象

端口对象

目的IP对象

内置应用对象

自定义应用对象

安全防护

日志记录

VPN应用

设备维护

自定义应用对象

根据域名定义应用

根据目的IP+端口定义应用

添加

序号	应用名称	应用分类	描述	操作
☐	1	11平台刀塔	网络游戏	
☐	2	175平台	网络游戏	
☐	3	300英雄	网络游戏	
☐	4	360测速	宽带测速	
☐	5	360安全卫士	软件更新	
☐	6	超凡三国争霸	网络游戏	
☐	7	三国争霸2	网络游戏	
☐	8	六间房	网页视频	
☐	9	超凡游戏	网络游戏	
☐	10	AcFun	网页视频	
☐	11	永恒之塔	网络游戏	
☐	12	阿里云CDN	网页下载	

根据域名定义应用

自定义应用对象

自定义应用对象

根据域名定义应用

根据目的IP+端口定义应用

添加

域名

根据域名定义应用

域名:

应用名称: weixin

确定 取消

当前还没有数据

根据目的IP+端口定义应用

自定义应用对象

自定义应用对象

根据域名定义应用

根据目的IP+端口定义应用

添加

序号

应用名称

根据目的IP+端口定义应用

开始地址:

结束地址:

协议: TCP/UDP

开始端口:

结束端口:

应用名称: weixin

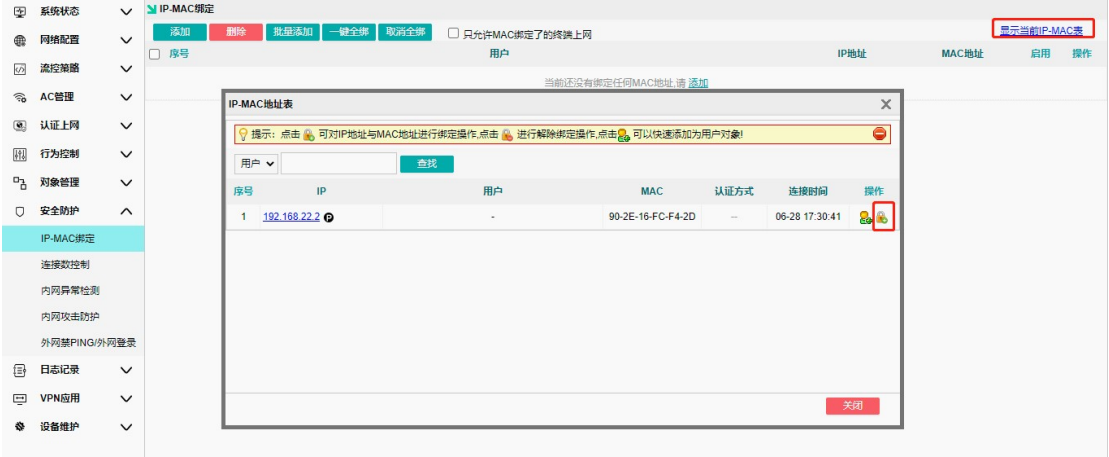
确定 取消

当前还没有数据

3.8. 安全防护

IP-MAC绑定

将IP-MAC绑定之后，由于不能够随意修改IP，所以能够避免IP冲突而影响到其他用户正常上网的情况。



连接数控制

限制源对象的TCP、UDP的最大连接数



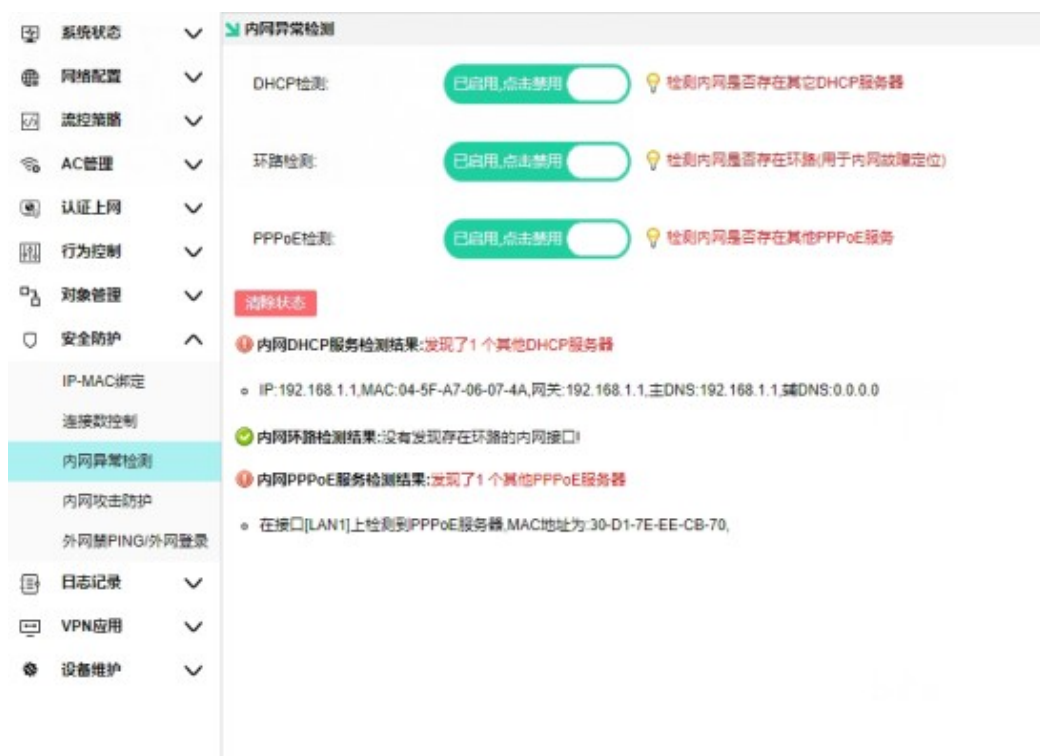
内网异常检测

开启DHCP检测可以搜索是否局域网内有其他DHCP服务器导致IP地址分配冲突。
AC网关作为旁路由的时候会搜到主路由为正常现象。
开启环路检测可以判断局域网的交换机是否存在链路回环，导致网络广播风暴从而上网质量很慢很不稳定。



常见例子:

LAN口中存在私接第三方路由, 并不小心接到路由器的LAN口, 产生DHCP冲突



内网攻击防护

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

IP-MAC绑定

连接数控制

内网异常检测

内网攻击防护

外网禁PING/外网登录

日志记录

VPN应用

设备维护

内网攻击防护

功能启用: 已启用,点击禁用

选择要防护的接口

☒ LAN1

参数设置

包阈值: 7000 (包数/每秒)

包阈值: 允许单IP每秒发送的最大包数, 参考值在5000~10000之间

☐ 内网口是否对接三层交换机 如果没有对接三层交换机请不要勾选

保存

外网禁PING/外网登录

可查看远程登录的参数和配置

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

IP-MAC绑定

连接数控制

内网异常检测

内网攻击防护

外网禁PING/外网登录

日志记录

VPN应用

设备维护

外网禁PING/外网登录

主机安全

☐ 禁止外网Ping路由

☒ 允许管理员通过外网IP远程登录

WEB服务端口: 80

主机DNS: 114.114.114.114 指本机(路由器)作为一个上网终端需要的DNS服务器地址

更新线路选择: 默认 指定设备系统升级和协议更新线路!

远程管理服务器:

设备备注:

☐ 在登录页显示

保存

3.9. 日志记录

用户认证日志

查看设备上线和下线情况

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

用户认证日志

在线人数日志

接口流量日志

系统日志

VPN应用

设备维护

用户认证日志记录

序号	时间	描述
1	2022-08-22 17:49:21	10.2.0.4 90-2E-16-FC-F4-2D 507 的用户上线
2	2022-08-22 17:48:41	507 的用户离线
3	2022-08-22 17:45:54	10.2.0.3 90-2E-16-FC-F4-2D 507 的用户上线

查找 首页 上一页 下一页 尾页 转到第 GO 共1页,当前第1页

在线人数日志

把终端添加为用户对象进行记录

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

用户认证日志

在线人数日志

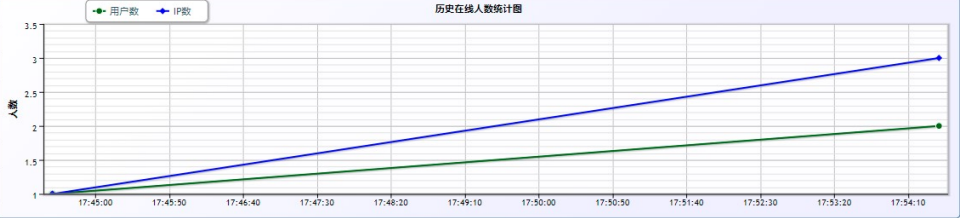
接口流量日志

系统日志

VPN应用

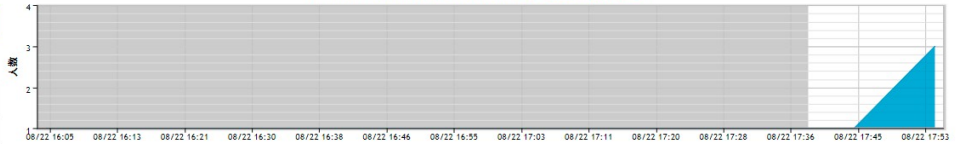
设备维护

历史在线人数统计图



时间段: 2022-08-15 ~ 2022-08-22 查询 今天 昨天 前天 近两天 近三天 近一周

2022-08-15 ~ 2022-08-22 历史在线人数总览图 (用鼠标选取区域可查看详情)



接口流量日志



系统日志

系统状态

网络配置

流量策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

用户认证日志

在线人数日志

接口流量日志

系统日志

VPN应用

设备维护

系统日志记录

序号

时间

描述

12023-06-28 17:30:16接口:WAN1上线,获得IP地址是:172.16.0.156

查找 首页 上一页 下一页 尾页 转到第GO 共1页,当前第1页

3. 10. VPN应用

PPTP

使用此功能需要AC作为一级主路由，WAN口接外网为运营商提供的公网IP。

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

PPTP

L2TP

VTUNS配置

VTUNS状态

设备维护

PPTP

PPTP VPN服务器

PPTP VPN接入状态

功能启用 已启用,点击禁用

客户端IP地址范围

网关IP 192.168.11.1

开始地址 192.168.11.100

结束地址 192.168.11.200

DNS配置

主DNS: 223.5.5.5

辅DNS: 114.114.114.114

检测在线间隔: 3分钟

MTU: ☐ 启用自定义MTU

MRU: ☐ 启用自定义MRU

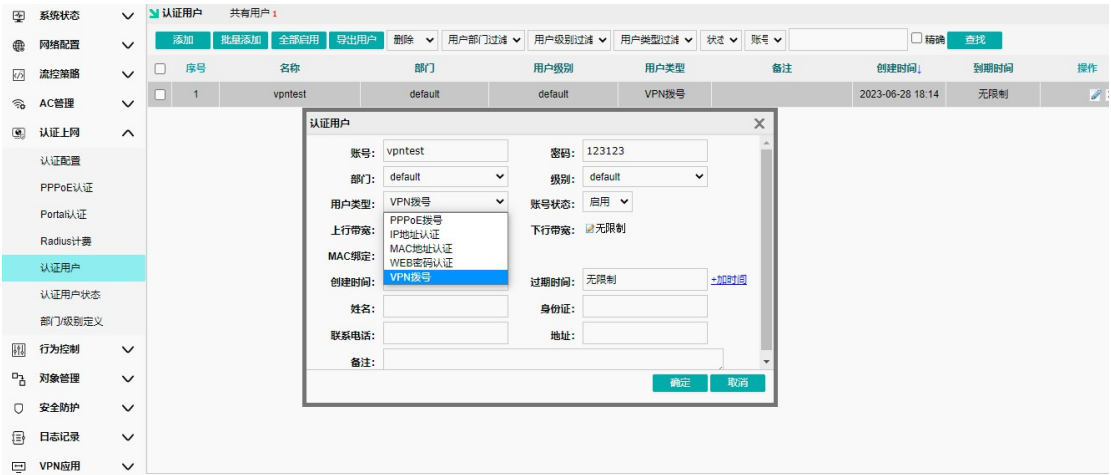
MPPE-128: ☐ 支持MPPE-128

提示: 点对点VPN的拨号用户, 统一在认证上网, 用户管理 > [认证用户](#)

保存

网关IP、地址池根据、DNS实际需要进行设置。

点击认证用户跳转到创建VPN认证用户



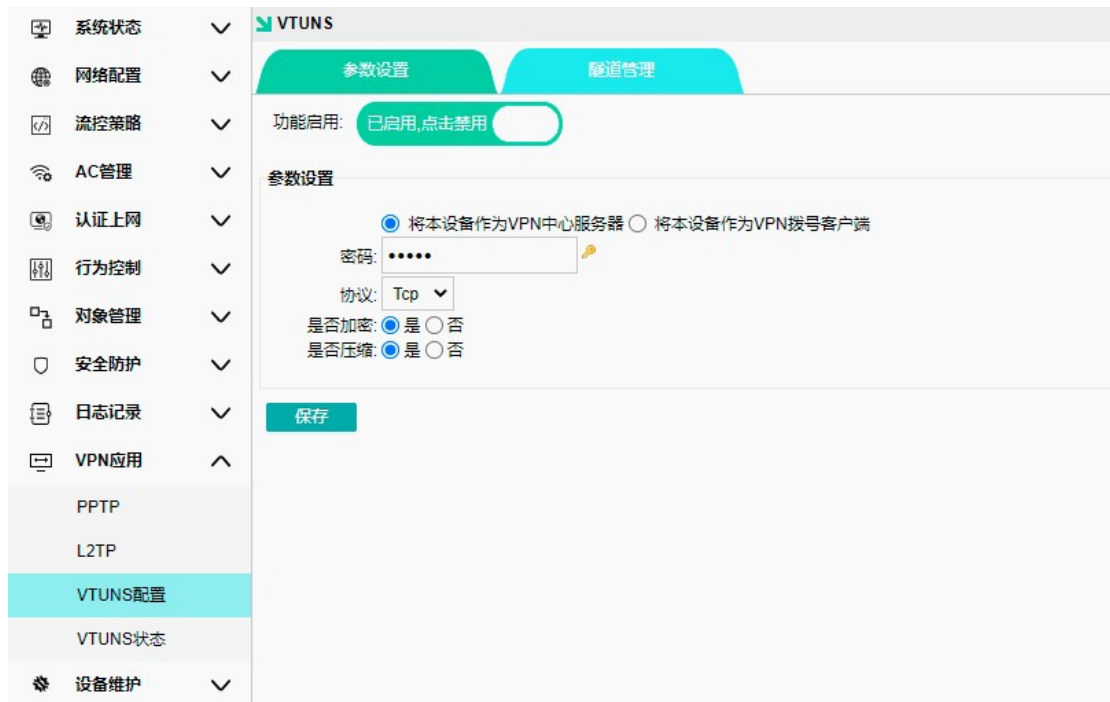
L2TP

使用此功能需要AC作为一级主路由，WAN口接外网为运营商提供的公网IP。
网关IP、地址池根据、DNS实际需要进行设置。

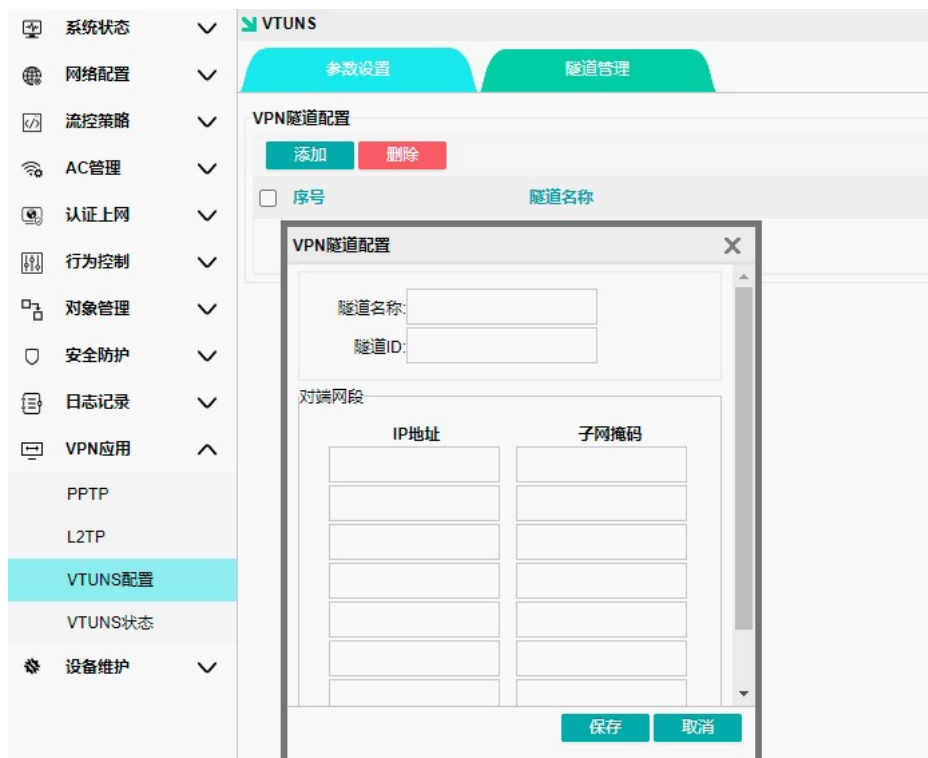


VTUNS

网对网建立 TCP/IP 上的虚拟通道, 用于两个局域网合并, 性能较好的一方设为服务器, 两边局域网的网段不能一样, 服务端需要有公网IP。



隧道管理，添加自定义隧道名称和隧道ID，填入VPN客户端的内网网段，比如填写 192.168.1.0，掩码 255.255.255.0 注意，隧道名称和隧道ID必须服务端和客户端，配置一致



3. 11. 设备维护

设备升级

在线升级、或选择特定固件升级

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

设备升级

密码修改

Ping检测

配置文件维护

重启设备

定时任务

设备升级

通过上传升级包的方式升级

文件路径:

选择文件

 未选择任何文件

开始升级

在线升级

您当前的版本已经是最新版,不需要升级!

密码修改

系统状态

网络配置

流控策略

AC管理

认证上网

行为控制

对象管理

安全防护

日志记录

VPN应用

设备维护

设备升级

密码修改

Ping检测

配置文件维护

重启设备

定时任务

密码修改

修改系统的密码, 请记住修改过的密码, 默认密码为: admin

旧密码:

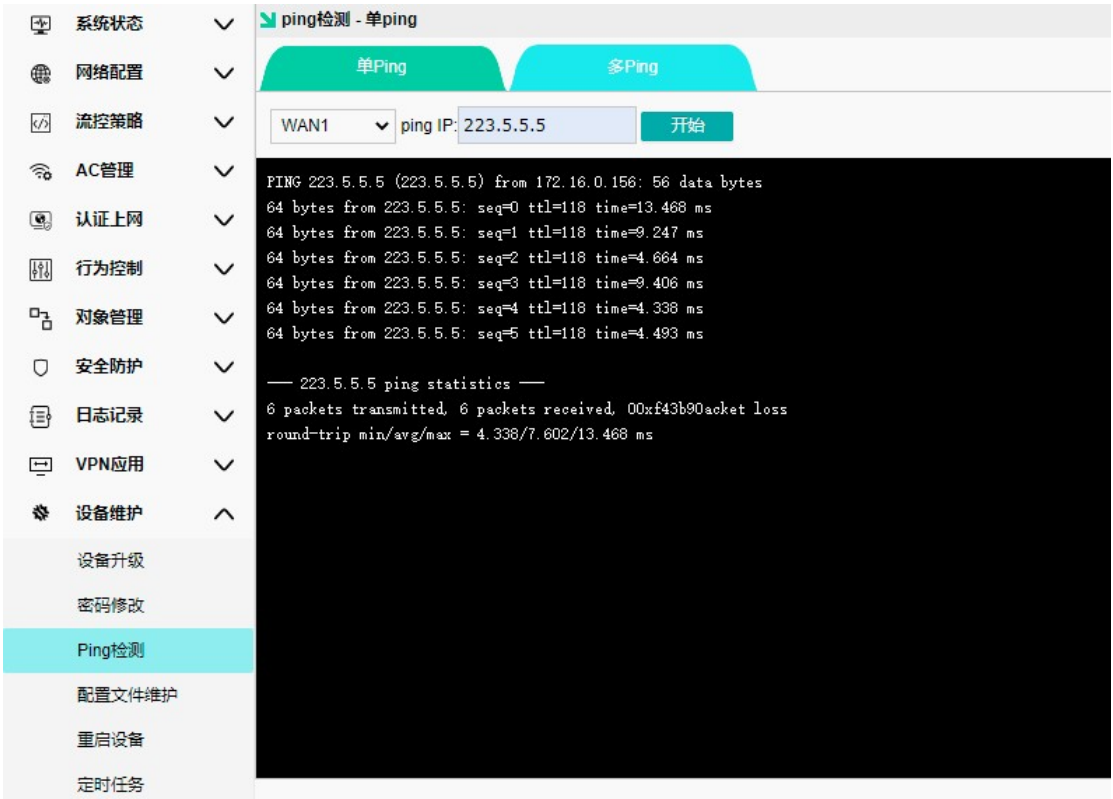
新密码:

确认密码:

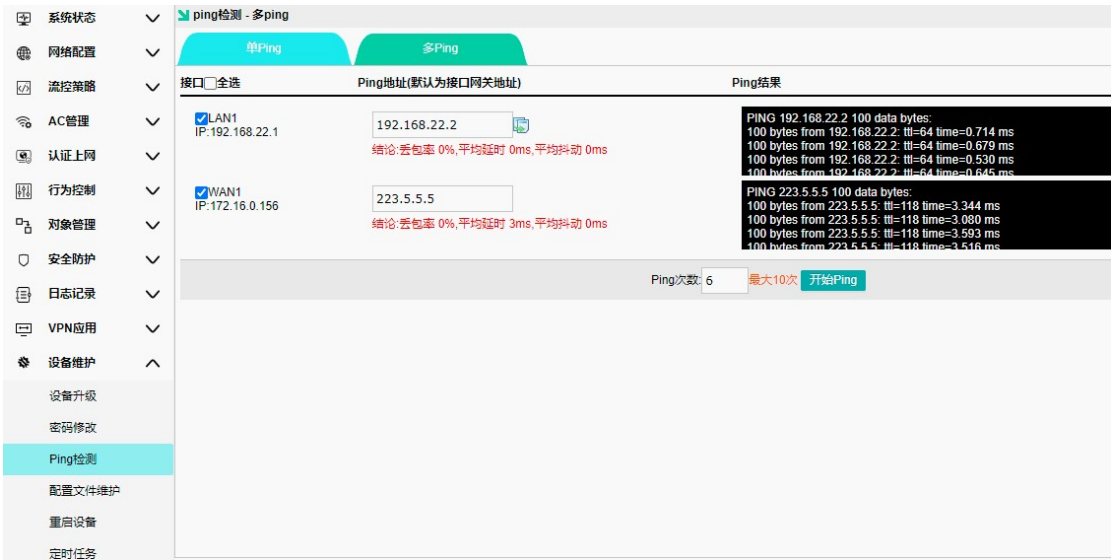
修改密码

Ping检测

用检查AC和指定IP之间是否通路。



多Ping



配置文件维护

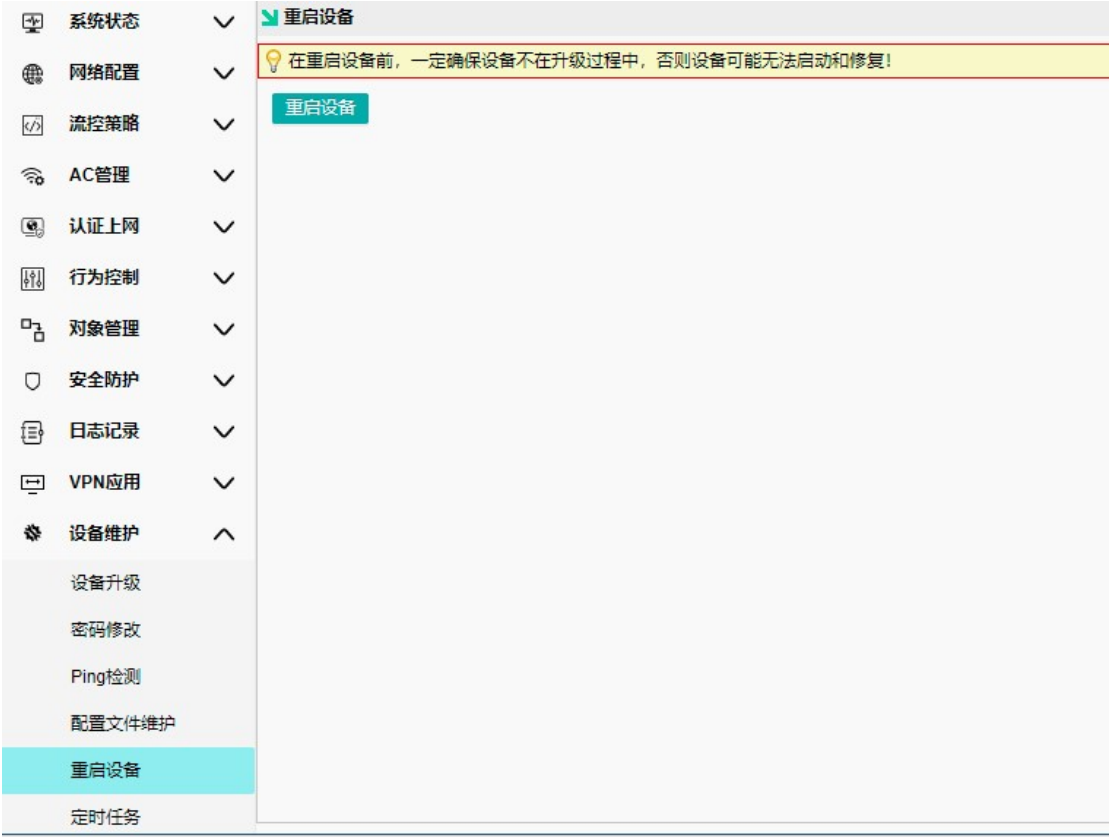
用于把网关的配置信息导出和导入，恢复出厂



邮件备份：填入发信、收信邮箱的参数，定时收取备份文件



重启设备



定时任务

设置网关的定时操作



时间同步

可选择不同的时区和主时间服务器

The screenshot shows the '时间同步' (Time Synchronization) configuration page. On the left is a sidebar menu with options: 流控策略, AC管理, 认证上网, 行为控制, 对象管理, 安全防护, 日志记录, VPN应用, 设备维护, 设备升级, 密码修改, Ping检测, 配置文件维护, 重启设备, 定时任务, 时间同步 (highlighted), and 云平台配置. The main content area has a title bar '时间同步' and a yellow warning box: '配置正确的网络时间服务器域名或IP,设备会定时(30分钟)和这个服务器同步时间'. Below this, there are three input fields: '时区:' with a dropdown menu showing '(GMT+08:00) 北京,重庆,香港,乌鲁木齐,台北', '主时间服务器:' with the text 'ntp.api.bz', and '备用时间服务器:' with the text 'time.windows.com'. A green '保存配置' (Save Configuration) button is located at the bottom left of the main content area.

云平台配置

AC绑定在云平台上，远程管理AC和AP。

填写云平台地址，在云平台上注册账号，登录云平台后填入AC的LAN口MAC地址进行绑定。

The screenshot shows the '云平台配置' (Cloud Platform Configuration) page. The left sidebar menu is identical to the previous page, with '云平台配置' (highlighted) at the bottom. The main content area has a title bar '云平台配置'. It features a '功能启用:' (Function Enabled) section with a green toggle switch labeled '已启用, 点击禁用'. Below this is a '云平台服务器地址:' (Cloud Platform Server Address) input field followed by a green '去注册' (Go Register) button. A green '保存配置' (Save Configuration) button is located at the bottom left of the main content area.