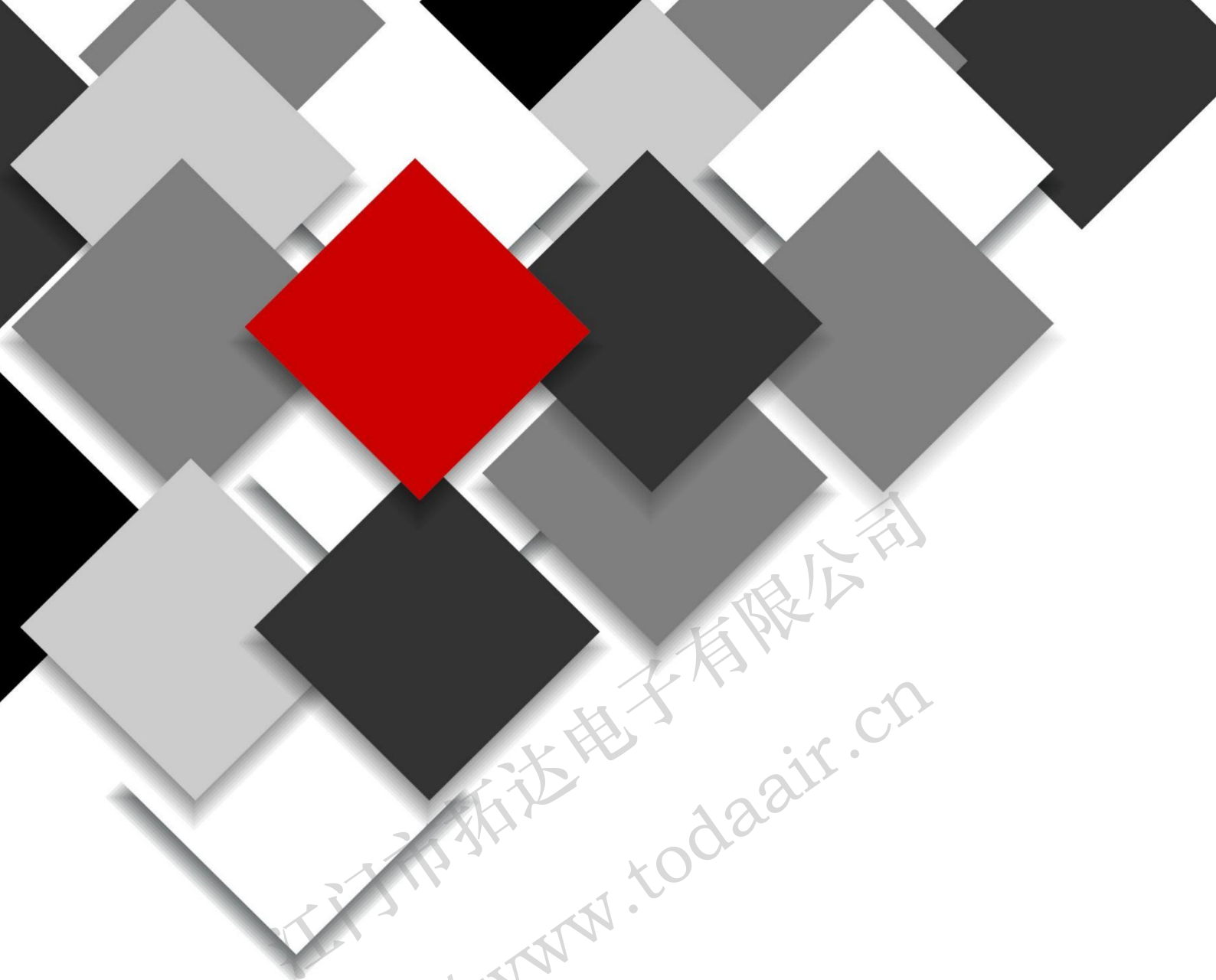




江门市拓达电子有限公司
<http://www.todaair.cn>

拓达网关使用说明书

更新时间：2019 年 11 月 03 日

拓达电子保留所有最终解释权，若有更新，恕不另行通知



TODAIR 拓达



目录

1	配置准备	- 1 -
1.1	网络设置	- 1 -
2	语言选择	- 1 -
3	系统概况	- 2 -
3.1	首页	- 2 -
3.2	网络状态	- 2 -
3.3	网络监控	- 2 -
4	网络配置	- 3 -
4.1	内外网配置	- 3 -
4.2	内网接口设置:	- 3 -
4.3	高级配置	- 4 -
4.4	DHCPv4 配置	- 4 -
4.5	DHCPv6 配置	- 4 -
4.6	聚合接口设置:	- 5 -
4.7	外网接口(WAN)设置:	- 5 -
4.7.1	DHCP 上网模式设置 (自动获取上级路由下发的 IP)	- 5 -
4.7.2	DHCPV6 配置方式与 DHCP 方式相同, DNS 可以填写 IPV6 DNS。 ..	- 6 -
4.7.3	静态 IP 上网模式设置(Static IP)	- 6 -
4.7.4	PPPoE 拨号上网模式设置	- 7 -
4.8	DHCP 服务配置	- 7 -
4.8.1	DHCP 服务信息	- 7 -
4.8.2	DHCPv6 配置	- 8 -
4.9	内网 VLAN	- 9 -
4.9.1	高级配置	- 9 -
4.9.2	DHCPv4 配置	- 9 -
4.9.3	DHCPv6 配置	- 9 -
4.10	VPN 客户端	- 10 -
4.10.1	PPTP 客户端	- 10 -
4.10.2	L2TP 客户端	- 10 -
4.11	静态路由	- 11 -
4.12	ARP 绑定	- 12 -
4.13	DHCP 静态分配	- 12 -
4.14	接口属性	- 12 -
5	状态监控	- 14 -
5.1	负载监控	- 14 -
5.1.1	性能负载	- 14 -
5.1.2	网络负载	- 14 -
5.2	内网用户	- 14 -
5.3	无线终端	- 16 -
5.4	认证用户	- 16 -
5.5	线路监控	- 17 -
5.6	设备注册	- 17 -

5.7	ARP 信息.....	- 18 -
5.8	系统路由表.....	- 18 -
6	智能流控.....	- 19 -
6.1	QoS 配置.....	- 19 -
6.2	带宽保障.....	- 19 -
6.3	端口分流.....	- 20 -
6.4	域名分流.....	- 22 -
6.5	负载均衡.....	- 23 -
6.6	运营商分流.....	- 23 -
7	防火墙.....	- 24 -
7.1	端口映射.....	- 24 -
7.1.1	基础配置.....	- 24 -
7.1.2	高级配置.....	- 24 -
7.2	主机放行.....	- 25 -
7.3	过滤规则 (ACL)	- 26 -
7.4	内网转发.....	- 27 -
7.5	共享阻断.....	- 27 -
7.6	连接数限制.....	- 28 -
7.7	DMZ 服务.....	- 28 -
8	VPN 服务.....	- 29 -
8.1	PPTP 服务器配置.....	- 29 -
8.1.1	基础配置.....	- 29 -
8.1.2	高级配置.....	- 29 -
8.2	L2TP 服务器配置.....	- 30 -
8.2.1	基础配置.....	- 30 -
8.2.2	高级配置.....	- 30 -
9	计费认证.....	- 31 -
9.1	认证子网配置.....	- 31 -
9.2	本地套餐管理.....	- 31 -
9.3	认证用户管理.....	- 32 -
9.4	PPPoE 服务.....	- 33 -
9.4.1	基础配置.....	- 33 -
9.4.2	高级配置.....	- 34 -
9.5	微信认证.....	- 34 -
9.6	本地 Portal 认证.....	- 35 -
9.6.1	展示配置.....	- 35 -
9.6.2	认证配置.....	- 35 -
1)	本地认证方式.....	- 35 -
2)	电话号码认证.....	- 36 -
3)	一键认证.....	- 36 -
4)	唯一密码认证.....	- 37 -
5)	WIFIDOG 认证.....	- 37 -
6)	CMCC-WEB 认证.....	- 38 -
7)	RADIUS 认证.....	- 39 -

8)	LDAP 权限认证	- 40 -
9)	短信验证码认证	- 41 -
9.7	白名单配置	- 42 -
9.8	黑名单配置	- 43 -
9.9	账户到期通告	- 43 -
9.10	本地公告	- 44 -
10	无线管理	- 44 -
10.1	无线状态	- 44 -
10.1.1	开启 AC 管理功能	- 44 -
10.2	模板分组	- 45 -
10.2.1	2.4g 无线设置	- 45 -
10.2.2	高级配置	- 46 -
10.2.3	5.8 无线设置	- 47 -
10.3	AP 列表	- 47 -
10.3.1	AP 绑定默认 WiFi 模板设置	- 48 -
10.3.2	ap 重启	- 48 -
10.3.3	移除 AP	- 48 -
10.3.4	固定 AP 的 ip 获取方式	- 49 -
10.3.5	固定 ap 的发射功率	- 49 -
10.3.6	固定 AP 的无线信道	- 50 -
10.3.7	固定 AP 的无线频宽	- 50 -
10.3.8	固定 AP 的 AC 指向	- 51 -
10.3.9	升级 AP	- 51 -
10.3.10	统一 ap 的登入管理密码	- 52 -
10.4	无线优化	- 52 -
10.5	黑白名单	- 53 -
11	CPE 管理（无线网桥管理）	- 54 -
11.1	全局配置	- 54 -
11.2	CPE 列表	- 54 -
11.2.1	管理 CPE	- 54 -
11.2.2	网络拓扑	- 55 -
12	统一云控	- 55 -
12.1	统一云控	- 55 -
12.2	智能组网	- 55 -
13	应用中心	- 56 -
13.1	UPnP 管理	- 56 -
13.2	动态域名	- 56 -
13.3	内网穿透	- 57 -
13.4	网络唤醒	- 57 -
14	安全中心	- 58 -
14.1	健康检测	- 58 -
14.2	路由体检	- 58 -
14.3	行为审计	- 58 -
15	系统设置	- 59 -

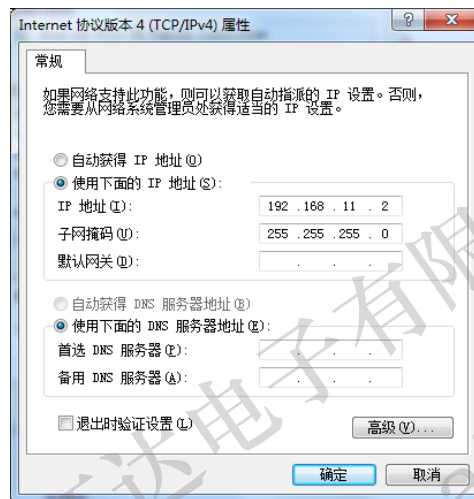
15.1	系统维护	- 59 -
15.2	远程访问	- 59 -
15.2.1	访问控制.....	- 59 -
15.2.2	远程日志记录.....	- 59 -
15.3	用户管理	- 60 -
15.4	网络诊断	- 60 -
15.4.1	PING 测试.....	- 60 -
15.4.2	路由追踪.....	- 61 -
15.5	管理工具	- 61 -
15.6	网络参数	- 61 -
15.7	时钟配置	- 62 -

江门市拓达电子有限公司
<http://www.todaair.cn>

1 配置准备

1.1 网络设置

PC（电脑）设置 IP 地址为自动获取或静态 IP 地址：192.168.11.x（x 为 2-254，确保不和网络中其他 IP 冲突），PC（电脑）网口与网关右侧第二个网口连接，PC 静态 IP 设置如下图：

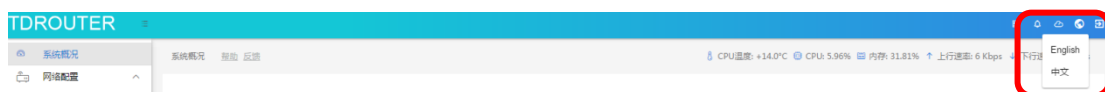


运行 Web 浏览器，在浏览器地址栏中输入 192.168.11.1（默认的管理 IP 地址）并回车。显示如下图，默认用户名：admin，密码：admin，单击登录按钮进入管理页面。



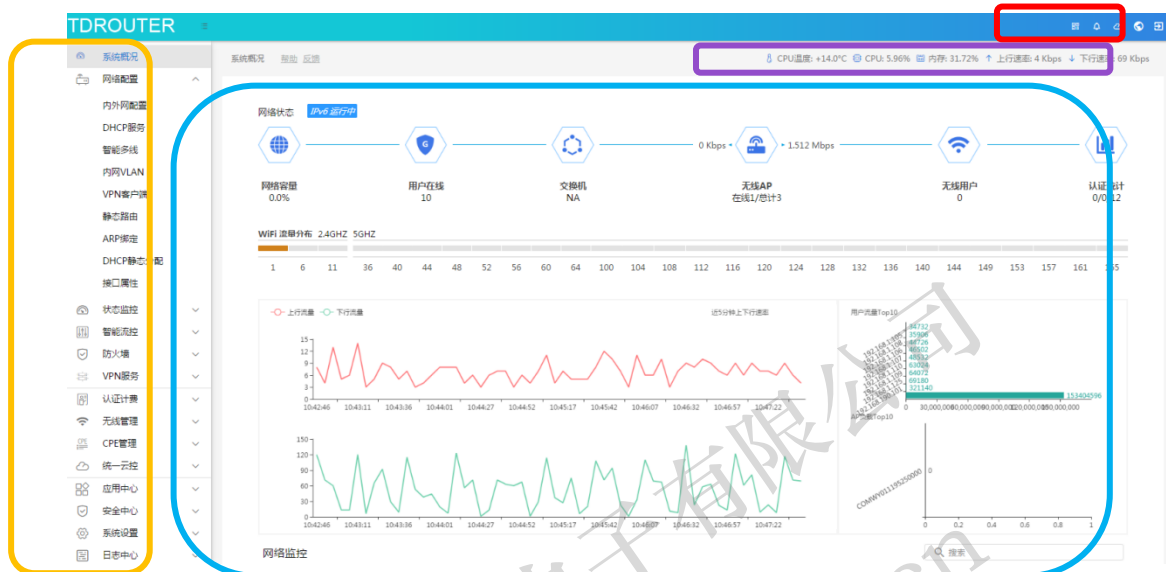
2 语言选择

登录界面提供中英文选项，登录界面后，也可根据右上角按钮更换语言选项。



3 系统概况

3.1 首页



- 如上图所示，为路由器系统概况整体展示图。展示数据编号及详解如下：
- 红框区域：展示网关的设备序列号、网关消息通知、云端登录地址、系统语言切换功能选项；
- 紫框区域：展示路由器当前 CPU 温度、CPU 使用率、内存使用率、上下行速率等信息；
- 橙框区域：网关配置页面导航栏；
- 蓝框区域：网关当前系统概况信息；

3.2 网络状态

通过鼠标悬浮至不同图标，可查看到外网、系统、无线和认证的使用情况



可实时查看近 5 分钟内网客户端的上下行速率使用情况



3.3 网络监控

可查看所有网络接口的基础信息：接口类型，IPV4/V6 地址，网关 IP 地址，MAC 地址。

名称	类型	状态	协议类型	IP地址	IPv6地址	网关	MAC地址	VLAN
lan	BOND	UP	static	192.168.1.1/255.255.255.0	2408:8256::3		1e:00:01:b7	0
lan	BOND	UP	static	192.168.1.1/255.255.255.0	2408:8256::3		1e:00:01:b8	0
lan	BOND	DOWN	static	192.168.1.1/255.255.255.0	2408:8256::3		1e:00:01:ba	0
lan	BOND	DOWN	static	192.168.1.1/255.255.255.0	2408:8256::3		1e:00:01:bb	0
wan	WAN	UP	pppoe	120.15/255.255.255.255	2408:8256::3	120.15	1e:00:01:bc	0

4 网络配置

4.1 内外网配置

在网口配置中包括三个类型，内网接口、聚合端口、外网接口。



- 内网接口(LAN): 表示内网网口，不同内网接口使用不同网段的 ip 地址。
- 聚合端口(BOND): 表示内网汇聚端口（网桥口），聚合端口均使用同一个 ip 地址。
- 外网接口(WAN): 表示广域网网口，连接外部网络使用。

4.2 内网接口设置：



- 点击需要修改的端口，接口类型选择内网接口
- MAC 地址：填写接口的物理 mac 地址，推荐选择随机填写
- IP 地址：填写内网接口的 IP 地址，例如：172.16.10.1
- 网络掩码：填写接口的子网掩码，默认为 255.255.255.0

4.3 高级配置

高级配置 ^

扩展地址

[添加](#)

操作	IP地址	网络掩码
没有可用数据		

IPv6前缀长度

该接口分发地址时使用的prefix长度

IPv6地址

接口地址尾部生成方式，可以使用的值: "eui64", "random", 或者固定值比如 "1"

DNS代理 ☐ 强制DNS代理

DHCP 模式 ☐ 关闭 ☐ 基础模式 ☒ 高级模式

- IPv6 前缀长度选择 60
- IPv6 地址：填写内网接口的 IPv6 地址，不填则使用系统默认 ipv6 地址
- 扩展地址：填写内网接口的扩展 IP 地址，可不填
- DNS 代理 勾选强制 DNS 代理强制使用网关 dns 地址

4.4 DHCPv4 配置

DHCPv4配置

DHCP 起始地址

DHCP 地址掩码

DHCP 分配网关

DHCP 地址池

DHCP 租约时间

主DNS

次DNS

- DHCP 起始地址：填写动态分配的起始地址
- DHCP 地址池大小：填写 DHCP 地址池数量的最大值
- DHCP 租用时间：填写客户端租用 IP 地址保留时间（单位：分钟）
- 主 DNS：填写 DHCP 服务器自动分配给客户机的主 DNS 服务器地址
- 次 DNS：填写 DHCP 服务器自动分配给客户机的次 DNS 服务器地址

4.5 DHCPv6 配置

DHCPv6配置

DHCPv6服务

DHCPv6模式

路由器通告服务(RA)

邻居发现协议代理(NDP)

IPv6 DNS

[保存](#)

- DHCPv6 服务 选择服务器，可选服务器模式 中继模式 混合模式，
- DHCPv6 模式 选择无状态+有状态 无状态、无状态 + 有状态、有状态

- 路由器通告服务(RA) 选择服务器模式 关闭、服务器模式、中继模式、混合模式
- 邻居发现协议代理(NDP) 选择关闭 关闭、中继模式、混合模式
- IPv6 DNS: 填写 DHCP 服务器自动分配给客户机的 IPV6 DNS 服务器地址

4.6 聚合接口设置:

- 点击接口类型，点击需要修改的端口，选择聚合接口
- MAC 地址：填写接口的物理地址
- IP 地址：填写接口的 IP 地址
- 网络掩码：填写接口的子网掩码，默认为 255.255.255.0，可根据使用修改设置

4.7 外网接口(WAN)设置:

连接外网四种方式

- DHCP IPv4 (动态获取 IPv4)
- DHCP IPv6 (动态获取 IPv6)
- Static IP (静态 IP，专线网络)
- PPPoE (宽带拨号)

4.7.1 DHCP 上网模式设置（自动获取上级路由下发的 IP）

- 点击需要修改的网口，接口类型选择外网接口（WAN）模式
- MAC 地址：接口的物理地址，可选择随机更换
- 接入方式：选择 DHCP
- 获取 IPv6 地址：关闭或开启，建议开启

- DHCPv6 服务：选择关闭
 - DNS：选填，非特殊情况建议使用当地运营商提供的 DNS，一般可用 114.114.114.114 或 8.8.8.8
 - 带宽：广域网出口的上行带宽、下行带宽，建议选择企业 1G 以上
 - 负载均衡选择：可按运营商进行分流，或自定义设置分流，或不参与均衡
 - 链路检测选择：可填写检测的网址进行 PING/HTTP/HTTP+PING 连通测试
- 注意：检查网口的 MAC 地址是否一致，如存在一致，应修改网口的不同 MAC 地址。

4.7.2 DHCPV6 配置方式与 DHCP 方式相同，DNS 可以填写 IPV6 DNS。

4.7.3 静态 IP 上网模式设置(Static IP)

The screenshot shows the 'Network Configuration' (网络配置) page in a web management interface. The left sidebar lists various system settings, with 'Network Configuration' (网络配置) selected. Under 'Network Configuration', 'Static IP' (静态 IP) is highlighted. The main area shows the configuration for the 'WAN' interface. The 'Interface Type' (接口类型) is set to 'External Interface' (外网接口). The 'Access Method' (接入方式) is set to 'Static' (Static). The 'IP Address' (IP 地址) is 100.100.100.11, 'Subnet Mask' (网络掩码) is 255.255.255.252, and 'Gateway' (网关) is 100.100.100.1. The 'DHCPv6 Service' (DHCPv6 服务) is set to 'Off' (关闭). The 'DNS' field is empty. The 'Bandwidth' (带宽) is set to 10000000. The 'Load Balancing' (负载均衡) is set to 'Do Not Participate in Load Balancing' (不参与均衡). The 'Link Detection' (链路检测) is set to 'Do Not Perform Link Detection' (不开链路检测).

- 点击需要修改的网口，接口类型选择外网接口（WAN）模式
 - MAC 地址：网口的物理地址
 - 接入方式：选择 Static
 - IP 地址:填写可连接外网的静态 ip 地址
 - 网络掩码: 填相应的子网掩码
 - 网关: 填相应的网关 ip 地址
 - IPv6 地址:选填
 - DHCPv6 服务:选择关闭
 - DNS：非特殊情况建议使用当地运营商提供的 DNS，一般可用 114.114.114.114 或 8.8.8.8
 - 带宽：填写广域网出口的上行带宽、下行带宽
 - 负载均衡选择：可按运营商进行分流，或自定义设置分流，或不参与均衡
 - 链路检测选择：可填写检测的网址进行 PING/HTTP/HTTP+PING 连通测试
- 注意：检查网口的 MAC 地址是否一致，如存在一致，应修改网口的不同 MAC 地址。

4.7.4 PPPoE 拨号上网模式设置

The screenshot shows the 'Network Configuration' page with the 'WAN' tab selected. The configuration fields are as follows:

- 接口类型: ☒ 内网接口 ☐ 聚合接口 ☒ 外网接口
- MAC地址: 00:38:bc:65:e7:92
- 接入方式: ☐ DHCP ☐ DHCPv6 ☐ Static ☒ PPPoE
- 获取IPv6地址: 自动
- 宽带账号: 07500000000
- 宽带密码: 12345678
- PPPoE 服务名称: 选填
- DHCPv6服务: ☒ 关闭 ☐ 开启
- DNS: 请输入DNS服务器地址(选填)
- 带宽: 10000000
- 负载均衡: 不参与均衡

- 点击需要修改的网口，接口类型选择外网接口（WAN）模式
- MAC 地址：网口的物理地址
- 接入方式：选择 PPPoE
- 获取 IPv6 地址:选择自动
- 宽带账号：填写运营商提供的宽带账号和密码
- DHCPv6 服务:选择关闭
- DNS：非特殊情况建议使用当地运营商提供的 DNS，一般可用 114.114.114.114 或 8.8.8.8
- 带宽：填写广域网出口的上行带宽、下行带宽
- 负载均衡选择：可按运营商进行分流，或自定义设置分流，或不参与均衡
- 链路检测选择：可填写检测的网址进行 PING/HTTP/HTTP+PING 连通测试

注意：检查网口的 MAC 地址是否一致，如存在一致，应修改网口的不同 MAC 地址。

4.8 DHCP 服务配置

4.8.1 DHCP 服务信息

The screenshot shows the 'DHCP Service' configuration page. It contains a table with the following data:

操作	内网接口	状态	DHCP 起始地址	DHCP 地址池	IPv4 DNS	网关地址	DHCPv6状态	DHCPv6模式
编辑 删除	lan	开启	192.168.120.100	600	114.114.114.114 223.5.5.5	192.168.88.1	关闭	无状态
编辑 删除	lan1	开启	172.16.10.100	150	114.114.114.114 223.5.5.5	172.16.10.1	关闭	无状态
编辑 删除	lan1_17	开启	172.17.17.100	150	223.5.5.5	172.17.17.1	关闭	无状态

- 内网接口：聚合接口、内网接口和虚拟子网接口
- 状态：接口开启或关闭
- DHCP 起始地址：动态分配的起始 IP 地址

- DHCP 地址池大小：DHCP 地址数的最大值
- DNS：DHCP 服务器分配给客户端的主 / 次 DNS 服务器地址
- 网关地址：对应的接口 IP 地址
- DHCPv6 状态：接口的 DHCPv6 服务开启 / 关闭
- DHCPv6 模式：接口的 DHCPv6 地址分配方式
- DHCP 添加 点击右上方“添加”按钮

当前服务接口

当前服务接口

DHCP 模式 ☐ 关闭 ☐ 基础模式 ☒ 高级模式

DHCPv4配置

DHCP 起始地址

DHCP 地址掩码

DHCP 分配网关

DHCP 地址池

DHCP 租约时间

主DNS

次DNS

- 接口：选择需要开启 dhcp 内网的接口或者虚拟子网接口
- DHCP 模式：关闭、基础模式、高级模式
- DHCP 起始地址：动态分配的开始 IP 地址
- DHCP 地址掩码：接口的子网掩码
- DHCP 网关地址：动态分配的网关 IP 地址
- DHCP 地址池大小：DHCP 地址数的最大值
- DHCP 租用时间：客户端租用 IP 地址保留时间（单位：分钟）
- 主 DNS：DHCP 服务器自动分配给客户机的主 DNS 服务器地址
- 次 DNS：DHCP 服务器自动分配给客户机的次 DNS 服务器地址

4.8.2 DHCPv6 配置

DHCPv6配置

DHCPv6服务

DHCPv6模式

路由器通告服务 (RA)

邻居发现协议代理 (NDP)

IPv6 DNS

- DHCPv6 模式：关闭、服务模式、中继模式、混合模式
- DHCPv6 模式：无状态、无状态+有状态、有状态
- 路由器通告服务(RA)：关闭、服务模式、中继模式、混合模式
- 邻居发现协议代理(NDP)：关闭、中继模式、混合模式
- IPv6 DNS：分配给客户端的 IPv6 DNS 服务器地址（选填）

4.9 内网 VLAN

通过内网接口虚拟出子网接口，可添加多个子网 VLAN，原理与单臂路由方法一致

点击右上方“添加”按钮

- 绑定物理口：选择内网接口，不能使用聚合端口
- VLAN ID：填写 vlan 标签（VLAN 号为 1~4094，不能重复）
- MAC 地址配置：接口的物理地址，点击随机即可生成 MAC
- IP 地址：填写虚拟子网的 IP 地址，例如：172.16.10.1
- 网络掩码：填写子网掩码，默认为 255.255.255.0

4.9.1 高级配置

扩展地址：选填

IPv6 前缀长度：建议禁用

IPv6 地址：选填，填写子网接口的 IPv6 地址，不填则使用内网 ipv6 地址

DNS 代理：勾选强制 DNS 代理，强制使用网关 dns 地址

4.9.2 DHCPv4 配置

DHCP 起始地址：填写动态分配的开始 IP 地址

DHCP 地址池大小：填写 DHCP 地址数的最大值

DHCP 租用时间：填写客户端租用 IP 地址保留时间

DNS1：填写 DHCP 服务器自动分配给客户机的主 DNS 服务器地址

DNS2：填写 DHCP 服务器自动分配给客户机的次 DNS 服务器地址

4.9.3 DHCPv6 配置

DHCPv6 模式：关闭、服务模式、中继模式、混合模式

DHCPv6 模式：无状态、无状态+有状态、有状态

路由器通告服务(RA)：关闭、服务模式、中继模式、混合模式

邻居发现协议代理(NDP)：关闭、中继模式、混合模式

IPv6 DNS：分配给客户端的 IPv6 DNS 服务器地址（选填）

4.10 VPN 客户端

选择 PPTP 或 L2TP，点击添加进行 VPN 拨号连接设置

4.10.1 PPTP 客户端

网络配置/VPN客户 帮助 反馈 CPU温度: +11.0°C

拨号名称: pptp1

启用: ☒

服务器地址/域名: 请输入服务器地址/域名

用户名: 请输入用户名

密码: 请输入密码

上行速率: 请输入上行速率(Kbps)

下行速率: 请输入下行速率(Kbps)

负载均衡: 默认均衡组

链路检测: ☐ 开启链路检测

- 拨号名称: 对 PPTP 拨号的名称的描述
- 启用: PPTP 服务的配置是否启用
- 服务器 IP 地址/域名: PPTP 服务器的 IP 地址或者域名
- 用户名: PPTP 拨号的用户名
- 密码: PPTP 拨号的密码
- 上行速率: PPTP 服务的上行速率
- 下行速率: PPTP 服务的下行速率
- 负载均衡: 选择默认均衡组
- 链路检测: 默认不开启

4.10.2 L2TP 客户端

网络配置/VPN客户 帮助 反馈 CPU温度: +10.0°C

拨号名称: l2tp1

启用: ☒

服务器地址/域名: 请输入服务器地址/域名

用户名: 请输入用户名

密码: 请输入密码

上行速率: 请输入上行速率(Kbps)

下行速率: 请输入下行速率(Kbps)

负载均衡: 默认均衡组

链路检测: ☐ 开启链路检测

拨号名称: 对 L2TP 拨号的名称的描述

启用: L2TP 服务的配置是否启用

服务器 IP 地址/域名: L2TP 服务器的 IP 地址或者域名

用户名: L2TP 拨号的用户名

密码: L2TP 拨号的密码

上行速率: PPTP 服务的上行速率

下行速率: PPTP 服务的下行速率

负载均衡: 选择默认均衡组

链路检测: 默认不开

4.11 静态路由

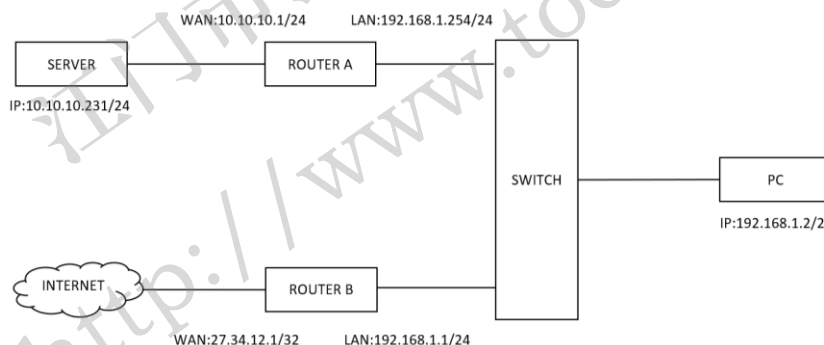
网络配置/静态路由/添加 帮助 反馈 CPU温度: +15.0°C CPU: 7.19%

线路	
目的地址	请输入目的地址
子网掩码	
网关	请输入网关
优先级	请输入优先级
备注	请输入备注

- 线路：根据环境所需选择接口，作接口路由转发
- 目的地址：目的设备所用的子网
- 子网掩码：目的所用的子网掩码
- 网关：目的 LAN 口的接口 IP 地址
- 优先级：默认值为 0
- 备注：此条路由的备注信息

如：

在一个公司网络中，不仅可以通过无线路由器 B 连接外网，还可以通过无线路由器 A 来连接公司内网服务器。在不修改本地连接的 IP 地址及网关情况下，公司电脑需要能够同时访问外网和内网服务器。配置实例如下图：



设置方式如下，在路由器 B 管理页面中，点击“网络配置-静态路由-添加”，如下图

网络配置/静态路由/添加 帮助 反馈

线路	lan
目的地址	10.10.10.0
子网掩码	255.255.255.0
网关	192.168.1.254
优先级	1
备注	SERVER/10.10.10.0

测试 PC 端能否 PING 通 SERVER，检测静态路由条目是否生效。如果能访问，则说明静态路由配置成功。

4.12 ARP 绑定

网络配置/ARP绑定/添加 帮助 反馈 CPU温度: +15.0°C

IP

请输入IP

MAC

请输入MAC

所属接口

备注

请输入备注

保存

取消

- IP 地址：终端的 IP 地址
- MAC 地址：终端的 MAC 地址
- 所属接口：IP 对应的 LAN 口
- 备注：绑定 IP 和 MAC 的备注描述

附：添加规则后，勾选规则再点击加入 DHCP 静态分配按钮，开启强制 mac 绑定 ip，开启之后 ip 和 mac 需要与绑定信息一致才能访问网络，对不符合规则的数据包丢弃。

4.13 DHCP 静态分配

网络配置/DHCP静态分配/添加 帮助 反馈 CPU温度: +15.0°C

IP

请输入IP

MAC

请输入MAC

备注

请输入备注

保存

取消

- IP 地址：终端的 IP 地址
- MAC 地址：终端的 MAC 地址
- 备注：绑定 IP 和 MAC 的备注描述

4.14 接口属性

网络配置/接口属性 帮助 反馈 CPU温度: +14.0°C CPU: 6.88% 内存: 27.39% 上行速率: 5 Kbps 下行速率: 3 Kbps

请输入内容

操作	接口名称	逻辑接口	链路状态	自动协商	端口速率	双工模式	收/发报文	收/发字节
编辑	eth0	lan	Down	Yes	Unknown!	Unknown!	0/0	0/0
编辑	eth1	lan	Down	Yes	Unknown!	Unknown!	1385/8007	222807/792100
编辑	eth2	lan	Up	Yes	100Mb/s	Full	216141/3132550	40034158/219884280
编辑	eth3	lan	Down	Yes	Unknown!	Unknown!	0/0	0/0
编辑	eth4	lan	Up	Yes	1000Mb/s	Full	1088764/3794298	683280735/1672429195
编辑	eth5	wan	Up	Yes	1000Mb/s	Full	3333859/1709973	1709587068/980882669

每页的行数: 20 1-6 / 6

操作 eth0

自动协商

☒ 自动协商

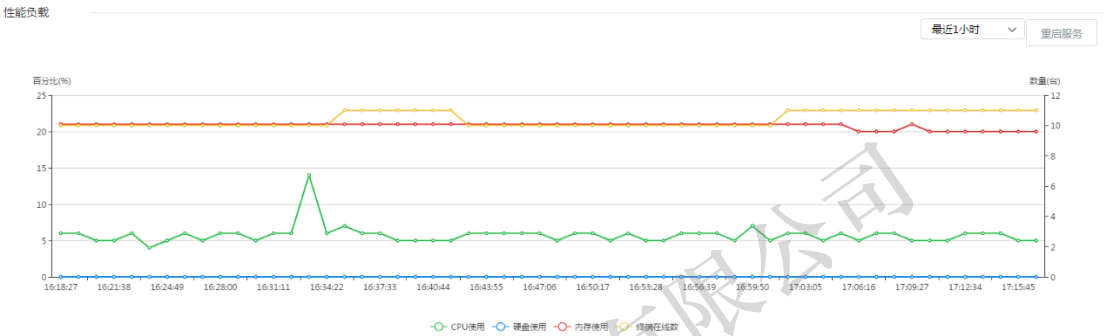
- 操作：点击编辑，可以开关端口自动协商，建议使用自动协商
- 接口名称：各个物理端口名称
- 逻辑接口：各个物理端口的使用状态，WAN/LAN
- 链路状态：各个物理端口的连接状态，关闭/未连接为 down，开启/连接为 up
- 自动协商：端口速率是否自动协商
- 端口速率：显示当前网口速率，关闭/未连接为 Unknown
- 双工模式：默认为全双工模式，关闭/未连接为 Unknown
- 收发报文：各个物理端口收发报文统计数量
- 收发字节：各个物理端口收发字节统计数量

5 状态监控

5.1 负载监控

5.1.1 性能负载

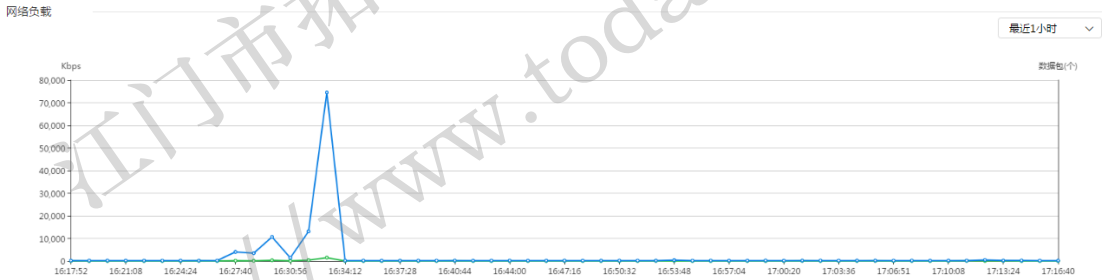
记录系统在运行过程中，硬件负载情况，点击重启服务按钮可重启 Web 服务



通过点击下端的 CPU 使用、内存使用、硬盘使用、终端在线数可以显示或隐藏对应的使用情况。

5.1.2 网络负载

记录系统在运行过程中，实时汇报网络负载，包括上行与下行带宽。



5.2 内网用户

可以按刷新按钮进行页面内容刷新，点击重启服务按钮可重启 Web 服务。

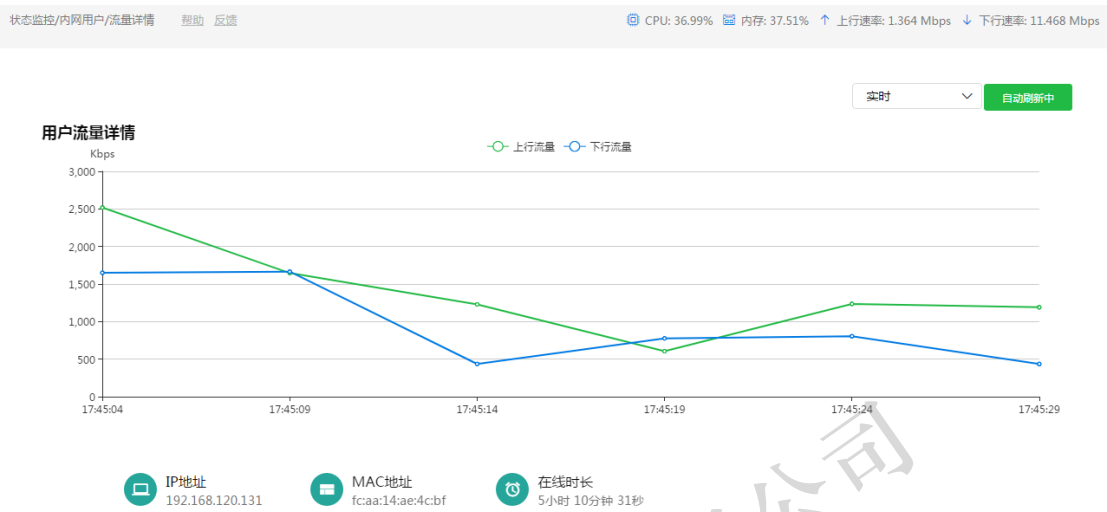
状态监控/内网用户 帮助 反馈 CPU温度: +11.0°C CPU: 5.65% 内存: 31.64% 上行速率: 4 Kbps 下行速率: 173 Kbps

Q 请输入内容 自动刷新中 重启服务 刷新

操作	IP地址	IPv6地址	MAC地址	主机名	来源	在线时长	会话数量	累计上行	累计下行	上行速率	下行速率
详情 加入黑名单 限速	192.168.1.107	-	74-96:37:06:02:9c	*	lan	9小时 25分钟 19秒	1	26.953 KB	3.377 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.108	-	74-96:37:08:d4:07	*	lan	9小时 25分钟 19秒	4	15.703 KB	15.219 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.110	-	74-96:37:05:fa:4c	*	lan	9小时 25分钟 19秒	3	26.953 KB	11.293 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.125	-	74-96:37:09:5b:09	*	lan	9小时 25分钟 19秒	3	26.953 KB	13.891 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.105	-	74-96:37:09:0f:4b	*	lan	9小时 25分钟 19秒	1	26.719 KB	4.326 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.106	-	74-96:37:09:29:fb	*	lan	9小时 25分钟 19秒	4	26.953 KB	11.813 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.190.101	-	74-96:37:09:30:4d	COMWY011195250000-AP	lan	9小时 25分钟 19秒	11	124.706 KB	167.363 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.111	-	74-96:37:09:0f:17	*	lan	9小时 25分钟 19秒	1	26.758 KB	3.074 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.109	-	74-96:37:09:29:7d	*	lan	9小时 25分钟 19秒	3	26.953 KB	15.746 KB	0 Kbps	0 Kbps
详情 加入黑名单 限速	192.168.1.150	-	00:e0:66:3f:31:71	WIN-E4DGAA9849G	lan	8小时 55分钟 37秒	43	5.467 MB	197.486 MB	0 Kbps	4 Kbps

每页的行数: 20 1-10 / 10 < >

点击操作中的详情可以实时查看对应用户的流量详情。



点击操作中的加入黑名单可以将终端加入黑名单，禁止终端接入网络。

请输入内容 自动刷新中 重启服务 刷新

	操作	IP地址	IPv6地址	MAC地址	主机名	来源	在线时长	会话数量	累计上行	累计下行
详情	加入黑名单	限速	172.16.10.188	74:96:37:09:5e:06	*	lan	5小时 12分钟 10秒	24	270.186 KB	830.109 KE
详情	加入黑名单	限速	192.168.88.55		*	lan	5小时 12分钟 10秒	16	250.421 KB	453.420 KE
详情	加入黑名单	限速	192.168.100.101		*	lan	5小时 12分钟 10秒	1	13.657 MB	144.896 MI
详情	加入黑名单	限速	192.168.120.131		Windows7-PC	lan	5小时 12分钟 10秒	26	17.329 MB	136.807 MI
详情	加入黑名单	限速	192.168.111.181		*	lan	5小时 12分钟 10秒	4	214.460 KB	248.460 KE
详情	加入黑名单	限速	172.16.10.187		*	lan	5小时 12分钟 10秒	24	273.421 KB	830.630 KE
详情	加入黑名单	限速	192.168.120.123		*	lan	5小时 12分钟 10秒	17	52.933 MB	1.537 MB
详情	加入黑名单	限速	172.16.10.193		SC-201608231216	lan	5小时 12分钟 10秒	8	4.526 MB	58.012 MB
详情	加入黑名单	限速	192.168.108.197		*	lan	5小时 12分钟 10秒	11	1.459 MB	17.489 MB

加入黑名单后，可在认证计费-黑名单配置-MAC 黑名单，通过删除按钮解除限制。

认证计费

认证子网配置 本地套餐管理 认证用户管理 PPPoE服务 微信认证 本地Portal认证 WIFIDOG认证 CMCC-WEB认证 RADIUS 配置 LDAP 配置 短信网关配置 白名单配置 黑名单配置

MAC黑名单

MAC黑名单 IP黑名单

请输入内容 添加 批量添加 导入 导出 反选 删除

	操作	MAC地址	备注
☐	编辑	30:59:b7:4b:73:3d	XBOX

每页的行数: 20 1-1 / 1

点击操作中的限速可以将终端的上下行速率限速

状态监控

负载监控 内网用户 无线终端 认证用户 线路监控 设备注册 ARP信息 系统路由表

请输入内容 自动刷新中 重启服务 刷新

	操作	IP地址	IPv6地址	MAC地址	主机名	来源	在线时长	会话数量	累计上行	累计下行	上行速率
详情	加入黑名单	限速	172.16.10.188	74:96:37:09:5e:06	*	lan	5小时 14分钟 18秒	22	271.453 KB	834.959 KB	0 Kbps
详情	加入黑名单	限速	192.168.88.55		*	lan	5小时 14分钟 18秒	7	251.798 KB	454.745 KB	0 Kbps
详情	加入黑名单	限速	192.168.100.101		*	lan	5小时 14分钟 18秒	1	13.657 MB	144.896 MB	0 Kbps
详情	加入黑名单	限速	192.168.120.131		Windows7-PC	lan	5小时 14分钟 18秒	29	17.455 MB	136.912 MB	9 Kbps
详情	加入黑名单	限速	192.168.111.181		*	lan	5小时 14分钟 18秒	1	214.580 KB	248.577 KB	0 Kbps
详情	加入黑名单	限速	172.16.10.187		*	lan	5小时 14分钟 18秒	22	274.676 KB	835.479 KB	0 Kbps
详情	加入黑名单	限速	192.168.120.123		*	lan	5小时 14分钟 18秒	21	54.018 MB	1.565 MB	0 Kbps
详情	加入黑名单	限速	172.16.10.193		SC-201608231216	lan	5小时 14分钟 18秒	3	4.526 MB	58.014 MB	0 Kbps
详情	加入黑名单	限速	192.168.108.197		*	lan	5小时 14分钟 18秒	9	1.464 MB	17.490 MB	0 Kbps

进行限速操作后，可在智能流控-带宽保障-MAC 限速，启用、停用或删除该配置。



5.3 无线终端

显示通过无线连接到网关的终端用户详细列表

操作	IP地址	MAC地址	主机名	所属AP	AP MAC	无线名称	在线时长	信号强度	接收速率	发射速率
下线	192.168.1.52	8C:8E:6A:5A:00:00		TDAP001127272727	74:8C:8E:6A:5A:00	测试	1天 9小时 16分钟 6秒	-61 dBm	35.0	139.1
下线	192.168.1.46	5c:8c:8e:6a:5a:00		TDAP001127272727	74:8C:8E:6A:5A:00	测试	1天 9小时 11分钟 5秒	-57 dBm	4.0	67.0
下线		a0:3b:99:00:00:00		TDAP001127272727	74:8C:8E:6A:5A:00	test1	56分钟 20秒	-69 dBm	65.0	65.0

- 操作：点击操作中的下线按钮，可让终端设备短时间断开无线连接，用户可重新连接。
- IP 地址：终端的 IP 地址
- MAC 地址：无线终端的 MAC 地址
- 主机名：无线终端在网络中显示的名称
- 所属 AP：无线终端连接的 AP 序列号
- AP MAC：AP 的 MAC 地址
- 无线名称：无线终端连接的 SSID 名称
- 在线时长：无线终端连接网络的时间
- 信号强度：无线终端连接 AP 当前的信号强度
- 接收/发射速率：无线终端当前的无线连接速率

5.4 认证用户

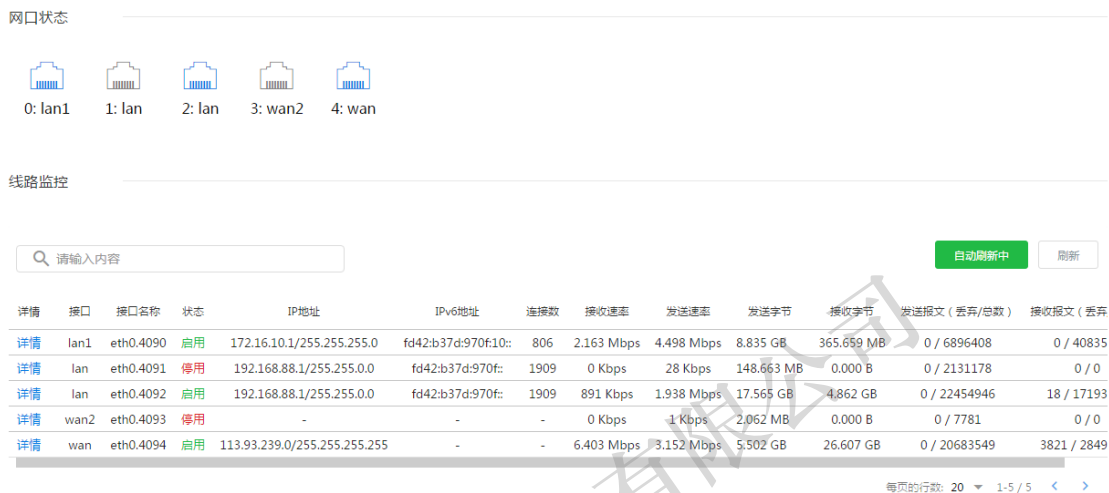
显示通过 Portal 认证用户详细列表

操作	IP地址	IPv6地址	MAC地址	用户名	认证方式	在线时长	会话数量
下线	172.17.17.139	fe80:107f:a58d:b58a:dc	80:3d:3e:10:5a	lan		14秒	0

- 操作：点击操作中的下线按钮，可让终端设备断开认证，用户需重新认证上网；加入黑名单，将终端加入黑名单，禁止终端接入网络。可在认证计费-黑名单配置-MAC 黑名单，通过删除按钮解除限制。
- IP/IPv6 地址：终端的 IPv4/IPv6 地址
- MAC 地址：终端的 MAC 地址
- 认证方式：通过 LAN 认证
- 在线时长：终端连接网络的时间

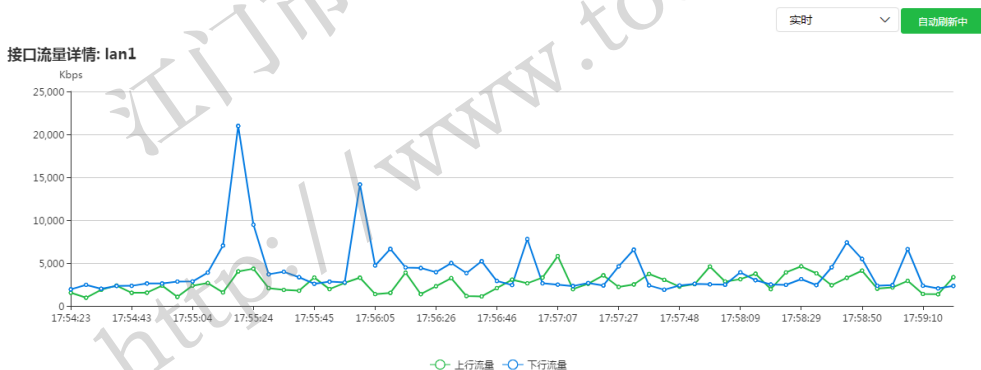
- 信号强度：终端连接 AP 当前的信号强度
- 会话数量：终端会话数量

5.5 线路监控



网口状态

- 显示蓝色为启用状态，灰色为断开或未连接状态
- 监控列表中显示各网口的 IPv4/IPv6 地址，会话连接数，接收/发送速率，发送/接收字节，发送/接收报文
- 点击详情可以实时查看接口流量信息



5.6 设备注册

可查看系统版本及序列号等信息

注册状态	
设备已注册	
授权信息	
型号	TDROUTER
设备序列号	TDAIR-0
设备厂商	
路由系统版本	v5.0.build20190914-1435-e4c7411

5.7 ARP 信息

地址解析协议，即 ARP（Address Resolution Protocol），是根据 IP 地址获取物理地址的一个 TCP/IP 协议。主机发送信息时将包含目标 IP 地址的 ARP 请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该 IP 地址和物理地址存入本机 ARP 缓存中并保留一定时间，下次请求时直接查询 ARP 缓存以节约资源。

该设备的 ARP 信息，包含 IPv4 /IPv6 的接口、IP 地址、MAC 地址以及 IP 类型信息。

IPv4

IPv6

Q

请输入内容

导出

加入DHCP静态分配

加入ARP绑定

反选

☐	所属接口	终端IP	终端MAC	类型
☐	br-lan1	172.16.10.148	b0e5edcc:38:03	STALE
☐	br-lan	192.168.120.143	74:96:37:06:a4:63	DELAY
☐	br-lan1	172.16.10.129	dca4:ca65:30:47	STALE
☐	br-lan1	172.16.10.123	48:c7:96:41:38:99	REACHABLE
☐	br-lan1	172.16.10.104	2c:5d:34:12:29:f1	STALE
☐	br-lan	192.168.110.182	44:19:b6:43:86:7a	REACHABLE
☐	br-lan	192.168.120.178	6c:f0:49:90:f1:65	DELAY
☐	br-lan	192.168.9.131	00:e0:4c:a5:76:53	REACHABLE
☐	br-lan	192.168.6.86	fc:aa:14:03:79:2f	REACHABLE

点击加入 ARP 绑定，可将 IP 与对应的 MAC 绑定

注意：ARP 绑定是用户根据自己的需求手工添加，但不绑定终端的 IP 地址，如需绑定 IP，可在 DHCP 静态分配中设置。

5.8 系统路由表

在计算机网络中，路由表（routing table）是所有路径信息的集合。存储着指向特定网络地址的路径，含有网络周边的拓扑信息，建立的主要目标是为了实现路由协议和静态路由选择

IPv4

IPv6

Q 请输入内容

目的地址	网关	线路	优先级
0.0.0.0/0	113.93.236.1	pppoe-wan	-
0.0.0.0/0	113.93.236.1	pppoe-wan	1
113.93.236.1	-	pppoe-wan	-
172.16.10.0/24	-	br-lan1	-
172.17.1.0/24	-	br-lan1_17	-
192.168.0.0/16	-	br-lan	-

每页的行数: 201 - 6 < >

每页的行数: 20 1-6 / 6 < >

6 智能流控

6.1 QoS 配置



- 流控状态：启用/停用 QoS 功能
- 流控模式：一键流控即使用预设的流控规则，选择精细流控则自定义的优先级规则生效
- P2P 阻断：P2P 数据阻断，禁止终端使用 P2P 连接
- 均衡模式：会话数均衡或 IP 地址均衡

6.2 带宽保障



可选择根据 IP 限速或者 MAC 限速

状态 ☒ 启用 ☐ 停用

流控策略名称 rule

选择接口IP

IPv4 IP、IP段(用 '-' 分隔)或子网(10.0.0.0/8) [添加](#)

☐ 192.168.100.100/24 [移除](#)

上行速率 200 / 400 *

下行速率 200 / 400 *

周期 ☐ 全选 ☒ 星期一 ☐ 星期二 ☒ 星期三 ☐ 星期四 ☒ 星期五 ☐ 星期六 ☐ 星期日

时间段 00:01:20 - 23:59:59 *

[保存](#) [取消](#)

- 状态：启用/停用限速
- 流控策略名称：自定义规则名称
- 选择接口 IP：选择内网终端连接的网关接口
- IPv4：可以填写单个 IP 或者 IP 段，如果选择 MAC 限速则填入 MAC
- 上行速率：保障最低带宽/最高带宽
- 下行速率：保障最低带宽/最高带宽
- 周期：勾选生效的一周时间
- 时间段：选择一天内生效的起始时间与终止时间

6.3 端口分流

控制内网用户优先使用的外网访问策略

状态 ☒ 启用 ☐ 停用

策略描述 New Rule

主机IP地址 IP、IP段(用 '-' 分隔)或子网(10.0.0.0/8) [添加](#)

☐ [移除](#)

流优先级 Priority

接口 wan

远端IP地址 [添加](#)

教育网 [移除](#)

- 状态：启用/停用端口分流
- 策略描述：自定义名称
- 主机 IP 地址：可以填写单个 IP 或者 IP 段

- 流优先级：Priority 首要优先
Express
Normal
Bulk
- 接口：广域网接口

高级配置 ^

远端IP地址	IP、IP段(用 '-' 分隔)或子网(10.0.0.0/8) 添加
	☐ 移除
协议	TCP
内部端口	端口或者端口范围(例: 8080或8080:8090) 添加
	☐ 移除
外网端口	端口或者端口范围(例: 8080或8080:8090) 添加
	☐ 移除
保存 取消	

- 远端 IP 地址：可以是单个 IP 地址或 IP 地址段，也可以留空
- 协议：ANY、TCP、UDP、TCP+UDP、ICMP、ICMPv6
- 内部端口：内部网络所用的端口或端口范围
- 外网端口：外部网络所用的端口或端口范围

6.4 域名分流

基础配置

状态	☒ 启用 ☐ 停用
策略描述	rule
主机IP地址	IP、IP段(用 '-' 分隔)或子网(10.0.0.0/8) 添加
	☐ 移除
策略优先级	Priority
接口	

高级配置 ^

域名	请输入域名 添加
	移除

控制内网用户优先使用的外网访问策略

状态：启用/停用域名分流

- 策略描述：自定义名称
- 主机 IP 地址：可以填写单个 IP 或者 IP 段
- 流优先级：Priority 首要优先
Express
Normal
Bulk
- 接口：广域网接口类型
- 域名：外网域名地址

6.5 负载均衡

接口 wan

均衡权重 1000000

负载均衡 中国电信

链路检测 ☒ 开启链路检测

判定次数(默认: 5) 1

检测周期(默认: 5) 5

检测方式(默认: PING) PING

输入用于检测的地址 www.sina.com

保存 取消

- 接口：广域网的接口
- 均衡权重：此值主要用于跟其他线路的负载做比较，系统会根据值的大小来决定线路的负载大小，默认值是依靠带宽值的大小来自动判定。若修改默认值，请根据线路的带宽比例设置参数，参数越大，通过的数据/用户就会越多。
- 负载均衡：指定负载线路的运营商分流策略
- 链路检测：启用/停用链路检测
- 判定次数：系统在一定时间范围内检测线路的 PING 次数（默认 5 次）
- 检测周期：系统 PING 检测间隔时间（默认 5 秒一次）
- 检测方式：PING、HTTP、HTTP+PING（默认 PING 方式）
- 输入用于检测的地址：检测连通的域名。

6.6 运营商分流

系统概况 网络配置 状态监控 智能分流 运营商分流

中国电信 中国联通 中国移动 教育网 自定义均衡组一 自定义均衡组二 自定义均衡组三

使用默认运营商定义文件 下载运营商定义文件 0 (0.0 B) 上传运营商定义文件

```
#####
# ISP 中国移动 所有IP地址段表
# 数据来自于: http://ispip.clang.cn/
# 数据生成时间: 2016-05-30 00:10:27
# 共计数据 29 条
# 脚本自动生成,如有错误或任何建议,请联系 admin[at]clang.cn
#####
36.128.0.0/10
39.128.0.0/10
43.251.244.0/22
45.121.172.0/22
45.121.176.0/22
103.20.112.0/22
103.21.176.0/22
103.62.24.0/22
111.0.0.0/10
112.0.0.0/10
117.128.0.0/10
120.192.0.0/10
183.192.0.0/10
```

运营商分流策略可以使用默认的 IP 地址段，也可以自定义上传指向文件，按当地运营商提供的 IP 地址填写。

7 防火墙

7.1 端口映射

在防火墙-端口映射，点击添加。

基础配置

状态	☒ 启用 ☐ 停用
映射说明	开放WEB
协议族	任意
协议	TCP+UDP
外网端口	866
	端口或者端口范围(例: 8080或8080:8090)
内部端口	80
	端口或者端口范围(例: 8080或8080:8090)
内网地址	192.168.1.112

高级配置

源IP	请输入源IP
源端口	端口或者端口范围(例: 8080或8080:8090)
	端口或者端口范围(例: 8080或8080:8090)
WAN口地址	请输入WAN口地址
	注：如果配置wan口地址外部只能通过这个地址访问,如果没有配置wan口地址,可通过所有wan口地址访问
端口回流	☒ 启用 ☐ 停用
	端口回流可以使端口映射的服务在内网也可以访问,如果需要在内网访问该服务,则需要开启

7.1.1 基础配置

- 状态：启用/停用端口映射
- 映射说明：填写此规则的名称备注
- 协议族：选择任意（包含 IPv4/IPv6）
- 协议：选择 TCP+UDP
- 外网端口：来自外部广域网的 IP 访问映射机器时的 WAN 口端口号，也可以是范围值（8080：8090），但不能与已有规则的端口号相同（如 80、443 等）
- 内部端口：访问内网服务器时使用的端口号，由服务器本身设定。
- 内网地址：内网需要映射的服务器 IP 地址

7.1.2 高级配置

- 源 IP：需要访问服务器的设备 IP 地址（可选填）
- 源端口：需要访问服务器的设备 IP 端口号（可选填）
- WAN 口地址：如果配置 wan 口地址，外部设备只能通过这个 WAN 口地址访问，如果没有配置 wan 口地址，可通过所有 wan 口地址访问。
- 端口回流：端口回流可以使端口映射的“IP+端口号”在内网也可以被访问，如果需要在内网访问该服务，则需要开启

7.2 主机放行

基于 MAC 的端口映射

IPv6 地址均为动态分配，目前根据 IPv6 的标准规定，为了提高网络环境安全性，最新的 IPv6 标准要求地址的分配一定是动态的，在这样的情况下，网关设备内网服务器的地址都可能是变化的，当网关和服务器的地址都是变化的情况下：

地址变化，而网关设备配置没有变化，会导致数据被过滤，为正确应对上述情况，需要基于 MAC 的自动放行规则配置，使得设备即使在 IPv6 地址变化的情况下，也能正确放行数据。

基础配置

The screenshot shows a configuration form with the following fields and options:

- 状态 (Status):** Radio buttons for ☒ 启用 (Enabled) and ☐ 停用 (Disabled).
- 映射说明 (Mapping Description):** Text input field containing "开放FTP,SSH,TELNET".
- 协议 (Protocol):** Dropdown menu showing "TCP".
- 内部端口 (Internal Port):** Text input field containing "21:23".
- MAC地址 (MAC Address):** Text input field with placeholder "请输入MAC地址". Below it is a list area with "添加" (Add) and "移除" (Remove) buttons.
- 同步地址至平台 (Synchronize Address to Platform):** Radio buttons for ☒ 启用 (Enabled) and ☐ 停用 (Disabled).
- 服务器类型 (Server Type):** Dropdown menu showing "WWW服务".
- Buttons:** "保存" (Save) and "取消" (Cancel) buttons at the bottom.

- 状态：启用/停用主机放行
- 映射说明：填写备注名称
- 协议：选择 TCP+UDP
- 内部端口：访问内网服务器时使用的端口号，由服务器本身设定。
- MAC 地址：填写内部主机的 MAC 地址
- 同步地址或平台：启用或停用，将 MAC 地址同步至平台
- 服务器类型：WWW 服务、FTP 服务、邮件服务、其他

7.3 过滤规则（ACL）

智能流控

防火墙

端口映射

主机放行

过滤规则

内网转发

共享阻断

连接数限制

DMZ服务

VPN服务

认证计费

无线管理

CPE管理

统一云控

应用中心

安全中心

系统设置

基础配置

状态 ☒ 启用 ☐ 停用

规则描述 拒绝访客访问网关

协议族 任意

源区 LAN

目的区 LAN

协议 TCP+UDP

源地址 172.16.18.0

IP地址或者IP子网,多个地址用空格分隔

目的地址 192.168.88.1

IP地址或者IP子网,多个地址用空格分隔

源端口 请输入源端口

端口或者端口范围(例: 8080或8080:8090),多个端口用空格分隔

目的端口 800

端口或者端口范围(例: 8080或8080:8090),多个端口用空格分隔

动作 DROP

保存 取消

- 状态：启用/停用过滤规则
- 规则描述：自定义策略的名称备注
- 协议族：任意(ANY)、IPv4、IPv6
- 源区：需要过滤的源区域
- 目的区：过滤的目的区域
- 协议：任意 ANY、TCP、UDP、TCP+UDP、ICMP、ICMPv6
- 源地址：需要过滤的源 IP 地址(IP 地址或者 IP 子网,多个地址用空格分隔)
- 目的地址：过滤的目的地址(IP 地址或者 IP 子网,多个地址用空格分隔)
- 源端口：选择 TCP 或 UDP，源端口或者端口范围(例: 8080 或 8080:8090),多个端口用空格分隔
- 目的端口：选择 TCP 或 UDP，目的端口或者端口范围(例: 8080 或 8080:8090),多个端口用空格分隔
- 动作：对过滤规则行为选择丢弃、接受、拒绝

案例：内网设备，IPv6 地址为 240e:399:129:f4:6914:3a99:c4da:aa3，需要开放 22（ssh 服务），23（telnet 服务），8080（网页服务）：
只需要创建一条放行（动作选择为 ACCEPT）过滤规则即可，配置协议为 IPv6，端口为 22 23 8080，就通过外网访问 IPv6 地址为 240e:399:129:f4:6914:3a99:c4da:aa3 的设备上运行的对应服务：

基础配置

状态	☒ 启用 ☐ 停用
规则描述	放行SSH TELNET WEB
协议族	IPv6
源区	WAN
目的区	LAN
协议	TCP
源地址	请输入 源地址
目的地址	240e:399:129:f4:6914:3a99:c4da:aa3
源端口	请输入 源端口
目的端口	22 23 8080
动作	ACCEPT

保存 取消

7.4 内网转发

该功能可以禁止 LAN 间访问，比如针对访客网络，可以禁止内网转发来实现可以访问外网但不能访问内网的功能

防火墙/内网转发 帮助 反馈

内网转发

禁止转发的接口

☐ 允许转发 ☒ 禁止转发

☐ lan ☐ lan1 ☐ lan1_17 ☒ lan1_18

保存

访客模式设置

例：在 LAN1 口下新建，vlan17，vlan18，在上图中禁止 lan1_18 内网转发，Lan、lan1、lan_17 可以互访，并可以访问 lan1_18，lan1_18 不能访问其他内网，可以访问外网。

7.5 共享阻断

共享阻断配置

禁止子网

☐ lan ☐ lan3 ☐ lan3_195

允许IP列表

IP、IP段(用“-”分隔)或子网(10.0.0.0/8) 添加

☐ 192.168.100.10 移除

保存

禁止子网：选择需要禁止的网口

允许 IP 列表：添加允许共享的 IP 或者 IP 段

7.6 连接数限制

状态 ☐ 启用 ☒ 停用

内网地址 [添加](#)
[移除](#)

协议 ☒ 所有 ☐ TCP ☐ UDP ☐ ICMP

外网端口
端口或者端口范围(例: 8080或8080:8090)

连接数 *

备注 *

- 状态：启用/停用连接数限制
- 内网地址：填写需要被限制的 IP 或者 IP 段
- 协议：所有、TCP、UDP、ICMP
- 外网端口：输入外网端口，默认不填是全端口
- 连接数：输入需要限制的最大数量
- 备注：填写相应注释

7.7 DMZ 服务

状态 ☒ 启用 ☐ 停用

接口 ▼

外网地址

内网地址 *

排除协议 ▼

排除端口
端口或者端口范围(例: 8080或8080:8090)

备注 *

- 状态：启用或停用
- 接口：选择所要使用的外网接口或者 ANY（全部）
- 外网地址：需要排除的外网 IP 地址
- 内网地址：需要做 DMZ 的内部 IP 地址
- 排除协议：选择协议（TCP、UCP、TCP+UDP）
- 排除端口：需要排除的端口号或端口号范围

8 VPN 服务

8.1 PPTP 服务器配置

8.1.1 基础配置

- PPTP 服务配置：功能是否启用；
- 本地地址：填写服务器 LAN 口的 IP 地址；
- 起始地址：地址池范围为客户端认证成功后虚通道被分配的 IP 地址
- DNS：DNS 域名解析服务器地址
- 工作模式：
 - A. NAT 模式：NAT 英文全称是“Network Address Translation”，中文意思是“网络地址转换”，允许一个整体机构以一个公用 IP 地址出现在 Internet 上。通过这种方法，您可以只申请一个合法 IP 地址，就把整个局域网中的计算机接入 Internet 中。
 - B. 路由模式：所有数据不进行 NAT 转发，直接将内网 IP 不做伪装的传送到外网，此模式适用于内网 IP 都为公网地址的时候使用。
- 服务线路：选择可以上网的外网接口
- 运行状态：显示该功能启用或停止状态

8.1.2 高级配置

高级配置 ^

8.2 L2TP 服务器配置

8.2.1 基础配置

基础配置

L2TP服务配置	☐ 开启 ☒ 关闭
本地地址	172.16.4.1
起始地址	172.16.4.2-200 IP范围,例如:172.16.3.2-200或172.16.3.1-255.254
DNS	172.16.4.1
工作模式	☒ NAT模式 ☐ 路由模式
服务线路	☐ lan ☒ wan ☐ lan1 ☐ lan1_17
运行状态	已停止

- L2TP 服务配置：功能是否启用；
- 本地地址：填写服务器 LAN 口的 IP 地址；
- 起始地址：地址池范围为客户端认证成功后虚通道被分配的 IP 地址
- DNS：DNS 域名解析服务器地址
- 工作模式：
- NAT 模式：NAT 英文全称是“Network Address Translation”，中文意思是“网络地址转换”，允许一个整体机构以一个公用 IP 地址出现在 Internet 上。通过这种方法，您可以只申请一个合法 IP 地址，就把整个局域网中的计算机接入 Internet 中。
- 路由模式：所有数据不进行 NAT 转发，直接将内网 IP 不做伪装的传送到外网，此模式适用于内网 IP 都为公网地址的时候使用。
- 服务线路：选择可以上网的外网接口
- 运行状态：显示该功能启用或停止状态

8.2.2 高级配置

高级配置

用户认证	☒ 开启 ☐ 关闭 关闭用户认证，则可以使用任意用户名密码拨号
认证方式	☒ 本地认证 ☐ RADIUS认证
认证协议	☒ pap ☒ chap ☒ mschap ☒ mschap-v2
MTU	1450
MRU	1450
异常断开检测时间	10 分钟
异常断开检测次数	3 次
MPPE加密	☒ 开启 ☐ 关闭
MPPE选项	☒ 拒绝40bit-MPPE请求 ☒ 拒绝56bit-MPPE ☒ 无状态
启用软件压缩	☐ 开启 ☒ 关闭
软件压缩选项	☒ 禁止BSD压缩 ☒ 禁止deflate压缩

保存

9 计费认证

9.1 认证子网配置

选择认证计费/认证子网配置，

如：需要认证的子网为 lan1_17（设定的 VLAN 17）是需要认证的网段，选择本地 portal 认证，保存生效。

认证全局配置

认证全局配置 ☒ MAC放行 ☐ IP放行 ☐ IP+MAC放行

保存

认证区域

接口	无认证	本地Portal认证
lan	☒	☐
lan1	☒	☐
lan1_17	☐	☒

本地 Portal 认证方式：

- 本地账号认证
- RADIUS 认证
- LDAP 认证
- 电话号码认证
- 短信验证码认证
- 一键认证
- 唯一密码认证
- 可跳转到“本地 Portal 认证”中选择需要的认证方式
- 注意 CMCC-Portal 认证不能和本地 Portal + RADIUS 的方式同时工作

9.2 本地套餐管理

本地套餐管理，配套本地账号认证使用，可做为账号流量设置的通用模板。

选择认证计费-本地套餐管理

- 1) 可修改 Default 本地套餐，点击编辑
- 2) 添加新的套餐内容，点击添加

智能流控
防火墙
VPN服务
认证计费
本地套餐管理
认证用户管理
PPPoE服务
微信认证
本地Portal认证

认证计费/本地套餐管理 帮助 反馈

CPU: 33.97% 内存: 33.77% 上行速率: 2.678 Mbps 下行速率: 5.676 Mbps

请输入内容 添加 高级配置 导入 导出 刷新 删除

操作	套餐名	总流量(MB)	套餐有效时长	自助服务	上行带宽(Kbps)	下行带宽(Kbps)
编辑	Default	0	长期有效	关闭	2000	2000

每页的行数: 20 1-1/1

套餐名

总流量(MB)
注：总流量为0 则不限制总流量

套餐有效时长单位 ☐ 分 ☐ 时 ☒ 天 ☐ 月

套餐有效时长
注：有效时长0 则套餐不计算时长

上行带宽(Kbps)

下行带宽(Kbps)

自助服务 ☐ 开启 ☒ 关闭

- 套餐名：输入套餐名（如：一天套餐，1 小时套餐）
- 总流量(MB)限制：0 为不限制
- 套餐有效时长单位：分、时、天、月
- 套餐有效时长：0 为不限制
- 上行带宽(Kbps)如：2000
- 下行带宽(Kbps)如：2000
- 自助服务选择关闭

9.3 认证用户管理

认证用户管理可实现本地 portal 认证、PPPoE 服务账号、PPTP、L2TP 客户端认证使用
设置 wifi 登录账号，提供给来访人员登录 WiFi 上网
选择认证计费——认证用户管理，点击编辑或者添加

认证计费/认证用户管理 帮助 反馈 CPU: 34.16% 内存: 33.48% 上行速率: 3.532 Mbps 下行速率: 11.411 Mbps

Q 请输入内容

☐	操作	状态	用户名	密码	认证协议	总流量(MB)	已使用流量(MB)	上行带宽(Kbps)	下行带宽(Kbps)	到期时间	套餐
☐	编辑	正常	yourname	yourpasswd	pptp / l2tp / pppoe / webportal	0	0	2000	2000	长期有效	自定义套餐

每页的行数: 20 1-1 / 1 < >

用户名	yourname
密码	yourpasswd
并发数量	3
	注：同时有多少用户可以登录，默认为1，为0时则不限制
短信通知	☐ 开启 ☒ 关闭
	注：选中则将账号信息发送到用户处
备注	-
可用认证方式	☒ PPTP ☒ L2TP ☒ PPPoE ☒ Webportal
套餐选择	自定义套餐
总流量(MB)	0
已使用流量(MB)	0
上行带宽(Kbps)	2000
下行带宽(Kbps)	2000
到期时间	2000/01/01 00:00:00 ☒ 长期有效
保存 取消	

- 用户名：如 yourname
- 密码：如 yourpasswd
- 并发数量：同一账号允许最大用户数同时登录，默认是 1，0 为则不限制
- 短信通知选择：关闭
- 备注：添加备注信息
- 可用认证方式：PPTP、L2TP、PPPoE、Webportal
- 套餐选择：可以选择本地套餐管理设置中设定好的模板，或者选择自定义不使用本地套餐管理的模板（参考 7.2）
- 到期时间：账号认证到期时间，到期后账号不能使用，需修改时间，勾选长期有效，则账号不设到期时间

9.4 PPPoE 服务

9.4.1 基础配置

基础配置

PPPoE服务	☒ 开启 ☐ 关闭
服务器IP	10.16.5.1
服务器子网掩码	255.255.0.0
主DNS	10.16.5.1
次DNS	223.5.5.5
PPPoE 服务名称	XinWei-PPPoE
允许任意服务器名接入	☒ 开启 ☐ 关闭
只允许拨号接口 PPPoE接入	☐ 开启 ☒ 关闭
服务线路	☐ lan ☐ lan1 ☒ lan1_17
运行状态	运行中

- PPPoE 服务：开启/关闭
- 服务器 IP：默认或按照内网 IP 填写
- 服务器子网掩码：默认或按照内网 IP 填写
- 主 DNS：DHCP 服务器自动分配给客户机的主 DNS 服务器地址
- 次 DNS：DHCP 服务器自动分配给客户机的次 DNS 服务器地址
- PPPoE 服务名称：PPPoE 服务器名称信息
- 允许任意服务器名接入：选择开启，否则需要客户端正确配置 pppoe 服务器名称
- 只允许拨号接口使用 PPPoE 接入：使用此功能后，只有通过 PPPoE 拨码的客户端才能访问路由器
- 拨号线路：客户端拨号所使用的接口（内网 IP 端口）

9.4.2 高级配置

高级配置 ^

用户认证	☒ 开启 ☐ 关闭	关闭用户认证，则可以使用任意用户名和密码拨号
到期仍可拨号	☐ 开启 ☒ 关闭	
认证方式	☒ 本地认证 ☐ RADIUS认证	
认证协议	☒ pap ☒ chap ☒ mschap ☒ mschap-v2	
MTU	1450	
MRU	1450	
异常断开检测时间	10	分钟
异常断开检测次数	3	次
MPPE加密	☒ 开启 ☐ 关闭	
MPPE选项	☒ 拒绝40bit-MPPE请求 ☒ 拒绝56bit-MPPE ☒ 无状态	
启用软件压缩	☐ 开启 ☒ 关闭	

- 用户认证：点击开启表示功能将可以使用，选择关闭此功能将不能使用
- 到期仍可拨号：开启/关闭
- 认证方式：选择本地认证，用户的账号为“认证用户管理”中存在的账号，若使用 radius，账号将使用 radius 服务器上的账号
- 认证协议：pap、chap、mschap、mschap-v2，默认全选
- MTU:1450
- MRU:1450
- 异常断开检测时间：默认 10 分钟
- 异常断开检测次数：默认为 3 次。
- MPPE 加密：开启/关闭
- MPPE 选项：拒绝 40bit-MPPE 请求、拒绝 56bit-MPPE、无状态，默认全选
- 启用软件压缩：开启/关闭
- 配置完成后，用户可通过拨号连接方式连接网络。

9.5 微信认证

本功能因腾讯微信连 WIFI 服务关闭的原因无法正常使用

9.6 本地 Portal 认证

9.6.1 展示配置

展示配置

欢迎信息	请输入欢迎信息，如：欢迎使用
联系信息	请输入联系信息，如：有问题请联系XXX
版权信息	江门市拓达有限公司
登录按钮提示	登录上网
自助按钮提示	上网续费
图片展示	图片大小不超过200K,图片名称不要含有空格等特殊字符 0 (0.0 B) +

- 欢迎信息：填写欢迎信息，如：登录 WiFi 上网
- 联系信息：填写帮助联系方式
- 版权信息：填写提供 WiFi 单位信息，如：todaair
- 登录按钮提示：填写登录按钮信息，如：登录上网
- 自助按钮提示：填写上网自助按钮信息，如：上网续费，自助注册
- 图片展示：可以上传门店照片或者广告图片，最多支持 5 张图片，图片格式为 JPG 或 PNG

9.6.2 认证配置

1) 本地认证方式

认证配置

认证方式	本地认证
本地自助终端	☒ 开启 ☐ 关闭
本地自助终端提示	Self-Service 提示：本地自助终端路径为 /user
成功跳转页面	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天 2
流量更新检测时间	30 分钟 设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板

认证方式：本地认证

本地自助终端：启用/关闭，建议关闭

本地自助终端提示：自助按钮提示内容

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

2) 电话号码认证

认证方式：电话号码认证

导出电话号码 清空电话号码

成功跳转页面：http://www.todaair.com

完整HTTP地址，例如：https://www.example.com/

认证时效：☐ 分钟 ☒ 小时 ☐ 天

2

流量更新检测时间：30 Minutes

设定时间内没有流量则自动下线用户

HTTPS跳转：☐ 开启 ☒ 关闭

模板：☒ 初始模板 ☐ 自定义模板

保存 取消

认证方式：电话号码认证（导出电话号码，清空电话号码）

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

3) 一键认证

认证方式：一键认证

成功跳转页面：http://www.todaair.com

完整HTTP地址，例如：https://www.example.com/

认证时效：☐ 分钟 ☒ 小时 ☐ 天

2

流量更新检测时间：30 Minutes

设定时间内没有流量则自动下线用户

HTTPS跳转：☐ 开启 ☒ 关闭

模板：☒ 初始模板 ☐ 自定义模板

保存 取消

认证方式：一键认证

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10

分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

4) 唯一密码认证

认证方式	唯一密码认证
密码	*****
成功跳转页面	http://www.todaair.com
	完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天
	2
流量更新检测时间	30 Minutes
	设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板
保存 取消	

认证方式：唯一密码认证

密码：认证页面中通过认证密码

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

5) WIFIDOG 认证

内网搭建了 WIFIDOG 认证服务器时，网关可以连接 WIFIDOG 服务器搭配 RADIUS 认证实现 WIFIDOG 认证上网

选择认证计费——本地 Portal 认证

认证配置	
认证方式	RADIUS认证
自助服务	http://www.example.com
	完整HTTP地址，例如：https://www.example.com/
成功跳转页面	http://www.example.com
	完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天
	2
流量更新检测时间	30 分钟
	设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板
保存 取消	

认证方式：RADIUS 认证

自助服务：完整 HTTP 地址，例如：https://www.example.com/

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

WIFIDOG 服务器参数配置，点击认证计费——WIFIDOG 认证

服务器地址	192.168.100.1 或www.example.com
服务器端口	1024 ~ 65500
认证接口	uri, 例如 user/path/1.html
保活接口	uri, 例如 user/path/1.html
跳转地址	例如：http://www.example.com 完整HTTP地址，例如：https://www.example.com/
注册ID	请输入注册ID

保存

帮助提示：

请严格遵循authpuppy与wifidog的通信协议

6) CMCC-WEB 认证

内网搭建了 CMCC-WEB 认证服务器时，网关可以连接 CMCC-WEB 服务器搭配 RADIUS 认证使用 CMCC-WEB 上网

认证方式：RADIUS 认证

自助服务：完整 HTTP 地址，例如：https://www.example.com/

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

认证方式	RADIUS认证
自助服务	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
成功跳转页面	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天 2
流量更新检测时间	30 分钟 设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板
保存 取消	

点击 认证计费——CMCC-WEB 认证，填写相关服务器参数，保存。

认证URL	请输入以http或https的认证URL
Portal服务器IP	请输入Portal服务器IP
管理IP	请输入与Portal服务器通信的IP 本设备用于和Portal 服务器通信的IP
流量更新检测时间	设定时间内没有流量则自动下线用户
保存	

7) RADIUS 认证

内网搭建了 RADIUS 认证服务器时，网关可以连接 RADIUS 服务器使用账号认证上网
认证方式：RADIUS 认证

自助服务：完整 HTTP 地址，例如：https://www.example.com/

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

认证配置

认证方式	RADIUS认证
自助服务	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
成功跳转页面	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天 2
流量更新检测时间	30 分钟 设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板
保存 取消	

RADIUS 服务器参数配置，点击认证计费——RADIUS 配置

RADIUS服务器IP地址	请输入RADIUS服务器IP地址 与RADIUS服务器通信的合法IP地址，例如：192.168.9.250
共享密钥	1-255个字符 与RADIUS服务器通信的共享密钥
记账端口	请输入数字，0代表不受限制 RADIUS记账端口，默认1813
认证端口	RADIUS认证端口，默认1812 RADIUS认证端口，默认1812
NAS标识	请输入NAS标识 与NAS设备通信的合法IP地址或字符串标识
绑定IP	请输入指定与Radius服务器通信的IP(可默认) 本设备用于和Radius 服务器通信的IP
连接状态	网关与RADIUS连接失败
保存 检查连接	

8) LDAP 权限认证

内网搭建了 LDAP 统一账号认证服务器时，网关可以连接 LDAP 服务器使用内网 LDAP 账号认证上网

认证配置

认证方式	LDAP权限认证
成功跳转页面	http://www.example.com 完整HTTP地址，例如：https://www.example.com/
认证时效	☐ 分钟 ☒ 小时 ☐ 天 2
流量更新检测时间	30 分钟 设定时间内没有流量则自动下线用户
HTTPS跳转	☐ 开启 ☒ 关闭
模板	☒ 初始模板 ☐ 自定义模板
保存 取消	

认证方式：LDAP 权限认证

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功连接上网时长，有效时间单位可选分钟、小时、天

流量更新检测时间：设定时间内没有流量则自动下线认证用户，可选关闭、5 分钟、10 分钟、30 分钟

HTTPS 跳转：启用/关闭，建议关闭

模板：选择初始模板

LDAP 服务器参数配置

点击 认证计费——LDAP 配置



LDAP 配置表单截图，包含以下字段：

- LDAP 服务器地址：请输入 LDAP 服务器地址，IP 例 192.168.1.1
- LDAP 服务器端口：请输入接口，例：LDAP 为 389，LDAPS 为 636
- Base DN：请输入 dc=domain, dc=com
- 绑定类型：匿名
- 保存按钮

LDAP 服务器地址：输入 LDAP 服务器 IP 地址

LDAP 服务器端口：输入 LDAP 服务器端口号，LDAP 为 389，LDAPS 为 636

Base DN：请输入 dc=domain, dc=com

绑定类型：匿名，使用者账号，指定 DN

9) 短信验证码认证

选择认证计费——本地 Portal 认证



短信验证码认证配置表单截图，包含以下字段：

- 认证方式：短信验证码认证
- 成功跳转页面：http://www.example.com
- 完整 HTTP 地址，例如：https://www.example.com/
- 认证时效：分钟、小时、天
- 流量更新检测时间：30 分钟
- 设定时间内没有流量则自动下线用户
- HTTPS 跳转：开启、关闭
- 模板：初始模板、自定义模板
- 保存、取消按钮

认证方式：短信验证码认证

成功跳转页面：填写 WiFi 认证成功之后的跳转页面，如：www.todaair.com

认证时效：填写 WiFi 认证成功有效时间，时间单位可选分钟、小时、天

流量更新检测时间：可选关闭、5 分钟、1 分钟、30 分钟，设定时间内没有流量则自动下线用户

HTTPS 跳转：选择关闭

HTTPS 跳转：启用/关闭，建议关闭
模板：选择初始模板

短信网关参数配置

网关服务商可选：Clickatell、阿里大于、互亿无线

短信网关选择

☐ Clickatell ☒ 阿里大于 ☐ 互亿无线

AppKey

请输入AppKey

密码

请输入密码

短信签名

请输入短信签名

开启模板ID

请填写在阿里平台上对应的模板ID

通告模板ID

请填写在阿里平台上对应的模板ID

验证码模板ID

请填写在阿里平台上对应的模板ID

开户模板

请输入平台上对应模板内容

通告模板

请输入平台上对应模板内容

验证码模板

请输入平台上对应模板内容

确定

为了更好的适配不同短信网关平台，需要对短信的模板做格式要求，请将设备端需要填充的内容统一使用##表示，变量名称请使用模板中定义的名称，以便成功发送。

例如下面的样式：

- 1、 开户短信模板：您的账号是：#account#，密码是：#password#，使用的套餐是：#custom#，上下行速率分别是：#upload# 和#download#，到期时间是：#expire#
 - 2、 到期通告短信模板：您的账号#account# 即将到期，请及时续费！
 - 3、 验证码短信模板：您的验证码:#code#，一次登录即可享用免费 WiFi！
- 备注：所有的模板内容须先在短信网关平台上面审核通过，才能使用

9.7 白名单配置

认证白名单可以通过添加 MAC 地址或者 MAC 地址两种方式，建议使用 MAC 方式

认证计费/白名单配置

CPU: 23.48% 内存: 47.33% 上行速率: 3.877 Mbps 下行速率: 21.711 Mbps

MAC白名单 IP白名单

请输入内容

添加 批量添加 导入 导出 反选 删除

	操作	MAC地址	备注
没有可用数据			

选择 MAC 白名单或 IP 白名单，点击添加或批量添加按钮，填写地址。

MAC地址 请输入MAC地址

备注 请输入备注

确定 取消

IP地址 请输入IP地址

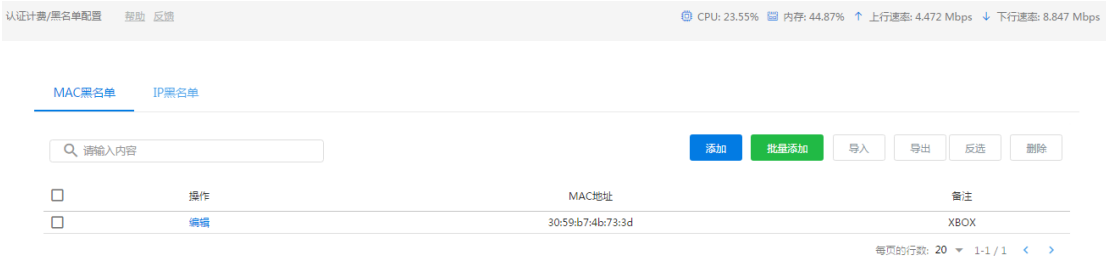
备注 请输入备注

确定 取消

认证上网白名单，添加之后 mac 或者 ip 地址，不需要认证即可上网。

9.8 黑名单配置

黑名单可以通过添加 mac 地址或者 ip 地址两种方式



选择 MAC 黑名单或者 IP 黑名单，点击添加或批量添加按钮，

认证上网黑名单，添加之后该 mac 或者 ip 地址，无法上网。
网关支持单个 ip 或者 mac 添加，或者批量添加

9.9 账户到期通告

开启之后，账号认证到期，系统会自动通过发出公告。

到期短信通知：如果搭配了短信平台使用，可以开启短信通知

到期 Portal 通知：使用 Portal 页面进行公告

Portal 通知后跳转地址：通知后跳转的 WEB 页面，如：https://www.baidu.com

到期通告间隔时间：多长时间公告一次，单位为小时

自动重置时间：指定时间内 Portal 通知没有成功，则自动停止对应用户的到期通知

通告端口：80、8080、ALL

通知内容：公告内容，可自行对通知内容进行编辑

9.10 本地公告

本地公告 ☒ 开启 ☐ 关闭

公告线路 ☐ lan ☐ lan1 ☐ lan1_17

通知内容

B I U L T - 格式化工具 字体大小 默认字体

保存

将本地公告开启，选择需要公告的线路，添加需要公告的内容

10 无线管理

10.1 无线状态

10.1.1 开启 AC 管理功能

- 点击无线管理——无线状态
- AC 功能：选择开启，才能管理 ap
- AC-AP 自动对时：选择开启
- AP 自动升级：选择关闭
- AP 定时重启：关闭/开启(设定 AP 重启周期)
- AC 定时重启：关闭/开启(设定 AC 重启周期)
- 无线自动优化：关闭/开启
- AP 看门狗：选择关闭
- 国家统一配置：按当前国家地区选择

全局配置

AC功能	☒ 开启 ☐ 关闭
AC-AP自动对时	☐ 开启 ☒ 关闭
AP自动升级	☐ 开启 ☒ 关闭
AP定时重启	☒ 开启 ☐ 关闭
	每天
AP重启时间	04:30
AC定时重启	☒ 开启 ☐ 关闭
	每天
AC重启时间	04:00
无线自动优化	☒ 开启 ☐ 关闭
AP看门狗	☐ 开启 ☒ 关闭
国家统一配置	中国

保存

10.2 模板分组

AP 模板可以批量设置 AP 的 SSID、加密，添加多个 SSID 等参数。



点击无线管理—模板分组，若 AP 绑定默认模板分组，选择默认分组 default 修改编辑。

10.2.1 2.4g 无线设置



- 无线名称：wifi 名称
- 加密方式：无密码、WPA-PSK、WPA2-PSK、WPA-PSK+ WPA2-PSK，选择后三个，可以填写无线加密的密码
- 高级特性：无线用户隔离（连接到此 WIFI 的终端都不能互访）、隐藏无线（默认不勾选），一键扫码（默认不勾选）
- 最大用户：AP 最大接入终端数
- 绑定 VLAN：默认为 0
- 如果需要多个 ssid，点击添加即可创建多个 ssid。

10.2.2 高级配置

高级配置 ^

信道	AUTO
漫游信号阈值	-95
U-APSD智能节电	☐ 开启 U-APSD是新型节能处理方式，能进一步提升终端节能能力，但由于部分终端对U-APSD功能的支持存在问题，所以这种情况下需要去关闭U-APSD功能。
RTS/CTS握手信号阈值	2347 解决数据冲突。当数据长度超过这个值时无线接入点需要先向接受端发rts信号，得到接受端反馈后才能发送数据。
信号强度	
频宽	AUTO
5G优先	☒ 开启 注：开启后2.4G和5G配置相同时，无线终端会优先连接5GWIFI
无线多媒体	☒ 开启
GBK无线名称	☐ 开启 开启GBK 可以解决部分终端（电脑等）显示中文无线名称乱码的问题
黑白名单	

- 信道：推荐选择 auto 自动调节，开启之后 ap 信道会自动调节。
- 漫游信号阈值：当无线终端达到设定的值 ap 就会断开无线连接，让终端漫游到下一个 ap 中。根据现场环境调节，推荐范围-80 到-85。
- U-APSD 智能节电：U-APSD 是新型节能处理方式，能进一步提升终端节能能力，但由于部分终端对 U-APSD 功能的支持存在问题，所以多数情况下按实际环境关闭 U-APSD 功能。
- RTS/CTS 握手信号阈值：解决数据冲突。当数据长度超过这个值时无线接入点需要先向接受端发 rts 信号，得到接受端反馈后才能发送数据。默认 2347 即可。
- 信号强度：WiFi 发射功率，默认为自动，为设备的最大功率，可根据现场环境调节信号强度。
- 频宽：WiFi 频宽，默认为自动，为 20MHz/40MHz，或者根据现场环境调节 20MHz。
- 5G 优先：开启后 2.4G 和 5.8GWIFI 配置相同时，若 ap 支持 5.8g 无线终端会优先连接 5GWIFI
- 无线多媒体：开启后，可以提高无线多媒体数据传输性能，默认开启。
- GBK 无线名称：开启 GBK 可以解决部分终端（电脑等）显示中文无线名称乱码的问题。
- 黑白名单：无线接入黑白名单，白名单模式只有白名单内的 mac 地址才能接入 WiFi，黑名单模式只有黑名单内的 mac 地址不能接入 WiFi。

10.2.3 5.8 无线设置

2.4G 5G

无线配置

添加

1

无线名称 请输入无线名称

加密方式

无线密码 请输入无线密码

高级特性 ☐ 无线用户隔离 ☐ 隐藏无线 ☐ 一键扫码

最大用户 请输入最大用户

绑定VLAN 可选, 0 到4094 , 0表示不绑定

删除

- 无线名称: wifi 名称
- 加密方式: 无密码、WPA-PSK、WPA2-PSK、WPA-PSK+ WPA2-PSK, 选择后三个, 可以填写无线加密的密码
- 高级特性: 无线用户隔离 (连接到此 WIFI 的终端都不能互访)、隐藏无线 (默认不勾选), 一键扫码 (默认不勾选)
- 最大用户: AP 最大接入终端数
- 绑定 VLAN: 默认为 0
- 如果需要多个 ssid, 点击添加即可创建多个 ssid。

注:

5.8G 的无线高级配置与 2.4G 的配置一致

如需要添加不同的模板分组, 点击模板分组中的添加按钮

10.3 AP 列表

打开无线管理——AP 列表, 全选所有 AP 或者选择需要修改 AP。

无线管理/AP列表 帮助 反馈

CPU温度: +7.0°C CPU: 4.66% 内存: 34.46% 上行速率: 1.380 Mbps 下行速率: 16.888 Mbps

请输入内容

自动刷新已停止 默认模板 反选 重启AP 绑定分组 解绑 网络配置 配置功率 配置信道 配置频宽

指定AC地址 导出AP信息 升级 同步管理密码 刷新

☒	型号	在线状态	设备名称	IP地址	MAC地址	已运行	模板分组
☒	IN3212Y-H	离线	AP	192.168.122.32	74:96:37:06:A4:54	0Day 0h6m	-
☒	IN3212Y-H	离线	TodaAir	192.168.122.31	74:96:37:06:a4:99	0Day 0h3m	-
☒	RF-WND-HS25E	在线	IN1212Y-H	192.168.121.93	74:96:37:00:00:01	0Day 3h53m	default
☒	IN1235KYW-H	在线	1235	172.16.10.105	74:96:37:06:0fdf	1Day 7h42m	default
☒	IN3212Y-H	在线	AP	172.16.10.106	74:96:37:09:5e:06	0Day 18h38m	default

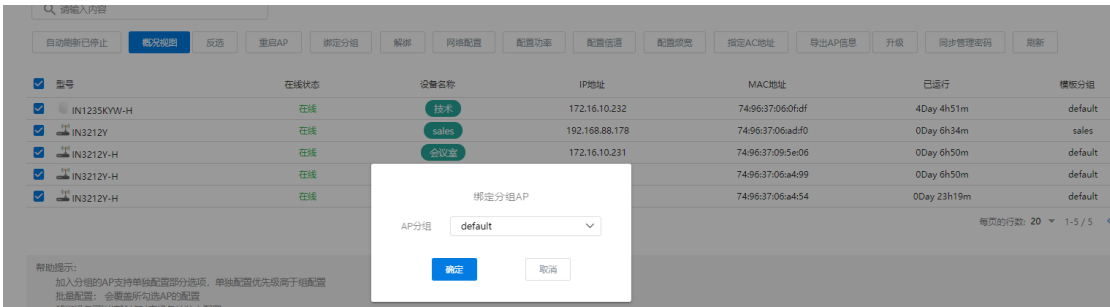
注:

加入分组的 AP 支持单独配置部分选项, 单独配置优先级高于组配置

批量配置: 会覆盖所勾选 AP 的配置

解绑设备可以清除掉对应设备的独立配置

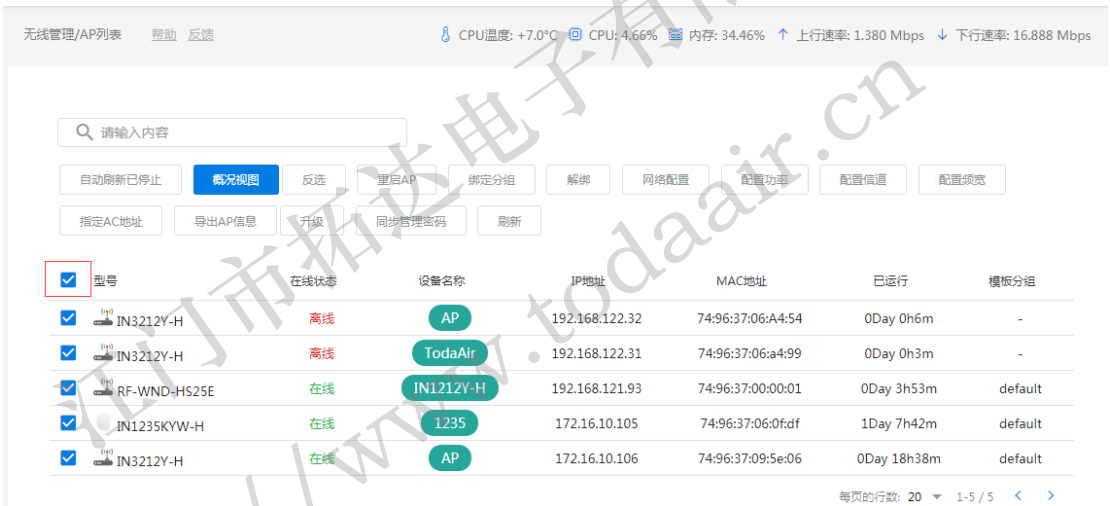
10.3.1 AP 绑定默认 WiFi 模板设置



点击绑定分组按钮，选择 AP 使用模板分组，保存设置。

10.3.2 ap 重启

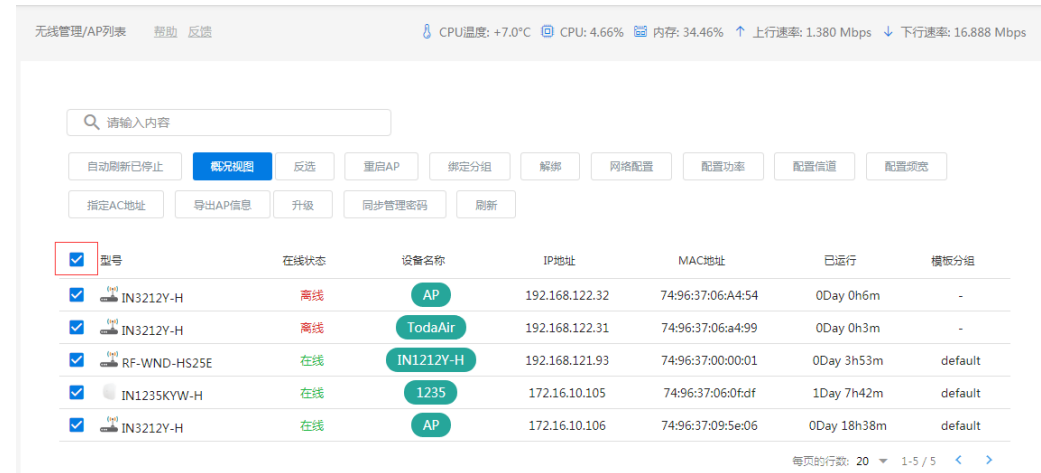
打开无线管理/AP 列表，全选所有 AP 或者选择需要重启 AP。



点击重启 AP 按钮，即可下发重启 AP 命令（需要 AP 在线）

10.3.3 移除 AP

打开无线管理/AP 列表，全选所有 AP 或者选择需要移除 AP。



点击解绑按钮，即可移除 AP（不需要 AP 在线）

10.3.4 固定 AP 的 ip 获取方式

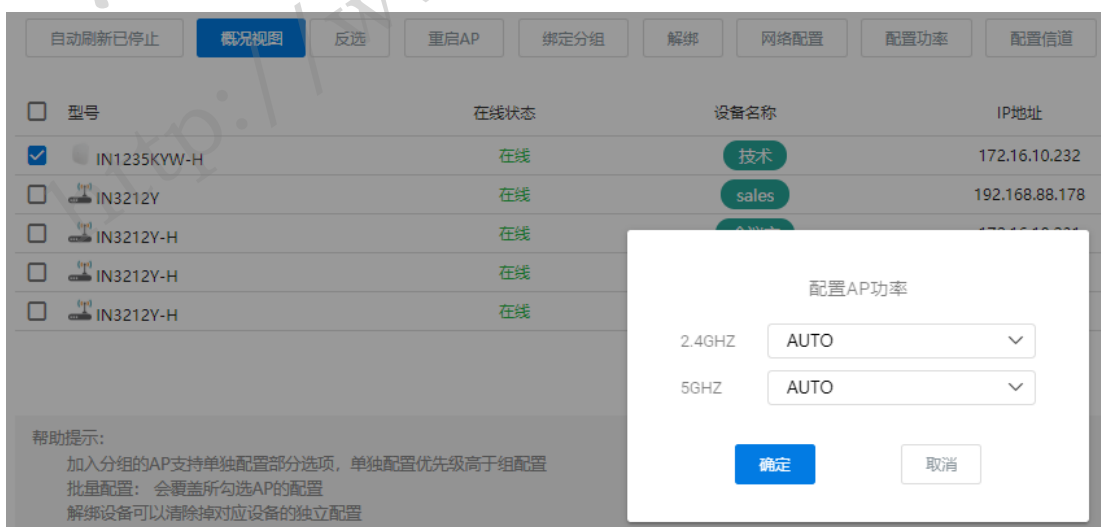
AP 可以通过网关来指定 AP 的两种 ip 获取方式，自动获取 ip 上网或固定 ip 地址上网。打开无线管理/AP 列表，选择修改上网方式的 AP。



点击网络配置，选择动态地址或者静态地址，默认动态地址，点击确定，网关就会统一下发上网模式配置。（需要 ap 在线）

10.3.5 固定 ap 的发射功率

ap 可以通过网关来指定 ap 的发射功率，可选自动发射功率或固定发射功率。打开无线管理/AP 列表，全选所有 AP 或者选择需要修改发射功率的 AP。



点击配置功率按钮，选择需要修改的 2.4g 或者 5ghz 发射功率值，默认自动发射功率，点击确定，网关就会统一下发 AP 发射功率配置。（需要 AP 在线）

10.3.6 固定 AP 的无线信道

AP 可以通过网关来统一指定 ap 的无线信道，可选自动 AP 信道或指定 AP 固定信道。
打开无线管理/AP 列表，全选所有 AP 或者选择需要修改发射功率的 AP。



点击配置信道，选择需要修改的 2.4g 或者 5G 无线信道，默认自动无线信道，点击确定，网关就会统一下发 AP 发射功率配置。（需要 AP 在线）

10.3.7 固定 AP 的无线频宽

AP 可以通过 AC 管理统一指定 AP 的无线频宽，可选自动频宽或固定 AP 无线频宽。
打开无线管理/AP 列表，全选所有 AP 或者选择需要修改无线频宽的 AP。

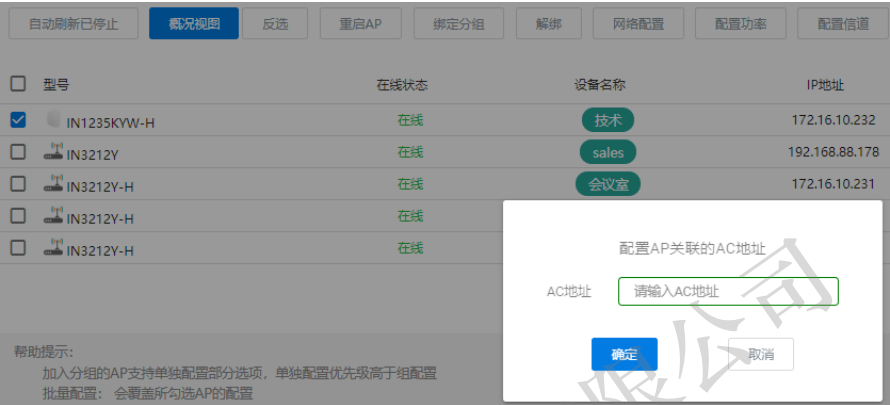


点击配置频宽，选择需要修改的 2.4g 或者 5ghz 无线频宽，默认自动无线频宽，点击确定，网关就会统一下发 AP 的无线频宽配置。（需要 AP 在线）

10.3.8 固定 AP 的 AC 指向

AP 可以通过 AC 管理来指定 AC 的 IP 地址指向，指向 AC 地址正常，否则指向地址不正确会导致 AP 离线，需要进入 AP 的 WEB 管理页面重新修改 AP 的 AC 指向地址。

打开无线管理/AP 列表，全选所有 AP 或者选择需要修改上网方式的 AP。



点击指向 AC 地址，输入 AC 地址，点击确定，网关就会统一下发配置。（AP 在线）

10.3.9 升级 AP

升级 AP 可以通过网关来统一升级 AP 固件版本，需要在固件管理界面里上传固件(相同的固件型号，否则会导致 AP 升级失败，无法启动) 到网关。



点击无线管理——固件管理——添加按钮

设备型号：选择需要添加固件固件型号

固件版本号：填写固件版本号

备注：填写固件版本备注

固件：上传固件文件

打开无线管理/AP 列表，全选所有 AP 或者选择需要升级 ap 固件版本的 AP。



点击升级按钮，网关就会统一下发固件升级 AP 刚上传到网关的固件。（AP 在线）

10.3.10 统一 ap 的登入管理密码

AP 通过 AC 管理修改 AP 的 WEB 管理密码，AP 密码会同步为网关登入密码。
打开无线管理/AP 列表，全选所有 AP 或者选择需要修改上网方式的 AP。



点击同步管理密码，提示点击确定，AC 管理统一修改 AP 的 WEB 管理密码。（需要 AP 在线）

10.4 无线优化



- 点击一键开局按钮，ap 会自动扫描环境的最优信道，扫描完成点击保存最优结果按钮，保存优化结果。
- 点击优化中按钮，ap 就会自动扫描附近的 WiFi 信息。
- 操作：点击查看干扰，即可打开扫描到附近的 WiFi 信息。
- 序列号：ap 序列号
- 在线状态：离线或者在线
- 优化状态：显示附近 WiFi 信息扫描完成状态
- Mac 地址：ap 的物理 mac 地址
- 2.4g 信道：ap 所使用的 2.4g 无线信道
- 5.8g 信道：ap 所使用的 5.8g 无线信道
- 2.4g 噪底：2.4gWiFi 漫游阈值
- 5.8g 噪底：5.8gWiFi 漫游阈值
- 2.4g 干扰源：附近的 2.4gWiFi 数量
- 5.8g 干扰源：附近的 5.8gWiFi 数量

10.5 黑白名单

黑白名单适用于无线管理——模板分组——高级配置——黑白名单
点击添加，选择黑名单或白名单

黑名单：禁止 MAC 名单用户通过无线连接

白名单：允许 MAC 名单用户通过无线连接

无线管理/黑白名单/编辑 帮助 反馈

名称

12

策略

☒ 黑名单 ☐ 白名单

MAC列表

11:22:33:44:55:66

保存

取消

注释：

一条 MAC 记录占一行，可以附带备注说明加在 MAC 后面，用空格隔开，也可以不加入说

明

示例一：AA:00:00:00:00:01 路由 MAC

示例二：AA:00:00:00:00:02

11 CPE 管理（无线网桥管理）

11.1 全局配置

全局配置

CPE定时重启

☒ 开启 ☐ 关闭

CPE重启时间

每天

CPE重启时间

04:30

无线自动优化

☒ 开启 ☐ 关闭

传输场景

☒ 通用场景 ☐ 电梯场景 ☐ 点对点传输场景 ☐ 移动漫游场景 ☐ 自定义场景

保存

- CPE 定时重启：开启/关闭，开启后，可选择天，周，月重启时间
- CPE 重启时间：具体每天的重启时间
- 无线自动优化：通过网关扫描附近干扰和网桥使用的频率，自动优化分配网桥使用的频率
- 传输场景：通用场景、电梯场景、点对点传输场景、移动漫游场景、自定义场景

11.2 CPE 列表

显示同一局域网中的 CPE，CPE 需要跟网关同一网段，面相关 CPE 配置为实时下发,下发后配置不会保存在 AC 设备中。

Q 请输入内容

自动刷新已停止

概况视图

反选

配置信道

配置功率

重启CPE

删除CPE

导出CPE信息

同步管理密钥

刷新

☐	型号	模式	群组	在线状态	设备名称	IP地址	MAC地址	已运行
☐	CPE-TodaAir	接收端	群组 1	在线	TD44-H-DIP	172.18.36.2	74-96-37-06-66-76	3Day 9h0m
☐	CPE-TodaAir	基站	群组 1	在线	TD44-H-DIP	172.18.36.1	74-96-37-00-23-46	0Day 10h29m

每页的行数: 20 1-2 / 2

帮助提示:

国家码不同的设备,不能同时配置信道,工作频段不同的设备,不能同时配置信道
由于CPE使用环境较为复杂,当前页面相关CPE配置为实时下发,下发后配置不会保存在AC设备中

- 型号：网桥具体的型号规格
- 模式：基站(发射端)、接收端
- 群组：不同分组组别
- 在线状态：在线/离线
- 设备名称：可修改设备备注信息
- IP 地址：网桥对应的 IP 地址
- MAC 地址：网桥的 MAC 地址
- 已运行：网桥通电运行时间

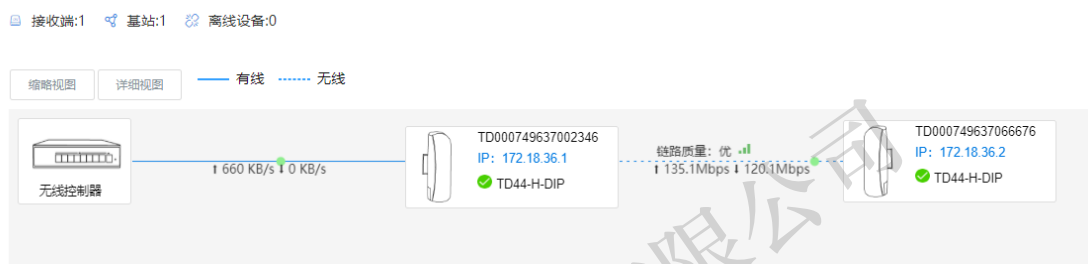
11.2.1 管理 CPE

- 自动刷新：启用后，10 秒自动刷新一次
- 视图：概况视图、无线视图、详情视图
- 反选：对已勾选的 CPE 反向选择
- 配置信道：勾选基站 CPE，修改需要的信道，不需要修改接收端信道
- 配置功能：勾选需要修改 CPE，修改无线发射功率

- 重启 CPE：勾选需要重启的 CPE，下发重启指令
- 删除 CPE：勾选需要删除的 CPE，删除视图中的 CPE，在线 CPE 会重新上线
- 同步管理密码：AC 管理统一修改 CPE 的 WEN 管理密码
- 刷新：刷新当前页面信息

11.2.2 网络拓扑

显示 CPE 列表中的网桥拓扑，链路质量，无线速率，当前传输速率，CPE 信息
绿色表示网桥在线正常，灰色表示网桥离线。



12 统一云控

12.1 统一云控

通过注册拓达云平台: <http://cloud.todacore.com>, 参考将平台账户里的绑定码输入到统一云控——绑定码中, 可通过平台中的远程通道, 远程访问网关设备。

设备序列号 TDAIRO

绑定码

备注名 NGROUTER

保存

12.2 智能组网

此功能目前测试中

13 应用中心

13.1 UPnP 管理

UPnP 是英语 Universal Plug and Play 的首字母缩写，一般翻译成通用即插即用。路由器 UPnP 功能用于实现局域网计算机和智能移动设备，通过网络自动彼此对等连接，而且连接过程无需用户的参与。

启用 UPnP 功能，需重启路由器。同时在 Windows 操作系统需启用 SSDP Discovery Service 及 Universal Plug and Play Device Host 两项服务。按下 win+R 打开运行，键入：services.msc 点击确定打开服务。

不建议普通用户开启 UPnP 功能，会增加网关的负载

网关开启 UPnP 方式：点击应用中心——UPnP 管理——服务配置



UPnP即插即用服务 ☒ 开启

默认线路设置 wan

离线自动清理 ☒ 开启

- UPnP 即插即用服务：开启
- 默认线路设置：选择外购线路
- 离线自动清理：开启

13.2 动态域名

动态域名服务可以在公网地址变化时实时更新域名解析记录，方便随时通过域名来获取您的设备公网地址与访问设备或与设备连接服务。您可以通过向列表中的动态域名服务商来申请使用该服务，具体配置参数请联系服务商，目前支持：阿里云 DNS、dynv6.com、dyndns.org、Oray.net、3322.org



服务商 Oray.net

是否开启 ☒ 是 ☐ 否

域名 www.aliyun.com *

账号 请输入账号 *

密码 请输入密码 *

协议族 ☐ IPv4 ☒ IPv6

解析类型 ☐ 接口 ☒ MAC地址

解析MAC地址 请输入MAC地址 *

注：

- 该项服务需要您的网络运营商给您的设备分配了公网地址，具体情况可咨询为您办理接入服务的网络运营商
- 可以通过 MAC 地址解析方式来将设备下接的设备地址解析到指定的域名上，实现内网地址的暴露，此时可以结合主机放行(IPv6)、过滤规则(IPv4)功能来使用
- IPv4/IPv6 解析支持、收费情况各个动态域名服务商不一样，请参考动态域名服务商说明

13.3 内网穿透

描述	请输入描述
是否开启	☒ 是 ☐ 否
服务器地址	*.everylinking.cn
服务器端口	默认4443
服务器token	请输入服务器提供的唯一Token
用户域名	请输入用户域名
协议类型	HTTP
本地地址	请输入本地地址
本地端口	请输入本地端口

- 描述：输入备注描述
- 是否开启：是/否
- 服务器地址：请向服务商来申请使用该服务
- 服务器端口：默认 4443
- 服务器 token：请输入服务器提供的唯一 Token
- 用户域名：请输入用户域名
- 协议类型：HTTP、HTTPS、TCP
- 本地地址：请输入本地地址
- 本地端口：请输入本地端口

13.4 网络唤醒

Wake-on-LAN 简称 WOL 或 WoL，中文多译为“网上唤醒”、“远程唤醒”技术。WOL 是一种技术，同时也是该技术的规范标准，它的功效在于让已经进入休眠状态或关机状态的计算机，透过局域网（多半为以太网）的另一端对其发令，使其从休眠状态唤醒、恢复成运作状态，或从关机状态转成引导状态。此外，与 WOL 相关的技术也包括远程下令关机、远程下令重启等相关的遥控机制。

立即执行唤醒

MAC地址

定期唤醒列表

☐	操作	MAC	终端状态	周期	日期	时间	备注	计划任务
没有可用数据								

立即执行唤醒：输入 MAC 地址，执行网络唤醒

MAC	请输入MAC地址	*
周期	一次	▼
日期		📅 *
时间		🕒 *
备注	请输入备注	

定期唤醒列表：点击添加，输入 MAC 地址，选择唤醒的周期和当天唤醒时间。

14 安全中心

14.1 健康检测

可对当前内网网络进行监测，包括内网 DHCP 监测、内网 PPPoE 监测、IP 冲突监测、内网环路监测，监测周期为 10 秒、60 秒、300 秒

主动健康监测
 ☒ 内网DHCP监测
 ☒ 内网PPPoE监测
 ☒ IP冲突监测
 ☒ 内网环路监测

监测周期

 秒

14.2 路由体检

在健康检测开启的情况下，可以对内网问题进行快速排查。

全面路由体检 快速排查您的设备

检测已完成

检测中...
检测系统健康状态

内存检测	检测已完成 内存使用: 总内存: 254.7MB 已使用: 96.4MB(I/O缓存 34.5MB) 未使用: 158.3MB 使用率: 38%
线路检测	检测已完成 正常: 接口wan 域名: www.baidu.com DNS耗时: 16 ms HTTP耗时: 38 ms 正常: 接口wan 域名: www.taobao.com DNS耗时: 12 ms HTTP耗时: 27 ms 正常: 接口wan 域名: www.qq.com DNS耗时: 16 ms HTTP耗时: 28 ms 正常: 接口wan 域名: www.jd.com DNS耗时: 18 ms HTTP耗时: 22 ms 正常: 接口wan5 域名: www.baidu.com DNS耗时: 13 ms HTTP耗时: 31 ms 正常: 接口wan5 域名: www.taobao.com DNS耗时: 10 ms HTTP耗时: 25 ms 正常: 接口wan5 域名: www.qq.com DNS耗时: 11 ms HTTP耗时: 25 ms 正常: 接口wan5 域名: www.jd.com DNS耗时: 12 ms HTTP耗时: 19 ms
内网DHCP检测	检测已完成 正常: 未发现其他DHCP服务
内网PPPoE检测	检测已完成 正常: 未发现其他PPPoE服务
内网冲突检测	检测已完成 正常: 未发现网络地址冲突

14.3 行为审计

此功能目前测试中，未开放。

15 系统设置

15.1 系统维护

- 系统信息：显示当前设备名称和上网模式
- 重启系统：显示设备运行时间和立即重启
- 在线升级：路由系统版本、型号、设备序列号（建议使用手动升级方式）
- 手动升级：点击“+”，选择正确的固件文件，点击上传，更新网关固件
- 上传备份：
 - a) 备份当前配置，下载备份文件 backup.cfg 到本地电脑
 - b) 上传备份，点击“+”，选择备份***.cfg 文件，点击上传，还原备份设置
 - c) 恢复出厂设置：还原出厂的默认设置

15.2 远程访问

15.2.1 访问控制

开启远程访问功能，不开启的情况下，不能通过 WAN 访问该网关 WEB 页面

访问控制

WEB访问控制	☒ 允许通过外网访问路由WEB管理界面
强制HTTPS WEB访问	☐ 访问WEB管理界面,强制使用HTTPS
HTTP访问端口	80 *
HTTPS访问端口	443 *
外网HTTP访问端口	800
外网HTTPS访问端口	4430

- Web 访问控制：勾选允许通过外网访问路由 WEB 管理界面，才能从外网口访问到网关。
- 强制 HTTPS WEB 访问：不勾选
- HTTP 访问端口：默认 80 (内网访问端口)
- HTTPS 访问端口：默认 443 (内网访问端口)
- 外网 HTTP 访问端口：默认 800，则为外网地址加英文“:”加 800，如 http://10.10.10.123:800
- 外网 HTTPS 访问端口：默认 4430，则为外网地址加英文“:”加 4430，如 https://10.10.10.1123:4430

15.2.2 远程日志记录

- 日志服务器需要另外搭建，配套网关使用
- 日志服务器：填写日志服务器 ip
- 服务器端口：填写日志服务器访问端口
- 传输协议：根据日志服务器选择 tcp 协议传输或者 upd 协议传输

15.3 用户管理

默认 WEB 管理员账号密码是 admin，点击编辑修改账号密码，通过添加新增访问者账号密码

用户名	admin	*
密码		*
确认密码		*
允许访问IP	0.0.0.0/0	
	IP地址或者IP子网,多个地址用空格分隔	
默认权限	管理员	▼

- 用户名：默认 admin，建议不修改
- 密码：修改的密码
- 确认密码：重复输入修改的密码
- 允许访问 IP：请谨慎配置允许访问的 IP(默认不限制)，输入格式支持：192.168.1.1, 192.168.1.1-192.168.1.200, 192.168.1.0/24, 192.168.1.0/255.255.255.0
- 默认权限：管理员、访客（admin 默认为管理员，不能修改）

15.4 网络诊断

PING 测试：通过网关 ping 其他 IP 地址测试链路连通性

15.4.1 PING 测试

PING测试		
IP地址或者域名	192.168.88.1	*
协议选择	IPv4	▼
指定源接口	ANY	▼
PING包次数	4	次
检测结果	PING 192.168.88.1 (192.168.88.1): 56 data bytes 64 bytes from 192.168.88.1: seq=0 ttl=64 time=4.374 ms 64 bytes from 192.168.88.1: seq=1 ttl=64 time=0.855 ms 64 bytes from 192.168.88.1: seq=2 ttl=64 time=0.778 ms	

- IP 地址或者域名：测试的 IP 地址或者域名
- 协议选择：IPv4 或 IPv6
- 指定源接口：ANY 或 WAN 口
- Ping 包次数：ping 测试次数（默认为 4 次）
- 检测结果：显示 PING 测试的结果

15.4.2 路由追踪

路由追踪

IP地址或者域名	www.baidu.com
协议选择	IPv4
指定源接口	wan
检测结果	<pre>tracert to www.baidu.com (14.215.177.39), 30 hops max, 38 byte packets 1 113.93.236.1 (113.93.236.1) 13.170 ms 3.481 ms 1.874 ms 2 119.146.174.37 (119.146.174.37) 13.127 ms 183.58.125.153 (183.58.125.153) 18.130 ms 119.146.174.61 (119.146.174.61) 18.903 ms</pre>

开始检测

- IP 地址或者域名：测试的 IP 地址或者域名
- 协议选择：IPv4 或 IPv6
- 指定源接口：ANY 或 WAN 口
- 检测结果：显示 PING 测试的结果

15.5 管理工具

telnet 客户端，可通过此工具 telnet 终端，如：网管交换机

Telnet客户端

交换机地址	请输入IP或域名, 如: 192.168.1.1
交换机端口	23

开始

交换机地址：需要 telnet 调试交换机的 ip

交换机端口：默认 23，按实际的交换机端口修改

15.6 网络参数

控制 ip 访问连接会话数，限制数过少会导致上网速度变慢。

- 系统最大会话数：不可修改
- 单 IP 最大会话数：默认 3000，0 为无限制
- 单 IP 最大 TCP 会话：默认 0 为无限制
- 单 IP 最大 UDP 会话：默认 800，0 为无限制

访问控制

系统最大会话数	850000
单IP最大会话数	3000
单IP最大TCP会话	0
单IP最大UDP会话	800

TCP 超时设置和 UDP 超时设置，建议不修改，默认即可。

TCP超时设置

连接超时	600
SYN发送超时	120
FIN等待超时	120
关闭连接超时	10
最后ACK超时	30
已建立连接超时	1800
SYN接受超时	60
时间等待超时	120
关闭等待	60

UDP超时设置

未答复超时	60
已确认超时	180

15.7 时钟配置

网关连接外网会自动校对网络时间，无需手动修改

系统时间	2019/09/25 12:25:50	
	同步系统时间	
自动对时	☒ 自动与服务器对时	
国际时区	Asia/Shanghai	▼
对时服务器1	0.pool.ntp.org	立即对时
对时服务器2	1.pool.ntp.org	立即对时
对时服务器3	2.pool.ntp.org	立即对时
对时服务器4	3.pool.ntp.org	立即对时
保存		