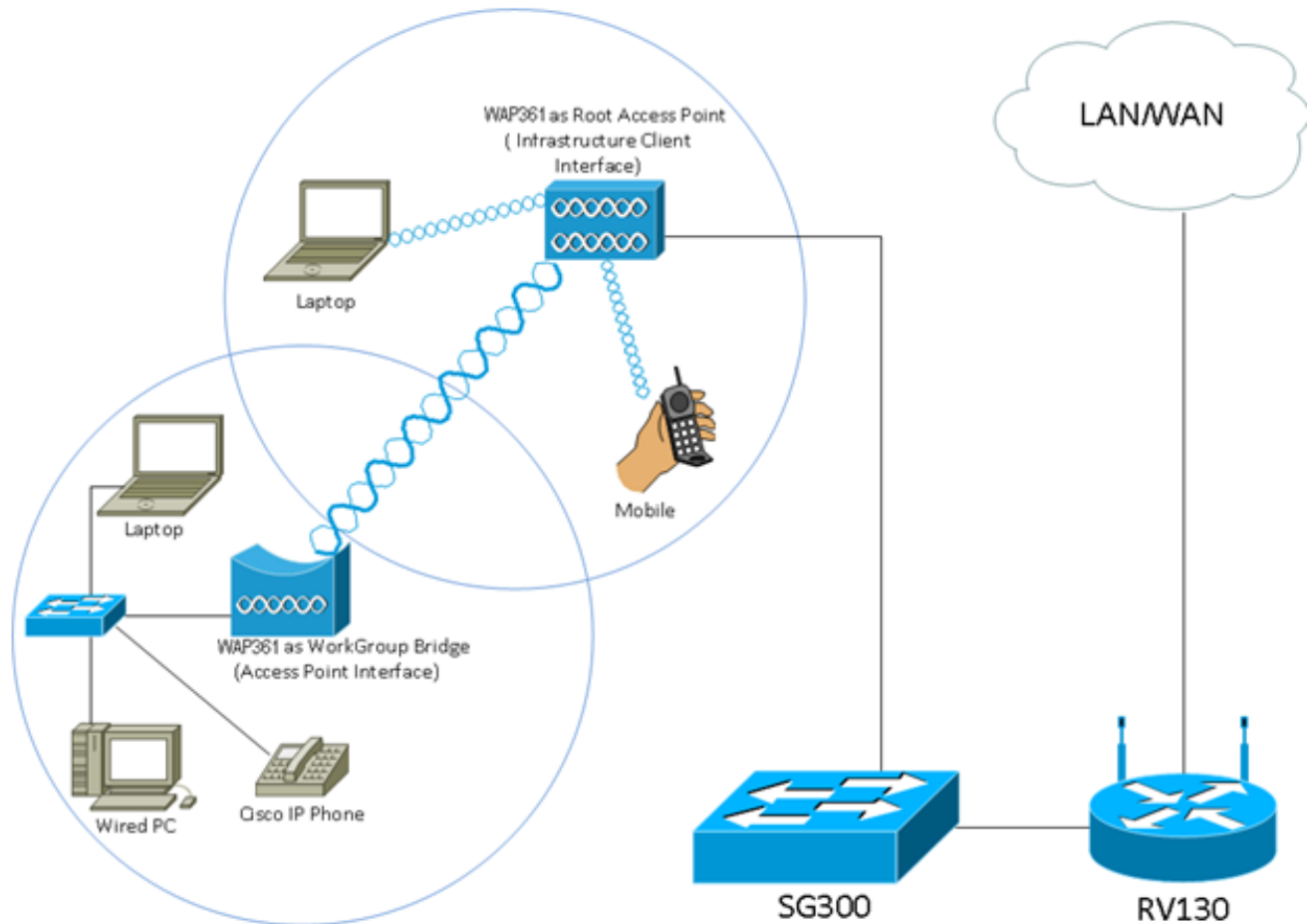


# 在无线接入点(WAP)上配置工作组桥

## 目标

工作组网桥功能使无线接入点(WAP)能够桥接远程客户端与与工作组网桥模式连接的无线局域网(LAN)之间的流量。与远程接口关联的WAP设备称为接入点接口，而与无线LAN关联的WAP设备称为基础设施接口。WorkGroup Bridge允许只有有线连接的设备连接到无线网络。当无线分发系统(WDS)功能不可用时，建议使用WorkGroup网桥模式作为替代模式。



**注意：**上面的拓扑说明了WorkGroup网桥模型示例。有线设备与连接到WAP的LAN接口的交换机相连。WAP充当接入点接口，连接到基础设施接口。

本文旨在向您展示如何在两个WAP之间配置工作组网桥。

## 适用设备

- WAP100系列
- WAP300系列
- WAP500系列

## 软件版本

- 1.0.0.17 - WAP571、WAP571E
- 1.0.1.7 — WAP150、WAP361
- 1.0.2.5 — WAP131、WAP351

- 1.0.6.5 — WAP121、WAP321
- 1.2.1.3 — WAP551、WAP561
- 1.3.0.3 — WAP371

## 配置WorkGroup网桥

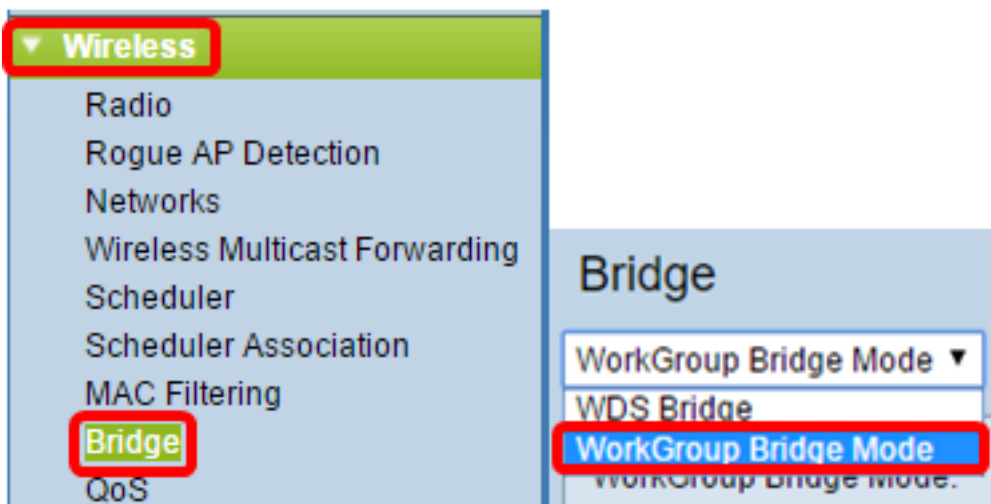
### 基础设施客户端接口

步骤1.登录到WAP的基于Web的实用程序，然后选择“无线”>“工作组桥”。

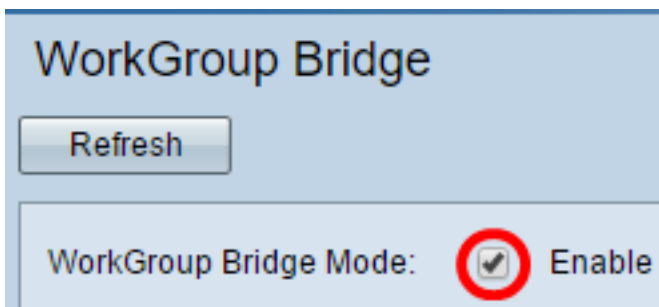
**注意：**菜单选项可能因您所使用设备的型号而异。除非另有说明，否则下面的图像从WAP361拍摄。



对于WAP571和WAP571E，选择Wireless > Bridge > WorkGroup Bridge Mode。



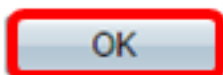
步骤2.选中Enable WorkGroup Bridge Mode ( 启用工作组网桥模式 ) 复选框。



**注意：**如果在WAP上启用集群，弹出窗口将通知您禁用集群，以便WorkGroup Bridge工作。单击 **OK** 继续。要禁用集群，请从**导航窗格**中选择单点设置，然后选择**接入点>禁用单点设置**。

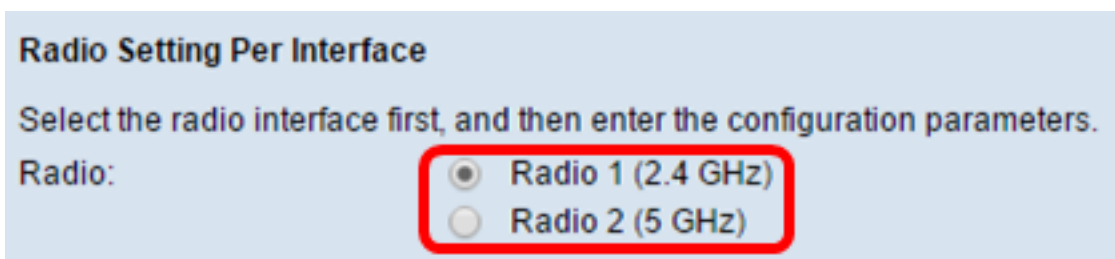


Workgroup Bridge cannot be enabled when clustering is enabled.



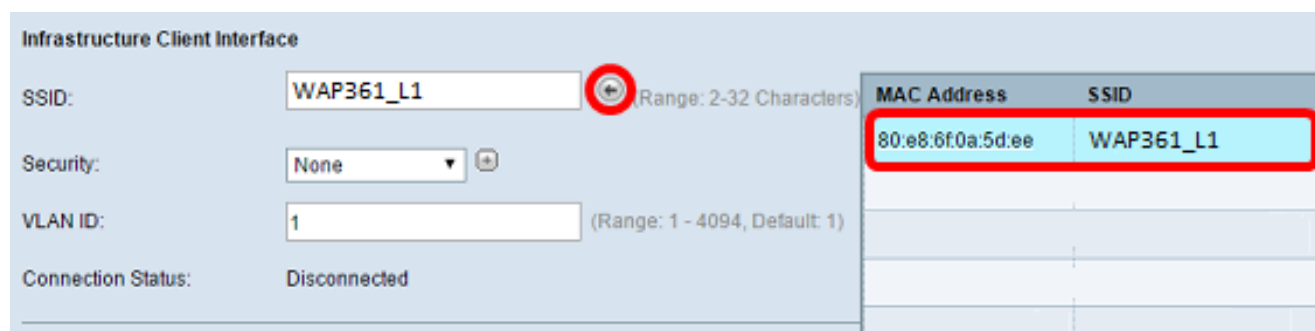
步骤3.单击工作组网桥的无线电接口。将一个无线电配置为工作组网桥时，另一个无线电将保持运行。无线电接口对应于WAP的无线电频带。WAP配备为在两个不同的无线电接口上广播。为一个无线电接口配置设置不会影响另一个无线电接口。无线电接口选项可能因WAP型号而异。某些WAP将Radio 1显示为2.4 GHz，而某些WAP将Radio 2显示为2.4 GHz。

**注意：**此步骤仅适用于以下双频WAP:WAP131、WAP150、WAP351、WAP361、WAP371、WAP561、WAP571、WAP571E。在本例中，选择Radio 1。



步骤4.在SSID字段中输入服务集标识符(SSID)名称，或单击字段旁边的箭头按钮扫描邻居。这用作设备与远程客户端之间的连接。您可以输入2到32个字符的基础设施客户端SSID。

**注意：**启用欺诈AP检测非常重要。要了解有关如何启用上述功能的详细信息，请单击[此处](#)。在本例中，点击箭头按钮以选择WAP361\_L1作为基础设施客户端接口的SSID。



步骤5.在Infrastructure Client Interface区域，从Security下拉列表中选择要作为上游WAP设备上的客户端站进行身份验证的安全类型。选项有：

- 无 — 打开或无安全。这是默认设置。如果选择此选项，请跳至[步骤18](#)。
- WPA个人 — WPA个人可支持长度为8-63个字符的密钥。建议使用WPA2，因为它具有更强大的加密标准。跳至[步骤6](#)进行配置。
- WPA企业 — WPA企业比WPA个人更高级，是推荐的身份验证安全。它使用受保护的可扩展身份验证协议(PEAP)和传输层安全(TLS)。跳至[步骤9](#)进行配置。此类安全通常用于办公环境，需要配置远程身份验证拨入用户服务(RADIUS)服务器。单击[此处](#)了解有关RADIUS服务器的详细信息。

Infrastructure Client Interface

SSID: WAP361\_L1

Security: WPA Personal (selected), None, WPA Personal, WPA Enterprise

VLAN ID:

Connection Status: Disconnected

**注意：**在本例中，选择WPA个人。

[步骤6](#).单击+并选中WPA-TKIP或WPA2-AES复选框，以确定基础设施客户端接口将使用哪种WPA加密。

**注意：**如果所有无线设备都支持WPA2，请将基础设施客户端安全设置为WPA2-AES。加密方法为WPA的RC4和WPA2的高级加密标准(AES)。建议使用WPA2，因为它具有更强大的加密标准。在本例中，使用WPA2-AES。

Security: WPA Personal

WPA Versions:  WPA-TKIP  WPA2-AES

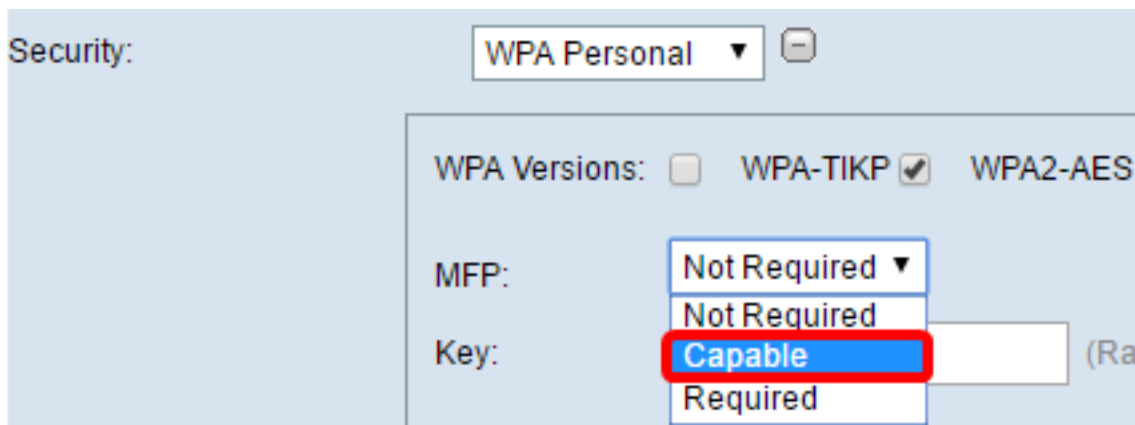
MFP: Not Required

Key: (Rare)

**步骤7.** ( 可选 ) 如果在步骤6中检查了WPA2-AES，请从Management Frame Protection(MFP)下拉列表选择一个选项，无论您是否希望WAP需要有受保护的帧。要了解有关MFP的详细信息，请单击[此处](#)。选项有：

- Not Required — 禁用客户端对MFP的支持。
- 支持 — 允许支持MFP的客户端和不支持MFP的客户端加入网络。这是WAP上的默认MFP设置。
- 必需 — 仅当协商MFP时，才允许客户端关联。如果设备不支持MFP，则不允许它们加入网络。

**注意：**在本例中，选择Capable。



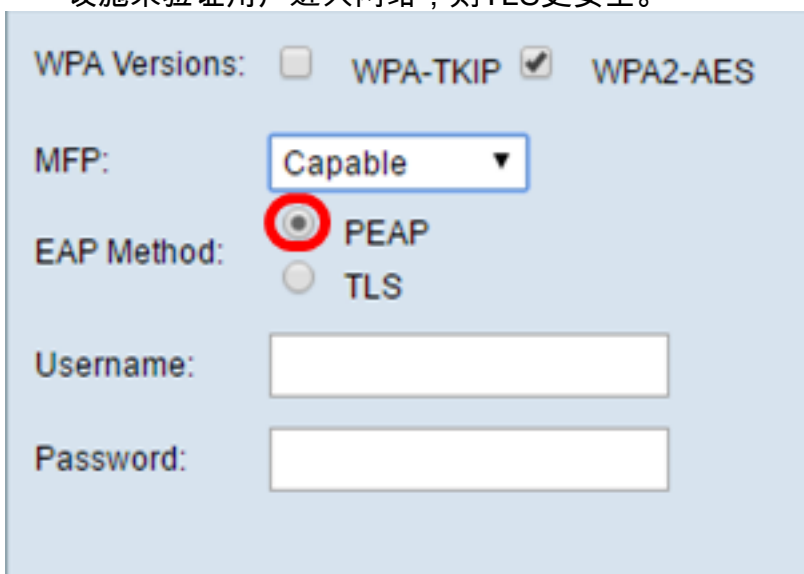
步骤8.在Key字段中输入WPA加密密钥。密钥长度必须为8-63个字符。这是字母、数字和特殊字符的组合。这是首次连接到无线网络时使用的密码。然后，跳至[步骤18](#)。



[步骤9](#).如果您在步骤5中选择了WPA企业，请点击EAP方法的单选按钮。

可用选项定义如下：

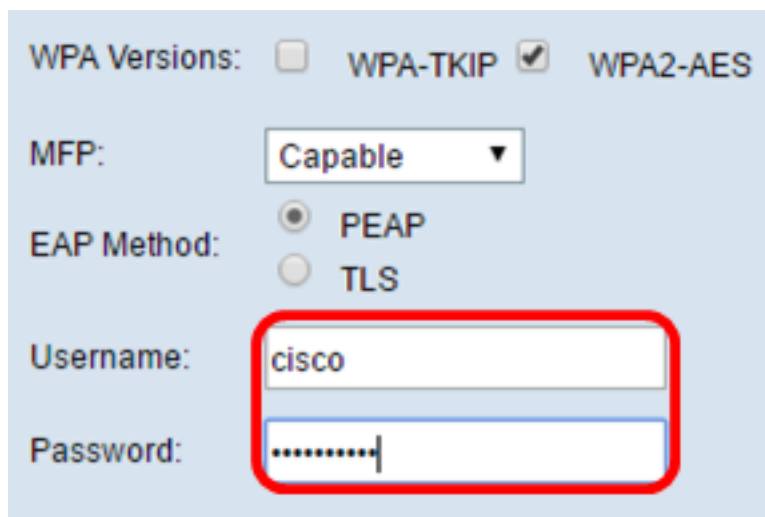
- PEAP — 此协议根据支持AES加密标准的WAP单独用户名和密码为每个无线用户提供。由于PEAP是基于密码的安全方法，因此Wi-Fi安全取决于客户端的设备凭证。如果您的密码薄弱或客户端不安全，PEAP可能会带来严重的安全风险。它依赖TLS，但避免在每个客户端上安装数字证书。相反，它通过用户名和密码提供身份验证。
- TLS - TLS要求每个用户拥有额外的证书以授予访问权限。如果您有额外的服务器和必要的基础设施来验证用户进入网络，则TLS更安全。



**注意：**在本例中，选择PEAP。

步骤10.在Username和Password字段中输入基础设施客户端的**用户名和密码**。这是用于连接

到基础设施客户端接口的登录信息；请参阅您的基础设施客户端界面以查找此信息。然后，跳至[步骤18](#)。



WPA Versions:  WPA-TKIP  WPA2-AES

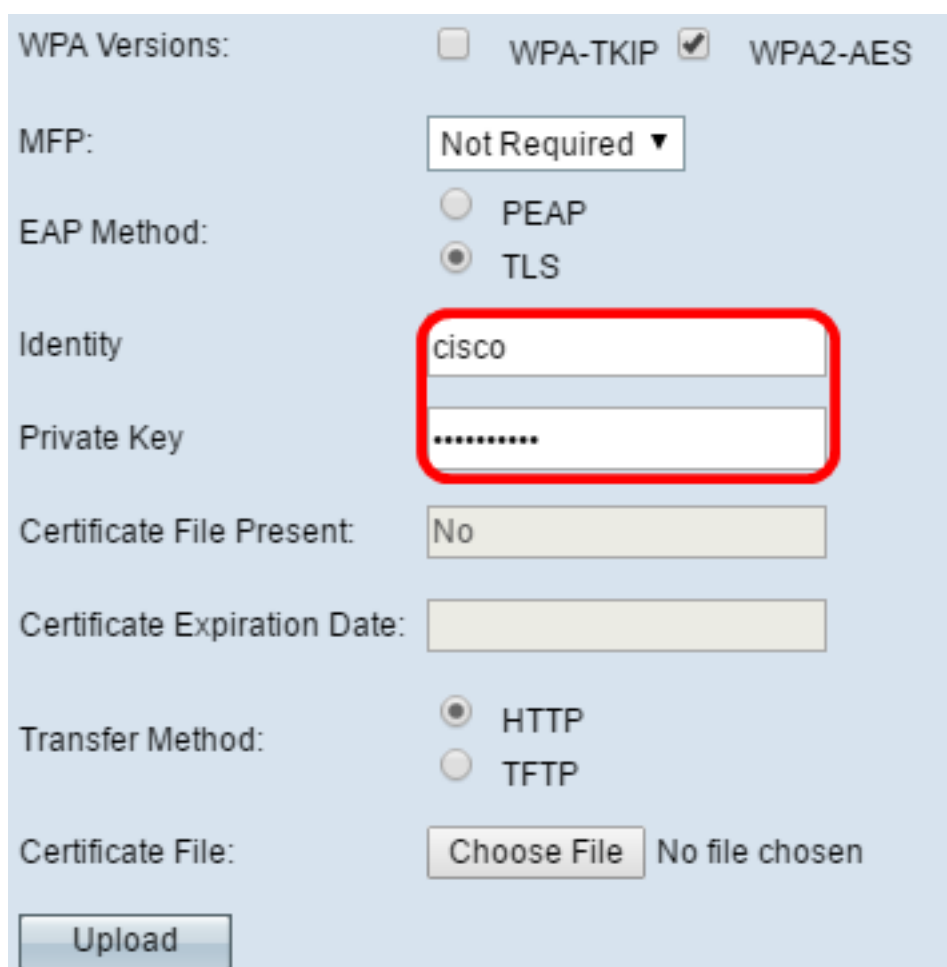
MFP:

EAP Method:  PEAP  TLS

Username:

Password:

步骤11.如果在步骤9中单击了TLS，请在“身份”和“私钥”字段中输入基础架构客户端的身份和私钥。



WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

[步骤12](#).在传输方法区域，单击以下选项的单选按钮：

- TFTP — 简单文件传输协议(TFTP)是简化的不安全文件传输协议(FTP)版本。它主要用于在企业网络之间分发软件或验证设备。如果单击了TFTP，请跳至[步骤15](#)。
- HTTP — 超文本传输协议(HTTP)提供简单的质询 — 响应身份验证框架，客户端可以使用该框架提供身份验证框架。

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

**注意：**如果WAP上已存在证书文件，则“证书文件存在”和“证书到期日期”字段将填入相关信息。否则，它们将为空。

## HTTP

步骤13.单击“选择文件”按钮以查找并选择证书文件。文件必须具有正确的证书文件扩展名(如 .pem或.pfx)，否则将不接受该文件。

**注意：**在本示例中，选择mini\_httpd(2)。pfx。

Transfer Method:  HTTP  TFTP

Filename:  mini\_httpd (2).pfx

步骤14.单击Upload上传所选证书文件。跳至[步骤18](#)。

Transfer Method:  HTTP  TFTP

Filename  mini\_httpd (2).pfx

“证书文件存在”和“证书过期日期”字段将自动更新。

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

## TFTP

[步骤15](#).如果在步骤12中单击了TFTP，请在文件名字段中输入证书文件的文件名。

**注意：**在本示例中，使用mini\_httpd.pem。



Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

步骤16.在TFTP Server IPv4 Address字段中输入TFTP Server地址。

注意：在本例中。192.168.1.20用作TFTP服务器地址。

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

步骤17.单击“**上**载****”按钮上载指定的证书文件。

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

“证书文件存在”和“证书过期日期”字段将自动更新。

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

[步骤18](#). 输入基础设施客户端接口的VLAN ID。默认值是 1。

**注意：**在本例中，使用默认VLAN ID。

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

## 接入点接口

步骤1. 选中Enable Status复选框以在接入点接口上启用桥接。

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

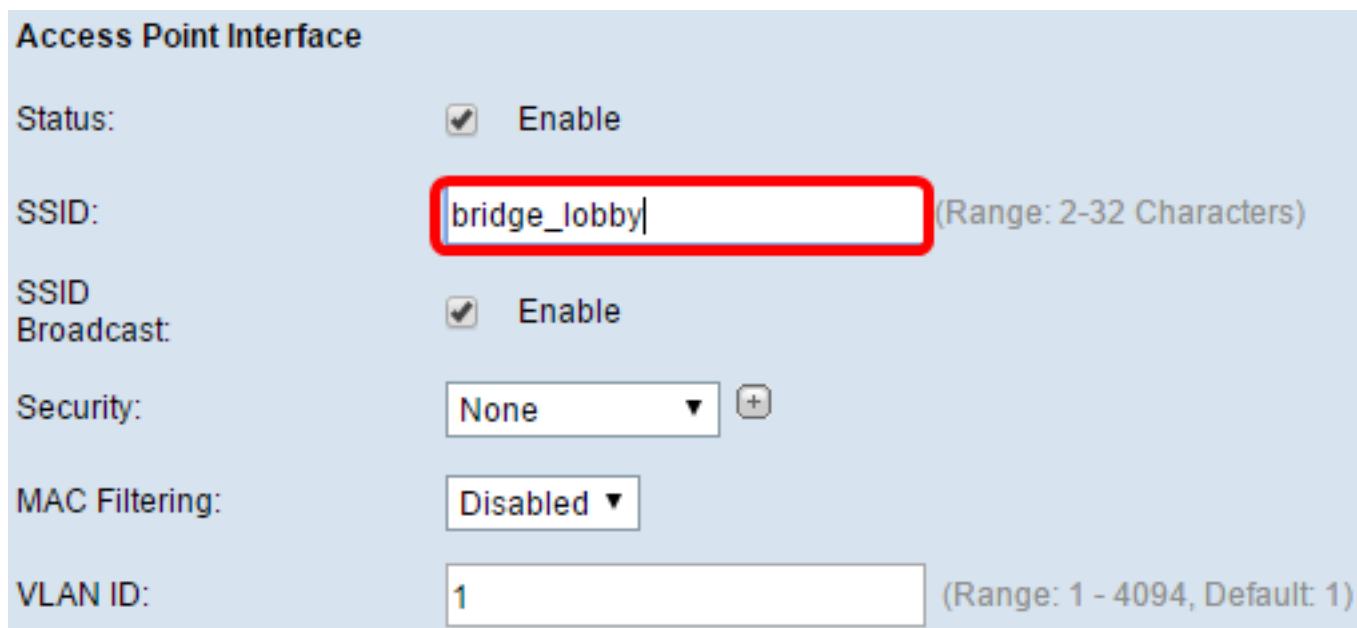
Security:   ▼

MAC Filtering:  ▼

VLAN ID:  (Range: 1 - 4094, Default: 1)

步骤2. 在SSID字段中输入接入点的SSID。SSID长度必须介于2到32个字符之间。默认为接入点SSID。

**注意：**在本例中，使用的SSID为bridge\_lobby。



**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)


SSID Broadcast:  Enable

Security:  (+)

MAC Filtering:  ▾

VLAN ID:  (Range: 1 - 4094, Default: 1)

步骤3. ( 可选 ) 如果不想广播SSID，请取消选中**Enable** SSID Broadcast复选框。这样做将使搜索无线接入点的用户看不到接入点；它只能由已经知道SSID的人连接。SSID广播默认启用。



**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  (+)

MAC Filtering:  ▾

VLAN ID:  (Range: 1 - 4094, Default: 1)

步骤4.从Security下拉列表中选择对WAP的下游客户端站进行身份验证的安全类型。

可用选项定义如下：

- 无 — 打开或无安全。这是默认值。如果选择[此选项](#)，请跳至步骤10。
- WPA个人 — Wi-Fi保护访问(WPA)个人可支持长8到63个字符的密钥。加密方法为TKIP或计数器密码模式(使用块链消息身份验证代码协议(CCMP))。与仅使用64位RC4标准的临时密钥完整性协议(TKIP)相比，建议使用带CCMP的WPA2，因为它具有更强大的加密标准高级加密标准(AES)。

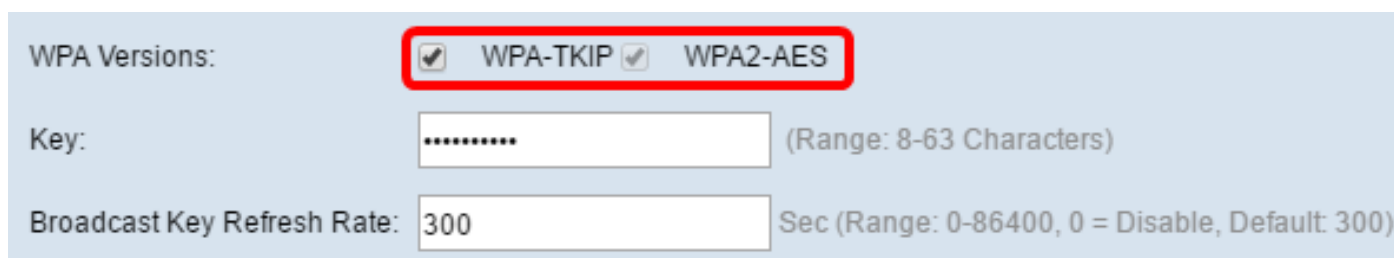


Security:  ▾ (+)

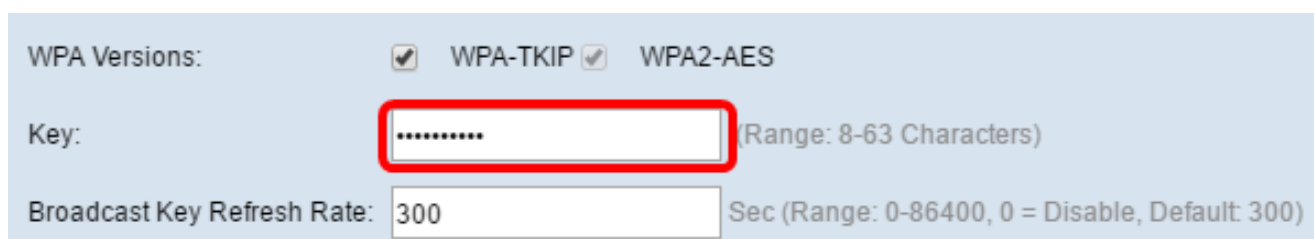
WPA Versions:  ▾

步骤5.选中WPA-TKIP或WPA2-AES复选框，以确定接入点接口将使用哪种WPA加密。默认情况下，这些功能已启用。

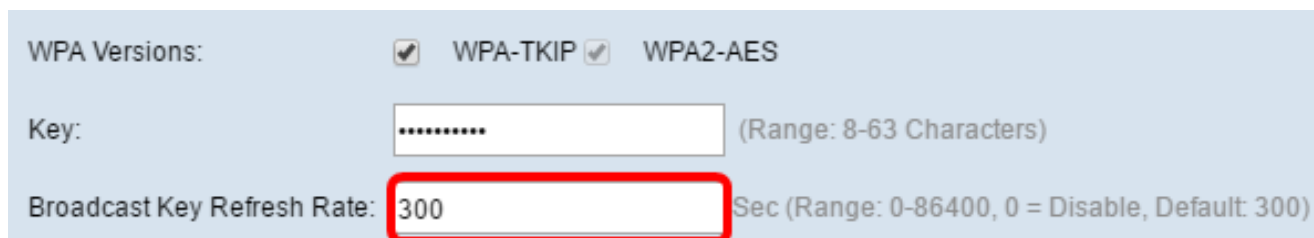
**注意：**如果所有无线设备都支持WPA2，则将基础设施客户端安全设置为WPA2-AES。加密方法为WPA的RC4和WPA2的高级加密标准(AES)。建议使用WPA2，因为它具有更强大的加密标准。在本例中，使用WPA2-AES。



步骤6.在Key字段中输入共享WPA密钥。密钥的长度必须为8-63个字符，并且可以包含字母数字字符、大小写字符和特殊字符。



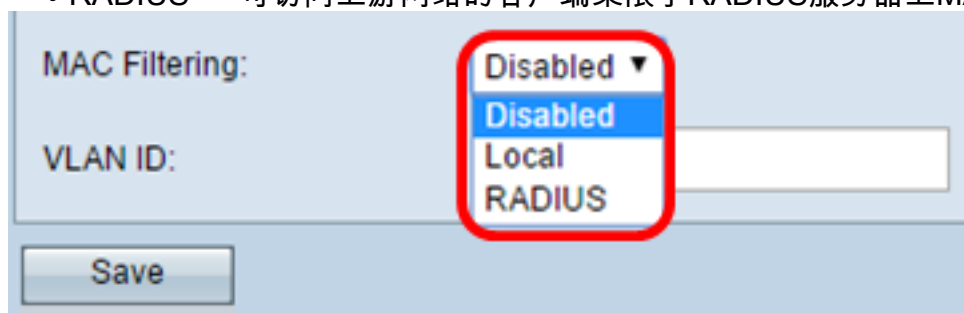
步骤7.在Broadcast Key Refresh Rate字段中输入速率。广播密钥刷新率指定与此接入点关联的客户端刷新安全密钥的间隔。速率必须介于0到86400之间，值为0将禁用该功能。默认值为300。



步骤8.从MAC过滤下拉列表中选择要为接入点接口配置的MAC过滤类型。启用后，根据用户所使用客户端的MAC地址，向用户授予或拒绝对WAP的访问权限。

可用选项定义如下：

- 已禁用 — 所有客户端都可以访问上游网络。这是默认值。
- 本地 — 可访问上游网络的客户端集仅限于在本地定义的MAC地址列表中指定的客户端。
- RADIUS — 可访问上游网络的客户端集限于RADIUS服务器上MAC地址列表中指定的客户端。



**注意：**在本例中，选择Disabled。

步骤9.在VLAN ID字段中为接入点接口输入VLAN ID。

**注意：**要允许数据包桥接，接入点接口和有线接口的VLAN配置应与基础设施客户端接口的VLAN配置匹配。

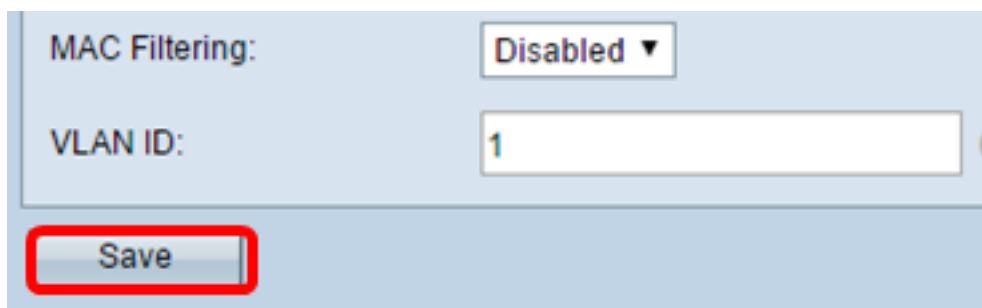


MAC Filtering: Disabled ▾

VLAN ID: 1

Save

[步骤10.](#)单击保存保存更改。



MAC Filtering: Disabled ▾

VLAN ID: 1

Save

现在，您应该已在无线接入点上成功配置工作组网桥。