

# 在CBW网络中使用RLAN进行端口配置

## 目标

本文的目标是创建远程局域网(RLAN)网络，并在思科业务无线(CBW)主接入点(AP)上分配端口和接入点组。

## 适用设备 | 软件版本

- 145AC([产品手册](#)) | 10.4.1.0 ([下载最新](#))
- 240AC([产品手册](#)) | 10.4.1.0 ([下载最新](#))

## 简介

CBW AP基于802.11 a/b/g/n/ac(Wave 2)，带内置天线。这些AP支持最新的802.11ac Wave 2标准，以实现更高的性能、更高的接入和更高的密度网络。

本文中引用的145AC和240AC AP能够用于传统或网状网络。本文将设备用于传统的无线网络。

如果您想了解网状网络的基本知识，请查看思科[业务：欢迎使用无线网状网络](#)。

如果您希望在网状网络中执行端口配置，请阅读[在网状模式下配置思科企业无线接入点的以太网端口](#)。

在传统无线网络中，RLAN用于使用主AP对有线客户端进行身份验证。有线客户端成功加入主AP后，LAN端口会在中央或本地交换模式之间交换流量。来自有线客户端的流量被视为无线客户端流量。

RLAN发送身份验证请求以对有线客户端进行身份验证。RLAN中有线客户端的身份验证类似于中央身份验证的无线客户端。

如果只需一个虚拟局域网(VLAN)，则无需配置RLAN。默认情况下，AP上有一个RLAN，即本征VLAN 1。它具有开放安全性，并且默认情况下，所有端口都分配给此RLAN。

如果您不熟悉所用术语，请查看思科[业务：新术语表](#)。

RLAN在网状网络中不起作用。网状网默认不启用，因此除非您之前在网状网模式下运行AP，否则您将设置为转到。

## 配置步骤

此切换部分突出显示初学者的提示。

## 登录

登录主AP的Web用户界面(UI)。为此，请打开Web浏览器并输入https://ciscobusiness.cisco。在继续之前，您可能会收到警告。输入您的凭证。您也可以通过在Web浏览器中输入https://[ipaddress] (主AP) 来访问主AP。

## 工具提示

如果您对用户界面中的字段有疑问，请检查以下工具提示：



## 查找“展开主菜单”图标时遇到问题？

导航至屏幕左侧的菜单，如果未看到菜单按钮，请单击此图标打开侧栏菜单。



## 思科业务应用

这些设备具有与Web用户界面共享某些管理功能的配套应用。并非Web用户界面中的所有功能都可在应用中使用。

[下载iOS应用](#) [下载Android应用](#)

## 常见问题

如果您仍有未回答的问题，您可以查看我们的常见问题文档。 [常见问题](#)

## 第 1 步

如果接入点尚未打开，请接通电源。检查指示灯的状态。当LED指示灯呈绿色闪烁时，请继续下一步。

启动接入点大约需要8-10分钟。LED会以多种模式闪烁绿色，快速交替通过绿色、红色和琥珀色，然后再次变为绿色。LED颜色强度和色相的变化可能很小。

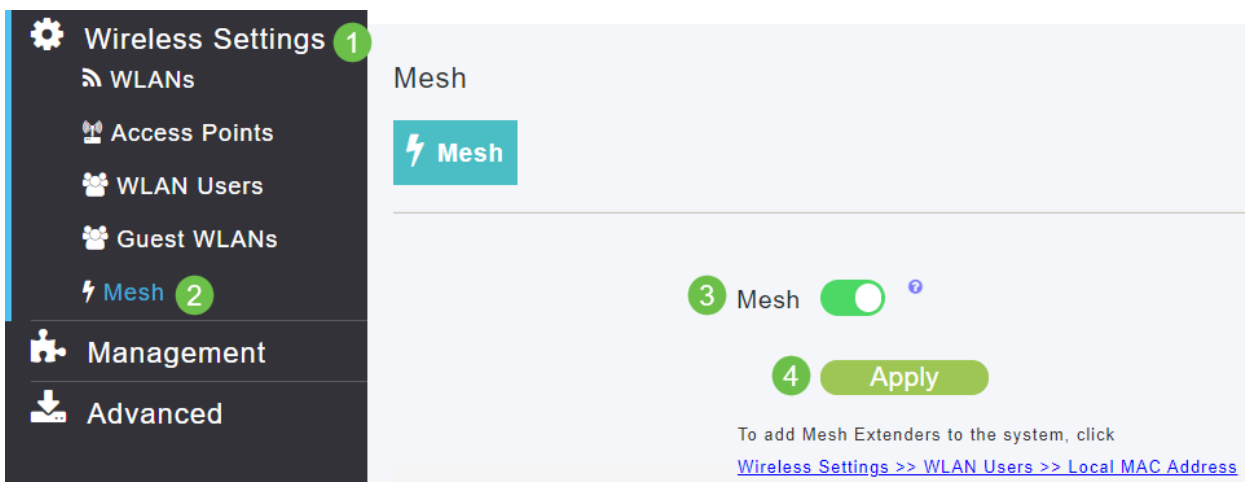
## 步骤 2

登录主AP的Web用户界面(UI)。打开Web浏览器并输入<https://ciscobusiness.cisco>您可能在继续之前收到警告。输入您的凭证。

您还可以通过在Web浏览器中输入主AP的IP地址来访问它。

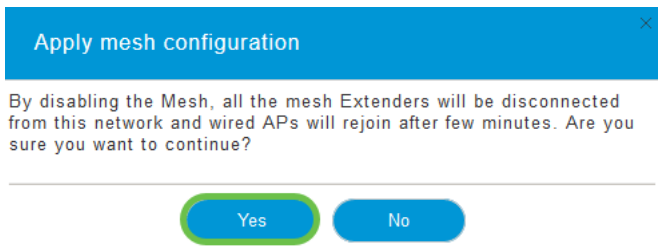
## 步骤 3

AP无法处于网状模式，RLAN无法工作。要关闭网状模式，请导航至“无线设置”>“网状”。选择以关闭网格。如果您的AP是新的，或者您知道网状模式未打开，则可以继续[步骤7](#)。



## 步骤 4

单击“是”(Yes)，确认要关闭网格模式。



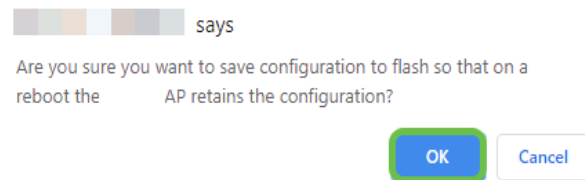
## 步骤 5

请务必单击Web UI屏幕右上角面板上的“保存”图标来保存配置。



## 步骤 6

单击“确定”确认保存。AP将重新启动。完成此操作需要8-10分钟。



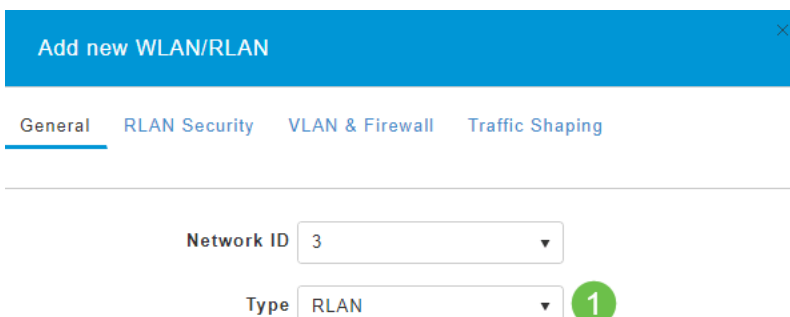
## 步骤 7

可以通过导航到Wireless Settings > WLANs来创建RLAN。然后选择Add new WLAN/RLAN (添加新WLAN/RLAN)。



## 步骤 8

选择RLAN。为配置文件创建名称。



## 第9步 ( 使用开放式安全 )

在“RLAN安全”选项卡下。在“安全类型”下，可以选择“打开”或802.1X。

在本例中，Security Type保留为默认值。

单击 **Apply**。这将自动激活此开放安全RLAN。跳至[步骤11](#)。

Edit RLAN

General **RLAN Security** VLAN & Firewall Traffic Shaping

Guest Network

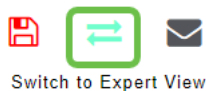
MAC Filtering  ?

Security Type Open 1

2 Apply Cancel

## 第10a步 ( 使用802.1X安全 )

要设置外部RADIUS，必须在Expert View的RADIUS下的Admin Accounts中配置RADIUS服务器。单击Web UI右上角菜单上的箭头图标可切换到“专家视图”。有关设置RADIUS服务器的详细信息，请[检出](#)



Switch to Expert View

## 第10b步 ( 使用802.1X安全 )

如果为安全类型选择802.1X，则必须选择更多选项。您需要选择以下选项：

- 主机模式 — 单主机或多主机
- 身份验证服务器 — 外部Radius或AP
- MAB模式 — 已启用或已禁用。要添加MAC地址，请按照下一步中的说明操作。

Add new WLAN/RLAN

General **RLAN Security** VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering  ?

Security Type 802.1X

Host Mode Single Host 1

Authentication Server External Radius ? 2

No Radius Server is configured for Authentication and Accounting. Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view)

MAB Mode

RADIUS Server

Add RADIUS Authentication Server 3

State	Server IP Address	Port
-------	-------------------	------

## 步骤 11 ( 可选 )

MAC身份验证绕行(MAB)模式意味着，如果您在WLAN用户下列出了MAC地址，则设备无需进行身份验证。列出的MAC地址可以绕过身份验证，以自动访问网络或自动拒绝。当IP电话插入交换机的PoE端口时，这将非常有用。

可以通过以下两种方式之一标记每个MAC地址：

1. 允许列出 — 设备接收自动访问。
2. 阻止列出 — 设备将自动被拒绝访问。

WLAN Users

Users 1

WLAN Users Local MAC Addresses ?

Search ?

+ Add MAC Address Refresh Number of Blocklist:0 Number of Allowlist:3

Action	MAC Address	Type	Profile Name	Description
3	a4: : :20	Allowlist	Any WLAN/RLAN	CBW145AC-0b20
	4c: : :68	Allowlist	Any WLAN/RLAN	CBW141ACM-7468
	4c: : :1	Allowlist	Any WLAN/RLAN	CBW140AC-cba1

## 步骤 12

在VLAN & Firewall(VLAN和防火墙)选项卡下，可以选择Use VLAN Tagging(使用VLAN标记)并选择VLAN ID编号。

General RLAN Security **VLAN & Firewall** Traffic Shaping

Client IP Management External DHCP Server

Use VLAN Tagging Yes 1

VLAN ID \* 5 2

Enable Firewall No

VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN

Apply Cancel

## 步骤 13 ( 可选 )

如果要配置访问控制列表(ACL)，可以选择启用防火墙(Enable Firewall)，允许或拒绝对特定IP地址或VLAN的访问。当有人插入网络端口设备连接到网络时，会使用此命令。

General RLAN Security **VLAN & Firewall** Traffic Shaping

Client IP Management External DHCP Server

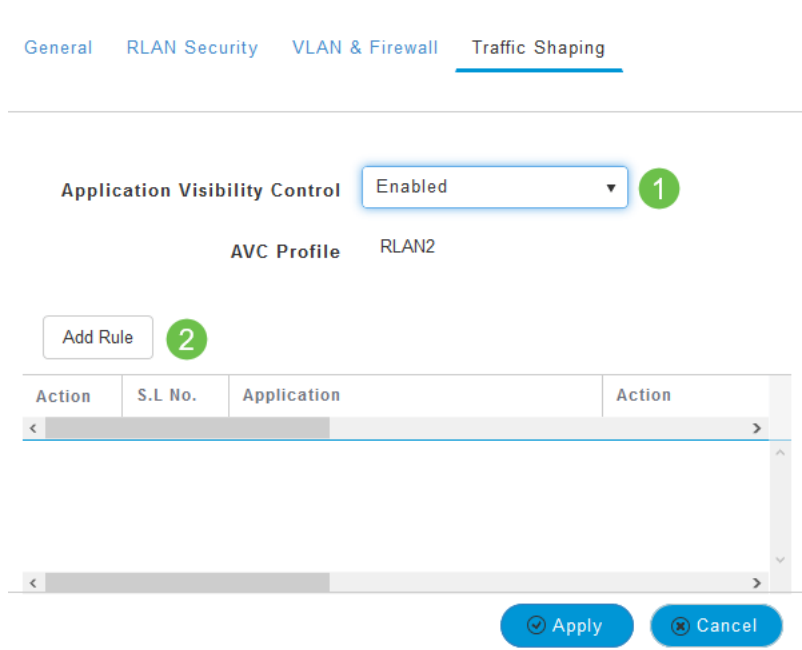
Use VLAN Tagging Yes

VLAN ID \* 5

Apply Cancel

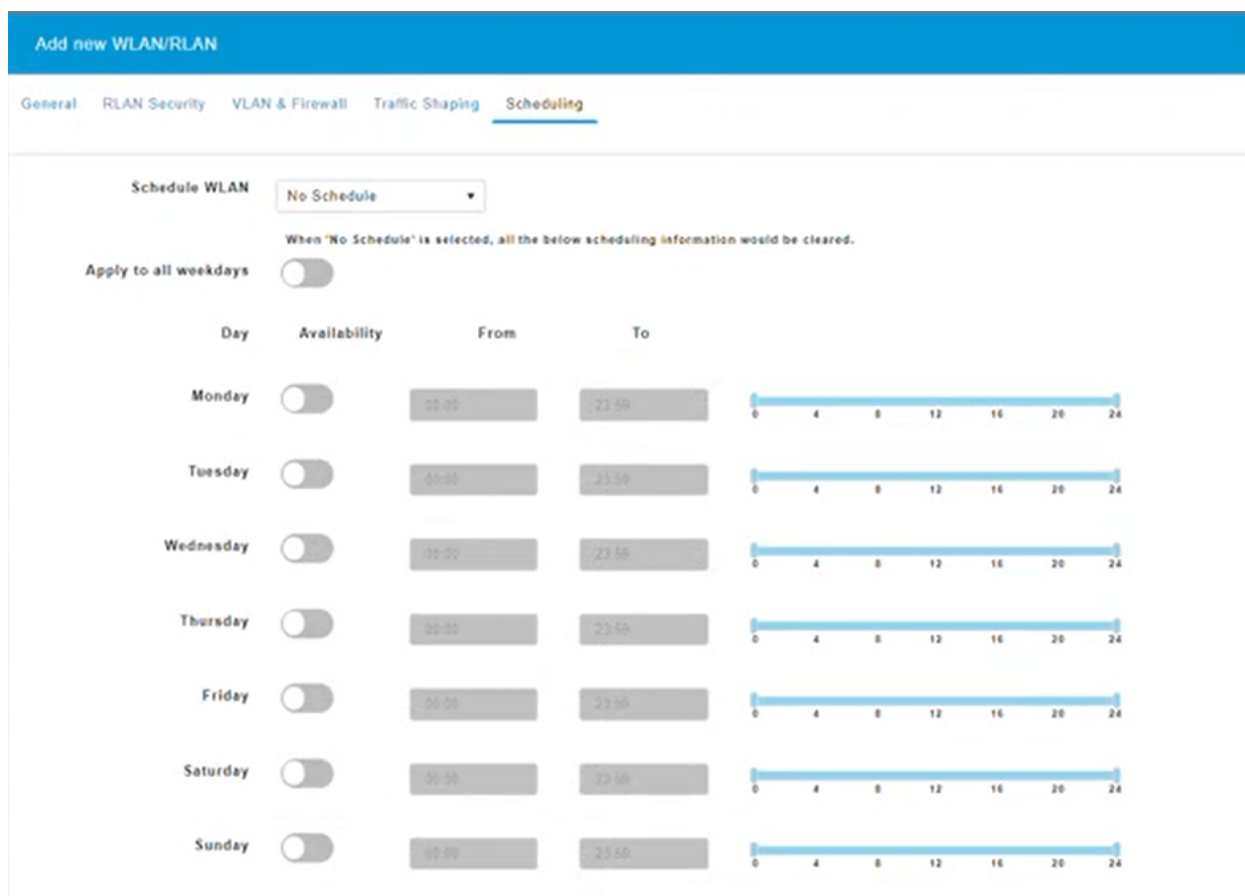
## 步骤 14 ( 可选 )

在“流量整形”选项卡下，可以通过启用应用可视性控制来配置流量整形。这会设置流量优先级。



## 步骤 15 ( 可选 )

在“计划”选项卡下，您可以选择计划。这将设置端口能够连接到网络的时间。



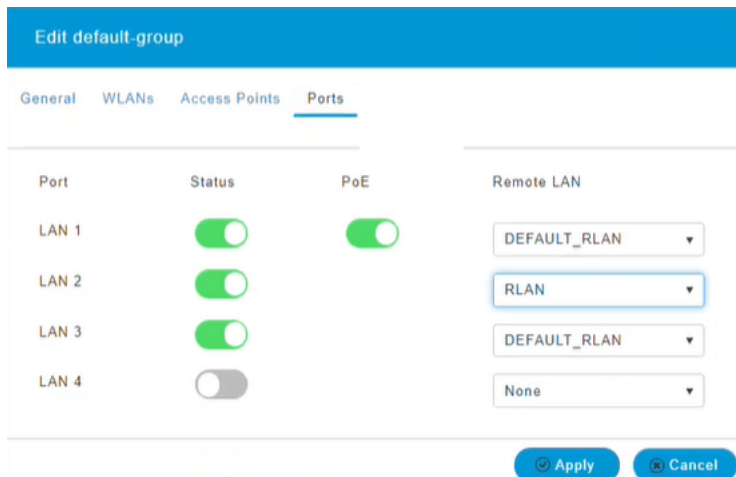
## 步骤 16 ( 可选 )

创建RLAN后，您可以导航到Wireless Settings > Access Point Groups。您可以在这里添加或编辑组。要查看此屏幕，您需要处于您在步骤10a中选择的专家视图中。



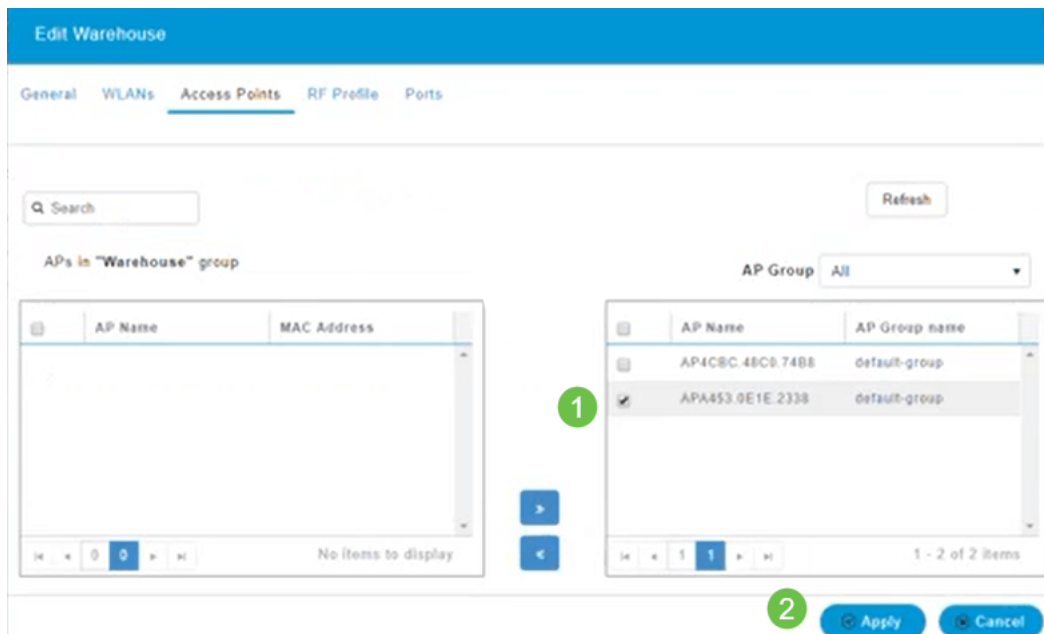
## 步骤 17

在Ports选项卡下，您可以将AP上的端口分配给特定远程LAN。



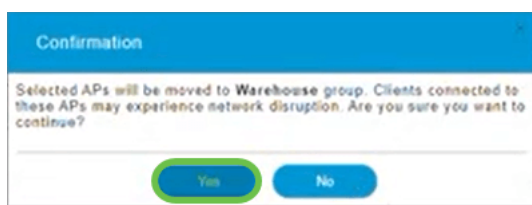
## 步骤 18

在Access Points选项卡下，您需要将特定接入点分配给该接入点组。单击 **Apply**。



## 步骤 19

选择是进行确认。



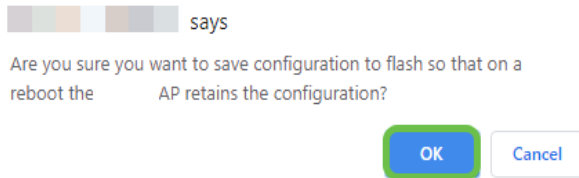
## 步骤 20

请务必单击Web UI屏幕右上角面板上的“保存”图标来保存配置。



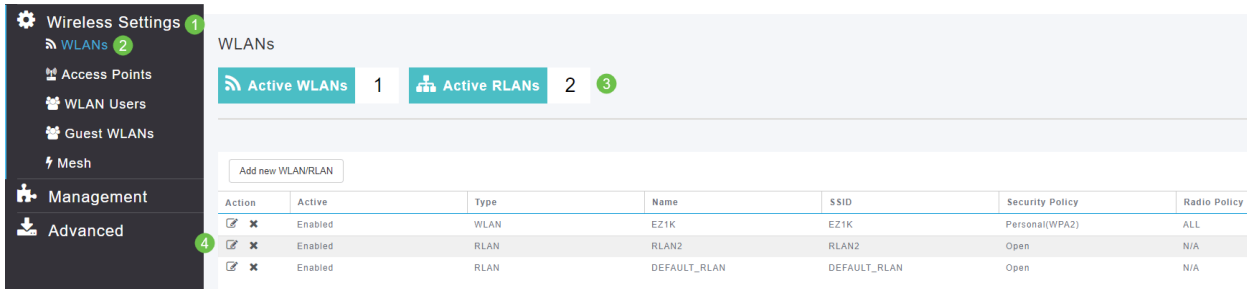
## 步骤 21

单击“确定”确认保存。AP将重新启动。完成此操作需要8-10分钟。



## 查看RLAN

要查看您创建的RLAN，请选择**Wireless Settings > WLANs**。您将看到活动RLAN数量增加到2，并列出新RLAN。

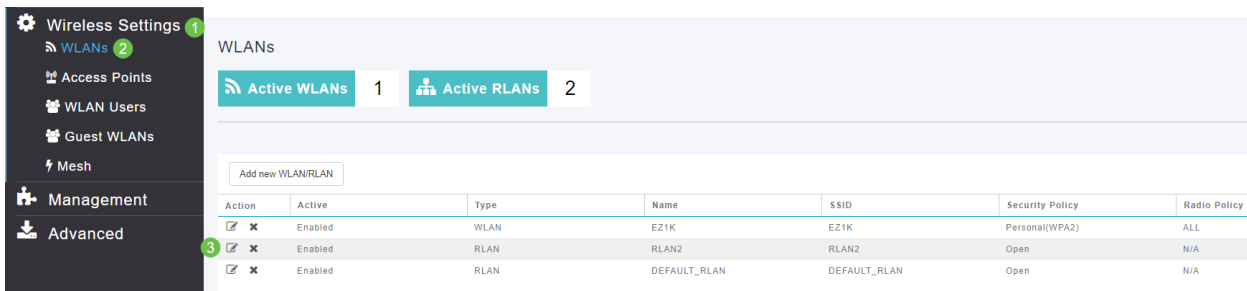


## 编辑RLAN

当您在设置RLAN结束时单击“应用”时，RLAN会自动激活。如果您需要禁用RLAN或进行任何其他更改，请执行以下简单步骤。

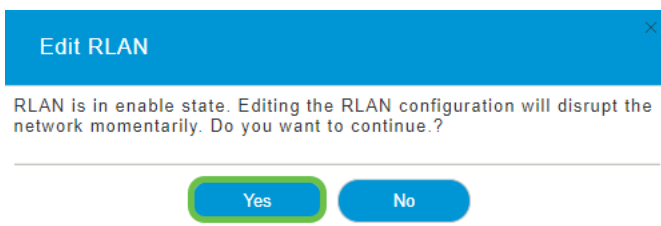
### 第 1 步

选择**Wireless Settings > WLANs**。单击编辑图标。



### 步骤 2

您将收到一个弹出窗口，通知您编辑RLAN会暂时中断网络。单击“是”确认要继续。



### 第3步 ( 启用/禁用 )

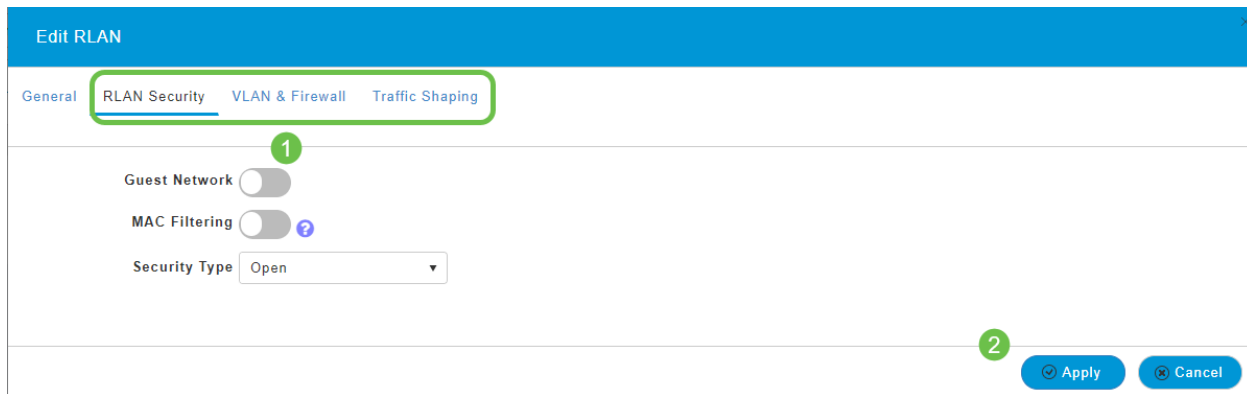
在“编辑WLAN/RLAN”窗口的“常规”下，选择已启用或已禁用以启用/禁用RLAN。单击 **Apply**。





## 第4步 ( 编辑其他设置 )

如果需要更改设置，请导航至RLAN Security、VLAN & Firewall或Traffic Shaping选项卡。进行更改后，单击“应用”。



## 步骤 5

请务必单击Web UI屏幕右上角面板上的“保存”图标来保存配置。



## 结论

您现在已在CBW网络上创建了RLAN。如果满足您的需求，您可以尽情享受并随时添加更多内容。

[常见问题](#) [RADIUS](#) [固件升级](#) [RLAN](#) [应用分析](#) [客户端分析](#) [主要AP工具](#) [Umbrella](#) [WLAN用户](#) [日志记录](#) [流量整形](#) [罗格](#) [干扰源](#) [配置管理](#) [端口配置网状模式](#) [欢迎使用CBW网状网络](#) [使用邮件身份验证和RADIUS记帐的访客网络](#) [故障排除](#) [将Draytek路由器与CBW配合使用](#)