
产品用户手册

版本号: V1.0

深圳市中新通信有限公司

目录

1	产品概述	1
1.1	产品介绍	1
1.2	主要特性	1
2	产品组成	2
2.1	装箱列表	2
2.2	系统组成	2
2.2.1	设备整体外观	2
2.2.2	设备指示灯示意图	2
3	设备配置	5
3.1	Web 页面介绍	5
3.1.1	登录 WEB 前台管理页面	5
3.1.2	基础页面功能分布	7
3.1.3	高级页面功能分布	7
3.2	无线路由器	8
3.2.1	无线路由器（Router-AP）模式配置	8
3.2.2	访客网络	12
3.3	无线 AP	17
3.3.1	无线 AP 配置（Bridge-AP）	17
3.4	无线网桥	20
3.4.1	中心站	20
3.4.2	远端站	23
3.5	无线终端	26
3.5.1	无线终端桥模式（Bridge-Station）	27
3.5.2	无线终端路由模式（Router-Station）	31

3.6	无线中继	36
3.7	无线回传+覆盖	41
3.8	高级模式—工作模式配置	45
3.9	高级模式—接口配置	46
3.9.1	接口→局域网配置	46
3.9.2	接口→广域网配置	47
3.9.3	接口→VLAN 配置	49
3.9.4	接口→客户端列表	50
3.9.5	接口→接口数据统计	51
3.10	高级模式—无线配置	52
3.10.1	无线→射频配置	52
3.10.2	无线→虚拟 AP 配置	54
3.10.3	无线→高级配置	57
3.10.4	无线→接入控制配置	60
3.10.5	无线→状态配置	63
3.10.6	无线→动态频率选择	64
3.11	高级模式—网络配置	65
3.11.1	网络→路由配置	65
3.11.2	网络→地址解析 (ARP)	67
3.11.3	网络→NAT 配置	68
3.11.4	网络→路由转发控制配置	70
3.11.5	网络→流量控制	71
3.11.6	网络→DMZ 配置	72
3.11.7	网络→DDOS	74
3.11.8	网络→UPNP	74
3.11.9	网络→网页入口	75

3.11.10	网络→网址过滤	77
3.11.11	网络→MAC 地址管理	78
3.11.12	网络→诊断配置	78
3.12	高级模式—系统配置	80
3.12.1	系统→配置管理配置	80
3.12.2	系统→设备管理配置	83
3.12.3	系统→用户管理配置	84
3.12.4	系统→时间配置	84
3.12.5	系统→工具	86
3.12.6	系统→管理接口配置	88
3.12.7	系统→系统日志	89
4	常见故障排除	92
5	附录	96
5.1	技术参数	96
5.2	术语表	96

1 产品概述

1.1 产品介绍

中新通信无线系列设备，使用2.4GHz和5GHz全频段为用户提供600M带宽，采用基于airX(空间自适应最佳通信)的波束赋形技术与802.11n标准相结合，实现最佳通信效果和性能，满足了无线网络应用的快速发展，为运营商开展具有更高吸引力、内容更丰富的网络服务提供了优秀的技术解决方案，同时确保运营商拥有卓越的服务品质和最佳的运营收入。中新通信无线系列智能设备帮助运营商、政府和企业实现在城市、农村等应用中提供高品质的WLAN服务，并能显著减少设备投入数量，有效降低成本。

1.2 主要特性

- 中英文双语界面，可实现全中文 SSID 配置、全中文配置页面
- 人性化“帮助”功能，使运维更加简洁
- 定制化 Portal，提供个性化服务
- BMS Cloud 云网管系统，实现集中管理
- 高密度用户接入，完美解决密集场景覆盖
- -102dBm 超高接收灵敏度，实现场景 1-2Km 半径超大范围覆盖
- 多样化的天线、PoE 模块，应对各种应用场景，灵活组网
- IP66 级防护等级，满足各种苛刻安装环境 IP66 级防护等级，满足各种苛刻安装环境

2 产品组成

2.1 装箱列表

表 2-1 设备包装清单

序号	名称	数量(单位)	备注
1	包装箱	1(个)	/
2	设备主机	1(台)	/
3	PoE 电源模块 (选配件)	1(台)	48V 直流 PoE 供电模块 交流转直流 48V PoE 供电模块, 包含 220V 线缆插头, 具体根据用户需求而定。
4	安装支架 (选配件)	1(套)	
5	千兆以太网浪涌抑制器 (选配件)	1(台)	/
6	高性能网线 (选配件)	1(套)	

2.2 系统组成

2.2.1 设备整体外观

2.2.2 设备指示灯示意图 (基站)

序号	指示灯名称	描述	功能
1	POWER	电源指示灯	长灭—断电 长亮—已加电
2	STATUS	系统状态指示灯	常灭—未进入系统 常亮—系统启动中 闪烁—系统正常运行中

3	LAN	以太网指示灯	常灭—端口没有连接 常亮—端口已正常连接 闪烁—端口正在进行数据传输
4	2.4GHz	射频指示灯	常灭—射频未开启 常亮—射频正常工作 闪烁—正在进行空口数据传输
5	5GHz	射频指示灯	常灭—射频未开启 常亮—射频正常工作 闪烁—正在进行空口数据传输
6	RES	瘦 AP 状态指示灯	常灭—瘦 AP 功能未工作 常亮—AP 已上线 闪烁—瘦 AP 初始化中

表 2-2 指示灯状态描述

表 2-3 设备外部接口描述

序号	名称	功能
	接地螺栓	此处连接接地线，保证设备电气安全。
	以太网口	以太网接口，用以设备供电及数据传输。
	RJ45 串口	RJ45 设备调试口，用于设备调试。
	RST 孔位	Reset 复位孔，用于硬件复位设备。

3 设备配置

3.1 Web 页面介绍

3.1.1 登录 WEB 前台管理页面

设置本地 IP 地址，先将本地 IP 地址设置为 192.168.62.X(2-254)网段，用网线连接设备设备。

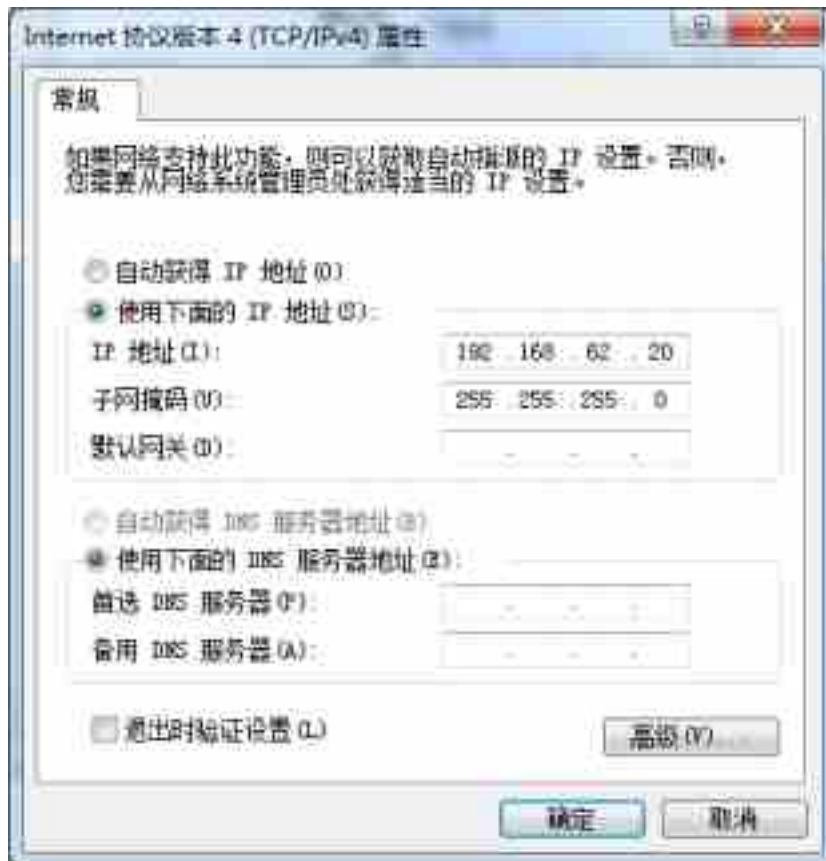


图 3-1 配置 IP 地址

在 WEB 浏览器中输入设备 IP 地址(缺省 IP 地址为 192.168.62.1)，弹出登录页面，如下图所示：

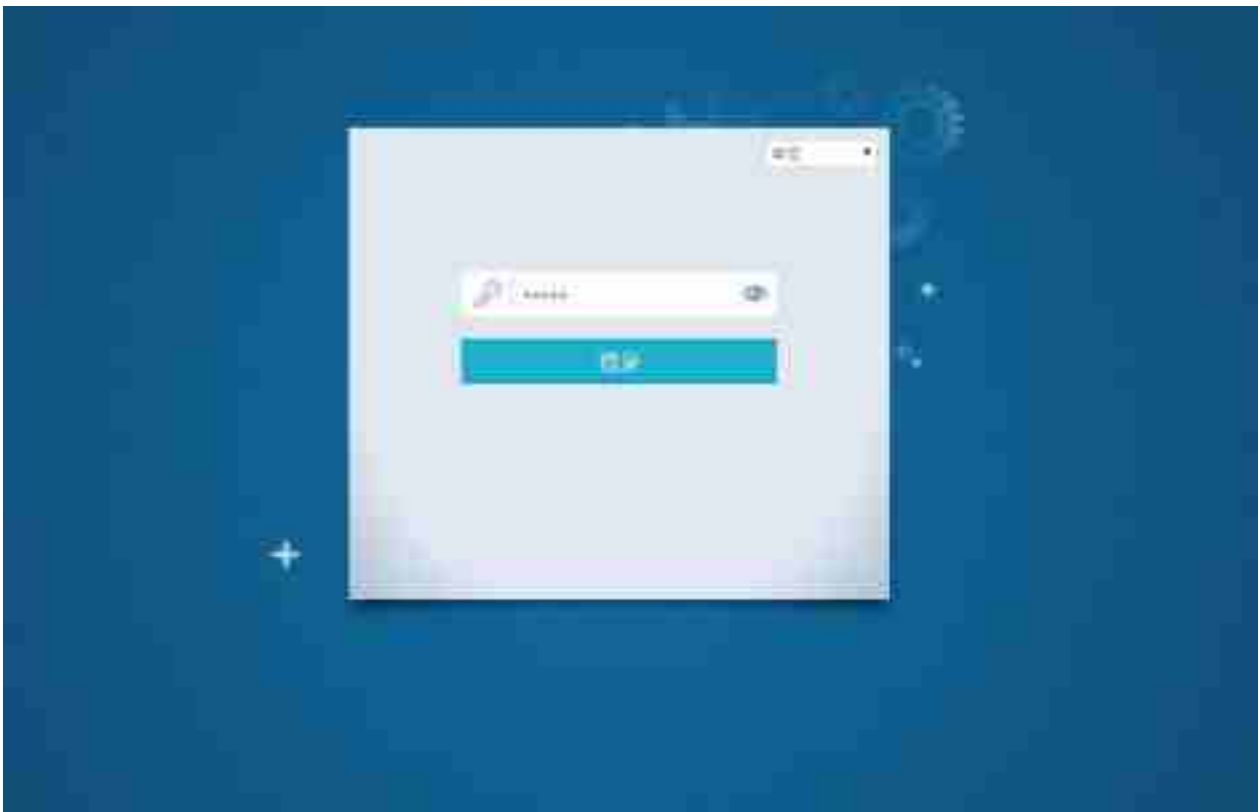



图 3-2 登陆主页

登录 WEB 需要用户名和密码，默认密码：**admin**

密码设置完成后，点击“登录”按钮，跳转到登录页面



图 3-3 基础页面

 注意：研华无线系列设备支持中、英双语界面。

3.1.2 基础页面功能分布

基础 Web 页面区域分布，如下图所示：



图 3-4 基础页面

3.1.3 高级页面功能分布

基础 Web 页面区域分布，如下图所示：



图 3-5 高级页面

3.2 无线路由器

3.2.1 无线路由器（Router-AP）模式配置

接入点模式下，设备工作在路由模式，此时以太网口作为 WAN 口，进行数据转发。

Router-AP 工作模式的基本配置，点击登录后，进入设备配置界面，点击配置向导选择无线路由器，如下图所示：



图 3-3 配置模式修改

选择工作场景为无线路由器，点击进入路由器配置界面，如下图：



图 3-7 配置模式修改

外网设置（广域网）

选择动态获取连接模式：端口自动获取 IP 地址，DNS 默认会通过 DHCP 服务器获取，如无特殊需求，不需要设置。

选择静态配置连接模式：静态配置 IP 地址和 DNS。

选择拨号上网连接模式：选择 PPPoE 连接模式，输入相应的用户名密码。

Auto-自动链接模式，Ddmon 当有数据请求时，尝试连接，Once-手动连接。

内网设置（局域网）

ip 地址：局域网 ip 地址设置：例如 192.168.62.1

子网掩码：子网掩码是逻辑上细分的 ip 网络，例如 255.255.255.0

dhcp 服务器：dhcp 服务器自动的对网络设备设置参数，这样网络设备在网络上可以进行通信。



图 3-8 配置模式修改

SSID 创建：根据客户需求创建或修改相应的无线网络名称。

认证模式：基础页面默认支持 OPEN、WPA-PSK、WPA2-PSK、WPA/WPA2-PSK Auto 认证方式（如果不能满足您的需求请到高级页面下重新进行配置）。



图 3-9 配置模式修改

如果想要配置更高级的选项，点击更多配置



图 3-9 配置模式修改

信道选择: 根据需求自动选择信道和手动选择信道。

国家码: 使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

功率配置: 可以手动调节发射功率

WDS: 允许连接到客户端的其它设备的数据通过 AP

单用户发送接收速率: 可以控制接入用户的发送接收速率

云 AC 地址: 配置管理设备的云 AC 地址

WAN 口可管理: 可以通过 WAN 口管理设备

3.2.2 访客网络

访客网络: 就是同一个设备释放两个不同的 SSID，访客网络是对应客户或者公众使用的网络，可以推送 Portal 认证页面，进行广告宣传。

在配置过程中，开启访客网络功能，配置如下：



图 3-10 访客网络配置

访客网络中可以配置欢迎标题，访客密码，访客网络的整体上传下载速率，也可以进行登录认证之后的推广页面设置，也可以在访客页面中增加页面链接。



图 3-11 访客网络配置

点击预览，访客页面效果如下：（访客上网终端接入弹出页面效果如下所示）



图 3-12 访客网络配置

访客网络配置修改：

如果正常配置了网络，只需开启访客网络，可以在网络管理选项中开启访客网络。

选择网络管理如下图：



图 3-13 访客网络配置

页面到配置页面最下方：



图 3-14 访客网络配置

点击插件管理，选择访客网络



图 3-15 访客网络配置

打开访客网络



图 3-16 访客网络配置

可以设置工作频段，欢迎标题，访客密码，访客网络的名称，访客网络整体的上传下载速率，可以添加推广页面，即登陆页面之后会跳转到推广页面上。也可以添加页面连接，连接的页面是 URL 连接，在未登陆访客前提的条件下对客户进行开放资源访问。

3.3 无线 AP

3.3.1 无线 AP 配置（Bridge-AP）

桥接-接入点模式。设备作为 AP 模式。输入密码登录设备管理页面，进入配置向导页面选择无线 AP，如下图所示：



图 3-17 无线 AP 配置



图 3-18 无线 AP 配置

静态地址设置：填写 IP 地址、掩码、网关和 DNS

动态获取设置：动态获取，即设备从上层 DHCP 获取地址



注意：当设备选择无线 AP 模式后再次选择动态获取地址，设备没有明确的访问地址，需要知道设备的分到 IP 地址才可以访问设备。



图 3-18 无线 AP 配置



图 3-18 无线 AP 配置



图 3-18 无线 AP 配置



图 3-18 无线 AP 配置

3.4 无线网桥

3.4.1 中心站

无线网桥模式。设备作为网桥模式。输入密码登录设备管理页面，进入配置向导页面选择无线网桥，如下图所示：



图 3-19 无线网桥配置



图 3-20 无线网桥配置

填写 IP 地址、掩码、网关和 DNS



图 3-21 无线网桥配置

工作模式：设置网桥的工作模式，是中心点还是远端，中心即发射端，远端即接收端

信道选择：根据需求自动选择信道和手动选择信道。

国家码：使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

距离：配置中心点到远端的距离范围

名称：设置中心的发射的无线名称，到对端去连接

密码：设置网络连接密码



图 3-22 无线网桥配置

基本配置已完成，点击更多配置



图 3-23 无线网桥配置

功率配置：可以手动调节发射功率

WDS：允许连接到客户端的其它设备的数据通过 AP（无线网桥建议打开）

单用户发送接收速率：可以控制接入用户的发送接收速率

云 AC 地址：配置管理设备的云 AC 地址



图 3-24 无线网桥配置

点击完成，网桥中心点配置已完成。

3.4.2 远端站

无线网桥模式。设备作为网桥模式。输入密码登录设备管理页面，进入配置向导页面选择无线网桥，如下图所示：



图 3-25 无线网桥配置



图 3-26 无线网桥配置

填写 IP 地址、掩码、网关和 DNS



注意：中心点和远端点尽量 IP 配在同一网段，且不能相同。



图 3-27 无线网桥配置

工作模式: 设置网桥的工作模式，是中心点还是远端，中心即发射端，远端即接收端

国家码: 使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

名称: 扫描无线网络，选择中心点对应的名称

密码: 输入无线连接密码

锁定: 可以锁定连接设备的 MAC 地址



图 3-28 无线网桥配置



图 3-29 无线网桥配置

功率配置：可以手动调节发射功率

WDS：允许连接到客户端的其它设备的数据通过 AP（无线网桥建议打开）

云 AC 地址：配置管理设备的云 AC 地址



图 3-30 无线网桥配置

配置完成。

3.5 无线终端

3.5.1 无线终端桥模式（Bridge-Station）

无线终端：在无线终端模式下，设备作为客户端与 AP 连接组网。在该模式下，设备可以作为桥终端（Bridge-Station）连接也可以作为路由终端（Router-Station）连接。

无线终端工作模式的基本配置，如下图所示：



图 3-31 无线终端配置



图 3-32 无线终端配置



图 3-33 无线终端配置

填写 IP 地址、掩码、网关和 DNS。



图 3-34 无线终端配置



图 3-35 无线终端配置

国家码：使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

名称：通过扫描选择对应连接的无线网络名称

密码：设置无线网络连接密码

锁定：可以锁定连接设备的 MAC 地址



图 3-36 无线终端配置

点击更多配置



图 3-37 无线终端配置

功率配置：可以手动调节发射功率

WDS: 允许连接到客户端的其它设备的数据通过 AP（无线网桥建议打开）

云 AC 地址: 配置管理设备的云 AC 地址



图 3-38 无线终端配置

配置已完成。

3.5.2 无线终端路由模式（Router-Station）

路由模式（Router-Station）: 在路由-客户端模式下，设备工作在客户端模式连接到其它 AP，将 WLAN 作为 WAN 口，进行数据转发。

无线终端工作模式的基本配置，如下图所示：



图 3-39 无线终端配置



图 3-40 无线终端配置

选择路由模式。



图 3-41 无线终端配置

外网设置（广域网）

选择动态获取连接模式：端口自动获取 IP 地址，DNS 默认会通过 DHCP 服务器获取，如无特殊需求，不需要设置。

选择静态配置连接模式：静态配置 IP 地址和 DNS。

选择拨号上网连接模式：选择 PPPoE 连接模式，输入相应的用户名密码。

Auto-自动链接模式，Ddmon 当有数据请求时，尝试连接，Once-手动连接。

内网设置（局域网）

ip 地址：局域网 ip 地址设置：例如 192.168.62.1

子网掩码：子网掩码是逻辑上细分的 ip 网络，例如 255.255.255.0

dhcp 服务器：dhcp 服务器自动的对网络设备设置参数，这样网络设备在网络上可以进行通信



图 3-42 无线终端配置



图 3-43 无线终端配置

国家码: 使用设备所在的国家。由于当地法律限制,该设置会影响设备发送的最大功率和可设置的信道。

名称: 通过扫描选择对应连接的无线网络名称

密码: 设置无线网络连接密码

锁定: 可以锁定连接设备的 MAC 地址



图 3-44 无线终端配置

点击更多配置



图 3-45 无线终端配置

功率配置：可以手动调节发射功率

WDS: 允许连接到客户端的其它设备的数据通过 AP（无线网桥建议打开）

云 AC 地址: 配置管理设备的云 AC 地址

WAN 口可管理: 通过 WAN 口管理设备



图 3-46 无线终端配置

配置完成。

3.6 无线中继

无线中继: 在无线中继模式下，设备作为客户端与 AP 连接组网。在该模式下，设备作为客户端接入上一级 AP，又作为 AP 为其它客户端无线连接。

无线终端工作模式的基本配置，如下图所示：



图 3-47 无线中继配置



图 3-48 无线中继配置

静态地址设置：填写 IP 地址、掩码、网关和 DNS

动态获取设置：动态获取，即设备从上层 DHCP 获取地址


 注意：当设备选择此模式后再次选择动态获取地址，设备没有明确的访问地址，需要知道设备的分到 IP 地址才可以访问设备。



图 3-49 无线中继配置



图 3-50 无线中继配置

扫描设备所连接的 AP 信号名称，进行连接。



图 3-51 无线中继配置

点击更多配置，配置设备的更多参数



图 3-52 无线中继配置

国家码：使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

信道：需注意此模式下信道不起作用

功率：设置设备的接收和发射功率

WDS：允许连接到客户端的其它设备的数据通过 AP

KeepAP: 仅用于中继模式且 VAP 为 Station 模式。当客户端未连接到上级 AP 时，仍打开 AP 接口。

单用户发送接收速率: 设置设备的单用户使用速率

云 AC: 设置设备的云 AC 管理地址



图 3-53 无线中继配置

点击完成，整体配置完成。

这样配置中继所转发的信号和上行扫描到的信号是一样的，如果想修改转发的信号名称，按如下操作



图 3-54 无线中继配置

登陆设备，点击网络管理—右上角无线配置—选择上图所标位置进行配置你所发射的无线网络名称，仍可以建多个 VAP，发射多个信号。

3.7 无线回传+覆盖

无线回传+覆盖模式，针对是双频设备，指其中一个射频做 AP 进行覆盖，另一个射频做 STA 接收上线无线信号进行回传。一般采用较多的是 2.4GHz 做覆盖，5GHZ 做回传。在光纤无法到达，有线无法施工情况下可以采用此种模式。

无线回传+覆盖工作模式的基本配置，如下图所示：



图 3-55 无线回传+覆盖模式配置

登陆设备后选择无线 AP+无线回传模式



图 3-56 无线回传+覆盖模式配置

网络模式：选择设备做桥模式和路由模式

回传模式：指选择 2.4GHz 做 STA 回传，还是 5GHz 做 STA 回传



图 3-57 无线回传+覆盖模式配置

填写 IP 地址、掩码、网关和 DNS



图 3-58 无线回传+覆盖模式配置

填写回传设备的 SSID（信号名称）及密码，可以采取扫描再进行连接。

锁定：针对 MAC 地址对上行设备进行绑定



图 3-59 无线回传+覆盖模式配置

填写无线覆盖的 SSID（信号名称）及密码。



图 3-60 无线回传+覆盖模式配置

点击更多配置



图 3-61 无线回传+覆盖模式配置

国家码： 使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

信道： 此处配置的信号为做无线 AP 射频的信道

功率： 设置设备的接收和发射功率

WDS： 允许连接到客户端的其它设备的数据通过 AP

单用户发送接收速率： 设置设备的单用户使用速率

云 AC: 设置设备的云 AC 管理地址



图 3-62 无线回传+覆盖模式配置

配置完成。

3.8 高级模式—工作模式配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“配置→工作模式”打开配置页面，如下图所示：



图 3-63 工作模式配置

可以发现设备有 6 中工作模式，分别为路由 AP，路由 STA，路由中继，桥 AP，桥 STA，桥中继 6 种模式

Bridge-AP: 网桥-接入点模式。WLAN 作为 AP 与以太网桥接在一起。

Bridge-Station: 在网桥-客户端模式下，WLAN 作为客户端与其它 AP (root AP) 连接，并与以太网桥接在一起。在该模式下，所连接 AP (root AP) 必须开启 WDS 功能。

Bridge-Repeater: 在网桥-中继模式下，WLAN 既作为客户端与上一级 AP (root AP) 连接，又作为 AP 为其它客户端提供无线连接。在该模式下，上一级 AP (root AP) 必须开启 WDS 功能。

Router-Station: 在路由-客户端模式下，WLAN 工作在客户端模式连接到其它 AP，将 WLAN 作为 WAN 口，进行数据转发。

Router-AP: 在路由-接入点模式下，WLAN 工作在 AP 模式，此时以太网口作为 WAN 口，进行数据转发。

Router-Repeater: 在路由-中继模式下，WLAN 既使用客户端模式作为 WAN 口与上一级 AP (root AP) 连接，又作为 AP 为其它客户端提供无线连接

3.9 高级模式—接口配置

3.9.1 接口→局域网配置

当设备做路由模式时设备做 **DHCP** 地址池，配置如下：



图 3-64 工作模式配置

ip 地址: 局域网 ip 地址设置：例如 192.168.1.1

子网掩码: 子网掩码是逻辑上细分的 ip 网络，例如 255.255.255.0

dhcp 服务器: dhcp 服务器自动的对网络设备设置参数，这样网络设备在网络上可以进行通信。

开始地址: DHCP 地址池的开始地址, 只填入子网号, 例如 IP:192.168.1.1

Netmask:255.255.255.0 , 开始号: 100, 表示从 192.168.1.100 开始。

结束地址: dhcp 地址池的结束地址。

租期类型: 服务器的租期类型: 时间单位和无限制。

Infinite: 无限制。

ipv6 地址: 格式: ipv6 地址/前缀长度例如: 3FFE:FFFF:0:CD30:0:0:0:0/64, 如果有连续的零, 可以用::代替,但只能用一次, 前缀长度最大为 128。

ipv6 DHCP: 网口自动获取 ipv6 地址。



注意: 设备的局域网和广域网不要在同一网段。

当设备做桥模式时设备配置如下:



图 3-65 高级-接口配置

设备可以选择动态获取或静态配置

ip 地址: 局域网 ip 地址设置: 例如 192.168.1.1

子网掩码: 子网掩码是逻辑上细分的 ip 网络, 例如 255.255.255.0

3.9.2 接口→广域网配置



图 3-66 高级-接口配置

选择 DHCP 连接模式：端口自动获取 IP 地址，DDNS 默认会通过 DHCP 服务器获取，如无特殊需求，不需要设置。

选择静态配置连接模式，静态配置 IP 地址和 DNS，如下图所示：



图 3-67 高级-接口配置

选择 **PPPoE** 连接模式：输入相应的用户名密码。

PPP 连接模式：Auto-自动链接模式，Demond-当有数据请求时，尝试连接，Once-手动连接。

选择连接模式，如下图所示：



The image shows a configuration page for a WAN interface. At the top, there is a title 'WAN' and two tabs: '设置' (Settings) and '状态' (Status). Below the title, there is a text field for the IP address, currently showing '202.96.209.6'. The main configuration area includes several fields and options:

- '连接模式' (Connection Mode): A dropdown menu set to 'PPPoE'.
- '用户名' (Username): An empty text input field.
- '密码' (Password): An empty text input field.
- '连接模式' (Connection Mode): A dropdown menu set to 'Auto'.
- '静态DNS服务器' (Static DNS Server): A text input field containing '202.106.0.20'.
- '备用DNS服务器' (Backup DNS Server): A text input field containing '8.8.8.8'.
- '手动MAC地址' (Manual MAC Address): A checkbox labeled '启用' (Enable) is checked. To its right, there is a note: '不支持修改WiFi口的Mac地址' (Does not support changing the MAC address of the WiFi port).
- 'MAC地址' (MAC Address): A text input field containing '14-03-14-00-01-9a'.

At the bottom of the configuration area, there is a blue button labeled '应用' (Apply).

图 3-68 高级-接口配置

3.9.3 接口→VLAN 配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“**接口→VLAN**”打开 VLAN 配置页面，如下图所示：



图 3-69 高级-接口配置

可以新建业务 VLAN 和管理 VLAN，操作完成之后，点击导航栏的“保存”，下一次设备重启之后使配置生效。

3.9.4 接口→客户端列表

输入用户名和密码，登录设备管理页面，点击左侧菜单“接口→客户端列表”，打开配置页面



图 3-70 高级-接口配置

该页面主要显示 DHCP 客户端信息，包括客户端的主机名、MAC 地址、IP 地址以及地址租期。当设备未启用 DHCP 服务器时，该列表为空。

3.9.5 接口→接口数据统计

输入用户名和密码，登录设备管理页面，点击左侧菜单“接口→接口数据统计”，打开配置页面



图 3-71 高级-接口配置

该页面统计了各个接口数据信息。

3.10 高级模式—无线配置

3.10.1 无线→射频配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“**无线→射频**”，打开 WLAN 射频配置页面，该页面显示 wifi0(2.4GHz 射频卡)及 wifi1(5GHz 射频卡)常用参数，如下图所示：



图 3-72 高级-无线配置

点击对应射频卡的“**修改**”，弹出 WLAN 射频配置修改窗口，在该窗口对射频参数进行详细修改，如下图所示：



图 3-73 高级-无线配置

在该选项卡中，可以根据现场需求配置国家码、模式、信道、传输功率、Tx Chain、Rx Chain、信道带宽、信标帧间隔、应答超时时间、A-MPDU 开关、A-MPDU 聚合子帧数、A-MPDU 聚合帧长度和 Short GI 开关相关参数。

射频配置相关参数介绍：

国家码：使用设备所在的国家。由于当地法律限制，该设置会影响设备发送的最大功率和可设置的信道。

模式：可选 b,g,n 分别对应不同的工作模式。

11G：工作在 2.4GHz 频段的 802.11g 模式，可兼容 802.11b 设备。

11B：工作在 2.4GHz 频段的 802.11b 模式。

11N(only2.4G)：纯 11N 模式，并且工作在 2.4GHz 下。

还可以混合选择 b,g,n 工作模式。

频宽：配合“模式”来使用，选择不同的模式时可以选择不同的信道带宽。

信道：射频工作的信道。当设置为 auto 时，在射频初始化时，会找到最佳的工作信道。该设置对于 Station 无效。

传输功率：可在 0-27dBm 之间手动调整射频输出功率。

Tx Chain：设置发送空间流数，可选单空间流或者双空间流。

Rx Chain：设置接收空间流数，可选单空间流或者双空间流。

5/10MHz：只有部分设备支持该功能。

20MHz：使用 20MHz 的信道带宽。

HT20/HT40：自动选择 20MHz 或 40MHz 作为信道带宽。当扩展信道繁忙时，AP 只会使用

20MHz 信道带宽。

Static HT40: 设置信道带宽为 40MHz。该功能仅用于测试目的。

信标帧间隔: 修改设备发送信标帧(beacon)间隔，一般保持默认参数 100ms。

应答超时时间: 应答报文超时时间。该参数影响最远的通信距离。

距离公式为: $\text{meter}=(\text{acktimeout} - 27)*150$ 。

A-MPDU 开关: A-MPDU 聚合的是经过 802.11 报文封装后的 MPDU，这里的 MPDU 是指经过 802.11 封装过的数据帧，开启后提高系统吞吐量，默认开启。

A-MPDU 聚合子帧数: 聚合 MPDU 数，一般保持默认参数。

A-MPDU 聚合帧长度: A-MPDU 最大帧长度，一般保持默认参数。

A-MSDU 开关: 开启或关闭 A-MSDU 聚合帧格式，一般保持默认参数。

Short GI 开关: 保护间隔开关，默认开启，在多径效应较明显的环境下建议关闭。

短前导码开关: 长前导码可以兼容旧的 11b 设备。使用短前导码可以获取到更高的传输速率。

BG 保护模式开关开启 802.11bg 保护模式后，在 802.11g 网络中检测到 802.11b 设备将会发送 RTS/CTS 序列。该功能用于保护不识别 OFDM 调制的帧设备。

配置完成之后点击“应用变更”并“保存→重启”使之生效。



注意：该配置页面带有*的参数需要在设备重启后方可生效。



注意：该配置页面参数影响用户实际业务，请慎重修改。

3.10.2 无线→虚拟 AP 配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“无线→虚拟 AP”，打开 WLAN VAP 配置页面，对 VAP 参数进行配置，如下图所示：



图 3-74 高级-无线配置

单个射频默认创建 3 个 WLAN 接口，访客网络对应的是第三个 WLAN 接口。可以对此 VAP 进行“修改”、“删除”操作，如下图所示：



图 3-75 高级-无线配置

ssid: 服务集标识符用于区分不同的虚拟接入点。手动输入需要发射的 SSID name，例如 TEST，或者点击“扫描”来查看周围的 ESSID。

编码: 如果 SSID 中包含有中文字符，手机和平板用户请选择 UTF-8,PC 用户请选择 GB2312 编码。

SSID 隐藏: 通过隐藏 SSID 以达到安全控制的目的，勾选后，需要客户端手动输入正确的 ESSID 才可正常关联。

隔离: 开启 AP 隔离，接入该 AP 的计算机或者网络设备之间将不能互相访问，来保障不同用户的安全。

WDS: 可以让无线虚拟 AP 之间通过无线进行桥接(中继), 而在中继的过程中并不影响其无线设备覆盖效果。

认证模式: 默认为开放式 Open, 可以根据需要开启不同的安全策略(详细安全策略释义见附录), 选择不同的认证模式, 页面将弹出对应的对话框来进行参数配置, 如下图所示:



图 3-76 高级-无线配置

加密: 支持 64、128 位 WEP 加密、WPA、WPA2 和 WAPI

认证: 支持 802.1x 认证、MAC 地址认证、PSK 认证、Portal、WAPI 等



图 3-77 高级-无线配置

修改完成完成之后点击“应用变更”，使配置生效。

3.10.3 无线→高级配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“无线→高级”，打开 WLAN VAP 高级配置页面，如下图所示：



图 3-78 高级-无线配置

VAP 高级配置相关介绍：

选择 VAP：在下拉选项中选择需要修改参数的 VAP ID。

RTS/CTS：RTS/CTS 协议，用来减少由隐藏节点问题所造成的冲突的机制，默认开启，设置 256。

WMM：WMM(Wi-Fi Multimedia)为 802.11 网络提供基本的 QoS(Quality of service)功能。WMM 包含四个优先级策略：Best Effect（性能最优），Background（后台），Video（视频），Voice（语音）。每个策略包含 5 个配置参数：CWmin(最小竞争窗口)，CWmax（最大竞争窗口），AIFSN（仲裁帧间间隔数），TXOP（Transmission Opportunity，发送机会，是无线信道接入的基本单元。获得 TXOP 的站点在 TXOP Limit 时间内可以不再重新竞争信道、连续使用信道传输多个数据帧。），ACM(Admission Control Mandatory，强制接入控制)。



图 3-79 高级-无线配置

VLAN 优先级处理: 允许对不同的 VLAN 数据配置不同的优先级策略。有四个优先级策略: Best Effect (性能最优), Background (后台), Video (视频), Voice (语音)。

WLAN 定时关闭: 这个功能可以帮您在指定的时间段内, 保持 WLAN 为关闭状态。

组播转单播: 将该 VAP 收到的组播包转换为单播包。通常用于 802.3 的数据包转换为 802.11 的数据包。802.11 的组播包使用较低的发送速率且无响应机制, 转换为单播包后可以提高系统吞吐量和数据传输的可靠性。该功能需要与开启单播转组播功能的设备同时使用。

单播转组播: 将该 VAP 收到的单播包转换为组播包。通常用于 802.11 的数据包转换为 802.3 的数据包。该功能需要与开启组播转单播功能的设备同时使用。

DTIM 周期: 投递传输指示信息, DTIM=1 表示每个 beacon 中都包含 DTIM, DTIM=2 表示每两个 beacon 中包含一个 DTIM, 以此类推。

最大接入用户数: 该 VAP 允许接入的最大用户数, 默认 255。

5G 优先接入:支持 5G 的终端优先接入 5G 的网络, 前提是 2.4GHz 和 5GHz 的 SSID 相同。

上行链路检测使能: 这个功能可以在检测到网络(上行链路)出现故障的时候, 自动关闭射频, 或链路恢复时自动开启射频。默认关闭。

上行链路检测地址: 需要输入一个 IP 地址来启用这个功能, 该功能启用以后, 此设备会持续的 ping 指定的 IP 地址, 如果连续 10 次 ping 不通,射频就会自动关闭。之后如果连续 10 次 ping 通, 射频就会自动开启。

踢掉弱信号用户:该功能会周期性检测用户信号强度, 并强制信号强度低于设定阈值的用户下线。弱信号用户的存在会影响整个系统的吞吐量。

WDS 广播转单播:该功能可以将发送的广播包转换为其每个 WDS 节点的单播包。广播包使用较低的发送速率并且没有响应机制, 转换为单播包可以提高数据传输的稳定性和效率。

强制速率: 该功能用于配置 VAP 强制要求的 802.11bg/802.11a 的速率。当 VAP 工作在 AP 模式时, 所有客户端必须强制或支持这些速率才能接入该 AP; 当 VAP 工作在 Station 模式时, 强制速率

与支持速率效果相同。强制速率和支持速率一起协商出数据通信所使用的 802.11bg/802.11a 的速率。。

支持速率：该功能用于配置 VAP 支持的 802.11bg/802.11a 的速率。强制速率和支持速率一起协商出数据通信所使用的 802.11bg/802.11a 的速率。

所有速率都不支持是不允许的，至少需要选择两个速率进行设置。

强制 MCS：该功能用于配置 VAP 强制要求的 802.11n 的 MCS 速率。当 VAP 工作在 AP 模式时，所有客户端必须强制或支持这些速率才能接入该 AP；当 VAP 工作在 Station 模式时，强制 MCS 与支持 MCS 效果相同。强制 MCS 和支持 MCS 一起协商出数据通信所使用的 802.11n 的速率。

支持 MCS：该功能用于配置 VAP 支持的 802.11n 的 MCS 速率。强制 MCS 和支持 MCS 一起协商出数据通信所使用的 802.11n 的速率。


VAP 高级配置还支持更加详细的 WMM 配置，点击“**详细配置**”对 Qos 进行更加详细的设置，如下图所示：

无线参数配置完成之后，点击“**应用变更**”使配置生效，如下图所示：



图 3-80 高级-无线配置

操作完成之后，点击“**保存**”，设备下一次重启之后使配置生效。

 **注意：**此配置页面的参数针对 VAP 的一些高级设置。如果您对这里不太了解，请不要进行更改。

3.10.4 无线→接入控制配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“无线→接入控制”，打开 WLAN 接入控制配置页面，如下图所示：



图 3-81 高级-无线配置

默认 WLAN 接入控制服务关闭，针对不同的 VAP 可以配置不同的接入控制列表。点击“新建列表”可以配置接入控制列表，如下图所示：



图 3-82 高级-无线配置

在“列表名称”中输入接入控制列表名称，点击“应用变更”创建新的接入控制列表，如下图所示：

WLAN接入控制

请从左侧的列表中为接入设备选择VLAN进行匹配。

VLAN	设备名称	状态	操作
vlan0		关闭	启用
vlan2		关闭	修改
vlan3		关闭	修改
vlan15		关闭	修改
vlan22		关闭	修改
vlan23		关闭	修改

接入控制列表

No.	名称	MAC地址列表	操作
1	qwe		修改 删除

新增列表

图 3-83 高级-无线配置

新创建的接入控制列表中没有用户 MAC 地址，需要手动添加，点击对应接入控制列表后的“修改”，编辑该控制列表，如下图所示：

修改接入控制列表

列表名称: allow1

No.	MAC地址	操作
-----	-------	----

新MAC地址: Format: 22:33:44:55:66:77 or 223344xxxxxx

图 3-84 高级-无线配置

在弹出的窗口输入正确的用户 MAC 地址，点击“增加”添加该 MAC 地址成功，一个列表可以添加多个用户 MAC 地址。对于列表中已有的 MAC 地址可以通过点击其后面的“删除”按钮来删除该 MAC 地址条目，如下图所示：

修改接入控制列表

列表名称: allow1

No.	MAC地址	操作
1	22:33:44:55:66:77	删除

新MAC地址: Format: 22:33:44:55:66:77 or 223344xxxxxx

图 3-85 高级-无线配置

该接入控制列表配置完成之后，点击“应用变更”使配置生效，如下图所示：



图 3-86 高级-无线配置

针对 VAP 的接入控制需要先创建接入控制列表，点击“修改”来应用到对应的 VAP，如下图所示：



图 3-87 高级-无线配置

在弹出的新窗口中，选择需要应用的接入控制列表名称，默认空即不应用任何接入列表，根据需要选择正确的接入列表，如下图所示：



图 3-88 高级-无线配置




“控制动作”默认 Disable，即不开启接入控制服务，根据需要选择正确的控制动作，其中“Allow”为允许接入列表中所有 MAC 地址访问该 WLAN，“Deny”为拒绝接入列表中所有 MAC 地址访问该 WLAN，如下图所示：



图 3-89 高级-无线配置

WLAN 接入控制配置完成之后，点击“应用变更”使配置生效，如下图所示：

操作完成之后，点击“保存”，设备下一次重启之后使配置生效。

-  注意：接入控制列表名称必须以字母开头，并且长度不能超过 32 个字符。
-  注意：接入控制列表中的用户 MAC 地址使用十六进制表示，字符与字符之间使用英文：隔开。
-  注意：同一个 VAP 同一时间内只能有一个接入控制列表和一个控制动作。

3.10.5 无线→状态配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“无线→状态”，打开 WLAN 状态查看页面，对 WLAN 状态进行查看，如下图所示：




图 3-90 高级-无线配置

该页面主要显示设备无线口的信息，用户可以通过选择不同的 VAP 来查看不同的无线口。若当前 VAP 配置为 STATION 模式，则该页面显示要连接的 AP 信息、发射功率、信号强度、传输速率、频率等信息；若当前 VAP 配置为 AP 模式，则该页面显示所有连接到该页面的 STATION 信息，包括 MAC 地址、发送速率、接收速率等。

点击“刷新”可以实时更新 VAP 下的用户列表，点击“Kick”可以强制踢掉某一个用户下线，点击“选择 VAP”下拉框可以选择查看不同的 VAP 用户列表，如下图所示：



图 3-91 高级-无线配置

 注意：使用“Kick”对某个客户端进行解关联，但是客户端可以再次自动关联到 AP。

3.10.6 无线→动态频率选择

输入用户名和密码，登录设备高级管理页面，点击左侧菜单“无线→状态”，打开 WLAN 状态查看页面，对 WLAN 状态进行查看，如下图所示：



图 3-92 高级-无线配置

可以选择设备的工作射频，打开或关闭动态频率选择功能

检测周期：触发动态频率选择的周期。

优于当前信道门限：动态频率选择时，信号强度差值需要高于此门限。

连续优于当前信道次数：动态频率选择时，切换信道需要连续优于当前信道的次数。



注意：只能用于我司设备直接连接，点对点，或点对多点网桥情景下使用。

3.11 高级模式—网络配置

3.11.1 网络→路由配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→路由”打开路由配置页面，如下图所示：



图 3-93 高级-网络配置

路由就是通过互联的网络把信息从源地址传输到目的地址的活动。路由发生在 OSI 网络参考模型中的第三层，即网络层路由引导封包转送，经过一些中间的节点后，到它们最后的目的地。做成硬件，则称为路由器。路由通常根据路由表（一个储存到各个目的地的最佳路径的表）来引导封包转送。因此为了有效率的转送封包，建立储存在路由器内存内的路由表是非常重要的。

点击“**新建**”添加新的静态路由信息，如下图所示：



图 3-94 高级-网络配置

按照实际组网添加正确的目的地址、目的地址子网掩码、网关信息，配置不同的跳数来区别不同的优先级，跳数越小优先级越高，最高为 0；指定正确的接口为数据发送的接口，如下图所示：

添加完成之后，点击“应用变更”使之生效。

操作完成之后，点击“保存”设备下一次重启之后使配置生效。



注意：静态路由信息添加之后无法编辑修改，只能删除之后重新添加。



注意：路由添加需要用户熟悉网络的拓扑连接，而且在网络拓扑发生变动时，也需要用户手工修改路由路径。如果路由信息配置不当，可能导致网络访问异常。

3.11.2 网络→地址解析（ARP）

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→地址解析”打开路由配置页面，如下图所示：



图 3-95 高级-网络配置

ARP: ARP(Address Resolution Protocol, 地址解析协议)是获取物理地址的一个 TCP/IP 协议。某节点的 IP 地址的 ARP 请求被广播到网络上后, 这个节点会收到确认其物理地址的应答, 这样的数据包才能被传送出去。

静态 ARP: 有些时候, 您需要具体的某个 IP 地址到硬件地址的映射关系, 而您很清楚这样的关系, 那么您就可以手动将其添加为永久性的 ARP Cache (高速缓存) 条目。

动态 ARP: ARP Cache (高速缓存) 中的大部分 ARP 映射条目都是系统自动生成的, 这取决于您设备的具体使用情况, 而且产生这些 ARP 条目的方法也是十分丰富的。

添加 ARP: 用户可以是一个 IP 地址和其对应的硬件地址组成一个映射来添加 ARP 条目, 这里的硬件地址通常是设备的 MAC 地址。

3.11.3 网络→NAT 配置

输入用户名和密码, 登录设备管理页面, 点击左侧菜单“网络→NAT”打开 NAT 配置页面, 如下图所示:



图 3-96 高级-网络配置

NAT(Network Address Translation, 网络地址转换)是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中, NAT 主要用于实现私有网络访问公共网络的功能。

点击“新建”可以添加新的 NAT 条目, 如下图所示:



图 3-97 高级-网络配置

操作完成之后点击“保存”, 设备下一次重启之后使配置生效。

源地址 NAT: 把 IP 包头中的源地址替换为指定的地址，应用场景：但我们有一个主机共享一个 Internet 连接时，我们可以通过源地址转换，把这些主机发出的 IP 包中的源地址，修改为所共享的 Interface 连接的地址。在实际使用时，可以根据需要把 IP 包中的端口也做转换。

目的地址 NAT: 把 IP 包头中的目的地址进行替换。应用场景：但在局域网内有一个 Web 服务器想要让 Interface 上的用户访问时，可以在防火墙上启用 DNAT，防火墙会把他收到的 HTTP 数据包，修改目的地址为内网的 Web 服务器地址。

伪装: 作用类似于源地址 NAT，但是不用指定共享的地址，仅需设定出接口和需要转换的地址。

3.11.4 网络→路由转发控制配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→路由转发控制”，打开路由转发控制配置页面，如下图所示：



图 3-98 高级-网络配置

用户可以通过添加路由转发规则来控制路由数据的转发。该设备实现方案是开启路由转发控制后，仅允许符合规则的数据包被转发。

该功能默认关闭，需要勾选“使能”开关并点击“应用变更”开启该功能，开启后默认缺省策略生效，可选“禁止→拒绝所有数据包转发”或者“允许→允许所有数据包转发”。

点击“新建”添加新的规则，类型可以选择“IP”或者“MAC”如下图所示：



图 3-99 高级-网络配置

名称：填写可唯一标识该规则的命名，不可由纯数字组成。

使能：勾选该选项之后该规则生效。

类型：可选则基于 IP 地址或者基于 MAC 地址过滤。

IPv4 源地址：可输入某一个 IP 地址、某一整段子网掩码 IP 地址、某几个不连续 IP 地址、某一段连续 IP 地址或者保持空值。

IPv4 目的地址：可输入某一个 IP 地址、某一整段子网掩码 IP 地址、某几个不连续 IP 地址、某一段连续 IP 地址或者保持空值。


双向：可以将报文的源地址和目的地址同时转换，这个功能应用于内部网络主机地址与公网上主机地址重叠的情况。

包数限制：默认为 0，也可设定限制的包数大小。

策略：选择该规则下的数据包策略是 Deny 拒绝还是 Allow 允许。

添加完成之后，点击“应用变更”使配置生效，如下图所示：

操作完成之后点击“保存”使配置下一次重启之后生效。

 **注意：**新建路由转发控制列表填写“名称”时不可以填写纯数字，并且不可以数字开头。

3.11.5 网络→流量控制

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络-流量控制”配置页面。可以通过流量控制来控制用户使用的流量，可以通过整个接口分配实现对用户流量的限制，也可以通过单用户对用户进行流量限制，如下图所示：



图 3-100 高级-网络配置

也可以通过 MAC 地址，配置固定用户的流量限制。

3.11.6 网络→DMZ 配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→DMZ”打开 DNS 配置页面，如下图所示：

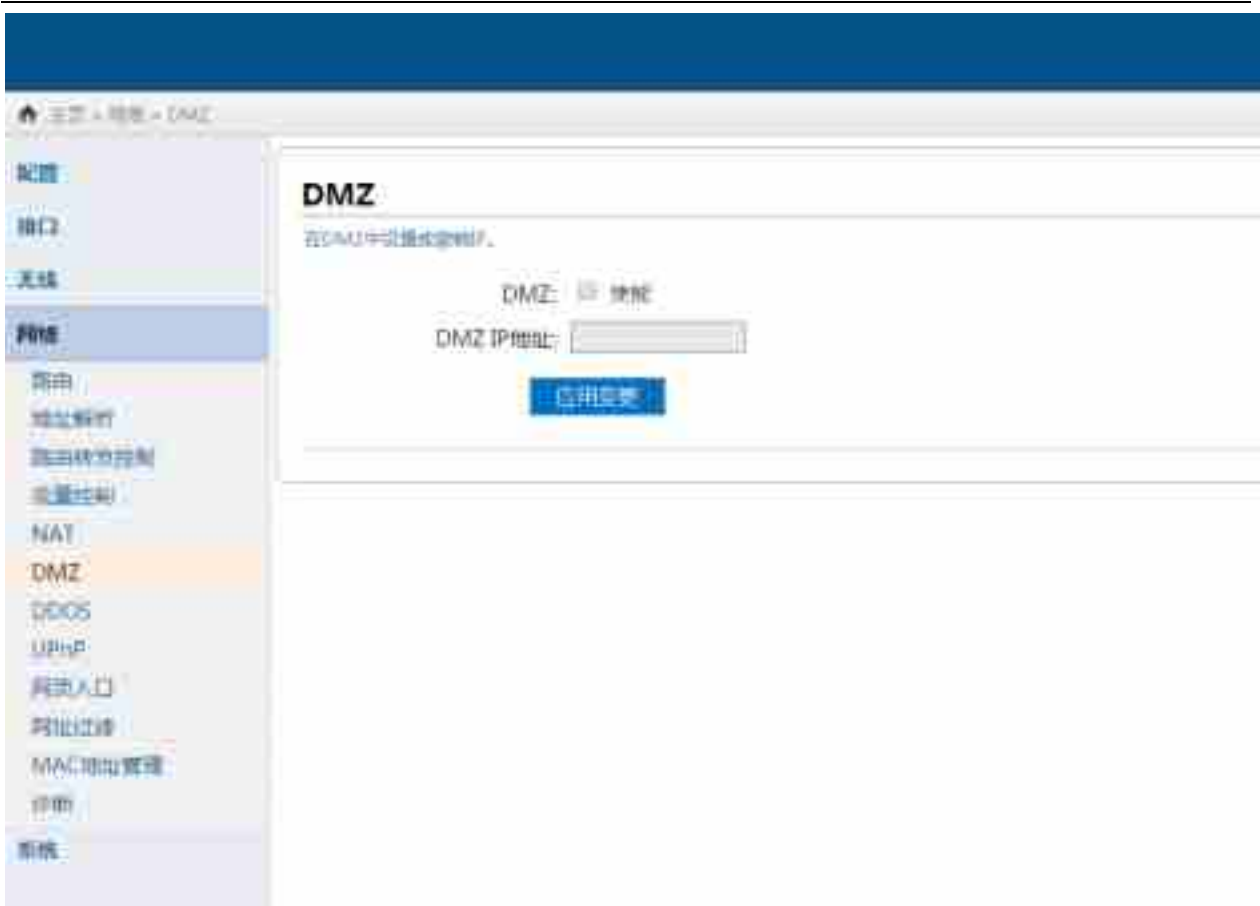


图 3-101 高级-网络配置

什么是 **dmz**:

DMZ(Demilitarized Zone)即俗称的非军事区，DMZ 可以理解为不同于外网和内网的特殊网络区域，DMZ 内通常放置一些不含机密的信息的公用服务器，比如 Web，Mail，FTP 等，这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到内网的机密信息，即使 dmz 服务器受到破坏，也不会对内网中的机密信息造成影响。

dmz 策略:

- (1)内网可以访问外网。
- (2)内网可以访问 DMZ。
- (3)外网不能访问内网。
- (4)外网可以访问 DMZ。
- (5)DMZ 不能访问内网。
- (6)DMZ 不能访问外网(有例外)

DMZ 使用:

可以将所有提供给外部用户使用的服务放置在 DMZ 服务器上，通常这些服务包括 WEB 服务器，邮件服务器，FTP 服务器，VoIP 服务器等。

DMZ 注意事项

DMZ 使用防火墙方案为要保护的内部网络增加了一道安全防线，通常认为是非常安全的。同时它提供了一个区域放置公共服务器，从而又能有效地避免一些互联应用需要公开，而与内部安全策略相矛盾的情况发生。在 DMZ 区域中通常包括堡垒主机、Modem 池，以及所有的公共服务器。DMZ 服务器只能用作用户连接，真正的后台数据需要放在内部网络中。

添加完成之后，点击“应用变更”使配置生效，如下图所示：

操作完成之后，点击“保存”，设备下一次重启之后使配置生效。

3.11.7 网络→DDOS

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→DDOS”打开 DDOS 配置页面，用户可以通过防火墙配置来加固网络安全性，如下图所示：



图 3-102 高级-网络配置

可以抵御一些常见的 DDOS（分布式拒绝服务）攻击。

操作完成之后，点击“应用变更”使之生效。

操作完成之后点击“保存”，设备下一次重启之后使配置生效。

3.11.8 网络→UPNP

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→UPnP”打开UPnP配置页面如下图所示：



图 3-103 高级-网络配置

注意事项：

1. 只有使用支持UPnP协议的应用程序（比如迅雷、电驴、PPLive、BT、MSN），才有必要开启本功能。
2. 因为现阶段版本的UPnP协议的安全性还未得充分保证，不使用时请关闭UPnP功能。
3. UPnP功能需要操作系统的支持(如Windows ME/Windows XP/Windows Vista/Windows 7)。

3.11.9 网络→网页入口

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→网页入口”打开网页入口配置页面如下图所示：



图 3-104 高级-网络配置

网页入口是指 Portal 认证的高级配置。

使能：只有选中使能，才能使用网页入口功能。

认证模式：用户通过网页认证的具体方式，分为直接认证、本地认证、远程认证、域控认证四种。

本地认证：用户需按照用户管理中的配置方式完成认证

远程认证：此方式用于网页认证的服务器在设备以外，认证流程由外置服务器决定。结合网管服务器可实现网页认证用户在不同 AP 之间的无缝漫游。

域控认证：域控服务器项应如下填写：

域服务器 IP：端口@根域名，如果有多个域，如

1.1.1.1:389@ad.com,2.2.2.2:389@ad2.com。

远程认证 URL：给用户重定向到的远程页面。

认证通过后跳转链接：当用户网页认证通过后，自动跳转到的 URL。若未设置，则跳转到用户最初所要访问的 URL。

登录进度条时长：当采用本地认证的确认认证或登录认证时，提交认证请求后，进度条的展示时间。

网页标题：在登录页面上显示的标题。提示：可使用
标签实现换行。

管理服务器：使能此选项，可通过云 AC 控制 Portal 用户的上下线，且支持 Portal 用户在不同设备间的无缝漫游。关闭此选项，则远程 Portal 服务器直接控制此设备的 Portal 用户上下线，但不支持在不同设备间的漫游。

保活周期：只有使能管理服务器时，才有此选项。设备每个保活周期向云 AC 发送一次保活，当连续 3 次未收到保活响应时，设备关闭 Portal 服务，保证接入的用户可正常使用网络。当保活响应正常时，则再次开启 Portal，用户可认证后正常使用网络。

开放资源：用户未完成 Portal 认证时，即可以访问的 IP 地址或域名。

高级配置：包含最大用户数、空闲超时时间、强制超时时间等配置。

缺省 DNS 返回 IP：当用户的 DNS 请求失败时，返回此缺省 IP 地址作为 DNS 请求的结果，保证能正常弹出网页入口页面。

3.11.10 网络→网址过滤

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→网址过滤”打开网址过滤配置页面如下图所示：



图 3-105 高级-网络配置

过滤模式：黑名单即不能访问的网址名单；白名单即只可以访问的网址名单

重定向页面：当用户访问的链接被拒绝时，将其重定向到我们所期望的页面。

时间策略：可以用时间段来限制用户访问的网址

3.11.11 网络→MAC 地址管理

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→MAC 地址管理”打开配置页面，如下图所示：



图 3-106 高级-网络配置

MAC 地址管理：该页面主要用于管理 Mac 地址及其别名。设置之后，在其他页面也会关联 mac 和别名。

批量导入：支持 CSV 格式的 EXCEL 文件导入，格式要求为两列，第一列为别名，第二列为 MAC 地址。格式错误的信息会被忽略！如果 MAC 地址重复，则新的别名会覆盖旧的。中文字符只支持 UTF-8 编码。

3.11.12 网络→诊断配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“网络→诊断”打开网络诊断配置页面，如下图所示：



图 3-107 高级-网络配置

用户可以通过网络诊断中的 Ping 功能用来检测设备和目标设备是否已连通及连接延时等。在“地址”栏输入远端 IP 地址或域名，点击“ping”按钮，系统将自动对该地址进行 ping 操作，等待执行结束之后会在工作区返回 ping 操作结果，包括丢包、延时等信息。如下图所示：

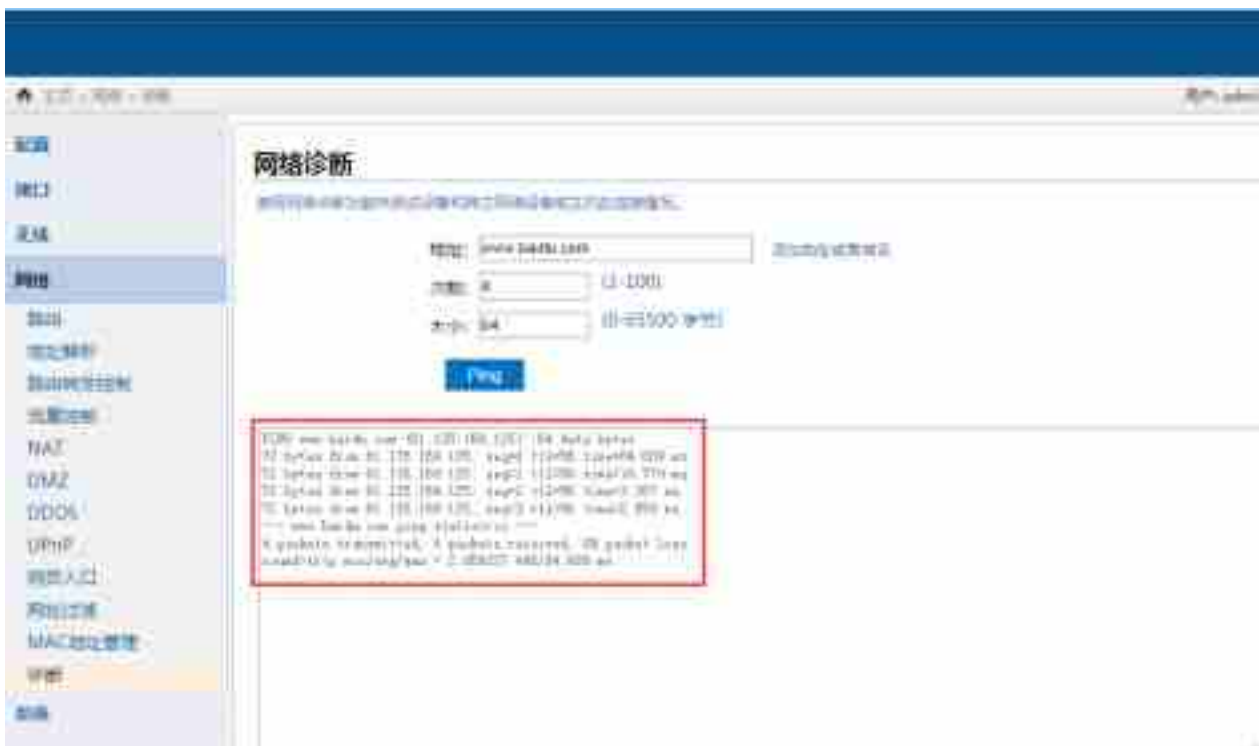


图 3-108 高级-网络配置

3.12 高级模式—系统配置

3.12.1 系统→配置管理配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“系统→配置管理”打开配置管理页面，用户可以通过配置管理页面对系统配置文件进行修改操作，如下图所示：



图 3-109 高级-系统配置

点击“保存”可以将当前配置保存到配置文件中，系统会提示操作成功或者失败，如下图所示：



图 3-110 高级-系统配置

点击“**恢复缺省**”可以将设备配置恢复到出厂设置，默认管理地址为 **192.168.1.1**，用户名和密码均为 **admin**。恢复缺省之后系统会提示“**重启设备?**”然后点击“**确定**”，如下图所示：



图 3-111 高级-系统配置

点击“**导出**”可以从设备中读取当前配置文件，并上传到 **PC** 机，如下图所示：

在弹出的窗口中点击“**保留**”，将设备当前配置文件上传到 **PC** 指定路径下。

点击“**选择文件**”可以读取 **PC** 上保存的配置文件，如下图所示：




图 3-112 高级-系统配置

点击“选择文件”选择 PC 上对应的配置文件，点击“加载”按钮导入该配置文件，然后会弹出窗口提示“重启设备？”然后点击“确定”，如下图所示：



图 3-113 高级-系统配置

 注意：恢复出厂配置和加载配置文件操作完成之后都需要重启设备使生效。

 注意：恢复出厂配置后设备管理 IP 和管理账号密码均恢复为缺省参数。

3.12.2 系统→设备管理配置

输入用户名和密码，登录设备前台管理页面，点击“系统→设备管理”菜单，打开设备管理页面，如下图所示：



图 3-114 高级-系统配置

点击“重启”可以重启这台设备，如果碰到设备工作不正常，可以尝试重启设备，如下图所示：



图 3-115 高级-系统配置

延迟重启：一段时间后进行重启命令

更新固件：可以从这里给设备升级到新版本，一般来说新的版本提供了更为强大的功能，运行也更加的稳定。当您获得新版本文件之后，只需要从这里点击浏览按钮，然后找到版本文件。点更新就可以给设备升级了。(在升级过程中，切记不能断电.)

点击“确定”完成设备重启，此时系统将提示操作成功，并且在工作区出现重启进度条，如下图所示：



注意：设备重启和固件版本升级前，请确保配置已保存。



警告：升级过程中切勿断电，防止造成系统故障。

3.12.3 系统→用户管理配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“系统→用户管理”打开用户管理页面，如下图所示：



图 3-116 高级-系统配置

系统默认的 admin 帐号不允许更改，但是您可以修改该帐号的密码。

密码最少 4 个字符，允许使用英文、符号或数字。

3.12.4 系统→时间配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“系统→时间”打开时间管理页面，如下图所示：



图 3-117 高级-系统配置

设备上电启动以后，默认时间是从 1970 年开始的。设备可以通过 NTP 功能，从网络里的 NTP 服务器获取当前时间。在当前的 Internet 环境中，有很多服务器都提供 NTP 服务。如果启用该功能，则需要填入 NTP 服务器的 IP 地址。另外，由于 NTP 获取到的时间默认是格林威治时间(时区 0)，所以还需要正确设置时区，设备才能正确的显示当地时间。

设备获取当前时间有三种方式：

NTP 服务器：需要开启 NTP 服务，配置一个正确的 NTP 服务器 IP 地址，例如 210.72.145.44 国家授时中心服务器地址。选择正确的时区，点击“**应用变更**”，系统会自动和对应的 NTP 服务器同步系统时间。

使用 NTP 服务同步系统时间需要设备能访问 Internet。

获取浏览器时间：设备还可以通过获取客户端浏览器时间来同步系统时间，如下图所示：




图图 3-118 高级-系统配置

点击“获取浏览器时间”后，工作区的日期和时间会立即同步浏览器当前时间，使用“获取浏览器时间”功能，前提需要保证设备和某一台 PC 链路正常。

操作完成之后点击“应用变更”使之生效。

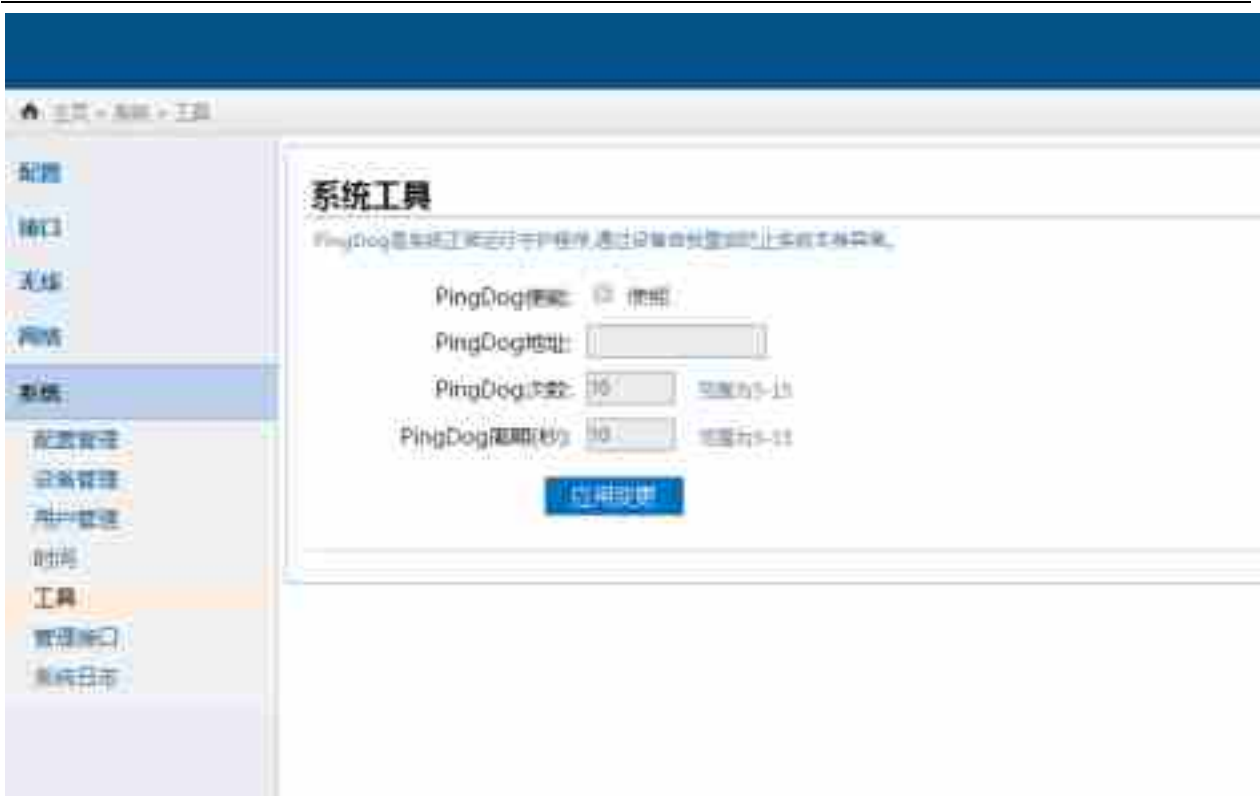
操作完成之后点击“保存”，设备下一次重启之后使配置生效。

 注意：当系统恢复缺省配置之后系统时间也将恢复缺省。

 注意：使用 NTP 服务时必须保证设备能访问 Internet。

3.12.5 系统→工具

输入用户名和密码，登录设备管理页面，点击左侧菜单“系统→工具”打开工具管理页面，如下图所示：



3-119 高级-系统配置

Pingdog 功能可以对链路进行检测，当链路不通时会重启设备。


需要输入一个 IP 地址(请确保该 IP 地址是存在且可以 ping 通的)来启用这个功能，该功能启用以后，此设备会持续的 ping 指定的 IP 地址，如果连续 10 次 ping 不通，设备就会自动重启。该功能默认关闭，根据实际情况选择是否开启。

勾选“使能”开关，开启 Pingdog 功能，在“**Pingdog 地址**栏”输入一个合法的 IP 地址，然后输入 pingdog 的次数和周期，如下图所示：



点击“应用变更”后生效，此时设备会持续 ping 192.168.66.53，如果连续 10 次不通设备将会重启。

操作完成之后，点击“保存”，设备下一次重启之后使配置生效。

 注意：此功能开启可能会导致设备自动重启，请谨慎操作。

3.12.6 系统→管理接口配置

输入用户名和密码，登录设备管理页面，点击左侧菜单“系统→管理接口”打开管理接口页面，如下图所示：



3-121 高级-系统配置

“主机名”当远程 telnet、ssh 登陆设备时显示该参数，可以保持默认值。主机名只支持英文字符和数字输入，重启后生效。

“设备编码”可输入具体的名称来唯一标识该设备信息，可以保持默认值。设备编码只支持英文输入，例如可以根据设备编码标识设备安装位置。

“网元编码”可以为该设备命名网元编码，该编码在网络中具备唯一性，主要给网管使用，用来区分每一个网元。

“位置信息”可以为该设备设置位置信息，主要给网管使用，便于确定设备所在的大体位置。

“经度、纬度”可以为该设备设置经度、纬度，主要给网管使用，便于确定设备所在的精确位置，设置如下图：

“**Https 配置**”使能开关默认关闭，开启之后可以通过 SSL 协议方式登录，比 HTTP 更安全，如下图所示：

“**Https 配置**”使能后，可以通过安全方式登录。

“**Tunnel 配置**”使能后，代表开启设备上的 Tunnel 服务器，其他用户可通过 tunnel 来访问本地 80 端口，主要用于网管的集中管理。

“**Telnet 配置**”使能开关默认关闭，开启之后可以允许远程通过 telnet 方式登录、管理设备。

“**SSH 设置**”使能开关默认关闭，开启之后可以允许远程通过 SSH 方式登录、管理设备。

“**SNMP 配置**”使能开关默认关闭，开启之后使网管可以通过 SNMP 协议管理 AP。

“**Trap 服务器地址**”默认为空，指定接收 Trap 的网管的 IP 地址。

“**服务器 IP 地址**”默认为空，一般由网管来下发 IP 地址，地址后面跟的是端口号。

“**周期**”、“**保活周期**”默认为空，一般由网管来下发，其值为 BMS 和 CPE 间的保活报文上报间隔。

操作完成之后，点击“**应用变更**”使之生效。

操作完成之后，点击“**保存**”，设备下一次重启之后使配置生效。



注意：当开启 Telnet 服务和 SSH 服务时，设备会有更大几率受到恶意攻击，请慎用。

3.12.7 系统→系统日志

输入用户名和密码，登录设备管理页面，点击左侧菜单“**系统→系统日志**”打开设备日志页面，如下图所示：



图 3-122 高级-系统配置

用户可以通过设备日志页面查看系统日志及配置日志服务器，并且通过日志来分析定位系统故障。勾选“远程日志使能”之后，可以开启远程日志功能，需要指定一个日志服务器 IP 地址，系统将发送系统日志到此服务器。

“**远程日志服务器**”在开启远程日志服务之后，需要配置一个日志服务器 IP 地址。

“**诊断信息**”中记录着该设备的大量运行信息，包括进程信息、CPU 利用率、内存使用情况、接口状态、无线信息等，你可以从中找到一些线索，来帮助你掌握设备运行状况，解决问题。

点击“**生成**”，会生成诊断信息。

生成诊断信息后，点击“**导出**”，会导出诊断信息到本地。

操作完成之后，点击“**应用变更**”使之生效。

操作完成之后，点击“**保存**”设备下一次重启之后使配置生效。



注意：日志信息对于故障定位、排查很有帮助，当出现故障之后，应第一时间分析并且备份日志信息。

4 常见故障排除

1. 设备有效覆盖区域内信号强度低，无法正常使用

- 首先确认测试点是否在设备有效覆盖区域内。
- 登陆设备管理页面，查看射频卡发射功率，确保发射功率正常。
- 登陆设备管理页面，查看国家码，不同的国家码影响发射功率。
- 如果是定向设备，确认天线俯仰角是否合适。
- 如果是全向设备，确认设备是否按照规范安装，确认设备高度计算覆盖盲区。
- 确认测试点和设备是否可视，最好保证测试点和设备完全可视。

2. 设备安装完成之后 PoE 指示灯不亮

- 确认供电线路是否正常。
- 确认 PoE 模块是否正常，是否为出厂原配 PoE。
- 确认设备、PoE 两端的网线接口连接正确。
- 确认网线质量、网线长度、水晶头工艺符合规范要求。

3. 设备安装完成之后测试吞吐量低

- 确认测试点是否在设备有效覆盖区域内。
- 确认信号强度、信号波动正常。
- 查看测试终端网卡属性是否开启节电模式。
- 确认 ping 包测试是否正常。
- 登陆设备查看用户列表是否有其他用户影响。
- 确认周围是否有其他无线信号恶意干扰。
- 确认测试终端是否正常，例如操作系统是否中毒，可以尝试替换其他终端对比测试。
- 分别测试有线链路和无线链路吞吐量，定位问题。
- 有线侧吞吐量低则排查网线、PoE 模块、交换机。
- 无线侧吞吐量低则排查无线环境、尝试更换信道，调整天线角度。

4. 设备下用户 ping 外网延时过大、丢包

- 更换测试终端对比测试。
- 分步 ping 包测试，将整个测试分解为测试终端到设备、设备到网关、网关到外网，执行分步 ping

测试之后分析定位故障原因，解决故障。

- 测试终端到设备侧 ping 包延时过大、丢包则尝试调整设备信道、发射功率、安装角度。
- 设备到网关侧 ping 包延时过大、丢包则排查设备到网关有线侧链路，着重排查 PoE 到设备的长

网线及 PoE 到交换机的短网线，也不排除个别光纤链路故障。

-
- 网关到外网侧 ping 包延时过大、丢包需要上报网络运营商协助排查。

5. 设备信号时有时无

- 确认测试点是否在设备的主瓣信号覆盖区域，旁瓣信号和反射信号有时候很强但是很不稳定。
- 当设备受到严重干扰时会出现这种情况，请进行信道扫描并选择最佳的可用信道，如果无法选择可用信道请更换设备安装位置以避开干扰。
- 确认设备供电是否正常，供电电压不稳也会导致信号时有时无，严重时会导致设备重启。

6. 客户端无法连接到设备的 SSID

- 确认是否能够搜索到设备发出的无线信号(SSID)，如果搜索不到，请确认设备侧无线接口是否开启、用户侧无线设备开关是否开启。
- 查看信号强度，如果信号太弱请换到一个信号较好的地方，或者使用研华 BXOCPE 系列产品对信号进行中继放大从而延伸设备覆盖范围。
- 如果信号强度较好，仍然连接不上，请重启无线网卡，刷新无线网络列表后再次进行连接。
- 如果信号强度很好，多次重启网卡后依然连接不上，请确认该 SSID 的认证方式是否正确。
- 登陆设备管理页面，确认设备配置是否对用户进行策略限制。

7. 客户端可以正常关联，但是无法上网

- 请检查 PC 机的 IP 地址等网络参数配置。
- 如果进行了数据加密，请确认无线信号的数据加密的加密方式和密钥是否正确。
- 登陆设备管理页面确认用户信息是否存在，避免用户关联到虚假 SSID。

8. 使用过程中时常掉线

- 首先确认该问题是单个用户问题还是设备下所有用户问题。
- 确认用户终端是否正常，可以尝试使用其他终端对比测试。
- 确认该位置信号强度是否正常、信号波动是否稳定。
- 如果用户使用 CPE 设备则排查终端到 CPE 之间有线链路是否正常、CPE 安装角度、方向、位置是否正确。
- 如果设备下所有用户存在该问题则排查设备信号是否正常、有线侧链路是否正常、检查设备周围无线环境尝试更换信道。

9. 用户无法弹出 Portal 页面

- 首先确认该问题是单个用户问题还是设备下所有用户问题。
- 单个用户问题则排查用户终端 IP 地址等网络参数配置、用户终端问题。

-
- 整个设备下共性问题则排查 AC、AP 侧配置是否正确；AP 上层链路是否正常。
 - 可以尝试在设备端通过有线连接网络检查有线侧链路和 Portal 服务器，如果通过有线能正常推送

Portal 则着重排查 AC、AP 配置。

10. 能上 QQ 但是无法打开网页

- 确认用户终端 IP 地址等网络参数配置是否正确，尤其是 DNS。
- 确认用户访问的网站为合法网站，没有被防火墙等安全策略过滤。
- 尝试更换终端测试。

11. 客户端 PPPoE 拨号失败

- 确认网络连接是否正常，网卡是否禁用。
- 根据返回错误代码初步判断故障原因，常见错误代码：
 - a) 错误 678，拨入方计算机没有应答，无法完成拨号网络连接，一般为局端问题，检查网线和网卡是否正常。
 - b) 错误 691，用户名密码错误，确认用户名密码是否正确，并且确认该用户是否欠费。
 - c) 错误 718，验证用户名时远程计算机没有响应，一般为 ADSL ISP 服务器故障。
 - d) 错误 720，拨号网络无法协调网络中服务器的协议设置，一般为非正常关机操作造成网络协议出错，删除所有网络组件重新安装网络。
 - e) 错误 738，服务器不能分配 IP 地址，ADSL ISP 服务器故障，ADSL 用户太多超过 ISP 能提供的 IP 地址。

12. 用户无法搜索到无线信号

- 确认当地环境存在无线网络覆盖。
- 确认用户网卡是否被禁用。
- 笔记本无线网卡硬件开关是否关闭。
- 用户开启了无线网卡软件配置客户端(例如 Inter 网卡开启了 Inter 配置软件，那么 Windows 自带的无线网卡软件将无法正常工作)。
- 设备是否正常工作。
- 信号强度是否很弱，导致用户无法搜索到该信号。

13. 用户无法获取 IP 地址

- 运行“cmd” --- “ipconfig/renew” 尝试查看“ipconfig”是否解决。
- 客户端网卡故障，禁用后启用网卡或者重启 PC 尝试解决。

-
- 业务 vlan 不通，需要各二层设备透传业务 vlan 数据，找维护部门确认。
 - DHCP server 的 IP 地址池中地址用完。

该页面显示设备、Radio 和 wlan 的信息。

设备信息包括设备类型名称、设备工作模式、eth0MAC、管理 IP 地址、设备硬件版本、设备固件版本和序列号。

Radio 信息包括 wifi0 和 wifi1 两块射频卡的工作模式、信道、功率、带宽、beacon 间隔时间、ACK timeout 时间和 short GI 开关信息。

wlan 信息会显示设备所有 VAP 信息；FitAP 默认没有发射 ESSID，所以显示为空。

5 附录

5.1 技术参数

表 6-1 定向设备安装高度/下倾角对照表

定向天线下倾角度		覆盖距离(米)				
		500	800	1000	1500	2000
天线高度 (米)	40	4° - 5°	3°	2° -3°	1° -2°	1°
	50	6°	3° 4°	3°	2°	1° -2°
	60	7°	4° -5°	3° -4°	2° -3°	1° -2°
	70	8°	5°	4°	2° -3°	2° -3°
	80	9° -10°	6°	4° -5°	3° -4°	2° -3°
	100	11° -12°	7° -8°	5° -6°	4°	3°
	120	13° -14°	8° -9°	6° -7°	4° -5°	3° -4°
	150	16° -17°	10-11°	8° -9°	5° -6°	4° -5°

5.2 术语表

表 6-2 国家/区域频率划分列表

国家/区域	5G 频段	2.4G 频段
澳大利亚	36-64,149-165	1-13
奥地利	36-48	1-13
加拿大	36-64,149-165	1-11
中国	149-165	1-13
丹麦	36-64,100-140	1-13
芬兰	36-64,100-140	1-13
法国	36-64	1-13
德国	36-64,100-140	1-13
香港	36-64,149-165	1-13
冰岛	36-64,100-140	1-13
爱尔兰	36-64,100-140	1-13
意大利	36-64,100-140	1-13
日本	34-46	11g: 1-13 11b: 1-14
列支敦士登	36-64	1-13
卢森堡	36-64,100-140	1-13
荷兰	36-64,100-140	1-13
新西兰	36-64,149-165	1-13
挪威	36-64,100-140	1-13
葡萄牙	36-64,100-140	1-13
新加坡	36-64,149-165	-13
西班牙	36-64,100-140	1-13
瑞典	36-64,100-140	1-13
瑞士	36-64	1-13
台湾	56-65,149-161	1-13
英国	36-64,100-140	1-13

国家/区域	5G 频段	2.4G 频段
美国	36-64,149-165	1-11

表 6-3 2.4G/5G 频率-信道列表

5G 信道	5G 中心频率(MHz)	2.4G 信道	2.4G 中心频率(MHz)
34	5170	1	2412
36	5180	2	2417
38	5190	3	2422
40	5200	4	2427
42	5210	5	2432
44	5220	6	2437
46	5230	7	2442
48	5240	8	2447
52	5260	9	2452
56	5280	10	2457
60	5300	11	2462
64	5320	12	2467
100	5500	13	2472
104	5520	14	2484
108	5540	/	/
112	5560	/	/
116	5580	/	/
120	5600	/	/
124	5620	/	/
128	5640	/	/
132	5660	/	/
136	5680	/	/
140	5700	/	/
149	5745	/	/
153	5765	/	/
157	5785	/	/
161	5805	/	/
165	5825	/	/

表 6-4 缩略语列表

序号	缩写	英文全称	中文解释
1.	AC	Access Controller	接入控制器
2.	ACK	Acknowledgement	确认字符，在数据通信传输中，接收站发给发送站的一种传输控制字符。它表示确认发来的数据已经接受无误。
3.	ACS	AdjacentChannel Selectivity	邻道选择性，是用来衡量存在相邻信道信号时，接收机在其指定信道频率上接收有用信号的能力，定义为接收机滤波器在指定信道上的衰减与在相邻信道上的衰减的比值。
4.	ADSL	Asymmetric Digital Subscriber Line	非对称数字用户环路，是一种新的数据传输方式。它采用频分复用技术把普通的电话线分成了电话、上行和下行三个相对独立的信道，从而避免了相互之间的干扰。
5.	AIFSN	Arbitration Inter Frame Spacing Number	仲裁帧间隙数在 802.11 协议中，空闲等待时长(DIFS)为固定值，而 WMM 针对不同 AC(接入分类)可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长，等待时间越短则获取信道的机会更大。
6.	airX	/	空间自适应最佳通信

序号	缩写	英文全称	中文解释
7.	A-MPDU	Aggregation MAC Protocol Data Unit	聚合 MAC 协议数据单元, A-MPDU 聚合的是经过 802.11 报文封装后的 MPDU, MPDU 是指经过 802.11 封装过的数据帧。
8.	A-MSDU	Aggregation MAC Service Data Unit	聚合媒介访问控制服务数据单元, 是指把多个 MSDU 通过一定的方式聚合成一个较大的载荷。
9.	AP	Access Point	接入点, 无线网络集线器(HUB)。无线客户端连接到接入点, 两个客户端之间的信息流量必须经过接入点。接入点经常简称为 AP。
10.	Beamforming	/	波束成形, 是发射端对数据先加权再发送, 形成窄的发射波束, 将能量对准目标用户, 从而提高目标用户的解调信噪比, 通常有两大类实现方式: MIMO Beamforming 和 DOA Beamforming。
11.	BSSID	Basic Service Set Identifier	广播式网络服务标识
12.	CAC	Call Admission Control	连接准入控制, 限制能使用高优先级队列(Voice 和 Video 队列)的客户端个数, 从而保证已经使用高优先级队列的客户端能够有足够的带宽。
13.	CHAP	Challenge Handshake Authentication Protocol	询问握手认证协议, 通过三次握手周期性的校验对端的身份, 在初始链路建立时完成, 可以在链路建立之后的任何时候重复进行。
14.	CPE	Customer Premise Equipment	客户端设备
15.	CWmax	Competition Window Maximum	最大竞争窗口, 决定了平均退避时间值, 和最小竞争窗口数值越大, 用户的平均退避时间越长。
16.	CWmin	Competition Window Miniature	最小竞争窗口, 决定了平均退避时间值, 这和最大竞争窗口数值越大, 用户的平均退避时间越长。
17.	dB	Decibel	是一个纯计数单位, 本意是表示两个量的比值大小, 没有单位, 对于功率, $dB = 10 \cdot \lg(A/B)$, 此处 A, B 代表参与比较的功率值。
18.	dBi	/	功率增益的单位, dBi 的参考基准为全方向性天线。
19.	dBm	/	即功率毫瓦, 功率与 P(瓦特)换算公式: $P_{dBm} = 30 + 10 \lg P$ (P: 瓦; P': 单位为 dbm), 0 dBm = 1mw。
20.	DDOS	Distributed Denial of Service	分布式拒绝服务攻击, 指借助于客户/服务器技术, 将多个计算机联合起来作为攻击平台, 对一个或多个目标发动 DoS 攻击, 从而成倍地提高拒绝服务攻击的威力。
21.	DHCP	Dynamic Host Configuration Protocol	动态主机配置协议。一种让服务器自动为客户端分配 IP 地址的协议, 而客户端不必再手动配置 IP 地址。
22.	DMZ	Demilitarized Zone	非军事化区, 作用是把 WEB, E-mail, 等允许外部访问的服务器单独接在该区端口, 使整个需要保护的内部网络接在信任区端口后, 不允许任何访问, 实现内外网分离, 达到用户需求。
23.	DNAT	Destination Network Address Translation	目的地址转换, 是将一组本地内部的地址映射到一组全球地址。
24.	DNS	Domain Name System	域名系统, 是因特网的一项核心服务, 它作为可以将域名和 IP 地址相互映射的一个分布式数据库, 能够使人更方便的访问互联网, 而不用去记住能够被机器直接读取的 IP 地址。
25.	DOS	Denial of Service	拒绝服务, 一种常用来使服务器或网络瘫痪的网络攻击手段。
26.	DSSS	Direct Sequence Spread Spectrum	直接序列展频技术, 通过利用高速率的扩频序列在发射端扩展信号的频谱, 而在接收端用相同的扩频码序列进行解扩, 把展开的扩频信号还原成原来的信号。

序号	缩写	英文全称	中文解释
27.	DTIM	Delivery Traffic Indication Message	投递传输指示信息，DTIM=1 表示每个 beacon 中都包含 DTIM，DTIM=2 表示每两个 beacon 中包含一个 DTIM，以此类推。
28.	EAP	Extensible Authentication Protocol	可扩展认证协议，是一种在 802.1x 中使用的标准信息格式。
29.	EDCA	Enhanced Distributed Channel Access	增强的分布式信道访问，是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。
30.	EMC	Electro Magnetic Compatibility	电磁兼容性，是指设备或系统在其电磁环境中符合要求运行并不对其环境中的任何设备产生无法忍受的电磁干扰的能力。
31.	ESSID	ExpandService Set Identifier	扩展的网络服务标识
32.	FatAP	/	Fat AP 是与 Fit AP 相对来讲的，Fat AP 将 WLAN 的实体层、加密、用户认证、网路管理等功能集于一身，即俗称的胖 AP。
33.	FCC	Federal Communications Commission	美国联邦通讯委员会，负责授权和管理除联邦政府使用之外的射频传输装置和设备。
34.	FitAP	/	Fit AP 是一个只有射频和通信功能的 AP，功能单一，不能独立工作，即俗称的瘦 AP。
35.	FTP	File Transfer Protocol	文件传输协议，是应用层的协议，它基于传输层，为用户服务，它们负责进行文件的传输。
36.	HTTP	Hypertext Transport Protocol	超文本传送协议，一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。
37.	IEEE	Institute of Electrical and Electronics Engineers	美国电气和电子工程师协会，是一个国际性的电子技术与信息科学工程师的协会，是世界上最大的专业技术组织之一。
38.	IKE	Internet Key Exchange	Internet 密钥交换协议，解决了在不安全的网络环境(如 Internet)中安全地建立或更新共享密钥的问题。
39.	IP	Internet Protocol	网络之间互连的协议，是为计算机网络相互连接进行通信而设计的协议。
40.	IP-67	Ingress Protection Rating	防护安全级别，6 代表防尘禁锢：尘埃无法进入物体整个直径不能超过外壳的空隙。7 代表防短时浸泡常温常压下，当外壳暂时浸泡在 1M 深的水里将不会造成有害影响。
41.	IPSEC	Internet Protocol Security	Internet 协议安全性，是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。
42.	Ipv4	Internet Protocol Version 4	网际协议版本 4，是互联网协议(Internet Protocol, IP) 的第四版，也是第一个被广泛使用，构成现今互联网技术的基石的协议。
43.	Ipv6	Internet Protocol Version 6	IPv6 是 IETF(互联网工程任务组，Internet Engineering Task Force)设计的用于替代现行版本 IP 协议(IPv4)的下一代 IP 协议。
44.	ISP	Internet Service Provider	互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务、和增值业务的电信运营商。
45.	L2TP	Layer 2 Tunneling Protocol	第二层隧道协议，是用来整合多协议拨号服务至现有的因特网服务提供商点。
46.	MAC	Medium Access Control	介质访问控制，定义了数据帧怎样在介质上进行传输。
47.	MCS	Modulation and Coding Scheme	调制与编码策略，802.11n 射频速率的配置通过 MCS 索引值实现。
48.	MIMO	Multiple-Input Multiple-Output	多出堕入技术，是一项运用于 802.11n 的核心技术。

序号	缩写	英文全称	中文解释
49.	MTBF	Mean Time Between Failure	平均无故障时间, 是衡量一个产品(尤其是电器产品)的可靠性指标。单位为小时。
50.	MTU	Maximum Transmission Unit	最大传输单元, 是指一种通信协议的某一层上面所能通过的最大数据包大小(以字节为单位)。
51.	NAT	Network Address Translation	网络地址转换, 是一种将私有(保留)地址转化为合法 IP 地址的转换技术, 它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。
52.	NTP	Network Time Protocol	网络时间协议, 是用来使计算机时间同步化的一种协议。
53.	OFDM	Orthogonal Frequency Division Multiplexing	正交频分复用技术, 将信道分成若干正交子信道, 将高速数据信号转换成并行的低速子数据流, 调制到在每个子信道上进行传输。
54.	OSI	Open System Interconnect	开放式系统互联, 国际标准化组织(ISO)制定了 OSI 模型。这个模型把网络通信的工作分为 7 层, 分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。
55.	PAP	Password Authentication Protocol	密码认证协议, 是 PPP 协议集中的一种链路控制协议, 主要是通过使用 2 次握手提供一种对等节点的建立认证的简单方法, 这是建立在初始链路确定的基础上的。
56.	PC	Personal Computer	个人计算机
57.	Ping	/	一个通信协议, 是 ip 协议的一部分, TCP/IP 协议的一部分, 利用它可以检查网络是否能够连通。
58.	PMK	Pairwise Master Key (Wireless Protocol Security Mechanism)	双万能钥匙(无线协议的安全机制)
59.	POE	Power Over Ethernet	有源以太网, 指的是在现有的以太网 Cat.5 布线基础架构不作任何改动的情况下, 在为一些基于 IP 的终端(如 IP 电话机、无线局域网接入点 AP、网络摄像机等)传输数据信号的同时, 还能为此类设备提供直流供电的技术。
60.	PPP	Point to Point Protocol	点对点协议, 为在点对点连接上传输多协议数据包提供了一个标准方法。
61.	PPPoE	Point-to-Point Protocol over Ethernet	以太网上的点对点协议, 可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。
62.	PPTP	Point to Point Tunneling Protocol	点对点隧道协议, 该协议是在 PPP 协议的基础上开发的一种新的增强型安全协议。
63.	QoS	Quality of Service	服务质量, 是网络的一种安全机制, 是用来解决网络延迟和阻塞等问题的一种技术。
64.	RTS/CTS	Request To Send/Clear To Send	请求发送/清除发送协议, 一种用来减少由隐藏节点问题所造成的冲突的机制, 主要用来解决“隐藏终端”问题。
65.	SMA	Sub-Miniature-A	无线电天线接口, 这种接口的无线设备是最最普及的。
66.	SNAT	Source Network Time Protocol	源地址转换, 将 ip 数据包的源地址转换成另外一个地址。
67.	SNMP	Simple Network Management Protocol	简单网络管理协议, 用以监测连接到网络上的设备是否有任何引起管理上关注的情况。
68.	SRP	Secure Remote Password	安全远程密码, 它是一个开放源代码认证协议。使用 SRP 的客户机/服务器不会在网络上以明文或加密的方式传送密码, 这样可以完全消除密码欺骗行为。
69.	SSH	Secure Shell	安全外壳协议, 目前较可靠, 专为远程登录会话和其他网络服务提供安全性的协议。
70.	SSID	Service Set Identifier	网络服务标识: 由一串字符组成, 为 WLAN 网络提供唯一的名称标识。
71.	TCP	Transmission Control Protocol	传输控制协议, 一种面向连接(连接导向)的、可靠的、基于字节流的传输层(Transport layer)通信协议。

序号	缩写	英文全称	中文解释
72.	TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/因特网互联协议，又名网络通讯协议，定义了电子设备如何连入因特网，以及数据如何在它们之间传输的标准。
73.	telnet	/	Telnet 是位于 OSI 模型的第 7 层---应用层上的一种协议，是一个通过创建虚拟终端提供连接到远程主机终端仿真的 TCP/IP 协议。
74.	TFTP	Trivial File Transfer Protocol	简单文件传输协议，是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。端口号为 69。
75.	TKIP	Temporal Key Integrity Protocol	临时密钥完整性协议
76.	TRAP	/	Trap 是发送给 SNMP 管理者的通知网络状况的警告消息。
77.	TXOP	Transmission Opportunity	传输机会，应用在支持 IEEE 802.11e Qos 标准的无线网络，是一个有界的时间区间，在这个时间段内，支持 Qos 的设备可以传送一连串的帧。一个 TXOP 由起始时间和最长持续时间来确定。
78.	UDP	User Datagram Protocol	用户数据包协议，是 OSI 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。
79.	Upnp	Universal Plug and Play	通用即插即用，UPnP 规范基于 TCP/IP 协议和针对设备彼此间通讯而制订的新的 Internet 协议。
80.	VAP	Virtual Access Point	虚拟访问点，使用多个 BSSIDs 在单个物理无线访问点的一种协议方法。
81.	VLAN	Virtual Local Area Network	虚拟局域网
82.	VoIP	Voice over Internet Protocol	互联网语音传输协议，将模拟声音讯号(Voice)数字化，以数据封包(Data Packet)的形式在 IP 数据网络 (IP Network)上做实时传递。
83.	WAPI	Wireless LAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础结构，是一种安全协议，同时也是中国无线局域网安全强制性标准。
84.	WDS	Wireless Distribution System	无线分布系统
85.	WEP	Wired Equivalent Privacy	有线等效加密，由加密系统创建，保护无线信息安全、防偷听的方法。
86.	WIDS/WIPS	Wireless Intrusion Detection Systems/ Wireless Intrusion Protection System	无线入侵检测系统/无线入侵防护系统
87.	Wi-Fi	Wireless Fidelity	Wi-Fi 是一种可以将个人电脑、手持设备(如 PDA、手机)等终端以无线方式互相连接的技术。
88.	WLAN	Wireless Local Area Networks	无线局域网，基于 IEEE802.11 标准的无线局域网允许在局域网环境中使用可以不必授权的 ISM 频段中的 2.4 或 5.8GHz 射频波段进行无线连接。
89.	WMM	Wi-Fi Multimedia	Wi-Fi 多媒体，是一种无线 QoS 协议，是 802.11e 协议的一个子集。用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。
90.	WPA	Wi-Fi Protected Access	WiFi 保护接入，一种新式的加密系统，创建保护无线信息不被偷听的机制。被认为比 WEP 要更加安全。
91.	WPA_EAP	Wi-Fi Protected Access-Extensible-Authentication-Protocol	WPA 扩展性认证协议
92.	WPA_PSK	Wi-Fi Protected Access-Pre-shared Key	WPA 共享密钥
