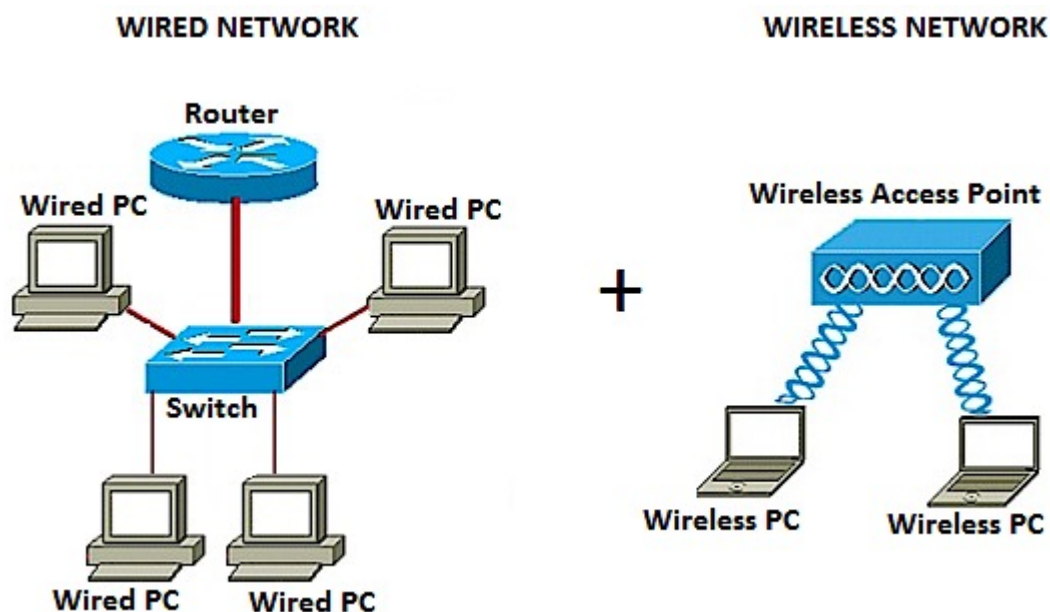


添加一个无线网络到一个现有有线网络使用无线接入点(WAP)

目标

无线接入点(WAP)是允许无线有能力设备连接到有线网络的网络设备。添加WAP到您的现有有线网络是有用的适应只有能力在无线连接上的那些设备。它是类似创建另一仅网络无线设备的，但是仍然是您的现有有线网络的部分例如显示在下图所示中。



在以上的网络图中，左侧部分显示一个现有有线网络。它包括四台有线计算机连接对交换机，连接到路由器。在正确的部分，无线网络显示两台无线计算机连接对WAP。

此条款目标如何将显示您添加无线网络对您的现有有线网络使用无线接入点。

可适用的设备

- WAP100系列
- WAP300系列
- WAP500系列

软件版本

- 1.0.6.5 — WAP121, WAP321
- 1.0.2.8 — WAP131, WAP351
- 1.0.1.7 — WAP150, WAP361
- 1.3.0.3 — WAP371
- 1.2.1.3 — WAP551, WAP561
- 1.0.0.17 — WAP571, WAP571E

添加无线网络到现有有线网络

建立无线网络

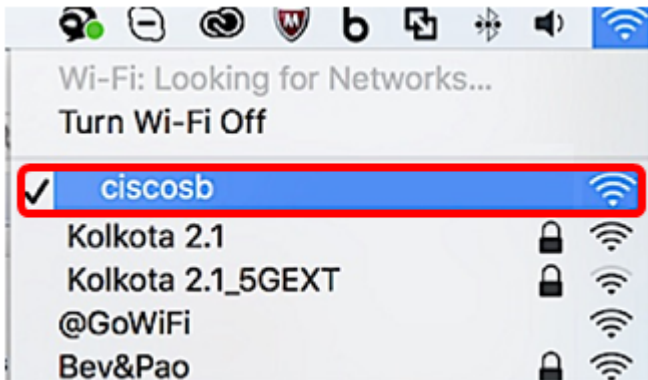
注意：镜像可能根据您的WAP确切的模型变化。用于此条款的镜像从WAP361被采取。

步骤1.使用由供应的以太网电缆，连接WAP到您的路由器或交换机。

注意：如果您的WAP没有在以太网(PoE)功能的电源，请连接AC电源适配器对WAP并且插入它到电源插座。

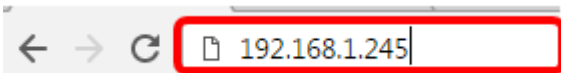
步骤2.连接您的无线计算机对无线网络WAP广播。

注意：Cisco接入点的默认服务设备标识器(SSID)或无线网络名称是ciscosb。



第 3 步：在无线计算机上，请通过启动Web浏览器和输入WAP的IP地址访问WAP的基于Web的工具在地址栏的。

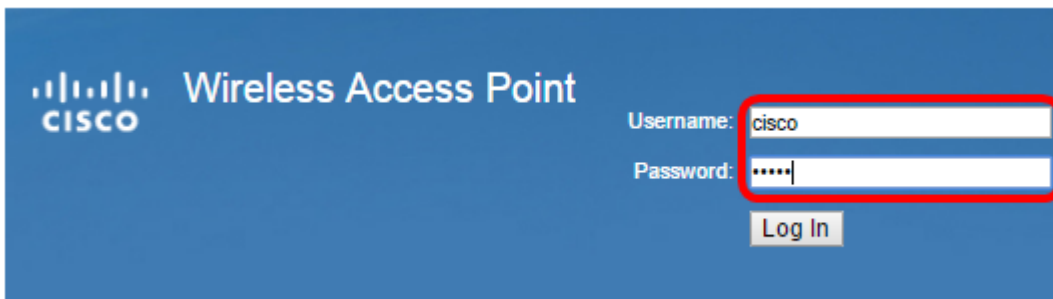
注意：在不认识您的WAP情况下的IP地址，您能使用Cisco FindIT发现工具或Cisco FindIT网络管理工具，如果这些应用程序在您的网络安装。这些应用程序将帮助您检查IP地址和接入点和其他Cisco设备的其他信息在您的网络内。[要了解更多信息，单击这里。](#)



注意：在上面镜像，192.168.1.245例如IP地址使用。这是Cisco接入点默认IP地址。

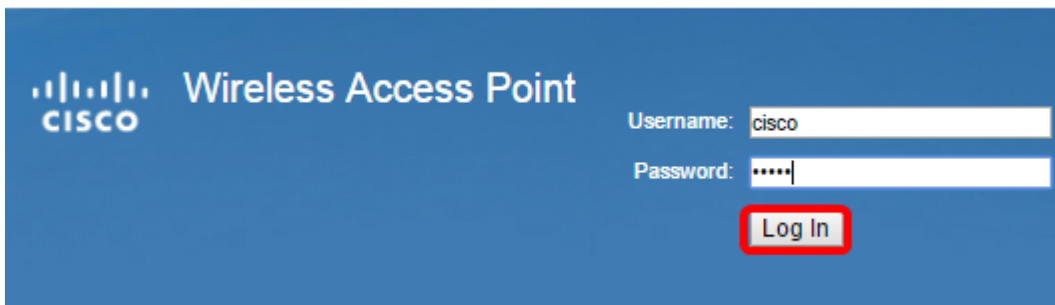
第 4 步：在验证窗口，请在用户名和密码字段输入WAP的用户名和密码，分别。

注意：您能设置对五个用户到每接入点您是去的添加对网络。这些用户是授权的那个通过他们的认证密钥访问基于Web的工具，但是仅一个这些用户能有读/写权限级别。并且，您能创建一个不同的用户名和密码对每个用户。[学习，如何请点击此处。](#)

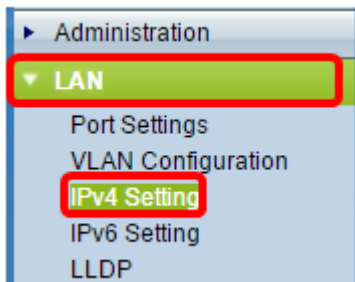


注意：默认用户的默认用户名和密码Cisco接入点的是cisco/cisco。

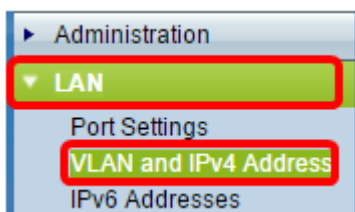
步骤5.点击“Login”。



第六步：在定位区域中，请选择LAN > IPv4设置。



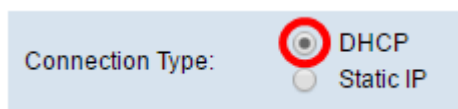
注意：如果使用WAP121、WAP321、WAP371、WAP551或者WAP561，请选择LAN > VLAN和IPv4地址。



注意：如果要使用IPv6寻址，为说明请点击[此处](#)。

步骤7. 点击单选按钮选择连接类型。

- DHCP —接入点获取其从一个动态主机配置协议(DHCP)服务器的IP地址在网络。
- 静态IP —您将是手工分配对WAP的IPv4地址的那个。



注意：在本例中，DHCP选择。这是默认设置。如果执行了此步骤，请跳过对[步骤12](#)。

步骤8. (可选)，如果选择在上一步的静态IP，输入您想要分配对WAP在静态IP地址字段的静态IP地址。确保您分配的IP地址在范围和您的网络一样。

Static IP Address:	192	. 168	. 1	. 112
Subnet Mask:	0	. 0	. 0	. 0
Default Gateway:	0	. 0	. 0	. 0

注意：在本例中，使用的IP地址是192.168.1.112。

步骤9. (可选)回车子网掩码在子网掩码字段。

Static IP Address:	192	168	1	112
Subnet Mask:	255	255	255	0
Default Gateway:	0	0	0	0

注意：在本例中，使用255.255.255.0。

步骤10.在默认网关字段进入路由器IP地址。

Static IP Address:	192	168	1	112
Subnet Mask:	255	255	255	0
Default Gateway:	192	168	1	1

注意：在本例中，192.168.1.1使用作为默认网关。

步骤 11在域名服务器(DNS)地区中，指南的单选按钮将自动地选择，一旦连接类型设置为静态IP。您能输入两个DNS地址在提供的字段。

Domain Name Servers:	<input type="radio"/> Dynamic
	<input checked="" type="radio"/> Manual
	192 . 168 . 1 . 1

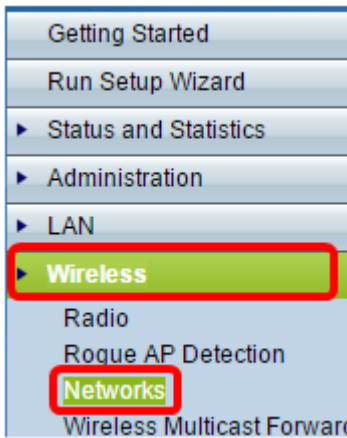
注意：在本例中，使用192.168.1.1。

步骤 12Click **Save**.

Connection Type:	<input type="radio"/> DHCP
	<input checked="" type="radio"/> Static IP
Static IP Address:	192 . 168 . 1 . 112
Subnet Mask:	255 . 255 . 255 . 0
Default Gateway:	192 . 168 . 1 . 1
Domain Name Servers:	<input type="radio"/> Dynamic
	<input checked="" type="radio"/> Manual
	192 . 168 . 1 . 1
Save	

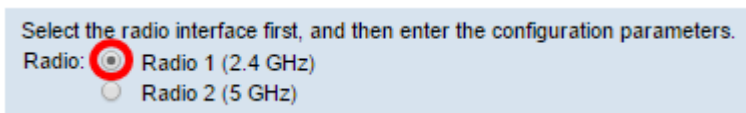
配置无线设置

步骤1.选择无线>网络。



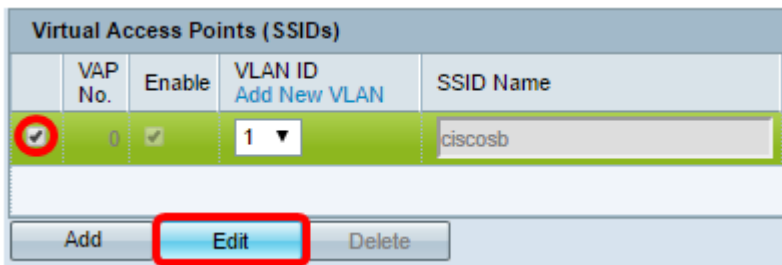
步骤2. (可选) , 如果使用一双波段接入点 , 点击单选按钮选择您要配置的无线接口。

- 无线电1 (2.4 GHz) —对于在2.4 GHz频率经营的无线客户端。
- 无线电2 (5 GHz) —对于在5个GHz频率经营的无线客户端。



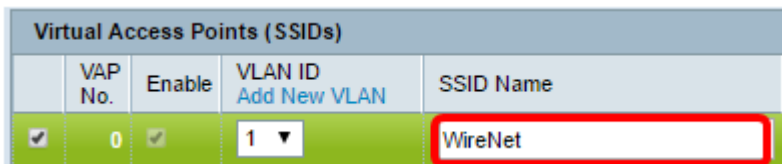
注意：在本例中，无线电1 (2.4 GHz)选择。

第 3 步：在虚拟访问访问接入点(Ssid)地区下，请检查在默认虚拟访问访问接入点(VAP)旁边的方框并且在它之下单击编辑按钮。



注意：您能根据您的设备确切的模型添加或创建在您的WAP的多个VAPs通过单击在Add按钮。对于WAP361，七其他VAPs可以创建。

第 4 步：在SSID名称下，请在提供的字段创建一个新名字对于您的无线网络。



注意：在本例中，使用金属网。

在SSID广播下的步骤5. (可选) , 检查或根据您的首选非选定方框。检查方框将允许您的无线网络广播其SSID或是可视对在其范围内的所有无线设备。非选定方框将躲藏起来从它所有无线设备。

Virtual Access Points (SSIDs)					
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	WireNet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

注意：在本例中，SSID广播被检查。

第六步：在安全下，请点击下拉菜单选择您在无线网络要设置安全的种类。选项有：

- 无—此选项将设置安全打开和允许所有无线设备连接到您的无线网络，不用密码或验证的询问。
- 个人的WPA — Wi-Fi保护访问(WPA)是设计的安全协议改善在有线等效保密(WEP)安全功能。WPA使用更加高，256-bit锁上并且改进数据加密和用户认证。此安全模式允许您使用临时密钥完整性协议(TKIP)算法或者最新，高级高级加密安全(AES)算法，如果设备是更新的并且支持它与WPA。两个选项，然而，实现更加强化的安全标准。
- WPA企业—在企业模式，Wi-Fi保护访问(WPA)与远程验证拨入用户服务(RADIUS)服务器验证一起使用。

Virtual Access Points (SSIDs)						
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	WireNet	<input checked="" type="checkbox"/>	WPA Personal None WPA Personal WPA Enterprise	

Add Edit Delete

Note:在本例中，个人的WPA选择。证券详细资料窗口然后可视。

步骤7.选择您在WPA版本地区要支持通过检查复选框客户端工作站的种类。

- WPA-TKIP — 此选项将允许只支持原始WPA和TKIP安全协议能连接到网络的无线客户端。
- WPA2-AES — 此WPA版本提供最好的安全每个IEEE 802.11i标准。根据最新的wi-fi联盟需求，WAP必须一直支持此模式。

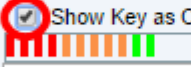
注意：如果网络有客户端的混合，请检查两个复选框。此设置让WPA和WPA2客户端工作站联合和验证，但是使用更加稳健的WPA2支持它的客户端。此WPA配置在若干安全位置准许更多互通性。

WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text"/> (Range: 8-63 Characters)	
	<input type="checkbox"/> Show Key as Clear Text	
Key Strength Meter:	<input type="text"/> Session Key Refresh Rate	
Broadcast Key Refresh Rate	<input type="text"/> 300	Sec (Range: 0-86400, 0 = Disable, Default: 300)

步骤 8在密钥字段，请输入密码包括的8到63字符。将设法连接到此无线网络的每个无线设备为此认证密钥将询问。

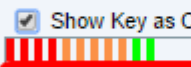
WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text"/> (Range: 8-63 Characters)	
	<input type="checkbox"/> Show Key as Clear Text	
Key Strength Meter:	<input type="text"/> Strong	
Broadcast Key Refresh Rate	<input type="text"/> 300	Sec (Range: 0-86400, 0 = Disable, Default: 300)

步骤9. (可选)检查显示密钥作为显示您创建的密码的明文文本框。

WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text" value="Str0ngPassw0rd!"/>	(Range: 8-63 Characters)
Key Strength Meter:	<input checked="" type="checkbox"/> Show Key as Clear Text  Strong	
Broadcast Key Refresh Rate	<input type="text" value="300"/>	Sec (Range: 0-86400, 0 = Disable, Default: 300)

注意：密钥强度公尺地区显示对有色人种的歧视根据依赖密钥您创建。在本例中，Str0ngPassw0rd!使用作为认证密钥。

步骤 10在广播密钥刷新率字段，请输入从0的一个值到86400秒。这是广播的间隔(组)密钥为客户端刷新关联与此VAP。

WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text" value="Str0ngPassw0rd!"/>	(Range: 8-63 Characters)
Key Strength Meter:	<input checked="" type="checkbox"/> Show Key as Clear Text  Strong	
Broadcast Key Refresh Rate	<input type="text" value="300"/>	Sec (Range: 0-86400, 0 = Disable, Default: 300)

注意：在本例中，使用300秒。这是默认值。

在MAC过滤器下的步骤11. (可选)，点击下拉列表禁用MAC过滤器或指定能访问此VAP的站点是否限制对MAC地址—已配置的全局列表。选项有：

- 已禁用—不使用MAC过滤。
- 本地—使用您在过滤页的MAC配置的MAC验证列表。
- RADIUS —使用在外部RADIUS服务器的MAC验证列表。

注意：要[学习如何配置过滤的MAC，请点击此处。](#)

SSID Name	SSID Broadcast	Security	MAC Filter
WireNet	<input checked="" type="checkbox"/>	WPA Personal ▼	Local ▼
			<input type="checkbox"/> Disabled <input checked="" type="checkbox"/> Local <input type="checkbox"/> RADIUS

注意：在本例中，本地选择。

步骤 12(可选)请检查或非选定复选框在信道隔离下根据您的首选启用或禁用它。当启用，WAP阻塞无线客户端之间的通信在同样VAP。WAP仍然允许其无线客户端和有线的设备之间的数据流在网络，在一条无线分布式系统(WDS)链路间和有其他无线客户端的关联与不同的VAP，但是不在无线客户端中。当禁用，无线客户端能通过发送流量通常互相通信通过WAP。

SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
WireNet	<input checked="" type="checkbox"/>	WPA Personal ▼	Local ▼	<input type="checkbox"/>
Show Details				

注意：在本例中，信道隔离禁用。这是默认设置。

步骤 13(可选)请检查或非选定复选框在波段操舵下根据您的首选启用或禁用它。此功能是为仅双波段WAPs。启用波段操舵通过操纵从2.4 GHz频段的双波段支持的客户端有效使用5 GHz频段到5 GHz频段，当两无线电是UP时。

SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
<input checked="" type="checkbox"/>	WPA Personal	Local	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[Show Details](#)

注意：在本例中，波段操舵启用。

步骤 14 Click **Save**.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/>	1	WireNet	<input checked="" type="checkbox"/>	WPA Personal	Local	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

[Show Details](#)

如下图所示所显示，您应该成功地当前添加无线网络到您的现有有线网络使用无线接入点。

