

WayOS

AP 使用说明书

尊敬的客户您好！承蒙惠顾 WayOS 产品，谨致谢意！

一、配置

如要配置，使用以太网线将 AP 连接到一台电脑上，配置好电脑的 IP 地址为 192.168.1.100，掩码 255.255.255.0，运行网页浏览器。

在地址栏中输入 AP 的 IP 地址 (http://192.168.1.1)，然后按回车键 (Enter)。请确保 AP 和您的电脑的 IP 地址在同一子网中。

注意：如果您已经更改了 AP 的默认 IP 地址，请确保输入正确的 IP 地址。输入用户名 (root) 和密码 (admin)。然后单击登录。



注意：如果您已经修改了密码，请确保输入了正确的密码。

成功登录后，AP 将出现以下界面（主页）：



二、系统状态

2.1 网络状态

当前位置: 系统状态 > 网络状态 系统时间: 2017-11-23 14:46:50 [返回首页](#)

网络状态

局域网信息

MAC 地址: 64:05:E9:03:D6:B7
IP 地址: 192.168.2.157
子网掩码: 255.255.255.0

广域网信息

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [末页](#) 前往第 页 [刷新](#)

广域网口	MAC地址	连接类型	IP地址	子网掩码	网关	DNS	MTU	连接状态	连接时间	操作

网络状态: 该页面显示当前局域网 IP 地址, MAC 地址、子网掩码等信息, 以及广域网当前连接时间、连接类型、连接状态。

2.2 运行状态

当前位置: 系统状态 > 运行状态 系统时间: 2017-11-23 14:47:48 [返回首页](#)

运行状态

运行信息

运行时间: 4时25分33秒
CPU 使用率: 1.00 %
总内存: 119.11 M
剩余内存: 68.55 M

连接数容量: 100000
当前连接数: 6

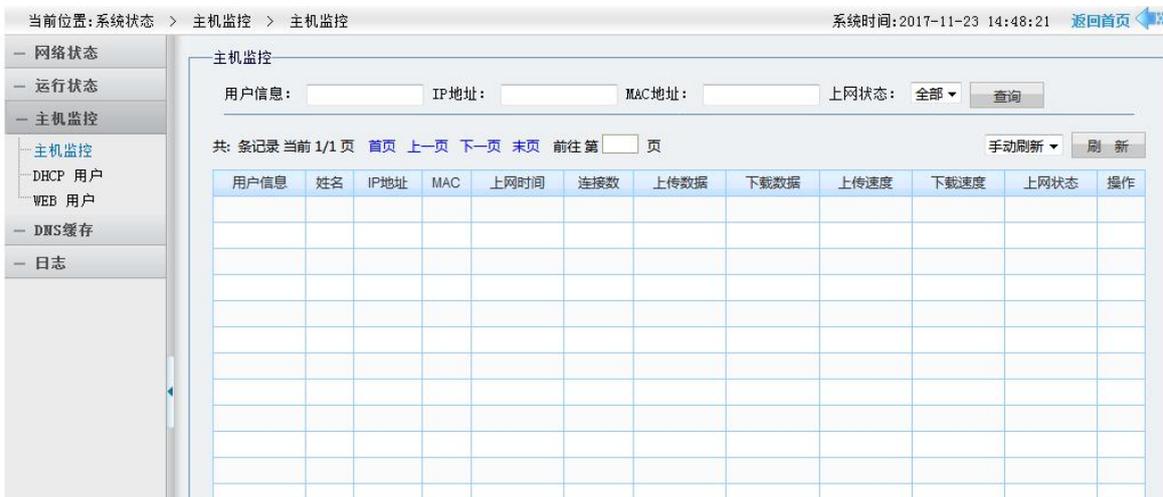
路由缓存容量: 16384
当前路由缓存: 13

skb数目: 2601
skb buf数目: 2601

系统状态: 此窗口为只读, 显示 AP 的运行信息, 包括内存和连接数、缓存等信息。

2.3 主机监控

2.3.1 主机监控

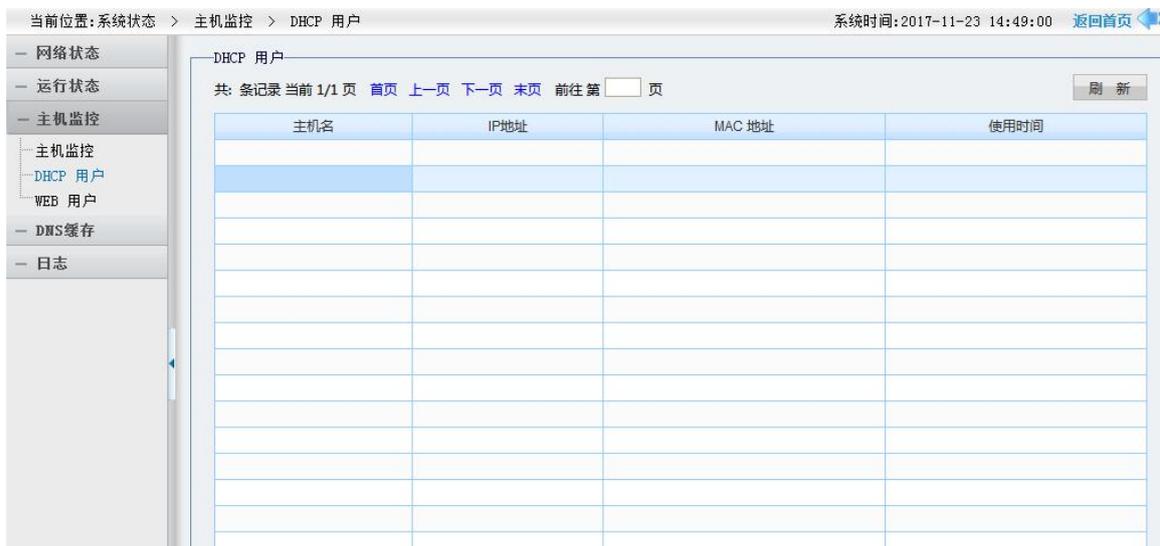


主机监控：该窗口显示用户上网的详细信息，包括上网时间，当前连接数，上传/下载数据总量等信息。

查看连接：显示单个主机的连接信息。信息包括主机每条连接使用的协议，本地端口，远端 IP，远端端口，运行时间等。

详细信息：查看主机的详细信息。可以查看到上网时间，连接数，DDOS 防御，上传/下载数据等详细信息。

2.3.2 DHCP 用户



DHCP 用户：此窗口显示所有 DHCP 自动获取 IP 的用户信息。

2.5 日志

当前位置: 系统状态 > 日志 系统时间: 2017-11-23 14:50:31 返回首页

日志

日志分类: 系统日志

系统日志

共: 686 条记录

刷新日志 删除日志 导出日志

模块	时间	消息
kernel		[19.727000] asf: module license Proprietary taints kernel.
kernel		[19.733000] Disabling lock debugging due to kernel taint
kernel	Nov 23 09:17:28	[19.753000] ****Address of trace_timer :85e32590
kernel	Nov 23 09:17:28	[19.792000] ath_hat: 0.9.17.1 (AR5416, AR9380, REGOPS_FUNC, W RITE_EEPROM, TX_DATA_SWAP, RX_DATA_SWAP, 11D)
kernel	Nov 23 09:17:28	[19.816000] ath_rate_atheros: Copyright (c) 2001-2005 Atheros Communications, Inc, All Rights Reserved
kernel	Nov 23 09:17:28	[19.840000] ath_dfs: Version 2.0.0
kernel	Nov 23 09:17:28	[19.840000] Copyright (c) 2005-2006 Atheros Communications, Inc. All Rights Reserved
kernel	Nov 23 09:17:28	[19.865000] ath_spectral: Version 2.0.0

日志: 该页面可以显示系统日志、ARP 日志、流量攻击日志、WEB 认证日志、访问控制日志，所有的日志都可以在这里查看到。

三、网络配置

3.1 局域网



局域网: 用于设置局域网参数。下面是各配置信息的说明:

自动获取 LAN 口 IP 地址: 该选项允许用户启用或禁用是否自动获取 LAN 口 IP 地址。

路由 IP 地址: 路由器的内网 IP 地址, 如果需要通过路由器来上网, 那么这个地址将是你电脑的默认网关。系统默认值是 192.168.1.1。

子网掩码: 用来确定路由器内网子网范围。系统默认值是 255.255.255.0。

默认网关: 用于 AP 能上网的网关地址。

DNS: 填入网络服务商提供给你的 DNS 服务器 IP 地址, 或者上级设备的网关地址。

MAC 地址: 根据内网的网络情况, 修改 MAC 地址。一般情况下默认的有 MAC 地址, 不需要调整。

酒店模式: 路由模式下生效, 开启酒店模式之后, 设备下面的电脑设置任意 IP 地址都可以上网, 可以设置跟 LAN 口不在同一个网段。(电脑的 IP、掩码、网关、DNS 允许设置任意地址, 但必须都设置) 开启酒店模式之后, 将放弃本地连接的 IP 地址, 而使用虚拟的 IP 地址

3.2 广域网



广域网: 该页面用于设置广域网参数。下面是各配置信息的说明:

连接类型: 您需要确定您的接入类型, 然后进行配置。

MTU 设置: 通常情况下这个参数不用设置, 保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

802.1x: 可以限制未经授权的用户/设备通过接入端口 (access port) 访问 LAN/WLAN。

MAC 地址: 根据内网的网络情况, 随机或克隆 MAC 地址。一般情况下默认的 MAC 地址, 不需要调整。

静态 DNS: 填入网络服务商提供给你的 DNS 服务器 IP 地址, 或者上级设备的网关地址。

工作模式: 通常我们都使用网关模式, 接口做 NAT 地址转换; 有些特殊环境可能会用到路由模式 (如内网机器全部使用公网 IP 的时候)。

DNS 解析优先级: 对于多 WAN 口接入时, 此值的大小决定了 DNS 解析的出口。

防御信息检测: 此功能用于防御运营商对线路的共享限制。

外网带宽: 广域网的上下行带宽值, 若您不清楚带宽值的换算, 可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内, 请手动设置出口带宽值大小。

运营商: 您的广域网线路的运营商, 例如网通或者电信。如果选择“不设置”, 则该线路需与策略路由功能配合使用。单 WAN 口接入环境可以不设置运营商。

基于时间控制: 可以控制在某个时间点断线或者重新拨号上网。

3.3 DHCP 配置



DHCP 配置: 为内网提供动态地址管理, 启用“DHCP 服务器”可以去省去电脑设置网络地址的麻烦。高级设置: 可以自定义许多 DHCP 服务器参数, 如将子网掩码设置 255. 255. 255. 255。

管理方式: 您可以选择普通、高级或者关闭。普通 DHCP 方式只能分配路由器 LAN 口网段的 IP, 高级 DHCP 方式可以任意分配 IP 段、掩码及 DNS 服务器地址。

普通设置:



高级设置



获取 DHCP 成功后自动绑定 IP/MAC: 用于内网设备获取 DHCP 成功后启用或者禁用自动绑定 IP/MAC。

开始地址: DHCP 服务器自动分配的内部 IP 的起始地址。

结束地址: DHCP 服务器自动分配的内部 IP 的结束地址。

释放时间: 设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间, 默认是 3600 秒。您可以自行设置。

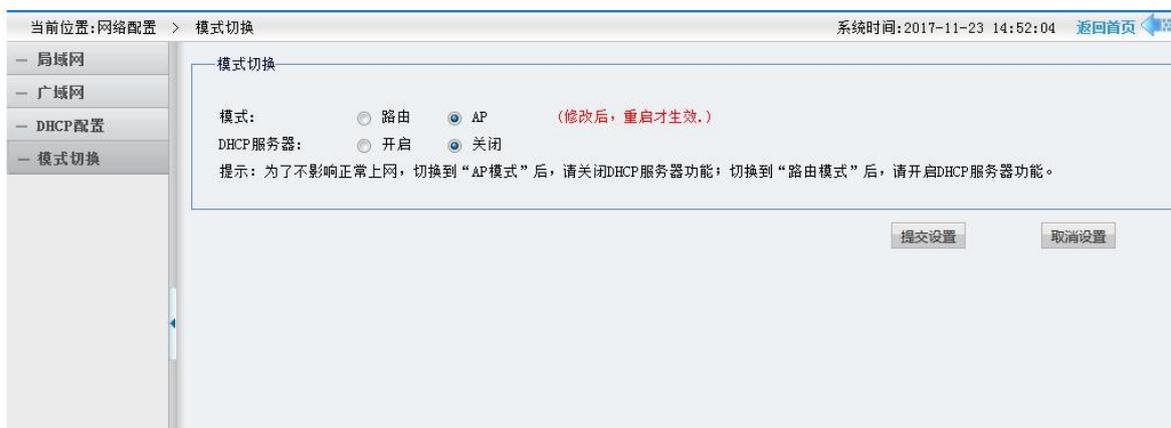
网关地址: DHCP 服务器给客户机分配的默认网关地址。

子网掩码: DHCP 服务器自动分配给客户机的掩码地址。

首选/备用DNS服务器地址: DHCP 服务器自动分配给客户机的 DNS 服务器地址。

Option43:AP 可通过 DHCP 的 Option 43 属性直接获取无线控制器的 IP 地址, 从而完成在 AP 在无线控制器上的注册

3.4 模式切换



模式切换: 该窗口用于 AP 模式和路由模式的切换, 为了不影响正常上网, 切换到“AP 模式”后, 请关闭 DHCP 服务器功能; 切换到“路由模式”后, 请开启 DHCP 服务器功能。

模式: 选择路由或者是 AP 模式, 默认为 AP 模式。

DHCP 服务器: 开启或者关闭 DHCP 服务器

四、无线配置

4.1 基本设置

当前位置: 无线配置 > 基本设置 系统时间: 2017-11-22 16:00:56 [返回首页](#)

- 基本设置
- 无线安全
- WDS 设置
- 用户列表

基本设置

加载无线模块: (启用后, 将加载无线模块, 转发性能会下降)

无线网络:

网络模式: 11b/g/n 混合 (一般保持默认的“11b/g/n 混合”即可)

我要WAYOS-WIFI (必填) 隐藏 隔离 编码: UTF-8

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 1: 我要WAYOS-WIFI (选填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 2: (选填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 3: (选填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 4: (选填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

MAC地址(BSSID): 64:05:E9:0B:99:10

无线频道: 自动选择 自动频道: 1 (扫描附近AP所使用的频道)

运行模式: 普通 增强

带宽: 20/40MHz

无线发射功率: 100 (范围是1-100, 默认是100)

主动断开客户端阈值: 基于信号强度: 0 dBm (为0表示不启用, 范围是0到-127; 当客户端连接信号低于设定阈值时主动断开连接)

基于接收速率: 0 Mbits (为0表示不启用; 当接收速率低于设定阈值时主动断开连接)

组播: 关闭

提示: 如果SSID中包含有中文字符, 手机和平板用户请选择UTF-8编码, PC用户请选择GB2312编码。
修改VLAN ID设置后, 重启生效。

基本设置: 用于无线基本参数的配置。

加载无线模块: 对无线功能的开启与关闭, 以及设置一些基本参数。开启或者关闭无线功能模块时路由都是需要重启的。无线模块的功能开关, 勾选表示开启无线功能, 开启之后路由会重启一次。去掉勾选表示关闭无线功能, 关闭时也会自动重启一次路由器。

无线网络: 打开/关闭无线网络。

网络模式: 可以选用 11ac/a/n, 11a/n 混合模式, 11a 单独模式

网络名称 (SSID): 服务集标识符 (SSID) 是一个为特定的无线局域网 (WLAN) 指定的名称。简单更改 SSID, 以连接到现有无线网络, 或建立新的无线网络。

SSID 最多可达 32 个字符并区分大小写。

隐藏: 隐藏此 SSID 名称, 不广播。其他无线设备将不能直接搜索到此 SSID

隔离: 相当于给此 SSID 下的用户划分了 VLAN, 使用户之间不能互相访问。

编码: GB-2312 和 UTF-8, 选用不同的编码方式在使用中文 SSID 时, 不同的设备可以正常显示。

限速模式: 对 SSID 单独限速, 不同的 SSID 设置不同网络环境, 分独立和共享模式。**网络名称 1/2/3/4:** 您可以给一个无线设备设置多个网络名称 (SSID), 再通过 AP 外隔离, 实现不同的 SSID 内的无线用户无法互相访问, 实现无线虚拟局域网。

MAC 地址 (BSSID): 无线接入点的 MAC 地址。

无线频道: 以无线信号作为传输媒体的数据信号传送通道, 您可以选择其中的任意一个频道来进行连接。

运行模式: 根据需求选择普通或是增强模式。

带宽: 允许您选择您想要运行的信道宽度。如果您没有使用任何 802.11n 无线设备则选择 20MHz。自动 20/40 MHz 允许您在网络上连接 802.11n 和 802.11b/g 无线设备。

无线发射功率: 设置无线发射功率大小。

主动断开客户端阈值: 为 0 表示不启用, 范围是 0 到 127; 当客户端连接信号低于设定阈值时主动断开连接。

组播: 分为组播转组播, 组播转单播

4.2 无线安全



无线安全: 该页面用于设置无线的各种加密模式, 以及对 MAC 地址的过滤。

选择网络名称 (SSID): 选择您要设置 SSID: 首先选择一个需要设置的 SSID 名称 (如果有多个 SSID 的话)。

安全设置: 分为开放式、共享式、WEPAUTO、WPA 个人、WPA2 个人、WPAP/WPA2 个人这 6 类。选择关闭则不采取任何加密方式。

开放式: WEP 加密的一种握手方式, 是通过 WEP 密钥来进行加密。

共享式: WEP 加密的另外一种握手方式, 也是通过 WEP 密钥进行加密, 加密类型与开放式加密情况一样。

WEPAUTO: 能够自动选择为开放式或者共享式, 加密类型方式和前两者

WPA 个人: 路由器将采用基于共享密钥的 WPA 模式。

WPA2 个人: 路由器将采用基于共享密钥的 WPA2 模式。

WPA/WPA2 个人: 与 WPA 个人和 WPA2 个人的设置方式一致。

无线 MAC 地址过滤: 提供了对无线访问策略的设置, 可以设置允许和拒绝所填入的 MAC 地址的接入。

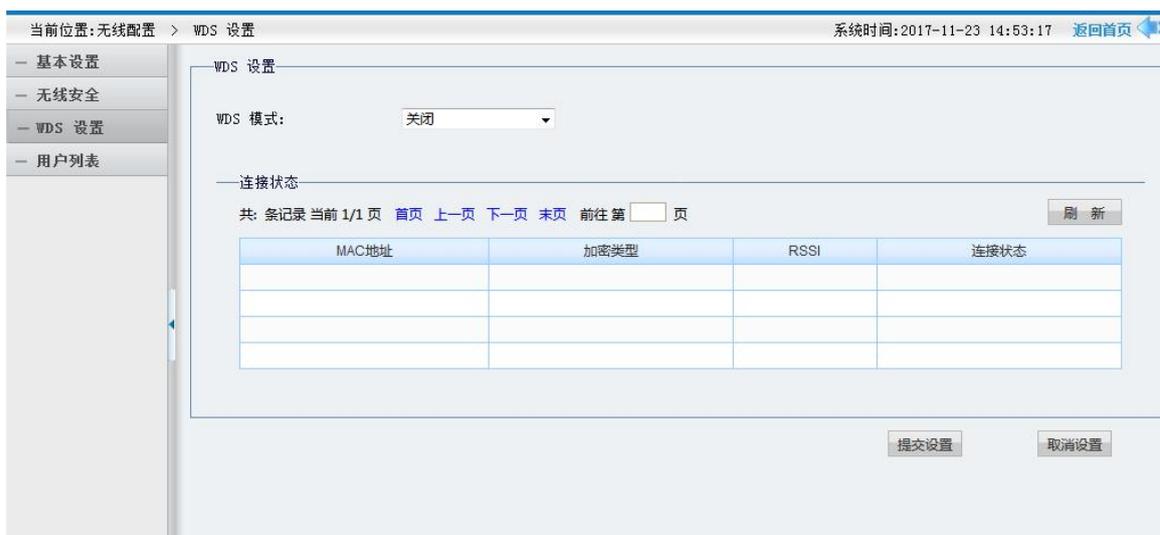
禁止使用过滤器: 使用 MAC 地址过滤功能。

允许如下客户端: 只允许列表中添加的 MAC 地址的设备连接无线。

阻止如下客户端: 禁止列表中添加的 MAC 地址的设备连接到无线网络。描述: 对添加的 MAC 地址的简单描述, 便于管理员识别不同的 MAC 地址。

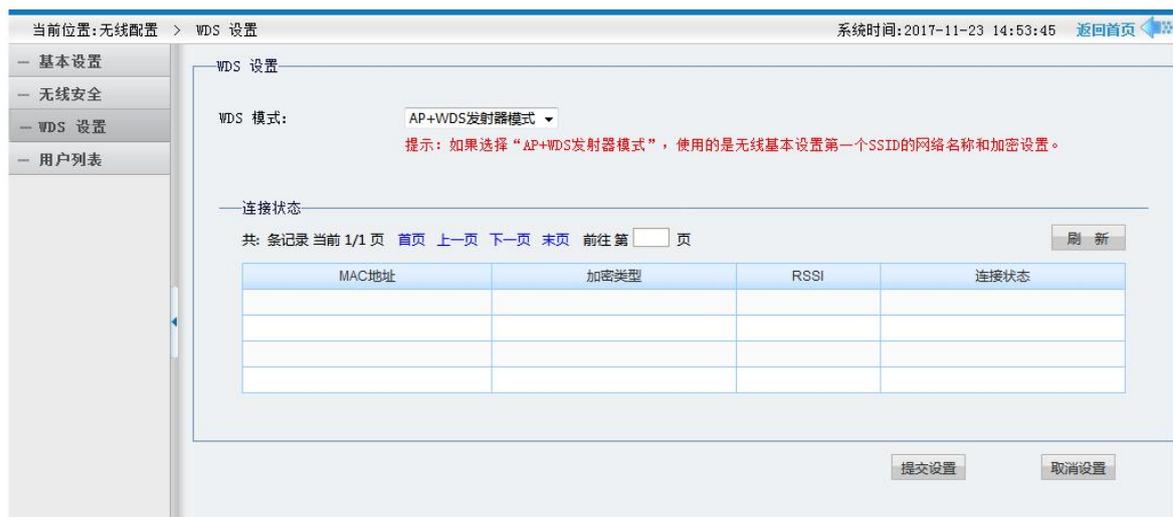
MAC 地址: 客户端设备的 MAC 地址。列表: 显示当前存在的用户情况。

4.3 WDS 设置

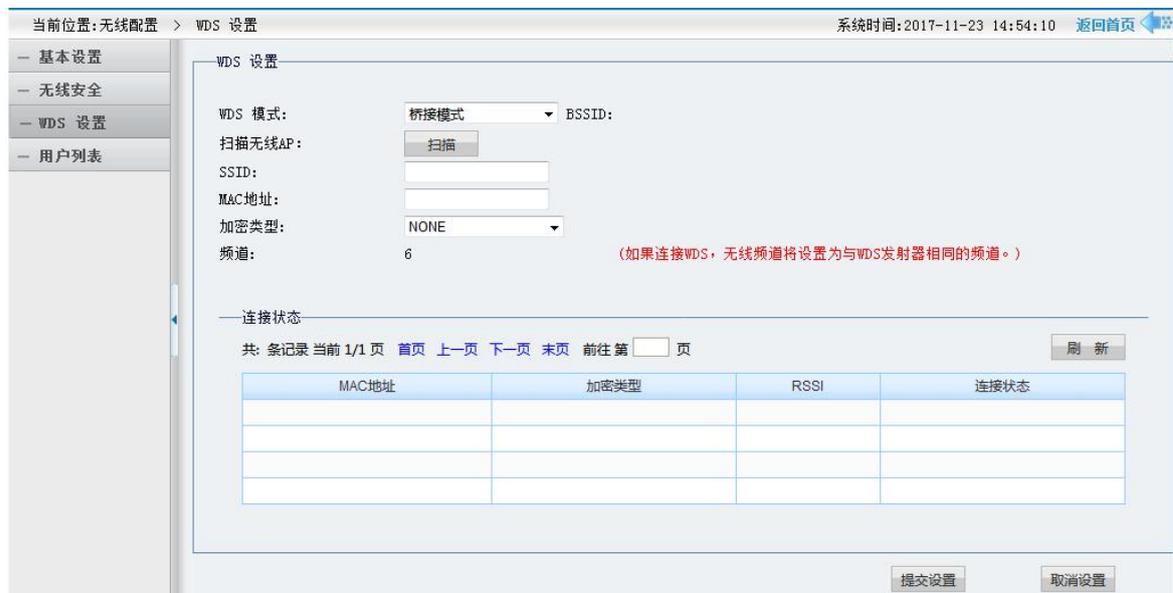


WDS 设置: WDS (无线分布式系统), 是一个在 IEEE 802.11 网络中多个无线访问点通过无线互连的系统。它允许将无线网络通过多个访问点进行扩展。这种可扩展性能, 使无线网络具有更大的传输距离和覆盖范围。共分为三种连接方式: AP+WDS 发射器模式, 桥接模式和中继模式。若选择关闭则不启用 WDS 功能。

AP+WDS 发射器模式: AP+WDS 发射器模式不需要填写任何信息, 使用的是无线基本设置第一个 SSID 的网络名称和加密设置。



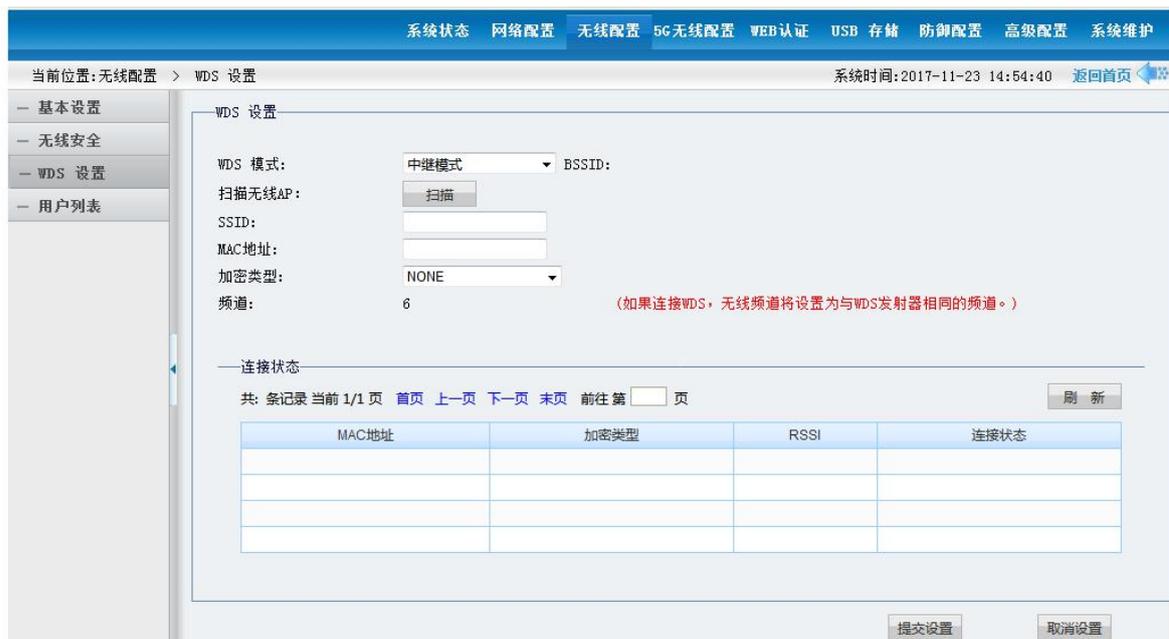
桥接模式：桥接模式需要填写对方设备的 BSSID, 本机的 SSID 则被屏蔽，只是作为中继模式的 SSID 的扩展形式。



MAC 地址：需要连接到的设备的 BSSID 地址。

加密典型：保证这个桥接的安全性设定的加密类型，一般为 NONE。

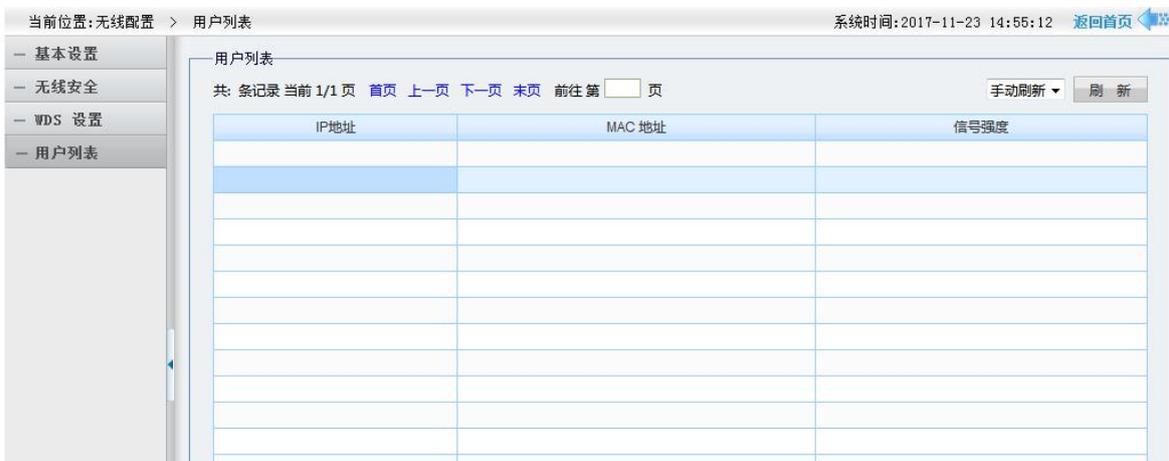
中继模式：中继模式也要填写所需要连接 AP 的 BSSID, 本机 AP 作为核心，其他的 AP 只是作为中继的一个扩展形式。



MAC 地址: 需要连接到的设备的 BSSID 地址。

加密典型: 保证这个桥接的安全性设定的加密类型, 一般为 NONE。

4.4 用户列表



用户列表: 该页面显示当前连接到路由的无线设备信息。

五、5G 无线配置

5.1 基本设置

当前位置:5G无线配置 > 基本设置 系统时间:2017-11-22 16:57:21 [返回首页](#)

- 基本设置
- 无线安全
- WDS 设置
- 用户列表

基本设置

加载无线模块: (启用后, 将加载无线模块, 转发性能会下降)

无线网络:

网络模式: 11AC/AN/A (一般保持默认的“11AC/AN/A”即可)

WAYOS-5G (必填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 1: (必填) 隐藏 隔离 编码: UTF-8

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 2: (必填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 3: (必填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

网络名称 4: (必填) 隐藏 隔离 编码: GB2312

限速模式: 关闭 上行: 0 下行: 0 KByte(千字节)

VLAN ID: 0 (0-4080)

最大用户数: 0 (0表示不限制)

MAC地址(BSSID): 64:05:E9:0B:99:18

无线频道: 频道 149 (扫描附近AP所使用的频道)

运行模式: 普通 增强

带宽: 20/40MHz

VHT BandWidth: 80MHz

无线发射功率: 100 (范围是1-100, 默认是100)

主动断开客户端阈值: 基于信号强度: 0 dBm (为0表示不启用, 范围是0到-127; 当客户端连接信号低于设定阈值时主动断开连接)

基于接收速率: 0 Mbits (为0表示不启用; 当接收速率低于设定阈值时主动断开连接)

组播: 关闭

提示: 如果SSID中包含有中文字符, 手机和平板用户请选择UTF-8编码, PC用户请选择GB2312编码。
修改VLAN ID设置后, 重启生效。

基本设置: 用于无线基本参数的配置。

加载无线模块: 对无线功能的开启与关闭, 以及设置一些基本参数。开启或者关闭无线功能模块时路由都是需要重启的。无线模块的功能开关, 勾选表示开启无线功能, 开启之后路由会重启一次。去掉勾选表示关闭无线功能, 关闭时也会自动重启一次路由器。

无线网络: 打开/关闭无线网络。

网络模式: 可以选用 11ac/a/n, 11a/n 混合模式, 11a 单独模式

网络名称 (SSID): 服务集标识符 (SSID) 是一个为特定的无线局域网 (WLAN) 指定的名称。简单更改 SSID, 以连接到现有无线网络, 或建立新的无线网络。

SSID 最多可达 32 个字符并区分大小写。

隐藏: 隐藏此 SSID 名称, 不广播。其他无线设备将不能直接搜索到此 SSID

隔离: 相当于给此 SSID 下的用户划分了 VLAN, 使用户之间不能互相访问。

编码: GB-2312 和 UTF-8, 选用不同的编码方式在使用中文 SSID 时, 不同的设备可以正常显示。

限速模式: 对 SSID 单独限速, 不同的 SSID 设置不同网络环境, 分独立和共享模式。**网络名称 1/2/3/4:** 您可以给一个无线设备设置多个网络名称 (SSID), 再通过 AP 外隔离, 实现不同的 SSID 内的无线用户无法互相访问, 实现无线虚拟局域网。

MAC 地址 (BSSID): 无线接入点的 MAC 地址。

无线频道: 以无线信号作为传输媒体的数据信号传送通道, 您可以选择其中的任意一个频道来进行连接。

运行模式: 根据需求选择普通或是增强模式。

带宽: 允许您选择您想要运行的信道宽度。如果您没有使用任何 802.11n 无线设备则选择 20MHz。自动 20/40 MHz 允许您在网络上连接 802.11n 和 802.11b/g 无线设备。

VHT bandwidth: 可以选择 20/40MHz, 或者 80MHz, 根据不同的距离选择不同的频率。

无线发射功率: 设置无线发射功率大小。

主动断开客户端阈值: 为 0 表示不启用, 范围是 0 到 127; 当客户端连接信号低于设定阈值时主动断开连接。

组播: 分为组播转组播, 组播转单播

5.2 无线安全

当前位置: 5G无线配置 > 无线安全 系统时间: 2017-11-23 14:55:51 返回首页

— 基本设置

— 无线安全

— WDS 设置

— 用户列表

无线安全

选择网络名称 (SSID): WAYOS-5G

— 加密设置

安全设置: 关闭 注意: 如需加密请选择WPA2个人/AES方式

— 无线MAC地址过滤

过滤方式: 禁止使用过滤器 允许如下客户端 阻止如下客户端

描述:

MAC地址:

— 列表

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [末页](#) 前往第 页

描述	MAC地址	操作

无线安全: 该页面用于设置无线的各种加密模式, 以及对 MAC 地址的过滤。

选择网络名称 (SSID): 选择您要设置 SSID: 首先选择一个需要设置的 SSID 名称 (如果有多个 SSID 的话)。

安全设置：分为开放式、共享式、WEPAUTO、WPA 个人、WPA2 个人、WPAP/WPA2 个人这 6 类。选择关闭则不采取任何加密方式。

开放式：WEP 加密的一种握手方式，是通过 WEP 密钥来进行加密。

共享式：WEP 加密的另外一种握手方式，也是通过 WEP 密钥进行加密，加密类型与开放式加密情况一样。

WEPAUTO：能够自动选择为开放式或者共享式，加密类型方式和前两者

WPA 个人：路由器将采用基于共享密钥的 WPA 模式。

WPA2 个人：路由器将采用基于共享密钥的 WPA2 模式。

WPA/WPA2 个人：与 WPA 个人和 WPA2 个人的设置方式一致。

无线 MAC 地址过滤：提供了对无线访问策略的设置,可以设置允许和拒绝所填入的 MAC 地址的接入。

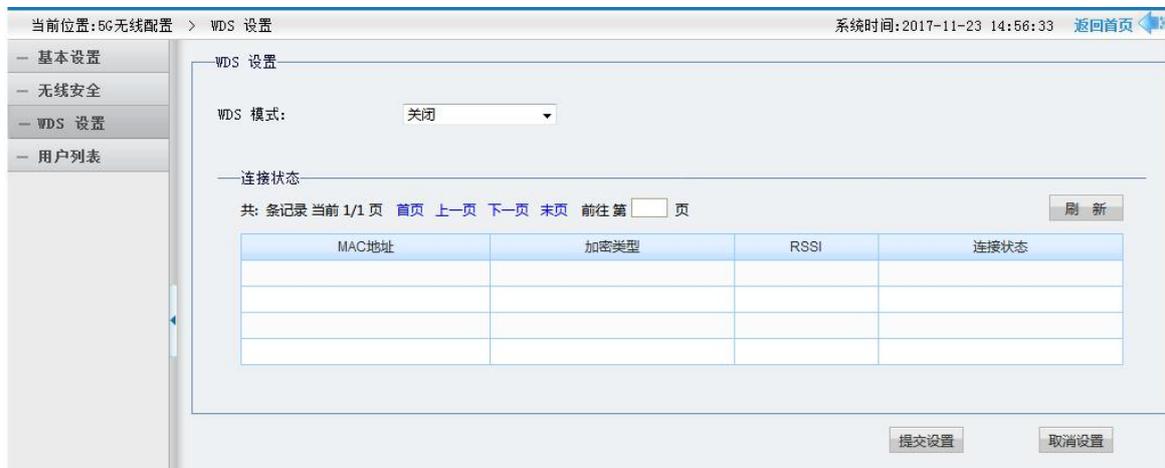
禁止使用过滤器：使用 MAC 地址过滤功能。

允许如下客户端：只允许列表中添加的 MAC 地址的设备连接无线。

阻止如下客户端：禁止列表中添加的 MAC 地址的设备连接到无线网络。描述：对添加的 MAC 地址的简单描述，便于管理员识别不同的 MAC 地址。

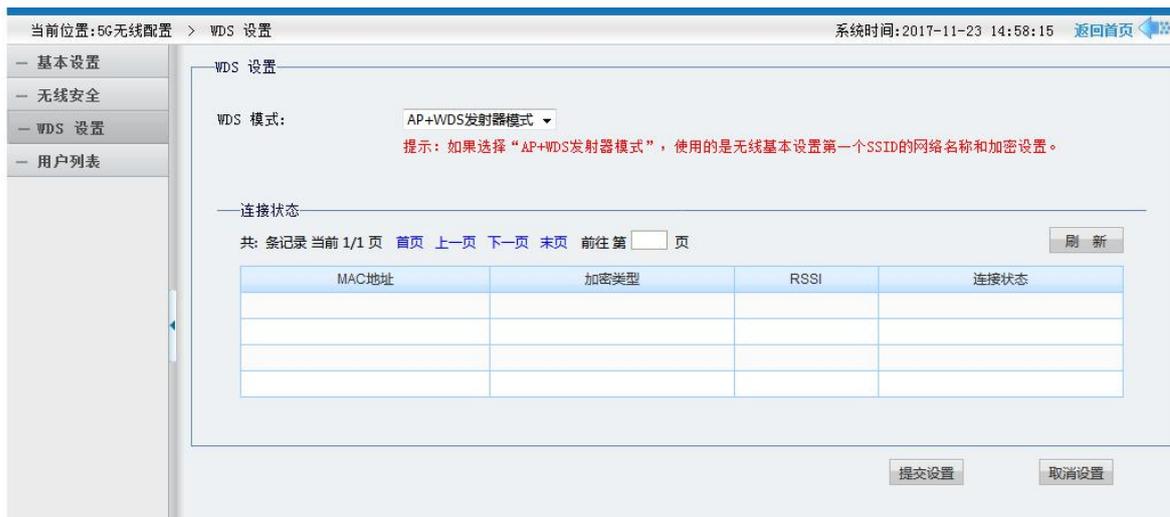
MAC 地址：客户端设备的 MAC 地址。列表：显示当前存在的用户情况。

5.3 WDS 设置

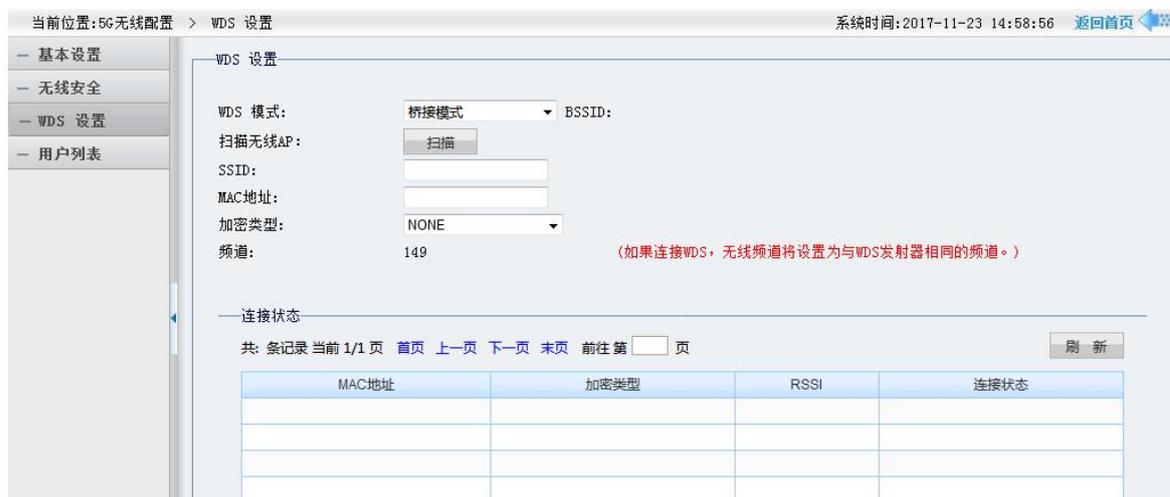


WDS 设置：WDS（无线分布式系统），是一个在 IEEE 802.11 网络中多个无线访问点通过无线互连的系统。它允许将无线网络通过多个访问点进行扩展。这种可扩展性能，使无线网络具有更大的传输距离和覆盖范围。共分为三种连接方式：AP+WDS 发射器模式，桥接模式和中继模式。若选择关闭则不启用 WDS 功能。

AP+WDS 发射器模式：AP+WDS 发射器模式不需要填写任何信息，使用的是无线基本设置第一个 SSID 的网络名称和加密设置。



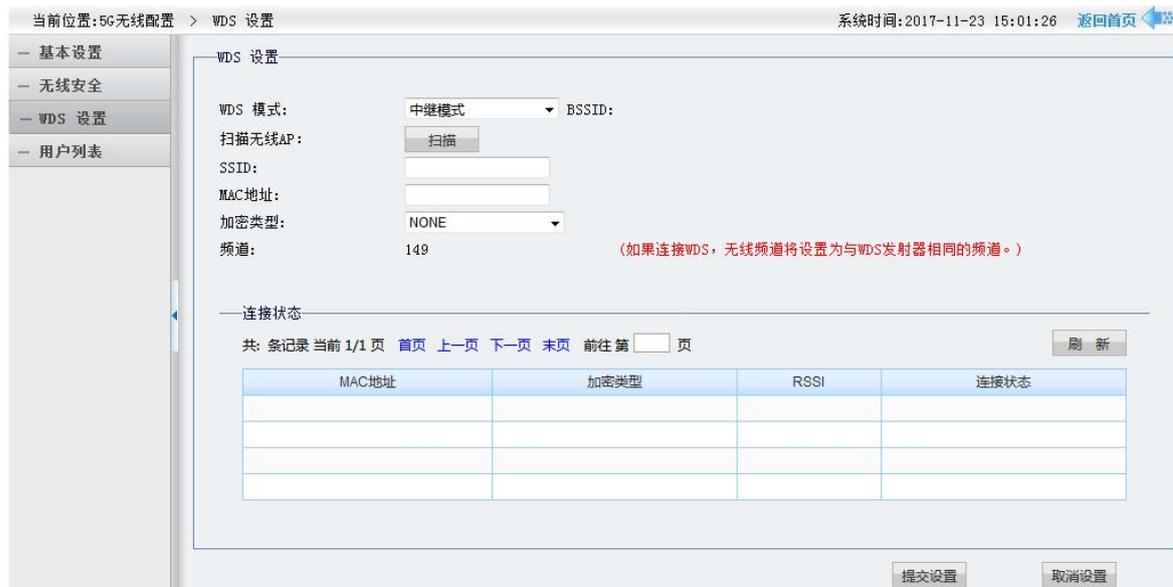
桥接模式: 桥接模式需要填写对方设备的 BSSID, 本机的 SSID 则被屏蔽, 只是作为中继模式的 SSID 的扩展形式。



MAC 地址: 需要连接到的设备的 BSSID 地址。

加密典型: 保证这个桥接的安全性设定的加密类型, 一般为 NONE。

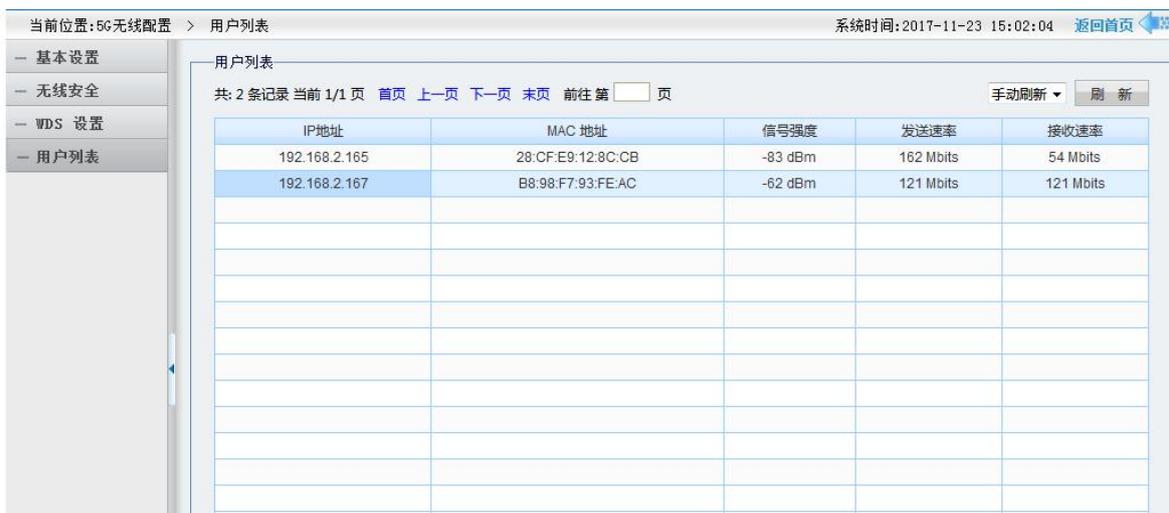
中继模式: 中继模式也要填写所需要连接 AP 的BSSID, 本机 AP 作为核心, 其他的 AP 只是作为中继的一个扩展形式。



MAC 地址: 需要连接到的设备的 BSSID 地址。

加密典型: 保证这个桥接的安全性设定的加密类型, 一般为 NONE。

5.4 用户列表



用户列表: 该页面显示当前连接到路由的无线设备信息。

六、WEB 认证

6.1 智慧WIFI



状态: 选择是否启用功能

二维码服务器: 可以与网吧二维码服务器对接使用
服务器:

系统自带: 默认与路由系统自带的服务器地址进行连接

自定义地址: 手动输入认证服务器、集中管理服务器地址进行连接

无线联盟: 与无线联盟服务器进行连接

设备安装位置: 填写设备安装所在的地区位置。

当前状态信息: 设备与服务器连接的状态。分为连接集中管理状态和连接认证管理状态。

6.2 基本设置



基本设置：该页面用于 web 认证的基本参数设置。

WEB 认证上网状态：开启或者关闭 WEB 认证上网功能。

允许上网的方式：选择允许用户上网的认证方式。ARP 绑定用户直接上网：IP 与 MAC 地址进行绑定过的用户可以直接上网。

WEB 认证类型：第三方 WEB 认证。

用户账号到期提前通知：账号到期之前提醒用户的通知时间。默认为提醒时间内每天第一次开启网页时出现，直到账号到期（或者延长期限）为止。

不需要认证的内部主机(基于 IP)：所添加的 IP 用户将不受任何一种认证方式的管制，可以直接上网，即认证排除的内网 IP，可以为空。

不需要认证的内部主机(基于 MAC)：所添加的 MAC 将不受任何一种认证方式的管制,可以为空。

允许访问的外网范围(基于 IP)：没有进行认证的用户也能访问的外网 IP 地址范围,可以为空。

允许访问的外网范围(基于域名)：没有进行认证的用户也能访问的外网域名，可以为空。

会话存活超时时间：设定用户多少时间没登录认证，则强制重新登录认证。

接口免认证：对有线和无线接口设置免认证，则接口不需要认证

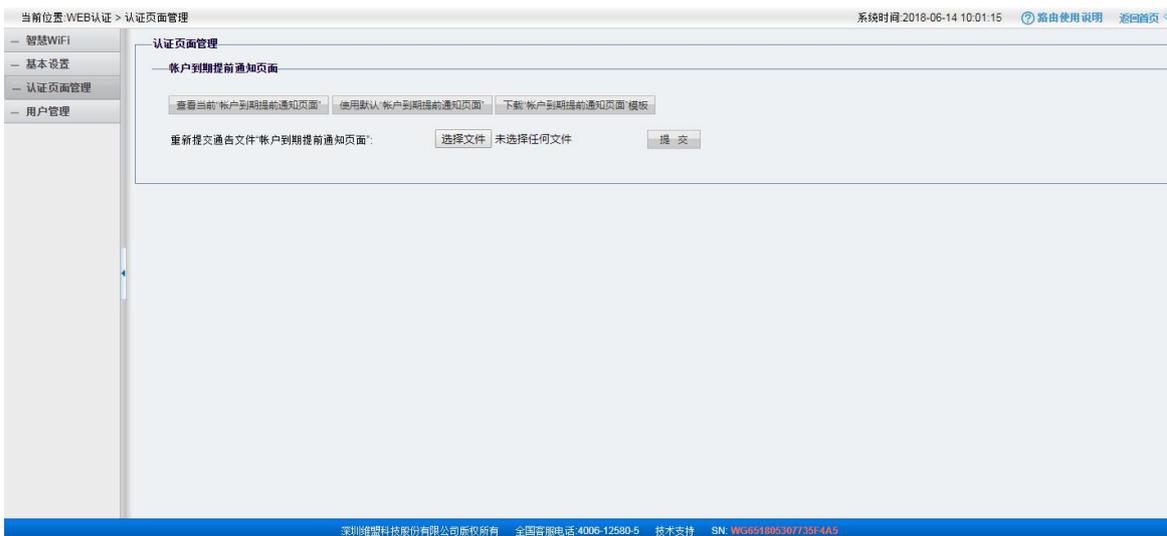
包时用户定时重设时长：对包时的用户设置定时重设时长。

状态：启用和禁用 WEB 简易认证

模式：有极速达，短信验证码，一键上网，口令卡的认证方式，可以根据自己的需求选择不同的认证模式。

账户在线时长：设置用户可以使用的时长

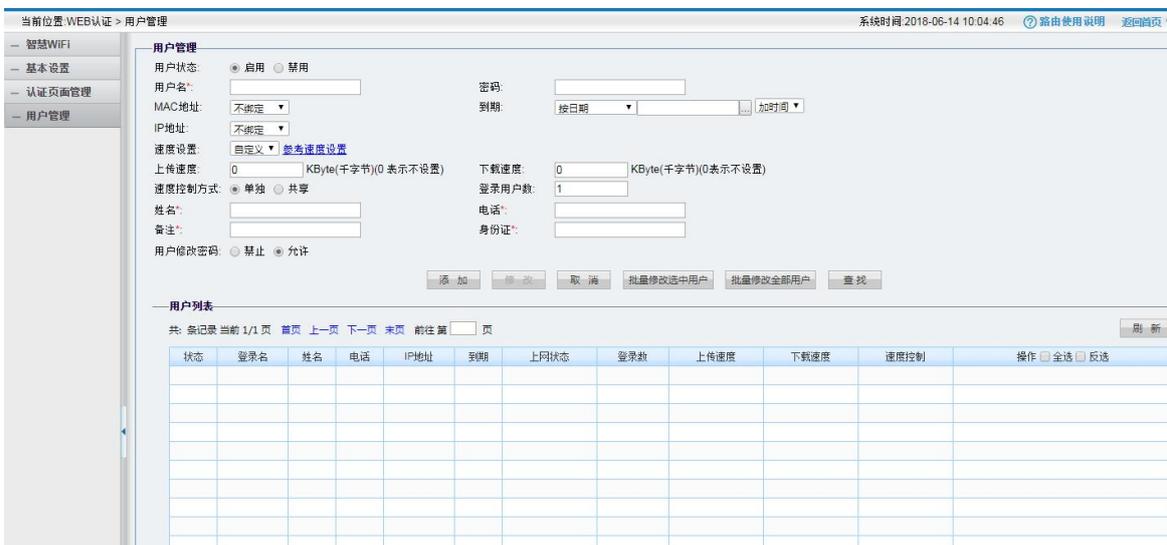
6.3 认证页面管理



认证页面管理：该页面用于对认证用户或者未经认证的用户所弹出的提示页面进行管理，该通告内容允许用户自定义其中的内容或者替换新的通告文件。

帐户到期提前通知页面：认证用户帐号到期之前的通知提醒页面，用户帐号快到期时，打网页的时候会自动弹出此通告内容。

6.4 用户管理



用户管理：该页面针对 Web 认证上网的用户进行添加、修改或删除的操作，如用户账号的建立、认证方式、到期时间、MAC 地址的绑定、备注信息等设置。

用户状态：选择禁用即表示禁用此用户，禁用后此用户将不能进行拨号上网（用户当前连接断开以后才生效）。

用户名：为用户创建一个登录的登陆用户名。

密码：用户创建一个登录的登陆密码。

MAC 地址：有不绑定、自动绑定、手动绑定 3 种形式可供选择。

到期时间：以对用户的上网期限进行限定。点击右边的“...”进行添加。

IP 地址：用于手动给用户指定 IP 地址。默认情况下系统会依照 IP 地址池自动为用户分配一个 IP。

速度设置：对用户的速度进行设置操作。

上传/下载速度：对该帐号的带宽使用做以限制，只允许使用指定的带宽速度值。默认为 0，表示不做限制。

速度控制方式：可以选择单独限制或者共享限制。单独限制：对帐号做单独限制，用户使用的最大速度不超多限制的速度值。共享限制：对一号多拨的用户有效，可以限制一个帐号在多人共享使用时，多人共享限制的速度值。

登陆用户数：设定该账号可以允许被多少个用户同时登陆使用，即一号多拨功能。（当允许登陆的用户数设置大于 1 时，绑定的MAC 地址将只会对第一个拨号的用户有效）

备注：对此用户的简单描述，方便管理员进行查看管理。点击用户列表中的操作栏，可以对账户进行修改、删除及断开等操作。

用户修改密码：禁止或允许用户操作修改密码。

七、防御配置

7.1 ARP 管理

7.1.1 ARP 列表

当前位置: 防御配置 > ARP 管理 > ARP 列表 系统时间: 2017-11-22 17:44:02 [返回首页](#)

ARP 列表

IP地址: MAC地址: 接口: 类型: 全部 状态: 全部

共: 2 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [末页](#) 前往第 页 [手动刷新](#)

描述	IP地址	MAC地址	接口	类型	状态	提示	操作
	192.168.2.110	00:E0:70:65:C9:FA	局域网	动态	正常		<input type="button" value="取消"/> <input type="button" value="静态"/> <input type="button" value="唯一"/> <input type="button" value="免认证"/>
	192.168.2.1	58:69:6C:39:B5:04	局域网	动态	正常		<input type="button" value="取消"/> <input type="button" value="静态"/> <input type="button" value="唯一"/> <input type="button" value="免认证"/>

ARP 列表: 显示当前局域网连接用户的 IP 及MAC 信息。可以查询 IP 地址, MAC 地址, 接口, 类型, 状态的主机信息。

唯一: 指只有 IP 和MAC 地址对应才能连接网络。

静态: IP 与MAC 地址绑定为静态以后, 用户手动更改 IP 或者MAC 地址不会影响网络使用, 但其他用户不能占用此 IP 跟MAC 地址。

取消: 取消已绑定静态或唯一类型, 变为动态。

免认证: 主机不需要通过路由器的认证设置

7.1.2 ARP 绑定

当前位置: 防御配置 > ARP 管理 > ARP 绑定 系统时间: 2017-11-23 15:04:21 返回首页

— ARP 管理

- ARP 列表
- ARP 绑定
- ARP 防御
- 日志
- + 访问控制
- MAC地址过滤
- 连接限制
- DDOS防御
- Ping WAN口
- 连接数设置

ARP 绑定

描述:

IP地址:

MAC地址:

类型: 静态 唯一

接口:

— 列表

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [末页](#) 前往第 页

描述	IP地址	MAC地址	类型	接口	操作

描述: ARP 绑定的描述。

IP 地址: 输入您要进行 ARP 绑定的 IP 地址。

MAC 地址: 输入您要进行 ARP 绑定的 MAC 地址, 可以通过“查询 MAC”来设置 MAC 地址。

类型: 分为两类:“静态”和“唯一”。“静态”:IP 与 MAC 地址绑定为静态以后, 用户手动更改 IP 或者 MAC 地址不会影响网络使用, 但其他用户不能占用此 IP 跟 MAC 地址。“唯一”:不但限制这个 IP 地址只能在这个 MAC 上使用, 同时也限制了在这个 MAC 地址只能使用指定的 IP 地址, (等同于, 这个 IP 地址只能指定网卡上使用, 同时, 这个网卡, 也只能使用指定的 IP 地址)。

接口: 指定那个接口上进行 ARP 绑定, 路由器的接口分为 LAN(内网)、WAN(外网)。

添加: 对绑定的 IP 添加到下面列表。

修改: 对绑定的用户进行修改。

取消: 取消对该用户的操作。

7.2 访问控制

7.2.1 访问控制

当前位置: 防御配置 > 访问控制 > 访问控制 系统时间: 2017-11-23 15:07:14 返回首页

+ ARP 管理
- 访问控制
 访问控制
 日志
- MAC地址过滤
- 连接限制
- DDOS防御
- Ping WAN口
- 连接数设置

访问控制

访问控制的方式: 关闭 允许规则之外的通过 禁止规则之外的通过 提交

规则编辑

状态: 启用 禁用

描述:

控制方式: 允许 阻止

执行顺序: (1-65535) 值越大越先被执行。

主机IP地址范围: (为空: 表示对该规定所有内部IP有效)

自定义IP协议: 取消选择

日志: 开启 关闭

基于时间控制: 启用

添加 修改 取消

列表

共: 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	描述信息	控制方式	执行顺序	日志	内部主机范围	自定义IP协议	基于时间控制	操作

访问控制的方式: 关闭: 访问控制规则不生效, 所有的数据都是允许通过的;

允许规则之外的通过: 对访问控制规则的中没有匹配上的数据包, 允许通过;

禁止规则之外的通过: 对访问控制规则的中没有匹配上的数据包, 禁止通过

状态: 对规则的控制开关, 选择启用表示激活该条规则。

描述: 对该条规则的简单文字描述, 该描述必须是唯一的。

控制方式: 对此规则通过或阻止进行控制。

执行顺序: 在进行访问规则匹配的时候, 该值决定了, 该规则的匹配顺序。数据从第一条规则开始匹配, 如果匹配, 则直接进行该规则处理, 如果不匹配, 则进行下一条规则匹配。

主机 IP 地址范围: 设置您要控制的主机范围。就是“内网地址”。

自定义 IP 协议: 您可以自行定义远端 IP、域名及端口协议, 并以此作为管控对象。

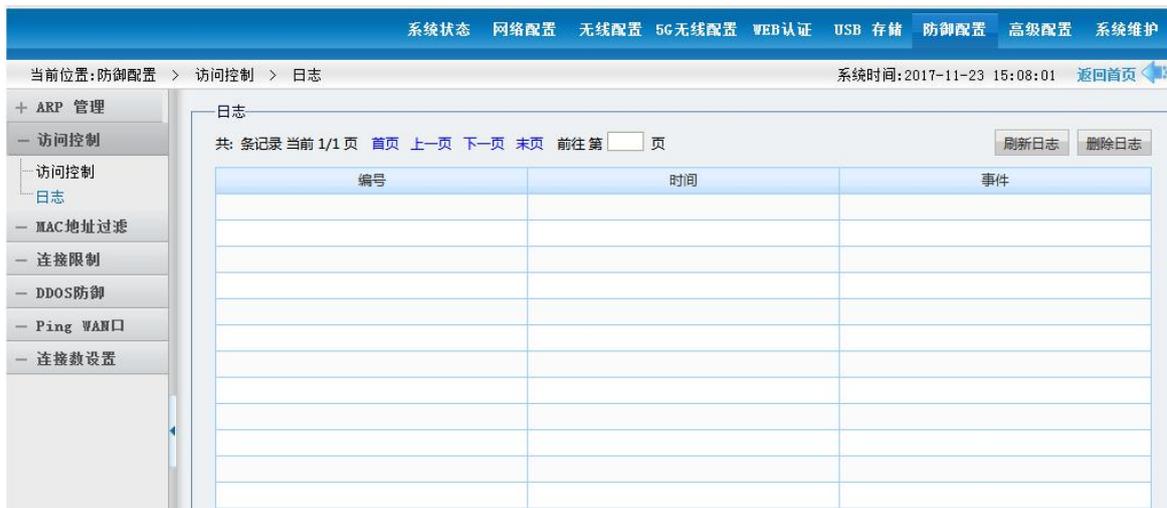
日志: 对于匹配上的数据包, 进行日志记录。

基于时间控制: 如果启用了“基于时间控制”, 那么该访问控制规则, 将在指定的时间段内生效。如下图所示:

每周: 您可以设置一周的哪几天生效。

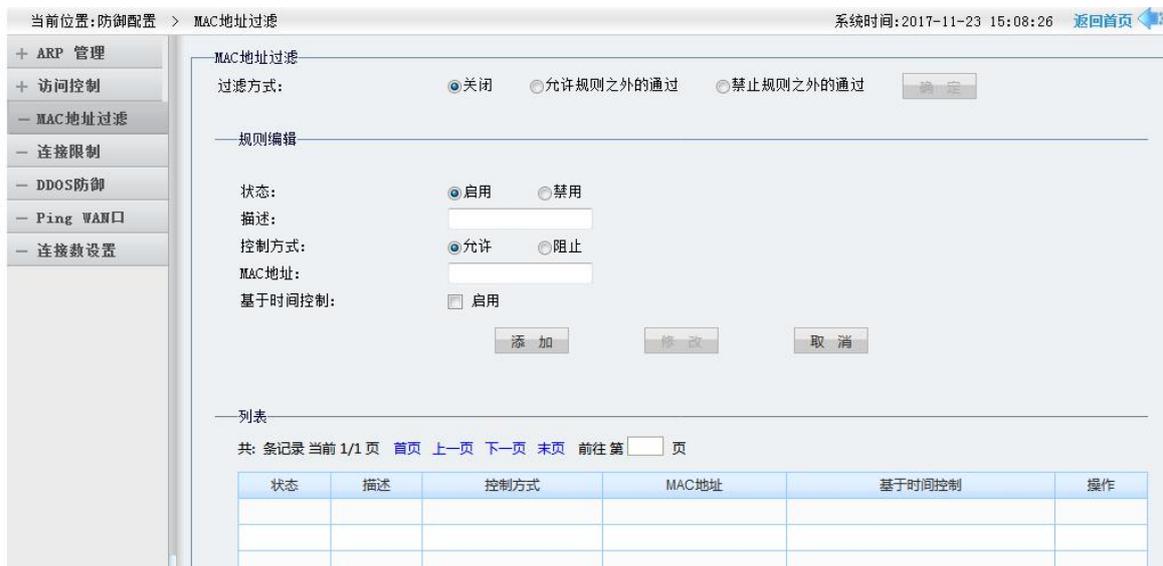
每天: 您可以设置一天的哪些时段生效。

7.2.2 日志



日志：记录访问控制规则产生的日志记录，需要在添加规则的时候先启用日志功能才会记录。

7.2.3 MAC 地址过滤



MAC 地址过滤：对 MAC 地址进行管理，允许或者禁止该 MAC 地址的用户通过。

MAC 地址过滤的方式：有‘关闭’、‘允许规则之外的通过’和‘禁止规则之外的通过’3 种选择，请根据需要来进行选择。

关闭：对列表中添加的所有规则将不做任何控制；

允许规则之外的通过：列表中添加的规则按照控制方式来执行，列表之外的不受限制，直接通过；

禁止规则之外的通过：列表之中的规则按照控制方式来执行，列表之外的所有地址将都被禁止通过。

状态：对规则的控制开关，选择启用表示激活该条规则。

描述： 对此规则的简单描述。

控制方式： 分为‘允许通过’和‘禁止通过’两类。用户可以选择此规则是否允许通过。

MAC 地址： 填入您要管控的 MAC 地址。格式为:00:0A:0B:0C:0D:0E 。

基于时间控制： 是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。启用后，如下图所示：

每周： 您可以设置一周的哪几天生效。

每天： 您可以设置一天的哪些时段生效。

7.3 连接限制

当前位置: 防御配置 > 连接限制 系统时间: 2017-11-23 15:09:17 [返回首页](#)

连接限制

默认主机连接数限制: ALL: 3000 TCP: 0 UDP: 0 ICMP: 0 OTHER: 0 (0 表示不限制)

规则编辑

状态: 启用 禁用

描述:

主机IP地址范围: (为空: 表示对该规定所有内部IP有效)

连接数限制: ALL TCP UDP (范围: 0-9999, 0表示不限制)

基于时间控制: 启用

列表

共: 条记录 当前 1/1 页 [首页](#) [上一页](#) [下一页](#) [末页](#) 前往第 页

状态	描述	主机IP地址范围	限制类型	限制数	基于时间控制	操作

默认主机连接数限制： 所有用户默认主机的连接数限制。当客户机连接数满了之后，由于新的连接出不去，就形同断网，所以请谨慎设置。

状态： 对规则的控制开关，选择启用表示激活该条规则。

描述： 对此规则的简单描述。

主机 IP 地址范围： 对指定的 IP 地址范围单独设置连接数规则，那么这些 IP 地址将只受规则限制，不受默认主机连接限制。

连接数限制： 可以单独对 TCP/UDP 连接限制或者做全部的限制。

基于时间控制： 如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

每周： 您可以设置一周的哪几天生效。

每天： 您可以设置一天的哪些时段生效

7.4 Ping WAN 口



Ping WAN 口: 路由器默认在外网是不可以 Ping 通WAN 口的，如果需要在外网能够 Ping 通WAN 口，请先开启该功能并提交设置。

7.5 连接数设置



路由器连接数容量: 主要用于设置路由器最大对外联机数目，默认连接数是根据机器内存自动获取的，默认情况下不需要做修改。点击高级设置，会出现以下界面：



该页面主要是对 TCP/UDP 超时进行设置，默认情况下不需要做修改。

八、高级配置

8.1 AC 平台客户端

当前位置:高级配置 > AC平台客户端 系统时间:2017-11-22 17:53:52 [返回首页](#)

AC平台客户端

状态: 启用

服务器地址:

设备名称:

最大用户数:

5G最大用户数:

发送功率: (1-100)

AP隔离: 否

旁路认证上网: 启用

备注:

DHCP服务器防御: 启用

DHCP服务器白名单: (MAC格式: 11:22:33:44:55:66 多个MAC之间用','分隔)

—当前状态信息—

已成功连接, 服务器地址'192.168.2.1', 设备名称''

AC 平台客户端: 用于连接 AC 平台服务端, 以便集中管理。

状态: 是否启用 AC 平台客户端。

服务器地址: AC 平台服务器的地址, 不填写表示客户端在内网自动寻找服务器。

设备名称: 设备标识, 默认为空。

最大用户数: 该设备所带的最大用户数。

5G 最大用户数: 该设备 5G 所带的最大用户数。

发送功率: 无线的发送功率。

AP 隔离: AP 隔离是否隔离。

旁路认证上网: 勾选启用其它用户可以通过认证上网。

备注: 简单的标识。

DHCP 服务器防御: 勾选启用 DHCP 服务器防御。

DHCP 服务器白名单: 添加确定的 DHCP 服务器。

8.2 端口映射

8.2.1 端口映射

当前位置: 高级配置 > 端口映射 > 端口映射 系统时间: 2017-11-23 15:13:03 返回首页

— AC平台客户端

— 端口映射

— 端口映射

— DMZ设置

+ 路由表

+ DNS代理

— WEB访问设置

端口映射

映射模式: 模式1 模式2 (模式1是修改源IP为路由器LAN口的IP, 可以做端口回流; 模式2是不修改源IP)

北京电信通: 开启 关闭

提交

规则编辑

状态: 开启 关闭

描述:

协议: TCP UDP TCP和UDP

源地址限制:

外部端口: - (不能为空, 端口范围: 1-65535)

内部端口: - (当外部端口只填一个时, 为空表示, 内部端口与外部端口相同)

内部主机地址:

广域网接口: (为空: 表示全部广域网)

添加 修改 取消

列表

共: 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	描述	协议	源地址限制	外部端口	内部端口	内部主机地址	广域网接口	操作
----	----	----	-------	------	------	--------	-------	----

状态: 对规则的控制开关, 选择启用表示激活该条规则。

描述: 对该条规则的简单文字描述。

协议: 分为 TCP、UDP、TCP 和 UDP。

源地址限制: 是可选项, 如果只想让一部 IP 地址访问您的内网服务时, 就需要配置该选项。允许输入(“1.2.3.4”, “1.2.3.4-2.3.4.5”, “1.2.3.0/24”)这三种格式。(示例中: 若只对总公司开放 1000 端口, 总公司的 IP 地址 (x.x.x.x/24)), 将 “源地址限制” 设置为 x.x.x.x/24, 即可。)

外部端口: 被映射的端口, WAN 中可见。(不能为空, 端口范围:1-65535)

内部端口: 当外部端口只填一个时, 内部端口为空表示, 内部端口与外部端口相同

内部主机 IP 地址: LAN 内部目标地址。

广域网接口: 选择对应的广域网接口, 为空: 表示选择所有的广域网口。

当前路由表：该页面是路由器当前自动生成的静态路由表。此路由表是系统自动生成的，提供给用户查看，不可以修改。

8.2.4 静态路由表

当前位置:高级配置 > 路由表 > 静态路由表 系统时间:2017-11-23 15:14:48 返回首页

AC平台客户端

- 端口映射
- 路由表
 - 当前路由表
 - 静态路由表
- DNS代理
- WEB访问设置

静态路由表

描述:

目的地址:

子网掩码:

网关:

Metric: (默认:0)

网络接口:

列表

共:0条记录 当前1页 首页 上一页 下一页 末页 前往第 页

目的地址	网关	子网掩码	Metric	网络接口	描述	操作

静态路由表：在一些特殊环境中，我们也需要手动去指定静态路由表的走向，此时，我们需要手动去添加静态路由表。

举例：该设备下层挂接有一台三层交换机，交换机的IP为192.168.1.244，该三层交换机下发的有一个172.15.2.1/24的网段，三层交换机下的主机使用172.15.2.X网段的IP上网，并使用172.15.2.1作为网关地址，那么，我们就需要添加如上所述的静态路由，才可以使三层交换机下的主机正常上网。

8.2.5 WEB访问设置

当前位置:高级配置 > WEB访问设置 系统时间:2017-11-23 15:15:22 返回首页

AC平台客户端

- 端口映射
- 路由表
- DNS代理
- WEB访问设置

WEB访问设置

HTTP访问端口:

认证通告端口: (为0表示和管理端口相同)

远程访问: 开启 关闭

远程访问端口:

管理员:

管理员密码:

管理员密码确认:

启用guest用户: 开启 关闭

guest用户:

guest用户密码:

guest用户密码确认:

WEB访问设置：该页面可以设置对路由器WEB界面的访问权限，包括用户名/密码的修改、管理员用户及普通用户的修改及远程访问功能的开启与关闭。管理员用户可以修改路由器任何设置，guest用户只能查看设置，不能修改设置。忘记管理员用户/密码之后只能通过按下reset按钮来恢复到出厂默认值，请牢记您的管

理员用户名及密码。默认管理员用户名是 admin 密码是 admin; guest 用户名与密码都是 guest。

HTTP 访问端口：本地局域网访问路由器时的端口。默认为 80。

认证通告端口：认证页面、通告页面等页面的弹出时使用的端口，如果为 0，表示和管理端口相同。

远程访问：选择开启表示激活远程访问。激活之后，在广域网也能访问到您的路由器 WEB 控制界面，方便管理员进行远程维护。默认为关闭。

远程访问端口：广域网远程访问路由 WEB 控制界面时的端口。默认为 8080。

管理员：自定义您的管理员账户。管理员具有对路由器的最高管理权限。

管理员密码：自定义您的管理员密码。管理员具有对路由器的最高管理权限。

管理员密码确认：重复键入密码，保证一致性和安全性。

启用 guest 用户：是否启用 guest 用户。Guest 用户只能查看路由设置，不能对路由设置做任何更改。默认不启用。

guest 用户：自定义您的 guest 用户名。

Guest 用户密码：自定义您的 guest 用户密码。

Guest 用户密码确认：重复键入密码，保证一致性和安全性。

九、系统维护

9.1 Ping 检测

该页面用于方便管理者了解网络对外联机的实际状况，可以借由此功能判断网络的状况。

当前位置: 系统维护 > Ping检测 系统时间: 2017-11-23 15:15:55 返回首页

Ping检测

输入地址:

网络接口:

(为空表示默认路由出口, LAN (代表局域网), WAN1 (广域网1), WAN2 (广域网2), vpn1 (vpn接口1), vpn2 (vpn接口2)... 或者, 您要设置的接口名称)

Ping包计数: 20 (1 - 1000)

Ping包大小: 1024 (字节)

— 检测信息 —

输入地址: 填写您需要检测的 IP 或者域名。

网络接口: 指定您需要检测的网络接口, 如果留空, 表示从默认的路由出口进行检测。

Ping 包计数: ping 数据包的检测个数。

Ping 包大小: 每个 ping 数据包的大小限制。

9.2 系统控制

用于将 AP 参数导入导出，恢复默认参数以及对 AP 执行重启操作。



保存参数：保存您的 AP 配置参数数据。以备 AP 调试后出现问题能及时恢复到以前的状态。

恢复系统参数：将您预先保存的系统配置文件导入到 AP（配置文件为 .cfg 格式的）。请不要将其他 AP 的配置文件导入到本 AP，否则将导致 AP 不能工作。

恢复默认设置：选择“恢复 AP 默认设置”，并点击确定。恢复之后 AP 会自动重启，重启完之后请使用默认 IP 及用户名/密码登录路由。AP 默认用户名为 admin，密码为 admin。

重启系统：点击“重启系统”按钮，在弹出的对话框中选择“确定”，AP 将会重新启动一次。

定时重启系统：激活之后设定的规则将只会在指定的时间段内生效。

每周：您可以设置一周的哪几天生效。

每天：您可以设置一天的哪些时段生效。

9.3 系统时间设定



系统时间设定：对路由器的时间进行设置。

9.4 固件升级

该界面可以对 AP 进行固件升级操作。升级前请先确认好 AP 的当前版本，看是否需要升级操作。点击‘浏览’按钮，选择新版本的存放路径之后，按下‘升级’按钮开始升级操作。升级时间一般会在一分钟左右完成。



9.5 申请控制

申请控制是用于外网访问设备的功能配置。点击申请控制，刷新状态，当前信息显示连接成功后，外网用户使用固定的智慧 WiFi 服务器地址加上这里提供的代理端口号，即可实现对设备的控制。

