283935

管理指南

思科 Small Business

WAP121 Wireless-N 接入点（支持 PoE）

和

WAP321 Wireless-N 可选频段接入点（支持 PoE）

目录

1

使用入门

本章介绍无线接入点 (WAP) 设备的基于 Web 的配置实用程序，具体包括以下主题：

启动基于 Web 的配置实用程序

本节介绍系统要求和如何导航基于 Web 的配置实用程序。

支持的浏览器

- Internet Explorer 7.0 或更高版本
- Chrome 5.0 或更高版本
- Firefox 3.0 或更高版本
- Safari 3.0 或更高版本

浏览器限制

- 如果使用的是 Internet Explorer 6，则无法直接使用 IPv6 地址访问 WAP 设备。但是，可以使用域名系统 (DNS) 服务器创建包含 IPv6 地址的域名，然后在地址栏中使用该域名代替 IPv6 地址。
- 如果使用的是 Internet Explorer 8，则可以从 Internet Explorer 配置安全设置。选择**工具 > Internet 选项**，然后选择**安全**选项卡。选择**本地 Intranet**，然后选择**站点**。选择**高级**，然后选择**添加**。将 WAP 设备 的 Intranet 地址 (http://*<ip-address>*) 添加到本地 Intranet 区域。也可将 IP 地址指定为子网 IP 地址，这样子网中的所有地址均会添加到本地 Intranet 区域。

- 如果管理站上有多个 IPv6 接口，则可以使用 IPv6 全局地址代替 IPv6 本地地址从浏览器访问 WAP 设备。

启动基于 Web 的配置实用程序

要打开 配置实用程序，请执行以下步骤：

步骤 1 打开 Web 浏览器。

在浏览器地址栏中输入要配置的 WAP 设备 的 IP 地址，然后按下 **Enter** 键。系统将显示*登录*页面。

- 要查找 IP 地址，可以使用 Cisco FindIT Network Discovery Utility。通过此工具，可以自动发现所有在与计算机相同的本地网段中支持的思科设备。有关详情，请转至 cisco.com 并进入 www.cisco.com/go/findit。
- 有关如何查找 WAP 设备 IP 地址的更多说明，请参阅 WAP 设备的《快速入门指南》。

步骤 2 输入用户名和密码。出厂默认用户名为 **cisco**，默认密码为 **cisco**。

步骤 3 点击 **Log In**。系统将打开 Access Point Setup Wizard 页。

如果这是首次使用默认用户名 (**cisco**) 和默认密码 (**cisco**) 登录，或者密码已过期，则会打开 *Change Admin Password* 页。输入新的密码并确认，接着点击**应用**，然后点击**关闭**。系统将保存新密码。然后，在*登录*页输入用户名 **cisco** 和新密码。

有关使用向导的说明，请参阅**使用接入点设置向导**。

注销

默认情况下，如果 配置实用程序 在 10 分钟内无活动，将会注销。有关更改默认超时时间的说明，请参阅 **HTTP/HTTPS 服务**。

要注销，请点击 配置实用程序 右上角的 **Logout**。

使用接入点设置向导

首次登录 WAP 设备（或 WAP 设备重置为出厂默认设置后），会出现 Access Point Setup Wizard 以帮助执行初始配置。请按照以下步骤完成向导：

注 如果点击**取消**跳过向导，会出现 Change Password 页。然后可以更改默认的登录密码。对于所有其他设置，应用出厂默认配置。

必须在更改密码后重新登录。

步骤 1 在向导的 Welcome 页上点击**下一步**。出现 Configure Device - IP Address 窗口。

步骤 2 如果希望 WAP 设备从 DHCP 服务器接收 IP 地址，请点击 **Dynamic IP Address (DHCP)**。或选择 **Static IP Address** 以手动配置 IP 地址。有关这些字段的说明，请参阅**虚拟局域网和 IPv4 地址设置**。

步骤 3 点击**下一步**。出现 Single Point Setup — Set a Cluster 窗口。有关单点设置的说明，请参阅**单点设置**。

步骤 4 要为 WAP 设备创建新的单点设置，请选择 **Create a New Cluster**，然后指定 **New Cluster Name**。使用相同的集群名称配置设备并在另一 WAP 设备中启用单点设置模式时，这些设备会自动加入组。

如果网络中已存在集群，可以通过点击 **Join an Existing Cluster** 将此设备添加到其中，然后输入 **Existing Cluster Name**。

如果此时不希望此设备加入单点设置，请点击 **Do not Enable Single Point Setup**。

（可选）可以在 AP Location 字段中输入文本以记录 WAP 设备的物理位置。

步骤 5 点击**下一步**。出现 Configure Device - Set System Date and Time 窗口。

步骤 6 选择所在时区，然后手动设置系统时间或设置 WAP 设备从 NTP 服务器获取时间。有关这些选项的说明，请参阅**时间设置**。

步骤 7 点击**下一步**。出现 Enable Security - Set Password 窗口。

步骤 8 输入**新密码**，然后在 **Confirm Password** 文本框中再次输入此密码。有关密码的详情，请参阅**用户帐户**。

注 如果想要禁用密码安全规则，则可以取消选中 Password Complexity 框。但是，思科强烈建议启用密码安全规则。

步骤 9 点击**下一步**。出现 Radio 1 界面的 Enable Security - Name Your Wireless Network 窗口。

步骤 10 输入 **Network Name**。此名称用作默认无线网络的 SSID。

步骤 11 点击**下一步**。出现 Enable Security - Secure Your Wireless Network 窗口。

步骤 12 选择安全加密类型并输入安全密钥。有关这些选项的说明，请参阅**系统安全**。

步骤 13 点击**下一步**。向导会显示 Enable Security - Assign the VLAN ID For Your Wireless Network 窗口。

步骤 14 为在无线网络中接收的流量输入 VLAN ID。

建议从默认设置 (1) 中为无线流量指定不同的 VLAN ID，以便将其与 VLAN 1 中的管理流量分开。

步骤 15 点击**下一步**。

对于 WAP121 设备，向导会显示 Summary - Confirm Your Settings 窗口。跳至**步骤 24**。

对于 WAP321 设备，向导会显示 Enable Captive Portal - Create Your Guest Network 窗口。

步骤 16 选择是否设置针对网络访客的身份验证方法（仅适用于 WAP321），然后点击**下一步**。

如果点击**否**，则跳至**步骤 24**。

如果点击**是**，向导会显示 Enable Captive Portal - Name Your Guest Network 窗口。

步骤 17 为 Radio 1 指定 **Guest Network Name**。

步骤 18 点击**下一步**。向导会显示 Enable Captive Portal - Secure Your Guest Network 窗口。

步骤 19 为访客网络选择安全加密类型并输入安全密钥。有关这些选项的说明，请参阅**系统安全**。

步骤 20 点击**下一步**。向导会显示 Enable Captive Portal - Assign the VLAN ID 窗口。

步骤 21 为访客网络指定 VLAN ID。访客网络 VLAN ID 应与管理 VLAN ID 不同。

步骤 22 点击**下一步**。向导会显示 Enable Captive Portal - Enable Redirect URL 窗口。

步骤 23 选择 **Enable Redirect URL**，然后在 Redirect URL 字段（包括 http://）中指定完全限定的域名或 IP 地址。如果指定，会在验证后将访客网络用户重新定向到指定的 URL。

步骤 24 点击**下一步**。向导会显示 Summary - Confirm Your Settings 窗口。

步骤 25 检查已配置的设置。点击 **Back** 以重新配置一个或多个设置。如果点击**取消**，所有设置将恢复为以前的值或默认值。

步骤 26 如果设置正确，请点击**提交**。 WAP 设置已保存并出现确认窗口。

步骤 27 点击**完成**。出现 Getting Started 窗口。

使用入门

为通过快速导航简化设备配置， Getting Started 页提供用于执行常见任务的链接。Getting Started 页是每次登录 配置实用程序 时的默认窗口。

Getting Started 页上的链接

类别	链接名称 （ 在页面上 ）	链接的页面
初始设置	Run Setup Wizard	使用接入点设置向导
	Configure Radio Settings	无线
	Configure Wireless Network Settings	网络
	Configure LAN Settings	局域网
	Run WPS	WPS 设置
	Configure Single Point Setup	单点设置
设备状态	System Summary	系统摘要
	Wireless Status	网络接口
快速访问	Change Account Password	用户帐户
	Upgrade Device Firmware	升级固件
	Backup/Restore Configuration	下载 / 备份配置文件
其他资源	支持	思科 WAP 支持站点链接。
	论坛	思科支持社区站点链接。
	无线规划工具	适用于 Cisco Small Business 的 Fluke Networks AirMagnet Planner 的链接。

窗口导航

本节介绍 配置实用程序 的功能。

配置实用程序报头

配置实用程序报头包含标准信息，显示在每页的顶端。可提供以下按钮：

按钮

按钮名称	说明
(User)	登录 WAP 设备 的用户帐户名称 （ Administrator 或 Guest ）。出厂默认用户名为 **cisco**。
Log Out	点击此按钮可注销 配置实用程序。
About	点击此按钮会显示 WAP 设备 类型和版本号。
帮助	点击此按钮会显示在线帮助。可以使用 UTF-8 编码通过浏览器查看在线帮助。如果在线帮助显示乱码，请确认浏览器中的编码设置是否设置为 UTF-8。

导航窗格

导航窗格或主菜单位于每个页面的左侧。导航窗格是 WAP 设备的顶层功能列表。如果主菜单项前面有一个箭头，选中此箭头可展开并显示每组子菜单。然后可以选中所需的子菜单项以打开关联页。

管理按钮

下表介绍了系统各页显示的常用按钮。

管理按钮

按钮名称	说明
添加	向表或数据库中添加新条目。
取消	取消对页面所做的更改。

管理按钮 （续）

按钮名称	说明
全部清除	清除日志表中的所有条目。
删除	删除表中的条目。请先选择一个条目。
编辑	编辑或修改现有条目。请先选择一个条目。
Refresh	用最新数据重新显示当前页。
保存	保存设置或配置。
Update	将新信息更新到启动配置中。

2

状态和统计信息

本章介绍如何显示状态和统计信息，具体包括以下主题：

- 系统摘要
- 网络接口
- 流量统计信息
- 工作组网桥发送 / 接收
- 关联客户端
- TSPEC 客户端关联
- TSPEC 状态和统计信息
- TSPEC AP 统计信息
- 无线统计信息
- 电子邮件警报状态
- 日志

系统摘要

System Summary 页显示基本信息，例如硬件型号说明、软件版本和自上次重新启动后的运行时间。

要查看系统信息，请在导航窗格中选择 **Status and Statistics** > **System Summary**。或在 Getting Started 页中选择 **Device Status** 下的 **System Summary**。

System Summary 页显示以下信息：

- **PID VID** - WAP 硬件型号和版本。
- **Serial Number** - 思科 WAP 设备的序列号。

- **Base MAC Address** - WAP MAC 地址。
- **Firmware Version** - 活动映像的固件版本号。
- **Firmware MD5 Checksum** - 活动映像的校验和。
- **Host Name** - 指定给设备的名称。
- **System Uptime** - 自上次重新启动后的运行时间。
- **System Time** - 当前系统时间。
- **Power Source** - 系统可以通过电源适配器供电或通过 PoE 供电端设备 (PSE) 接受以太网供电。

TCP/UDP 服务表显示有关 WAP 中所使用协议和服务的基本信息。

- **Service** - 服务名称（如果可用）。
- **Protocol** - 服务使用的底层传输协议（TCP 或 UDP）。
- **Local IP Address** - WAP 设备上连接至此服务的远程设备的 IP 地址（如果有）。**All** 表示设备中的任何 IP 地址都可以使用此服务。
- **Local Port** - 此服务的端口号。
- **Remote IP Address** - 使用此服务的远程主机的 IP 地址（如果有）。**All** 表示此服务可用于访问系统的所有远程主机。
- **Remote Port** - 任何与此服务进行通信的远程设备的端口号。
- **Connection State** - 服务的状态。对于 UDP，此表中仅显示状态为 “活动”的连接。如果处于 “活动”状态，则 WAP 设备和客户端或服务器之间已建立连接。 TCP 状态包括：
  - **Listening** - 此服务正在监听连接请求。
  - **Active** - 已建立连接会话并且正在发送和接收数据包。
  - **Established** - 根据与此协议有关的每个设备的角色，已在 WAP 设备和服务器或客户端之间建立连接会话。
  - **Time Wait** - 关闭序列已启动， WAP 在关闭连接之前等待系统定义的超时时间（通常为 60 秒）。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

网络接口

使用 Network Interfaces 页显示有关有线和无线接口的配置和状态信息。要显示 Network Interfaces 页，请在导航窗格中选择 **Status and Statistics** > **Network Interface**。

Network Interfaces 页显示以下信息：

- **LAN Status** - 这些设置适用于内部接口。对于 WAP321，此信息用于指示是否启用 Green Ethernet 模式。

  要更改上述任一设置，请点击**编辑**链接。点击 “编辑”之后，重新定向至 VLAN and IPv4 Address Settings 页。有关这些字段的说明，请参阅**虚拟局域网和 IPv4 地址设置**。

- **Radio Status** - 这些设置包含 Wireless Radio 模式（Enabled 或 Disabled）、与无线接口关联的 MAC 地址、 802.11 模式 (a/b/g/n) 以及此接口使用的信道。

  要更改无线设置，请点击**编辑**链接。点击 “编辑”之后，重新定向至 Radio 页。有关这些字段的说明，请参阅**无线**。

- **Interface Status** - 此表列出每个虚拟接入点 (VAP) 和每个无线分布式系统 (WDS) 接口的状态信息。

  如果已配置 VAP，此表会列出 SSID（服务集标识符）、管理状态（Up 或 Down）、无线接口的 MAC 地址、 VLAN ID、任何关联调度程序简档的名称以及当前状态（活动或不活动）。状态用于指示 VAP 是否与客户端交换数据。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

流量统计信息

使用 Traffic Statistics 页查看有关 WAP 的基本信息。它还可以实时显示以太网接口、VAP 和任何 WDS 接口的发送和接收统计信息。所有的发送和接收统计信息反映自 WAP 上次启动后的收发总数。如果重新启动 WAP，这些数字表示自重新启动后的收发总数。

要显示 Traffic Statistics 页，请在导航窗格中选择 **Status and Statistics** > **Traffic Statistics**。

Traffic Statistics 页显示各方向流量的汇总数据和统计信息。

- **Network Interface** - 以太网接口以及各 VAP 和 WDS 接口的名称。

  每个 VAP 接口名称均后跟 SSID（用括号括起）。

- **Total Packets** - 此 WAP 设备发送（在发送表中）或接收（在接收表中）的数据包的总数。
- **Total Bytes** - 此 WAP 设备发送（在发送表中）或接收（在接收表中）的字节的总数。
- **Total Dropped Packets** - 此 WAP 设备发送（在发送表中）或接收（在接收表中）的已丢弃数据包的总数。
- **Total Dropped Bytes** - 此 WAP 设备发送（在发送表中）或接收（在接收表中）的已丢弃字节的总数。
- **Errors** - 与此 WAP 设备中发送和接收数据相关的错误的总数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

工作组网桥发送 / 接收

WorkGroup Bridge Transmit/Receive 页显示工作组网桥中工作站之间的数据包和流量字节数。有关配置工作组网桥的详情，请参阅**工作组网桥**。

要显示 WorkGroup Bridge Transmit/Receive 页，请在导航窗格中选择 **Status and Statistics** > **WorkGroup Bridge**。

配置为工作组网桥接口的每个网络接口显示以下字段：

- **Network Interface** - 以太网或 VAP 接口的名称。
- **Status and Statistics** - 是断开接口还是管理性地将其配置为 Up 或 Down。
- **VLAN ID** - 虚拟局域网 (VLAN) ID。可以使用虚拟局域网在同一 WAP 设备上建立多个内部和访客网络。 VLAN ID 是在 VAP 选项卡上设置的。请参阅**配置 VAP**。
- **Name (SSID)** - 无线网络名称。此字母数字密钥还称为 SSID，可以唯一标识无线局域网。 SSID 是在 VAP 选项卡上设置的。请参阅**配置 VAP**。

针对每个工作组网桥接口，显示发送和接收方向的更多信息：

- **Total Packets** - 工作组网桥中的有线客户端与无线网络之间桥接的数据包总数。
- **Total Bytes** - 工作组网桥中的有线客户端与无线网络之间桥接的字节总数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

关联客户端

可以使用 Associated Clients 页查看与特定接入点关联的客户端工作站。

要显示 Associated Clients 页，请在导航窗格中选择 **Status and Statistics** > **Associated Clients**。

显示关联的工作站以及有关每个工作站发送和接收的数据包流量的信息。

- **Total Number of Associated Clients** - 当前与 WAP 设备 关联的客户端总数。
- **Network Interface** - 与客户端关联的 VAP。
- **Station** - 关联无线客户端的 MAC 地址。
- **Status** - Authenticated and Associated Status 页显示底层 IEEE 802.11 身份验证和关联状态，无论客户端使用哪种安全类型连接 WAP 设备，都会显示此状态。此状态不显示 IEEE 802.1X 身份验证或关联状态。

  需要注意与此字段相关的以下几个要点：

  - 如果 WAP 设备安全模式为 None 或 Static WEP，将如期出现客户端的身份验证和关联状态；即如果客户端显示为已通过 WAP 设备的身份验证，则可以发送和接收数据。（这是因为 Static WEP 仅使用 IEEE 802.11 身份验证。）
  - 如果 WAP 设备使用 IEEE 802.1X 或 WPA 安全，即使客户端关联实际上没有通过第二层安全性进行身份验证，可能也会显示为已验证（通过 IEEE 802.11 安全）。
- **From Station/To Station** - 对于 From Station，计数器可指示无线客户端接收的数据包数或字节数。对于 To Station，计数器可指示从 WAP 设备发送到无线客户端的数据包数和字节数。
  - **Packets** - 从无线客户端接收（发送）的数据包数。
  - **Bytes** - 从无线客户端接收（发送）的字节数。
  - **Drop Packets** - 接收（发送）后已丢弃的数据包数。
  - **Drop Bytes** - 接收（发送）后已丢弃的字节数。
  - **TS Violate Packets (From Station)** - 从客户端 STA 发送到 WAP 设备的超过其活动流量流 (TS) 上行链路带宽的数据包数，或要求对尚未允许进入的客户端 STA 执行准入控制的接入类别的数据包数。
  - **TS Violate Packets (To Station)** - 从 WAP 设备发送到客户端 STA 的超过其活动 TS 下行链路带宽的数据包数，或要求对尚未允许进入的客户端 STA 执行准入控制的接入类别的数据包数。

- **Up Time** - 客户端已与 WAP 设备关联的时间长度。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

TSPEC 客户端关联

TSPEC Client Associations 页提供有关此接入点发送和接收的 TSPEC 客户端数据的实时信息。TSPEC Client Associations 页中的表格会显示自关联启动后发送和接收的语音与视频数据包以及状态信息。

TSPEC 是从支持 QoS 的无线客户端发送到 WAP 设备的流量规范，需要对其代表的通信流 (TS) 进行一定量的网络访问。流量流是无线客户端识别的数据包集合，属于特定用户优先级。语音流量流的一个例子是 Wi-Fi CERTIFIED 电话听筒，可将其编解码器生成的数据包标记为语音优先流量。视频流量流的一个例子是无线笔记本电脑上的视频播放器应用程序，可优先进行从企业服务器馈送的视频会议。

要查看 TSPEC 客户端关联统计信息，请在导航窗格中选择 **Status and Statistics > TSPEC Client Associations**。

TSPEC Client Associations 页显示以下信息：

状态和统计信息：

- **Network Interface** - 客户端使用的无线接口。
- **SSID** - 与此 TS 客户端关联的服务集标识符。
- **Station** - 客户端工作站 MAC 地址。
- **TS Identifier** - TSPEC 流量会话标识符（范围介于 0 至 7 之间）。
- **Access Category** - TS 接入类别（语音或视频）。
- **Direction** - 此 TS 的流量方向。方向可以是以下选项之一：
  - 上行链路 - 从客户端到设备。
  - 下行链路 - 从设备到客户端。
  - 双向
- **User Priority** - 此 TS 的用户优先级 (UP)。UP 是在 IP 报头的 UP 部分中随每个数据包一起发送的。典型值如下所示：
  - 对于语音，为 6 或 7
  - 对于视频，为 4 或 5

值可能随其他优先流量会话而异。

- **Medium Time** - TS 流量占用传输媒体的时间。
- **Excess Usage Events** - 客户端超过为其 TSPEC 确定的媒体时间的次数。忽略少有的轻度违反情况。
- **VAP MAC Address** - 虚拟接入点 MAC 地址。

统计信息：

- **Network Interface** - 客户端使用的无线接口。
- **Station** - 客户端工作站 MAC 地址。
- **TS Identifier** - TSPEC 流量会话标识符（范围介于 0 至 7 之间）。
- **Access Category** - TS 接入类别（语音或视频）。
- **Direction** - 此 TS 的流量方向。方向可以是以下选项之一：
  - 上行链路 - 从客户端到设备。
  - 下行链路 - 从设备到客户端。
  - 双向
- **From Station** - 显示从无线客户端接收的数据包数和字节数以及接收后已丢弃的数据包数和字节数。
  - **Packets** - 超过允许 TSPEC 的数据包数。
  - **Bytes** - 尚未建立 TSPEC 并且 WAP 设备要求准入时的字节数。
- **To Station** - 从 WAP 设备发送到无线客户端的数据包数和字节数以及发送时已丢弃的数据包数和字节数。
  - **Packets** - 超过允许 TSPEC 的数据包数。
  - **Bytes** - WAP 设备要求准入时尚未建立 TSPEC 的字节数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

TSPEC 状态和统计信息

TSPEC Status and Statistics 页提供以下信息：

- 按无线列出的有关 TSPEC 会话的摘要信息。
- 按 VAP 列出的有关 TSPEC 会话的摘要信息。
- 无线接口和网络接口的实时发送和接收统计信息。

显示的所有传输和接收统计信息是自 WAP 设备上次启动后的收发总数。如果重新启动 WAP 设备，这些数字可指示自重新启动后的发送和接收总数。

要查看 TSPEC 状态和统计信息，请在导航窗格中选择 **Status and Statistics > TSPEC Status and Statistics**。

TSPEC Status and Statistics 页提供以下无线局域网 (Radio) 和 VAP 接口的状态信息：

- **Network Interface** - 无线或 VAP 接口的名称。
- **Access Category** - 与此流量流（语音或视频）关联的当前接入类别。
- **Status** - 是启用 (Up) 还是禁用 (Down) 相应接入类别的 TSPEC 会话。

  注 状态是配置状态（并不一定代表当前的会话活动）。
- **Active Traffic Stream** - 此无线和接入类别的当前活动的 TSPEC 流量流数。
- **Traffic Stream Clients** - 与此无线和接入类别关联的流量流客户端数。
- **Medium Time Admitted** - 为此接入类别通过传输媒体传输数据分配的时间。此值应小于或等于允许此 TS 通过媒体使用的最大带宽。
- **Medium Time Unallocated** - 此接入类别未使用带宽的时间。

单独针对无线功能接口中的发送和接收通道，显示以下统计信息：

- **Access Category** - 与此流量流（语音或视频）关联的接入类别。
- **Total Packets** - 此无线发送（在发送表中）或接收（在接收表中）的指定接入类别的 TS 数据包总数。
- **Total Bytes** - 指定接入类别接收的字节总数。

单独针对网络接口 (VAP) 中的发送和接收通道，显示以下统计信息：

- **Total Voice Packets** - 此 WAP 设备为此 VAP 发送（在发送表中）或接收（在接收表中）的 TS 语音数据包总数。

- **Total Voice Bytes** - 此 WAP 设备为此 VAP 发送（在发送表中）或接收（在接收表中）的 TS 语音字节总数。
- **Total Video Packets** - 此 WAP 设备为此 VAP 发送（在发送表中）或接收（在接收表中）的 TS 视频数据包总数。
- **Total Video Bytes** - 此 WAP 设备为此 VAP 发送（在发送表中）或接收（在接收表中）的 TS 视频字节总数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

TSPEC AP 统计信息

TSPEC AP Statistics 页提供有关 WAP 设备接受和拒绝的语音与视频流量流的信息。要查看 TSPEC AP Statistics 页，请在导航窗格中选择 **Status and Statistics > TSPEC AP Statistics**。

- **TSPEC Statistics Summary for Voice ACM** - 接受和拒绝的语音流量流总数。
- **TSPEC Statistics Summary for Video ACM** - 接受和拒绝的视频流量流总数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

无线统计信息

可以使用 Radio Statistics 页显示无线功能接口的数据包级和字节级统计信息。要查看 Radio Statistics 页，请在导航窗格中选择 **Status and Statistics > Radio Statistics**。

- **Packets Received** - WAP 设备接收的数据包总数。
- **Packets Transmitted** - WAP 设备发送的数据包总数。
- **Bytes Received** - WAP 设备接收的字节总数。
- **Bytes Transmitted** - WAP 设备发送的字节总数。
- **Packets Receive Dropped** - WAP 设备接收但已丢弃的数据包数。
- **Packets Transmit Dropped** - WAP 设备发送但已丢弃的数据包数。
- **Bytes Receive Dropped** - WAP 设备接收但已丢弃的字节数。
- **Bytes Transmit Dropped** - WAP 设备发送但已丢弃的字节数。

- **Fragments Received** - WAP 设备接收的分片帧数。
- **Fragments Transmitted** - WAP 设备发送的分片帧数。
- **Multicast Frames Received** - 通过目标 MAC 地址中设置的多播位接收的 MSDU（MAC 服务数据单元）帧数。
- **Multicast Frames Transmitted** - 在目标 MAC 地址中设置多播位的情况下成功发送的 MSDU 帧数。
- **Duplicate Frame Count** - 接收帧并且 Sequence Control 字段指示它为重复帧的次数。
- **Failed Transmit Count** - 由于发送尝试超过短重试次数限制或长重试次数限制，导致 MSDU 发送失败的次数。
- **FCS Error Count** - 在接收的 MPDU 帧中检测到的 FCS（帧检查顺序）错误数。
- **Transmit Retry Count** - 一次或多次重试后成功发送 MSDU 的次数。
- **ACK Failure Count** - 没有如期接收到的 ACK 帧数。
- **RTS Failure Count** - 没有接收到响应 RTS 帧的 CTS 帧数。
- **WEP Undecryptable Count** - 由于无线无法解密而丢弃的帧数。由于帧无法解密或是通过 WAP 设备不支持的隐私选项加密的，可以将此类帧丢弃。
- **RTS Success Count** - 接收到的响应 RTS 帧的 CTS 帧数。
- **Multiple Retry Count** - 多次重试后成功发送 MSDU 的次数。
- **Frames Transmitted Count** - 一次成功发送 MSDU 的次数。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

电子邮件警报状态

Email Alert Status 页提供有关根据 WAP 设备中生成的系统日志消息发送的电子邮件警报的信息。要查看 Email Alert Status 页，请在导航窗格中选择 **Status and Statistics > Email Alert Status**。

- **Email Alert Status** - 已配置的电子邮件警报状态。状态为 Enabled 或 Disabled。默认值为 Disabled。
- **Number of Emails Sent** - 已发送的电子邮件总数。范围是 32 位的无符号整数。默认值为 0。

- **Number of Emails Failed** - 发送失败的电子邮件总数。范围是 32 位的无符号整数。默认值为 0。
- **Time Last Email Sent** - 发送上一封电子邮件的星期、日期和时间。

日志

Log 页显示生成日志条目的系统事件列表，例如登录尝试次数和配置更改。系统会在重新启动时清除日志，也可以由管理员清除日志。最多可以显示 512 个事件。根据需要从列表中删除较早的条目，为新事件释放空间。

要查看 Log 页，请在导航窗格中选择 **Status and Statistics > Log Status**。

- **Time Stamp** - 事件发生时的系统时间。
- **Severity** - 事件是由错误 (err) 引起的还是用于提供信息 (info)。
- **Service** - 与事件关联的软件组件。
- **Description** - 事件说明。

可以点击 **Refresh** 刷新屏幕并显示最新信息。

用户可以点击**全部清除**以清除日志中的所有条目。

3

管理

本章介绍如何配置全局系统设置和执行诊断。

具体包括以下主题：

- 系统设置
- 用户帐户
- 时间设置
- 日志设置
- 电子邮件警报
- HTTP/HTTPS 服务
- 管理访问控制
- 升级固件
- 固件恢复
- 下载 / 备份配置文件
- 配置文件属性
- 复制 / 保存配置
- 重新启动
- 发现 - Bonjour
- 数据包捕获
- 支持信息

系统设置

通过 System Settings 页，可以配置用于识别网络内 WAP 设备的信息。

要配置系统设置，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **System Settings**。

步骤 2 输入以下参数：

- **Host Name** - 对此 WAP 设备人为分配的名称。按照惯例，此名称是节点的完全限定的域名。默认主机名由 **wap** 与 WAP 设备 MAC 地址的最后 6 位十六进制数字连接组成。Host Name 标签只能包含字母、数字和连字符。Host Name 标签不能以连字符开头或结尾。不允许使用其他符号、标点字符或空格。 Host Name 可以包含 1 到 63 个字符。
- **System Contact** - WAP 设备的联系人。System Contact 可以包含 0 到 255 个字符，可以包含空格和特殊字符。
- **System Location** - 有关 WAP 设备物理位置的说明。System Location 可以包含 0 到 255 个字符，可以包含空格和特殊字符。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

用户帐户

默认情况下， WAP 设备中配置了一个管理用户：

- 用户名：**cisco**
- Password:**cisco**

User Accounts 页可用来配置最多 4 个其他用户和更改用户密码。

添加用户

要添加新用户，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **User Accounts**。

User Account Table 显示当前配置的用户。用户 **cisco** 是在系统中预先配置的，具有读 / 写权限。

所有其他用户可以拥有只读访问权限，但没有读 / 写访问权限。

步骤 2 点击**添加**。文本框中会出现新行。

步骤 3 选中新用户对应的框，然后选择**编辑**。

步骤 4 输入一个介于 1 至 32 个字母数字字符之间的 **User Name**。用户名仅允许使用数字 0 到 9 和字母 a 到 z（大写或小写）。

步骤 5 输入一个介于 1 至 64 个字符之间的 **New Password** ，然后在 **Confirm New Password** 文本框中输入同一密码。

输入密码时，竖条的数量和颜色会发生变化，可用来指示密码强度，如下所示：

- 红色 - 密码不满足最低复杂性要求。
- 橙色 - 密码能够满足最低复杂性要求，但是密码强度较弱。
- 绿色 - 密码较强。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

注 要删除用户，请选中用户名旁边的复选框，然后选择**删除**。要永久保存删除内容，请在完成后选择**保存**。

更改用户密码

要更改用户密码，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **User Accounts**。

User Account Table 显示当前配置的用户。用户 **cisco** 是在系统中预先配置的，具有读 / 写权限。用户 **cisco** 的密码可以更改。

步骤 2 选择要配置的用户，然后点击**编辑**。

步骤 3 输入一个介于 1 至 64 个字符之间的 **New Password** ，然后在 **Confirm New Password** 文本框中输入同一密码。

输入密码时，竖条的数量和颜色会发生变化，可用来指示密码强度，如下所示：

- 红色 - 密码不满足最低复杂性要求。
- 橙色 - 密码能够满足最低复杂性要求，但是密码强度较弱。
- 绿色 - 密码较强。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

注 如果更改密码，必须重新登录系统。

时间设置

系统时钟可以为软件事件（例如消息日志）提供网络同步的时间戳服务。可以手动配置系统时钟，也可以将 WAP 设备配置为从服务器获取时钟数据的网络时间协议 (NTP) 客户端。

使用 Time Settings 页手动设置系统时间，或者将系统配置为从预先配置的 NTP 服务器获取其时间设置。默认情况下，将 WAP 设备 配置为从预定义的 NTP 服务器列表获取其时间。

页面顶端会显示当前的系统时间与 System Clock Source 选项。

要利用 NTP 使 WAP 设备自动获取其时间设置，请执行以下步骤：

步骤 1 对于 System Clock Source 字段，选择 **Network Time Protocol (NTP)**。

步骤 2 配置以下参数：

- **NTP Server/IPv4/IPv6 Address Name** - 指定 NTP 服务器的 IPv4 地址、IPv6 地址或主机名。会列出默认的 NTP 服务器。

  主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点系列不能超过 253 个字符。

- **Time Zone** - 选择所在位置的时区。

步骤 3 如果夏令时适用于所在时区，请选择 **Adjust Time for Daylight Savings**。选择之后，请配置以下字段：

- **Daylight Savings Start** - 选择夏令时开始的星期、日、月和时间。
- **Daylight Savings End** - 选择夏令时结束的星期、日、月和时间。
- **Daylight Savings Offset** - 指定夏令时开始前时钟拨快和结束后时钟拨回的分钟数。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

要手动配置时间设置，请执行以下步骤：

步骤 1 对于 System Clock Source 字段，选择 **Manually**。

步骤 2 配置以下参数：

- **System Date** - 从下拉列表中选择当前月、日和年。
- **System Time** - 选择 24 小时制时钟格式的当前小时和分钟，例如 22:00:00 表示晚上 10 点。
- **Time Zone** - 选择所在位置的时区。

步骤 3 如果夏令时适用于所在时区，请选择 **Adjust Time for Daylight Savings**。选择之后，请配置以下字段：

- **Daylight Savings Start** - 选择夏令时开始的星期、日、月和时间。
- **Daylight Savings End** - 选择夏令时结束的星期、日、月和时间。
- **Daylight Savings Offset** - 指定夏令时开始前时钟拨快和结束后时钟拨回的分钟数。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

日志设置

可以使用 Log Settings 页将日志消息保存在永久性存储器中。还可以将日志发送到远程主机。

配置永久日志

如果系统意外重新启动，日志消息可用于诊断原因。但在系统重新启动时会擦除日志消息，除非启用永久日志记录。

注意 启用永久日志记录会耗尽闪存（非易失性存储器），降低网络性能。仅在调试问题时启用永久记录。确保完成问题调试之后禁用永久日志记录。

要配置永久日志记录，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Log Settings**。

步骤 2 配置以下参数：

- **Persistence** - 点击 **Enable** 将系统日志保存到非易失性存储器，以便在 WAP 设备重新启动时保留日志。最多可以在非易失性存储器中保存 128 条日志消息。达到 128 条的限制时，最新的日志消息会覆盖最早的日志消息。清除此字段可将系统日志保存到易失性存储器。系统重新启动时会删除易失性存储器中的日志。
- **Severity** - 事件写入非易失性存储器中的日志时必须具有的最低严重性级别。例如，如果指定 2（关键），则将关键、警报和紧急级别的事件记录到非易失性存储器。而将严重性级别为 3 到 7 的错误消息写入易失性存储器。
- **Depth** - 可以存储在易失性存储器中的最大消息数（最多为 512 条）。达到在此字段中配置的数量时，最新的日志事件会覆盖最早的日志事件。请注意，可以存储在非易失性存储器（永久日志）中的最大日志消息数是 128，该数是不可配置的。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

远程日志服务器

内核日志是一个全面的系统事件（显示在 System Log 中）和内核消息（例如错误条件）列表。

无法直接从 Web 界面查看内核日志消息。必须先设置远程日志服务器才能接收和捕获日志。然后可以配置 WAP 设备以登录远程日志服务器。

WAP 设备系统日志消息的远程日志服务器集合提供以下功能：

- 允许从多个 AP（接入点）聚合系统日志消息
- 可存储的消息历史记录要长于单个 WAP 设备
- 触发脚本管理操作和警报

要指定网络中的主机作为远程日志服务器，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Log Settings**。

步骤 2 配置以下参数：

- **Remote Log** - 使 WAP 设备 将日志消息发送到远程主机。如果禁用此参数，所有的日志消息都将保留在本地系统中。
- **Server IPv4/IPv6 Address/Name** - 远程日志服务器的 IPv4 地址、IPv6 地址或主机名。

  主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点系列不能超过 253 个字符。
- **UDP Port** - 远程主机上系统日志进程的逻辑端口号。范围介于 1 至 65535 之间，默认端口号为 514。

  建议使用默认端口。如果选择重新配置日志端口，确保指定给系统日志的端口号可供使用。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

如果已启用 Remote Log 主机，点击**保存**可激活远程日志记录。WAP 设备可将用于显示的内核消息实时发送到远程日志服务器监控器、指定的内核日志文件或其他存储器，具体取决于所做的配置。

如果已禁用 Remote Log 主机，点击**保存**可禁用远程日志记录。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

电子邮件警报

通过电子邮件警报功能，可以在发生特殊系统事件时将消息发送到已配置的电子邮件地址。

此功能支持邮件服务器配置、消息严重性配置以及最多 3 个用于发送紧急和非紧急电子邮件警报的电子邮件地址配置。

提示 不要使用个人电子邮件地址，以免不必要地暴露个人电子邮件登录凭据。改用单独的电子邮件帐户。还要注意，许多电子邮件帐户默认保留所有已发送邮件的副本。具有此类电子邮件帐户访问权限的任何人都能访问已发送邮件。检查电子邮件设置，确保其符合企业的隐私策略。

要配置 WAP 设备 以发送电子邮件警报，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Email Alert**。

步骤 2 在 Global Configuration 区域中配置以下参数：

- **Administrative Mode** - 选择全局启用电子邮件警报功能。
- **From Email Address** - 输入显示为电子邮件发件人的地址。此地址是一个包含 255 个字符的字符串，仅能使用可打印字符。默认情况下，不配置任何地址。
- **Log Duration** - 选择发送预定消息的频率。范围介于 30 至 1440 分钟之间。默认值为 30 分钟。
- **Scheduled Message Severity** - 将此严重性级别或更高级别的日志消息组合在一起，并按 Log Duration 指定的频率发送到已配置的电子邮件地址。从以下值中进行选择：None、 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Info 和 Debug。如果设置为 None，则不发送任何预定严重性级别的消息。默认严重性级别为 Warning。
- **Urgent Message Severity** - 将此严重性级别或更高级别的日志消息立即发送到已配置的电子邮件地址。从以下值中进行选择：None、 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Info 和 Debug。如果设置为 None，则不发送任何紧急严重性级别的消息。默认值为 Alert。

步骤 3 在 Mail Server Configuration 区域中配置以下参数：

- **Server IPv4 Address/Name** - 输入发送 SMTP （简单电子邮件传输协议）服务器的 IP 地址或主机名。（可以和电子邮件提供商核对此主机名。）服务器地址必须是有效的 IPv4 地址或主机名。IPv4 地址应采用类似于 xxx.xxx.xxx.xxx (192.0.2.10) 的格式。

主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点系列不能超过 253 个字符。

- **Data Encryption** - 输入出站电子邮件警报的安全模式。可以使用安全 TLS（传输层安全性）协议或默认开放式协议发送警报。使用安全 TLSv1 协议可以防止在公用网络上的通信过程中遭受窃听和篡改。
- **Port** - 输入用于出站电子邮件的 SMTP 端口号。范围是介于 0 至 65535 之间的有效端口号，默认端口号为 465。此端口通常取决于电子邮件提供商使用的模式。
- **Username** - 输入将用于发送这些电子邮件的电子邮件帐户用户名。通常（但并非总是），用户名是包含域（例如 Name@example.com）的完整电子邮件地址。指定帐户将用作发件人的电子邮件地址。用户名可以包含 1 至 64 个字母数字字符。
- **Password** - 输入将用于发送这些电子邮件的电子邮件帐户密码。密码可以包含 1 至 64 个字符。

步骤 4 配置电子邮件地址和主题行。

- **To Email Address 1/2/3** - 最多可输入 3 个用于接收电子邮件警报的地址。每个电子邮件地址都必须有效。
- **Email Subject** - 输入显示在电子邮件主题行中的文本。主题是最多可以包含 255 个字符的字母数字字符串。

步骤 5 点击 **Test Mail** 发送测试电子邮件以验证配置的电子邮件帐户。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

电子邮件警报示例

以下示例显示如何填写 Mail Server Configuration 参数：

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommends the following settings:
```

```
Data Encryption:TLSv1
SMTP Server:smtp.live.com
SMTP Port:587
Username:Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password:Your Windows Live account password

Yahoo!Mail
Yahoo requires using a paid account for this type of service.Yahoo recommends
the following settings:
Data Encryption:TLSv1
SMTP Server:plus.smtp.mail.yahoo.com
SMTP Port:465 or 587
Username:Your email address, without the domain name such as myName (without
@yahoo.com)
Password:Your Yahoo account password
```

以下示例显示常规日志电子邮件的样例格式：

```
From:AP-192.168.2.10@mailserver.com
Sent:Wednesday, September 09, 2009 11:16 AM
To:administrator@mailserver.com
Subject:log message from AP

TIME           PriorityProcess Id          Message
Sep 8 03:48:25 info    login[1457]         root login on ttyp0
Sep 8 03:48:26 info    mini_http-ssl[1175] Max concurrent connections of 20
reached
```

HTTP/HTTPS 服务

使用 HTTP/HTTPS Service 页启用和配置基于 Web 的管理连接。如果对安全管理会话使用 HTTPS（安全超文本传输协议），还可以使用 HTTP/HTTPS Service 页管理所需的 SSL（安全套接字层）证书。

配置 HTTP 和 HTTPS 服务

要配置 HTTP 和 HTTPS 服务，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **HTTP/HTTPS Service**。

步骤 2 配置以下全局设置：

- **Maximum Sessions** - 可以同时使用的 Web 会话数量，包含 HTTP（超文本传输协议）和 HTTPS（安全超文本传输协议）。

用户登录 WAP 设备配置实用程序时，系统即创建一个会话。在用户注销或会话超时过期之前一直保留此会话。范围介于 1 至 10 个会话之间，默认值为 5。如果达到最大会话数量，下一位尝试登录配置实用程序的用户将收到有关会话限制的错误消息。

- **Session Timeout** - 非活动用户保持登录 WAP 设备配置实用程序状态的最长时间（分钟）。达到配置的超时时间时，自动注销用户。范围介于 1 至 60 分钟之间，默认值为 10 分钟。

步骤 3 配置 HTTP 和 HTTPS 服务：

- **HTTP Server** - 启用通过 HTTP 的访问。默认情况下，启用 HTTP 访问。如果禁用，使用此协议的任何当前连接将断开。
- **HTTP Port** - 用于 HTTP 连接的逻辑端口号，介于 1025 至 65535 之间。HTTP 连接的默认端口号是众所周知的 IANA（互联网编号分配机构）端口号 80。
- **HTTPS Server** - 启用通过安全 HTTP 的访问。默认情况下，启用 HTTPS 访问。如果禁用，使用此协议的任何当前连接将断开。
- **HTTPS Port** - 用于 HTTP 连接的逻辑端口号，介于 1025 至 65535 之间。HTTP 连接的默认端口号是众所周知的 IANA 端口号 443。
- **Redirect HTTP to HTTPS** - 将 HTTP 端口的管理 HTTP 访问尝试重新定向至 HTTPS 端口。此字段仅在禁用 HTTP 访问时可用。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

管理 SSL 证书

要使用 HTTPS 服务， WAP 设备必须具有有效的 SSL 证书。 WAP 设备可以生成证书，也可以从网络或 TFTP（普通文件传输协议）服务器下载证书。

要通过 WAP 设备生成证书，请点击 **Generate SSL Certificate**。此操作应在 WAP 设备 获取 IP 地址后完成，这样可以确保证书的公用名与 WAP 设备 的 IP 地址匹配。通过生成新的 SSL 证书可以重新启动安全 Web 服务器。在浏览器接受新证书之前，安全连接无法正常工作。

在 Certificate File Status 区域中，可以查看 WAP 设备上当前是否存在证书以及以下相关信息：

- Certificate File Present
- Certificate Expiration Date
- Certificate Issuer Common Name

如果 WAP 设备上存在 SSL 证书（带有 .pem 扩展名），可以将其下载到计算机上作为备份。在 Download SSL Certificate (From Device to PC) 区域中，对于 **Download Method** 选择 **HTTP** 或 **TFTP**，然后点击 **Download**。

- 如果选择 HTTP，系统会提示确认下载，然后浏览在网络中保存此文件的位置。
- 如果选择 TFTP，则出现其他字段，要求输入指定给已下载文件的文件名和下载文件的 TFTP 服务器地址。

还可以将证书文件（带有 .pem 扩展名）从计算机上载到 WAP 设备。在 Upload SSL Certificate (From PC to Device) 区域中，对于 **Upload Method** 选择 **HTTP** 或 **TFTP**。

- 对于 HTTP，浏览网络位置，选择文件，然后点击 **Upload**。
- 对于 TFTP，输入与 TFTP 服务器上相同的 **File Name** 和 **TFTP Server IPv4 Address**，然后点击 **Upload**。文件名不能包含以下字符：空格、<、>、|、\、:、(、)、&、;、#、?、* 和两个或更多的连续句点。

上载成功时会出现确认消息。

管理访问控制

可以创建访问控制列表 (ACL)，最多可列出 5 个 IPv4 主机和 5 个 IPv6 主机，经授权它们可以访问 WAP 设备配置实用程序。如果禁用此功能，任何人通过提供正确的 WAP 设备用户名和密码，都可以从任一网络客户端访问配置实用程序。

如果启用管理 ACL，仅允许通过 Web 和 SNMP（简单网管协议）访问指定的 IP 主机。

注意 验证输入的任何 IP 地址。如果输入的 IP 地址与管理计算机不匹配，将失去对配置接口的访问权限。强烈建议为管理计算机指定静态 IP 地址，这样地址就不会随着时间而改变。

要创建访问列表，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Management Access Control**。

步骤 2 对于 **Management ACL Mode** 选择 **Enable**。

步骤 3 最多输入允许访问的 5 个 IPv4 地址和 5 个 IPv6 地址。

步骤 4 验证 IP 地址是否正确。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

升级固件

当新版本的 WAP 设备固件可用时，可以升级设备上的固件以充分利用新功能和增强功能。 WAP 设备 使用 TFTP 或 HTTP 客户端升级固件。

上载新固件并且系统重新启动后，新添加的固件将成为主映像。如果升级失败，原始固件仍用作主映像。

注 升级固件时，接入点保留现有的配置信息。

TFTP 升级

要使用 TFTP 升级接入点的固件，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Update Firmware**。

会出现产品 ID (PID) 以及活动和非活动固件版本。

步骤 2 选择 **TFTP for Transfer Method**。

步骤 3 在 **Source File Name** 字段中输入映像文件的名称（ 1 至 256 个字符 ），包括要上载映像所在目录的路径。

例如，要上载位于 /share/builds/ap 目录下的 ap_upgrade.tar 映像，请输入：*/share/builds/ap/ap_upgrade.tar*

提供的固件升级文件必须是 tar 文件。不要尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不起作用。

文件名不能包含以下字符：空格、<、>、|、\、:、(、)、&、;、#、?、* 和两个或更多的连续句点。

步骤 4 输入 **TFTP Server IPv4 Address**，然后点击 **Upgrade**。

上载新软件可能需要数分钟。上载新软件或中止软件上载时，不要刷新页面或导航至其他页。此过程完成后，接入点重新启动并恢复正常运行。

步骤 5 要验证固件升级是否成功完成，请登录用户界面，显示 Upgrade Firmware 页，然后查看活动的固件版本。

HTTP 升级

要使用 HTTP 进行升级，请执行以下步骤：

步骤 1 选择 **HTTP for Transfer Method**。

步骤 2 如果知道新文件的名称和路径，请在 **Source File Name** 字段中将其输入。否则点击 **Browse** 按钮以查找网络中的固件映像文件。

提供的固件升级文件必须是 tar 文件。不要尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不起作用。

步骤 3 点击 **Upgrade** 以应用新的固件映像。

上载新软件可能需要数分钟。上载新软件或中止软件上载时，不要刷新页面或导航至其他页。此过程完成后，接入点重新启动并恢复正常运行。

步骤 4 要验证固件升级是否成功完成，请登录用户界面，显示 Upgrade Firmware 页，然后查看活动的固件版本。

固件恢复

WAP 设备 具有固件恢复功能，可在映像下载失败之后还原 WAP 设备 的有效映像。如果在映像下载过程中电源中断， WAP 设备 可能无法启动。在此情况下，尽管映像无法使用，但可将固件映像从闪存载入 RAM 的启动加载器文件仍能继续工作。HTTP 服务器嵌入在启动加载器文件中，使管理员能够通过局域网端口连接到 WAP 设备，并使用 Web 浏览器来下载和安装新的固件映像。

WAP 设备 启动之后，如果启动加载器无法在闪存中找到有效映像，则 WAP 设备将进入 HTTP 固件恢复模式。在此模式下，启动加载器会将内部网络端口设置为以下静态 IP 地址：

- IP 地址：192.168.1.254

- 网络掩码：255.255.255.0
- 默认网关：192.168.1.1

HTTP 服务器启动并侦听端口 80 上的客户端连接。

注 仅在映像需要恢复时，基于 Web 的配置实用程序中会显示 Firmware Recovery 页。

要使用此功能下载新固件映像，请执行以下步骤：

步骤 1 直接将 PC 连接到局域网端口。

步骤 2 将管理 PC 上的 IP 地址和掩码配置为与交换机处于同一子网中。

注 如果默认网关 IP 地址为 192.168.1.1，则可以通过网络访问系统。

步骤 3 打开 Web 浏览器并在地址栏中输入交换机的 IP 地址 (192.168.1.254)。

注 HTTP 固件恢复功能支持以下浏览器：

- Firefox 3.0 及更高版本
- Internet Explorer 6 及更高版本

会显示 Firmware Recovery 页。无需身份验证。

网页中将显示 PIC VID（产品 ID 和供应商 ID）、序列号以及 WAP 设备 的 MAC 地址。

步骤 4 选择 **Browse**，然后选择一个有效的固件映像进行下载。

在下载文件时将显示一个进度条。下载成功之后将显示以下消息：

100% Complete
File downloaded successfully.Please wait while the file is being written to flash. System will automatically reboot.

管理员选择的文件已下载到 RAM，并已验证文件是否满足以下条件：

- 文件的 CRC 良好。
- 为此平台构建了 STK 文件。
- STK 文件大小在分区限制范围之内（为此文件保留了 4.5 MB 的空间）。

如果满足这些条件，此文件将写入闪存，并且系统会使用新固件重新启动。

如果未通过其中任一检查，则映像无法写入闪存，并且恢复过程将会停止。用户可以使用正确的映像文件重新开始恢复过程。

如果由于浏览器窗口刷新或关闭而使传输中止，系统将清除会话且会话立即超时。如果由于网络无法访问而使传输中止，会话则会在 45 秒后超时。在会话超时之后，可以再次开始恢复过程。

下载 / 备份配置文件

WAP 设备 配置文件采用 XML 格式，包含有关 WAP 设备设置的所有信息。可以将配置文件备份（上载）到网络主机或 TFTP 服务器，以手动编辑内容或创建备份。编辑备份的配置文件后，可以将其下载到接入点以修改配置。

WAP 设备 保留以下配置文件：

- **Startup Configuration** - 保存到闪存的配置文件。
- **Backup Configuration** - 作为备份保存在 WAP 设备中的其他配置文件。
- **Mirror Configuration** - 如果 Startup Configuration 至少在 24 小时内未进行修改，则会自动保存为 Mirror Configuration 文件。 Mirror Configuration 文件是过去 Startup Configuration 的快照。可通过恢复出厂设置保留 Mirror Configuration，这样将 Mirror Configuration 复制到 Startup Configuration，可在恢复出厂设置后将其用于恢复系统配置。

注 除了下载这些文件并将其上载到其他系统外，还可以将其复制为 WAP 设备上的不同文件类型。请参阅**复制 / 保存配置**。

备份配置文件

要将配置文件备份（上载）到网络主机或 TFTP 服务器，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Download/Backup Configuration File**。

步骤 2 选择 **Via TFTP** 或 **Via HTTP/HTTPS** 作为 **Transfer Method**。

步骤 3 选择 **Backup (AP to PC)** 作为 **Save Action**。

步骤 4 仅对于 TFTP 备份，输入 **Destination File Name**（扩展名为 .xml）。还包含此文件在服务器上的路径，然后输入 **TFTP Server IPv4 Address**。

文件名不能包含以下字符：空格、<、>、|、\、:、(、)、&、;、#、?、* 和两个或更多的连续句点。

步骤 5 仅对于 TFTP 备份，输入 **TFTP Server IPv4 Address**。

步骤 6 选择要备份的配置文件：

- **Startup Configuration** - WAP 设备上次启动时使用的配置文件类型。这不包含已应用但尚未保存到 WAP 设备的任何配置更改。
- **Backup Configuration** - WAP 设备中保存的备份配置文件类型。
- **Mirror Configuration** - 如果 Startup Configuration 至少在 24 小时内未进行修改，则会自动保存为 Mirror Configuration 文件。 Mirror Configuration 文件是过去 Startup Configuration 的快照。可通过恢复出厂设置保留 Mirror Configuration，这样将 Mirror Configuration 复制到 Startup Configuration，可在恢复出厂设置后将其用于恢复系统配置。

步骤 7 点击**保存**开始备份。对于 HTTP 备份，会出现一个窗口，可用来浏览所需的文件保存位置。

下载配置文件

可以将文件下载到 WAP 设备，以便更新配置或将 WAP 设备 恢复为以前备份的配置。

要将配置文件下载到 WAP 设备，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Download/Backup Configuration File**。

步骤 2 选择 **Via TFTP** 或 **Via HTTP/HTTPS** 作为 **Transfer Method**。

步骤 3 选择 **Download (PC to AP)** 作为 **Save Action**。

步骤 4 仅对 TFTP 下载，输入 **Source File Name**（扩展名为 .xml）。包含此文件在服务器上的路径，然后输入 **TFTP Server IPv4 Address**。

文件名不能包含以下字符：空格、<、>、|、\、:、(、)、&、;、#、?、* 和两个或更多的连续句点。

步骤 5 选择 WAP 设备 上要替换为下载文件的配置文件：**Startup Configuration** 或 **Backup Configuration**。

如果下载的文件覆盖 Startup Configuration 文件并通过有效性检查，下载的配置将在 WAP 设备 下次重新启动时生效。

步骤 6 点击**保存**开始升级或备份。对于 HTTP 下载，会出现一个窗口，可用来浏览以选择要下载的文件。下载完成后，会出现一个指示下载成功的窗口。

注意 下载配置文件时，请确保 WAP 设备 电源不中断。如果在下载配置文件时发生断电现象，文件将会丢失，并且必须重新启动下载过程。

配置文件属性

通过 Configuration Files Properties 页，可以清除启动或备份配置文件。如果清除启动配置文件，备份配置文件将在下次重新启动 WAP 设备 时变为活动文件。

要删除启动或备份配置文件，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Configuration Files Properties**。

步骤 2 选择 **Startup Configuration** 或 **Backup Configuration** 文件类型。

步骤 3 点击 **Clear Files**。

复制 / 保存配置

通过 Copy/Save Configuration 页，可以在 WAP 设备 文件系统内复制文件。例如，可以将备份配置文件复制为启动配置文件类型，这样下次启动 WAP 设备时即可使用。

要将文件复制为另一文件类型，请执行以下步骤：

步骤 1 在导航窗格中选择 **Administration** > **Copy/Save Configuration**。

步骤 2 选择 **Source File Name**：

- **Startup Configuration** - WAP 设备上次启动时使用的配置文件类型。这不包含已应用但尚未保存到 WAP 设备的任何配置更改。
- **Backup Configuration** - WAP 设备中保存的备份配置文件类型。

- **Mirror Configuration** - 如果 Startup Configuration 至少在 24 小时内未进行修改，则会自动保存为 Mirror Configuration 文件。 Mirror Configuration 文件是过去 Startup Configuration 的快照。可通过恢复出厂设置保留 Mirror Configuration，这样将 Mirror Configuration 复制到 Startup Configuration，可在恢复出厂设置后将其用于恢复系统配置。

步骤 3 对于 **Destination File Name**，请选择正在复制文件所要替换的文件类型。

步骤 4 点击**保存**开始复制过程。

完成后，会出现显示 Copy Operation Successful 消息的窗口。

重新启动

可以使用 Reboot 页重新启动 WAP 设备。

步骤 1 要重新启动 WAP，在导航窗格中选择 **Administration** > **Reboot**。

步骤 2 请选择以下选项之一：

- **Reboot** - 使用启动配置重新启动 WAP。
- **Reboot to Factory Default** - 使用出厂默认配置文件重新启动 WAP。其他任何自定义设置均会丢失。

会显示一个窗口，可用来确认或取消重新启动。当前的管理会话可能会终止。

步骤 3 点击 **OK** 重新启动。

发现 - Bonjour

通过 Bonjour，可以使用多播域名服务器 (mDNS) 发现 WAP 设备 及其服务。Bonjour 可向网络通告服务并对支持的服务类型进行查询答复，从而简化小型企业环境中的网络配置。

WAP 设备 可以通告以下服务类型：

- **Cisco-specific device description** (csco-sb) - 通过此服务，客户端可以发现思科 WAP 设备以及小型企业网络中部署的其他产品。

- **Management user interfaces** - 此服务可识别 WAP 设备中可用的管理界面（HTTP 和 SNMP）。

将已启用 Bonjour 的 WAP 设备连接到网络后，任何 Bonjour 客户端均可发现和访问配置实用程序，而无需预先配置。

系统管理员可以使用已安装的 Internet Explorer 插件来发现 WAP 设备。基于 Web 的配置实用程序在浏览器中显示为标签。

Bonjour 在 IPv4 和 IPv6 网络中均可工作。

通过 Bonjour 发现 WAP 设备的步骤：

步骤 1 在导航窗口中选择 **Administration** > **Discovery - Bonjour**。

步骤 2 选择 **Enable**。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

数据包捕获

通过无线数据包捕获功能，可以捕获和存储 WAP 设备所接收和发送的数据包。然后，可以由网络协议分析程序对捕获的数据包进行分析，用于故障排除或性能优化。以下是两种数据包捕获方法：

- 本地捕获方法 - 捕获的数据包存储在 WAP 设备上的文件中。 WAP 设备可以将此文件传输到 TFTP 服务器。此文件采用 pcap 格式，可以使用 Wireshark、OmniPeek 等工具进行检查。
- 远程捕获方法 - 捕获的数据包可以实时重新定向到运行 Wireshark 工具的外部计算机。

WAP 设备可以捕获以下类型的数据包：

- 无线接口接收和发送的 802.11 数据包。无线接口捕获的数据包包含 802.11 报头。
- 以太网接口接收和发送的 802.3 数据包。
- 内部逻辑接口（例如 VAP 和 WDS 接口）接收和发送的 802.3 数据包。

点击 **Administration > Packet Capture** 以显示 Packet Capture 页。在 Packet Capture 页，可以进行以下操作：

- 配置数据包捕获参数。
- 启动本地或远程数据包捕获。
- 查看当前的数据包捕获状态。
- 下载数据包捕获文件。

数据包捕获配置

通过 Packet Capture Configuration 区域，可以配置参数和启动数据包捕获。

要配置数据包捕获设置，请执行以下步骤：

步骤 1 配置以下参数：

- **Capture Beacons** - 启用或禁用捕获无线检测或无线传输的 802.11 信标。
- **Promiscuous Capture** - 启用或禁用捕获处于活动状态时的混杂模式。

  在混杂模式下，无线接收信道中的所有流量，包括并非发送给此 WAP 设备的流量。无线在混杂模式下运行时，它会继续向关联的客户端提供服务。不会转发并非发送给此 WAP 设备的数据包。

  捕获完成后，无线立即恢复为非混杂模式运行。
- **Radio Client Filter** - 启用或禁用无线局域网客户端过滤器，仅捕获指定 MAC 地址的无线局域网客户端收发的帧。
- **Client Filter MAC Address** - 指定无线局域网客户端过滤的 MAC 地址。

  注 仅在 802.11 接口中执行捕获时， MAC 过滤器处于活动状态。
- **Packet Capture Method** - 请选择以下选项之一：
  - **Local File** - 捕获的数据包存储在 WAP 设备上的文件中。
  - **Remote** - 捕获的数据包可以实时重新定向到运行 Wireshark 工具的外部计算机。

步骤 2 请根据所选方法，参考 “本地数据包捕获”或 “远程数据包捕获”部分中的步骤继续操作。

注 对数据包捕获配置参数的更改在数据包捕获重新启动后生效。在数据包捕获运行时修改这些参数不会影响当前的数据包捕获会话。要开始使用新的参数值，必须停止并重新启动现有的数据包捕获会话。

本地数据包捕获

要启动本地数据包捕获，请执行以下步骤：

步骤 1 确保对于 **Packet Capture Method** 选择 **Local File**。

步骤 2 配置以下参数：

- **Capture Interface** - 输入数据包捕获的捕获接口类型：
  - **radio1** - 无线接口 中的 802.11 流量。
  - **eth0** - 以太网接口中的 802.3 流量。
  - **VAP0** - VAP0 流量。
  - **VAP1** 至 **VAP15**（如果配置）- 指定 VAP 中的流量。
  - **brtrunk** - WAP 设备中的 Linux 网桥接口。
- **Capture Duration** - 输入捕获持续时间（秒）。范围介于 10 至 3600 之间，默认值为 60。
- **Max Capture File Size** - 输入允许的最大捕获文件大小 (KB)。范围介于 64 至 4096 之间，默认值为 1024。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

步骤 4 点击 **Start Capture**。

在 Packet File Capture 模式下，WAP 设备将捕获的数据包存储在 RAM 文件系统中。数据包捕获会在激活后继续执行，直到发生以下事件之一：

- 捕获时间达到已配置的持续时间。
- 捕获文件达到其最大大小。
- 管理员停止捕获。

如果 WAP 设备上的某个数据包捕获激活，此页的 Packet Capture Status 区域会显示数据包捕获状态。

- **Current Capture Status** - 数据包捕获是在运行还是已停止。

- **Packet Capture Time** - 过去的捕获时间。
- **Packet Capture File Size** - 当前捕获文件的大小。

点击 **Refresh** 从 WAP 设备显示最新数据。

注 要停止数据包文件捕获，请点击 **Stop Capture**。

远程数据包捕获

通过远程数据包捕获功能，可以将远程端口指定为数据包捕获的目标端口。此功能可以与 Windows 版本的 Wireshark 网络分析程序一起使用。数据包捕获服务器在 WAP 设备中运行，通过到 Wireshark 工具的 TCP 连接发送捕获的数据包。Wireshark 是一个免费提供的开源工具，可以从 http://www.wireshark.org 下载。

运行 Wireshark 工具的 Microsoft Windows 计算机可用来显示、记录和分析已捕获的流量。远程数据包捕获设备是 Windows 版本的 Wireshark 工具的标准功能。Linux 版本不能与 WAP 设备一起使用。

使用远程捕获模式时， WAP 设备不在其文件系统中本地存储任何已捕获数据。

如果在 Wireshark 计算机与 WAP 设备之间安装防火墙，必须允许这 3 个端口的流量通过防火墙。还必须将防火墙配置为允许 Wireshark 计算机启动到 WAP 设备的 TCP 连接。

要在 WAP 设备中启动远程捕获，请执行以下步骤：

步骤 1 点击 **Administration** > **Packet Capture**。

步骤 2 启用 **Promiscuous Capture**。

步骤 3 对于 **Packet Capture Method** 选择 **Remote**。

步骤 4 对于 **Remote Capture Port** 使用默认端口 (2002)，或者如果使用的不是默认端口，请输入用于将 Wireshark 连接到 WAP 设备所需的端口号。端口号范围介于 0 至 65535 之间。

步骤 5 如果要保存这些设置供以后使用，请点击**保存**。（但是，不会将选择的 **Remote** 保存为 **Packet Capture Method**。）

步骤 6 点击 **Start Capture**。

要启动 Microsoft Windows 版本的 Wireshark 网络分析程序工具，请执行以下步骤：

步骤 1 在同一台计算机上启动 Wireshark 工具。

步骤 2 在菜单中选择 **Capture** > **Options**。会出现一个弹出窗口。

步骤 3 在 **Interface** 中选择 **Remote**。会出现一个弹出窗口。

步骤 4 在 **Host** 中输入 WAP 设备的 IP 地址。

步骤 5 在 **Port** 中输入 WAP 的端口号。例如，如果使用了默认端口，请输入 2002，或者如果使用的不是默认端口，请输入相应的端口号。

步骤 6 点击 **OK**。

步骤 7 选择要从中捕获数据包的接口。在 Wireshark 弹出窗口中， IP 地址旁边会显示一个下拉列表，可用来从中选择接口。接口可以是以下类型之一：

WAP 设备中的 Linux 网桥接口
--rpcap://[192.168.1.220]:2002/brtrunk
有线局域网接口
-- rpcap://[192.168.1.220]:2002/eth0
Radio 1 中的 VAP0 流量
-- rpcap://[192.168.1.220]:2002/wlan0
802.11 流量
-- rpcap://[192.168.1.220]:2002/radio1
在 WAP321 中， VAP1 至 VAP7 流量
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
在 WAP321 中， VAP1 至 VAP3 流量
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3

最多可以同时跟踪 WAP 设备中的 4 个接口。但必须为每个接口单独启动一个 Wireshark 会话。要启动其他的远程捕获会话，请重复执行 Wireshark 配置步骤；无需在 WAP 设备中进行配置。

注 系统使用 4 个连续的端口号，从为远程数据包捕获会话配置的端口开始。验证这 4 个连续的端口号是否可用。如果不使用默认端口，建议使用大于 1024 的端口号。

在无线接口中捕获流量时，可以禁用信标捕获，但其他的 802.11 控制帧仍发送到 Wireshark。通过设置显示过滤器，可以仅显示以下内容：

- 跟踪中的数据帧
- 特定基本服务集 ID (BSSID) 的流量
- 两个客户端之间的流量

以下是一些有用的显示过滤器的示例：

- 排除信标和 ACK/RTS/CTS 帧：

  !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- 仅数据帧：

  wlan.fc.type == 2

- 特定 BSSID 的流量：

  wlan.bssid == 00:02:bc:00:17:d0

- 特定客户端收发的所有流量：

  wlan.addr == 00:00:e8:4e:5f:8e

在远程捕获模式下，通过网络接口之一将流量发送到运行 Wireshark 的计算机。根据 Wireshark 工具的位置，可以通过以太网接口或无线之一发送流量。为避免跟踪数据包引起流量溢出，WAP 设备自动安装捕获过滤器以滤出指定到 Wireshark 应用程序的所有数据包。例如，如果将 Wireshark IP 端口配置为 58000，则将此捕获过滤器自动安装到 WAP 设备中：

不在端口范围 58000-58004

由于性能和安全问题，数据包捕获模式未保存在 WAP 设备的 NVRAM（非易失性随机存取存储器）中；如果重置 WAP 设备，系统将禁用捕获模式，然后必须将其重新启用以继续捕获流量。数据包捕获参数（不是模式）保存在 NVRAM 中。

启用数据包捕获功能可能会产生安全问题：未经授权的客户端可能会连接 WAP 设备并跟踪用户数据。WAP 设备性能在数据包捕获期间也会受到负面影响，并且此影响会逐渐缩小，即使没有活动的 Wireshark 会话也是如此。要最大程度地减少流量捕获期间对 WAP 设备性能产生的影响，请安装捕获过滤器以限制发送到 Wireshark 工具的流量。捕获 802.11 流量时，捕获的大部分帧往往是信标（通常所有 AP 每 100 ms 发送一次）。虽然 Wireshark 支持信标帧的显示过滤器，但不支持捕获过滤器，无法阻止 WAP 设备将捕获的信标数据包转发到 Wireshark 工具。为减少捕获 802.11 信标对性能的影响，请禁用捕获信标模式。

数据包捕获文件下载

可以通过 TFTP 将捕获文件下载到配置的 TFTP 服务器或通过 HTTP(S) 下载到计算机。触发捕获文件下载命令后，捕获自动停止。

由于捕获文件位于 RAM 文件系统中，如果重置 WAP 设备，此文件将消失。

要使用 TFTP 下载数据包捕获文件，请执行以下步骤：

步骤 1 选择 **Use TFTP to download the capture file**。

步骤 2 如果与默认值不同，请输入 **TFTP Server Filename** 进行下载。默认情况下，捕获的数据包存储在 WAP 设备的文件夹文件 /tmp/apcapture.pcap 中。

步骤 3 在提供的字段中指定 **TFTP Server IPv4 Address**。

步骤 4 点击 **Download**。

要使用 HTTP 下载数据包捕获文件，请执行以下步骤：

步骤 1 选择 **Use TFTP to download the captured file**。

步骤 2 点击 **Download**。会出现一个确认窗口。

步骤 3 点击 **OK**。会出现一个对话框，可用来选择保存文件的网络位置。

支持信息

通过 Support Information 页，可以下载包含 AP 相关详细配置信息的文本文件。此文件包含软件和硬件版本信息、 MAC 和 IP 地址、功能的管理和运行状态、用户配置的设置、流量统计信息及其他信息。可以向技术支持人员提供此文本文件，协助他们排除故障问题。

要显示 Support Information 页，在导航窗格中选择 **Administration > Support Information**。

点击 **Download** 以基于当前系统设置生成此文件。稍等片刻后出现一个窗口，可用来将此文件保存到计算机上。

4

局域网

本章介绍如何配置 WAP 设备的端口、网络和时钟设置。

具体包括以下主题：

- 端口设置
- 虚拟局域网和 IPv4 地址设置
- IPv6 地址

端口设置

通过 Port Settings 页，可以查看和配置将 WAP 设备物理连接到局域网的端口的设置。

要查看和配置局域网设置，请执行以下步骤：

步骤 1 在导航区域选择 **LAN** > **Port Settings**。

Operational Status 区域中显示用于局域网端口的端口类型和链路特性，其配置与 Administrative Settings 区域中相同。如果通过配置或自动协商更改设置，可以点击 **Refresh** 以显示最新设置。

步骤 2 启用或禁用 **Auto Negotiation**。

- 如果启用，端口与其链路伙伴协商以设置可用的最快链路速度和双工模式。
- 如果禁用，可以手动配置端口速度和双工模式。

步骤 3 如果禁用自动协商，请选择 **Port Speed**（对于 WAP121，选择 10/100 Mb/s；对于 WAP321，选择 10/100/1000 Mb/s）和双工模式（半双工或全双工）。

步骤 4 启用或禁用 **Green Ethernet Mode**（仅适用于 WAP321）。

- Green Ethernet Mode 是自动断电模式，可以在链路伙伴的信号不存在时降低芯片功耗。无论端口是否启用自动协商，都可以使用 Green Ethernet Mode。

- 如果启用 Green Ethernet Mode，WAP 设备可在线中的电量消失时自动进入低功耗模式，并在检测到电量时恢复正常运行。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

虚拟局域网和 IPv4 地址设置

可以使用 VLAN and IPv4 Address Settings 页配置局域网接口的设置，包括指定静态或动态 IPv4 地址。

要配置局域网设置，请执行以下步骤：

步骤 1 在导航区域选择 **LAN** > **VLAN and IPv4 Address**。

此页显示 Global Settings 和 IPv4 Settings。 Global Settings 区域中显示局域网接口端口的 MAC（媒体接入控制）地址。此字段是只读字段。

步骤 2 配置以下全局设置：

- **Untagged VLAN** - 启用或禁用虚拟局域网标记。如果启用（默认值），将为所有流量标记 VLAN ID。

  默认情况下，接入点的所有流量都使用 VLAN 1（默认的非标记虚拟局域网）。这意味着在禁用非标记虚拟局域网、更改非标记流量的 VLAN ID、使用 RADIUS（远程验证拨入用户服务）更改 VAP 或客户端的 VLAN ID 之前，不对任何流量进行标记。

- **Untagged VLAN ID** - 为非标记 VLAN ID 指定介于 1 至 4094 之间的数字，默认值为 1。将在此字段中指定的虚拟局域网流量转发到网络时，不会为此流量标记 VLAN ID。

  VLAN 1 既是默认的非标记虚拟局域网，也是默认的管理虚拟局域网。如果要将管理流量与非标记虚拟局域网流量分开，请在路由器中配置新的 VLAN ID，然后在 WAP 设备中使用这个新的 VLAN ID。

- **Management VLAN ID** - 与用于访问 WAP 设备的 IP 地址关联的虚拟局域网。对于 Management VLAN ID，提供介于 1 至 4094 之间的数字，默认值为 1。

  此虚拟局域网也是默认的非标记虚拟局域网。如果已在网络中通过不同的 VLAN ID 配置管理虚拟局域网，必须在 WAP 设备中更改管理虚拟局域网的 VLAN ID。

步骤 3 配置以下 IPv4 设置：

- **Connection Type** - 默认情况下，思科 WAP121 和 WAP321 中的 DHCP 客户端会自动广播网络信息请求。如果要使用静态 IP 地址，必须禁用 DHCP 客户端并手动配置 IP 地址和其他网络信息。

  从列表中选择以下值之一：

  - **DHCP** - WAP 设备 从局域网的 DHCP 服务器获取其 IP 地址。
  - **Static IP** - 手动配置 IPv4 地址。 IPv4 地址应采用类似于 xxx.xxx.xxx.xxx (192.0.2.10) 的格式。
- **Static IP Address, Subnet Mask, and Default Gateway** - 如果选择指定静态 IP 地址，请输入 IP 信息。
- **Domain Name Servers** - 从列表中选择一个选项：
  - **Dynamic** - WAP 设备从局域网的 DHCP 服务器获取 DNS 服务器地址。
  - **Manual** - 手动配置一个或多个 DNS 服务器地址。最多在文本框中输入两个 IP 地址。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

IPv6 地址

可以使用 IPv6 Addresses 页将 WAP 设备配置为使用 IPv6 地址。

要配置 IPv6 地址设置，请执行以下步骤：

步骤 1 在导航区域选择 **LAN** > **IPv6 Addresses**。

步骤 2 配置以下设置：

- **IPv6 Connection Type** - 选择 WAP 设备如何获取 IPv6 地址：
  - **DHCPv6** - IPv6 地址是由 DHCPv6 服务器指定的。
  - **Static IPv6** - 手动配置 IPv6 地址。 IPv6 地址应采用类似于 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) 的格式。
- **IPv6 Administration Mode** - 启用 IPv6 管理访问。

- **IPv6 Auto Configuration Administration Mode** - 启用 WAP 设备中的 IPv6 自动地址配置。

  如果启用， WAP 设备 通过处理局域网端口接收的路由器通告获取其 IPv6 地址和网关。 WAP 设备可以拥有多个自动配置的 IPv6 地址。

- **Static IPv6 Address** - 静态 IPv6 地址。WAP 设备可以拥有一个静态 IPv6 地址（即使此地址已自动配置）。
- **Static IPv6 Address Prefix Length** - 静态地址的前缀长度，介于 0 至 128 之间的整数，默认值为 0。
- **Static IPv6 Address Status** - 显示以下值之一：
  - **Operational** - IP 地址已确认为局域网中的唯一地址，可以在接口中使用。
  - **Tentative** - 指定静态 IP 地址时，WAP 设备自动启动重复地址检测 (DAD) 进程。正在确认 IPv6 地址是否为网络中的唯一地址时，此地址处于暂定状态。在此状态下， IPv6 地址无法用于发送或接收普通流量。
  - **Blank (no value)** - 未指定 IP 地址或指定的地址没有运行。
- **IPv6 Autoconfigured Global Addresses** - 如果已经为 WAP 设备自动指定一个或多个 IPv6 地址，系统会列出这些地址。
- **IPv6 Link Local Address** - 本地物理链路使用的 IPv6 地址。此链路的本地地址不可配置，可通过使用 IPv6 邻居发现进程指定。
- **Default IPv6 Gateway** - 静态配置的默认 IPv6 网关。
- **IPv6 DNS Nameservers** - 请选择以下值之一：
  - **Dynamic** - 通过 DHCPv6 动态获取 DNS 名称服务器。
  - **Manual** - 在提供的字段中最多指定两个 IPv6 DNS 名称服务器。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

5

无线

本章介绍如何配置无线功能操作的属性。

具体包括以下主题：

- 无线
- 恶意 AP 检测
- 网络
- 调度程序
- 调度程序关联
- 带宽利用率
- MAC 过滤
- WDS 网桥
- 工作组网桥
- 服务质量
- WPS 设置
- WPS 过程

无线

无线设置直接控制无线在 WAP 设备中的特性及其与物理媒体的交互，即 WAP 设备发出信号的方式以及信号的类型。

要配置无线设置，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **Radio**。

步骤 2 在 Global Settings 区域中配置 **TSPEC Violation Interval**，该间隔是 WAP 设备报告关联客户端未遵守强制准入控制过程的时间间隔（秒）。通过系统日志和 SNMP 陷阱进行报告。输入介于 0 至 900 秒之间的时间。默认值为 300 秒。

步骤 3 在 Basic Settings 区域中配置以下设置：

注 当地法规可能会禁止使用某些无线模式。某些模式在部分国家 / 地区不可用。

- **Radio** - 打开或关闭无线接口。默认情况下，无线为关闭状态。
- **MAC Address** - 上述接口的媒体接入控制 (MAC) 地址。 MAC 地址由制造商指定，无法更改。
- **Mode** - 无线使用的 IEEE 802.11 标准和频率。：
  - 802.11a - 仅 802.11a 客户端可以连接到 WAP 设备。
  - 802.11b/g—802.11b 和 802.11g 客户端可以连接到 WAP 设备。
  - 802.11a/n—以 5-GHz 频率运行的 802.11a 客户端和 802.11n 客户端可以连接到 WAP 设备。
  - 802.11b/g/n（默认值）—以 2.4 GHz 频率运行的 802.11b、 802.11g 和 802.11n 客户端可以连接到 WAP 设备。
  - 5 GHz 802.11n—仅以 5 GHz 频率运行的 802.11n 客户端可以连接到 WAP 设备。
  - 2.4 GHz 802.11n—仅以 2.4 GHz 频率运行的 802.11n 客户端可以连接到 WAP 设备。
- **Channel Bandwidth** - 802.11n 规范除了允许使用传统 20 MHz 信道，也允许将共存的 20/40 MHz 信道用于其他模式。20/40 MHz 信道可提高数据速率，但会减少可用于其他 2.4 GHz 和 5 GHz 设备的信道。

  默认情况下，如果无线模式包括 802.11n，信道带宽会设置为 20/40 MHz 以同时启用两个信道带宽。如果将该字段设置为 20 MHz，则仅可使用 20 MHz 信道的信道带宽。

- **Primary Channel**（仅使用 20/40 MHz 带宽的 802.11n 模式）- 可以将一个 40 MHz 信道视为是由频率域中两个相邻的 20 MHz 信道组成的。通常，将这两个 20 MHz 信道称为 Primary Channel 和 Secondary Channel。 Primary Channel 用于传统客户端和仅支持 20 MHz 信道带宽的 802.11n 客户端。

  请选择以下选项之一：

  - **Upper** - 将 Primary Channel 设置为 40 MHz 频段中大于 20 MHz 的信道。
  - **Lower** - 将 Primary Channel 设置为 40 MHz 频段中小于 20 MHz 的信道。Lower 是默认选择。

- **Channel** - 无线用于发送和接收的无线频谱部分。

  可用信道的范围由无线接口的模式和国家 / 地区代码的设置决定。如果选择 **Auto** 作为信道设置， WAP 设备会扫描可用信道并选择检测到的流量最少的信道。

  每种模式都会提供多个信道，具体取决于频谱如何获得通信委员会 (FCC)、国际电信联盟 (ITU-R) 等国家和跨国监管机构的许可。

步骤 4 在 Advanced Settings 区域中配置以下设置：

- **Short Guard Interval Supported** - 此字段仅在所选的无线模式包含 802.11n 时可用。

  保护间隔是 OFDM（正交频分多路复用）符号之间的无响应时间（纳秒）。保护间隔可以避免符号间干扰 (ISI) 和载波间干扰 (ICI)。 802.11n 模式允许将此保护间隔从 a 和 g 定义的 800 纳秒减少到 400 纳秒。减少保护间隔可以使数据吞吐量提高 10%。

  与 WAP 设备通信的客户端还必须支持较短的保护间隔。

  请选择以下选项之一：

  - **是** - WAP 设备与支持较短保护间隔的客户端通信时以 400 纳秒的保护间隔发送数据。“是”为默认选择。
  - **No** - WAP 设备以 800 纳秒的保护间隔发送数据。

- **Protection** - 保护功能包含用于保证 802.11 传输不会干扰传统工作站或应用。默认情况下，启用保护 (Auto)。启用保护后，如果传统设备属于 WAP 设备，则会调用保护功能。

  可以禁用保护 (Off)，但特定范围内的传统客户端或 WAP 设备会受 802.11n 传输的影响。模式为 802.11b/g 时，还可以使用保护功能。在此模式下启用保护时，可从 802.11g 传输保护 802.11b 客户端和 WAP 设备。

  注 此设置不影响客户端与 WAP 设备进行关联的能力。

- **Beacon Interval** - 发送信标帧的时间间隔。 WAP 设备按规定的时间间隔发送信标帧，宣布无线网络的存在。默认特性是每 100 毫秒发送 1 个（或每秒发送 10 个）信标帧。

  输入一个介于 20 至 2000 毫秒之间的整数。默认值为 100 毫秒。

- **DTIM Period** - 发送流量指示图 (DTIM) 周期。输入一个介于 1 至 255 个信标之间的整数。默认值为 2 个信标。

  DTIM 消息是某些信标帧中包含的元素。用于指示当前在低功率模式下处于睡眠状态的客户端工作站在 WAP 设备中已有等待接收的缓存数据。

  指定的 DTIM 周期用于指示由此 WAP 设备服务的客户端应多久检查一次仍在 WAP 设备中等待接收的缓存数据。

  以信标为测量单位。例如，如果将该字段设置为 1，客户端每接收到 1 个信标会检查一次 WAP 设备中的缓存数据。如果将该字段设置为 10，客户端每接收到 10 个信标会检查一次。

- **Fragmentation Threshold** - 帧大小阈值（字节）。有效整数必须是介于 256 至 2346 之间的偶数，默认值为 2346。

  分片阈值用于限制通过网络发送的数据包（帧）的大小。如果数据包大小超过设置的分片阈值，分片激活并且数据包以多个 802.11 帧发送。

  如果正在发送的数据包大小等于或小于阈值，则不使用分片。将阈值设置为最大值（2346 字节，即默认值）可以有效禁用分片。

  分片会导致更多开销，这不仅仅是因为分片需要分割和重新组合帧的额外工作，还因为它增加了网络中的消息流量。但是，如果正确配置，分片有助于提高网络性能和可靠性。

  发送较小帧（通过使用较小的分片阈值）可能会有助于避免一些干扰问题，例如使用微波炉时。

  默认情况下，关闭分片。除非怀疑存在无线干扰，否则建议不要使用分片。应用于各个分片的其他报头增加了网络中的开销，会显著减少吞吐量。

- **RTS Threshold** - 发送请求 (RTS) 阈值。有效的整数范围必须介于 0 至 2347 之间，默认值为 2347 个八位字节。

  RTS 阈值表示 MPDU（MAC 协议数据单元）中的八位字节数，低于此阈值将不执行 RTS/CTS（请求发送 / 允许发送协议）握手。

  更改 RTS 阈值有助于通过 WAP 设备控制流量，尤其当一个 WAP 设备具有多个客户端时更是如此。如果指定较低的阈值， WAP 设备将更频繁地发送 RTS 数据包，这会占用更多带宽并减少数据包的吞吐量。但是，发送更多的 RTS 数据包可以帮助网络从干扰或冲突中恢复，忙碌网络或遇到电磁干扰的网络中可能会发生此类干扰或冲突。

- **Maximum Associated Clients** - 允许在任何一个时刻访问此 WAP 设备的每个无线的最大工作站数。可以输入一个介于 0 至 200 之间的整数，默认值为 200 个工作站。
- **Transmit Power** - 此 WAP 设备的发射功率电平的百分比值。

  默认值 100% 可以向 WAP 设备提供最大的广播范围并减少所需的接入点数，比其他较低的百分比值更具成本效益。

  要增加网络容量，请使 WAP 设备相互间更靠近并降低发射功率值。这有助于减少接入点之间的重叠和干扰。由于较弱的无线信号不太可能传播到网络的物理位置之外，较低的发射功率设置还可以使网络更加安全。

  一些信道范围和国家 / 地区代码组合的最大发射功率相对较低。尝试将发射功率设置为较低范围（例如 25% 或 12%）时，可能不会发生预期的功率下降，因为某些功率放大器具有最低发射功率要求。
- **Fixed Multicast Rate** - 广播和多播数据包的传输速率 (Mbps)。如果无线客户端可以处理已配置的速率，此设置在发生无线多播视频流的环境中会很有用。

  如果选择 **Auto**， WAP 设备会选择关联客户端的最佳速率。有效值范围由已配置的无线模式决定。
- **Legacy Rate Sets** - 速率以兆位 / 秒表示。

  Supported Rate Sets 表示 WAP 设备支持的速率。可以选中多个速率（选中一个复选框以选择或取消选择速率）。 WAP 设备会基于误码率、客户端工作站与 WAP 设备的距离等因素自动选择效率最高的速率。

  Basic Rate Sets 表示为建立与网络中的其他接入点和客户端工作站的通信，WAP 设备向网络通告的速率。这通常比由 WAP 设备广播所支持速率集的子集效率更高。
- **MCS (Data Rate) Settings** - WAP 设备通告的调制和编码方案 (MCS) 索引值。MCS 可以增加 802.11n 无线客户端的吞吐量。

  选中 MCS 索引号下面的复选框可以启用该索引，取消选中可以将其禁用。无法同时禁用所有索引。

  WAP 设备支持 MCS 索引 0 至 15。MCS 索引 15 允许使用最大的传输速率 300 Mbps。如果未选择 MCS 索引，无线在 MSC 索引 0 中运行，这样允许使用最大的传输速率 15 Mbps。

  仅在无线模式包含 802.11n 支持时，可以配置 MCS 设置。
- **Broadcast/Multicast Rate Limiting** - 通过限制整个网络传输的数据包数，多播和广播速率限制可以改进整体的网络性能。

默认情况下，禁用 Multicast/Broadcast Rate Limiting 选项。在启用 Multicast/Broadcast Rate Limiting 之前，禁用以下字段：

- **Rate Limit** - 多播和广播流量的速率限制。速率限制应大于 1，但小于 50 个数据包 / 秒。低于此速率限制的任何流量总是符合条件并传输至相应的目标位置。默认的最大速率限制设置为 50 个数据包 / 秒。
- **Rate Limit Burst** - 以字节为测量单位的流量，即使流量大于定义的最大速率，也允许作为临时的突发流量传递。默认的最大速率限制突发设置为 75 个数据包 / 秒。

- **TSPEC Mode** - 控制 WAP 设备中的整体 TSPEC（流量规范）模式。默认情况下，关闭 TSPEC 模式。选项如下：
  - **On** - WAP 设备根据 Radio 页中配置的 TSPEC 设置处理 TSPEC 请求。如果 WAP 设备处理来自支持 QoS 的设备中的流量（例如 Wi-Fi CERTIFIED 电话），请使用此设置。
  - **Off** - WAP 设备会忽略来自客户端工作站的 TSPEC 请求。对于时效性强的流量，如果不希望使用 TSPEC 给予支持 QoS 的设备优先权，请使用此设置。
- **TSPEC Voice ACM Mode** - 控制语音接入类别的强制准入控制 (ACM)。默认情况下，关闭 TSPEC Voice ACM 模式。选项如下：
  - **On** - 需要某个工作站向 WAP 设备发送 TSPEC 带宽请求，然后发送或接收语音流量流。 WAP 设备以请求结果作为响应，如果允许使用 TSPEC，结果包含分配的媒体时间。
  - **Off** - 工作站可以发送和接收优先的语音流量，无需使用经允许的 TSPEC；WAP 设备会忽略来自客户端工作站的语音 TSPEC 请求。
- **TSPEC Voice ACM Limit** - 为了获取访问权限，WAP 设备尝试使用语音 AC 通过无线媒体传输的流量上限。默认限值为总流量的 20%。
- **TSPEC Video ACM Mode** - 控制视频接入类别的强制准入控制。默认情况下，关闭 TSPEC Video ACM 模式。选项如下：
  - **On** - 需要某个工作站向 WAP 设备发送 TSPEC 带宽请求，然后发送或接收视频流量流。 WAP 设备以请求结果作为响应，如果允许使用 TSPEC，结果包含分配的媒体时间。
  - **Off** - 工作站可以发送和接收优先的视频流量，无需使用经允许的 TSPEC；WAP 设备会忽略来自客户端工作站的视频 TSPEC 请求。
- **TSPEC Video ACM Limit** - 为了获取访问权限，WAP 设备尝试使用视频 AC 通过无线媒体传输的流量上限。默认限值为总流量的 15%。

- **TSPEC AP Inactivity Timeout** - WAP 设备在删除下行链路流量规范之前检测其为闲置状态的时间长度。有效的整数范围介于 0 至 120 秒之间，默认值为 30 秒。
- **TSPEC Station Inactivity Timeout** - WAP 设备在删除上行链路流量规范之前检测其为闲置状态的时间长度。有效的整数范围介于 0 至 120 秒之间，默认值为 30 秒。
- **TSPEC Legacy WMM Queue Map Mode** - 启用或禁用队列中作为 ACM 运行的混合传统流量。默认情况下，关闭此模式。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

注意 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况，WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

恶意 AP 检测

恶意 AP 是在未获得系统管理员明确授权的情况下即安装在安全网络中的接入点。恶意接入点存在安全威胁，因为进入网络的任何人会无意或恶意安装廉价的无线 WAP 设备，未经授权的用户可能会借此访问网络。

WAP 设备对每个无线中的所有信道进行 RF（射频）扫描，可检测出网络范围内的所有 AP。如果检测到恶意 AP，会将其显示在 Rogue AP Detection 页上。如果列为恶意的 AP 是合法的，可以将其添加到 Known AP List 中。

注 Detected Rogue AP List 和 Trusted AP List 可提供采取进一步措施所需的信息。AP 对这些列表中的恶意 AP 不会有任何的控制，无法对通过 RF 扫描检测到的 AP 应用任何安全策略。

如果启用 AP 检测，无线会定期从其运行信道切换以扫描同一频段内的其他信道。

查看 Rogue AP List

可以启用和禁用恶意 AP 检测。要启用无线以收集有关恶意 AP 的信息，点击 Radio 1（或 WAP561 设备的 Radio 2）的 **AP Detection** 然后点击**保存**。

会出现有关检测到的和受信任的恶意接入点的信息。可以点击 **Refresh** 刷新屏幕，然后显示以下最新信息：

- **Action** - 如果 AP 出现在 Detected Rogue AP List 中，可以点击 **Trust** 将 AP 移到 Trusted AP List 中。

  如果 AP 出现在 Trusted AP List 中，可以点击 **Untrust** 将 AP 移到 Detected Rogue AP List 中。

  注 Detected Rogue AP List 和 Trusted AP List 可提供信息。WAP 设备 对这些列表中的 AP 不会有任何的控制，无法对通过 RF 扫描检测到的 AP 应用任何安全策略。

- **MAC Address** - 恶意 AP 的 MAC 地址。
- **Beacon Interval** - 恶意 AP 使用的信标间隔。

  信标帧由 AP 按规定的时间间隔发送，宣布无线网络的存在。默认特性是每 100 毫秒发送 1 个（或每秒发送 10 个）信标帧。

  注 Beacon Interval 是在**无线**页上设置的。

- **Type** - 设备类型：
  - AP 表示恶意设备是在基础设施模式下支持 IEEE 802.11 无线网络架构的 AP。
  - Ad hoc 表示在 Ad hoc 模式下运行的恶意工作站。设置为 Ad hoc 模式的工作站彼此直接通信，无需使用传统 AP。 Ad hoc 模式是 IEEE 802.11 无线网络架构，也称作对等模式或独立基本服务集 (IBSS)。
- **SSID** - WAP 设备的服务集标识符 (SSID)。

  SSID 是最多为 32 个字符的字母数字字符串，可以唯一标识无线局域网。还可称为网络名称。

- **Privacy** - 表示恶意设备上是否存在任何安全性：
  - Off 表示恶意设备上的 Security 模式设置为 None（无安全性）。
  - On 表示恶意设备上具有一些安全性。

  注 可以使用**网络**页配置 AP 的安全性。

- **WPA** - 打开还是关闭恶意 AP 的 WPA 安全性。

- **Band** - 恶意 AP 中正在使用的 IEEE 802.11 模式。（例如，IEEE 802.11a、IEEE 802.11b、 IEEE 802.11g。）

  显示的数字表示相应的模式：

  - 2.4 表示 IEEE 802.11b、 802.11g 或 802.11n 模式 （或这些模式的组合）。
  - 5 表示 IEEE 802.11a 或 802.11n 模式 （或这两种模式）。

- **Channel** - 当前广播恶意 AP 的信道。

  信道可定义无线用于发送和接收的无线频谱部分。

  注 可以使用**无线**页设置信道。

- **Rate** - 当前传输恶意 AP 的速率 （兆位 / 秒）。

  当前速率始终都是 Supported Rates 中所示速率之一。

- **Signal** - 从恶意 AP 发出的无线信号的强度。如果将鼠标指针悬停在这些条上，会出现用分贝 (dB) 表示强度的数字。
- **Beacons** - 自首次发现信标后从恶意 AP 接收的信标总数。
- **Last Beacon** - 从恶意 AP 接收的最后一个信标的日期和时间。
- **Rates** - 恶意 AP 的支持和基本 （通告）速率集。速率以兆位 / 秒 (Mbps) 为单位显示。

  会列出所有 Supported Rates，其中 Basic Rates 以粗体显示。速率集是在**无线**页中配置的。

创建并保存 Trusted AP List

要创建 Trusted AP List 并将其保存到文件中，请执行以下步骤：

步骤 1 在 Detected Rogue AP List 中，对已知的 AP 点击 **Trust**。受信任的 AP 会移到 Trusted AP List 中。

步骤 2 在 Download/Backup Trusted AP List 区域，选择 **Backup (AP to PC)**。

步骤 3 点击**保存**。

列表包含已添加到 Known AP List 中的所有 AP 的 MAC 地址。默认情况下，文件名为 Rogue2.cfg。可以使用文本编辑器或 Web 浏览器打开文件并查看其中的内容。

导入 Trusted AP List

可以从保存的列表中导入已知 AP 列表。可能要从另一 AP 获取或基于文本文件创建列表。如果 AP 的 MAC 地址出现在 Trusted AP List 中，不会将其检测为恶意 AP。

要从文件导入 AP 列表，请执行以下步骤：

步骤 1 在 Download/Backup Trusted AP List 区域，选择 **Download (PC to AP)**。

步骤 2 点击 **Browse**，然后选择要导入的文件。

导入的文件必须是扩展名为 .txt 或 .cfg 的纯文本文件。文件中的条目是十六进制格式的 MAC 地址，每隔八位字节用冒号隔开，例如 00:11:22:33:44:55。条目之间必须用一个空格隔开。对于要接受文件的 AP，必须仅包含 MAC 地址。

步骤 3 选择是替换现有的 Trusted AP List 还是将导入文件中的条目添加到 Trusted AP List 中。

a. 选择 **Replace** 可以导入列表并替换 Known AP List 的内容。

b. 选择 **Merge** 可以导入列表并将导入文件中的 AP 添加到 Known AP List 当前显示的 AP 中。

步骤 4 点击**保存**。

导入完成后，屏幕刷新，导入文件中的 AP 的 MAC 地址出现在 Known AP List 中。

网络

虚拟接入点 (VAP) 将无线局域网分为多个广播域，这些域是以太网虚拟局域网的无线对等体。 VAP 在一个物理 WAP 设备中模拟多个接入点。 WAP121 最多支持 4 个 VAP， WAP321 最多支持 8 个 VAP。

除了 VAP0，可以单独启用或禁用其他所有的 VAP。VAP0 是物理无线接口，只要无线启用即保持启用状态。要禁用 VAP0 的运行，必须禁用无线本身。

每个 VAP 都通过一个用户配置的服务集标识符 (SSID) 来识别。多个 VAP 无法使用相同的 SSID 名称。可以单独启用或禁用每个 VAP 的 SSID 广播。默认情况下，启用 SSID Broadcast。

SSID 命名约定

VAP0 的默认 SSID 为 ciscosb。已创建的其他各个 VAP 都拥有空的 SSID 名称。可以将所有 VAP 的 SSID 配置为其他值。

SSID 可以是由任何字母数字组成的条目，区分大小写，字符数介于 2 至 32 之间。允许使用可打印字符和空格 (ASCII 0x20)，不包括以下 6 个字符：

?、"、$、[、\、] 和 +。

允许使用的字符包括：

ASCII 0x20、0x21、0x23、0x25 到 0x2A、0x2C 到 0x3E、0x40 到 0x5A、0x5E 到 0x7E。

此外，以下 3 个字符无法用作首字符：

!、# 和 ;（分别为 ASCII 0x21、 0x23 和 0x3B）。

不允许使用结尾和前导空格 (ASCII 0x20)。

注 这意味着允许在 SSID 中使用空格，但不能用作首字符或最后的字符，也允许使用句点 “.” (ASCII 0x2E)。

VLAN ID

每个 VAP 都与一个虚拟局域网关联，可通过 VLAN ID (VID) 识别。 VID 可以是介于 1 至 4094（含 1 和 4094）之间的任何值。 WAP121 支持 5 个活动虚拟局域网（其中 4 个用于无线局域网， 1 个是管理虚拟局域网）。 WAP321 支持 9 个活动虚拟局域网（8 个用于无线局域网， 1 个是管理虚拟局域网）。

默认情况下，指定给 WAP 设备的配置实用程序的 VID 是 1，这也是默认的非标记 VID。如果管理 VID 和指定给 VAP 的 VID 相同，则与此特定 VAP 关联的无线局域网客户端可以管理 WAP 设备。如有需要，可以创建访问控制列表 (ACL) 以便从无线局域网客户端中禁用管理。

配置 VAP

要配置 VAP，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **Networks**。

步骤 2 选中要配置的 VAP 相应的 **Enabled** 复选框。

- 或 -

如果 VAP0 是系统中配置的唯一的 VAP，并且要添加 VAP，请点击**添加**。然后，选择此 VAP 并点击**编辑**。

步骤 3 配置以下参数：

- **VLAN ID** - 要与 VAP 关联的虚拟局域网的 VID。

注意 务必输入在网络中正确配置的 VLAN ID。如果 VAP 将无线客户端与错误配置的虚拟局域网进行关联，可能会导致网络问题。
当无线客户端使用此 VAP 连接到 WAP 设备时， WAP 设备将使用在此字段中输入的 VLAN ID 标记来自无线客户端的所有流量，除非输入端口的 VLAN ID 或使用 RADIUS 服务器为虚拟局域网指定一个无线客户端。 VLAN ID 的范围介于 1 至 4094 之间。

注 如果将 VLAN ID 更改为与当前管理 VLAN ID 不同的 ID，则与此特定 VAP 关联的无线局域网客户端无法管理设备。可在 LAN 页验证非标记和管理 VLAN ID 的配置。有关详情，请参阅**虚拟局域网和 IPv4 地址设置**。

- **SSID Name** - 无线网络的名称。 SSID 是最多包含 32 个字符的字母数字字符串。为每个 VAP 选择唯一的 SSID。

  注 如果作为无线客户端连接到正在管理的同一 WAP 设备，重置 SSID 将会断开与 WAP 设备的连接。需要先保存这一新设置，再重新连接到新的 SSID。

- **Broadcast SSID** - 启用和禁用 SSID 的广播。

  指定是否允许 WAP 设备在其信标帧中广播 SSID。默认情况下，启用 Broadcast SSID 参数。如果 VAP 不广播其 SSID，则客户端工作站的可用网络列表中不会显示网络名称。反而必须将正确的网络名称手动输入到客户端的无线连接实用程序中，这样网络才可以连接。

  禁用广播 SSID 足以避免客户端无意间连接到网络，但即使是黑客发起的最简单的连接或监控未加密流量的企图也无法阻止。禁止 SSID 广播可以为其他暴露的网络（例如访客网络）提供最低级别的保护，其中最重要的是要便于客户端获取连接并且不会提供敏感信息。

- **Security** - 访问 VAP 所需的身份验证类型：
  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

如果选择 None 以外的安全模式，则会出现其他字段。这些字段已在**配置安全设置**中介绍。

注 建议使用可提供较强安全保护的 WPA Personal 或 WPA Enterprise 作为身份验证类型。对不支持 WPA Personal/Enterprise 的传统无线计算机或设备，仅使用 Static WEP 或 Dynamic WEP。如果需要将 Security 设置为 Static WEP 或 Dynamic WEP，请将无线配置为 802.11a 或 802.11b/g 模式（请参阅**无线**）。802.11n 模式限制将 Static WEP 或 Dynamic WEP 用作安全模式。

- **MAC Filtering** - 指定是否将可以访问此 VAP 的工作站限制为已配置的 MAC 地址全局列表。可以选择以下 MAC 过滤类型之一：
  - **Disabled** - 不使用 MAC 过滤。
  - **Local** - 使用在 **MAC 过滤**页中配置的 MAC 验证列表。
  - **RADIUS** - 使用外部 RADIUS 服务器上的 MAC 验证列表。
- **Channel Isolation** - 启用和禁用工作站隔离。
  - 如果禁用此选项，无线客户端可以通过 WAP 设备发送流量，从而与另一个客户端进行正常通信。
  - 如果启用此选项， WAP 设备将阻止同一 VAP 上的无线客户端之间的通信。WAP 设备仍允许网络中其无线客户端与有线设备之间、通过 WDS 链路以及与不同 VAP 关联的其他无线客户端之间的数据流量，但不允许其无线客户端之间的数据流量。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

注意 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

注 要删除 VAP，请选中 VAP 并点击**删除**。要永久保存删除内容，请在完成后点击**保存**。

配置安全设置

以下各节介绍基于在 Networks 页的 Security 列表中选择的内容配置的安全设置。

None (Plain-text)

如果选择 **None** 作为安全模式，不可以在 WAP 设备 上配置其他安全设置。此模式表示 WAP 设备 收发的数据未经加密。此安全模式在最初配置网络或解决问题期间会很有用，但因其不太安全，不建议在内部网络中经常使用。

Static WEP

有线对等保密 (WEP) 是用于 802.11 无线网络的数据加密协议。通过静态 64 位 （ 40 位密钥 + 24 位初始化向量 (IV) ）或 128 位 （ 104 位密钥 + 24 位初始化向量 ）共享密钥配置网络中的所有无线工作站和接入点以加密数据。

Static WEP 并非可用的最安全模式，但可提供比将安全模式设置为 None (Plain-text) 更多的保护，因为此模式可以避免外部人员轻易发现未加密的无线流量。

WEP 基于静态密钥加密通过无线网络移动的数据。（ 加密算法是称为 RC4 的流密码。）

以下参数用于配置 Static WEP：

- **Transfer Key Index** - 密钥索引列表。提供从 1 到 4 的密钥索引。默认值为 1。

  Transfer Key Index 表示 WAP 设备使用哪个 WEP 密钥加密其发送的数据。

- **Key Length** - 密钥的长度。请选择以下选项之一：
  - 64 位
  - 128 位
- **Key Type** - 密钥类型。请选择以下选项之一：
  - ASCII
  - Hex
- **WEP Keys** - 最多可以指定 4 个 WEP 密钥。在每个文本框中，为每个密钥输入一个字符串。输入的密钥取决于所选的密钥类型：
  - ASCII—包括大写和小写字母、数字以及特殊字符 （ 例如 @ 和 # ）。
  - Hex—包括 0 到 9 的数字以及 A 到 F 的字母。

  按照 Characters Required 字段中指定的字符数对每个密钥使用相同数量的字符。这些 RC4 WEP 密钥可以与使用 WAP 设备的工作站共享。

必须配置每个客户端工作站，以按照 WAP 设备中指定的设置在同一时槽使用上述其中一个相同的 WEP 密钥。

- **Characters Required** - 输入到 WEP Key 字段中的字符数量由所选的密钥长度和密钥类型决定。例如，如果使用 128 位 ASCII 密钥，必须在 WEP 密钥中输入 26 个字符。所需的字符数量基于密钥长度和密钥类型的设置方式自动更新。
- **802.1X Authentication** - 当安全模式为 Static WEP 时，身份验证算法定义用于确定是否允许客户端工作站与 WAP 设备进行关联的方法。

  通过选择以下选项之一指定要使用的身份验证算法：

  - **Open System** 身份验证允许任何客户端工作站与 WAP 设备进行关联，无论该客户端工作站是否拥有正确的 WEP 密钥。此算法还可用于纯文本、IEEE 802.1X 和 WPA 模式。如果将身份验证算法设置为 Open System，任何客户端都可以与 WAP 设备进行关联。

    注 仅仅因为允许客户端工作站关联，无法确保该客户端工作站与 WAP 设备交换流量。客户端工作站必须拥有正确的 WEP 密钥，才能成功地从 WAP 设备访问和解密数据，并将可读数据传输至 WAP 设备。
  - **Shared Key** 身份验证要求客户端工作站拥有正确的 WEP 密钥，这样才能与 WAP 设备进行关联。如果将身份验证算法设置为 Shared Key， WEP 密钥错误的客户端工作站无法与 WAP 设备进行关联。
  - 同时选择 **Open System** 和 **Shared Key**。如果同时选择这两种身份验证算法，配置为在共享密钥模式下使用 WEP 的客户端工作站必须拥有有效的 WEP 密钥，这样才能与 WAP 设备进行关联。此外，即使配置为将 WEP 用作开放系统（共享密钥模式未启用）的客户端工作站没有正确的 WEP 密钥，也可与 WAP 设备进行关联。

Static WEP 规则

如果使用 Static WEP，以下规则适用：

- 所有的客户端工作站必须将无线局域网 (WLAN) 安全性设置为 WEP，并且所有客户端必须拥有 WAP 设备中指定的一个 WEP 密钥，这样才能对 AP 到工作站的数据传输进行解码。
- WAP 设备必须拥有客户端用于工作站到 AP 传输的所有密钥，这样才能对工作站传输的数据进行解码。
- 相同密钥在所有节点（AP 和客户端）中必须占用相同时槽。例如，如果 WAP 设备将 abc123 密钥定义为 WEP 密钥 3，则客户端工作站也必须将该字符串定义为 WEP 密钥 3。

- 客户端工作站可以使用不同的密钥将数据传输至接入点。（它们也可以使用相同密钥，但使用相同密钥不太安全，因为这意味着一个工作站可以对另一个工作站正在发送的数据进行解密。）
- 在某些无线客户端软件中，可以配置多个 WEP 密钥并定义客户端工作站传输密钥索引，然后设置这些工作站以使用不同的密钥对其传输的数据进行加密。这可以确保相邻接入点无法对其他接入点传输的数据进行解码。
- 无法在接入点与其客户端工作站之间混合使用 64 位和 128 位的 WEP 密钥。

Dynamic WEP

Dynamic WEP 指 802.1x 技术和可扩展身份验证协议 (EAP) 的组合。通过 Dynamic WEP 的安全性， WEP 密钥可以动态更改。

EAP 消息是使用称为局域网的可扩展身份验证协议封装 (EAPOL) 通过 IEEE 802.11 无线网络发送的。 IEEE 802.1X 提供定期刷新的动态生成的密钥。 RC4 流密码用于对每个 802.11 帧的帧体和循环冗余校验 (CRC) 进行加密。

此模式需要使用外部 RADIUS 服务器对用户进行身份验证。 WAP 设备要求使用支持 EAP 的 RADIUS 服务器，例如 Microsoft Internet Authentication Server。要使用 Microsoft Windows 客户端，身份验证服务器必须支持受保护的 EAP (PEAP) 和 MSCHAP V2。

可以使用 IEEE 802.1X 模式支持的多种身份验证方法中的任何一种，包括证书、Kerberos 和公共密钥身份验证。必须配置客户端工作站以使用与 WAP 设备相同的身份验证方法。

以下参数用于配置 Dynamic WEP：

- **Use Global RADIUS Server Settings** - 默认情况下，每个 VAP 都使用为 WAP 设备定义的全局 RADIUS 设置（请参阅 **RADIUS 服务器**）。但可以配置每个 VAP 以使用一组不同的 RADIUS 服务器。

  要使用全局 RADIUS 服务器设置，请确保选中此复选框。

  要对 VAP 使用单独的 RADIUS 服务器，请取消选中此复选框，然后在以下字段中输入 RADIUS 服务器的 IP 地址和密钥：

- **Server IP Address Type** - RADIUS 服务器使用的 IP 版本。

  可以在地址类型之间进行切换以配置 IPv4 和 IPv6 全局 RADIUS 地址设置，但 WAP 设备仅可连接 RADIUS 服务器或与此字段中所选地址类型对应的服务器。

- **Server IP Address 1** 或 **Server IPv6 Address 1** - 此 VAP 的主 RADIUS 服务器的地址。

第一个无线客户端尝试通过 WAP 设备进行身份验证时， WAP 设备会向主服务器发送身份验证请求。如果主服务器响应身份验证请求，WAP 设备会继续将此 RADIUS 服务器用作主服务器，身份验证请求也会发送至指定的地址。

IPv4 地址应采用类似于 xxx.xxx.xxx.xxx (192.0.2.10) 的格式。IPv6 地址应采用类似于 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) 的格式。

- **Server IP Address 2** 至 **4** 或 **Server IPv6 Address 2** 至 **4** - 最多 3 个 IPv4 或 IPv6 备份 RADIUS 服务器地址。

  如果没有通过主服务器的身份验证，将按顺序尝试每个已配置的备份服务器。

- **Key** - WAP 设备用于向主 RADIUS 服务器进行身份验证的共享密钥。

  最多可以使用 63 个标准字母数字字符和特殊字符。此密钥区分大小写，必须与 RADIUS 服务器上配置的密钥相匹配。输入的文本显示为星号。

- **Key 2** 至 **Key 4** - 与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。**Server IP (IPv6) Address 2** 的服务器使用 **Key 2**， **Server IP (IPv6) Address 3** 的服务器使用 **Key 3**，以此类推。

- **Enable RADIUS Accounting** - 可以对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量等。

  如果启用 RADIUS 记帐，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。

- **Active Server** - 管理性地选择活动的 RADIUS 服务器，而不是由 WAP 设备尝试按顺序连接每个已配置的服务器并选择正在运行的第一个服务器。

- **Broadcast Key Refresh Rate** - 针对与此 VAP 关联的客户端刷新广播（组）密钥的间隔。

  默认值为 300 秒，有效范围介于 0 至 86400 秒之间。值 0 表示不刷新广播密钥。

- **Session Key Refresh Rate** - WAP 设备针对与此 VAP 关联的每个客户端刷新会话（单播）密钥的间隔。

  有效范围介于 0 至 86400 秒之间。值 0 表示不刷新广播密钥。

WPA Personal

WPA Personal 是 Wi-Fi 联盟 IEEE 802.11i 标准，包含 AES-CCMP 和 TKIP 加密。WPA 的个人版本使用预先共享密钥 (PSK)，而不使用 IEEE 802.1X 和 EAP，后者在 Enterprise WPA 安全模式下使用。PSK 仅用于凭据的初始检查中。WPA Personal 还称为 WPA-PSK。

此安全模式向后兼容支持最初的 WPA 的无线客户端。

以下参数用于配置 WPA Personal：

- **WPA Versions** - 要支持的客户端工作站的类型：
  - **WPA** - 网络中拥有支持最初的 WPA 的客户端工作站，但没有支持更新的 WPA2 的客户端工作站。
  - **WPA2** - 网络中的所有客户端工作站都支持 WPA2。此协议版本可以依据 IEEE 802.11i 标准提供最佳安全性。

  如果网络混合使用不同的客户端，即某些客户端支持 WPA2，而其他客户端仅支持最初的 WPA，则选中上述两个复选框。通过此设置， WPA 和 WPA2 客户端工作站可以进行关联和身份验证，但对支持 WPA2 的客户端使用更稳健的 WPA2。此 WPA 配置提高了互操作性，可以代替某些安全性。
- **Cipher Suites** - 要使用的密码套件：
  - TKIP
  - CCMP (AES)

  可以选择任意一个或两个都选。TKIP 和 AES 客户端都可以与 WAP 设备进行关联。 WPA 客户端必须拥有以下密钥之一才能与 WAP 设备进行关联：
  - 有效的 TKIP 密钥
  - 有效的 AES-CCMP 密钥

  如果客户端没有配置为使用 WPA Personal，则不能与 WAP 设备进行关联。
- **Key** - 用于 WPA Personal 安全性的共享密钥。输入最少为 8 个字符、最多为 63 个字符的字符串。可接受的字符包括大写和小写字母、数字以及特殊字符（例如 @ 和 # ）。
- **Key Strength Meter** - WAP 设备针对所用的不同字符类型数（大写和小写字母、数字以及特殊字符）、字符串长度等复杂性标准检查密钥。如果启用 WPA-PSK 复杂性检查功能，除非密钥满足最低标准，否则不可接受。有关配置复杂性检查的详情，请参阅 **WPA-PSK 复杂性**。
- **Broadcast Key Refresh Rate** - 针对与此 VAP 关联的客户端刷新广播（组）密钥的间隔。默认值为 300 秒，有效范围介于 0 至 86400 秒之间。值 0 表示不刷新广播密钥。

WPA Enterprise

WPA Enterprise with RADIUS 是 Wi-Fi 联盟 IEEE 802.11i 标准的实施，包含 CCMP (AES) 和 TKIP 加密。企业模式需要使用 RADIUS 服务器对用户进行身份验证。

此安全模式向后兼容支持最初的 WPA 的无线客户端。

以下参数用于配置 WPA Enterprise：

- **WPA Versions** - 要支持的客户端工作站的类型：
  - **WPA** - 如果网络中的所有客户端工作站支持最初的 WPA，但不支持更新的 WPA2，则选择 WPA。
  - **WPA2** - 如果网络中的所有客户端工作站支持 WPA2，建议使用可依据 IEEE 802.11i 标准提供最佳安全性的 WPA2。
  - **WPA 和 WPA2** - 如果网络混合使用不同的客户端，即某些客户端支持 WPA2，而其他客户端仅支持最初的 WPA，则同时选择 WPA 和 WPA2。通过此设置， WPA 和 WPA2 客户端工作站可以进行关联和身份验证，但对支持 WPA2 的客户端使用更稳健的 WPA2。此 WPA 配置提高了互操作性，可以代替某些安全性。
- **Enable pre-authentication** - 如果仅为 WPA Versions 选择 WPA2 或同时选择 WPA 和 WPA2，可以对 WPA2 客户端启用预身份验证。

  如果想要 WPA2 无线客户端发送预身份验证数据包，请点击 **Enable pre-authentication**。预身份验证信息是从 WAP 设备中继的，此设备当前由客户端将其用作目标 WAP 设备。启用此功能可以帮助加快与多个 AP 连接的漫游客户端的身份验证速度。

  如果已经为 WPA Versions 选择 WPA，则此选项不适用，因为最初的 WPA 不支持此功能。
- **Cipher Suites** - 要使用的密码套件：
  - TKIP
  - CCMP (AES)
  - TKIP 和 CCMP (AES)

  默认情况下，同时选择 TKIP 和 CCMP。如果同时选择 TKIP 和 CCMP，配置为使用 WPA with RADIUS 的客户端工作站必须具有以下地址和密钥之一：
  - 有效的 TKIP RADIUS IP 地址和 RADIUS 密钥
  - 有效的 CCMP (AES) IP 地址和 RADIUS 密钥

- **Use Global RADIUS Server Settings** - 默认情况下，每个 VAP 都使用为 WAP 设备定义的全局 RADIUS 设置（请参阅 **RADIUS 服务器**）。但可以配置每个 VAP 以使用一组不同的 RADIUS 服务器。

  要使用全局 RADIUS 服务器设置，请确保选中此复选框。

  要对 VAP 使用单独的 RADIUS 服务器，请取消选中此复选框，然后在以下字段中输入 RADIUS 服务器的 IP 地址和密钥：

- **Server IP Address Type** - RADIUS 服务器使用的 IP 版本。

  可以在地址类型之间进行切换以配置 IPv4 和 IPv6 全局 RADIUS 地址设置，但 WAP 设备仅可连接 RADIUS 服务器或与此字段中所选地址类型对应的服务器。

- **Server IP Address 1** 或 **Server IPv6 Address 1** - 此 VAP 的主 RADIUS 服务器的地址。

  如果将 **IPv4** 选作 **Server IP Address Type**，请输入默认情况下所有 VAP 使用的 RADIUS 服务器的 IP 地址，例如 192.168.10.23。如果选择 **IPv6**，请输入主要的全局 RADIUS 服务器的 IPv6 地址，例如 2001:DB8:1234::abcd。

- **Server IP Address 2** 至 **4** 或 **Server IPv6 Address 2** 至 **4** - 最多 3 个 IPv4 和 / 或 IPv6 地址，用作此 VAP 的备份 RADIUS 服务器。

  如果没有通过主服务器的身份验证，将按顺序尝试每个已配置的备份服务器。

- **Key 1** - 全局 RADIUS 服务器的共享密钥。最多可以使用 63 个标准字母数字字符和特殊字符。密钥区分大小写，必须在 WAP 设备和 RADIUS 服务器上配置相同的密钥。输入的文本显示为星号，可防止他人看到键入的 RADIUS 密钥。

- **Key 2** 至 **Key 4** - 与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。**Server IP (IPv6) Address 2** 的服务器使用 **Key 2**， **Server IP (IPv6) Address 3** 的服务器使用 **Key 3**，以此类推。

- **Enable RADIUS Accounting** - 可以对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量等。

  如果启用 RADIUS 记帐，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。

- **Active Server** - 管理性地选择活动的 RADIUS 服务器，而不是由 WAP 设备尝试按顺序连接每个已配置的服务器和选择正在运行的第一个服务器。

  Broadcast Key Refresh Rate - 针对与此 VAP 关联的客户端刷新广播（组）密钥的间隔。

  默认值为 300 秒。有效范围介于 0 至 86400 秒之间。值 0 表示不刷新广播密钥。

- **Session Key Refresh Rate** - WAP 设备针对与此 VAP 关联的每个客户端刷新会话（单播）密钥的间隔。

  有效范围介于 0 至 86400 秒之间。值 0 表示不刷新会话密钥。

调度程序

无线和 VAP 调度程序可用来配置 VAP 的特定时间间隔规则或要使用的无线，从而自动启用或禁用 VAP 和无线。

要使用此功能，一种方法是仅在工作时间安排要运行的无线以实现安全性并减少功耗。还可以使用调度程序允许仅在一天中的特定时间访问无线客户端的 VAP。

WAP 设备最多支持 16 个简档。仅将有效规则添加到简档中。最多可以将 16 条规则组合在一起以构成一个调度简档。属于同一简档的周期时间条目不会重叠。

添加调度程序简档

最多可以创建 16 个调度程序简档名称。默认情况下，不创建任何简档。

要查看调度程序状态和添加调度程序简档，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **Scheduler**。

步骤 2 确保 **Administrative Mode** 处于启用状态。默认情况下，禁用此选项。

Scheduler Operational Status 区域显示调度程序的当前工作状态：

- **Status** - 调度程序的工作状态：状态包括 Up 和 Down。默认值为 Down。
- **Reason** - 调度程序工作状态的原因。可能的值包括：
  - IsActive - 管理性地启用调度程序。
  - ConfigDown - 运行状态为中断，因为全局配置已禁用。
  - TimeNotSet - 既未手动，也未通过 NTP 在 WAP 设备上设置时间。

步骤 3 要添加简档，请在 **Scheduler Profile Configuration** 文本框中输入简档名称，然后点击**添加**。简档名称最多可以包含 32 个字母数字字符。

配置调度程序规则

最多可以为一个简档配置 16 条规则。每条规则都会指定无线或 VAP 可以使用的启动时间、结束时间和星期几。这些规则本身具有周期性，每周可以重复使用。有效规则必须包含启动时间和结束时间的所有参数（星期几、小时和分钟）。规则之间不能存在冲突；例如，可以配置一个在每个工作日启动的规则，再配置一个在每个周末启动的规则，但无法配置一个每天启动的规则，再配置一个周末启动的规则。

要为简档配置规则，请执行以下步骤：

步骤 1 从 **Select a Profile Name** 列表中选择简档。

步骤 2 点击 **Add Rule**。

规则表中会显示新规则。

步骤 3 选中 **Profile Name** 旁边的框并点击**编辑**。

步骤 4 从 **Day of the Week** 菜单中选择规则的循环时间表。可以配置每天、每个工作日、每个周末（周六和周日）或一周中的任何一天启动的规则。

步骤 5 设置启动和结束时间：

- **Start Time** - 开始使用无线或 VAP 的时间。时间采用 HH:MM 24 小时格式。范围是 <00-23>:<00-59>。默认值为 00:00。
- End Time - 停止使用无线或 VAP 的时间。时间采用 HH:MM 24 小时格式。范围是 <00-23>:<00-59>。默认值为 00:00。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

注 调度程序简档必须与无线接口或 VAP 接口关联才会生效。请参阅**调度程序关联**页。

注 要删除规则，从 **Profile Name** 列中选择简档，然后点击**删除**。

调度程序关联

调度程序简档必须与无线局域网接口或 VAP 接口关联才会生效。默认情况下，不创建任何调度程序简档，也没有简档与任何无线或 VAP 关联。

仅一个调度程序简档可以与无线局域网接口或每个 VAP 接口关联。一个简档可以与多个 VAP 关联。如果删除与 VAP 或无线局域网接口关联的调度程序简档，也会删除相应的关联。

要将调度程序简档与无线局域网接口或 VAP 关联，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **Scheduler Association**。

步骤 2 对于无线局域网接口或 VAP，从 **Profile Name** 列表中选择简档。

Interface Operational Status 列显示当前是启用还是禁用接口。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

带宽利用率

通过 “带宽利用率”页配置在 WAP 设备禁止新客户端关联之前可使用的无线带宽。默认情况下，此功能为禁用状态。

要启用带宽利用率，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **Bandwidth Utilization**。

步骤 2 针对 **Bandwidth Utilization** 设置点击 **Enable**。

步骤 3 在 **Maximum Utilization Threshold** 框中输入在 WAP 设备禁止新客户端关联之前无线中允许的网络带宽利用百分比。

有效的整数范围介于 0 至 100% 之间。默认值为 70%。如果设置为 0，无论利用率为多少，都将允许所有新的关联。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

MAC 过滤

媒体接入控制 (MAC) 过滤可用于仅排除或允许列出的客户端工作站通过接入点进行验证。在**网络**页依据 VAP 启用和禁用 MAC 验证。根据 VAP 的配置方式， WAP 设备可能会参照外部 RADIUS 服务器中存储的 MAC 过滤器列表或在 WAP 设备中本地存储的 MAC 过滤器列表。

在 WAP 设备中本地配置 MAC 过滤器列表

WAP 设备仅支持一个本地 MAC 过滤器列表，即此同一列表适用于能使用本地列表的所有 VAP。可以配置过滤器，仅访问列表中的 MAC 地址或仅拒绝访问列表中的 MAC 地址。

最多可以将 512 个 MAC 地址添加到过滤器列表中。

要配置 MAC 过滤，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **MAC Filtering**。

步骤 2 选择 WAP 设备使用过滤器列表的方式：

- **Allow only stations in the list** - 拒绝不在 Stations List 中的任何工作站通过 WAP 设备访问网络。
- **Block all stations in list** - 仅拒绝该列表中出现的工作站通过 WAP 设备访问网络。允许所有其他工作站访问。

  注 过滤器设置还适用于 RADIUS 服务器上存储的 MAC 过滤器列表 （ 如果存在 ）。

步骤 3 在 **MAC Address** 字段中，输入允许或阻止的 MAC 地址，然后点击**添加**。

MAC 地址出现在 **Stations List** 中。

步骤 4 在此列表完成前一直输入 MAC 地址，然后点击**保存**。更改将保存到 Startup Configuration。

注 要从 Stations List 中删除 MAC 地址，请选中相应地址，然后点击 **Remove**。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

在 RADIUS 服务器上配置 MAC 验证

如果配置一个或多个 VAP 以使用在 RADIUS 身份验证服务器上存储的 MAC 过滤器，必须在 RADIUS 服务器上配置工作站列表。列表的格式如下表所述：

RADIUS 服务器属性	说明	值
User-Name (1)	客户端工作站的 MAC 地址。	有效的以太网 MAC 地址。
User-Password (2)	用于查找客户端 MAC 条目的固定全局密码。	NOPASSWORD

WDS 网桥

无线分布式系统 (WDS) 可用来连接多个 WAP121 和 WAP321 设备。通过 WDS，接入点可以彼此进行无线通信。在为漫游客户端和多个无线网络的管理提供无缝体验时，此功能非常重要。此功能还可以通过减少所需的布线量简化网络基础设施。可以基于要连接的链路数量在点对点或点对多点桥接模式下配置 WAP 设备。

在点对点模式下， WAP 设备接受客户端关联并与无线客户端和其他中继器通信。WAP 设备通过在接入点之间建立的隧道转发要发送给其他网络的所有流量。此网桥不添加到步跳数中，可用作简单的第 2 层 OSI 网络设备。

在点对多点桥接模式下，一个 WAP 设备可用作多个接入点之间的通用链路。在此模式下，中心 WAP 设备可接受客户端关联并与客户端和其他中继器通信。所有其他接入点仅与中心 WAP 设备关联，然后中心 WAP 设备将数据包转发到相应的无线网桥以进行路由。

WAP 设备 还可用作中继器。在此模式下， WAP 设备 用作两个可能相隔太远以致超出信元范围的 WAP 设备 之间的连接。用作中继器时， WAP 设备 没有到局域网的有线连接，通过无线连接重复发送信号。WAP 设备用作中继器时不需要特殊配置，因此没有中继器模式设置。无线客户端仍可以连接到用作中继器的 WAP 设备。

在 WAP 设备上配置 WDS 之前，请注意以下准则：

- WDS 仅适用于思科 WAP121 和思科 WAP321 设备。
- 所有加入 WDS 链路的思科 WAP 设备必须拥有以下相同设置：
  - Radio
  - IEEE 802.11 Mode

- 信道带宽
- Channel（不建议使用 Auto 模式）

注 在 802.11n 2.4 GHz 频段中进行桥接时，将 Channel Bandwidth 设置为 20 MHz，而不是默认值 20/40 MHz。在 2.4 GHz 20/40 MHz 频段中，如果在此区域中检测到任何 20 MHz WAP 设备，工作带宽可以从 40 MHz 更改为 20 MHz。信道带宽不匹配会导致链路断开。

有关配置这些设置的详情，请参阅**无线**（基本设置）。

- 使用 WDS 时，务必在加入 WDS 链路的两个 WAP 设备上都配置 WDS。
- 在任何 WAP 设备对之间仅可以有一个 WDS 链路。即远程 MAC 地址在特定 WAP 设备的 WDS 页上可能仅出现一次。

要配置 WDS 网桥，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **WDS Bridge**。

步骤 2 对 **Spanning Tree Mode** 选择 **Enable**。启用后， STP 可以帮助阻止交换环路。如果配置 WDS 链路，建议使用 STP。

步骤 3 对 **WDS Interface** 选择 **Enable**。

步骤 4 配置其余参数：

- **Remote MAC Address** - 指定目标 WAP 设备的 MAC 地址，即收发或传输数据的 WDS 链路另一端的 WAP 设备。

提示 可以在 Status and Statistics > Network Interface 页中找到此 MAC 地址。

- **Encryption** - WDS 链路中使用的加密类型，无需与桥接的 VAP 匹配。对于 WDS 网桥， WDS Encryption 设置是唯一的。其选项包括 None、 WEP 和 WPA Personal。

  如果不担心会遇到有关 WDS 链路的安全问题，可以决定不设置任何类型的加密。或者，如果担心安全问题，可以选择 Static WEP 或 WPA Personal。在 WPA Personal 模式下， WAP 设备对整个 WDS 链路使用 WPA2-PSK with CCMP (AES) 加密。有关加密选项的详情，请参阅此过程之后的 **WDS 链路中的 WEP** 或 **WDS 链路中的 WPA/PSK**。

步骤 5 最多对另外 3 个 WDS 接口重复上述步骤。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

步骤 7 对另一个设备或连接到网桥的设备重复此过程。

提示 可以通过转至 Status and Statistics > Network Interface 页验证桥接链路是否正在运行。在 Interface Status 表中， WLAN0:WDS(x) 的状态应为 Up。

注意 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

WDS 链路中的 WEP

选择 WEP 作为加密类型时，会显示以下更多字段。

- **Key Length** - 如果启用 WEP，将 WEP 密钥长度指定为 **64 位**或 **128 位**。
- **Key Type** - 如果启用 WEP，请指定 WEP 密钥类型：**ASCII** 或 **Hex**。
- **WEP Key** - 如果选择 **ASCII**，请输入 0 至 9、 a 至 z 以及 A 至 Z 的任意组合。如果选择 **Hex**，请输入十六进制数字（ 0 至 9 和 a 至 f 或 A 至 F 的任意组合）。这些 RC4 加密密钥可以与使用 WAP 设备的工作站共享。

  请注意，必需的字符数会显示在此字段右边，并基于 **Key Type** 和 **Key Length** 字段中的选择而改变。

WDS 链路中的 WPA/PSK

选择 WPA/PSK 作为加密类型时，会显示以下更多字段。

- **WDS ID** - 为已创建的新 WDS 链路输入合适的名称。还必须在 WDS 链路的另一端输入相同的 WDS ID。如果对于 WDS 链路中的两个 WAP 设备，此 WDS ID 不相同，它们之间将不能通信和交换数据。

  WDS ID 可以是任何字母数字的组合。

- **Key** - 为 WDS 网桥输入唯一的共享密钥。还必须为 WDS 链路另一端的 WAP 设备输入此唯一的共享密钥。如果对于两个 WAP，此密钥不相同，它们之间将不能通信和交换数据。

  WPA-PSK 密钥是最少为 8 个字符、最多为 63 个字符的字符串。可接受的字符包括大写和小写字母、数字以及特殊字符（例如 @ 和 # ）。

工作组网桥

通过 WAP 设备 的工作组网桥功能， WAP 设备可以扩展远程网络的可访问性。在 WorkGroup Bridge 模式下， WAP 设备 可以用作无线局域网中的无线工作站 (STA)。它可以在远程有线网络或关联无线客户端与使用 WorkGroup Bridge 模式连接的无线局域网之间桥接流量。

工作组网桥功能同时支持 STA 模式和 AP 模式运行。WAP 设备可以在一个基本服务集 (BSS) 中作为 STA 设备运行，而在另一个 BSS 中作为 WAP 设备 运行。如果启用 WorkGroup Bridge 模式， WAP 设备 仅支持与其关联的无线客户端的一个 BSS 以及 WAP 设备作为无线客户端关联的另一个 BSS。

建议仅在 WDS 网桥功能无法用于对等 WAP 设备 时使用 WorkGroup Bridge 模式。WDS 是一个更好的解决方案，优先于工作组网桥解决方案。如果桥接思科 WAP121 和 WAP321 设备，请使用 WDS。否则请考虑使用工作组网桥。如果启用工作组网桥功能，则不会应用 VAP 配置，仅应用工作组网桥配置。

注 在 WAP 设备 中启用 WorkGroup Bridge 模式时， WDS 功能将无法工作。

在 WorkGroup Bridge 模式下， WAP 设备管理的 BSS 在 WAP 设备模式下运行时称为接入点接口，关联的 STA 称为下游 STA。另一个 WAP 设备 （ 即与作为 STA 的 WAP 设备关联的设备 ）管理的 BSS 称为基础设施客户端接口，而另一个 WAP 设备 称为上游 AP。

连接到 WAP 设备有线接口的设备以及与此设备的接入点接口关联的下游工作站可以访问通过基础设施客户端接口连接的网络。为了能够桥接数据包，接入点接口和有线接口的虚拟局域网配置应与基础设施客户端接口的虚拟局域网配置匹配。

WorkGroup Bridge 模式可以用作范围扩展器，确保 BSS 可以提供对远程或难以访问的网络的访问权限。可以配置单频以便将数据包从关联的 STA 转发到同一 ESS 中的另一个 WAP 设备，而无需使用 WDS。

在 WAP 设备上配置工作组网桥之前，请注意以下准则：

- 所有加入工作组网桥的 WAP 设备必须拥有以下相同设置：
  - Radio
  - IEEE 802.11 Mode
  - 信道带宽
  - Channel （ 不建议使用 Auto 模式 ）

  有关配置这些设置的详情，请参阅**无线** （ 基本设置 ）。
- WorkGroup Bridge 模式当前仅支持 IPv4 流量。

- 单点设置中不支持 WorkGroup Bridge 模式。

要配置 WorkGroup Bridge 模式，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **WorkGroup Bridge**。

步骤 2 对 **WorkGroup Bridge Mode** 选择 **Enable**。

步骤 3 为基础设施客户端接口（上游）配置以下参数：

- **SSID** - BSS 的 SSID。

  注 SSID for SSID Scanning 旁边有一个箭头，此功能在默认情况下禁用，仅在 Rogue AP Detection 中的 AP Detection（该功能在默认情况下也禁用）启用时启用。

- **Security** - 用于作为上游 WAP 设备中的客户端工作站进行身份验证的安全类型。选项有：
  - **None**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise**

  有关 WEP 和 WPA Personal 安全设置的详情，请参阅**配置安全设置**。

- **VLAN ID** - 与 BSS 关联的虚拟局域网。

  注 基础设施客户端接口将通过已配置的凭据与上游 WAP 设备进行关联。WAP 设备可以从上行链路的 DHCP 服务器中获取其 IP 地址。或者，也可以指定一个静态 IP 地址。**Connection Status** 字段表示 WAP 是否连接到上游 WAP 设备。可以点击此页顶部的 **Refresh** 按钮以查看最新的连接状态。

步骤 4 为接入点接口配置以下更多的字段：

- **Status** - 对于接入点接口选择 **Enable**。
- **SSID** - 接入点接口的 SSID 无需与基础设施客户端 SSID 相同。但如果尝试支持漫游类型的方案， SSID 和安全性必须相同。
- **SSID Broadcast** - 选择是否要广播下游 SSID。默认情况下，启用 SSID Broadcast。
- **Security** - 用于身份验证的安全类型。选项有：
  - **None**

- **Static WEP**
- **WPA Personal**

- **MAC Filtering** - 请选择以下选项之一：
  - **Disabled** - 可访问上游网络的 AP BSS 中的客户端组并不仅限于 MAC 地址列表中指定的客户端。
  - **Local** - 可访问上游网络的 AP BSS 中的客户端组仅限于本地定义的 MAC 地址列表中指定的客户端。
  - **RADIUS** - 可访问上游网络的 AP BSS 中的客户端组仅限于 RADIUS 服务器上的 MAC 地址列表中指定的客户端。

  如果选择 Local 或 RADIUS，请参阅 **MAC 过滤**了解创建 MAC 过滤器列表的说明。
- **VLAN ID** - 使用与基础设施客户端接口中通告的相同 VLAN ID 配置接入点接口。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

关联的下游客户端现在可连接到上游网络。

服务质量

服务质量 (QoS) 设置可提供在处理差异化的无线流量（例如 IP 电话 (VoIP)、其他类型的音频、视频、流媒体和传统的 IP 数据）时配置传输队列的功能，进而优化吞吐量和提高性能。

要在 WAP 设备 中配置 QoS，请为不同类型的无线流量设置有关传输队列的参数，并指定最小和最大传输等待时间（通过争用窗口）。

WAP 增强型分布式信道接入 (EDCA) 参数会影响从 WAP 设备流向客户端工作站的流量。

工作站 EDCA 参数会影响从客户端工作站流向 WAP 设备的流量。

正常使用情况下， WAP 设备和工作站 EDCA 的默认值无需更改。更改这些值会影响提供的 QoS。

要配置 WAP 设备和工作站 EDCA 参数，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **QoS**。

步骤 2 从 **EDCA Template** 列表中选择一个选项：

- **WFA Defaults** - 用 WiFi 联盟默认值（最适合一般的混合流量）填充 WAP 设备和工作站 EDCA 参数。
- **Optimized for Voice** - 用最适合语音流量的值填充 WAP 设备和工作站 EDCA 参数。
- **Custom** - 可用来选择自定义的 EDCA 参数。

下面 4 个队列是为从 WAP 传输至工作站的不同类型的数据定义的。如果选择 Custom 模板，可以配置用于定义队列的参数，否则将这些参数设置为适合所选内容的预定义值。这 4 个队列为：

- Data 0 (Voice) - 高优先级队列，延迟最短。会将 VoIP、流媒体等时效性强的数据自动发送到此队列中。
- Data 1 (Video) - 高优先级队列，延迟最短。会将时效性强的视频数据自动发送到此队列中。
- Data 2 (Best Effort) - 中优先级队列，中等吞吐量和延迟。会将大多数的传统 IP 数据发送到此队列中。
- Data 3 (Background) - 最低优先级的队列，吞吐量较高 。会将需要最大吞吐量并且时效性不强的批量数据（例如 FTP 数据）发送到此队列中。

步骤 3 配置以下 EDCA 和工作站 EDCA 参数：

注 仅在上一步选择 Custom 时才可以配置这些参数。

- **Arbitration Inter-Frame Space** - 数据帧的等待时间。等待时间用时槽计算。AIFS 的有效值是 1 到 255。
- **Minimum Contention Window** - 输入用于确定重试传输的初始随机退避等待时间（窗口）的算法。

  此值是确定初始随机退避等待时间所处范围的上限（毫秒）。

  生成的第一个随机数是介于 0 和此处指定的数字之间的一个数。

  如果第一个随机退避等待时间在数据帧发送之前过期，则重试计数递增，而随机退避值（窗口）加倍。在随机退避值的大小达到 Maximum Contention Window 中定义的数字之前，此值会一直成倍增加。

有效值为 1、3、7、15、31、63、127、255、511 或 1024。此值必须小于 Maximum Contention Window 的值。

- **Maximum Contention Window** - 随机退避值成倍增加的上限（毫秒）。在发送数据帧或达到 Maximum Contention Window 大小之前，此值会一直成倍增加。

  达到 Maximum Contention Window 大小后，将一直重试，直至达到允许的最大重试次数。

  有效值为 1、3、7、15、31、63、127、255、511 或 1024。此值必须大于 Minimum Contention Window 的值。

- **Maximum Burst** (WAP only) - 仅适用于从 WAP 流向客户端工作站的流量的 WAP EDCA 参数。

  此值指定无线网络中数据包突发所允许的最大突发长度（毫秒）。数据包突发是多个传输的帧的集合，没有报头信息。开销的减少会提高吞吐量和改进性能。

  有效值为 0.0 到 999。

- **Wi-Fi MultiMedia (WMM)** - 选择 **Enable** 以启用 Wi-Fi MultiMedia (WMM) 扩展。默认情况下，启用此字段。启用 WMM 后，会启用无线媒体接入的 QoS 优先级和协调。启用 WMM 后， WAP 设备 中的 QoS 设置可以控制从 WAP 设备流向客户端工作站（AP EDCA 参数）的下行流量以及从客户端工作站流向 AP（工作站 EDCA 参数）的上行流量。

  禁用 WMM 会停用从客户端工作站流向 WAP 设备的上行流量的工作站 EDCA 参数的 QoS 控制。禁用 WMM 后，仍可以设置有关从 WAP 设备流向客户端工作站（AP EDCA 参数）的下行流量的一些参数。

- **TXOP Limit** (Station only) - TXOP Limit 是一个工作站 EDCA 参数，仅适用于从客户端工作站流向 WAP 设备的流量。传输机会 (TXOP) 是在 WME 客户端工作站有权启动通过无线媒体 (WM) 传输到 WAP 设备时的时间间隔（毫秒）。TXOP Limit 的最大值是 65535。

步骤 4 配置以下更多设置：

- **No Acknowledgement** - 选择 **Enable** 以指定 WAP 设备不应将具有 QosNoAck 的帧确认为服务等级值。
- **Unscheduled Automatic Power Save Delivery** - 选择 **Enable** 以启用作为电源管理方法的 APSD（自动省电发送）。如果 VoIP 电话通过 WAP 设备访问网络，建议使用 APSD。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

注意 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

WPS 设置

本节介绍 WAP 设备中 Wi-Fi 保护设置 (WPS) 协议及其配置。

WPS 概述

WPS 是用于简单建立无线网络而不会影响网络安全性的标准。通过此标准，无线客户端用户和 WAP 设备管理员无需知道网络名称、密钥和其他不同的加密配置选项。

WPS 通过允许管理员使用按钮或 PIN 建立无线网络方便网络设置，可以避免手动输入网络名称 (SSID) 和无线安全参数。

- **按钮**：WPS 按钮在产品上或是用户界面上的可点击按钮。
- **个人标识号 (PIN)**：可以在产品的用户界面中查看 PIN。

通过要求新客户端设备的用户和无线局域网管理员拥有对各自设备的物理访问权限或安全的远程访问权限， WPS 可保持网络安全性。

使用方案

以下是典型的 WPS 使用方案：

- 用户想要在已启用 WPS 的无线局域网中注册客户端工作站。（注册的客户端设备可能会检测网络并提示用户进行注册，尽管这一过程并非必需。）用户按下客户端设备上的按钮即可触发注册。此时， WAP 设备管理员可按下 WAP 设备上的按钮。在简短的 WPS 协议消息交换期间， WAP 设备可通过可扩展身份验证协议 (EAP) 为新客户端提供新的安全配置。这两个设备取消关联，然后重新关联并通过新设置进行身份验证。
- 用户想要通过向 WAP 设备管理员提供客户端设备的 PIN，在已启用 WPS 的无线局域网中注册客户端工作站。管理员在 WAP 设备的配置实用程序中输入此 PIN，然后触发设备注册。新注册的设备与 WAP 设备交换 WPS 消息，包括新的安全配置、取消关联、重新关联和身份验证。

- WAP 设备管理员购买已经过 Wi-Fi 联盟认证并与 WPS 2.0 版本兼容的新 WAP 设备，想要将该设备添加到现有（有线或无线）网络中。管理员打开 WAP 设备，然后访问支持 WPS 注册协议的网络主机。管理员在此外部寄存器的配置实用程序中输入 WAP 设备的 PIN，然后触发 WPS 注册过程。（在有线局域网中，通过通用即插即用 (UPnP) 协议传输 WPS 协议消息。）主机将 WAP 作为新网络设备注册，并通过新安全设置配置 WAP。
- WAP 设备管理员刚刚通过 WPS 将新的 WAP 设备添加到现有（无线或有线）网络中，想要授予对新客户端设备的网络访问权限。设备可通过上述的 PIN 或按钮控制 (PBC) 方法注册，但这次设备是通过外部寄存器使用独自作为代理的 WAP 设备注册的。
- 不支持 WPS 的无线设备必须加入已启用 WPS 的无线局域网。管理员在这种情况下无法使用 WPS，而要通过已启用 WPS 的 WAP 设备的 SSID、公共共享密钥和密码模式手动配置设备。设备加入网络。

PIN 是将最后一位数用作校验和值的八位数或无校验和的四位数。这些数字中的每位数可能都包含前导零。

WPS 角色

WPS 标准为其架构中的不同组成部分分配特定角色：

- **Enrollee** - 可以加入无线网络的设备。
- **AP** - 提供无线接入网络的设备。
- **Registrar** - 颁发注册设备的安全凭据和配置 AP 的实体。

WAP 设备可以用作 AP 设备，支持内置寄存器。它们不能用作注册设备。

在 VAP 中启用和禁用 WPS

管理员可以仅在一个 VAP 中启用或禁用 WPS。 WPS 仅在此 VAP 满足以下条件时可以使用：

- 将 WAP 设备配置为广播 VAP SSID。
- 在 VAP 中禁用 MAC 地址过滤。
- 在 VAP 中禁用 WEP 加密。
- 将 VAP 配置为使用 WPA-Personal 安全或 None。如果启用 WPA2-PSK 加密模式，则必须配置有效的预先共享密钥 (PSK) 并且必须启用 CCMP (AES) 加密。
- 操作性地启用 VAP。

如果不满足上述任一条件，即操作性地禁用 WPS。

注 在 VAP 中禁用 WPS 并不会取消关联以前通过该 VAP 中 WPS 进行身份验证的任何客户端。

外部和内部注册

WAP 设备无需自己处理客户端在网络中的注册。 WAP 设备可以使用其内置寄存器或用作外部寄存器的代理。可以通过有线或无线局域网访问外部寄存器。外部寄存器可能还会配置已启用 WPS 的 BSS 的 SSID、加密模式和公共共享密钥。此功能对现成部署非常有用，即管理员首次仅将新的 WAP 设备连接到局域网时。

如果 WAP 设备 使用内置寄存器，无论是直接在 WAP 设备上配置还是由外部寄存器通过 WPS 获得与 WPS 服务关联的 VAP 的配置， WAP 设备都会使用该配置注册新的客户端。

客户端注册

按钮控制

WAP 设备 使用以下两种方法之一通过 WPS 注册 802.11 客户端：按钮控制 (PBC) 方法或个人标识号 (PIN) 方法。

PBC 方法是指潜在客户端的用户按下注册设备上的按钮后，以及已启用内置寄存器的 WAP 设备的管理员按下类似（硬件或软件）按钮后进行注册的方法。此顺序从注册过程开始，然后客户端设备加入网络。虽然思科 WAP 设备不支持实际的硬件按钮，但管理员可以使用基于 Web 的配置实用程序中的软件按钮启动特定 VAP 的注册。

注 没有对按下客户端设备和 WAP 设备上的按钮顺序进行规定。任一设备都可以启动注册。但如果按下 WAP 设备 上的软件按钮，而任何客户端在 120 秒之后没有尝试注册， WAP 设备 会终止挂起的 WPS 注册事务处理。

PIN 控制

客户端还可能会使用 PIN 通过寄存器注册。例如， WAP 设备 管理员可能会通过输入客户端的 PIN 为特定 VAP 启动注册事务处理。客户端检测到已启用 WPS 的设备时，用户可以向 WAP 设备 提供其 PIN 以继续注册过程。WPS 协议完成后，客户端即可安全加入网络。客户端也可以启动此过程。

和 PBC 方法一样，如果 WAP 设备 开始注册事务处理，而任何客户端在 120 秒之后没有尝试注册， WAP 设备 也会终止挂起的事务处理。

（可选）使用内置寄存器

虽然 WAP 设备 支持 WPS 的内置寄存器，但该用法是可选的。外部寄存器配置 WAP 设备 后，无论是否启用 WAP 设备的内置寄存器（默认情况下启用）， WAP 设备 都可以用作该外部寄存器的代理。

锁定功能

每个 WAP 设备 都会在非易失性随机存取存储器 (NVRAM) 中存储一个兼容 WPS 的设备 PIN。如果管理员想要允许未配置的 WAP 设备 （ 即仅具有出厂默认设置的设备，包括在 VAP 中启用的 WPS ）加入网络，则 WPS 需要使用此 PIN。在这种情况下，管理员可从 WAP 设备 的配置实用程序中获取 PIN 值。

如果网络完整性在某种程度上已受到破坏，则管理员可能会希望更改 PIN。WAP 设备会提供一种方法，用于生成新的 PIN 并将此值存储在 NVRAM 中。如果 NVRAM 中的值受到破坏、擦除或丢失， WAP 设备 会生成的新 PIN 并将其存储在 NVRAM 中。

用于注册的 PIN 方法在遇到暴力破解时可能比较脆弱。网络入侵者会尝试伪装成无线局域网中的外部寄存器，然后极力应用兼容 WPS 的 PIN，企图获得 WAP 设备的 PIN 值。要解决这个漏洞，如果寄存器在 60 秒内尝试 3 次都未能提供正确的 PIN， WAP 设备 将禁止外部寄存器在接下来 60 秒进一步尝试在已启用 WPS 的 VAP 中通过 WAP 设备 进行注册。锁定持续时间会随着后续尝试失败而增加，最长为 64 分钟。 WAP 设备的注册功能在连续 10 次尝试失败后进入永久锁定状态。重置设备以重新启动注册功能。

但在此锁定期间，无线客户端工作站可能会通过 WAP 设备 的内置寄存器 （ 如果启用 ）注册。 WAP 设备 还会继续为外部寄存器的注册请求提供代理服务。

WAP 设备 可提供更多的安全功能以保护其设备 PIN。 WAP 设备 通过外部寄存器完成注册并且由此产生的 WPS 事务处理结束后，设备 PIN 会自动重新生成。

VAP 配置更改

WPS 协议可以在 WAP 设备中为已启用 WPS 的 VAP 配置以下参数：

- 网络 SSID
- 密钥管理选项 （ WPA-PSK，或 WPA-PSK 和 WPA2-PSK ）
- 密码选项 （ CCMP/AES，或 TKIP 和 CCMP/AES ）
- 网络 （ 公共共享 ）密钥

如果对 WPS 启用了 VAP，这些配置参数可以更改，并且在 WAP 设备重新启动之后保持不变。

外部注册

WAP 设备 支持在有线和无线局域网中通过 WPS 外部寄存器 (ER) 进行注册。在无线局域网中，外部寄存器在信标帧的特定 WPS 信息单元 (IE) 内通告其功能；在有线局域网中，外部寄存器通过 UPnP 宣布其存在。

WPS v2.0 不需要通过用户界面使用 ER 注册。管理员可以通过以下方法使用 ER 注册 WAP 设备：

步骤 1 在 WAP 设备中输入 ER PIN。

步骤 2 在 ER 的用户界面中输入 WAP 设备 PIN。

注 如果 WAP 设备 已在其需要此类配置的信标帧的特定 WPS IE 或 UPnP 消息内声明，注册过程还可以按照 VAP Configuration Changes 部分的规定配置 WAP 设备。

WAP 设备 最多可以同时用作 3 个外部寄存器的代理。

WPS 事务处理的互斥操作

可以为 WPS 启用 WAP 设备 中的任何一个 VAP。在 WAP 设备 中，一次至多可以执行一个 WPS 事务处理（例如， 802.11 客户端的注册和关联）。 WAP 设备 管理员可以从 基于 Web 的配置实用程序 中终止正在执行的事务处理。但不应在事务处理期间更改 VAP 的配置，也不应在身份验证过程中更改 VAP。建议采纳这一限制，但不强制在 WAP 设备 中执行。

与 WPS 1.0 版本的向后兼容性

虽然 WAP 设备支持 WPS 2.0 版本，但 WAP 设备 可以与经过 Wi-Fi 联盟认证、符合 WPS 协议 1.0 版本的注册设备和寄存器进行互操作。

配置 WPS 设置

可以通过 WPS Setup 页启用作为支持 WPS 设备的 WAP 设备 并配置基本设置。如果准备使用此功能注册新设备或将 WAP 设备 添加到已启用 WPS 的网络中，请使用 **WPS 过程**页。

注意 出于安全原因，建议（而不是必须）在配置 WPS 时使用到 基于 Web 的配置实用程序 的 HTTPS 连接。

要将 WAP 设备 配置为支持 WPS 的设备，请执行以下步骤：

步骤 1 在导航窗格中选择 **Wireless** > **WPS Setup**。

WPS Setup 页显示全局参数和状态以及 WPS 实例的参数和状态。实例是与网络中的 VAP 关联的 WPS 的实施。 WAP 设备 仅支持一个实例。

步骤 2 配置全局参数：

- **Supported WPS Version** - WAP 设备 支持的 WPS 协议版本。
- **WPS Device Name** - 提供默认的设备名称。可以指定介于 1 至 32 个字符之间的不同名称，包含空格和特殊字符。
- **WPS Global Operational Status** - WPS 协议在 WAP 设备 上的状态是启用还是禁用。默认情况下，此功能处于启用状态。
- **WPS Device PIN** - 系统生成的 WAP 设备 的 8 位 WPS PIN。管理员可能会使用此生成的 PIN 通过外部寄存器注册 WAP 设备。

  可以点击 **Generate** 以生成新的 PIN。如果网络完整性已受到破坏，建议生成新的 PIN。

步骤 3 配置 WPS 实例的参数：

- **WPS Instance ID** - 实例的标识符。由于仅有一个实例，唯一选项就是 wps1。
- **WPS Mode** - 启用或禁用实例。
- **WPS VAP** - 与此 WPS 实例关联的 VAP。
- **WPS Built-in Registrar** - 启用内置寄存器功能。启用后，注册设备（通常是无线局域网客户端）可以通过 WAP 设备注册。如果禁用该功能， WAP 设备中的寄存器功能会关闭，并且注册设备需要通过网络中的另一寄存器注册。在这种情况下，网络中的另一设备可以用作寄存器，而 WAP 设备则用作转发客户端注册请求和寄存器响应的代理。
- **WPS Configuration State** - 指定是否在 WPS 过程中从外部寄存器配置 VAP。可以将该选项设置为以下值之一：
  - **Unconfigured** - 使用 WPS 配置 VAP 设置，然后状态将更改为 Configured。
  - **Configured** - 外部寄存器没有配置 VAP 设置，这些设置将保留现有配置。

步骤 4 点击 **Update**。更改将保存到 Startup Configuration。

会出现实例的工作状态及其原因。有关可能会使实例禁用的条件的详情，请参阅 “在 VAP 中启用或禁用 WPS”。

实例状态

Instance Status 区域显示以下有关所选 WPS 实例的信息：

- **WPS Operational Status** - 是否运行 WPS 实例。
- **AP Lockdown Status** - AP 是否处于锁定模式下，在此模式下会阻止外部寄存器通过 AP 注册。在锁定状态下，无论锁定是临时还是永久，此字段都会报告锁定的开始时间，如果是临时锁定，还会报告锁定期的持续时间。如果不是锁定模式，则状态显示为 **Disabled**。
- **Failed Attempts with Invalid PIN** - 外部寄存器尝试通过 WAP 设备进行注册但失败的次数。

在锁定状态下，显示以下字段：

- **AP Lockdown Duration** - WAP 的锁定持续时间（分钟）。如果 WAP 永久锁定，此值设置为 – 1。
- **AP Lockdown Timestamp** - WAP 设备锁定的时间。

可以点击 **Refresh** 用最新的状态信息更新页面。

WPS 过程

可以通过 WPS Process 页使用 WPA 在网络中注册客户端工作站。如果客户端工作站支持 PIN 或按钮方法，可以使用这些方法注册客户端。

使用 PIN 方法注册客户端

要使用 PIN 方法注册客户端工作站，请执行以下步骤：

步骤 1 从客户端设备获取 PIN。 PIN 可能打印在硬件上或从设备的软件界面中获取。

步骤 2 在导航窗格中选择 **Wireless** > **WPS Process**。

步骤 3 在 **PIN Enrollment** 文本框中输入客户端的 PIN，然后点击 **Start**。

步骤 4 在 2 分钟内，在客户端设备的软件界面中输入 WAP PIN。 WAP PIN 可在 **WPS 设置** 页中配置。

在客户端设备中输入 PIN 时， WPS Operational Status 更改为 Adding Enrollee。注册过程完成后，WPS Operational Status 更改为 Ready，Transaction Status 更改为 Success。

注册客户端时， WAP 设备的内置寄存器或网络中的外部寄存器继续通过已启用 WPS 的 BSS 的 SSID、加密模式和公共共享密钥来配置客户端。

注意 也可以反向执行此注册顺序，即或许可以通过输入 WAP 设备的 PIN 在客户端工作站中启动该过程。但出于安全原因，**不建议**使用此方法，因为客户端可使用此方法在 AP 中配置 SSID 和安全设置。管理员不应仅与受信任的设备共享 PIN。

使用按钮方法注册客户端

要使用按钮方法注册客户端工作站，请执行以下步骤：

步骤 1 点击 **PBC Enrollment** 旁边的 **Start**。

步骤 2 按下客户端工作站上的硬件按钮。

注 或者，也可以在客户端工作站上启动此过程，然后点击 WAP 设备中的 PBC Enrollment Start 按钮。

按下客户端工作站上的按钮时， WPS Operational Status 更改为 Adding Enrollee。注册过程完成后， WPS Operational Status 更改为 Ready， Transaction Status 更改为 Success。

注册客户端时， WAP 设备的内置寄存器或网络中的外部寄存器继续通过已启用 WPS 的 BSS 的 SSID、加密模式和公共共享密钥来配置客户端。

查看实例状态信息

Instance Status 部分显示以下在 **WPS Instance ID** 列表中所选的 WPS 实例的信息：

- **WPS Status** - 是启用还是禁用所选的 WPS 实例。
- **WPS Configuration State** - 是否会在 WPS 过程中从外部寄存器配置 VAP。

- **Transaction Status** - 最后的 WPS 事务处理的状态。可能的值包括 None、Success、 WPS Message Error 和 Timed Out。
- **WPS Operational Status** - 当前或最近 WPS 事务处理的状态。可能的值包括 Disabled、Ready、Configuring、Proxying 和 Adding Enrollee。如果自启用 WPS 后未发生任何 WPS 事务处理，则会显示 Ready。
- **AP Lockdown Status** - 当前实例是否处于锁定状态。
- **Failed Attempts with Invalid PIN** - 由于密码无效而导致尝试验证外部寄存器失败的次数。

查看实例摘要信息

WPS 实例的信息如下所示：

- **WPS Radio**
- **WPS VAP**
- **SSID**
- **Security**

如果 WPS Setup 页中的 WPS Configuration State 字段设置为 Unconfigured，则由外部寄存器配置 SSID 和 Security 值。如果该字段设置为 Configured，则由管理员配置这些值。

注 可以点击 **Refresh** 用最新的状态信息更新页面。

6

系统安全

本章介绍如何在 WAP 设备 中配置安全设置。

具体包括以下主题：

- **RADIUS 服务器**
- **802.1X 请求方**
- **密码复杂性**
- **WPA-PSK 复杂性**

RADIUS 服务器

多个功能需要与 RADIUS 身份验证服务器进行通信。例如，在 WAP 设备 中配置虚拟接入点 (VAP) 时，可以配置用于控制无线客户端访问的安全方法（请参阅**无线**页）。“动态 WEP（有线等效保密）和 WPA（Wi-Fi 安全访问）企业”安全方法使用外部 RADIUS 服务器对客户端进行身份验证。MAC（媒体接入控制）地址过滤功能还可以配置为使用 RADIUS 服务器控制访问，其中客户端访问仅限于列表范围内。强制网络门户功能也可使用 RADIUS 对客户端进行身份验证。

可以使用 Radius Server 页配置这些功能使用的 RADIUS 服务器。最多可以配置 4 个全局可用的 IPv4 或 IPv6 RADIUS 服务器，但必须选择对于全局服务器的 RADIUS 客户端是否可以在 IPv4 或 IPv6 模式下工作。其中一个服务器始终用作主服务器，其他服务器则可以充当备份服务器。

注 除了使用全局 RADIUS 服务器，还可以配置每个 VAP（虚拟接入点）以使用特定的 RADIUS 服务器组。请参阅**网络**页。

要配置全局 RADIUS 服务器，请执行以下步骤：

步骤 1 在导航窗格中选择 **Security** > **RADIUS Server** 。

步骤 2 输入以下参数：

- **Server IP Address Type** - RADIUS 服务器使用的 IP 版本。

可以在地址类型之间进行切换以配置 IPv4 和 IPv6 全局 RADIUS 地址设置，但 WAP 设备仅可连接 RADIUS 服务器或与此字段中所选地址类型对应的服务器。

- **Server IP Address 1** 或 **Server IPv6 Address 1** - 主全局 RADIUS 服务器的地址。

  第一个无线客户端尝试通过 WAP 设备进行身份验证时， WAP 设备向主服务器发送身份验证请求。如果主服务器响应身份验证请求， WAP 设备继续将此 RADIUS 服务器用作主服务器，身份验证请求也会发送至指定的地址。

- **Server IP Address**（**2** 至 **4**）或 **Server IPv6 Address**（**2** 至 **4**）- 最多 3 个 IPv4 或 IPv6 备份 RADIUS 服务器地址。

  如果没有通过主服务器的身份验证，将按顺序尝试每个已配置的备份服务器。

- **Key 1** - WAP 设备用于向主 RADIUS 服务器进行身份验证的共享密钥。

  可以使用 1 至 64 个标准字母数字字符和特殊字符。此密钥区分大小写，必须与 RADIUS 服务器上配置的密钥相匹配。输入的文本显示为星号。

- **Key**（**2** 至 **4**）- 与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。位于 **Server IP (IPv6) Address 2** 的服务器使用 **Key 2**，位于 **Server IP (IPv6) Address 3** 的服务器使用 **Key 3**，以此类推。

- **Enable RADIUS Accounting** - 可以对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量等。

  如果启用 RADIUS 记帐，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

802.1X 请求方

通过 IEEE 802.1X 身份验证，接入点可以获取对安全有线网络的访问权限。可以将此接入点作为有线网络中的 802.1X 请求方（客户端）。可以对使用 MD5 算法加密的用户名和密码进行配置，以允许接入点使用 802.1X 进行身份验证。

在使用基于 IEEE 802.1X 端口的网络访问控制的网络中，请求方在 802.1X 身份验证器获取访问权限之前无法获取对网络的访问权限。如果网络使用 802.1X，必须在 WAP 设备中配置 802.1X 身份验证信息，这样 WAP 设备即可向身份验证器提供这些信息。

802.1X Supplicant 页分为以下 3 个区域：Supplicant Configuration、 Certificate File Status 和 Certificate File Upload。

Supplicant Configuration 区域用于配置 802.1X 工作状态和基本设置。

步骤 1 在导航窗格中选择 **System Security** > **802.1X Supplicant**。

步骤 2 输入以下参数：

- **Administrative Mode** - 启用 802.1X 请求方功能。
- **EAP Method** - 用于加密身份验证用户名和密码的算法。
  - **MD5** - RFC 3748 中定义的散列函数，可提供基本安全。
  - **PEAP** - 受保护的可扩展身份验证协议，可以通过将其封装在 TLS（传输层安全性）隧道内提供高于 MD5 的安全级别。
  - **TLS** - 传输层安全性，如 RFC 5216 中定义，是可以提供高安全性级别的开放标准。
- **Username** - WAP 设备在响应来自 802.1X 身份验证器的请求时使用此用户名。用户名可以包含 1 至 64 个字符。允许使用可打印的 ASCII 字符，包括大写和小写字母、数字以及除引号之外的所有特殊字符。
- **Password** - WAP 设备在响应来自 802.1X 身份验证器的请求时使用此 MD5 密码。密码的长度应介于 1 至 64 个字符之间。允许使用可打印的 ASCII 字符，包括大写和小写字母、数字以及除引号之外的所有特殊字符。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况，WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

Certificate File Status 区域中显示当前证书是否存在：

- **Certificate File Present** - 指示 HTTP SSL 证书文件是否存在。如果存在，此字段显示 “是”。默认设置为 “否”。
- **Certificate Expiration Date** - 指示 HTTP SSL 证书文件的过期时间。范围是有效日期。

Certificate File Upload 区域用于将证书文件上载到 WAP 设备：

步骤 1 选择 **HTTP** 或 **TFTP** 作为 **Transfer Method**。

步骤 2 如果选择了 HTTP，请点击 **Browse** 选择文件。

注 要配置 HTTP 和 HTTPS 服务器设置，请参阅 **HTTP/HTTPS 服务**。

如果选择了 TFTP，则输入 **Filename** 和 **TFTP Server IPv4 Address**。文件名不能包含以下字符：空格、<、>、|、\、:、(、)、&、;、#、?、* 和两个或更多的连续句点。

步骤 3 点击 **Upload**。

会出现一个确认窗口，然后出现一个进度条指示上载状态。

密码复杂性

可以为用于访问 WAP 设备配置实用程序的密码配置复杂性要求。复杂密码可以提高安全性。

要配置密码复杂性要求，请执行以下步骤：

步骤 1 在导航窗格中选择 **Security** > **Password Complexity**。

步骤 2 对于 **Password Complexity** 设置，选择 **Enable**。

步骤 3 配置以下参数：

- **Password Minimum Character Class** - 在密码字符串中必须出现的最少字符类别数。4 个可用的字符类别包括可使用标准键盘输入的大写字母、小写字母、数字和特殊字符。
- **Password Different From Current** - 选择需要用户在其当前密码过期后输入不同密码。如果不选择此项，用户可以在密码过期后重新输入同一密码。
- **Maximum Password Length** - 最大密码字符长度的范围介于 64 至 80 之间，默认值为 64 个字符。
- **Minimum Password Length** - 最小密码字符长度的范围介于 0 至 32 之间，默认值为 8 个字符。
- **Password Aging Support** - 选择密码过期的配置时间段。
- **Password Aging Time** - 新创建密码的有效期天数，范围介于 1 至 365 天，默认值为 180 天。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

WPA-PSK 复杂性

在 WAP 设备上配置 VAP 时，可以选择安全地对客户端进行身份验证的方法。如果选择 WPA 个人协议（也称为 WPA 预先共享密钥或 WPA-PSK）作为任何 VAP 的安全方法，可以使用 WPA-PSK Complexity 页为身份验证过程中使用的密钥配置复杂性要求。较复杂的密钥可以提高安全性。

要配置 WPA-PSK 复杂性，请执行以下步骤：

步骤 1 在导航窗格中选择 **Security** > **WPA-PSK Complexity**。

步骤 2 对于 **WPA-PSK Complexity** 设置，点击 **Enable**， WAP 设备便可根据配置的标准检查 WPA-PSK 密钥。如果取消选中此框，将不使用其中的任一设置。默认情况下，禁用 WPA-PSK Complexity。

步骤 3 配置以下参数：

- **WPA-PSK Minimum Character Class** - 在密钥字符串中必须出现的最少字符类别数。4 个可用的字符类别包括可使用标准键盘输入的大写字母、小写字母、数字和特殊字符。默认值为 3。
- **WPA-PSK Different From Current** - 选择以下选项之一：
  - **Enable** - 用户必须在其当前密钥过期后配置不同密钥。
  - **Disable** - 用户可以在其当前密钥过期后使用旧密钥或以前的密钥。
- **Maximum WPA-PSK Length** - 最大密钥长度是 32 至 63 个字符，默认值为 63 个字符。
- **Minimum WPA-PSK Length** - 最小密钥长度是 8 至 16 个字符，默认值为 8 个字符。选中此框可以将字段设为可编辑字段并激活这一要求。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

7

客户端服务质量

本章简要介绍客户端服务质量 (QoS) 并说明 Client QoS 菜单提供的 QoS 功能。具体包括以下主题：

- 客户端 QoS 全局设置
- ACL
- 类映射
- 策略映射
- 客户端 QoS 关联
- 客户端 QoS 状态

客户端 QoS 全局设置

可以使用 Client QoS Global Settings 页在 WAP 设备中启用或禁用服务质量功能。

如果禁用 **Client QoS Mode**，也会全局禁用所有 ACL、速率限制和 DiffServ 配置。

如果启用此模式，还可以在特定 VAP 上启用或禁用 Client QoS 模式。请参阅**客户端 QoS 关联**页的 **Client QoS Mode** 设置。

ACL

ACL 是允许和拒绝条件的集合，也称为规则，可以通过阻止未经授权的用户和允许授权用户访问特定资源提供安全性。 ACL 可以阻止未经授权的用户尝试访问网络资源。

WAP 设备 最多支持 50 个 IPv4、 IPv6 和 MAC （ 媒体接入控制 ） ACL。

IPv4 和 IPv6 ACL

IP ACL 可以将第 3 层和第 4 层的流量分类。

每个 ACL 组最多包含 10 个应用于 WAP 设备发送或接收的流量的规则。每个规则指定特定字段的内容是否可用于允许或拒绝对网络的访问。规则可基于不同标准，应用于一个数据包内的一个或多个字段，例如源或目标 IP 地址、源或目标端口或者数据包内带有的协议。

注 已创建的每个规则末尾处都存在隐式拒绝。为避免拒绝全部流量，强烈建议在 ACL 内添加允许规则以允许流量。

MAC ACL

MAC ACL 是第 2 层 ACL。可以配置此类规则以检查帧的字段，例如源或目标 MAC 地址、 VLAN ID 或服务等级。如果帧进入或退出 WAP 设备端口（取决于是在上行还是下行方向应用此 ACL），则 WAP 设备检查帧并基于帧内容检查 ACL 内容。如果任一规则与内容匹配，将对帧采取允许或拒绝操作。

配置 ACL

在 ACL Configuration 页配置 ACL 和规则，然后对指定 VAP 应用这些规则。

以下步骤简要介绍 ACL 的配置过程：

步骤 1 在导航窗格中选择 **Client QoS** > **ACL**。

步骤 2 指定 ACL 的名称。

步骤 3 选择要添加的 ACL 类型。

步骤 4 添加 ACL。

步骤 5 将新规则添加到 ACL。

步骤 6 配置规则的匹配标准。

步骤 7 通过**客户端 QoS 关联**页对一个或多个 VAP 应用 ACL。

以下步骤详细介绍 ACL 的配置过程：

步骤 1 在导航窗格中选择 **Client QoS** > **ACL**。

步骤 2 输入以下参数以新建 ACL：

- **ACL Name** - 用于标识 ACL 的名称。名称可以包含 1 至 31 个字母数字和特殊字符。不允许使用空格。
- **ACL Type** - 要配置的 ACL 类型：
  - IPv4
  - IPv6
  - MAC

  IPv4 和 IPv6 ACL 基于第 3 层和第 4 层标准控制对网络资源的访问。MAC ACL 基于第 2 层标准控制访问。

步骤 3 点击 **Add ACL**。

此页显示用于配置 ACL 的其他字段。

步骤 4 配置规则参数：

- **ACL Name - ACL Type** - 要使用新规则配置的 ACL。此列表包含在 ACL Configuration 部分添加的所有 ACL。
- **Rule** - 要采取的操作：
  - 选择 **New Rule** 可以为所选的 ACL 配置新规则。
  - 如果规则已存在（即使是为了用于其他 ACL 而创建的），可以通过选择规则编号将此规则添加到所选 ACL 或修改此规则。

  如果 ACL 具有多个规则，则这些规则按照其添加到 ACL 的顺序应用于数据包或帧。有一个隐式全部拒绝规则作为最终规则。
- **Action** - ACL 规则是允许还是拒绝操作。

  如果选择 Permit，此规则将允许满足规则标准的所有流量进入或退出 WAP 设备（取决于选择的 ACL 方向）。不合标准的流量会遭到丢弃。

  如果选择 Deny，此规则将阻止满足规则标准的所有流量进入或退出 WAP 设备（取决于选择的 ACL 方向）。除非此规则是最终规则，否则将转发不合标准的流量。由于每个 ACL 末尾处都存在隐式全部拒绝规则，未显式允许的流量会遭到丢弃。

- **Match Every Packet** - 如果选择此字段，无论拥有允许或拒绝操作的规则内容为何，都会匹配帧或数据包。

  如果选择此字段，则无法配置任何其他匹配标准。默认情况下，对于新规则，选择 Match Every Packet 选项。必须清除此选项才可以配置其他匹配字段。

对于 IPv4 ACL，配置以下参数：

- **Protocol** - 选择基于 IPv4 数据包中的 IP Protocol 字段值或 IPv6 数据包中的 Next Header 字段值使用第 3 层或第 4 层协议匹配条件的 Protocol 字段。

  如果选择 Protocol，请选择以下选项之一：

  - **Select From List** - 选择以下协议之一：IP、ICMP、IGMP、TCP 或 UDP。
  - **Match to Value** - 输入一个介于 0 至 255 之间的 IANA 指定的标准协议 ID。选择此方法可以识别在 Select From List 中未按名称列出的协议。

- **Source IP Address** - 需要数据包的源 IP 地址以匹配此处列出的地址。在相应字段中输入 IP 地址以应用此标准。
- **Wild Card Mask** - 源 IP 地址的通配符掩码。

  通配符掩码确定所使用的位和忽略的位。通配符掩码 255.255.255.255 表示没有重要的位。通配符掩码 0.0.0.0 表示所有位都很重要。选中 Source IP Address 时需要此字段。

  通配符掩码通常是反子网掩码。例如，要将标准与一个主机地址匹配，请使用通配符掩码 0.0.0.0。要将标准与 24 位子网（例如 192.168.10.0/24）匹配，请使用通配符掩码 0.0.0.255。

- **Source Port** - 将源端口包含在规则的匹配条件中。源端口在数据报头中标识。

  如果选择 Source Port，请选择端口名称或输入端口号。

  - **Select From List** - 与要匹配的源端口关联的关键字：ftp、ftpdata、http、smtp、 snmp、 telnet、 tftp、 www。

    上述的每个关键字都可以转换为其等效的端口号。

  - **Match to Port** - 与数据报头中标识的源端口匹配的 IANA 端口号。端口范围介于 0 至 65535 之间，包含以下三种不同类型的端口：

    0 至 1023 - 已知端口

    1024 至 49151 - 已注册端口

    49152 至 65535 - 动态和 / 或专用端口

- **Destination IP Address** - 需要数据包的目标 IP 地址以匹配此处列出的地址。在相应字段中输入 IP 地址以应用此标准。
- **Wild Card Mask** - 目标 IP 地址的通配符掩码。

  通配符掩码确定所使用的位和忽略的位。通配符掩码 255.255.255.255 表示没有重要的位。通配符掩码 0.0.0.0 表示所有位都很重要。选中 Source IP Address 时需要此字段。

  通配符掩码通常是反子网掩码。例如，要将标准与一个主机地址匹配，请使用通配符掩码 0.0.0.0。要将标准与 24 位子网（例如 192.168.10.0/24）匹配，请使用通配符掩码 0.0.0.255。
- **Destination Port** - 将目标端口包含在规则的匹配条件中。目标端口在数据报头中标识。

  如果选择 Destination Port，请选择端口名称或输入端口号。

  - **Select From List** - 选择与要匹配的目标端口关联的关键字：ftp、ftpdata、http、 smtp、 snmp、 telnet、 tftp、 www。

    上述的每个关键字都可以转换为其等效的端口号。
  - **Match to Port** - 与数据报头中标识的目标端口匹配的 IANA 端口号。端口范围介于 0 至 65535 之间，包含以下三种不同类型的端口：

    0 至 1023 - 已知端口

    1024 至 49151 - 已注册端口

    49152 至 65535 - 动态和 / 或专用端口
- **IP DSCP** - 基于其 IP DSCP 值匹配数据包。

  如果选择 IP DSCP，请选择以下选项之一作为匹配标准：

  - **Select From List** - DSCP 确保转发 (AS)、服务等级 (CS) 或加速转发 (EF) 值。
  - **Match to Value** - 自定义 DSCP 值，范围介于 0 至 63 之间。
- **IP Precedence** - 基于其 IP 优先权值匹配数据包。如果选择此字段，请输入一个介于 0 至 7 之间的 IP 优先权值。
- **IP TOS Bits** - 指定一个值以将 IP 报头中的数据包服务类型位用作匹配标准。

  数据包中的 IP TOS 字段定义为 IP 报头中所有八位的服务类型八位字节。 IP TOS Bits 值是介于 00 至 ff 之间的两位十六进制数字。

  高位的 3 位代表 IP 优先权值。高位的 6 位代表 IP 差分服务代码点 (DSCP) 值。

- **IP TOS Mask** - 输入 IP TOS Mask 值以标识 IP TOS Bits 值中用于与数据包的 IP TOS 字段值比较的数位位置。

  IP TOS Mask 值是介于 00 至 ff 之间的两位十六进制数字，代表反（即通配符）掩码。IP TOS Mask 中的零值位表示 IP TOS Bits 值中用于与数据包的 IP TOS 字段值比较的数位位置。例如，要检查 IP TOS 值是否已设置 7 位和 5 位并清除 1 位（其中 7 位是最高位），请使用 IP TOS Bits 值 0 和 IP TOS Mask 00。

对于 IPv6 ACL，配置以下参数：

- **Protocol** - 选择基于 IPv4 数据包中的 IP Protocol 字段值或 IPv6 数据包中的 Next Header 字段值使用第 3 层或第 4 层协议匹配条件的 Protocol 字段。

  如果选择此字段，请选择要按关键字或协议 ID 匹配的协议。

- **Source IPv6 Address** - 如果选择此字段，需要数据包的源 IPv6 地址以匹配此处列出的地址。在相应字段中输入 IPv6 地址以应用此标准。
- **Source IPv6 Prefix Length** - 输入源 IPv6 地址的前缀长度。
- **Source Port** - 选择此选项以便将源端口包含在规则的匹配条件中。源端口在数据报头中标识。如果选择此选项，请选择端口名称或输入端口号。
- **Destination IPv6 Address** - 如果选择此字段，需要数据包的目标 IPv6 地址以匹配此处列出的地址。在相应字段中输入 IPv6 地址以应用此标准。
- **Destination IPv6 Prefix Length** - 输入目标 IPv6 地址的前缀长度。
- **Destination Port** - 选择此选项以便将目标端口包含在规则的匹配条件中。目标端口在数据报头中标识。如果选择此选项，请选择端口名称或输入端口号。
- **IPv6 Flow Label** - IPv6 数据包特有的一个 20 位数字。此数字由终端站用于表示路由器中的 QoS 处理情况（范围介于 0 至 1048575 之间）。
- **IP DSCP** - 基于其 IP DSCP 值的匹配数据包。如果选择此选项，请选择以下选项之一作为匹配标准：
  - **Select From List** - DSCP 确保转发 (AS)、服务等级 (CS) 或加速转发 (EF) 值。
  - **Match to Value** - 自定义 DSCP 值，范围介于 0 至 63 之间。

对于 MAC ACL，配置以下参数：

- **EtherType** - 选择此选项可以将匹配标准与以太网帧报头中的值相比较。

  选择 EtherType 关键字或输入 EtherType 值以指定匹配标准。

  - **Select from List** - 选择以下协议类型之一：appletalk、arp、ipv4、ipv6、ipx、 netbios、 pppoe。

- **Match to Value** - 输入与数据包匹配的自定义协议标识符。此值是介于 0600 至 FFFF 之间的四位十六进制数。

- **Class of Service** - 选择此字段并输入可与以太网帧比较的 802.1p 用户优先级。

  有效范围介于 0 至 7 之间。此字段位于 first/only 802.1Q VLAN 标记中。

- **Source MAC Address** - 选择此字段并输入可与以太网帧比较的源 MAC 地址。

- **Source MAC Mask** - 选择此字段并输入源 MAC 地址掩码以指定源 MAC 中可与以太网帧比较的位。

  对于 MAC 掩码中的每个数位位置，0 表示相应的地址位是高位，1 表示地址位可以忽略。例如，要仅检查 MAC 地址的前四个八位字节，则使用 MAC 掩码 00:00:00:00:ff:ff。MAC 掩码 00:00:00:00:00:00 可检查所有的地址位，用于匹配一个 MAC 地址。

- **Destination MAC Address** - 选择此字段并输入可与以太网帧比较的目标 MAC 地址。

- **Destination MAC Mask** - 输入目标 MAC 地址掩码以指定目标 MAC 中可与以太网帧比较的位。

  对于 MAC 掩码中的每个数位位置，0 表示相应的地址位是高位，1 表示地址位可以忽略。例如，要仅检查 MAC 地址的前四个八位字节，则使用 MAC 掩码 00:00:00:00:ff:ff。MAC 掩码 00:00:00:00:00:00 可检查所有的地址位，用于匹配一个 MAC 地址。

- **VLAN ID** - 选择此字段并输入可与以太网帧比较的特定 VLAN ID。

  此字段位于 first/only 802.1Q VLAN 标记中。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

注 要删除 ACL，确保在 **ACL Name-ACL Type** 列表中选择此 ACL，选择 **Delete ACL**，然后点击**保存**。

类映射

客户端 QoS（服务质量）功能包含差分服务支持 (DiffServ)，通过此支持，可以根据定义的单跳行为将流量分类为流并为流量提供特定的 QoS 处理。

基于 IP 的标准网络可用于提供尽力数据传送服务。尽力服务意味着网络可以及时传送数据，但不能保证会及时传送。拥塞期间，数据包可能会延迟、不定期发送或丢弃。对于典型的 Internet 应用程序（例如电子邮件和文件传输），服务质量稍有下降是可以接受的，在许多情况下这并不明显。但在时间要求严格的应用程序（例如语音或多媒体）中，任何程度的服务质量下降都会产生不良影响。

DiffServ 配置从定义类映射开始，类映射可用于根据 IP 协议和其他标准对流量进行分类。然后，每个类映射可以与用来定义流量类处理方式的策略映射进行关联。可以将包含时效性强的流量的类指定给优先权高于其他流量的策略映射。

可以使用 Class Map 页定义流量类。使用**策略映射**页定义策略并将其与类映射进行关联。

添加类映射

要添加类映射，请执行以下步骤：

步骤 1 在导航窗格中选择 **Client QoS** > **Class Map**。

步骤 2 输入 **Class Map Name**。名称可以包含 1 至 31 个字母数字和特殊字符。不允许使用空格。

步骤 3 从 **Match Layer 3 Protocol** 列表中选择一个值：

- **IPv4** - 类映射仅适用于 WAP 设备中的 IPv4 流量。
- **IPv6** - 类映射仅适用于 WAP 设备中的 IPv6 流量。

Class Map 页会显示其他字段，具体取决于所选的第 3 层协议：

使用 Match Criteria Configuration 区域中的这些字段以便使数据包与类匹配。选中要用作类标准的每个字段的复选框并在相关字段中输入数据。一个类可以拥有多个匹配标准。

可用的匹配标准字段取决于类映射是 IPv4 还是 IPv6 类映射。

定义类映射

要配置类映射，请执行以下步骤：

步骤 1 从 **Class Map Name** 列表中选择类映射。

步骤 2 配置以下参数（请注意仅对于 IPv4 或 IPv6 类映射显示的参数）：

- **Match Every Packet** - 匹配条件适用于第 3 层数据包中的所有参数。

  如果选择此选项，所有的第 3 层数据包都将符合条件。

- **Protocol** - 基于 IPv4 数据包中的 IP Protocol 字段值或 IPv6 数据包中的 Next Header 字段值，使用第 3 层或第 4 层协议匹配条件。

  如果选择此字段，请选择要按关键字匹配的协议或输入协议 ID。

  - **Select From List** - 与所选协议匹配：IP、ICMP、IPv6、ICMPv6、IGMP、TCP、 UDP。
  - **Match to Value** - 与未按名称列出的协议匹配。输入协议 ID。协议 ID 是 IANA 指定的标准值。范围是介于 0 至 255 之间的数字。

- **Source IP Address** 或 **Source IPv6 Address** - 需要数据包的源 IP 地址以匹配此处列出的地址。选中此框，然后输入 IP 地址。

- **Source IP Mask**（仅 IPv4）- 源 IP 地址掩码。

  DiffServ 的掩码是 IP 点分十进制格式的网络式位掩码，可指示目标 IP 地址中用于匹配数据包内容的部分。

  DiffServ 掩码 255.255.255.255 表示所有位都重要，掩码 0.0.0.0 表示所有位都不重要。 ACL 通配符掩码则与此相反。例如，要将标准与一个主机地址匹配，请使用掩码 255.255.255.255。要将标准与 24 位子网（例如 192.168.10.0/24）匹配，请使用掩码 255.255.255.0。

- **Source IPv6 Prefix Length**（仅 IPv6）- 源 IPv6 地址的前缀长度。

- **Destination IP Address** 或 **Destination IPv6 Address** - 需要数据包的目标 IP 地址以匹配此处列出的地址。在相应字段中输入 IP 地址以应用此标准。

- **Destination IP Mask**（仅 IPv4）- 目标 IP 地址掩码。

  DiffServ 的掩码是 IP 点分十进制格式的网络式位掩码，可指示目标 IP 地址中用于匹配数据包内容的部分。

DiffServ 掩码 255.255.255.255 表示所有位都重要，掩码 0.0.0.0 表示所有位都不重要。 ACL 通配符掩码则与此相反。例如，要将标准与一个主机地址匹配，请使用掩码 255.255.255.255。要将标准与 24 位子网（例如 192.168.10.0/24）匹配，请使用掩码 255.255.255.0。

- **Destination IPv6 Prefix Length**（仅 IPv6）- 目标 IPv6 地址的前缀长度。
- **IPv6 Flow Label**（仅 IPv6）- IPv6 数据包特有的一个 20 位数字。此数字由终端站用于表示路由器中的 QoS 处理情况（范围介于 0 至 1048575 之间）。
- **IP DSCP** - 请参阅 Service Type 字段下方的说明。
- **Source Port** - 将源端口包含在规则的匹配条件中。源端口在数据报头中标识。

  如果选择此字段，请选择端口名称或输入端口号。

  - **Select From List** - 匹配与源端口关联的关键字：ftp、 ftpdata、 http、 smtp、 snmp、 telnet、 tftp、 www。

    上述的每个关键字都可以转换为其等效的端口号。

  - **Match to Port** - 将数据报头中的源端口号与指定的 IANA 端口号进行匹配。端口范围介于 0 至 65535 之间，包含以下三种不同类型的端口：

    0 至 1023 - 已知端口

    1024 至 49151 - 已注册端口

    49152 至 65535 - 动态和 / 或专用端口

- **Destination Port** - 将目标端口包含在规则的匹配条件中。目标端口在数据报头中标识。

  如果选择此字段，请选择端口名称或输入端口号。

  - **Select From List** - 将数据报头中的目标端口与所选的关键字进行匹配：ftp、 ftpdata、 http、 smtp、 snmp、 telnet、 tftp、 www。

    上述的每个关键字都可以转换为其等效的端口号。

  - **Match to Port** - 将数据报头中的目标端口与指定的 IANA 端口号进行匹配。端口范围介于 0 至 65535 之间，包含以下三种不同类型的端口：

    0 至 1023 - 已知端口

    1024 至 49151 - 已注册端口

    49152 至 65535 - 动态和 / 或专用端口

- **EtherType** - 比较匹配标准与以太网帧报头中的值。

选择 EtherType 关键字或输入 EtherType 值以指定匹配标准。

- **Select From List** - 将数据报头中的 Ethertype 与所选的协议类型进行匹配：appletalk、 arp、 ipv4、 ipv6、 ipx、 netbios、 pppoe。
- **Match to Value** - 将数据报头中的 Ethertype 与指定的自定义协议标识符进行匹配。此值可以是介于 0600 至 FFFF 之间的四位十六进制数。

- **Class of Service** - 数据包的匹配服务 802.1p 用户优先级值类。有效范围介于 0 至 7 之间。
- **Source MAC Address** - 可与以太网帧比较的源 MAC 地址。
- **Source MAC Mask** - 源 MAC 地址掩码，用于指定目标 MAC 中可与以太网帧比较的位。

  对于 MAC 掩码中的每个数位位置，0 表示相应的地址位是高位，1 表示地址位可以忽略。例如，要仅检查 MAC 地址的前四个八位字节，则使用 MAC 掩码 00:00:00:00:ff:ff。 MAC 掩码 00:00:00:00:00:00 可检查所有的地址位，用于匹配一个 MAC 地址。
- **Destination MAC Address** - 可与以太网帧比较的目标 MAC 地址。
- **Destination MAC Mask** - 目标 MAC 地址掩码，用于指定目标 MAC 中可与以太网帧比较的位。

  对于 MAC 掩码中的每个数位位置，0 表示相应的地址位是高位，1 表示地址位可以忽略。例如，要仅检查 MAC 地址的前四个八位字节，则使用 MAC 掩码 00:00:00:00:ff:ff。 MAC 掩码 00:00:00:00:00:00 可检查所有的地址位，用于匹配一个 MAC 地址。
- **VLAN ID** - 数据包的匹配 VLAN ID。 VLAN ID 范围介于 0 至 4095 之间。

以下显示的是 IPv4 专用的服务类型字段。可以指定其中一个用于将数据包与类标准进行匹配的服务类型。

- **IP DSCP** - 用作匹配标准的差分服务代码点 (DSCP) 值：
  - **Select from List** - DSCP 类型列表。
  - **Match to Value** - 指定的 DSCP 值，范围介于 0 至 63 之间。
- **IP Precedence**（仅 IPv4）- 将数据包的 IP 优先权值与类标准的 IP 优先权值进行匹配。 IP 优先权范围介于 0 至 7 之间。
- **IP TOS Bits**（仅 IPv4）- 将 IP 报头中的数据包服务类型位用作匹配标准。

  IP TOS 位值的范围介于 00 至 FF 之间。高位的 3 位代表 IP 优先权值。高位的 6 位代表 IP 差分服务代码点 (DSCP) 值。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

注 要删除类映射，请在 **Class Map Name** 列表中将其选中，然后点击**删除**。如果类映射已附加到策略，则无法将其删除。

策略映射

基于定义的标准对数据包进行分类和处理。分类标准由**类映射**页的类定义。处理由 Policy Map 页的策略属性定义。策略属性可能在每个类实例的基础上定义，决定了如何处理与类标准匹配的流量。

WAP 设备最多支持 50 个策略映射。一个策略映射最多可以包含 10 个类映射。

要添加和配置策略映射，请执行以下步骤：

步骤 1 在导航窗格中选择 **Client QoS** > **Policy Map**。

步骤 2 输入 **Policy Map Name**，名称可以包含 1 至 31 个字母数字字符和特殊字符。不允许使用空格。

步骤 3 点击 **Add Policy Map**。此页刷新，出现用于配置策略映射的其他字段。

步骤 4 在 Policy Class Definition 区域，确保 **Policy Map Name** 列表中显示新建的策略映射。

步骤 5 在 **Class Map Name** 列表中选择要应用此策略的类映射。

步骤 6 配置以下参数：

- **Police Simple** - 创建类的流量管制方式。简单管制方式使用单一数据速率和突发流量，会引发两种后果：遵守和不遵守。如果选中此字段，请配置以下字段之一：
  - **Committed Rate** - 流量必须遵守的承诺速率 (Kbps)。范围介于 1 至 1000000 Kbps 之间。
  - **Committed Burst** - 流量必须遵守的承诺的突发流量（字节）。范围介于 1 至 204800000 字节之间。
- **Send** - 指定如果符合类映射标准，将转发关联流量流的所有数据包。
- **Drop** - 指定如果符合类映射标准，将丢弃关联流量流的所有数据包。

- **Mark Class of Service** - 使用 802.1p 报头优先级字段中的指定服务等级值标记关联流量流的所有数据包。如果数据包还未包含此报头，请插入一个。 CoS 值是介于 0 至 7 之间的整数。
- **Mark IP DSCP** - 使用从列表中选择或指定的 IP DSCP 值标记关联流量流的所有数据包。
  - **Select from List** - DSCP 类型列表。
  - **Match to Value** - 指定的 DSCP 值。该值是介于 0 至 63 之间的整数。
- **Mark IP Precedence** - 使用指定的 IP 优先权值标记关联流量流的所有数据包。IP 优先权值是介于 0 至 7 之间的整数。
- **Disassociate Class Map** - 从在 Policy Map Name 列表中选择的策略中删除在 Class Map Name 列表中选择的类。
- **Member Classes** - 列出当前定义为所选策略成员的所有 DiffServ 类。如果没有类与策略关联，此字段为空。

步骤 7 点击**保存**。更改将保存到 Startup Configuration。

注 要删除策略映射，请在 **Policy Map Name** 列表中将其选中，然后点击**删除**。

客户端 QoS 关联

Client QoS Association 页可以对连接到网络的无线客户端的某些 QoS 方面进行额外的控制，例如允许单个客户端发送和接收的带宽量。要控制一般类别的流量（例如 HTTP 流量或来自特定子网的流量），可以配置 ACL 并将其指定给一个或多个 VAP。

除了控制一般的流量类别外，客户端 QoS 可用来配置通过差分服务 (DiffServ) 为每个客户端调整不同的微流。在网络上对入站和出站客户端进行身份验证时， DiffServ 策略对于创建可应用于每个无线客户端的一般微流定义和处理特性都是很有用的工具。

要配置客户端 QoS 关联参数，请执行以下步骤：

步骤 1 在导航窗格中选择 **Client QoS** > **Client QoS Association**。

步骤 2 从 VAP 列表中选择要为其配置客户端 QoS 参数的 VAP。

步骤 3 对于 **Client QoS Global**，选择 **Enable** 以启用此功能。

步骤 4 对于所选 VAP，配置以下参数：

- **Client QoS Mode** - 选择 **Enable** 以便在所选 VAP 中启用客户端 QoS 功能。
- **Bandwidth Limit Down** - 从 WAP 设备到客户端的最大允许传输速率（位 / 秒 (bps)）。有效范围介于 0 至 300 Mbps。
- **Bandwidth Limit Up** - 从客户端到 WAP 设备的最大允许传输速率（位 / 秒 (bps)）。有效范围介于 0 至 300 Mbps。
- **ACL Type Down** - 适用于出站（WAP 设备到客户端）方向流量的 ACL 类型，可以是以下选项之一：
  - IPv4 - 此 ACL 检查与 ACL 规则匹配的 IPv4 数据包。
  - IPv6 - 此 ACL 检查与 ACL 规则匹配的 IPv6 数据包。
  - MAC - 此 ACL 检查与 ACL 规则匹配的第 2 层帧。
- **ACL Name Down** - 应用于出站方向流量的 ACL 的名称。

  将数据包或帧交换到出站接口后，将根据 ACL 规则检查是否存在匹配项。如果允许，则传输数据包或帧；如果拒绝，则将其丢弃。
- **ACL Type Up** - 应用于入站（客户端到 WAP 设备）方向流量的 ACL 类型，可以是以下选项之一：
  - IPv4 - 此 ACL 检查与 ACL 规则匹配的 IPv4 数据包。
  - IPv6 - 此 ACL 检查与 ACL 规则匹配的 IPv6 数据包。
  - MAC - 此 ACL 检查与 ACL 规则匹配的第 2 层帧。
- **ACL Name Up** - 应用于进入 WAP 设备的入站方向流量的 ACL 的名称。

  WAP 设备收到数据包或帧时，将根据 ACL 规则检查是否存在匹配项。如果允许，则处理数据包或帧；如果拒绝，则将其丢弃。
- **DiffServ Policy Down** - 应用于来自 WAP 设备的出站（WAP 设备到客户端）方向流量的 DiffServ 策略名称。
- **DiffServ Policy Up** - 应用于发送到 WAP 设备的入站（客户端到 WAP 设备）方向流量的 DiffServ 策略名称。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

客户端 QoS 状态

Client QoS Status 页显示应用于当前与 WAP 设备关联的每个客户端的客户端 QoS 设置。

要显示 Client QoS Status 页，请在导航窗格中选择 **Client QoS** > **Client QoS Status**。

使用以下字段配置客户端 QoS 状态：

- **Station** - Station 菜单包含当前与 WAP 设备关联的每个客户端的 MAC 地址。要查看对客户端应用的 QoS 设置，请从列表中选择其 MAC 地址。
- **Global QoS Mode** - 是在全局还是在 WAP 设备中启用 QoS。此状态可在**客户端 QoS 关联**页配置。
- **Client QoS Mode** - 是否在关联 VAP 中启用 QoS。此状态可在**客户端 QoS 关联**页配置。
- **Bandwidth Limit Down** - 从 WAP 设备到客户端的最大允许传输速率（位 / 秒 (bps)）。有效范围介于 0 至 4294967295 bps 之间。
- **Bandwidth Limit Up** - 从客户端到 WAP 设备的最大允许传输速率 （位 / 秒 (bps)）。有效范围介于 0 至 4294967295 bps 之间。
- **ACL Type Up** - 应用于入站（客户端到 WAP 设备）方向流量的 ACL 类型，可以是以下选项之一：
  - IPv4：此 ACL 检查与 ACL 规则匹配的 IPv4 数据包。
  - IPv6：此 ACL 检查与 ACL 规则匹配的 IPv6 数据包。
  - MAC：此 ACL 检查与 ACL 规则匹配的第 2 层帧。
- **ACL Name Up** - 应用于进入 WAP 的入站方向流量的 ACL 的名称。 WAP 收到数据包或帧时，将根据 ACL 规则检查是否存在匹配项。如果允许，则处理数据包或帧；如果拒绝，则将其丢弃。
- **ACL Type Down** - 适用于出站（WAP 到客户端）方向流量的 ACL 类型，可以是以下选项之一：
  - IPv4：此 ACL 检查与 ACL 规则匹配的 IPv4 数据包。
  - IPv6：此 ACL 检查与 ACL 规则匹配的 IPv6 数据包。
  - MAC：此 ACL 检查与 ACL 规则匹配的第 2 层帧。

- **ACL Name Down** - 应用于出站方向流量的 ACL 的名称。将数据包或帧交换到出站接口后，将根据 ACL 规则检查是否存在匹配项。如果允许，则传输数据包或帧；如果拒绝，则将其丢弃。
- **DiffServ Policy Up** - 应用于发送到 WAP 设备的入站（客户端到 WAP 设备）方向流量的 DiffServ 策略名称。
- **DiffServ Policy Down** - 应用于来自 WAP 设备的出站（WAP 设备到客户端）方向流量的 DiffServ 策略名称。

8

简单网络管理协议

本章介绍如何配置简单网络管理协议 (SNMP) 以执行配置和统计信息收集任务。

具体包括以下主题：

- SNMP 概述
- 通用 SNMP 设置
- 视图
- 组
- 用户
- 目标

SNMP 概述

SNMP 定义用于记录、存储和共享网络设备相关信息的标准。 SNMP 有助于网络管理、故障排除和维护。

WAP 设备支持 SNMP 版本 1、2 和 3。除非特别说明，否则所有的配置参数仅适用于 SNMPv1 和 SNMPv2c。任何 SNMP 管理的网络的重要组件包含托管设备、SNMP 代理和管理系统。代理将有关其设备的数据存储在管理信息库 (MIB) 中，并在收到请求时将这些数据返回 SNMP 管理器。托管设备可以是网络节点，例如 WAP 设备、路由器、交换机、网桥、集线器、服务器或打印机。

WAP 设备可以用作 SNMP 管理的设备以无缝集成到网络管理系统中。

通用 SNMP 设置

可以使用 General 页启用 SNMP 和配置基本协议设置。

要配置通用 SNMP 设置，请执行以下步骤：

步骤 1 在导航窗格中选择 **SNMP** > **General**。

步骤 2 对于 **SNMP** 设置，选择 **Enabled**。默认情况下，禁用 SNMP。

步骤 3 指定用于 SNMP 流量的 **UDP Port**。

默认情况下，SNMP 代理仅侦听来自端口 161 的请求，但可以配置此设置以便代理侦听其他端口的请求。有效范围介于 1025 至 65535 之间。

步骤 4 配置 SNMPv2 设置：

- **Read-only Community** - 用于 SNMPv2 访问的只读社区名称。有效范围介于 1 至 256 个字母数字和特殊字符之间。

  社区名称可以用作简单身份验证功能，限制网络中可以向 SNMP 代理请求数据的机器。此名称还可以用作密码，如果发送方知道此密码，会认为请求可信。

- **Read-write Community** - 用于 SNMP 设置请求的读写社区名称。有效范围介于 1 至 256 个字母数字和特殊字符之间。

  设置社区名称和设置密码类似。仅接受可通过此社区名称识别的机器所发送的请求。

- **Management Station** - 确定可以通过 SNMP 访问 WAP 设备的工作站。请选择以下选项之一：

  - **All** - 不限制可以通过 SNMP 访问 WAP 设备的工作站集。
  - **User Defined** - 允许的 SNMP 请求集仅限于指定用户。

- **NMS, IPv4 Address/Name** - 可以对托管设备执行 get 和 set 请求的机器的 IPv4 IP 地址、 DNS 主机名、网络管理系统 (NMS) 子网或机器集。

  DNS 主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点系列不能超过 253 个字符。

  对于社区名称，此设置提供有关 SNMP 设置的安全级别。SNMP 代理仅接受此处指定的 IP 地址、主机名或子网的请求。

要指定子网，请按照 *address/mask_length* 的格式输入一个或多个子网地址范围，其中 *address* 是 IP 地址， *mask_length* 是掩码位数。支持 *address/mask* 和 *address/mask_length* 格式。例如，如果输入范围 192.168.1.0/24，这将指定 IP 地址为 192.168.1.0，子网掩码为 255.255.255.0 的子网。

此地址范围用于指定选定 NMS 的子网。仅允许 IP 地址在此范围内的机器在托管设备上执行 get 和 set 请求。在上述示例中，地址介于 192.168.1.1 至 192.168.1.254 之间的机器可以在设备上执行 SNMP 命令。(始终为子网地址保留子网范围中以后缀 .0 标识的地址，始终为广播地址保留范围中以 .255 标识的地址。)

再举一个例子，如果输入范围 10.10.1.128/25， IP 地址介于 10.10.1.129 至 10.10.1.254 之间的机器可以在托管设备上执行 SNMP 请求。在此例中，10.10.1.128 是网络地址， 10.10.1.255 是广播地址。会指定共计 126 个地址。

- **NMS IPv6 Address/Name** - 可以对托管设备执行 get 和 set 请求的机器的 IPv6 地址、 DNS 主机名或子网。 IPv6 地址应采用类似于 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) 的格式。

  主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点系列不能超过 253 个字符。

步骤 5 配置 SNMPv2 陷阱设置：

- **Trap Community** - 与 SNMP 陷阱关联的全局社区字符串。从设备发送的陷阱将此字符串作为社区名称提供。有效范围介于 1 至 60 个字母数字和特殊字符之间。
- **Trap Destination Table** - 最多包含 3 个用于接收 SNMP 陷阱的 IP 地址或主机名的列表。选中此框，选择 **Host IP Address Type** (IPv4 或 IPv6)，然后添加 **Hostname/IP Address**。

  例如， DNS 主机名为 snmptraps.foo.com。由于 SNMP 陷阱是从 SNMP 代理随机发送的，指定用于发送陷阱的准确位置很重要。最多可以拥有 3 个 DNS 主机名。确保选中 **Enabled** 复选框，然后选择合适的 **Host IP Address Type**。

  另请参阅前面步骤中有关主机名的注释。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

注 保存新设置后，相应的过程可能会停止并重新启动。如果发生这种情况， WAP 设备可能会断开连接。建议在连接断开对无线客户端的影响最小时更改 WAP 设备的设置。

视图

SNMP MIB 视图是 MIB 分级结构中的视图子树系列。视图子树是通过位串掩码值的对象标识符 (OID) 子树值配对标识的。每个 MIB 视图是通过两组视图子树定义的，这些视图子树可包含在此 MIB 视图中或从 MIB 视图中排除。可以创建 MIB 视图以控制 SNMPv3 用户可以访问的 OID 范围。

WAP 设备 最多支持 16 个视图。

以下注释汇总了一些有关 SNMPv3 视图配置的重要准则。请在继续操作前阅读所有注释。

注 名称为 all 的 MIB 视图是在系统中默认创建的。此视图包含系统支持的所有管理对象。

注 默认情况下， view-all 和 view-none SNMPv3 视图是在 WAP 设备中创建的。这些视图无法删除或修改。

要添加和配置 SNMP 视图，请执行以下步骤：

步骤 1 在导航窗格中选择 **SNMP** > **Views**。

步骤 2 点击**添加**可以在 SNMPv3 Views 表中添加新行。

步骤 3 选中新行的框，然后点击**编辑**：

- **View Name** - 输入用于标识 MIB 视图的名称。视图名称最多可包含 32 个字母数字字符。
- **Type** - 选择视图子树或子树系列是包含在 MIB 视图中还是从 MIB 视图中排除。
- **OID** - 输入要包含在视图中或从视图中排除的子树的 OID 字符串。

  例如，系统子树由 OID 字符串 .1.3.6.1.2.1.1 指定。
- **Mask** - 输入 OID 掩码。此掩码的长度应为 47 个字符。 OID 掩码的格式为 xx.xx.xx (.)... 或 xx:xx:xx....(:)，长度应为 16 个八位字节。每个八位字节是用句点 (.) 或冒号 (:) 分隔的两个十六进制字符。此字段仅接受十六进制字符。

  例如， OID 掩码 FA.80 是 11111010.10000000。

  family 掩码用于定义视图子树系列。 family 掩码指示对 family 的定义具有重要作用的关联 family OID 字符串的子标识符。视图子树系列可用来有效地控制对表中某行的访问。

步骤 4 点击**保存**。视图会添加到 SNMPv3 Views 列表中，所做的更改也保存到 Startup Configuration。

注 要删除视图，请在列表中选择相应视图，然后点击 **Delete**。

组

通过 SNMPv3 组，可以将用户组合到具有不同授权和访问权限的组中。每组都与以下 3 个安全级别之一关联：

- noAuthNoPriv
- authNoPriv
- authPriv

通过将 MIB 视图关联到读取或写入访问权限组，可以分别控制对每组 MIB 的访问权限。

默认情况下， WAP 设备包含以下两组：

- **RO** - 使用身份验证和数据加密的只读组。此组的用户使用 MD5 密钥 / 密码进行身份验证，使用 DES 密钥 / 密码进行加密。必须定义 MD5 和 DES 密钥 / 密码。默认情况下，此组的用户拥有对默认 all MIB 视图的读取访问权限。
- **RW** - 使用身份验证和数据加密的读 / 写组。此组的用户使用 MD5 密钥 / 密码进行身份验证，使用 DES 密钥 / 密码进行加密。必须定义 MD5 和 DES 密钥 / 密码。默认情况下，此组的用户拥有对默认 all MIB 视图的读写访问权限。

注 不能删除默认组 RO 和 RW。

注 WAP 设备 最多支持 8 个组。

要添加和配置 SNMP 组，请执行以下步骤：

步骤 1 在导航窗格中选择 **SNMP** > **Groups**。

步骤 2 点击**添加**可以在 SNMPv3 Groups 中添加新行。

步骤 3 选中新组的复选框，然后点击**编辑**。

步骤 4 配置以下参数：

- **Group Name** - 用于标识组的名称。默认组名称为 RO 和 RW。

  组名称最多可包含 32 个字母数字字符。

- **Security Level** - 设置组的安全级别，可以是以下选项之一：
  - **noAuthentication-noPrivacy** - 无身份验证和数据加密 （ 无安全性 ）。

- **Authentication-noPrivacy** - 有身份验证，但无数据加密。使用此安全级别，用户可以发送使用 MD5 密钥 / 密码的 SNMP 消息进行身份验证，但不使用 DES 密钥 / 密码进行加密。
- **Authentication-Privacy** - 有身份验证和数据加密。使用此安全级别，用户可以发送用于身份验证的 MD5 密钥 / 密码和用于加密的 DES 密钥 / 密码。

  对于需要身份验证、加密或两者都需要的组，必须在 SNMP Users 页定义 MD5 和 DES 密钥 / 密码。

- **Write Views** - 对此组的 MIB 的写入访问权限，可以是以下选项之一：
  - **write-all** - 此组可以创建、更改和删除 MIB。
  - **write-none** - 此组不能创建、更改和删除 MIB。
- **Read Views** - 对此组的 MIB 的读取访问权限：
  - **view-all** - 允许此组查看和读取所有 MIB。
  - **view-none** - 此组不能查看或读取 MIB。

步骤 5 点击**保存**。组会添加到 SNMPv3 Groups 列表中，所做的更改也保存到 Startup Configuration。

注 要删除组，请在列表中选择相应组，然后点击 **Delete**。

用户

可以使用 SNMP Users 页定义用户、将安全级别关联到每个用户以及为每个用户配置安全密钥。

可以从预定义或用户定义的组中将每个用户映射到 SNMPv3 组，（可选）还可以针对每个用户配置身份验证和加密。对于身份验证，仅支持 MD5 类型。对于加密，仅支持 DES 类型。 WAP 设备 中没有默认的 SNMPv3 用户，最多可以添加 8 个用户。

要添加 SNMP 用户，请执行以下步骤：

步骤 1 在导航窗格中选择 **SNMP** > **Users**。

步骤 2 点击**添加**可以在 SNMPv3 Users 表中添加新行。

步骤 3 选中新行的框，然后点击**编辑**。

步骤 4 配置以下参数：

- **User Name** - 用于标识 SNMPv3 用户的名字。用户名最多可包含 32 个字母数字字符。
- **Group** - 用户映射到的组。默认组为 RWAuth、RWPriv 和 RO。可以在 SNMP Groups 页定义其他组。
- **Authentication Type** - 用于来自用户的 SNMPv3 请求的身份验证类型，可以是以下选项之一：
  - **MD5** - 要求对来自此用户的 SNMP 请求进行 MD5 身份验证。
  - **None** - 不需要对来自此用户的 SNMPv3 请求进行身份验证。
- **Authentication Pass Phrase** -（如果将 MD5 指定为身份验证类型）通过通行短语， SNMP 代理可以对此用户发送的请求进行身份验证。通行短语的长度应介于 8 至 32 个字符之间。
- **Encryption Type** - 用于来自用户的 SNMP 请求的隐私类型，可以是以下选项之一：
  - **DES** - 对来自用户的 SNMPv3 请求使用 DES 加密。
  - **None** - 来自此用户的 SNMPv3 请求不需要隐私。
- **Encryption Pass Phrase** -（如果将 DES 指定为隐私类型）用于对 SNMP 请求进行加密的通行短语。通行短语的长度应介于 8 至 32 个字符之间。

步骤 5 点击**保存**。用户会添加到 SNMPv3 Users 列表中，所做的更改也保存到 Startup Configuration。

注 要删除用户，请在列表中选择相应用户，然后点击 **Delete**。

目标

SNMPv3 目标通过使用 SNMP 管理器的通知消息发送 SNMP 通知。对于 SNMPv3 目标，仅发送通知，不发送陷阱。对于 SNMP 版本 1 和 2，发送陷阱。通过目标 IP 地址、 UDP 端口和 SNMPv3 用户名定义每个目标。

注 SNMPv3 用户配置（请参阅**用户**页）应在配置 SNMPv3 目标之前完成。

注 WAP 设备 最多支持 8 个目标。

要添加 SNMP 目标，请执行以下步骤：

步骤 1 在导航窗格中选择 **SNMP** > **Targets**。

步骤 2 点击**添加**。会在表中添加新行。

步骤 3 选中新行的框，然后点击**编辑**。

步骤 4 配置以下参数：

- **IP Address** - 输入用于接收目标的远程 SNMP 管理器的 IPv4 地址。
- **UDP Port** - 输入用于发送 SNMPv3 目标的 UDP 端口。
- **Users** - 输入与目标关联的 SNMP 用户的名字。要配置 SNMP 用户，请参阅**用户**页。

步骤 5 点击**保存**。用户会添加到 SNMPv3 Targets 列表中，所做的更改也保存到 Startup Configuration。

注 要删除 SNMP 目标，请在列表中选择相应用户，然后点击 **Delete**。

9

强制网络门户

本章介绍强制网络门户 (CP) 功能，通过此功能，可以在建立用户身份验证之前阻止无线客户端访问网络。可以配置 CP 验证，允许访客和已通过身份验证的用户进行访问。

注 强制网络门户功能仅适用于思科 WAP321 设备。

授予访问权限前，必须针对已授权的强制网络门户组或用户的数据库验证已通过身份验证的用户。数据库可以存储在本地 WAP 设备或 RADIUS 服务器中。

强制网络门户包含两个 CP 实例。可以通过不同的验证方法为每个 VAP 或 SSID 单独配置每个实例。思科 WAP321 设备可以与为 CP 身份验证配置的一些 VAP 以及为普通无线身份验证方法配置的其他 VAP 同时运行，例如 WPA 或 WPA Enterprise。

本章包括以下主题：

- **强制网络门户全局配置**
- **实例配置**
- **实例关联**
- **Web 门户自定义**
- **本地组**
- **本地用户**
- **已通过身份验证的客户端**
- **身份验证失败的客户端**

强制网络门户全局配置

通过 Global CP Configuration 页，可以控制 CP 功能的管理状态，并对影响 WAP 设备中配置的所有强制网络门户实例的全局设置进行配置。

要配置 CP 全局设置，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal** > **Global Configuration**。

步骤 2 配置以下参数：

- **Captive Portal Mode** - 启用 WAP 设备中的 CP 操作。
- **Authentication Timeout** - 要通过门户访问网络，客户端必须先在身份验证网页中输入身份验证信息。此字段指定 WAP 设备使关联无线客户端保持身份验证会话打开状态的秒数。如果客户端未能在允许的超时时间内输入身份验证凭据，客户端可能需要刷新身份验证网页。默认的身份验证超时为 300 秒。范围介于 60 至 600 秒之间。
- **Additional HTTP Port** - HTTP 流量使用 HTTP 管理端口，默认情况下此端口为 80。可以为 HTTP 流量配置其他端口。输入介于 1025 至 65535 之间的端口号或 80 端口号。 HTTP 和 HTTPS 端口不能相同。
- **Additional HTTPS Port** - 通过 SSL 的 HTTP 流量 (HTTPS) 使用 HTTPS 管理端口，默认情况下此端口为 443。可以为 HTTPS 流量配置其他端口。输入介于 1025 至 65535 之间的端口号或 443 端口号。 HTTP 和 HTTPS 端口不能相同。

Captive Portal Configuration Counters 区域显示只读的 CP 信息：

- **Instance Count** - 当前在 WAP 设备中配置的 CP 实例数。最多可以配置两个实例。
- **Group Count** - 当前在 WAP 设备中配置的 CP 组数。最多可以配置两组。默认情况下存在 Default Group，此组无法删除。
- **User Count** - 当前在 WAP 设备中配置的 CP 用户数。最多可以配置 128 个用户。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

实例配置

最多可以创建两个强制网络门户实例，每个 CP 实例包含一组已定义的实例参数。实例可以与一个或多个 VAP 关联。可以配置不同的实例，在用户尝试访问关联 VAP 时以不同方式响应他们。

注 创建实例之前，请先查看以下要点：

- 是否需要添加新 VAP？如果需要，请转至**网络**添加 VAP。
- 是否需要添加新组？如果需要，请转至**本地组**添加组。
- 是否需要添加新用户？如果需要，请转至**本地用户**添加用户。

要创建 CP 实例并配置其设置，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal** > **Instance Configuration**。

步骤 2 确保从 **Captive Port Instances** 列表中选择 **Create**。

步骤 3 使用 1 到 32 个字母数字字符输入 **Instance Name** 并点击 **Save**。

步骤 4 从 **Captive Port Instances** 列表中选择实例名称。

会再次出现 Captive Portal Instance Parameters 字段，其中包含更多选项。

步骤 5 配置以下参数：

- **实例 ID** - 实例 ID。此字段是不可配置的。
- **Administrative Mode** - 启用和禁用 CP 实例。
- **Protocol** - 指定 HTTP 或 HTTPS 作为 CP 实例的协议用于验证过程。
  - **HTTP** - 验证期间不使用加密。
  - **HTTPS** - 使用安全套接字层 (SSL)，此协议需要使用证书来提供加密。

    证书会在连接时提供给用户。
- **Verification** - CP 用于验证客户端的身份验证方法：
  - **Guest** - 用户不需要通过数据库进行身份验证。
  - **Local** - WAP 设备使用本地数据库对用户进行身份验证。
  - **RADIUS** - WAP 设备使用远程 RADIUS 服务器上的数据库对用户进行身份验证。

- **Redirect** - 指定 CP 应将新通过身份验证的客户端重新定向到已配置的 URL。如果清除此选项，用户会在成功验证后看到特定于区域设置的欢迎页面。
- **Redirect URL** - 如果启用 URL Redirect Mode，输入新通过身份验证的客户端所重新定向到的 URL（包括 http://）。范围介于 0 至 256 个字符之间。
- **Away Timeout** - 客户端取消与 WAP 的关联后，用户保留在通过 CP 身份验证的客户端列表中的时间长度。如果此字段中指定的时间于客户端尝试重新进行身份验证前过期，则从通过身份验证的客户端列表中删除此客户端条目。范围介于 0 至 1440 分钟之间。默认值为 60 分钟。

  注 还会为每个用户配置离开超时值。请参阅**本地用户**页。除非此处配置的值设置为 0（默认值），否则在 Local Users 页上设置的离开超时值优先于此值。值 0 表示使用实例超时值。
- **Session Timeout** - CP 会话的有效剩余时间（秒）。时间达到零后，将取消对客户端的身份验证。范围介于 0 至 1440 分钟之间。默认值为 0。
- **Maximum Bandwidth Upstream** - 使用强制网络门户时客户端可以传输流量的最大上载速度（兆位 / 秒）。此设置限制了客户端可以将数据发送到网络中的带宽。范围介于 0 至 300 Mbps 之间。默认值为 0。
- **Maximum Bandwidth Downstream** - 使用强制网络门户时客户端可以接收流量的最大下载速度（兆位 / 秒）。此设置限制了客户端可以从网络接收数据的带宽。范围介于 0 至 300 Mbps 之间。默认值为 0。
- **User Group Name** - 如果 Verification Mode 为 Local 或 RADIUS，请将现有的用户组指定给 CP 实例。允许属于一组的所有用户通过此门户访问网络。
- **RADIUS IP Network** - 选择 WAP RADIUS 客户端是否使用配置的 IPv4 或 IPv6 RADIUS 服务器地址。
- **Global RADIUS** - 如果 Verification Mode 为 RADIUS，请将此选项设置为默认全局 RADIUS 服务器列表，对客户端进行身份验证。（有关配置全局 RADIUS 服务器的信息，请参见 **RADIUS 服务器**。）如果您需要 CP 功能使用其他 RADIUS 服务器组，请取消选中该框并且在此页面的字段中配置这些服务器。
- **RADIUS Accounting** - 可以对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量。

  如果启用 RADIUS 记帐，也会对主 RADIUS 服务器、所有的备份服务器以及全局或本地配置的服务器启用此功能。
- **Server IP Address 1 或 Server IPv6 Address 1** - 此 VAP 的主 RADIUS 服务器的 IPv4 或 IPv6 地址。IPv4 地址应采用类似于 xxx.xxx.xxx.xxx (192.0.2.10) 的格式。IPv6 地址应采用类似于 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) 的格式。

第一个无线客户端尝试通过 VAP 进行身份验证时， WAP 设备向主服务器发送身份验证请求。如果主服务器响应身份验证请求，WAP 设备继续将此 RADIUS 服务器用作主服务器，身份验证请求也会发送至指定的地址。

- **Server IP Address (2 至 4)** 或 **Server IPv6 Address (2 至 4)** - 最多 3 个 IPv4 或 IPv6 备份 RADIUS 服务器地址。

  如果没有通过主服务器的身份验证，将按顺序尝试每个已配置的备份服务器。

- **Key 1** - WAP 设备用于向主 RADIUS 服务器进行身份验证的共享密钥。

  最多可以使用 63 个标准字母数字字符和特殊字符。此密钥区分大小写，必须与 RADIUS 服务器上配置的密钥相匹配。输入的文本显示为星号。

- **Key 2 至 Key 4** - 与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。位于 Server IP Address 1 的服务器使用 Key 1，Server IP Address 2 使用 Key 2，以此类推。

- **Locale Count** - 与实例关联的区域设置数量。在 Web Customization 页，最多可以为每个 CP 实例创建和指定三个不同的区域设置。

- **Delete Instance** - 删除当前实例。

步骤 6 点击**保存**。更改将保存到 Startup Configuration。

实例关联

创建实例后，可以使用 Instance Association 页将 CP 实例关联到 VAP。关联的 CP 实例设置应用于尝试在 VAP 中验证身份的用户。

要将实例关联到 VAP，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal** > **Instance Association**。

步骤 2 为实例所要关联的每个 VAP 选择实例名称。

步骤 3 点击**保存**。更改将保存到 Startup Configuration。

Web 门户自定义

CP 实例与 VAP 关联后，需要创建区域设置（身份验证网页）并将其映射到 CP 实例。用户访问与强制网络门户实例关联的 VAP 时，会看到身份验证页。通过 Web Portal Customization 页，可以为网络中的不同区域设置创建唯一页并自定义页面上的文本和图像。

要创建并自定义 CP 身份验证页，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal > Web Portal Customization**。

步骤 2 从 **Captive Portal Web Locale** 列表中选择**创建**。

最多可以在网络中创建三个具有不同区域设置的不同身份验证页面。

步骤 3 输入要指定给页面的 **Web Locale Name**。名称可以包含 1 至 32 个字母数字字符。

步骤 4 从 **Captive Portal Instances** 列表中选择与此区域设置关联的 CP 实例。

可以将多个区域设置与一个实例进行关联。用户尝试访问与 CP 实例关联的特定 VAP 时，与该实例关联的区域设置作为链接显示在身份验证页上。用户可以选择一个链接以切换到该区域设置。

步骤 5 点击**保存**。更改将保存到 Startup Configuration。

步骤 6 从 **Captive Portal Web Locale** 列表中选择创建的区域设置。

此页显示用于修改区域设置的其他字段。 **Locale ID** 和 **Instance Name** 字段无法编辑。可编辑字段使用默认值进行填充。

步骤 7 配置以下参数：

- **Background Image Name** - 作为页面背景显示的图像。可以点击 **Upload/Delete Custom Image** 以上载强制网络门户实例的图像。请参阅 “上载和删除图像”。
- **Logo Image Name** - 显示在页面左上角的图像文件。此图像仅供品牌宣传，例如公司徽标。如果将自定义徽标图像上载到 WAP 设备，可以从列表中将其选中。
- **Foreground color** - 6 位十六进制格式的前景颜色 HTML 编码。范围介于 1 至 32 个字符之间。默认值为 #999999。
- **Background color** - 6 位十六进制格式的背景颜色 HTML 编码。范围介于 1 至 32 个字符之间。默认值为 #BFBFBF。
- **Separator** - 粗水平线的颜色 HTML 编码，将页眉与页面正文分开，采用 6 位十六进制格式。范围介于 1 至 32 个字符之间。默认值为 #BFBFBF。

- **Locale Label** - 区域设置的说明性标签，包含 1 至 32 个字符。默认值为 English。
- **Locale** - 区域设置的缩写，包含 1 至 32 个字符。默认值为 en。
- **Account Image** - 显示在登录字段上方的图像文件，用于描述已通过身份验证的登录。
- **Account Label** - 指示用户输入用户名的文本。范围介于 1 至 32 个字符之间。
- **User Label** - 用户名文本框的标签。范围介于 1 至 32 个字符之间。
- **Password Label** - 用户密码文本框的标签。范围介于 1 至 64 个字符之间。
- **Button Label** - 用户点击此按钮上的标签，可以提交其用户名 / 密码进行身份验证。范围介于 2 至 32 个字符之间，默认值为 Connect。
- **Fonts** - 用于 CP 页上所有文本的字体名称。可以输入多个字体名称，用逗号逐个分隔。如果第一个字体无法在客户端系统中使用，则使用下一个字体，依此类推。对于包含空格的字体名称，请用引号括住整个名称。范围介于 1 至 512 个字符之间。默认值为 MS UI Gothic、 Arial、 sans-serif。
- **Browser Title** - 浏览器标题栏中显示的文本。范围介于 1 至 128 个字符之间。默认值为 Captive Portal。
- **Browser Content** - 页眉中显示在徽标右侧的文本。范围介于 1 至 128 个字符之间。默认值为 Welcome to the Wireless Network。
- **Content** - 页面正文中显示在用户名和密码文本框下方的说明性文本。范围介于 1 至 256 个字符之间。默认值为 To start using this service, enter your credentials and click the connect button.
- **Acceptance Use Policy** - 显示在 Acceptance Use Policy 框中的文本。范围介于 1 至 4096 个字符之间。默认值为 Acceptance Use Policy。
- **Accept Label** - 指示用户选中此复选框以确认阅读并接受 Acceptance Use Policy 的文本。范围介于 1 至 128 个字符之间。默认值为 Check here，表示用户已阅读并接受 Acceptance Use Policy。
- **No Accept Text** - 用户提交登录凭据但未选中 Acceptance Use Policy 复选框时显示在弹出窗口中的文本。范围介于 1 至 128 个字符之间。默认值为 Error:You must acknowledge the Acceptance Use Policy before connecting!
- **Work In Progress Text** - 在身份验证期间显示的文本。范围介于 1 至 128 个字符之间。默认值为 Connecting, please be patient....
- **Denied Text** - 用户未通过身份验证时显示的文本。范围介于 1 至 128 个字符之间。默认值为 Error Invalid Credentials, please try again!

- **Welcome Title** - 客户端已对 VAP 进行身份验证时显示的文本。范围介于 1 至 128 个字符之间。默认值为 Congratulations!
- **Welcome Content** - 客户端已连接网络时显示的文本。范围介于 1 至 256 个字符之间。默认值为 You are now authorized and connected to the network.
- **Delete Locale** - 删除当前区域设置。

步骤 8 点击**保存**。更改将保存到 Startup Configuration。

步骤 9 点击**预览**查看更新页面。

注 可以点击**预览**以显示已保存到 Startup Configuration 的文本和图像。如果进行了更改，请点击**保存**，然后点击**预览**以查看更改。

上载和删除图像

用户开始访问与强制网络门户实例关联的 VAP 时，会出现身份验证页。可以使用自己的徽标或其他图像自定义身份验证页。

最多可以上载 18 张图像（假定有 6 个区域设置，每个区域设置有 3 张图像）。所有图像必须为 5 千字节或更小，必须为 GIF 或 JPG 格式。

图像大小需要调整以适合指定大小。为达到最佳效果，徽标和帐户图像应和默认图像的比例相似，具体如下所示：

图像类型	用途	默认宽度与高度
背景	显示为页面背景。	10 × 800 像素
徽标	显示在页面左上方，用于提供品牌信息。	168 × 78 像素
帐户	显示在登录字段上方，用于描述已通过身份验证的登录。	295 × 55 像素

要将二进制图形文件上载到 WAP 设备，请执行以下步骤：

步骤 1 在 Web Portal Customization 页，点击 **Background Image Name**、 **Logo Image Name** 或 **Account Image** 字段旁边的 **Upload/Delete Custom Image**。

会出现 Web Portal Custom Image 页。

步骤 2 浏览以选择图像。

步骤 3 点击 **Upload**。

步骤 4 点击 **Back** 返回 Web Portal Custom Image 页。

步骤 5 选择要配置的 **Captive Portal Web Locale**。

步骤 6 对于 **Background Image Name**、 **Logo Image Name** 或 **Account Image** 字段，选择新上载的图像。

步骤 7 点击**保存**。

注 要删除图像，在 Web Portal Custom Image 页的 **Delete Web Customization Image** 列表中将其选中，然后点击**删除**。无法删除默认图像。

本地组

为每个本地用户指定一个用户组。为每组指定一个 CP 实例。组便于管理向用户指定 CP 实例。

名称为 Default 的用户组是内置的，无法删除。最多还可再创建两个用户组。

要添加本地用户组，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal** > **Local Groups**。

步骤 2 输入**组名**，然后点击**保存**。更改将保存到 Startup Configuration。

注 要删除组，请在 **Captive Portal Groups** 列表中将其选中，选中 **Delete Group** 复选框，然后点击**保存**。

本地用户

可以配置强制网络门户实例以适应访客用户和授权用户。访客用户没有指定的用户名和密码。

授权用户提供有效的用户名和密码，此用户名和密码必须先针对本地数据库或 RADIUS 服务器进行验证。通常，为授权用户指定的 CP 实例是与不同于访客用户的 VAP 进行关联的。

可以使用 Local Users 页在本地数据库中配置最多 128 位授权用户。

要添加和配置本地用户，请执行以下步骤：

步骤 1 在导航窗格中选择 **Captive Portal** > **Local Users**。

步骤 2 输入**用户名**，然后点击**保存**。

会显示其他字段，用于配置用户。

步骤 3 输入以下参数：

- **User Password** - 输入包含 8 至 64 个字母数字和特殊字符的密码。用户必须输入密码才可以通过强制网络门户登录网络。
- **Show Password as Clear Text** - 如果启用，将显示键入的文本。如果禁用，输入时不隐藏文本。
- **Away Timeout** - 客户端取消与 AP 的关联后，用户保留在通过 CP 身份验证的客户端列表中的时间长度。如果此字段中指定的时间于客户端尝试重新进行身份验证前过期，则从通过身份验证的客户端列表中删除此客户端条目。范围介于 0 至 1440 分钟之间。默认值为 60。除非用户值设置为 0，否则此处配置的超时值优先于为强制网络门户实例配置的值。如果设置为 0，则使用为 CP 实例配置的超时值。
- **Group Name** - 指定的用户组。配置每个 CP 实例以支持特定的用户组。
- **Maximum Bandwidth Up** - 使用强制网络门户时，客户端可以传输流量的最大上载速度（兆位 / 秒）。此设置限制了用于将数据发送到网络中的带宽。范围介于 0 至 300 Mbps 之间。默认值为 0。
- **Maximum Bandwidth Down** - 使用强制网络门户时客户端可以接收流量的最大下载速度（兆位 / 秒）。此设置限制了用于从网络接收数据的带宽。范围介于 0 至 300 Mbps 之间。默认值为 0。
- **Delete User** - 删除当前用户。

步骤 4 点击**保存**。更改将保存到 Startup Configuration。

已通过身份验证的客户端

Authenticated Clients 页提供有关已在任何强制网络门户实例进行身份验证的客户端的信息。

要查看已通过身份验证的客户端列表，请在导航窗格中选择 **Captive Portal** > **Authenticated Clients**。

- **MAC Address** - 客户端的 MAC 地址。
- **IP Address** - 客户端的 IP 地址。
- **User Name** - 客户端的强制网络门户用户名。
- **Protocol** - 用户用于建立连接的协议（HTTP 或 HTTPS）。
- **Verification** - 用于在强制网络门户对用户进行身份验证的方法，可以是以下值之一：
  - **Guest** - 用户不需要通过数据库进行身份验证。
  - **Local** - WAP 设备使用本地数据库对用户进行身份验证。
  - **RADIUS** - WAP 设备使用远程 RADIUS 服务器上的数据库对用户进行身份验证。
- **VAP ID** - 与用户关联的 VAP。
- **Radio ID** - 无线的 ID。由于 WAP321 具有单频，此字段始终显示 Radio1。
- **Captive Portal ID** - 与用户关联的强制网络门户实例的 ID。
- **Session Timeout** - CP 会话的有效剩余时间（秒）。时间达到零后，将取消对客户端的身份验证。
- **Away Timeout** - 客户端条目的有效剩余时间（秒）。定时器在客户端取消与 CP 的关联时开始计时。时间达到零后，将取消对客户端的身份验证。
- **Received Packets** - WAP 设备从用户工作站接收的 IP 数据包数。
- **Transmitted Packets** - 从 WAP 设备发送到用户工作站的 IP 数据包数。
- **Received Bytes** - WAP 设备从用户工作站接收的字节数。
- **Transmitted Bytes** - 从 WAP 设备发送到用户工作站的字节数。

点击**刷新**以显示 WAP 设备中的最新数据。

身份验证失败的客户端

Failed Authenticated Clients 页列出有关尝试在强制网络门户进行身份验证但失败的客户端的信息。

要查看身份验证失败的客户端列表，请在导航窗格中选择 **Captive Portal** > **Failed Authentication Clients**。

- **MAC Address** - 客户端的 MAC 地址。
- **IP Address** - 客户端的 IP 地址。
- **User Name** - 客户端的强制网络门户用户名。
- **Verification** - 客户端尝试在强制网络门户进行身份验证时所用的方法，可以是以下值之一：
  - **Guest** - 用户不需要通过数据库进行身份验证。
  - **Local** - WAP 设备使用本地数据库对用户进行身份验证。
  - **RADIUS** - WAP 设备使用远程 RADIUS 服务器上的数据库对用户进行身份验证。
- **VAP ID** - 与用户关联的 VAP。
- **Radio ID** - 无线的 ID。由于 WAP321 具有单频，此字段显示 Radio1。
- **Captive Portal ID** - 与用户关联的强制网络门户实例的 ID。
- **Failure Time** - 身份验证失败的时间。包含显示失败时间的时间戳。

点击**刷新**以显示 WAP 设备中的最新数据。

10

单点设置

本章介绍如何通过多个 WAP 设备配置单点设置。

具体包括以下主题：

- 单点设置概述
- 接入点
- 会话
- 信道管理
- 无线相邻设备

单点设置概述

思科 WAP121 和 WAP321 设备支持单点设置。单点设置可提供一种用于管理和控制多个设备间无线服务的集中方法。可以使用单点设置创建无线设备的单个组或集群。WAP 设备集群化后，可以将无线网络作为单个实体进行查看、部署、配置并保证安全。创建无线集群后，单点设置还有助于无线服务间的信道规划，从而减少无线干扰并最大限度地提高无线网络的带宽。

首次设置 WAP 设备时，可以使用 Setup Wizard 单点设置或加入现有的单点设置。如果不想使用 Setup Wizard，可以使用基于 Web 的配置实用程序。

管理 WAP 设备间的单点设置

单点设置可以在网络的同一子网中创建 WAP 设备的动态、可识别配置的集群或组。一个集群仅支持一组已配置的 WAP121 或 WAP321 设备。一个集群不支持在同一组中混合使用 WAP121 和 WAP321 设备。

通过单点设置，可以在同一子网或网络中管理多个集群，但这些集群是作为单个独立实体进行管理的。下表显示单点设置的无线服务限制。

组 / 集群类型	每个单点设置的 WAP 设备数	每个单点设置的活动客户端数	最大客户端数（活动和空闲）
WAP121	4	40	64
WAP321	8	160	256

集群可以传播配置信息，例如 VAP（虚拟接入点）设置、QoS（服务质量）队列参数和无线参数。配置设备的单点设置时，如果其他设备加入集群，则将此设备的设置（无论这些设置是手动设置还是默认设置）传播到这些设备。要组成一个集群，请确保满足以下先决条件或条件：

步骤 1 计划单点设置集群。确保要组成集群的两个或更多 WAP 设备属于同一型号。例如，思科 WAP121 设备只能与其他思科 WAP121 设备组成集群。

强烈建议在所有集群化的 WAP 设备上运行最新的固件版本。

注 固件升级**不会**传播到集群中的所有 WAP 设备；必须单独升级每个设备。

步骤 2 设置将在同一 IP 子网中组成集群的 WAP 设备，确认其互联并可通过交换局域网访问。

步骤 3 启用所有 WAP 设备的单点设置。请参阅**接入点**。

步骤 4 确认 WAP 设备全部引用相同的单点设置名称。请参阅**接入点**。

单点设置协商

如果为单点设置启用并配置 WAP 设备，则此设备开始每 10 秒发送一次定期通告以宣布其存在。如果存在与集群标准匹配的其他 WAP 设备，则仲裁开始确定将主配置分发到其余集群成员的 WAP 设备。

以下规则适用于单点设置集群的形成和仲裁：

- 对于现有的单点设置集群，无论何时管理员更新任何集群成员的配置，都会将配置更改传播到所有的集群成员，并且配置的 WAP 设备可控制集群。
- 两个独立的单点设置集群合为一个集群时，则最近修改的集群将仲裁配置，并覆盖和更新组成集群的所有 WAP 设备的配置。
- 如果集群中的 WAP 设备在超过 60 秒的时间内没有收到来自 WAP 设备的通告（例如，如果设备断开与集群中其他设备的连接），则从集群中删除此设备。

- 如果单点设置模式下的 WAP 设备断开连接，不要立即从集群中将其丢弃删除。如果未删除设备，使其保持连接并重新加入集群，同时在连接断开期间对其进行了配置更改，该设备将在连接恢复时向其他集群成员传播这些更改。
- 如果断开集群中某个 WAP 设备的连接并将其删除，后来使其重新加入集群，并且在连接断开期间集群进行了配置更改，则在此设备重新加入集群时将向其传播这些更改。如果断开连接的设备和集群中都进行了配置更改，则首先选择更改量最大的设备，其次才会选择最近更改的设备，将其配置传播到集群。（即，如果 WAP1 的更改量较大，但 WAP2 的更改时间最近，则选择 WAP1。如果它们的更改量相同，但 WAP2 的更改时间最近，则选择 WAP2。）

从单点设置中删除的 WAP 设备的运行

如果以前是集群成员的 WAP 设备断开与集群的连接，则适用以下指导原则：

- 与集群断开连接会阻止 WAP 设备接收最新的运行配置设置。断开连接会使整个生产网络中相应的无缝无线服务暂停。
- WAP 设备继续使用上次从集群接收的无线参数运行。
- 与非集群 WAP 设备关联的无线客户端继续与此设备进行关联，无线连接也不会中断。换句话说，与集群断开连接并不一定会阻止与该 WAP 设备关联的无线客户端继续访问网络资源。
- 如果与集群断开连接是因与局域网基础架构的物理或逻辑断开引起的，则无线客户端的网络服务可能会受影响，具体要取决于故障性质。

单点设置中配置设置和参数的传播

下表汇总了可在组成集群的所有 WAP 设备之间共享和传播的配置。

在单点设置中传播的通用配置设置和参数	
强制网络门户	密码复杂性
客户端 QoS	用户帐户
电子邮件警报	QoS
HTTP/HTTPS 服务（除 SSL 证书配置外）	包括 TSpec 设置的无线设置（有一些例外情况）
日志设置	恶意 AP 检测

在单点设置中传播的通用配置设置和参数	
MAC 过滤	调度程序
管理访问控制	SNMP General 和 SNMPv3
网络	WPA-PSK 复杂性
时间设置	

在单点设置中传播的无线配置设置和参数
模式
分片阈值
RTS 阈值
速率集
主信道
保护
固定多播速率
广播或多播速率限制
信道带宽
支持的较短保护间隔

在单点设置中不传播的无线配置设置和参数
信道
信标间隔
DTIM 周期
最大工作站数
发射功率

在单点设置中不传播的其他配置设置和参数	
带宽利用率	端口设置
Bonjour	虚拟局域网和 IPv4
IPv6 地址	WDS 网桥
IPv6 隧道	WPS
数据包捕获	工作组网桥

接入点

通过 Access Points 页，可以在 WAP 设备中启用或禁用单点设置、查看集群成员和配置成员位置及成员的集群名称。还可以点击成员的 IP 地址，在该设备中配置和查看数据。

为单点设置配置 WAP 设备

要配置每个单点设置集群成员的位置和名称，请执行以下步骤：

步骤 1 在导航窗格中选择 **Single Point Setup > Access Points**。

默认情况下，单点设置在 WAP 设备 中为禁用状态。此设置禁用时，会显示 **Enable Single Point Setup** 按钮。如果启用单点设置，则会显示 **Disable Single Point Setup** 按钮。仅在单点设置禁用时可以编辑单点设置的选项。

此页右侧的图标指示是否启用单点设置，如果启用，则显示当前加入集群的 WAP 设备数量。

步骤 2 如果禁用单点设置，为每个单点设置集群成员配置以下信息。

- **Location** - 输入接入点物理位置的说明，例如 Reception。此字段可选。
- **Cluster Name** - 输入 WAP 设备所加入集群的名称，例如 Reception_Cluster。

  集群名称不发送给其他的 WAP 设备。必须在每个成员设备中配置相同的名称。对于网络中配置的每个单点设置，集群名称必须是唯一的。默认名称为 ciscosb-cluster。

- **Clustering IP Version** - 指定集群中的 WAP 设备与其他集群成员进行通信所用的 IP 版本。默认版本为 IPv4。

  如果选择 IPv6，单点设置可以使用链路本地地址、自动配置的 IPv6 全局地址和静态配置的 IPv6 全局地址。确保在使用 IPv6 时集群中的所有 WAP 设备仅使用链路本地地址或仅使用全局地址。

  单点设置仅适用于使用相同类型 IP 寻址的设备。它不适合部分 WAP 设备拥有 IPv4 地址、而部分 WAP 设备拥有 IPv6 地址的设备组。

步骤 3 点击 **Enable Single Point Setup**。

此 WAP 设备开始在子网中搜索通过相同集群名称和 IP 版本配置的其他 WAP 设备。潜在的集群成员每 10 秒发送一次通告以宣布其存在。

搜索其他集群成员时，状态可指示正在应用配置。刷新此页可以查看新配置。

如果已通过相同的集群设置配置一个或多个 WAP 设备，则 WAP 设备加入集群并在表中显示每个成员的信息。

步骤 4 对要加入单点设置的其他 WAP 设备重复上述步骤。

查看单点设置信息

启用单点设置时， WAP 设备 会自动与配置相同的其他 WAP 设备形成一个集群。在 Access Points 页，表中会列出检测到的 WAP 设备并显示以下信息：

- **Location** - 接入点物理位置的说明。
- **MAC Address** - 接入点的媒体接入控制 (MAC) 地址。此地址是网桥 (br0) 的 MAC 地址，通过此地址其他设备可以从外部找到 WAP 设备。
- **IP 地址** - 接入点的 IP 地址。

请注意，单点设置状态和 WAP 设备数量通过采用图表形式显示在页面右侧。

将新接入点添加到单点设置集群

要将当前处于独立模式的新接入点添加到单点设置集群，请执行以下步骤：

步骤 1 转至独立接入点中基于 Web 的配置实用程序。

步骤 2 在导航窗格中选择 **Single Point Setup > Access Points**。

步骤 3 选择与为集群成员配置的名称相同的 **Cluster name**。

步骤 4 （可选）在 Location 字段中输入接入点物理位置的说明，例如 Reception。

步骤 5 点击 **Enable Single Point Setup**。

此接入点自动加入单点设置。

从单点设置集群中删除接入点

要从单点设置集群中删除接入点，请执行以下步骤：

步骤 1 在显示检测到的设备的表中，点击要删除组成集群的 WAP 设备的 IP 地址。

系统会显示该 WAP 设备基于 Web 的配置实用程序。

步骤 2 在导航窗格中选择 **Single Point Setup > Access Points**。

步骤 3 点击 **Disable Single Point Setup**。

该接入点的 **Single Point Setup** 状态字段会显示 **Disabled**。

导航至特定 WAP 设备的配置信息

单点设置集群中的所有 WAP 设备具有相同的配置（如果可配置项可以传播）。连接哪个 WAP 设备并不重要，因为集群中任何 WAP 设备的管理 - 配置更改会传播给其他成员。

但是，可能会存在想要在特定 WAP 设备中查看或管理信息的情况。例如，可能想要查看接入点的状态信息，例如客户端关联或事件。在这种情况下，可以在 Access Points 页点击表中的 IP 地址以显示特定接入点基于 Web 的配置实用程序。

使用 URL 中的 IP 地址导航至 WAP 设备

还可以使用以下格式直接在 Web 浏览器地址栏中输入作为 URL 的接入点 IP 地址，链接到特定 WAP 设备基于 Web 的配置实用程序：

http://*IPAddressOfAccessPoint* （如果使用 HTTP）

https://IPAddressofAccessPoint（如果使用 HTTPS）

会话

Sessions 页显示与单点设置集群中的 WAP 设备关联的无线局域网客户端的信息。每个无线局域网客户端可通过其 MAC 地址以及当前连接的设备位置进行标识。

注 对于组成集群的 WAP 设备中的每个无线，Sessions 页最多可显示 20 个客户端。要查看与特定 WAP 设备关联的所有无线局域网客户端，请直接在该设备中查看 Status > Associated Clients 页。

要查看无线局域网客户端会话的特定统计信息，请从显示列表中选择一项，然后点击 **Go**。可以查看有关空闲时间、数据速率和信号强度的信息。

此环境下的会话是具有唯一 MAC 地址的客户端设备（工作站）中的用户保持与无线网络连接的时间段。会话从无线局域网客户端登录网络时开始，在无线局域网客户端出于一些其他原因有意注销或断开连接时结束。

注 会话不同于关联，后者用于说明无线局域网客户端与特定接入点的连接。在同一会话内，无线局域网客户端关联可以从组成集群的某个接入点转换到另一接入点。

要查看与集群关联的会话，请在导航窗格中选择 **Single Point Setup > Sessions**。

以下是对于具有单点设置的每个无线局域网客户端显示的数据。

- **AP Location** - 接入点的位置。

  位置来源于 Administration > System Settings 页中指定的位置。

- **User MAC** - 无线客户端的 MAC 地址。

  MAC 地址是可唯一识别每个网络节点的硬件地址。

- **Idle** - 此无线局域网客户端保持不活动状态的时间长度。

  无线局域网客户端不接收或发送数据时即视为不活动状态。

- **Rate** - 协商的数据速率。实际的传输速率可能因开销而异。

  数据传输速率以兆位 / 秒 (Mbps) 为单位。此值应在针对接入点所用模式设置的通告速率范围之内。例如，对于 802.11a，此范围介于 6 至 54 Mbps 之间。

- **Signal** - 无线局域网客户端从接入点接收的射频 (RF) 信号的强度。此测量值称为接收信号强度指示 (RSSI)，介于 0 至 100 之间。

- **Receive Total** - 无线局域网客户端在当前会话期间接收的数据包总数。

- **Transmit Total** - 在此会话期间传输到无线局域网客户端的数据包总数。

- **Error Rate** - 在此接入点进行传输期间丢弃帧的时间百分比。

要按特定指示对表中显示的信息进行排序，请点击排序所依据的列标签。例如，如果要查看按信号强度排序的表行，请点击 “信号”列标签。

信道管理

Channel Management 页显示单点设置集群中的 WAP 设备的当前和规划的信道分配。

如果启用信道管理，则 WAP 设备 自动分配单点设置集群中的 WAP 设备使用的无线信道。自动信道分配可以减少互相干扰（或集群外的其他 WAP 设备的干扰），最大限度地提高了 Wi-Fi 带宽，从而有助于保持无线网络的高效通信。

默认情况下，自动信道分配功能为禁用状态。信道管理的状态会（已启用或已禁用）传播到单点设置集群中的其他设备。

按照指定间隔，信道管理器（即向集群提供配置的设备）将组成集群的所有 WAP 设备映射到不同的信道，并测量集群成员的干扰电平。如果检测到严重的信道干扰，信道管理器会自动按照效率算法（或自动信道规划）将部分或所有设备重新分配至新信道。如果信道管理器确定需要进行更改，则会向所有的集群成员发送重新分配信息。还会生成系统日志消息，指示发送方设备和新 / 旧信道分配。

要配置并查看单点设置成员的信道分配，请执行以下步骤：

步骤 1 在导航窗格中选择 **Single Point Setup** > **Channel Management**。

在 Channel Management 页，可以查看集群中所有 WAP 设备的信道分配，停止或开始自动信道管理。还可以使用高级设置改变会触发信道重新分配的干扰减少可能性，更改自动更新的时间表以及重新配置用于分配的信道集。

步骤 2 要开始自动信道分配，请点击 **Start**。

信道管理覆盖默认的集群行为，即同步属于集群成员的所有 WAP 设备的无线信道。如果启用信道管理，则不会将此集群的无线信道同步到其他设备。

如果启用自动信道分配，信道管理器会定期映射单点设置集群中的 WAP 设备使用的无线信道，如有必要，还会重新分配信道以减少集群成员或集群外设备的干扰。自动将无线信道策略设置为静态模式，并且对于 Wireless > Radio 页的 **Channel** 字段不提供 **Auto** 选项。

有关当前和建议的信道分配的信息，请参阅 “查看信道分配和设置锁定”。

步骤 3 要停止自动信道分配，请点击 **Stop**。

不会进行信道使用映射或信道重新分配。仅手动更新可以影响信道分配。

查看信道分配和设置锁定

如果启用信道管理，此页显示 Current Channel Assignations 表和 Proposed Channel Assignments 表。

Current Channel Assignments 表

Current Channel Assignments 表按 IP 地址列出单点设置集群中的所有 WAP 设备。

此表提供以下有关当前信道分配的详细信息。

- **Location** - 设备的物理位置。
- **IP 地址** - 接入点的 IP 地址。
- **Wireless Radio** - 无线的 MAC 地址。
- **Band** - 接入点进行广播所在的频段。
- **Channel** - 此接入点当前进行广播所在的无线信道。
- **Locked** - 强行将接入点保留在当前信道。
- **Status** - 显示设备中无线功能的状态。（部分 WAP 设备可能具有多个无线功能，而每个无线均显示在表中的单独一行中。）无线状态是 Up （工作）或 Down （不工作）。

为接入点进行选择时，自动信道管理规划在优化策略过程中不会为 WAP 设备重新分配其他信道。而是将具有锁定信道的 WAP 设备作为规划要求考虑在内。

点击**保存**更新锁定设置。锁定设备显示 Current Channel Assignations 表和 Proposed Channel Assignments 表的相同信道。锁定设备会保留其当前信道。

Proposed Channel Assignments 表

Proposed Channel Assignments 表显示将在下次更新时分配给每个 WAP 设备的建议信道。锁定信道不重新分配，优化设备间的信道分布时需要考虑锁定设备必须保留在其当前信道。可以将未锁定的 WAP 设备分配给与其以前所用信道不同的信道，具体要取决于规划结果。

对于单点设置中的每个 WAP 设备， Proposed Channel Assignments 表显示和 Current Channel Assignations 表相同的位置、 IP 地址和无线功能。此表还会显示建议信道，即如果应用信道规划可为此 WAP 设备重新分配的无线信道。

配置高级设置

通过 Advanced settings 区域，可以自定义和制定单点设置的信道规划。

默认情况下，每小时自动重新分配一次信道，但仅在干扰可以减少 25% 或更多时执行。即使网络繁忙，也会重新分配信道。默认设置可以满足需要实施信道管理的大多数情况。

可以更改高级设置以配置以下设置：

- **Change channels if interference is reduced by at least** - 为了应用建议的规划必须达到的最小干扰减少百分比。默认值为 75%。使用下拉菜单选择介于 5% 至 75% 之间的百分比。通过使用此设置，可以设置信道重新分配效率的阈值增益，因此网络就不会因微小的效率增益而频繁中断。

  例如，如果信道干扰必须减少 75%，而建议的信道分配仅使干扰减少 30%，则不会重新分配信道。但是，如果将最小信道干扰增益重置为 25% 并单击**保存**，则将实施建议的信道规划并根据需要重新分配信道。

- **Determine if there is better set of channels every** - 自动更新的时间表。提供的间隔范围介于 30 分钟至 6 个月之间。

  默认值为 1 小时，这意味着会重新分配信道的使用并每小时应用一次生成的信道规划。

如果更改了这些设置，请点击**保存**。更改将保存到 Active Configuration 和 Startup Configuration。

无线相邻设备

对于集群中每个无线功能范围内的， Wireless Neighborhood 页最多可显示 20 个设备。（例如，如果 WAP 设备拥有两个无线功能，则集群中会显示 40 个设备。） Wireless Neighborhood 页还会区分集群成员和非集群成员。

Wireless Neighborhood 视图可以帮助：

- 检测并定位无线域中的意外（或恶意）设备，这样可以采取措施以限制关联的风险。

- 验证覆盖范围预期。通过评估可见 WAP 设备以及其他设备的信号强度，可以验证部署是否达到规划目标。
- 检测故障。覆盖模式的意外更改在彩色编码表中一目了然。

要查看相邻设备，请在导航窗格中选择 **Single Point Setup** > **Wireless Neighborhood**。要查看在特定单点设置中检测到的所有设备，请导航至成员的 Web 界面并在导航窗格中选择 **Wireless** > **Rogue AP Detection**。

对于每个相邻接入点，显示以下信息：

- **Display Neighboring APs** - 选择以下单选按钮之一以更改视图：
  - **In cluster** - 仅显示属于集群成员的相邻 WAP 设备。
  - **Not in cluster** - 仅显示不属于集群成员的相邻 WAP 设备。
  - **Both** - 显示所有的相邻 WAP 设备（集群成员和非成员）。
- **Cluster** - 表顶端的列表显示一起组成集群的所有 WAP 设备的 IP 地址。（此列表与 **Single Point Setup** > **Access Points** 页中的成员列表相同。）

  如果集群中仅有一个 WAP 设备，则仅显示一个 IP 地址，表示此 WAP 设备本身形成一组。

  可以点击 IP 地址以查看有关特定 WAP 设备的更多详细信息。
- **Neighbors** - 组成集群的一个或多个设备的相邻设备按 SSID（网络名称）在左列列出。

检测到的相邻设备自身还可以是集群成员。同时也是集群成员的相邻设备始终显示在上方带有一个粗条的列表顶端，并包含一个位置指示器。

Neighbors 列表中每个 WAP 设备右侧的彩条显示每个相邻 WAP 设备的信号强度，信号强度与其 IP 地址显示在列顶端的集群成员检测到的一样。

条形颜色指示信号强度：

- 深蓝条 - 深蓝条和高信号强度数字（例如 50）表示从相邻设备检测到的良好信号强度，与在该列上方列出其 IP 地址的设备检测到的一样。
- 浅蓝条 - 浅蓝条和低信号强度数字（例如 20 或更低）表示从相邻设备检测到的中等或弱信号强度，与在该列上方列出其 IP 地址的设备检测到的一样。
- 白色条 - 白色条和数字 0 表示在此列上方列出其 IP 地址的设备检测不到某个集群成员检测到的相邻设备。
- 浅灰色条 - 浅灰色条和无信号强度数字表示从相邻设备检测不到任何信号，但相邻设备可能已由其他集群成员检测到。

- 深灰色条 - 深灰色条和无信号强度数字表示与其上方列出的 IP 地址对应的 WAP 设备自身。会显示信号强度 0，因为不会测量此设备自己的信号强度。

查看集群成员的详细信息

要查看集群成员的详细信息，请在此页顶端点击成员的 IP 地址。

以下的设备详细信息出现在 Neighbors 列表下方。

- **SSID** - 相邻接入点的服务集标识符。
- **MAC 地址** - 相邻接入点的 MAC 地址。
- **Channel** - 接入点当前进行广播所在的信道。
- **Rate** - 此接入点当前的传输速率（兆位 / 秒）。当前速率始终都是 Supported Rates 中所示速率之一。
- **Signal** - 从接入点检测到的无线信号的强度，以分贝 (dB) 为单位。
- **Beacon Interval** - 接入点使用的信标间隔。
- **Beacon Age** - 从此接入点接收的最后一个信标的日期和时间。

A

取消身份验证消息原因代码

客户端从 WAP 设备取消身份验证时，会向系统日志发送一条消息。消息包含可能有助于确定客户端取消身份验证原因的原因代码。点击 **Status and Statistics > Log Status** 即可查看日志消息。

下表说明了取消身份验证原因代码。

原因代码	含义
0	保留
1	未指定原因
2	以前的身份验证不再有效
3	由于发送站 (STA) 正在离开或已离开独立基本服务集 (IBSS) 或 ESS 而取消身份验证
4	由于处于不活动状态而取消关联
5	由于 WAP 设备无法处理当前所有的关联 STA 而取消关联
6	从尚未进行身份验证的 STA 收到第 2 类帧
7	从尚未关联的 STA 收到第 3 类帧
8	由于发送 STA 正在离开或已离开基本服务集 (BSS) 而取消关联
9	STA 请求的（重新）关联未通过响应 STA 进行身份验证
10	由于功效管理中的信息不可接受而取消关联
11	由于支持的信道元素中的信息不可接受而取消关联
12	由于 BSS 传输管理而取消关联
13	元素无效，即在此标准中定义的元素的内容不符合第 8 条规定
14	消息完整性代码 (MIC) 失败

原因代码	含义
15	四次握手超时
16	组密钥握手超时
17	四次握手中的元素与（重新）关联请求 / 探测响应 / 信标帧不同
18	组密码无效
19	成对密码无效
20	AKMP 无效
21	RSNE 版本不受支持
22	RSNE 功能无效
23	IEEE 802.1X 身份验证失败
24	由于安全策略拒绝了密码套件

B

快速索引

思科提供了大量的资源来帮助您和您的客户尽享 思科 WAP121 和 WAP321 接入点 所带来的任何优势。

支持	
思科 Small Business 技术支持社区	www.cisco.com/go/smallbizsupport
思科 Small Business 技术支持和资源	www.cisco.com/go/smallbizhelp
电话支持联系方式	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
思科 Small Business 固件下载	www.cisco.com/go/smallbizfirmware 选择一个链接，下载思科 Small Business 产品的固件。无需登录。 Cisco.com 上的 Download （下载）区域 (www.cisco.com/go/software) 提供了针对所有其他思科 Small Business 产品（包括网络存储系统）的下载（该网站需要注册 / 登录）。
思科 Small Business 开源请求	www.cisco.com/go/smallbiz_opensource_request
产品文档	
支持以太网供电 (PoE) 的思科 Small Business WAP121 和 WAP321 Wireless-N 接入点快速入门指南和管理指南	http://www.cisco.com/go/100_wap_resources or http://www.cisco.com/go/300_wap_resources

思科 Small Business	
思科 Small Business 合作伙伴中心（合作伙伴需要登录）	www.cisco.com/web/partners/sell/smb
思科 Small Business 主页	www.cisco.com/smb