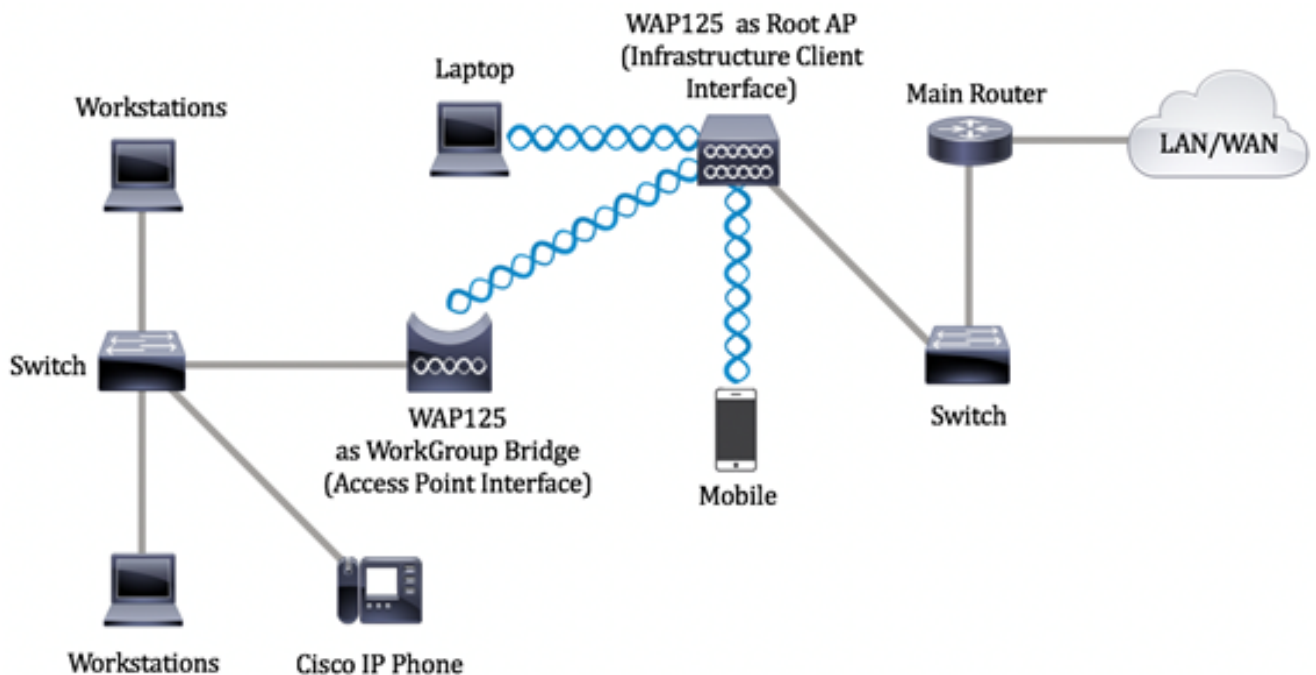


# 在WAP125或WAP581接入点上配置WorkGroup Bridge设置

## 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。

下面的拓扑说明了示例WorkGroup Bridge模型。有线设备与连接到WAP的LAN接口的交换机相连。在以下示例中，WAP125充当连接到基础设施客户端接口的接入点接口。



本文提供有关如何在两个无线接入点之间配置WorkGroup网桥设置的说明。

## 适用设备

- WAP125
- WAP581

## 软件版本

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## 配置WorkGroup网桥设置

在WAP设备上配置工作组网桥之前，请注意以下准则：

- 参与WorkGroup Bridge的所有WAP设备必须具有以下相同设置：

— 无线电

- IEEE 802.11模式

— 通道带宽

— 通道（不建议自动）

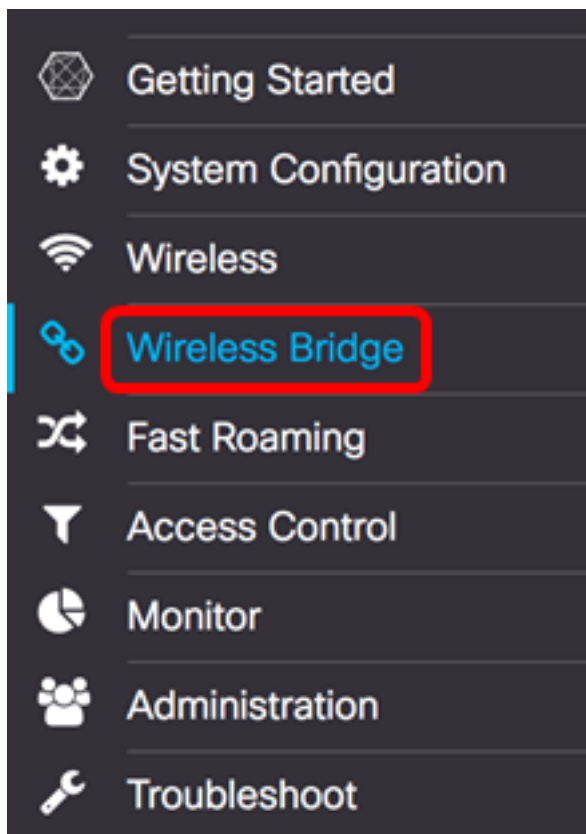
**注意：**要了解如何在WAP125上配置这些设置，请单击[此处](#)获取说明。对于WAP581，请单击[此处](#)。

- 工作组网桥模式当前仅支持IPv4流量。
- 单点设置不支持工作组网桥模式。如果您有WAP581接入点，请在配置工作组网桥设置之前先禁用SPS或群集。有关如何在WAP上配置SPS设置的说明，请单击[此处](#)。

## 配置基础设施客户端接口

步骤1.登录WAP的基于Web的实用程序，然后选择**Wireless Bridge**。

**注意：**可用选项可能因设备的确切型号而异。在本例中，使用WAP125。



步骤2.单击WorkGroup单选按钮。

# Wireless Bridge

Wireless Bridge Mode:   WDS  WorkGroup

步骤3.选中Uplink复选框。




<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

步骤4.单击“编辑”图标。



<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

步骤5.选中Enabled复选框以启用Infrastructure Client Interface。



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input checked="" type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)

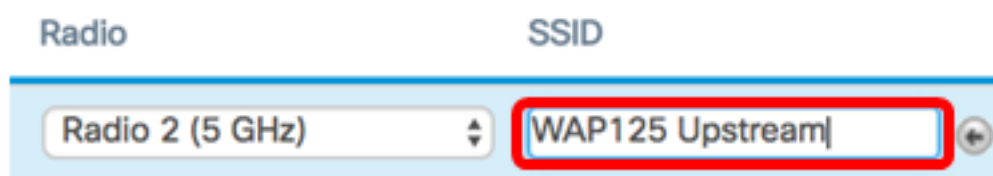
步骤6.选择工作组网桥的无线电接口。将一个无线电配置为工作组网桥时，另一个无线电将保持运行。无线电接口对应于WAP的无线电频带。WAP配备为在两个不同的无线电接口上广播。为一个无线电接口配置设置不会影响另一个无线电接口。

Enabled	Radio
<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Radio 2 (5 GHz)

**注意：**在本例中，选择无线电2(5 GHz)。

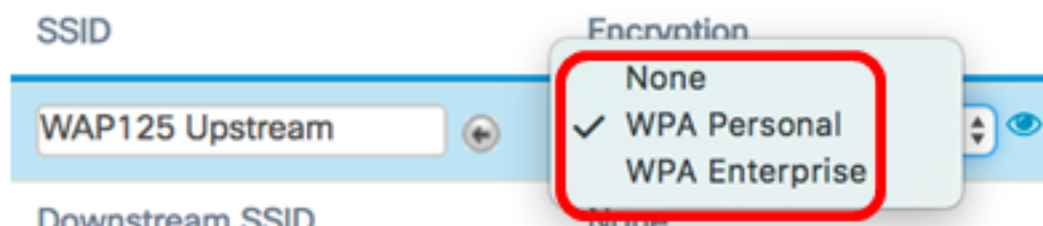
步骤7.在SSID字段中输入服务集标识符(SSID)的名称。这用作设备与远程客户端之间的连接。您可以输入2到32个字符的基础设施客户端SSID。

**注意：**在本例中，使用WAP125 Upstream。




**注意：**SSID旁边的箭头可用于SSID扫描。此功能默认为禁用状态，仅在欺诈AP检测中启用AP检测时启用，默认情况下也禁用此功能。

步骤8.从Encryption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22](#)。
- 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。
- 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12](#)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。

**注意：**在本例中，选择WPA个人。

步骤9.单击图  标并选中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。

## Security Setting

WPA Versions:  WPA-TKIP  WPA2-AES

**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。

步骤10. ( 可选 ) 如果在步骤9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。

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

**注意：**在本例中，选择Capable。

步骤11.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21](#)。

MFP:

Key:

Show Key as Clear Text

[步骤12](#).如果在步骤8中选择了WPA企业，请单击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。如果选择此选项，请跳至[步骤14](#)。

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

**注意：**在本例中，选择PEAP。

步骤13.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21](#)。

EAP Method:  PEAP  TLS

Username:

Password:

Show Key as Clear Text

**步骤14.**如果在步骤12中单击了TLS，请在“身份”和“私钥”字段中输入基础设施客户端的身份和私钥。

EAP Method:  PEAP  TLS

Identity:

Private Key:

Show Key as Clear Text

**步骤15.**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18](#)。
- 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。

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

**注意：**如果WAP上已存在证书文件，则Certificate File Present和Certificate Expiration Date字段将填入相关信息。否则，它们将为空。

## HTTP

**步骤16.**单击“浏览”按钮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：**在本例中，选择Certificate.pfx。

步骤17.单击**Upload**上传所选证书文件。跳至[步骤21](#)。

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  Certificate.pfx

证书文件存在(Certificate File Present)和证书过期日期(Certificate Expiration Date)字段将自动更新。

### TFTP

[第18步](#)。(可选)如果在第15步中单击了TFTP，请在Filename字段中输入证书文件的文件名。

Transfer Method:  HTTP  TFTP

Filename

**注意：**在本例中，使用Certificate.pfx。

步骤19.在TFTP Server IPv4 Address字段中输入TFTP Server地址。

Transfer Method:  HTTP  TFTP

Filename: Certificate.pfx

TFTP Server IPv4 Address: 192.168.100.108

**注意：**在本例中。192.168.100.108用作TFTP服务器地址。

步骤20.单击“**上載**”按钮上載指定的证书文件。

Transfer Method:  HTTP  TFTP

Filename: Certificate.pfx

TFTP Server IPv4 Address: 192.168.100.108

**Upload**

证书文件存在(Certificate File Present)和证书过期日期(Certificate Expiration Date)字段将自动更新。

步骤21.单击**OK**关闭Security Setting窗口。

**OK** cancel

Connection Status区域指示WAP是否连接到上游WAP设备。

Encryption	Connection Status
WPA Personal	Disconnected

步骤22.输入基础设施客户端接口的VLAN ID。默认值是 1。

Connection Status	VLAN ID
Disconnected	1

**注意：**在本例中，使用默认VLAN ID。

步骤23.单击“**保存**”以保存已配置的设置。



Save

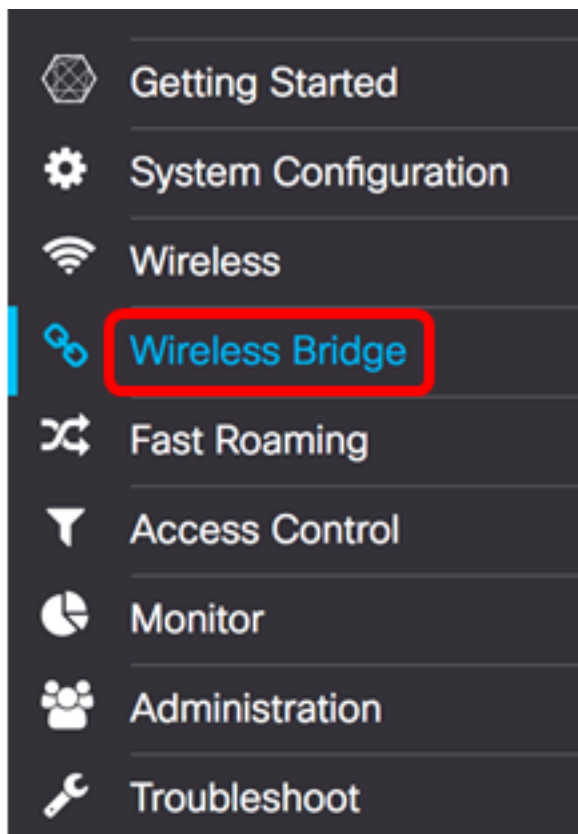
Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	<input type="text" value="1"/>	N/A	N/A
N/A	1	<input checked="" type="checkbox"/>	Disabled

现在，您应该已成功配置WAP上的基础设施客户端接口设置。

## 配置接入点客户端接口

步骤1. 登录WAP的基于Web的实用程序，然后选择**Wireless Bridge**。

**注意：**可用选项可能因设备的确切型号而异。在本例中，使用WAP125。



步骤2. 单击WorkGroup单选按钮。

# Wireless Bridge

Wireless Bridge Mode:  ?  WDS  WorkGroup

步骤3.选中Downlink复选框。



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

步骤4.单击“编辑”按钮。



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

步骤5.选中Enabled复选框以启用接入点接口上的桥接。

<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
-------------------------------------	----------	-------------------------------------	-----------------

步骤6.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。默认值为Downstream SSID。

Radio 2 (5 GHz)	<input type="text" value="WAP125 Downstream"/>
-----------------	--

**注意：**在本例中，使用的SSID是WAP125 Downstream。

步骤7.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13。
- 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)。



步骤8. (可选) 选中WPA-TKIP复选框以确定接入点接口将使用的WPA-TKIP加密。默认情况下启用该接口。

**注意：**WPA-AES灰显，无法禁用。在本例中，未选中WPA-TKIP。

## Security Setting

WPA Versions:

WPA-TKIP  WPA2-AES

步骤9.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。

WPA Versions:

WPA-TKIP  WPA2-AES

Key: ?

.....

Show Key as Clear Text

步骤10.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。

Broadcast Key Refresh Rate: ?

86400

**注意：**在本例中，使用86400。

步骤11.从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。

Broadcast Key Refresh Rate: ?

MFP:

**注意：**在本例中，选择Capable。

步骤12.单击OK保存安全设置。

## Security Setting

WPA Versions:  WPA-TKIP  WPA2-AES

Key: ?

Show Key as Clear Text

Broadcast Key Refresh Rate: ?

MFP:

“连接状态”区域指示“不适用”或“不适用”。

Encryption	Connection Status
WPA Personal	Disconnected
<input type="text" value="WPA Personal"/> <span>?</span>	<input type="text" value="N/A"/>

**步骤13.**在接入点接口的VLAN ID字段中输入VLAN ID。

**注意：**要允许桥接数据包，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。

步骤14.如果要广播下游SSID，请选中SSID Broadcast复选框。SSID广播默认启用。

VLAN ID	SSID Broadcast	Client Filter
1	N/A	N/A

1	<input checked="" type="checkbox"/>	Disabled
---	-------------------------------------	----------

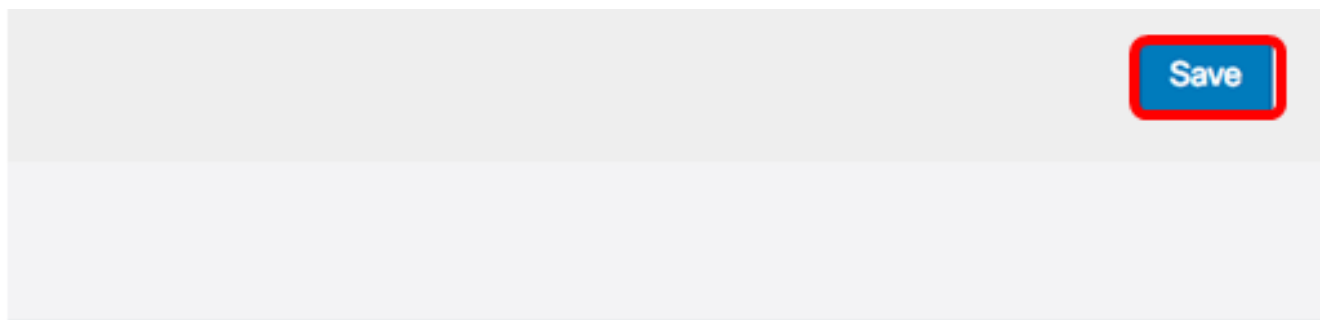
步骤15.从MAC Filtering下拉列表中选择要为接入点接口配置的MAC过滤类型。启用后，根据用户所使用客户端的MAC地址，向用户授予或拒绝对WAP的访问权限。

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16.单击“保存”以保存更改。



Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	1	N/A	N/A

N/A	1	<input checked="" type="checkbox"/>	Disabled
-----	---	-------------------------------------	----------

您现在应该已成功配置无线接入点上的WorkGroup Bridge设置。