管理指南

支持 PoE 的思科 WAP571 Wireless-AC/N 高级双频无线接入点

思科 WAP571E Wireless-AC/N 高级双频无线户外接入点

Cisco 和 Cisco 徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。若要查看思科的商标列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有人的财产。文中的“合作伙伴”用词并不表示思科与其他任一公司有合作关系。 (1110R)

© 2018 Cisco Systems, Inc. 保留所有权利。

© 2015 Cisco Systems, Inc. 保留所有权利。

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 地址访问接入点。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”**。将接入点的内部网地址 (http://<*ip 地址*>) 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。
- 如果管理工作站上有多个 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接入点。

注销

默认情况下，如果基于 Web 的接入点配置实用程序在 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，请单击基于 Web 的接入点配置实用程序右上角的**“退出”**。

使用接入点设置向导

首次登录接入点 （或重置为出厂默认设置后），会出现“接入点设置向导”以帮助执行初始配置。请按照以下步骤完成向导：

使用接入点设置向导

注 如果单击**“取消”**跳过向导，系统将显示**“更改密码”**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“欢迎”页上单击**“下一步”**。系统将显示“配置设备 - 固件升级”窗口。

步骤 2 单击**“浏览”**按钮，查找网络中的固件映像文件。

注 所提供的固件升级文件必须是 tar 文件。请勿尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不受支持。

步骤 3 单击**“升级”**应用新的固件映像。或单击**“跳过”**，系统将显示“配置设备 - 配置恢复”窗口。

注 上传新固件可能需要数分钟。上传新固件时，不要刷新页面或导航至其他页面，否则固件上传会中止。上传过程完成后，接入点将重新启动并恢复正常运行。

步骤 4 单击**“浏览”**按钮，查找网络中的配置文件。

注 配置文件必须为 XML 格式，其中包含有关 WAP 设备设置的所有信息。

步骤 5 单击**“升级”**以应用所选的配置文件。或单击**“跳过”**，系统将显示“配置设备 - IP 地址”窗口。

注 恢复配置文件可能需要几分钟时间。在恢复配置文件或中断配置文件恢复时，请不要刷新页面或导航至其他页面。上传过程完成后，接入点将重新启动并恢复正常运行。

步骤 6 如果希望 WAP 设备从 DHCP 服务器接收 IP 地址，请单击**“动态 IP 地址 (DHCP)”**。还可以选择**“静态 IP 地址”**以手动配置 IP 地址。有关这些字段的说明，请参阅 IPv4 设置。

步骤 7 单击**“下一步”**。系统将显示“集群设置 - 设置集群”窗口。有关 Single Point Setup 的说明，请参阅集群设置概述。

步骤 8 要为 WAP 设备创建新的集群设置，请选择**“创建新集群”**，然后指定**“新集群名称”**。使用相同的集群名称配置设备并在另一 WAP 设备中启用集群设置模式时，这些设备会自动加入组。

如果网络中已存在集群，可以通过单击**“加入现有集群”** 将此设备添加到其中，然后输入**“现有集群名称”**。

如果此时不希望此设备加入 Single Point Setup，请单击**“不要启用集群设置”**。

（可选）可以在“AP 位置”字段中输入文本以记录 WAP 设备的物理位置。

步骤 9 单击**“下一步”**。系统将显示“配置设备 - 设置系统日期和时间”窗口。

步骤 10 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。

注 如果想要设置计算机的时间和日期，“系统时间”旁边有一个箭头可用于从当前计算机设置时间。

步骤 11 单击**“下一步”**。系统将显示“启用安全性 - 设置密码”窗口。

步骤 12 输入**“新密码”**，然后在“确认密码”中再次输入此密码以再次确认。可以在**“用户名”**字段中更改用户名。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“密码复杂性”框。但是，思科强烈建议启用密码安全规则。

步骤 13 单击**“下一步”**。系统将显示无线电 1 界面的“启用安全性 - 为您的无线网络命名”窗口。

注 对于此窗口以及后面两个窗口（“无线安全性”和“VLAN ID”），首先为无线电 1 界面配置这些设置。在这些窗口重新出现后，即可为无线电 2 配置这些设置。

步骤 14 输入**网络名称**。此名称用作默认无线网络的 SSID。

步骤 15 单击**“下一步”**。系统将显示“启用安全性 - 对您的无线网络进行安全设置”窗口。

步骤 16 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 17 单击**“下一步”**。向导会显示“启用安全性 - 为您的无线网络分配 VLAN ID”窗口。

步骤 18 为在无线网络中接收的流量输入一个 VLAN ID。

应从默认设置 (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 19 单击**“下一步”**。

步骤 20 对于 WAP571/E 设备，“网络名称”、“无线安全性”和“VLAN ID”页会显示如何配置无线电 2。完成对无线电 2 的配置后，单击**“下一步”**。

向导会显示“启用网页认证 - 创建您的访客网络”窗口。

步骤 21 选择是否设置用于网络访客的身份验证方法，然后单击 **Next**。

如果单击**“否”**，则跳至步骤 29。

如果单击**“是”**，向导会显示“启用网页认证 - 为您的访客网络命名”窗口。

步骤 22 为无线电 1 指定**“访客网络名称”**。对于 WAP571/E 设备，选择访客网络是使用**“无线电 1”**还是**“无线电 2”**。

步骤 23 单击**“下一步”**。向导会显示“启用网页认证 - 对您的访客网络进行安全设置”窗口。

步骤 24 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 25 单击**“下一步”**。向导会显示“启用网页认证 - 分配 VLAN ID”窗口。

步骤 26 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 27 单击**“下一步”**。向导会显示“启用网页认证 - 启用重定向 URL”窗口。

步骤 28 选择**“启用重定向 URL”**，然后在“重定向 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 29 单击**“下一步”**。向导会显示“摘要 - 确认您的设置”窗口。

步骤 30 检查已配置的设置。单击 **“上一步”**以重新配置一个或多个设置。如果单击 **“取消”**，所有设置将恢复为以前的值或默认值。

步骤 31 如果设置正确，请单击**“提交”**。WAP 设置已保存并出现确认窗口。

步骤 32 单击 **“完成”**。系统显示登录窗口后，可使用更改的密码登录接入点。

使用入门

为通过快速导航简化设备配置，“使用入门”页提供用于执行常见任务的链接。“使用入门”页是每次登录基于 Web 的接入点配置实用程序时的默认窗口。

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
	配置无线射频设置	无线射频
	配置无线网络设置	网络
	配置 LAN 设置	LAN （局域网）
	配置集群配置	集群配置概述
设备状态	系统摘要	系统摘要
	无线状态	网络接口
快速访问	更改帐户密码	用户帐户
	升级设备固件	管理固件
	备份/恢复配置	下载/备份配置文件

窗口导航

使用导航功能访问基于 Web 的实用程序。

配置实用程序页眉

配置实用程序页眉包含标准信息，显示在每页的顶端。页眉可提供以下按钮：

导航窗格/主菜单

按钮名称	说明
（用户）	登录接入点的用户帐户名称 （Administrator 或 Guest）。出厂默认用户名为 **cisco**。
退出	单击此按钮，可退出基于 Web 的接入点配置实用程序。
语言	将鼠标指针悬停在此按钮上，然后选择语言。
关于	单击此按钮，可显示接入点类型和版本号。

按钮名称	说明
帮助	单击此按钮，可显示在线帮助。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

此表介绍了系统中各页面上显示的常用按钮。

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。
全部清除	清除日志表中的所有条目。
关于	单击此按钮，可显示接入点类型和版本号。
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。
刷新	用最新数据重新显示当前页。
保存	保存设置或配置。
更新	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
- 无线组播转发统计信息
- 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
- 无线射频统计信息
- 电子邮件警报状态
- 日志

系统摘要

“系统摘要”页显示各种基本信息，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。

若要查看系统信息，请选择**“状态和统计信息”>“系统摘要”**。或在“使用入门”页中选择**“设备状态”**下的**“系统摘要”**。

“系统摘要”页显示以下信息：

- **PID VID** — WAP 硬件型号和版本。
- **序列号** — 思科 WAP 设备的序列号。
- **基本 MAC 地址** — WAP MAC 地址。
- **固件版本 （活动映像）** — 活动映像的固件版本号。
- **固件 MD5 校验和 （活动映像）** — 活动映像的校验和。
- **固件版本 （非活动）** — 备份映像的固件版本号。
- **固件 MD5 校验和 （非活动）** — 备份映像的校验和。
- **主机名** — 指定给设备的名称。
- **系统运行时间** — 自上次重新启动后的运行时间。
- **系统时间** — 当前系统时间。
- **电源** — 系统从 PoE 供电设备接受以太网供电 (PoE)。

TCP/UDP 服务表显示有关 WAP 中所使用协议和服务的基本信息。

- **服务** — 服务的名称 （如果可用）。
- **协议** — 服务使用的底层传输协议 （TCP 或 UDP）。
- **本地 IP 地址** — WAP 设备上连接至此服务的远程设备的 IP 地址 （如果有）。**“全部”**表示设备中的任何 IP 地址都可以使用此服务。
- **本地端口** — 服务的端口号。
- **远程 IP 地址** — 使用此服务的远程主机的 IP 地址 （如果有）。**“全部”**表示此服务可用于访问系统的所有远程主机。
- **远程端口** — 任何与此服务进行通信的远程设备的端口号。

- **连接状态 —** 服务的状态。对于 UDP，此表中仅显示状态为“活动”或“已建立”(Established) 的连接。 TCP 状态包括：
  - **监听 —** 表示服务正在监听连接请求。
  - **活动 —** 已建立连接会话并且正在发送和接收数据包。
  - **“已建立”(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。
  - **“等待时间”(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）。

可以单击**“刷新”**刷新屏幕并显示最新信息。

网络接口

“网络接口”页显示有关有线和无线接口的配置和状态信息。要查看网络接口信息，请选择“状态和统计信息”>“网络接口”。

系统将显示以下信息：

- **LAN 状态 —** 显示 LAN 接口的信息，具体包括：
  - **MAC 地址 —** WAP 设备的 MAC 地址。
  - **IP 地址 —** WAP 设备的 IP 地址。
  - **子网掩码 —** WAP 设备的子网掩码。
  - **默认网关 —** WAP 设备的默认网关。
  - **域名服务器 - 1 —** WAP 设备所使用的域名服务器 1 的 IP 地址。
  - **域名服务器 - 2 —** WAP 设备所使用的域名服务器 2 的 IP 地址。
  - **IPv6 地址 —** WAP 设备的 IPv6 地址。
  - **自动配置的 IPv6 全局地址 —** 自动配置的 IPv6 全局地址。
  - **IPv6 链路本地地址 —** WAP 设备的 IPv6 链路本地地址。
  - **默认 IPv6 网关 —** WAP 设备的默认 IPv6 网关。
  - **IPv6-DNS-1 —** WAP 设备所使用的 IPv6 DNS 服务器 1 的 IPv6 地址。
  - **IPv6-DNS-2 —** WAP 设备所使用的 IPv6 DNS 服务器 2 的 IPv6 地址。

上述设置适用于内部接口。要更改其中任何设置，请单击“编辑”链接。您将被重定向至 **IPv4 设置**页面。

- **端口状态 —** 显示 LAN 接口的状态。
- **接口 —** 以太网接口的编号。
  - **链路状态 —** 以太网接口的状态。
  - **端口速度 —** 以太网接口的速度。
  - **双工模式 —** 以太网接口的双工模式。
  - **绿色以太网状态 —** 以太网接口的状态。

要更改其中任何设置，请单击“编辑”链接。您将被重定向至**端口设置**页面。

- **VLAN 状态 —** 显示所有现有 VLAN 的信息，具体包括：
  - **VLAN ID —** VLAN 的标识符。
  - **说明 —** VLAN 的说明。
  - **Eth —** 接口是 VLAN 的已添加标签的或未添加标签的成员。

要更改其中任何设置，请单击“编辑”链接。您将被重定向至 **VLAN 配置**页面。

- **无线射频状态 —** 显示无线射频接口的信息，具体包括：
  - **无线射频 —** 显示是否为无线射频接口启用了无线射频模式。
  - **MAC 地址 —** 无线射频接口所关联的 MAC 地址。
  - **模式 —** 无线射频接口所使用的 802.11 模式 (a/b/g/n/ac)。
  - **信道 —** 无线射频接口所使用的信道。
  - **运行带宽 —** 无线射频接口所使用的运行带宽。

要更改其中任何设置，请单击“编辑”链接。您将被重定向至**无线射频**页面。

- **接口状态 —** 显示每个虚拟接入点 (VAP) 和每个无线分布式系统 (WDS) 接口的状态信息，具体包括：
- **接口 —** WAP 设备的无线接口。
- **名称 (SSID) —** 无线接口的名称。
- **状态 —** VAP 的管理状态 （正常或异常）。
- **MAC 地址 —** 无线射频接口的 MAC 地址。

- **VLAN ID —** 无线射频接口的 VLAN ID。
- **配置文件 —** 任何关联的调度程序配置文件的名称。
- **状态 —** 当前的状态 （活动或非活动）。状态用于指示 VAP 是否正在与客户端交换数据。

单击**“刷新”**刷新屏幕并显示最新信息。

流量统计信息

使用“流量统计信息”页查看有关 WAP 的基本信息。它还可以实时显示以太网接口、虚拟接入点 (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“流量统计信息”页，请在导航窗格中选择**“状态和统计信息”>“流量统计信息”**。

“流量统计信息”页显示各方向流量的摘要数据和统计信息。

- **网络接口 —** 以太网接口以及各 VAP 和 WDS 接口的名称。

  WLAN0 和 WLAN1 优先于 VAP 接口名称以指示无线射频接口 （WLAN0 代表 Radio 1， WLAN1 代表 Radio 2）。
- **数据包总数 —** 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。
- **字节总数 —** 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。
- **已丢弃的数据包总数 —** 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。
- **已丢弃的字节总数 —** 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。
- **错误 —** 与此 WAP 设备中发送和接收数据相关的错误的总数。

可以单击**“刷新”**刷新屏幕并显示最新信息。

无线组播转发统计信息

“无线组播转发统计信息”页提供一些有关当前接入点的基本信息，并实时显示接入点上无线组播流量接口及两个无线射频接口上所有 VAP 的发送和接收统计信息。所有显示的发送和接收统计信息都是自接入点上次启动后的收发总数。如果重新启动接入点，这些数字表示自重新启动后的发送和接收总数。

要显示“无线组播转发统计信息”页，请在导航窗格中选择**“状态和统计信息”>“无线组播转发统计信息”**。

发送和接收统计信息

- **网络接口 —** 以太网接口以及各 VAP 和 WDS 接口的名称。

  WLAN0 和 WLAN1 优先于 VAP 接口名称以指示无线射频接口 （WLAN0 代表 Radio 1， WLAN1 代表 Radio 2）。
- **组播数据帧 —** 显示已接收的组播数据帧数。
- **组播数据转发 —** 显示已转发的组播数据帧数。
- **组播数据溢出 —** 显示已泛洪的组播数据帧数。
- **已发送的组播数据 —** 显示已发送的组播数据帧数。
- **已丢弃的组播数据 —** 显示已丢弃的组播数据帧数。
- **MFDB 缓存命中数 —** 显示 MFDB 缓存命中数。
- **MFDB 缓存丢失数 —** 显示 MFDB 缓存丢失数。

IGMP 统计信息

- **网络接口 —** 以太网接口以及各 VAP 和 WDS 接口的名称。

  WLAN0 和 WLAN1 优先于 VAP 接口名称以指示无线射频接口 （WLAN0 代表 Radio 1， WLAN1 代表 Radio 2）。
- **IGMP 帧 —** 显示已接收的 IGMP 帧数。
- **IGMP 帧转发 —** 显示已接收的 IGMP 查询数。
- **已发送的 IGMP 帧 —** 显示已显示的 IGMP 报告数。
- **MFDB 缓存命中数 —** 显示 MFDB 缓存命中数。
- **MFDB 缓存丢失数 —** 显示 MFDB 缓存丢失数。

组播组

- **网络接口 —** 以太网接口以及各 VAP 和 WDS 接口的名称。

  WLAN0 和 WLAN1 优先于 VAP 接口名称以指示无线射频接口 （WLAN0 代表 Radio 1， WLAN1 代表 Radio 2）。

- **组播组 —** 显示组播组 IP 地址。
- **工作站 —** 显示组播组工作站 MAC 地址。
- **数据包 —** 显示已接收的组播组工作站数据包数。

可以单击“刷新”刷新屏幕并显示最新信息。

工作组网桥发送/接收

“工作组网桥发送/接收”页显示工作组网桥上工作站间流量的具体数据包数和字节数。有关配置工作组网桥的详情，请参阅工作组网桥。

要显示“工作组网桥发送/接收”页，请在导航窗格中选择**“状态和统计信息”>“工作组网桥发送/接收”**。

配置为工作组网桥接口的每个网络接口显示以下字段：

- **网络接口 —** 以太网或 VAP 接口的名称。WLAN0 代表 Radio 1，WLAN1 代表 Radio 2。
- **状态和统计信息 —** 表示接口是处于断开状态，还是由管理员配置为“启用”(Up) 或“禁用”(Down)。
- **VLAN ID —** 虚拟局域网 (VLAN) ID。您可以使用 VLAN 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。
- **名称 (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。

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：

- **数据包总数 —** 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。
- **字节总数 —** 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。

可以单击**“刷新”**刷新屏幕并显示最新信息。

关联客户端

可以使用“关联客户端”页查看与特定接入点关联的客户端工作站。

要显示“关联客户端”页，请在导航窗格中选择**“状态和统计信息”>“关联客户端”**。

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。

- **关联客户端的总数 —** 当前与接入点关联的客户端总数。
- **网络接口 —** 与客户端关联的 VAP。 WLAN0 和 WLAN1 优先于 VAP 接口名称以指示无线射频接口 （WLAN0 代表 Radio 1， WLAN1 代表 Radio 2）。
- **工作站 —** 关联无线客户端的 MAC 地址。
- **状态** -“已验证和已关联状态”(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“无”或“静态 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“静态 WEP”仅使用 IEEE 802.11 身份验证。）
  - 如果 WAP 设备使用 IEEE 802.1X 或 WPA 安全模式，那么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）。
- **发送工作站/收件人工作站 —** 对于发送工作站，计数器可指示无线客户端发送的数据包数或字节数。对于收件人工作站，计数器可指示从 W收件人工作站 设备发送到无线客户端的数据包数和字节数。
  - **数据包 —** 从无线客户端接收 （发送）的数据包数。
  - **字节 —** 从无线客户端接收 （发送）的字节数。
  - **丢弃数据包 —** 接收 （发送）后已丢弃的数据包数。
  - **丢弃字节 —** 接收 （发送）后已丢弃的字节数。
  - **“流量流超限数据包数（发送工作站）”(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。
  - **“流量流超限数据包数 （收件人工作站） ”(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。

- **关联时间 —** 客户端已与 WAP 设备关联的时间长度。

可以单击**“刷新”**刷新屏幕并显示最新信息。

TSPEC 客户端关联

“TSPEC 客户端关联”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 客户端关联”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，此类应用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**“状态和统计信息”>“TSPEC 客户端关联”**。

“TSPEC 客户端关联”页显示以下信息：

状态和统计信息：

- **网络接口 —** 客户端使用的无线射频接口。 WLAN0 代表 Radio 1， WLAN1 代表 Radio 2。
- **SSID —** 与此 TS 客户端关联的服务集标识符。
- **工作站 —** 客户端工作站 MAC 地址。
- **TS 标识符 —** TSPEC 流量会话标识符 （范围介于 0 至 7 之间）。
- **接入类别 —** TS 接入类别 （语音或视频）。
- **方向 —** 此 TS 的流量方向。 “方向”可以是以下选项之一：
  - “上行链路”(uplink) — 从客户端到设备。
  - “上行链路”(downlink) — 从设备到客户端。
  - “双向”(bidirectional)
- **用户优先级 —** 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

具体值可能会因其他优先流量会话而异。

- **介质时间 —** TS 流量占用传输介质的时间。
- **超时使用次数 —** 客户端超过为其 TSPEC 确定的介质时间的次数。非经常性的轻度违反情况会被忽略。
- **VAP MAC 地址 —** 虚拟接入点 MAC 地址。

统计信息：

- **网络接口 —** 客户端使用的无线射频接口。
- **工作站 —** 客户端工作站 MAC 地址。
- **TS 标识符 —** TSPEC 流量会话标识符 （范围介于 0 至 7 之间）。
- **接入类别 —** TS 接入类别 （语音或视频）。
- **方向 —** 此 TS 的流量方向。 “方向”可以是以下选项之一：
  - “上行链路”(uplink) — 从客户端到设备。
  - “上行链路”(downlink) — 从设备到客户端。
  - “双向”(bidirectional)
- **发送工作站 —** 显示从无线客户端接收的数据包数和字节数。
  - **数据包 —** 超过允许 TSPEC 的数据包数。
  - **字节 —** WAP 设备要求准入且尚未建立 TSPEC 时的字节数。
- **收件人工作站 —** 从 WAP 设备发送到无线客户端的数据包数和字节数。
  - **数据包 —** 超过允许 TSPEC 的数据包数。
  - **字节 —** WAP 设备要求准入且尚未建立 TSPEC 时的字节数。

可以单击**“刷新”**刷新屏幕并显示最新信息。

TSPEC 状态和统计信息

“TSPEC 状态和统计信息”页提供以下信息：

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

显示的所有发送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，这些数字将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**“状态和统计信息”>“TSPEC 状态和统计信息”**。

“TSPEC 状态和统计信息”页提供以下无线局域网 （无线射频）和 VAP 接口的状态信息：

- **网络接口 —** 无线射频或 VAP 接口的名称。 WLAN0 代表 Radio 1， WLAN1 代表 Radio 2。
- **接入类别 —** 与此流量流 （语音或视频）关联的当前接入类别。
- **状态 —** 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）。

- **活动流量流 —** 此无线射频和接入类别的当前活动的 TSPEC 流量流数。
- **流量流客户端数 —** 与此无线射频和接入类别关联的流量流客户端数。
- **允许的介质时间 —** 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。
- **未分配的介质时间 —** 此接入类别未使用带宽的时间。

单独针对无线射频接口中的发送和接收通道，显示以下统计信息：

- **接入类别 —** 与此流量流 （语音或视频）关联的接入类别。
- **数据包总数 —** 此无线射频发送 （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。
- **字节总数 —** 指定接入类别已接收的字节总数。

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：

- **语音数据包总数 —** 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。
- **语音字节总数 —** 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。

- **视频数据包总数 —** 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。
- **视频字节总数 —** 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。

可以单击**“刷新”**刷新屏幕并显示最新信息。

TSPEC AP 统计信息

“TSPEC AP 统计信息”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 统计信息”页，请在导航窗格中选择**“状态和统计信息”>“TSPEC AP 统计信息”**。

- **TSPEC 语音 ACM 统计信息摘要 —** 已接受和已拒绝的语音流量流的总数。
- **TSPEC 视频 ACM 统计信息摘要 —** 已接受和已拒绝的视频流量流的总数。

可以单击**“刷新”**刷新屏幕并显示最新信息。

无线射频统计信息

可以使用“无线射频统计信息”页显示各个无线射频接口的数据包级和字节级统计信息。要查看“无线射频统计信息”页，请在导航窗格中选择**“状态和统计信息”>“无线射频统计信息”**。

对于 WAP571/E 设备，选择要查看其统计信息的无线射频。

- **已接收的数据包数 —** WAP 设备接收的数据包总数。
- **已发送的数据包数 —** WAP 设备发送的数据包总数。
- **已接收的字节数 —** WAP 设备接收的字节总数。
- **已发送的字节数 —** WAP 设备发送的字节总数。
- **已丢弃的接收数据包数 —** WAP 设备接收但已丢弃的数据包数。
- **已丢弃的发送数据包数 —** WAP 设备发送但已丢弃的数据包数。
- **已丢弃的接收字节数 —** WAP 设备接收但已丢弃的字节数。
- **已丢弃的发送字节数 —** WAP 设备发送但已丢弃的字节数。

- **已接收的分片数 —** WAP 设备接收的分片帧数。
- **已发送的分片数 —** WAP 设备发送的分片帧数。
- **已接收的组播帧数 —** 通过目的 MAC 地址中设置的多播位接收的 MSDU（MAC 服务数据单元）帧数。
- **已发送的组播帧数 —** 在目的 MAC 地址中设置多播位的情况下成功发送的 MSDU 帧数。
- **重复帧计数 —** 接收帧并且“序列控制”(Sequence Control) 字段指示它为重复帧的次数。
- **发送失败计数 —** 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 错误计数 —** 在接收的 MPDU 帧中检测到的 FCS （帧检查顺序）错误数。
- **发送重试计数 —** 一次或多次重试后成功发送 MSDU 的次数。
- **ACK 失败计数 —** 没有如期接收到的 ACK 帧数。
- **RTS 失败计数 —** 没有接收到响应 RTS 帧的 CTS 帧数。
- **WEP 无法解密计数** - 由于无线射频无法解密而丢弃的帧数。丢弃帧的原因可能是该帧未加密，也可能是该帧使用了 WAP 设备不支持的隐私选项进行加密。
- **RTS 成功计数 —** 接收到的响应 RTS 帧的 CTS 帧数。
- **多次重试计数 —** 多次重试后成功发送 MSDU 的次数。
- **已发送帧计数 —** 一次成功发送 MSDU 的次数。

可以单击**“刷新”**刷新屏幕并显示最新信息。

电子邮件警报状态

“电子邮件警报状态”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“电子邮件警报状态”页，请在导航窗格中选择**“状态和统计信息”>“电子邮件警报状态”**。

- **电子邮件警报状态 —** 已配置的电子邮件警报状态。状态为“已启用”或“已禁用”。默认值为“已禁用”。
- **已发送的电子邮件数 —** 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。

- **失败电子邮件数 —** 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。
- **最后一封电子邮件的发送时间 —** 发送上一封电子邮件的星期、日期和时间。

可以单击**“刷新”**以显示最新信息。

日志

“日志”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，管理员也可以手动清除日志。最多可以显示 512 个事件。可根据需要从列表中删除较早的条目，为新事件留出空间。

要查看“日志”页，请在导航窗格中选择**“状态和统计信息”>“日志”**。

- **时间戳 —** 事件发生时的系统时间。
- **严重程度 —** 事件是由错误 (err) 引起的还是用于提供信息 (info)。
- **服务 —** 与事件关联的软件组件。
- **说明 —** 事件的说明。

可以单击**“刷新”**刷新屏幕并显示最新信息。

也可以单击**“全部清除”**清除日志中的所有条目。

3

管理

本节介绍如何配置全局系统设置，以及如何执行诊断。

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
- LED 显示
- HTTP/HTTPS 服务
- 管理访问控制
- 管理固件
- 下载/备份配置文件
- 配置文件属性
- 复制/保存配置
- 重启
- 发现 - Bonjour
- 数据包捕获
- 支持信息
- 生成树设置

系统设置

通过“系统设置”页，可以配置用于识别网络内 WAP 设备的信息。

配置系统设置

要配置系统设置，请执行以下步骤：

步骤 1 选择**“管理”>“系统设置”**。

步骤 2 输入以下参数：

- **主机名 —** 使用管理权限为 WAP 设备分配的名称。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。“主机名”标签只能包含字母、数字和连字符。“主机名”标签不能以连字符开头或结尾，也不允许使用其他符号、标点字符或空格。“主机名”可以包含 1 到 63 个字符。
- **系统联系人 —** WAP 设备的联系人。“系统联系人”的长度介于 0 到 255 个字符之间，可以包含空格和特殊字符。
- **系统位置 —** 有关 WAP 设备物理位置的说明。“系统位置”可以包含 0 到 255 个字符，可以包含空格和特殊字符。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

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**
- 密码：**cisco**

通过“用户帐户”页，可以配置最多 4 个其他用户，并且可以更改用户密码。

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**“管理”>“用户帐户”**。

“用户帐户表”将显示当前已配置的用户。用户 **cisco** 是系统中预先配置的用户，具有“读/写访问权限”。

所有其他用户可以拥有“只读访问权限”，但不能拥有“读/写访问权限”。

步骤 2 单击**“添加”**。文本框中会出现新行。

步骤 3 选中新用户对应的复选框，然后选择**“编辑”**。

步骤 4 输入**“用户名”**，应介于 1 至 32 个字母数字字符之间。用户名只能使用数字 0 到 9 和字母 a 到 z（大写或小写）。

步骤 5 输入**“新密码”**（介于 1 至 64 个字符之间），然后在**“确认新密码”**文本框中输入同一密码。

输入密码时，指示条的数量和颜色会发生变化，以指示密码强度，如下所示：

- **红色 —** 密码未满足最低复杂性要求。
- **橙色 —** 密码满足最低复杂性要求，但是密码强度较弱。
- **绿色 —** 密码安全性较强。

步骤 6 单击**“保存”**。更改将保存到“启动配置”。

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**“管理”>“用户帐户”**。

“用户帐户表”将显示当前已配置的用户。用户 **cisco** 是系统中预先配置的用户，具有“读/写访问权限”。用户 **cisco** 的密码可以更改。

步骤 2 选择要配置的用户，然后单击**“编辑”**。

步骤 3 输入**“新密码”**（介于 1 至 64 个字符之间），然后在**“确认新密码”**文本框中输入同一密码。

输入密码时，指示条的数量和颜色会发生变化，以指示密码强度，如下所示：

- **红色** — 密码未满足最低复杂性要求。
- **橙色** — 密码满足最低复杂性要求，但是密码强度较弱。
- **绿色** — 密码安全性较强。

步骤 4 单击**"保存"**。更改将保存到"启动配置"。

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。您既可以手动配置系统时钟，也可以将 WAP 设备配置为网络时间协议 (NTP) 客户端，从服务器获取时钟数据。

通过"时间设置"页，可以手动设置系统时间，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，接入点会配置为从预定义的 NTP 服务器列表获取时间。

页面顶端会显示当前的系统时间以及"系统时钟源"选项。

要利用 NTP 使 WAP 设备自动获取时间设置，请执行以下步骤：

自动通过 NTP 获取时间设置

要自动通过 NTP 获取时间设置，请执行以下步骤：

步骤 1 对于"系统时钟源"字段，选择**"网络时间协议 (NTP)"**。

步骤 2 配置以下参数：

- **NTP 服务器/IPv4/IPv6 地址名称** — 指定 NTP 服务器的 IPv4 地址、 IPv6 地址或主机名。系统会列出默认 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 (.) 分隔各个标签。整个标签和句点字串的长度不能超过 253 个字符。

- **时区** — 选择所在位置的时区。

步骤 3 如果所在时区适用夏令时，请选择**"调整夏令时时间"**。选择之后，请配置以下字段：

- **夏令时开始时间 —** 选择夏令时开始的星期、日、月和时间。
- **夏令时结束时间 —** 选择夏令时结束的星期、日、月和时间。
- **夏令时时差 —** 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 单击**"保存"**。更改将保存到"启动配置"。

手动配置时间设置

要手动配置时间设置，请执行以下步骤：

步骤 1 对于"系统时钟源"字段，选择**"手动"**。

步骤 2 配置以下参数：

- **系统日期 —** 从下拉列表中选择当前月、日和年。
- **系统时间 —** 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。

注 "系统时间"字段旁边有一个箭头，如果您想使用计算机的时间和日期，可利用此箭头通过相应的计算机设置时间。

- **时区 —** 选择您所在位置的时区。

步骤 3 如果所在时区适用夏令时，请选择**"调整夏令时时间"**。选择之后，请配置以下字段：

- **夏令时开始时间 —** 选择夏令时开始的星期、日、月和时间。
- **夏令时结束时间 —** 选择夏令时结束的星期、日、月和时间。
- **夏令时时差 —** 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 单击**"保存"**。更改将保存到"启动配置"。

日志设置

通过"日志设置"页，可以将日志消息保存在永久性存储器中，也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，您可以使用日志消息来诊断原因。但是，除非启用永久日志记录，否则系统重新启动时会擦除日志消息。

注意 启用永久日志记录会占用闪存 （非易失性存储器），并降低网络性能。请仅在调试问题时启用永久日志记录，并确保在完成问题调试之后禁用永久日志记录。

配置永久日志记录

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**“管理”>“日志设置”**。

步骤 2 配置以下参数：

- **永久保存 —** 单击**“启用”**可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。非易失性存储器中最多可以保存 128 条日志消息。达到 128 条的上限时，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。
- **严重程度 —** 事件写入非易失性存储器中的日志时必须达到的最低严重性级别。例如，如果指定 2 （严重），则将严重、警报和紧急级别的事件记录到非易失性存储器。而严重性级别为 3 到 7 的错误消息则会写入易失性存储器。
- **深度 —** 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，此值不可配置。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

Remote Log Server

“内核日志”是一个全面的系统事件 （显示在“系统日志”中）和内核消息 （例如错误状况）列表。

您无法直接从 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，然后才能配置 WAP 设备以登录远程日志服务器。 WAP 设备最多支持两台远程日志服务器。

远程日志服务器的 WAP 设备系统日志消息收集功能具有以下特点：

- 可从多个接入点聚合系统日志消息

- 可存储比单个 WAP 设备更多的消息历史记录
- 可触发基于脚本的管理操作和警报

将主机指定为远程日志服务器

要将网络中的主机指定为远程日志服务器，请执行以下步骤：

步骤 1 在导航窗格中，依次选择 **Administration （管理） > Log Settings （日志设置）**。

步骤 2 在“Remote Log Server Table” （远程日志服务器表）中配置以下参数：

- **Remote Log Server （远程日志服务器） —** 输入远程日志服务器的 IPv4 或 IPv6 地址，或者主机名。

  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。整个标签和句点字串的长度不能超过 253 个字符。

- **Enable （启用） —** 选中以启用此远程日志服务器，然后定义日志严重程度和 UDP 端口。

  Log Severity （日志严重程度） — 选择发送给远程日志服务器的事件必须具有的严重性级别。

- **UDP 端口 —** 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，请确保指定给系统日志的端口号是可用的。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

如果已启用“远程日志”主机，单击**“保存”**将激活远程日志记录。 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，具体取决于实际配置。

如果已禁用“远程日志”主机，单击**“保存”**将禁用远程日志记录。

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。建议在断开连接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证。请使用单独的电子邮件帐户。还要注意，许多电子邮件帐户会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可以访问已发送邮件。所以请检查电子邮件设置，确保其符合企业的隐私策略。

配置接入点以发送电子邮件警报

要配置接入点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**“管理”>“电子邮件警报”**。

步骤 2 在“全局配置”区域中，配置以下参数：

- **管理模式 —** 选择此项可全局启用电子邮件警报功能。
- **电子邮件发件人地址 —** 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，系统未配置任何地址。
- **日志持续时间 —** 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。
- **预定的消息严重程度 —** 系统会将此严重性级别或更高级别的日志消息组合在一起，并按“日志持续时间”指定的频率发送到已配置的电子邮件地址。可选择以下值：无、紧急、警报、严重、错误、警告、注意、信息和调试。如果设置为“无”，系统将不执行“预定的消息严重程度”操作。默认严重性级别为“警告”。
- **紧急消息严重程度 —** 系统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。可选择以下值：无、紧急、警报、严重、错误、警告、注意、信息和调试。如果设置为“无”，系统将不执行“紧急消息严重程度”操作。默认设置为“警报”。

步骤 3 在“邮件服务器配置”区域中，配置以下参数：

- **服务器 IPv4 地址/名称 —** 输入传出 SMTP（简单电子邮件传输协议）服务器的 IP 地址或主机名。（您可以向电子邮件提供商确认此主机名。）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 (.) 分隔各个标签。整个标签和句点字串的长度不能超过 253 个字符。

- **数据加密 —** 输入出站电子邮件警报的安全模式。系统可以使用安全 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。
- **端口 —** 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。
- **用户名 —** 输入用于发送这些邮件的电子邮件帐户的用户名。通常情况下 （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。
- **密码 —** 输入用于发送这些邮件的电子邮件帐户的密码。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。

- **收件人电子邮件地址 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是有效的地址。
- **电子邮件主题 —** 输入在电子邮件主题行中显示的文本。主题是最多可以包含 255 个字符的字母数字字符串。

步骤 5 单击**“测试邮件”**发送测试电子邮件，以验证已配置的电子邮件帐户。

步骤 6 单击**“保存”**。更改将保存到“启动配置”。

电子邮件警报示例

以下示例显示了“邮件服务器配置”参数的填写方式：

```
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
```

以下示例显示了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
```

LED 显示

WAP 设备附带一个 LED 指示灯。通过“LED 显示”页，可以启用或禁用该 LED，并将 LED 与已配置的调度程序配置文件相关联。

默认情况下， “LED 显示”设置为**“启用”**。如果将“LED 显示”设置为**“禁用”**， LED 将会熄灭。当“LED 显示”值设置为**“关联调度程序”**时，此项会显示一个下拉框，用于选择调度程序配置文件。在启用时， LED 会指示 WAP 设备的相关状态和活动。

更改 LED 显示

要更改 LED 显示，请执行以下步骤：

步骤 1 在导航窗格中选择**“管理”>“LED 显示”**。

步骤 2 从下拉框中选择**“启用/禁用/关联调度程序”**。

步骤 3 从下拉选择列表中，选择用于“关联调度程序 LED 显示”的配置文件名称。默认情况下， LED 未关联任何配置文件。下拉选择列表中会显示**“无线”>“调度程序”**页中已配置的调度程序配置文件名称。

当 LED 关联到调度程序配置文件时，此列会根据当天该时刻是否存在活动的配置文件规则来显示状态。

步骤 4 单击**“保存”**。更改将保存到“启动配置”。

HTTP/HTTPS 服务

通过“HTTP/HTTPS 服务”页，可以启用和配置基于 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），您还可以使用“HTTP/HTTPS 服务”页来管理所需的 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**“管理”>“HTTP/HTTPS 服务”**。

步骤 2 配置以下全局设置：

- **最大会话数 —** 可以同时使用的 Web 会话数，包括 HTTP （超文本传输协议）会话和 HTTPS （安全超文本传输协议）会话。

  用户登录 WAP 设备配置实用程序时，系统即会创建一个会话。在用户注销或会话超时过期之前，此会话将一直保留。数值范围介于 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。

- **会话超时值 —** 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，单位为分钟。当达到配置的超时时间时，用户将自动注销。数值范围介于 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 服务器 —** 启用通过 HTTP 的访问。默认情况下， HTTP 访问处于启用状态。如果禁用此设置，当前使用此协议的所有连接都将断开。
- **HTTP 端口 —** 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 服务器 —** 启用通过安全 HTTP 的访问。默认情况下，HTTPS 访问处于启用状态。如果禁用此设置，当前使用此协议的所有连接都将断开。
- **HTTPS 端口 —** 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。

- **将 HTTP 重定向至 HTTPS —** 将 HTTP 端口的管理 HTTP 访问尝试重定向至 HTTPS 端口。此字段仅在禁用 HTTP 访问时可用。

步骤 4 单击**“保存”**。更改将保存到“启动配置”。

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，请单击**“生成 SSL 证书”**。此操作应在接入点获取 IP 地址后完成，这样可以确保证书的通用名称与接入点的 IP 地址匹配。生成新 SSL 证书会重新启动安全 Web 服务器。在浏览器接受新证书之前，安全连接将无法正常工作。

在“证书文件状态”区域中，可以查看 WAP 设备上当前是否存在证书及以下相关信息：

- 存在证书文件
- 证书过期日期
- 证书颁发机构通用名称

如果 WAP 设备上存在 SSL 证书 （扩展名为 .pem 的文件），可将其下载到计算机上进行备份。在“下载 SSL 证书 （从设备到 PC） ”区域中，对于**“下载方式”**，选择**“HTTP”**或**“TFTP”**，然后单击**“下载”**。

- 如果选择“HTTP”，系统会提示确认下载，然后要求您选择在网络中保存此文件的位置。
- 如果选择“TFTP”，则会出现更多字段，要求您输入为下载文件指定的文件名，以及下载文件的 TFTP 服务器地址。

还可以从计算机向 WAP 设备上传证书文件 （扩展名为 .pem 的文件）。在“上传 SSL 证书 （从 PC 到设备） ”区域中，对于**“上传方式”**，选择**“HTTP”**或**“TFTP”**。

- 如果选择“HTTP”，请浏览网络位置，选择文件，然后单击**“上传”**。
- 如果选择“TFTP”，请输入与 TFTP 服务器上的现有文件相同的**“文件名”**以及**“TFTP 服务器 IPv4 地址”**，然后单击**“上传”**。文件名不能包含以下字符：空格、<、 >、 |、 \、 :, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

如果上传成功，系统会显示确认消息。

管理访问控制

您可以创建访问控制列表 (ACL)，列出经授权可以访问 WAP 设备配置实用程序的 IPv4 主机和 IPv6 主机 （每种主机最多 5 个）。如果禁用此功能，任何人只要提供正确的 WAP 设备用户名和密码，都将能够从任何网络客户端访问配置实用程序。

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

注意 请对您所输入的所有 IP 地址进行验证。如果输入的 IP 地址与管理计算机不匹配，则会无法访问配置接口。强烈建议为管理计算机指定静态 IP 地址，这样地址就不会随时间推移而发生变化。

创建访问列表

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**“管理”>“管理访问控制”**。

步骤 2 对于**“管理 ACL 模式”**，选择**“启用”**。

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

步骤 4 验证 IP 地址是否正确。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

管理固件

WAP 设备会保留两个固件映像。一个映像是活动的，另一个则是非活动的。如果在启动期间未能载入活动映像，系统会载入非活动映像，并使其成为活动映像。您也可以手动切换活动映像和非活动映像。

当新版本的接入点固件可用时，您可以升级设备上的固件，以便充分利用新功能和增强功能。本接入点使用 TFTP 或 HTTP 客户端进行固件升级。

在您上传新固件并重新启动系统后，新添加的固件将成为主映像。如果升级失败，原始固件仍将作为主映像。

注 升级固件时，接入点会保留现有的配置信息。

要手动切换接入点上运行的固件映像，请执行以下步骤：

步骤 1 在导航窗格中选择**“管理”>“管理固件”**。

步骤 2 单击**“交换活动映像”**。

此时会出现一个对话框，提示您确认固件映像切换以及随后的重新启动操作。

步骤 3 单击**“确定”**以继续。

此过程可能需要几分钟时间，在此期间接入点将无法访问。映像切换过程中，请勿切断接入点的电源。映像切换完成时，接入点将重新启动。随后，接入点将使用与升级前相同的配置设置继续正常运行。

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**“管理”>“管理固件”**。

系统会显示产品 ID (PID VID) 以及活动和非活动固件版本。

步骤 2 选择**“使用 TFTP 作为传输方式”**。

步骤 3 在**“源文件名”**字段中，输入映像文件的名称 （1 至 128 个字符），应包含所要上传的映像所在目录的路径。

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

所提供的固件升级文件必须是 tar 文件。请勿尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不受支持。

文件名不能包含以下字符：空格、<、>、|、\、:, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

步骤 4 输入**“TFTP 服务器 IPv4 地址”**，然后单击**“升级”**。

上传新软件可能需要几分钟时间。在上传新软件或中断软件上传时，请不要刷新页面或导航至其他页面。上传过程完成后，接入点将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，打开“升级固件”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**“使用 HTTP 作为传输方式”**。

步骤 2 如果知道新文件的名称和路径，可在**“源文件名”**字段中直接输入。否则，请单击**“浏览”**按钮，查找网络中的固件映像文件。

所提供的固件升级文件必须是 tar 文件。请勿尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不受支持。

步骤 3 单击**“升级”**应用新的固件映像。

上传新软件可能需要几分钟时间。在上传新软件或中断软件上传时，请不要刷新页面或导航至其他页面。上传过程完成后，接入点将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，打开“升级固件”页，然后查看活动的固件版本。

下载/备份配置文件

接入点配置文件为 XML 格式，其中包含有关 WAP 设备设置的所有信息。您可以将配置文件备份 （上传）到网络主机或 TFTP 服务器，以便手动编辑内容或创建备份。编辑备份的配置文件后，您可以将其下载到接入点，达到修改配置的目的。

接入点会保留以下配置文件：

- **启动配置 —** 保存到闪存的配置文件。
- **备份配置 —** 作为备份保存在 WAP 设备中的其他配置文件。
- **镜像配置 —** 如果“启动配置”至少有 24 小时无任何修改，则会自动保存为“镜像配置”文件。 “镜像配置”文件是过去的“启动配置”的快照。在恢复出厂设置时， “镜像配置”可以保留，因此在恢复出厂设置后，可通过将“镜像配置”复制到“启动配置”来还原系统配置。

注 配置文件不仅可以下载/上传到其他系统，还可以在 WAP 设备上复制为不同的文件类型。请参阅复制/保存配置。

备份配置文件

要将配置文件备份 （上传）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**“管理”>“下载/备份配置文件”**。

步骤 2 对于**“传输方式”**，选择**“通过 TFTP”**或**“通过 HTTP/HTTPS”**。

步骤 3 对于**“保存操作”**，选择**“备份 （AP 到 PC） ”**。

步骤 4 如果选择 TFTP 备份，请输入**“目标文件名”**（扩展名为 .xml）。文件名应包含此文件在服务器上的路径。随后，输入**“TFTP 服务器 IPv4 地址”**。

文件名不能包含以下字符：空格、<、>、|、\、:, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

步骤 5 如果选择 TFTP 备份，请输入**“TFTP 服务器 IPv4 地址”**。

步骤 6 选择要备份的配置文件：

- **启动配置 —** 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。
- **备份配置 —** WAP 设备中保存的备份配置文件类型。
- **镜像配置 —** 如果“启动配置”至少有 24 小时无任何修改，则会自动保存为“镜像配置”文件。 “镜像配置”文件是过去的“启动配置”的快照。在恢复出厂设置时， “镜像配置”可以保留，因此在恢复出厂设置后，可通过将“镜像配置”复制到“启动配置”来还原系统配置。

步骤 7 单击**“保存”**开始备份。对于 HTTP 备份，系统会显示一个窗口，您可以通过该窗口浏览所需的文件保存位置。

您可以将配置文件下载到接入点，以便更新配置或将接入点恢复为以前备份的配置。

下载配置文件

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**“管理”>“下载/备份配置文件”**。

步骤 2 对于**“传输方式”**，选择**“通过 TFTP”**或**“通过 HTTP/HTTPS”**。

步骤 3 对于**“保存操作”**，选择**下载 （PC 到 AP）**。

步骤 4 如果选择 TFTP 下载，请输入**“源文件名”**（扩展名为 .xml）。文件名应包含此文件在服务器上的路径。随后，输入**“TFTP 服务器 IPv4 地址”**。

文件名不能包含以下字符：空格、<、>、|、\、:, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

步骤 5 选择接入点上要使用下载文件替换的配置文件类型：**“启动配置”**或**“备份配置”**。

如果使用下载文件覆盖“启动配置”文件，并且该文件通过了有效性检查，则下载的配置将在接入点下次重新启动时生效。

步骤 6 单击**“保存”**开始升级或备份。对于 HTTP 下载，系统会显示一个窗口，您可以通过该窗口浏览所需的文件保存位置。下载完成后，系统会显示一个窗口，指示下载成功。

注意 下载配置文件时，请确保接入点电源保持不中断。如果在下载配置文件时发生断电，文件将会丢失，必须重新执行下载过程。

配置文件属性

通过“配置文件属性”页，可以清除“启动配置”文件或“备份配置”文件。如果清除“启动配置”文件，“备份配置”文件将在接入点下次重新启动时变为活动文件。

接入点启动时，会尝试应用启动配置。如果接入点在启动配置中发现任何问题，则会尝试应用镜像配置。如果由于某种原因导致无法应用镜像配置，接入点会尝试应用备份配置。

删除启动配置文件或备份配置文件

要删除“启动配置”文件或“备份配置”文件，请执行以下步骤：

步骤 1 在导航窗格中选择**“管理”>“配置文件属性”**。

步骤 2 选择**“启动配置”**或**“备份配置”**文件类型。

步骤 3 单击**“清除文件”**。

复制/保存配置

通过“复制/保存配置”页，可以在接入点文件系统中复制文件。例如，可以将“备份配置”文件复制为“启动配置”文件类型，以便在下次启动 WAP 设备时使用该文件。

将文件复制为其他文件类型

要将文件复制为其他文件类型，请执行以下步骤：

步骤 1 在导航窗格中选择**“管理”>“复制/保存配置”**。

步骤 2 选择**“源文件名”**：

- **启动配置 —** 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。
- **备份配置 —** WAP 设备中保存的备份配置文件类型。
- **镜像配置 —** 如果“启动配置”至少有 24 小时无任何修改，则会自动保存为“镜像配置”文件。“镜像配置”文件是过去的“启动配置”的快照。在恢复出厂设置时，“镜像配置”可以保留，因此在恢复出厂设置后，可通过将“镜像配置”复制到“启动配置”来还原系统配置。

步骤 3 对于**“目标文件名”**，选择正在复制的文件所要更换到的文件类型。

步骤 4 单击**“保存”**开始复制过程。

完成后，系统会显示一个窗口，提示“复制操作已成功”。

重启

重启接入点

通过“重启”页，可以重新启动接入点。

步骤 1 要重新启动 WAP，请在导航窗格中选择**“管理”>“重启”**。

步骤 2 选择以下选项之一：

- **重启 —** 使用“启动配置”重新启动 WAP。
- **使用出厂默认配置重启 —** 使用出厂默认配置文件重新启动 WAP。任何自定义设置都将丢失。

系统会显示一个窗口，要求您确认或取消重启。当前管理会话可能会终止。

步骤 3 单击**“确定”**可执行重启。

发现 - Bonjour

通过 Bonjour，可以使用多播域名服务器 (mDNS) 发现接入点及其服务。Bonjour 可向网络通告服务，并答复所支持的服务类型发出的查询请求，从而简化小型企业环境中的网络配置。

本接入点可以通告以下服务类型：

- **思科特定设备说明 (csco-sb) —** 通过此服务，客户端可以发现企业网络中部署的思科 WAP 设备以及其他产品。
- **管理用户界面 —** 此服务可识别 WAP 设备中可用的管理界面（HTTP、HTTPS 和 SNMP）。

将启用 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。

默认情况下， Bonjour 处于启用状态。

更改管理状态

要更改管理状态，请执行以下步骤：

步骤 1 在导航窗口中选择**“管理”>“发现 - Bonjour”**。

步骤 2 单击**“启用”**以启用 Bonjour，或取消选中**“启用”**以禁用 Bonjour。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

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 设备可以将文件传输到 TFTP 服务器，或者通过 HTTP(S) 下载到计算机。此文件为 pcap 格式，可使用 Wireshark 或 OmniPeek 等工具进行检查。

- **远程捕获 —** 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。
- **CloudShark 捕获 —** 捕获的数据包可以实时上传到 CloudShark 设备中。CloudShark 设备负责管理捕获，以便对所有捕获执行命名、标记和搜索操作。

注 CloudShark 是一个 Web 网络分析程序，可使用任意 Web 浏览器访问，无需任何其他实用程序、插件或下载文件。

WAP 设备可以捕获以下类型的数据包：

- 无线射频接口接收和发送的 802.11 数据包。无线射频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。

单击**“管理”>“数据包捕获”**，显示“数据包捕获”页。在“数据包捕获”页中，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。

通过“数据包捕获配置”区域，可以配置参数和启动数据包捕获。

配置数据包捕获

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：

- **捕获信标 —** 启用或禁用捕获无线射频检测或无线射频传输的 802.11 信标。
- **混杂捕获 —** 在捕获处于活动状态时，启用或禁用混杂模式。

  在混杂模式下，无线射频会接收信道中的所有流量，包括非发送给此 WAP 设备的流量。无线射频在混杂模式下运行时，会继续向关联的客户端提供服务，但不会转发非发送给此 WAP 设备的数据包。

  捕获完成后，无线射频立即恢复为非混杂模式运行。

- **无线射频客户端过滤器 —** 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。
- **客户端过滤器 MAC 地址 —** 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 过滤器才处于活动状态。

- **数据包捕获方式 —** 请选择以下选项之一：
  - **本地文件 —** 捕获的数据包存储在 WAP 设备上的文件中。
  - **远程 —** 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。
  - **CloudShark —** 捕获的数据包可以实时上传到 CloudShark 设备中。

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**“数据包捕获方式”**选择**“本地文件”**。

步骤 2 配置以下参数：

- **捕获接口 —** 输入数据包捕获的捕获接口类型：
  - **radio1 —** 无线射频接口 Radio 1 上的 802.11 流量。
  - **radio2 —** Radio 2 上的 802.11 流量。
  - **eth0 —** 以太网端口上的 802.3 流量。
  - **wlan0 —** Radio 1 上的 VAP0 流量。
  - **wlan1 —** Radio 2 上的 VAP0 流量。
  - **wlan0vap1** 至 **wlan0vap7 —** 指定 VAP 中 Radio 1 上的流量。
  - **wlan1vap1** 至 **wlan1vap7 —** 指定 VAP 中 Radio 2 上的流量。
  - **wlan0wds0** 至 **wlan0wds3 —** 指定 WDS 接口上的流量。
  - **brtrunk —** WAP 设备中的 Linux 网桥接口。

- **捕获持续时间 —** 输入捕获持续时间，单位为秒。范围介于 10 至 3600 之间。默认值为 60。对于使用 CloudShark 的无限制数据包捕获方法，此值可以为 0。
- **最大捕获文件大小 —** 输入允许的最大捕获文件大小，单位为 KB。范围介于 64 至 4096 之间。默认为 1024。对于使用 CloudShark 的数据包捕获方法，不启用此选项。

步骤 3 单击**"保存"**。更改将保存到"启动配置"。

步骤 4 单击**"开始捕获"**。

在"数据包文件捕获"模式下， WAP 设备会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设置处于活动状态，此页的"数据包捕获状态"区域会显示数据包捕获状态。

- **当前捕获状态 —** 数据包捕获是正在运行还是已经停止。
- **数据包捕获时间 —** 已经过的捕获时间。
- **数据包捕获文件大小 —** 当前捕获文件的大小。如果使用的是捕获文件大小受限的免费 CloudShark 帐户，此大小通常大于 CloudShark 中的捕获文件大小。
- **CloudShark 捕获文件上传状态 —** 如果所选的 CloudShark 数据包捕获文件成功上传，系统会显示一个链接。可以单击**"查看 CloudShark 上的捕获结果"**超链接，以打开浏览器窗口并查看 CloudShark 设备上捕获的数据包。

注 如果上传失败，系统会显示错误消息。

单击**"刷新"**显示 WAP 设备的最新数据。

注 要停止数据包文件捕获，请单击**"停止捕获"**。

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。

在 WAP 设备上启动远程捕获

要在 WAP 设备上启动远程捕获，请执行以下步骤：

步骤 1 单击**“管理”**>**“数据包捕获”**。

步骤 2 启用**“混杂捕获”**。

步骤 3 对于**“数据包捕获方式”**，选择**“远程”**。

步骤 4 对**“远程捕获端口”**使用默认端口 (2002)；如果不使用默认端口，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，请单击**“保存”**。

步骤 6 单击**“开始捕获”**。

启动网络分析程序

要启动 Microsoft Windows 版本的 Wireshark 网络分析程序，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**“捕获”**>**“选项”**。系统将显示一个弹出窗口。

步骤 3 对于**“接口”**，选择**“远程”**。系统将显示一个弹出窗口。

步骤 4 在**“主机”**字段中，输入 WAP 设备的 IP 地址。

步骤 5 在**“端口”**字段中，输入 WAP 的端口号。例如，如果使用默认端口，请输入 2002；如果不使用默认端口，请输入相应的端口号。

步骤 6 单击**“确定”**。

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，请从中选择接口。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 上的 VAP0 流量
-- rpcap://[192.168.1.220]:2002/wlan0
802.11 流量
-- rpcap://[192.168.1.220]:2002/radio1
WAP571/E 中 Radio 1 上的 VAP1 至 VAP7 流量
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
WAP571/E 中 Radio 2 上的 VAP1 至 VAP7 流量
-- rpcap://[192.168.1.220]:2002/wlan1vap1 ~ wlan1vap7

您最多可以同时跟踪 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。

在无线射频接口中捕获流量时，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，并且此影响会逐渐减小，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（通常所有接入点每 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。

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。捕获文件位于 RAM 文件系统中，如果重置 WAP 设备，此文件将会消失。

使用 TFTP 下载数据包捕获文件

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**“使用 TFTP 下载捕获文件”**。

步骤 2 如果不使用默认设置，请输入**“TFTP 服务器文件名”**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 在相应的字段中，指定**“TFTP 服务器 IPv4 地址”**。

步骤 4 单击**“下载”**。

使用 HTTP 下载数据包捕获文件

要使用 HTTP 下载数据包捕获文件，请执行以下步骤：

步骤 1 取消选择**“使用 TFTP 下载捕获文件”**。

步骤 2 单击**“下载”**。系统会显示确认窗口。

步骤 3 单击**“确定”**。随即会出现一个对话框，请在其中选择保存文件的网络位置。

支持信息

通过“支持信息”页，可以下载包含接入点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。您可以将此文本文件提供给技术支持人员，以便于他们对问题进行故障排除。

要显示“支持信息”页，请在导航窗格中选择**“管理”>“支持信息”**。

单击**“下载”**，以当前系统设置为基础生成文件。稍等片刻后，系统会显示一个窗口，用于将文件保存到您的计算机。

生成树设置

通过“生成树设置”页，可以配置思科 WAP571/E 的 STP 设置。

在思科 WAP571 上配置 STP 设置

要在思科 WAP571/E 上配置 STP 设置，请执行以下步骤：

步骤 1 选择**“管理”>“生成树设置”**。

步骤 2 配置以下参数：

STP 状态 — 在思科 WAP571/E 上全局启用或禁用 STP。默认情况下， STP 是启用状态。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

4

LAN （局域网）

本章介绍如何配置 WAP 设备的端口、 VLAN、 IPv4 和 IPv6 设置。

具体包括以下主题：

- 端口设置
- VLAN 配置
- IPv4 设置
- IPv6 设置
- IPv6 隧道
- LLDP

端口设置

通过“端口设置”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。

配置端口设置

要配置“端口设置”，请执行以下步骤：

步骤 1 选择**“LAN”>“端口设置”**。

“端口设置表”包括以下状态和配置，适用于 2 个接口 （Eth0 至 Eth1）：

- **链路状态 —** 指示当前端口链路的状态。
- **端口速度 —** 在查看模式中，会显示当前端口速度。在编辑模式中，如果“自动协商”被禁用，请选择一种端口速度，例如 100 Mbps 或 10 Mbps。只有“自动协商”启用时才支持 1000 Mbps 的速度。
- 双工模式 — 在查看模式中，会显示当前端口的双工模式。在编辑模式中，如果“自动协商”被禁用，请选择“半双工”或“全双工”。

自动协商 — 如果启用，端口会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”。

绿色以太网 —“绿色以太网模式”同时支持自动断电模式和 EEE （节能以太网， IEEE 802.3az）模式。只有在端口已启用自动协商时，才可以使用“绿色以太网模式”。自动关闭电源模式可以在链路伙伴的信号不存在时降低芯片功耗。 WAP 设备可在线路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。 EEE 模式支持在链路利用率低时使用静默时间，允许链路两端同时禁用每个 PHY 的部分工作电路以节省能源。

- **绿色以太网状态 —** 显示当前 EEE 状态。

步骤 2 选中要编辑的接口，然后单击“编辑”按钮进入编辑模式。然后输入您的设置。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

注 WAP571/E 始终带有两个支持链路聚合模式的 Eth0 和 Eth1 端口。链路伙伴也必须支持链路聚合。 Eth1 将始终遵循 Eth0 配置。

VLAN 配置

使用“VLAN 配置”页可查看和配置 VLAN 设置。

要配置 VLAN 设置，请执行以下步骤：

步骤 1 选择**“LAN”>“VLAN 配置”**。

步骤 2 在“VLAN 设置表”中，每条 VLAN 记录都包含以下字段：

- **VLAN ID —** VLAN 的标识符。每个 VLAN ID 都介于 1 至 4094 之间，且应不同于其他 VLAN ID。
- **说明 —** 相关 VLAN 的说明。长度应小于 64 个字符，且应由以下字符组成：A-Z、 a-z、 0-9、 _。

步骤 3 **“管理 VLAN”—** 管理 VLAN 是用于通过 Web GUI 访问 WAP 设备的 VLAN。必须有且仅有一个 VLAN 作为管理 VLAN。如果没有从属于管理 VLAN 的 （有线或无线）接口，用户将没有能用于访问配置实用程序的接口。

- **Eth0 - Eth1 —** 每个端口最多只应有一个未添加标签的 VLAN。选项如下：
  - **未添加标签 —** 端口是 VLAN 的成员。 VLAN 中从此端口发送的数据包将处于未添加标签状态。此端口接收的未添加标签数据包将被分类到 VLAN （已添加标签）。

- **已添加标签 —** 端口是 VLAN 的成员。 VLAN 中从此端口发送的数据包将使用 VLAN 报头进行标记。
- **已排除 —** 端口不属于 VLAN。

注 VLAN ID 1 不能删除。如果删除 VLAN 相关的（有线或无线）端口，WAP 设备将自动把自己的 VLAN ID 设置为 1。

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。

IPv4 设置

使用“IPv4 设置”页可配置静态或动态 IPv4 地址分配。

要配置 IPv4 地址设置，请执行以下步骤：

步骤 1 选择**“LAN”>“IPv4 设置”**。

步骤 2 配置以下 IPv4 设置：

- **连接类型 —** 默认情况下， WAP 设备中的 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。

  请选择以下选项之一：

  - **DHCP —** WAP 设备从局域网的 DHCP 服务器获取其 IP 地址。
  - **静态 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。
- 静态 IP 地址、子网掩码和默认网关 — 如果希望指定静态 IP 地址，请在这些字段中输入 IP 信息。
- **域名服务器 —** 请选择以下其中一个选项：
  - **动态 —** WAP 设备从局域网的 DHCP 服务器获取 DNS 服务器地址。
  - **手动 —** 手动配置一个或多个 DNS 服务器地址。最多在提供的字段中输入两个 IP 地址。

步骤 3 配置以下 IPv4 DCHP 自动配置设置：

- **DHCP Auto Configuration Options （DHCP 自动配置选项） —** 默认情况下，此选项处于启用状态。如果无线接入点使用的是出厂默认设置，它会首先尝试使用 DHCP 选项进行自动配置。

  在自动配置过程中：

  - 无线接入点会在仅启用以太网接口的情况下启动 （WLAN 接口会关闭）。
  - 除显示用户界面外，不会为用户提供任何服务。
  - 在经过“Wait Interval” （等待间隔）或配置文件完成 TFTP 上传后 （以先到为准），“DHCP Auto Configuration Options” （DHCP 自动配置选项）会自动变为禁用状态。
  - 如果禁用 DHCP 客户端 （例如使用静态 IP 地址进行配置）或禁用“DHCP Auto Configuration Options” （DHCP 自动配置选项），自动配置过程会立即中止。

  WAP 设备上的 DHCP 客户端会自动广播对 DHCP 选项 66 和 67 的请求。如果启用“DHCP”和“DHCP Auto Configuration Options” （DHCP 自动配置选项），无线接入点在下次启动时，会依据从用于 DHCP 请求的 DHCP 服务器收到的信息进行自动配置。

注 用户/管理员上传的配置会覆盖自动配置，以确保用户/管理员选择的配置文件具有更高的优先级。如果是在任何其他情况下重新启动无线接入点 （固件升级/手动重新启动等），都将使用现有自动配置设置。

- **Backup TFTP Server IPv4 address/Host Name （备份 TFTP 服务器 IPv4 地址/主机名） —** 如果您配置了 TFTP 服务器地址，当自动配置失败时，无线接入点会使用该地址从 DHCP 服务器指定的其他 TFTP 服务器检索文件。您可以输入 IPv4 地址或主机名信息。如果使用主机名格式，您必须确保能够连接到 DNS 服务器，以便将主机名转换为 IP 地址。

  此设置值会在无线接入点下次启动时用于自动配置过程。

- **Configuration File Name （配置文件名） —** 如果您指定了配置文件名，而启动文件名不是从 DHCP 服务器进行接收的，那么无线接入点在自动配置过程中会从 TFTP 服务器检索您指定的文件。如果不指定此值，无线接入点会默认使用“config.xml”。如果指定此值，文件扩展名必须为 xml。

  此设置值会在无线接入点下次启动时用于自动配置过程。

- **Wait Interval （等待间隔） —** 如果配置此设置，无线接入点会使用本地配置，并在“等待间隔”结束后向用户提供已启用的服务。如果 TFTP 事务在此指定间隔内未完成初始化，无线接入点会中止自动配置过程。

  此设置值会在无线接入点下次启动时用于自动配置过程。

- **Status Log （状态日志） —** 此字段用于显示自动配置完成或中止的原因。

步骤 4 单击 **Save**（保存）。更改将保存到“Startup Configuration”（启动配置）。

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 设置

使用“IPv6 设置”页可将 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 选择**“LAN”>“IPv6 设置”**。

步骤 2 配置以下参数：

- **IPv6 连接类型 —** 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。
  - **静态 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。

注 如果配置了“静态 IPv6”，将禁用 DHCPv6。在配置了“DHCPv6”后，如果配置存在，则可运行“静态 IPv6”。

- **IPv6 管理模式 —** 启用或禁用 IPv6 管理访问。
- **IPv6 自动配置管理模式 —** 启用或禁用 WAP 设备中的 IPv6 自动地址配置。

  如果启用， WAP 设备会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。
- **静态 IPv6 地址 —** 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）。
- **静态 IPv6 地址前缀长度 —** 静态地址的前缀长度，介于 0 至 128 之间的整数，默认值为 0。
- **静态 IPv6 地址状态 —** 请选择以下其中一个选项：
  - **“可使用”(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。

- **不确定 —** 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。
- **“空 （无值） ”(Blank [no value]) —** 未指定 IP 地址或指定的地址没有运行。

- **自动配置的 IPv6 全局地址 —** 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 链路本地地址 —** 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。
- **默认 IPv6 网关 —** 静态配置的默认 IPv6 网关。
- **IPv6 域名服务器 —** 请选择以下其中一个选项：
  - **动态 —** 通过 DHCPv6 动态获取 DNS 名称服务器。
  - **手动 —** 在提供的字段中手动指定最多两个 IPv6 DNS 名称服务器。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

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 隧道

WAP571/E 设备支持站内自动隧道寻址协议 (ISATAP)。通过 ISATAP， WAP 设备可以通过局域网发送 IPv4 数据包内封装的 IPv6 数据包。通过此协议， WAP 设备可以与支持 IPv6 的远程主机通信，即使连接它们的局域网不支持 IPv6 也没有问题。

WAP 设备可以用作 ISATAP 客户端。已启用 ISATAP 的主机或路由器必须位于局域网中。路由器的 IP 地址或主机名是在 WAP 设备上配置的 （默认情况下是 isatap）。如果将其配置为主机名， WAP 设备会与 DNS 服务器进行通信以将此名称解析为一个或多个 ISATAP 路由器地址。然后 WAP 设备将请求消息发送到路由器。已启用 ISATAP 的路由器回复通告消息后， WAP 设备和路由器建立隧道。为隧道接口指定链路本地和全局 IPv6 地址，隧道接口可以用作 IPv4 网络中的虚拟 IPv6 接口。

IPv6 主机发起与通过 ISATAP 路由器连接的 WAP 设备之间的通信时， ISATAP 路由器将 IPv6 数据包封装到 IPv4 数据包中。

要使用 ISATAP 配置 IPv6 隧道，请执行以下步骤：

步骤 1 在导航区域选择**“LAN”>“IPv6 隧道”**。

步骤 2 配置以下参数：

- **ISATAP 状态** — 启用或禁用 WAP 设备中的 ISATAP 的管理模式。
- **支持 ISATAP 的主机** — ISATAP 路由器的 IP 地址或 DNS 名称。默认值为 isatap。
- **ISATAP 查询间隔** — 指定接入点应向 DNS 服务器发送查询以尝试将 ISATAP 主机名解析为 IP 地址的频率。 WAP 仅在 ISATAP 路由器的 IP 地址未知时发送 DNS 查询。有效范围介于 120 至 3600 秒之间。默认值为 120 秒。
- **ISATAP 请求间隔** — 指定 WAP 应向其通过 DNS 查询消息获取的 ISATAP 路由器发送路由器请求消息的频率。 WAP 仅在没有活动 ISATAP 路由器时发送路由器请求消息。有效范围介于 120 至 3600 秒之间。默认值为 120 秒。

步骤 3 单击**“保存”**。设置将保存到“启动配置”。

建立隧道后，页面中显示**“ISATAP IPv6 链路本地地址”**和**“ISATAP IPv6 全局地址”**。这些是 IPv4 网络的虚拟 IPv6 接口地址。

LLDP

链路层发现协议 (LLDP) 由 EEE 802.1AB 标准定义，允许 UAP 通告有关它自身的信息（例如系统名称、系统功能和电源要求）。此类信息可以帮助识别系统拓扑并检测局域网中的不良配置。此接入点还支持链路层发现协议-媒体终端发现 (LLDP-MED) 协议，该协议可标准化设备彼此传输的其他信息元素，从而改善网络管理。

配置 LLDP 设置

要配置 LLDP 设置，请执行以下步骤：

步骤 1 在导航区域选择**“LAN”>“LLDP”**。

步骤 2 配置以下参数：

- **LLDP 模式** — 接入点中 LLDP 的管理模式。在启用 LLDP 后，接入点会将 LLDP 协议数据单元发送给邻居设备。
- **发送间隔** — LLDP 消息传输间隔的秒数。有效范围介于 5 至 32768 秒之间。默认的值为 30 秒。

- **POE 优先级 —** 扩展电源信息元素中由接入点发送的优先级。当供电设备 (PSE)（例如交换机）没有足够的容量为所有连接的设备供电时， PoE 优先级可帮助 PSE 确定在分配功率时应优先考虑哪些受电设备。 PoE 优先级可以是以下类型之一：
  - 严重
  - 高
  - 低
  - 未知

步骤 3 单击**“保存”**。设置将保存到系统中。

5

无线

本章介绍如何配置无线射频操作的属性。

具体包括以下主题：

- 无线射频
- 恶意 AP 检测
- 网络
- 无线组播转发
- 调度程序
- 调度程序关联
- MAC 过滤
- 网桥
- QoS

无线射频

无线射频设置直接控制无线射频在 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。

配置无线射频设置

要配置无线射频设置，请执行以下步骤：

步骤 1 在导航窗格中选择**“无线”>“无线射频”**。

步骤 2 在“全局设置”区域中配置**“TSPEC 违规间隔”**，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 选择**"无线射频"** 接口进行配置 （Radio 1 或 Radio 2）。

步骤 4 在"基本设置"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射频模式。某些模式在部分国家/地区不可用。

- **无线射频 —** 打开或关闭无线射频接口。默认情况下，无线射频为开启状态。

注 如果您启用了带宽为 80 MHz 的 5 GHz 无线射频且此无线射频承载了非常大的流量，则 WAP 设备所需的电源功率将超过 IEEE 802.3af PoE 标准提供的电源功率 (12.95 W)。强烈建议在使用 80 MHz 信道时，应使用 802.3at 供电设备 (PSE) 为 WAP 设备供电。如果 WAP 设备所需电源功率超过 PSE 提供的最大功率，则 WAP 设备可能会重启。

- **MAC 地址 —** 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。
- **模式 —** 无线射频使用的 IEEE 802.11 标准和频率。Radio 1 的"模式"设置默认值是 802.11a/n/ac，Radio 2 的"模式"设置默认值是 802.11b/g/n。请为每个无线射频选择一个可用的模式。

  Radio 1 支持以下无线射频模式：

  - 802.11a — 仅 802.11a 客户端可以连接到 WAP 设备。
  - 802.11a/n/ac — 以 5-GHz 频率运行的 802.11a、 802.11n 和 802.11ac 客户端可以连接到 WAP 设备。
  - 802.11n/ac — 以 5-GHz 频率运行的 802.11n 和 802.11ac 客户端可以连接到 WAP 设备。

  Radio 2 支持以下无线射频模式：

  - 802.11b/g — 802.11b 和 802.11g 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。
  - 802.11n 2.4-GHz — 仅以 2.4 GHz 频率运行的 802.11n 客户端可以连接到 WAP 设备。
- **信道带宽** （仅 802.11n 和 802.11ac 模式） — 802.11n 规范除了允许将传统 20 MHz 信道用于其他模式，也允许使用 40 MHz 信道带宽。 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。

  802.11ac 规范除了允许使用 20 MHz 和 40 MHz 信道，也允许使用 80 MHz 信道带宽。

  如果将该字段设置为 20 MHz，则仅可使用 20MHz 信道的信道带宽。对于 802.11ac 模式，如果将该字段设置为 40 MHz，则无线射频将无法使用 80 MHz 信道带宽。

- **主信道**（仅使用 20 或 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“主信道”和“备用信道”。“主信道”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：

  - **“高频”(Upper)** — 将“主信道”设置为 40 MHz 频段中大于 20 MHz 的信道。
  - **“低频”(Lower)** — 将“主信道”设置为 40 MHz 频段中小于 20 MHz 的信道。“低频”(Lower) 是默认选择。

- **信道** — 无线射频用于发送和接收的无线射频频谱部分。

  可用信道的范围由无线射频接口的模式和国家/地区代码的设置决定。如果选择 **“自动”**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美国联邦通信委员会 (FCC)、国际电信联盟 (ITU-R) 等国家和跨国监管机构的许可。

- **Spectrum Analysis Mode （频谱分析模式）** — 频谱分析模式的状态，可以是“Disable”（禁用）、“Dedicated Spectrum Analyzer”（专用频谱分析器）或“Hybrid Spectrum Analyzer”（混合频谱分析器）。默认设置为“Disable”（禁用）。

步骤 5 在“高级设置”区域中配置以下设置：

- **Air Time Fairness**— 此设置用于启用/禁用 Air Time Fairness 功能。此功能可以解决高速数据传输被低速数据传输拖慢的问题。
- **DFS 支持** — 此字段仅在所选的无线射频模式在 5 GHz 频率下运行时可用。

  对于在 5 GHz 频段下运行的无线射频，当“DFS 支持”已开启且调节域需要在相应信道上进行雷达检测时，系统将激活 802.11h 的动态频率选择 (DFS) 和发射功率控制 (TPC) 功能。

  DFS 功能不仅可以要求无线设备共用频谱，还可以避免雷达系统在 5 GHz 频段下发生同信道运行。DFS 要求因调节域而异，具体取决于接入点的国家/地区代码设置。

  当使用 802.11h 无线模式时，以下是有关 IEEE 802.11h 标准的几个要点：

  - 802.11h 仅适用于 5 GHz 频段。 2.4 GHz 频段不需要此标准。
  - 如果接入点在启用 802.11h 的域中运行，则接入点会尝试使用所分配的信道。如果信道已由以前的雷达检测阻止或接入点在信道中检测到雷达，则接入点会自动选择不同的信道。

- 如果启用 802.11h，由于雷达扫描，接入点在 5 GHz 频段中至少 60 秒无法使用。
- 当使用 802.11h 时，设置 WDS 链路可能比较困难。这是因为 WDS 链路中两个接入点的工作信道可能会不断改变，具体取决于信道使用和雷达干扰。如果两个接入点在同一信道中运行，仅 WDS 可以正常工作。有关 WDS 的详请，请参阅网桥。

- **支持的较短保护间隔 —** 此字段仅在所选的无线射频模式包含 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。
  - **否 —** WAP 设备以 800 纳秒的保护间隔发送数据。

- **保护 —** 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的规则。默认情况下，启用“保护” （自动）。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 （“关闭”[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。

- **信标间隔 —** 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 周期 —** 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。

- **分片阈值 —** 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。

  无法对已聚合的 802.11n 或 802.11ac 帧 (AMPDU) 进行分片。分片仅适用于传统无线射频模式（802.11a 或 802.11b/g）。

  默认情况下，关闭分片。除非怀疑存在无线射频干扰，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 阈值 —** 发送请求 (RTS) 阈值。有效的整数范围必须介于 0 至 65535 之间，默认值为 65535 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。

  RTS 阈值仅适用于传统 802.11 数据帧（例如不适用于 802.11n 或 802.11ac）。如果使用的是 802.11n 和 802.11ac， AMPDU 传输会受到 RTS/CTS 交换的保护，而与帧长度无关。

- **带宽利用率 — 在 WAP 设备禁止新客户端关联之前可使用的无线射频带宽。有效的整数范围介于 0 至 100% 之间。如果设置为 0，无论利用率为多少，都将允许所有新的关联。默认值为 0。**

- **最大关联客户端数 —** 允许在任何一个时刻访问此 WAP 设备的每个无线射频的最大工作站数。可输入一个介于 0 至 200 之间的整数。默认值为 200 个工作站。双频 WAP571/E 设备最多共可支持 400 个客户端。
- **发射功率 —** 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。
- **帧突发支持 — 通常，启用帧突发支持有助于改善下行方向的无线射频性能。**
- **固定组播速率 —** 广播和组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，此设置在发生无线组播视频流的环境中会很有用。

  如果选择**自动**， 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射频模式决定。
- **传统速率集 —** 速率以兆位/秒表示。

  “支持的速率集”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。

  “基本速率集”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。
- **广播/组播速率限制 —** 通过限制整个网络传输的数据包数，组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“广播/组播速率限制”选项。在启用“广播/组播速率限制”之前，禁用以下字段：

  - **速率限制 —** 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。
  - **速率限制突发 —** 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 模式 —** 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：
  - **“开启”(On) —** WAP 设备根据“无线射频”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。
  - **“关闭”(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 语音 ACM 模式 —** 控制语音接入类别的强制准入控制 (ACM)。默认情况下，关闭“TSPEC 语音 ACM 模式”。选项如下：
  - **“开启”(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，结果包含分配的介质时间。
  - **“关闭”(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 语音 ACM 限制 —** 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 视频 ACM 模式 —** 控制视频接入类别的强制准入控制。默认情况下，关闭“TSPEC 视频 ACM 模式”。选项如下：
  - **“开启”(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，结果包含分配的介质时间。
  - **“关闭”(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 视频 ACM 限制 —** 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 不活动超时值 —** 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 工作站不活动超时值 —** 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 传统 WMM 队列映射模式 —** 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。

- **TurboQAM —** 此功能可以启用/禁用适用于 Broadcom 至 Broadcom 链路的 VHT Broadcom 特定扩展。 VHT 功能支持 802.11ac 草案未规定的 256QAM VHT 速率。这些速率全部都处于 VHT LDPC 模式（MCS 9 Nss 1 20Mhz、MCS 9 Nss 2 20Mhz 和 MCS 6 Nss 3 80Mhz）。 802.11ac PHY 支持 VHT 功能。

步骤 6 单击**“保存”**。更改将保存到“启动配置”。

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。建议在断开连接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

恶意接入点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接入点，未经授权的用户可能会借此访问网络。

接入点对每个无线射频中的所有信道进行 RF （射频）扫描，可检测出网络范围内的所有接入点。如果检测到恶意接入点，会将其显示在“恶意 AP 检测”页上。如果列为恶意的接入点是合法的，可以将其添加到“已知 AP 列表”中。

注 “已检测到的恶意 AP 列表”和“受信任的 AP 列表”可提供采取进一步措施所需的信息。接入点对这些列表中的恶意接入点不会有任何的控制，无法对通过 RF 扫描检测到的接入点应用任何安全策略。

要查看有关恶意接入点的详情，请在主导航窗格中选择“无线”>“恶意 AP 检测”。

要查看有关恶意接入点的详情，请选择**“无线”>“恶意 AP 检测”**。

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

查看恶意 AP 列表

可以启用和禁用恶意 AP 检测。要启用无线射频以收集有关恶意接入点的信息，单击 Radio 1 或 Radio 2 的**“AP 检测”**旁边的**“启用”**，然后单击**“保存”**。

恶意 AP 检测无法进行刷新，并且检测到恶意接入点后，相应的 SSID 仍将保留在数据库中。

系统会显示有关检测到的和受信任的恶意接入点的信息。可以单击**"刷新"**刷新屏幕，然后显示以下最新信息：

- **操作 —** 如果接入点出现在"已检测到的恶意 AP 列表"中，可以单击**"信任"**将接入点移到"受信任的 AP 列表"中。

  如果接入点出现在"受信任的 AP 列表"中，可以单击**"不可信任"**将接入点移到"已检测到的恶意 AP 列表"中。

注 "已检测到的恶意 AP 列表"和"受信任的 AP 列表"可提供信息。对这些列表中的接入点不会有任何的控制，无法对通过 RF 扫描检测到的接入点应用任何安全策略。

- **MAC 地址 —** 恶意接入点的 MAC 地址。
- **无线射频 —** 表示恶意接入点是在 Radio 1 (WLAN0) 还是 Radio 2 (WLAN1) 上检测到的。
- **信标间隔 —** 恶意接入点使用的信标间隔。

  信标帧由接入点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 "信标间隔"是在无线射频页上设置的。

- **类型 —** 设备类型：
  - 接入点表示恶意设备是在基础设施模式下支持 IEEE 802.11 无线网络架构的接入点。
  - 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，无需使用传统接入点。 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。
- **隐私 —** 表示恶意设备上是否存在任何安全性：
  - "关闭"(Off) 表示恶意设备上的"安全模式"设置为"无" （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接入点的安全性。

- **WPA —** 打开还是关闭恶意接入点的 WPA 安全性。
- **频段 —** 恶意接入点中正在使用的 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、 802.11n 或 802.11ac 模式 （或这些模式的组合）。

- **信道 —** 当前广播恶意接入点的信道。

  信道可定义无线射频用于发送和接收的无线射频频谱部分。

注 可以使用无线射频页设置信道。

注 当接入点在 DFS 信道中运行时，禁止扫描。因此不会检测到任何恶意接入点。

- **速率 —** 当前传输恶意接入点的速率 （兆位/秒）。

  当前速率始终都是“支持的速率”中所示速率之一。

  报告的速率是从接入点传输到客户端的最后一个数据包的速率。此值在基于接入点和客户端之间的信号质量的通告速率集中有所不同，并且广播帧或组播帧也以此速率进行发送。当接入点使用默认速率向 STA 发送广播帧时，对于 2.4 Ghz 无线射频，此字段报告的值将为 1 Mbps；对于 5 Ghz 无线射频，此字段报告的值将为 6 Mbps。空闲的客户端最可能报告较低的默认速率。

- **信号 —** 从恶意接入点发出的无线射频信号的强度。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。
- **信标 —** 自首次发现信标后从恶意接入点接收的信标总数。
- **最后一个信标 —** 从恶意接入点接收的最后一个信标的日期和时间。
- **速率 —** 恶意接入点的支持和基本 （通告）速率集。速率以兆位/秒 (Mbps) 为单位显示。

  会列出所有“支持的速率”，其中“基本速率”以粗体显示。速率集是在无线射频页中配置的。

创建并保存受信任的 AP 列表

要创建受信任的 AP 列表并将其保存到文件中，请执行以下步骤：

步骤 1 在“已检测到的恶意 AP 列表”中，对已知的接入点单击**“信任”**。受信任的接入点会移到“受信任的 AP 列表”中。

步骤 2 在“下载/备份受信任的 AP 列表”区域，选择**“备份 （AP 到 PC） ”**。

步骤 3 单击**“保存”**。

列表包含已添加到“已知 AP 列表”中的所有接入点的 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。

导入受信任的 AP 列表

可以从保存的列表中导入已知 AP 列表。可能要从另一接入点获取或基于文本文件创建列表。如果接入点的 MAC 地址出现在“受信任的 AP 列表”中，不会将其检测为恶意接入点。

要从文件导入 AP 列表，请执行以下步骤：

步骤 1 在“下载/备份受信任的 AP 列表”区域，选择**“下载 （PC 到 AP） ”**。

步骤 2 单击**“浏览”**，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。对于要接受文件的接入点，必须仅包含 MAC 地址。

步骤 3 选择是替换现有的“受信任的 AP 列表”还是将导入文件中的条目添加到“受信任的 AP 列表”中。

a. 选择**“取代”**可以导入列表并替换“已知 AP 列表”的内容。

b. 选择**“合并”**可以导入列表并将导入文件中的接入点添加到“已知 AP 列表”当前显示的接入点中。

步骤 4 单击**“保存”**。

导入完成后，屏幕刷新，导入文件中的接入点的 MAC 地址出现在“已知 AP 列表”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。接入点最多支持 16 个 VAP。除了 VAP0，可以单独启用或禁用其他所有的 VAP。 VAP0 是物理无线射频接口，只要无线射频启用即保持启用状态。要禁用 VAP0 的运行，必须禁用无线射频本身。

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 广播”。

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)。

允许使用的字符包括：

从 0x20 到 0x7E 的 ASCII 字符。

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。 WAP571/E 设备支持 33 个活动虚拟局域网（其中 32 个是无线局域网， 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，这也是默认的未标记 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**“无线”>“网络”**。

步骤 2 选择要在其上配置 VAP 的**“无线射频”**接口 （**Radio 1** 或 **Radio 2**）。

步骤 3 选中要配置的 VAP 相应的**“已启用”**复选框。

— 或 —

如果 VAP0 是系统中配置的唯一的 VAP，并且要添加 VAP，请单击**“添加”**。然后，选择此 VAP 并单击**“编辑”**。

步骤 4 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”页验证未标记和管理 VLAN ID 的配置。有关详细信息，请参阅 VLAN 配置。

- **SSID 名称 —** 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。

- **SSID 广播 —** 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“广播 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。

- **安全 —** 访问 VAP 所需的身份验证类型：
  - 无
  - 静态 WEP
  - 动态 WEP
  - WPA 个人
  - WPA 企业

  如果选择“无”以外的安全模式，则会出现其他字段。建议使用可提供较强安全保护的“WPA 个人”或“WPA 企业”作为身份验证类型。对不支持“WPA 个人/WPA 企业”的传统无线计算机或设备，仅使用“静态 WEP”或“动态 WEP”。如果需要将“安全”设置为“静态 WEP”或“动态 WEP”，请将无线射频配置为 802.11a 或 802.11b/g 模式（请参阅无线射频）。 802.11n 模式限制将“静态 WEP”或“动

态 WEP”用作安全模式。

- **MAC 过滤 —** 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 （请参阅 **MAC 过滤**）。可以选择以下 MAC 过滤类型之一：
  - **已禁用 —** 不使用 MAC 过滤。
  - **本地 —** 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。
- **信道隔离 —** 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。

注 “信道隔离”适用于连接到一个接入点的同一 VAP 的客户端，但不适用于连接到不同接入点的同一 VAP 的客户端。因此，连接到一个接入点的同一 VAP 的客户端将无法相互执行 Ping 命令，连接到不同接入点的同一 VAP 的客户端可以成功相互执行 Ping 命令。

- **频段切换 —** 当两个无线射频都启用时，会启用频段切换。进行频段切换时，不会考虑无线射频的 802.11n 带宽。即使 5 GHz 无线射频刚好使用 20 MHz 带宽，在配置带宽切换后，接入点会尝试将客户端切换到 5 GHz 无线射频。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

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。建议在断开连接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”并单击**“删除”**。要永久保存删除内容，请在完成后单击**“保存”**。

配置安全设置

以下各节介绍基于在“网络”页的“安全”列表中选择的内容配置的安全设置。

无 （纯文本）

如果选择**"无"**作为安全模式，则不可以在接入点上配置其他安全设置。此模式表示接入点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。

静态 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。

"静态 WEP"并非可用的最安全模式，但可提供比将安全模式设置为"无 （纯文本） "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"静态 WEP"：

- **传输密钥索引 —** 密钥索引列表。提供从 1 到 4 的密钥索引。默认值为 1。

  "传输密钥索引"表示 WAP 设备使用哪个 WEP 密钥加密其发送的数据。

- **密钥长度 —** 密钥的长度。请选择以下选项之一：
  - 64 位
  - 128 位
- **密钥类型 —** 密钥类型。请选择以下选项之一：
  - ASCII
  - 十六进制
- **WEP 密钥 —** 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 #）。
  - 十六进制 — 包括 0 到 9 的数字以及 A 到 F 的字母。

  按照"所需的字符数"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。
- **所需的字符数 —** 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 验证 —** 当安全模式为“静态 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：

  - **“开放系统”**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“开放系统”，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。

  - **“共享密钥”**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“共享密钥”， 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**“开放系统”**和**“共享密钥”**。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。

静态 WEP 规则

如果使用“静态 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，这样才能对接入点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接入点传输的所有密钥，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 （接入点和客户端）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。

动态 WEP

“动态 WEP”指 802.1x 技术和可扩展身份验证协议 (EAP) 的组合。通过“动态 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“动态 WEP”：

- **使用全局 RADIUS 服务器设置 —** 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：

- **服务器 IP 地址类型 —** 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。

- **服务器 IP 地址 1** 或 **服务器 IPv6 地址 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。

- **服务器 IP 地址 2** 至 **4** 或 **服务器 IPv6 地址 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。

- **密钥** — 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。

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

- **启用 RADIUS 帐务** — 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 帐务，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。

- **活动服务器** — 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。

- **广播密钥刷新速率** — 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。

- **会话密钥刷新速率** — 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 30 至 86400 秒之间。值 0 表示不刷新会话密钥。

WPA 个人

“WPA 个人”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，后者在企业 WPA 安全模式下使用。 PSK 仅用于凭据的初始检查中。 “WPA 个人”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 个人”：

- **WPA 版本** — 要支持的客户端工作站的类型：
  - **WPA-TKIP** — 网络中拥有一些仅支持最初的 WPA 和 TKIP 安全协议的客户端工作站。请注意，根据 WiFi 联盟的最新要求，不允许对接入点仅选择 WPA-TKIP。
  - **WPA2-AES** — 网络中的所有客户端工作站都支持 WPA2 版本和 AES-CCMP 密码/安全协议。此 WPA 版本可以依据 IEEE 802.11i 标准提供最佳安全性。根据 WiFi 联盟的最新要求，接入点必须始终支持此模式。

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。

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

- **密钥 —** 用于“WPA 个人”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 #）。
- **密钥强度计 —** 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。
- **广播密钥刷新速率 —** 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 企业

WPA Enterprise with RADIUS 是 Wi-Fi 联盟 IEEE 802.11i 标准的实施，其中包含 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 企业”：

- **WPA 版本 —** 要支持的客户端工作站的类型：
  - **WPA-TKIP —** 网络中拥有一些仅支持最初的 WPA 和 TKIP 安全协议的客户端工作站。请注意，根据 WiFi 联盟的最新要求，不允许对接入点仅选择 WPA-TKIP。
  - **WPA2-AES —** 网络中的所有客户端工作站都支持 WPA2 版本和 AES-CCMP 密码/安全协议。此 WPA 版本可以依据 IEEE 802.11i 标准提供最佳安全性。根据 WiFi 联盟的最新要求，接入点必须始终支持此模式。
- **MFP （管理帧保护） —** 为其他未受保护的和未加密的 802.11 管理帧提供安全保护。仅在启用 WPA2 安全和 CCMP 字段后，才会显示此字段。它可以配置为以下三个复选框值。默认值为“支持”。
  - 不需要
  - 支持

- 必需

- **启用预身份验证 —** 如果仅为“WPA 版本”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，请单击“启用预身份验证”。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接入点连接的漫游客户端的身份验证速度。

  如果已经为“WPA 版本”选择 WPA，则此选项不适用，因为最初的 WPA 不支持此功能。

  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

- **使用全局 RADIUS 服务器设置 —** 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：

- **服务器 IP 地址类型 —** 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。

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

  如果将 **IPv4** 选作**“服务器 IP 地址类型”**，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。

- **服务器 IP 地址 2** 至 **4** 或 **服务器 IPv6 地址 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。

- **密钥 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。

- **密钥 2** 至 **密钥 4 —** 与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。**服务器 IP (IPv6) 地址 2** 的服务器使用 **密钥 2**，**服务器 IP (IPv6) 地址 3** 的服务器使用 **密钥 3**，以此类推。
- **启用 RADIUS 帐务 —** 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 帐务，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。
- **活动服务器 —** 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。
- **广播密钥刷新速率 —** 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。
- **会话密钥刷新速率 —** 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 30 至 86400 秒之间。值 0 表示不刷新会话密钥。

无线组播转发

“无线组播转发”功能提供了一种在无线媒体上转发组播流量的有效方式，并解决了由于在无线局域网中重复单播组播帧所引发的组播传输问题。

此功能使用 IGMP 帧跟踪加入的组成员，并且组播数据包在进行单播 MAC 转换后仅发送给相关成员。

通过 WMF （无线组播转发），数据帧就好像使用单播发送一样，数据传输更加可靠，并且当动态每工作站速率控制能够根据链路错误和噪声状况执行时，便可实现稳健传输。

组播组成员可以是 STA 端点，还支持 STA 设备间的串流。组播串流服务器可连接到任何局域网端口。

配置无线组播转发设置

要配置“无线组播转发”设置，请执行以下步骤：

步骤 1 在导航窗格中选择**“无线”>“无线组播转发”**。

步骤 2 配置以下参数：

- **无线组播转发 —** 在思科 WAP571/E 上全局启用或禁用无线组播转发。

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。建议在断开连接对无线客户端的影响最小时更改 WAP 设备的设置。

调度程序

无线射频和 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射频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。

接入点最多支持 16 个配置文件。仅将有效规则添加到配置文件中。最多可以将 16 条规则组合在一起以构成一个调度配置文件。属于同一配置文件的周期时间条目不会重叠。

最多可以创建 16 个调度程序配置文件名称。默认情况下，不创建任何配置文件。

添加调度程序配置文件

要查看调度程序状态和添加调度程序配置文件，请执行以下步骤：

步骤 1 在导航窗格中选择**“无线”>“调度程序”**。

步骤 2 确保**“管理模式”**处于启用状态。默认情况下，禁用此选项。

“调度程序运行状态”区域显示调度程序的当前运行状态：

- **状态 —** 调度程序的运行状态。状态包括“已启用”和“已禁用”。默认值为“已禁用”。
- **原因 —** 调度程序运行状态的原因。可能的值包括：
  - **处于活动状态 —** 管理性地启用调度程序。
  - **管理模式已禁用 —** 运行状态为“已禁用”，因为全局配置已禁用。
  - **系统时间过时 —** 系统时间不同步。

步骤 3 要添加配置文件，请在**“调度程序配置文件配置”**文本框中输入配置文件名称，然后单击**“添加”**。配置文件名称最多可以包含 32 个字母数字字符。

配置调度程序规则

最多可以为一个配置文件配置 16 条规则。每条规则都会指定无线射频或 VAP 可以使用的开始时间、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。有效规则必须包含开始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。

为配置文件配置规则

要为配置文件配置规则，请执行以下步骤：

步骤 1 从**“选择配置文件名称”**列表中选择配置文件。

步骤 2 单击**“添加规则”**。

规则表中会显示新规则。

步骤 3 选中**“配置文件名称”**旁边的框并单击**“编辑”**。

步骤 4 从**“星期几”**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（星期六和星期日）或一周中的任何一天启动的规则。

步骤 5 设置开始时间和结束时间：

- **开始时间 —** 开始使用无线射频或 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。
- 结束时间 — 停止使用无线射频或 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 单击**“保存”**。更改将保存到“启动配置”。

注 调度程序配置文件必须与无线射频接口或 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**“配置文件名称”**列中选择配置文件，然后单击**“删除”**。

调度程序规则的范围

以下介绍调度程序规则的范围。

- 设置为仅在特定日启动的规则不会影响其他日。
- 使用组 （例如“每天”、 “工作日”或“周末”）的规则会影响多日。

- 为“周末”设置的规则仅会影响“星期六”和“星期日”，而不会影响其余日。默认的调度程序特性是，如果在控制无线射频启用时间长度的相应日没有明确的规则，则启用无线射频。
- 调度程序功能设计为每个规则都设置一个无线射频或 VAP 启用时间的范围。
- “星期几”条目可用于创建规则的范围。此规则仅影响限定的范围。“周末”仅表示“星期六”和“星期日”。“每天”表示每一日。如果设置了这些规则，“星期几”GUI 条目将限定规则范围：周末、每天、工作日、星期日、星期一等。
- 这允许详细的规则设置。如果某个范围不包括相应周的每一日，则不存在已创建的隐式全部拒绝规则。通过设置相应范围为仅启用 1 分钟，可创建“拒绝”或“禁用”规则。如果将无线射频或 VAP 设置为除明确允许启用的时间外始终禁用，则需要设置一个范围为“每天”的规则，该规则仅在从午夜 00:00 到 00:01 的 1 分钟内有效。这意味着无线射频每天仅启用 1 分钟。然后可以为想要启用无线射频的每个时间段添加例外规则。

常见用例如下：

- 从星期一到星期五每天上午 9:00 到下午 5:00 启用无线射频
- 在周末不启用无线射频

使用以下两个规则创建配置文件：

工作日：开始时间：9:00 结束时间：17:00

周末开始时间：00:00 结束时间：00:01

调度程序关联

调度程序配置文件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配置文件，也没有配置文件与任何无线射频或 VAP 关联。

仅一个调度程序配置文件可以与无线局域网接口或每个 VAP 接口关联。一个配置文件可以与多个 VAP 关联。如果删除与 VAP 或无线局域网接口关联的调度程序配置文件，也会删除相应的关联。

将调度程序配置文件与无线局域网接口或 VAP 关联

要将调度程序配置文件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**“无线”>“调度程序关联”**。选择要在其中关联调度程序配置文件的**“无线射频”**接口 （**Radio 1** 或 **Radio 2**）。

步骤 2 对于无线局域网接口或 VAP，从**“配置文件名称”**列表中选择配置文件。

接口运行状态列显示当前是启用还是禁用接口。

步骤 3 单击**“保存”**。更改将保存到“启动配置”。

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。

配置 MAC 过滤

配置 MAC 过滤的步骤：

步骤 1 在导航窗格中选择**“无线”>“MAC 过滤”**。

步骤 2 选择 WAP 设备使用过滤器列表的方式：

- **仅允许列表中的工作站 —** 拒绝不在“工作站列表”中的任何工作站通过 WAP 设备访问网络。
- **阻止列表中所有的工作站 —** 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 地址”**字段中，输入允许或阻止的 MAC 地址，然后单击**“添加”**。

MAC 地址出现在**"工作站列表"**中。

步骤 4 在此列表完成前一直输入 MAC 地址，然后单击**"保存"**。更改将保存到"启动配置"。

注 要从"工作站列表"中删除 MAC 地址，请选中相应地址，然后单击**"删除"**。

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。建议在断开连接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
用户名 (1)	客户端工作站的 MAC 地址。	有效的以太网 MAC 地址。
用户密码 (2)	用于查找客户端 MAC 条目的固定全局密码。	NOPASSWORD

网桥

本章介绍两种类型的网桥。具体包括以下主题：

WDS 网桥

无线分布式系统 (WDS) 可用于连接多个 WAP571/E 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。

接入点还可用作中继器。在此模式下，接入点用作两个可能相隔太远以致超出信元范围的接入点之间的连接。用作中继器时，接入点没有到局域网的有线连接，通过无线连接重复发送信号。接入点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：

- 对于不允许客户端关联的纯桥接模式，建议对 VAP0 使用复杂的 WPA 密钥或禁用 SSID 广播。
- 所有加入同一 WDS 链路的思科 WAP 设备必须拥有以下相同设置：
  - 无线射频
  - IEEE 802.11 模式
  - 信道带宽
  - 信道 （不建议使用“自动”模式）

注 在 802.11n 2.4 GHz 频段中进行桥接时，将“信道带宽”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，请参阅无线射频 （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**“无线”>“网桥”**。

步骤 2 请从下拉菜单选项中选择“WDS 网桥”。

步骤 3 对要配置的**“WDS 接口”**选中**“启用”**。

步骤 4 配置其余参数：

- **远程 MAC 地址 —** 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“状态和统计信息”>“网络接口”页中找到此 MAC 地址。

- **加密 —** 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 加密设置是唯一的。其选项包括“无”、 “WEP”和“WPA 个人”。WPA2-PSK 是 WDS 链路加密和 VAP 安全的选项。管理员只有选择这些选项，才能执行它们。

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“静态 WEP”或“WPA 个人”。在“WPA 个人”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**。

注 “静态 WEP”仅适用于无线射频在以下传统模式下工作的场合：在 5 GHz 无线射频下工作的 802.11a 和在 2.4 GHz 无线射频下工作的 802.11b/g。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

步骤 6 对另一个设备或连接到网桥的设备重复此过程。

提示 可以通过转到“状态和统计信息”>“网络接口”页验证网桥链路是否正在运行。在“接口状态”表中， WLAN0:WDS(x) 的状态应为“Up”。

注 即使 WDS 链路中断，远程网络中的伙伴 WDS 接入点仍将保留它从连接到主网络中 WDS 接入点的 DHCP 服务器获取的管理 IP 地址。在 WDS 接口管理性关闭后，会释放 IP 地址。

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。建议在断开连接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。

- **密钥长度 —** 如果启用 WEP，将 WEP 密钥长度指定为 **64 位**或 **128 位**。
- **密钥类型 —** 如果启用 WEP，请指定 WEP 密钥类型：**ASCII** 或**十六进制**。
- **WEP 密钥 —** 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**“密钥类型”**和**“密钥长度”**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。

- **密钥 —** 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 #）。

利用接入点的工作组网桥功能， WAP 设备可以扩展远程网络的可访问性。在“工作组网桥”模式下，接入点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与使用“工作组网桥”模式连接的无线局域网之间桥接流量。

工作组网桥

“工作组网桥”功能支持 STA 模式。 WAP 设备可以在基本服务集 (BSS) 上作为 STA 设备工作。当启用“工作组网桥”模式时，接入点仅支持一个可作为无线客户端与接入点进行关联的 BBS。

建议仅在 WDS 网桥功能无法用于对等接入点时使用“工作组网桥”模式。 WDS 是更好的解决方案，优先于工作组网桥解决方案。如果桥接思科 WAP571/E 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 在接入点中启用“工作组网桥”模式时， WDS 功能将无法工作。

在“工作组网桥”模式下，一个 WAP 设备 （即作为 STA 与 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 设备称为上游接入点。

这些连接到 WAP 设备有线接口的设备可以访问通过基础设施客户端接口连接的网络。

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：
  - 无线射频
  - IEEE 802.11 模式
  - 信道带宽
  - 信道 （不建议使用“自动”模式）

  有关配置这些设置的详情，请参阅无线射频 （基本设置）。
- “工作组网桥”模式当前仅支持 IPv4 流量。
- “集群配置”中不支持“工作组网桥”模式。

要配置“工作组网桥”模式，请执行以下步骤：

步骤 1 在导航窗格中选择**“无线”>“网桥”**。

步骤 2 请从下拉菜单选项中选择“工作组网桥模式”。

步骤 3 对**“工作组网桥模式”**选择**“启用”**。

步骤 4 选择要在其中配置“工作组网桥”模式的无线射频接口 （**Radio 1** 或 **Radio 2**）。

步骤 5 为基础设施客户端接口 （上游）配置以下参数：

- **SSID —** BSS 的 SSID。

注 “SSID 扫描的 SSID”旁边有一个箭头，此功能在默认情况下禁用，仅在“恶意 AP 检测”中的“AP 检测” （该功能在默认情况下也禁用）启用时启用。

- **安全 —** 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：
  - 无
  - **静态 WEP**
  - **WPA 个人**
  - **WPA 企业**

- **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证与上游 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。 “连接状态”字段表示 WAP 是否连接到上游 WAP 设备。可以单击“刷新”按钮查看最新连接状态。

即使 WGB 接入点 （用作连接到上游接入点的客户端的接入点）与上游接入点取消关联，它仍将保留从上游 DHCP 服务器获取的管理 IP 地址。

注 “静态 WEP”仅适用于无线射频在以下传统模式下工作的场合：在 5 GHz 无线射频下工作的 802.11a 和在 2.4 GHz 无线射频下工作的 802.11b/g。

QoS

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。

要在接入点中配置 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。

配置 WAP 设备和工作站 EDCA 参数

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“无线”>“QoS”**。选择要在其上配置 QoS 设置的无线射频接口（**Radio 1** 或 **Radio 2**）。

步骤 2 从**“EDCA 模板”**列表中选择一个选项：

- **WFA 默认值** — 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。
- **针对语音优化** — 用最适合语音流量的值填充 WAP 设备和工作站 EDCA 参数。
- **自定义** — 可用来选择自定义的 EDCA 参数。

下面四个队列是为从 WAP 传输至工作站的不同类型的数据定义的。如果选择“自定义”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。这四个队列为：

- **数据 0（语音）** — 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。
- **数据 1（视频）** — 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。
- **数据 2（尽力服务）** — 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。
- **数据 3（后台）** — 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。

- **仲裁帧间间隔 —** 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。
- **最小争用时间 —** 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“最大争用时间”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 1023。此值必须小于“最大争用时间”的值。
- **最大争用时间 —** 随机退避值成倍增加的上限 （毫秒）。在发送数据帧或达到“最大争用时间”大小之前，此值会一直成倍增加。

  达到“最大争用时间”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 1023。此值必须大于“最小争用时间”的值。
- **最大突发** （仅 WAP） **—** 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 多媒体 (WMM) —** 选择**“启用”**以启用“Wi-Fi 多媒体 (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，接入点中的 QoS 设置可以控制从 WAP 设备流向客户端工作站 （接入点 EDCA 参数）的下行流量以及从客户端工作站流向接入点 （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 限制** （仅工作站） — 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 限制”的最大值是 65535。

步骤 4 配置以下更多设置：

- **无确认** — 选择**“启用”**以指定 WAP 设备不应将具有 QosNoAck 的帧确认为服务等级值。
- **无计划的自动节电交付** — 选择**“启用”**以启用作为电源管理方法的 APSD （自动节电发送）。如果 VoIP 电话通过 WAP 设备访问网络，建议使用 APSD。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

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。建议在断开连接对无线客户端的影响最小时更改 WAP 设备的设置。

6

频谱分析器

本章介绍此接入点设备的频谱分析器功能。

频谱分析器

配置频谱分析器

频谱分析器

通过频谱分析功能，可以全面监控无线射频 (RF) 环境，从而能够管理无线网络。此功能提供了一个无线网络管理员角色，令用户能够查看有关 RF 环境的实时信息和历史信息。

频谱分析可以扫描 2.4 GHz 和 5 GHz 频段中所有用于非 Wi-Fi 接口的 IEEE 802.11 信道，对接口进行分类，并在本地事件日志中记录网络边缘发生的所有干扰事件。

注 频谱分析器可记录以下干扰：模拟无绳电话、无线摄像头、微波炉、 S 波段运动检测器、窄带干扰器、宽带干扰器和未知干涉。

“频谱分析器”页提供了频谱分析器功能的状态以及查看频谱数据的链接。

配置频谱分析器

要配置“频谱分析器”，请执行以下步骤：

步骤 1 在导航窗格中选择 **Spectrum Analyzer （频谱分析器）**。

步骤 2 系统将显示“Spectrum Analysis Mode” （频谱分析模式）的状态。此状态可能是“Dedicated Spectrum Analyzer” （专用频谱分析器）、“Hybrid Spectrum Analyzer” （混合频谱分析器）或“Disable” （禁用）。默认设置为“Disable” （禁用）。频谱分析器在同一时间只能支持一个无线射频。

注 在专用模式下，无线射频有超过 10% 的时间会被用于频谱分析，客户端连接可以工作，但是性能没有保证。在混合模式下，客户端连接可以得到保证，但是吞吐量有可能会受到影响。

步骤 3 单击 **Save**（保存）。更改将保存到“Startup Configuration”（启动配置）。

步骤 4 当扫描模式设置为“Dedicated Spectrum Analyzer”（专用频谱分析器）或“Hybrid Spectrum Analyzer”（混合频谱分析器）时，按 **View Spectrum Data**（查看频谱数据）按钮可以启动频谱查看器。

注 频谱查看器只能通过 IPv4 地址访问。

7

系统安全

本章介绍如何在接入点中配置安全设置。

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，在接入点中配置虚拟接入点 (VAP) 时，可以配置用于控制无线客户端访问的安全方法（请参阅无线射频页）。“动态 WEP”和“WPA 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 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。网页认证功能也可使用 RADIUS 对客户端进行身份验证。

可以使用“Radius 服务器”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。

配置全局RADIUS服务器

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**“系统安全”>“RADIUS 服务器”**。

步骤 2 输入以下参数：

- **服务器 IP 地址类型 —** 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。

- **服务器 IP 地址 1** 或 **服务器 IPv6 地址 1 —** 主要的全局 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。

- **服务器 IP 地址 （2 至 4）** 或 **服务器 IPv6 地址 （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。

- **密钥 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。

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

- **启用 RADIUS 帐务 —** 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 帐务，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 单击**“保存”**。更改将保存到“启动配置”。

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 请求方”页分为以下 3 个区域：请求方配置、证书文件状态和证书文件上传。

“请求方配置”区域用于配置 802.1X 运行状态和基本设置。

要配置 802.1X 请求方，请执行以下步骤：

步骤 1 在导航窗格中选择**“系统安全”>“802.1X 请求方”**。

步骤 2 单击**“刷新”**可更新证书文件状态。

步骤 3 输入以下参数：

- **管理模式** — 启用 802.1X 请求方功能。
- **EAP 方法** — 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。
- **用户名** — 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。
- **密码** — 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。

注 在 EAP-TLS 模式下， WAP 设备在响应来自 802.1X 身份验证器的请求时使用此身份标识。 WAP 设备支持 PEM 格式的证书文件。证书文件必须包含专用密钥和根证书。 WAP 设备要求此证书文件受密码保护。 WAP 设备将使用专用密钥密码来对此证书文件进行解锁。

步骤 4 单击**“保存”**。更改将保存到“启动配置”。

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。建议在断开连接对无线客户端的影响最小时更改 WAP 设备的设置。

“ 证书文件状态 ” 区域中显示当前证书是否存在：

- **存在证书文件 —** 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”。
- **证书过期日期 —** 指示 HTTP SSL 证书文件的过期时间。范围是有效日期。

“证书文件上传”区域用于将证书文件上传到接入点：

步骤 1 选择**“HTTP”**或**“TFTP”** 作为**“传输方式”**。

步骤 2 如果选择了“HTTP”，请单击**“浏览”**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”，请输入**“文件名”**和**“TFTP 服务器 IPv4 地址”**。文件名不能包含以下字符：空格、 <、 >、 |、 \、 :, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

步骤 3 单击**“上传”**。

会出现一个确认窗口，然后出现一个进度条指示上传状态。

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。

配置密码复杂性要求

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**“系统安全”>“密码复杂性”**。

步骤 2 对于**“密码复杂性”**设置，选择**“启用”**。

步骤 3 配置以下参数：

- **密码最小字符类别 —** 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。
- **密码不同于当前密码 —** 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。
- **最大密码长度 —** 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。
- **最小密码长度 —** 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。
- **密码过期支持 —** 选择密码过期的配置时间段。
- **密码过期时间 —** 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 单击**“保存”**。更改将保存到“启动配置”。

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 复杂性”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。

配置WPA-PSK复杂性

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**“系统安全”>“WPA-PSK 复杂性”**。

步骤 2 对于**“WPA-PSK 复杂性”**设置，单击**“启用”**，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 复杂性”。

步骤 3 配置以下参数：

- **WPA-PSK 最小字符类别 —** 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 不同于当前值 —** 选择以下选项之一：
  - **启用 —** 用户必须在其当前密钥过期后配置不同密钥。
  - **禁用 —** 用户可以在其当前密钥过期后使用旧密钥或以前的密钥。
- **最大 WPA-PSK 长度 —** 最大密钥长度是 32 至 63 个字符，默认值为 63 个字符。
- **最小 WPA-PSK 长度 —** 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 单击**“保存”**。更改将保存到“启动配置”。

8

客户端 QoS

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

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

全局设置

可以使用“客户端 QoS 全局设置”页在 WAP 设备中启用或禁用服务质量功能。

如果禁用**“客户端 QoS”**，也会全局禁用速率限制和差分服务 (DiffServ) 配置。

如果启用此模式，还可以在特定 VAP 或以太网上启用或禁用“客户端 QoS 模式”。请参阅客户端 QoS 关联页的**“客户端 QoS 模式”**设置。

类映射

QoS 功能包含差分服务 (DiffServ) 支持，通过此支持，可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 （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 （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“类映射”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。

配置 IPv4 类映射

要添加并配置 IPv4 类映射，请执行以下步骤：

步骤 1 选择**“客户端 QoS”>“类映射”**。

步骤 2 在“类映射名称”字段中，输入新类映射的名称。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。

步骤 3 从“类映射类型”列表中选择 IPv4 作为类映射的类型。 IPv4 类映射仅适用于 WAP 设备中的 IPv4 流量。

步骤 4 在“匹配标准配置”区域中，配置以下参数以将数据包匹配到类：

- **类映射名称 —** 从列表中选择 IPv4 类映射。
- **匹配每个数据包 —** 匹配条件适用于第 3 层数据包中的所有参数。如果启用，所有的第 3 层数据包都将匹配条件。
- **协议 —** 基于 IPv4 数据包中的“IP 协议”字段值或 IPv6 数据包中的“下一报头”字段值，使用第 3 层或第 4 层协议匹配条件。选择要按关键字匹配的协议或输入协议 ID：
  - **从列表中选择 —** 与所选协议匹配：IP、 ICMP、 IGMP、 TCP、 UDP。
  - **匹配值 —** 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。
- **源 IP —** 需要数据包的源 IPv4 地址，以匹配在适当字段中定义的 IPv4 地址。
  - **源 IP 地址 —** 输入要应用此条件的 IPv4 地址。
  - **源 IP 掩码 —** 输入源 IPv4 地址掩码。 DiffServ 的掩码是 IP 点分十进制格式的网络式位掩码，可指示目的 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。

- **源端口** — 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。
  - **从列表中选择** — 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。
  - **匹配端口** — 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
  - **掩码** — 端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 1 表示该位重要， 0 表示该位应忽略。
- **目的 IP** — 需要数据包的目的 IPv4 地址，以匹配适当字段中定义的 IPv4 地址。
  - **目的 IP 地址** — 输入 IPv4 地址以应用此条件。
  - **目的 IP 掩码** — 输入目的 IP 地址掩码。
- **目的端口** — 将目的端口包含在规则的匹配条件中。目的端口在数据报头中标识。
  - **从列表中选择** — 将数据报头中的目的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。
  - **匹配端口** — 将数据报头中的目的端口与指定的 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
  - **掩码** — 端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 1 表示该位重要， 0 表示该位应忽略。
- **服务类型** — 指定在将数据包匹配到类条件时要使用的服务类型。
  - **IP DSCP 从列表中选择** — 选择要用作匹配标准的 DSCP 值。
  - **IP DSCP 匹配值** — 输入自定义 DSCP 值，范围介于 0 至 63 之间。
  - **IP 优先级** — 将数据包的 IP 优先级值匹配到在此字段中定义的 IP 优先级值。IP 优先级范围介于 0 至 7 之间。

- **IP TOS 位 —** 将 IP 报头中数据包的服务类型 (ToS) 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 优先级值。高位的 6 位代表 IP DSCP 值。
- **IP TOS 掩码 —** 输入“IP TOS 掩码”值，以标识“IP TOS 位”值中用于与数据包的 IP ToS 字段值比较的数位位置。

  “IP TOS 掩码”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 掩码”中的零值位表示“IP TOS 位”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 位”值 0 和“IP TOS 掩码”值 00。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

注 要删除类映射，请在“类映射名称”列表中将其选中，然后单击“删除”。如果类映射已附加到策略，则无法将其删除。

配置 IPv6 类映射

要添加并配置 IPv6 类映射，请执行以下步骤：

步骤 1 选择**“客户端 QoS”>“类映射”**。

步骤 2 在“类映射名称”字段中，输入新类映射的名称。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。

步骤 3 从“类映射类型”列表中选择 IPv6 作为类映射的类型。 IPv6 类映射仅适用于 WAP 设备中的 IPv6 流量。

步骤 4 在“匹配标准配置”区域中，配置以下参数以将数据包匹配到类：

- **类映射名称 —** 从列表中选择 IPv6 类映射。
- **匹配每个数据包 —** 匹配条件适用于第 3 层数据包中的所有参数。如果启用，所有的第 3 层数据包都将匹配条件。
- **协议 —** 基于 IPv4 数据包中的“IP 协议”字段值或 IPv6 数据包中的“下一报头”字段值，使用第 3 层或第 4 层协议匹配条件。选择要按关键字匹配的协议或输入协议 ID：
  - **从列表中选择 —** 与所选协议匹配：IPv6、 ICMPv6、 TCP、 UDP。
  - **匹配值 —** 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。

- **源 IPv6** — 需要数据包的源 IPv6 地址，以匹配适当字段中定义的 IPv6 地址。
  - **源 IPv6 地址** — 输入要应用此条件的 IPv6 地址。
  - **源 IPv6 前缀长度** — 输入源 IPv6 地址的前缀长度。
- **源端口** — 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。
  - **从列表中选择** — 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。
  - **匹配端口** — 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
  - **掩码** — 端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位（0 至 0xFFFF）。 1 表示该位重要， 0 表示该位应忽略。
- **目的 IPv6** — 需要数据包的目的 IPv6 地址，以匹配适当字段中定义的 IPv6 地址。
  - **目的 IPv6 地址** — 输入要应用此条件的 IPv6 地址。
  - **目的 IPv6 前缀长度** — 输入目的 IPv6 地址的前缀长度。
- **目的端口** — 将目的端口包含在规则的匹配条件中。目的端口在数据报头中标识。
  - **从列表中选择** — 将数据报头中的目的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。
  - **匹配端口** — 将数据报头中的目的端口与指定的 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
  - **掩码** — 端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位（0 至 0xFFFF）。 1 表示该位重要， 0 表示该位应忽略。
- **IPv6 流标签** — 输入 IPv6 数据包特有的 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 —** 用作匹配标准的 DSCP 值。
  - **从列表中选择 —** 从列表中选择 DSCP 类型。
  - **匹配值 —** 输入自定义 DSCP 值，范围介于 0 至 63 之间。

步骤 5 单击**"保存"**。更改将保存到"启动配置"。

注 要删除类映射，请在"类映射名称"列表中将其选中，然后单击"删除"。如果类映射已附加到策略，则无法将其删除。

配置 MAC 类映射

要配置 MAC 类映射，请执行以下步骤：

步骤 1 选择**"客户端 QoS">"类映射"**。

步骤 2 在"类映射名称"字段中，输入新类映射的名称。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。

步骤 3 从"类映射类型"列表中选择 MAC 作为类映射的类型。 MAC 类映射适用于第 2 层标准。

步骤 4 在"匹配标准配置"区域中，配置以下参数以将数据包匹配到类：

- **类映射名称 —** 从列表中选择 MAC 类映射。
- **匹配每个数据包 —** 如果启用，所有的第 2 层数据包都将匹配条件。
- **以太网类型 —** 比较匹配标准与以太网帧报头中的值。选择"以太网类型"关键字或输入"以太网类型"值以指定匹配标准：
  - **从列表中选择 —** 将数据报头中的"以太网类型"与所选的协议类型进行匹配：appletalk、 arp、 ipv4、 ipv6、 ipx、 netbios、 pppoe。
  - **匹配值 —** 将数据报头中的"以太网类型"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。
- **服务等级 —** 指定数据包的匹配服务 802.1p 用户优先级值的类。有效范围介于 0 至 7 之间。
- **源 MAC —** 将源 MAC 地址包含在规则的匹配条件中。
  - **源 MAC 地址 —** 输入要与以太网帧比较的源 MAC 地址。
  - **源 MAC 掩码 —** 输入源 MAC 地址掩码，用于指定目的 MAC 地址中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，应使用 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，用于匹配单个 MAC 地址。

- **目的 MAC —** 将目的 MAC 地址包含在规则的匹配条件中。
  - **目的 MAC 地址 —** 输入要与以太网帧比较的目的 MAC 地址。
  - **目的 MAC 掩码 —** 输入目的 MAC 地址掩码以指定目的 MAC 地址中与以太网帧比较的位。
- **VLAN ID —** 指定数据包的匹配 VLAN ID。 VLAN ID 范围介于 0 至 4095 之间。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

注 要删除类映射，请在“类映射名称”列表中将其选中，然后单击“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“策略映射”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。

添加和配置策略映射

要添加和配置策略映射，请执行以下步骤：

步骤 1 选择**“客户端 QoS”>“策略映射”**。

步骤 2 在“策略映射名称”字段中，输入策略映射的名称。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 单击**“添加策略映射”**。

步骤 4 在“策略类定义”区域中，为策略映射配置以下参数：

- **策略映射名称 —** 选择要配置的策略映射。
- **类映射名称 —** 选择要应用此策略的类映射。

- **简单策略 —** 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。

  如果启用此功能，请配置以下字段之一：

  - **承诺速率 —** 流量必须遵守的承诺速率 (Kbps)。范围介于 1 至 1000000 Kbps 之间。
  - **承诺突发数据量 —** 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。

- **发送 —** 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。
- **丢弃 —** 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。
- **标记服务等级 —** 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。
- **标记 IP DSCP —** 使用从列表中选择的 IP DSCP 值标记关联流量流的所有数据包。
  - **从列表中选择 —** DSCP 类型的列表。
- **标记 IP 优先级 —** 使用指定的 IP 优先级值标记关联流量流的所有数据包。 IP 优先级值是介于 0 至 7 之间的整数。
- **取消关联类映射 —** 从在“策略映射名称”列表中选择的策略中删除在“类映射名称”列表中选择的类。
- **成员类 —** 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 5 单击**“保存”**。更改将保存到“启动配置”。

注 要删除策略映射，请在“策略映射名称”列表中将其选中，然后单击“删除”。

注 仅在策略映射未与任何 VAP 关联时，才能将其删除。

注 IPv6 类映射不支持策略标记参数 （例如标记服务等级、标记 IP DSCP 和标记 IP 优先级）。

客户端 QoS 关联

“QoS 关联”页提供对无线和以太网接口的特定 QoS 方面的更多控制权。该页面还提供了用于控制单个客户端所允许发送和接收的带宽量的选项。

除控制一般的流量类别外，客户端 QoS 可用于配置通过差分服务 (DiffServ) 为每个客户端调整各种微流。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。

配置 QoS 关联参数

要配置 QoS 关联参数，请执行以下步骤：

步骤 1 选择**“客户端 QoS”>“客户端 QoS 关联”**。

步骤 2 在“接口”字段中，选择要配置 QoS 参数的无线射频或以太网接口。

步骤 3 对于**所选接口**，选择**“已启用”**。

步骤 4 对于所选接口，配置以下参数：

- **下行带宽限制 —** 输入从 WAP 设备到客户端的最大允许传输速率，单位为位/秒 (bps)。有效范围介于 0 至 1300 Mbps 之间。
- **上行带宽限制 —** 输入从客户端到 WAP 设备的最大允许传输速率，单位为位/秒 (bps)。有效范围介于 0 至 1300 Mbps 之间。
- **差分服务策略 —** 对所选接口选择应用于发送到 WAP 设备的流量的差分服务 (DiffServ) 策略。

步骤 5 单击**“保存”**。更改将保存到“启动配置”。

客户端 QoS 状态

“客户端 QoS 状态”页显示策略映射和类映射的详细信息，其中包括一个策略映射包含哪些类映射以及此策略映射绑定到哪些接口。

IPv4 QoS、 IPv6 QoS 和 MAC QoS 表显示在“类映射”页上定义的类映射的信息，包括：

- **成员类 —** 类映射名称。
- **全部匹配 —** 显示此映射是否匹配所有数据包。

规则字段 — 显示此类映射的详细定义。有关详情，请参阅类映射。

“策略映射”表显示在“策略映射”页上定义的策略映射的信息，包括：

- **策略映射名称 —** 策略映射名称。
- **绑定的接口 —** 显示此策略映射已关联到哪个接口。
- **类映射名称 —** 列出此策略映射包含的类映射。

策略 — 显示此类映射的策略详细信息。有关详情，请参阅策略映射。

可以单击**“刷新”**刷新屏幕并显示最新信息。

9

ACL

本节介绍如何在 WAP 设备上配置 ACL 功能。具体包括以下主题：

- ACL 规则
- ACL 关联
- ACL 状态

ACL 规则

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。

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

IPv4 和 IPv6 ACL

IP ACL 可以将第 3 层和第 4 层流量分类。

每个 ACL 都包含一组应用到 WAP 设备所接收的流量的规则。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，例如源或目的 IP 地址、源或目的端口或者数据包内带有的协议。

注 每个已创建的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。通过配置此类规则可以检查帧的字段，例如源或目的 MAC 地址、 VLAN ID 或服务等级。当帧进入 WAP 设备的端口时， WAP 设备会检查该帧，并根据 ACL 规则检查帧的内容。如果任一规则与内容匹配，则会对帧采取允许或拒绝操作。

配置 ACL 的工作流程

通过“ACL 规则”页，可以配置 ACL 和规则，并将规则应用到指定接口。

配置 ACL

要配置 ACL，请执行以下步骤：

步骤 1 选择**“ACL”>“ACL 规则”**。

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“ACL 关联”页将 ACL 应用到一个或多个接口。

配置 IPv4 ACL

要配置 IPv4 ACL，请执行以下步骤：

步骤 1 选择**“ACL”>“ACL 规则”**。

步骤 2 在“ACL 名称”字段中，输入用于识别 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。

步骤 3 从“ACL 类型”列表中，选择“IPv4”作为 ACL 的类型。IPv4 ACL 基于第 3 层和第 4 层标准控制对网络资源的访问。

步骤 4 单击“添加 ACL”。

步骤 5 在“ACL 规则配置”区域中，配置以下 ACL 规则参数：

- **ACL 名称 - ACL 类型 —** 选择要使用新规则进行配置的 ACL。
- **规则 —** 选择“新建规则”，可为所选 ACL 配置新规则。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。设备有一个隐式“全部拒绝”规则作为最终规则。
- **操作 —** 选择 ACL 规则是允许还是拒绝某个操作。
- 如果选择“允许”，该规则将允许所有符合规则标准的流量进入 WAP 设备。不符合标准的流量会被丢弃。
- 如果选择“拒绝”，该规则将阻止所有符合规则标准的流量进入 WAP 设备。除非此规则是最终规则，否则不符合标准的流量将被转发。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。

- **匹配每个数据包 —** 如果启用此字段，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。如果启用此功能，则无法配置任何其他匹配标准。对于新规则，此选项默认处于选中状态。要配置其他匹配字段，则必须禁用此选项。
- **协议 —** 基于 IPv4 数据包中的“IP 协议”字段值或 IPv6 数据包中的“下一报头”字段值，使用第 3 层或第 4 层协议匹配条件。您可以选择下列选项之一，或者选择“任意”：
  - **从列表中选择 —** 选择以下协议之一：IP、 ICMP、 IGMP、 TCP 或 UDP。
  - **匹配值 —** 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未在“从列表中选择”中列出的协议。
- **源 IP —** 需要数据包的源 IP 地址，以匹配在适当字段中定义的地址。
  - **源 IP 地址 —** 输入要应用此条件的 IP 地址。
  - **通配符掩码 —** 输入源 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“源 IP 地址”时必须填写此字段。

    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。
- **源端口 —** 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。
  - **从列表中选择 —** 选择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。
  - **匹配端口 —** 输入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
  - **掩码 —** 输入端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 0 表示该位重要， 1 表示该位应忽略。

- **目的 IP —** 需要数据包的目的 IP 地址，以匹配适当字段中定义的地址。
  - **目的 IP 掩码 —** 输入要应用此条件的 IP 地址。

    通配符掩码 — 输入目的 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“源 IP 地址”时必须填写此字段。

    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。
- **目的端口 —** 将目的端口包含在规则的匹配条件中。目的端口在数据报头中标识。
  - **从列表中选择 —** 选择与要匹配的目的端口关联的关键字：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。
  - **匹配端口 —** 输入与数据报头中标识的目的端口匹配的 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
  - **掩码 —** 输入端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 0 表示该位重要， 1 表示该位应忽略。
- **服务类型 —** 根据特定服务类型匹配数据包。
  - **IP DSCP 从列表中选择 —** 根据 DSCP 确保转发 (AS)、服务等级 (CS) 或加速转发 (EF) 值匹配数据包。
  - **IP DSCP 匹配值 —** 根据自定义 DSCP 值匹配数据包。如果选择此字段，请输入一个介于 0 至 63 之间的值。
  - **IP 优先级 —** 根据数据包的 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 优先级值。
  - **IP TOS 位 —** 指定一个值，以将 IP 报头中的数据包 ToS 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 位”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 优先级值。高位的 6 位代表 IP 差分服务代码点 (DSCP) 值。

- **IP TOS 掩码 —** 输入“IP TOS 掩码”值，以标识“IP TOS 位”值中用于与数据包的 IP ToS 字段值比较的数位位置。

  “IP TOS 掩码”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 掩码”中的零值位表示“IP TOS 位”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 位”值 0 和“IP TOS 掩码”值 00。

步骤 6 单击**“保存”**。更改将保存到“启动配置”。

注 要删除某个 ACL，请在“ACL 名称 - ACL 类型”列表中选择该 ACL，选择“删除 ACL”，然后单击“保存”。

配置 IPv6 ACL

要配置 IPv6 ACL，请执行以下步骤：

步骤 1 选择**“ACL”>“ACL 规则”**。

步骤 2 在“ACL 名称”字段中，输入用于识别 ACL 的名称。

步骤 3 从“ACL 类型”列表中，选择“IPv6”作为 ACL 的类型。IPv6 ACL 基于第 3 层和第 4 层标准控制对网络资源的访问。

步骤 4 单击“添加 ACL”。

步骤 5 在“ACL 规则配置”区域中，配置以下 ACL 规则参数：

- **ACL 名称 - ACL 类型 —** 选择要使用新规则进行配置的 ACL。
- **规则 —** 选择“新建规则”，可为所选 ACL 配置新规则。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。设备有一个隐式“全部拒绝”规则作为最终规则。
- **操作 —** 选择 ACL 规则是允许还是拒绝某个操作。
- 如果选择“允许”，该规则将允许所有符合规则标准的流量进入 WAP 设备。不符合标准的流量会被丢弃。
- 如果选择“拒绝”，该规则将阻止所有符合规则标准的流量进入 WAP 设备。除非此规则是最终规则，否则不符合标准的流量将被转发。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。
- **匹配每个数据包 —** 如果启用此字段，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。如果启用此功能，则无法配置任何其他匹配标准。

对于新规则，此选项默认处于选中状态。要配置其他匹配字段，则必须禁用此选项。

- **协议** — 选择要按关键字或协议 ID 匹配的协议。
- **源 IPv6** — 需要数据包的源 IPv6 地址，以匹配适当字段中定义的 IPv6 地址。
  - **源 IPv6 地址** — 输入要应用此条件的 IPv6 地址。
  - **源 IPv6 前缀长度** — 输入源 IPv6 地址的前缀长度。
- **源端口** — 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。
  - **从列表中选择** — 如果选择此项，请从列表中选择端口名称。
  - **匹配端口** — 输入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
  - **掩码** — 输入端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 0 表示该位重要， 1 表示该位应忽略。
- **目的 IPv6** — 需要数据包的目的 IPv6 地址，以匹配适当字段中定义的 IPv6 地址。
  - **目的 IPv6 地址** — 输入要应用此条件的 IPv6 地址。
  - **目的 IPv6 前缀长度** — 输入目的 IPv6 地址的前缀长度。
- **目的端口** — 将目的端口包含在规则的匹配条件中。目的端口在数据报头中标识。
  - **从列表中选择** — 如果选择此项，请从列表中选择端口名称。
  - **匹配端口** — 输入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
  - **掩码** — 输入端口掩码。掩码确定所使用的位和忽略的位。仅允许十六进制位 (0-0xFFFF)。 0 表示该位重要， 1 表示该位应忽略。
- **IPv6 流标签** — 指定 IPv6 数据包特有的 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）。

- **IPv6 DSCP —** 根据数据包的 IP DSCP 值匹配数据包。如果选择此选项，请选择以下选项之一作为匹配标准：
  - **从列表中选择 —** 选择以下值之一：DSCP 确保转发 (AS)、服务等级 (CS) 或加速转发 (EF)。
  - **匹配值 —** 输入自定义 DSCP 值，范围介于 0 至 63 之间。

步骤 6 单击**"保存"**。更改将保存到"启动配置"。

注 要删除某个 ACL，请在"ACL 名称 - ACL 类型"列表中选择该 ACL，选中"删除 ACL"，然后单击"保存"。

配置 MAC ACL

配置 MAC ACL

要配置 MAC ACL，请执行以下步骤：

步骤 1 选择**"ACL">"ACL 规则"**。

步骤 2 在"ACL 名称"字段中，输入用于识别 ACL 的名称。

步骤 3 从"ACL 类型"列表中，选择"MAC"作为 ACL 的类型。 MAC ACL 基于第 2 层标准控制访问。

步骤 4 单击"添加 ACL"。

步骤 5 在"ACL 规则配置"区域中，配置以下 ACL 规则参数：

- **ACL 名称 - ACL 类型 —** 选择要使用新规则进行配置的 ACL。
- **规则 —** 选择"新建规则"，可为所选 ACL 配置新规则。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。设备有一个隐式"全部拒绝"规则作为最终规则。
- **操作 —** 选择 ACL 规则是允许还是拒绝某个操作。
- 如果选择"允许"，该规则将允许所有符合规则标准的流量进入 WAP 设备。不符合标准的流量会被丢弃。
- 如果选择"拒绝"，该规则将阻止所有符合规则标准的流量进入 WAP 设备。除非此规则是最终规则，否则不符合标准的流量将被转发。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。
- **匹配每个数据包 —** 如果启用此字段，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。如果启用此功能，则无法配置任何其他匹配标准。

对于新规则，此选项默认处于选中状态。要配置其他匹配字段，则必须禁用此选项。

- **以太网类型 —** 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。您可以选择“以太网类型”关键字或输入“以太网类型”值，以指定匹配标准。
  - **从列表中选择 —** 选择以下协议类型之一：appletalk、 arp、 ipv4、 ipv6、 ipx、 netbios、 pppoe。
  - **匹配值 —** 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。
- **服务等级 —** 输入要与以太网帧比较的 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。
- **源 MAC —** 需要数据包的源 MAC 地址，以匹配在适当字段中定义的地址。
  - **源 MAC 地址 —** 输入要与以太网帧比较的源 MAC 地址。
  - **源 MAC 掩码 —** 输入源 MAC 地址掩码，此值用于指定源 MAC 中要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，应使用 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，用于匹配单个 MAC 地址。
- **目的 MAC —** 需要数据包的目的 MAC 地址，以匹配在适当字段中定义的地址。
  - **目的 MAC 地址 —** 输入要与以太网帧比较的目的 MAC 地址。
  - **目的 MAC 掩码 —** 输入目的 MAC 地址掩码，以指定目的 MAC 中要与以太网帧比较的位。
- **VLAN ID —** 输入要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 6 单击**“保存”**。更改将保存到“启动配置”。

注 要删除某个 ACL，请在“ACL 名称 - ACL 类型”列表中选择该 ACL，选中“删除 ACL”，然后单击“保存”。

ACL 关联

“ACL 关联”页提供了与无线接口和以太网接口绑定的 ACL 的列表。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接口。

将 ACL 关联到接口

要将 ACL 关联到接口，请执行以下步骤：

步骤 1 选择**“ACL”>“ACL 关联”**。

步骤 2 在“接口”字段中，单击您想要为其配置 ACL 参数的无线射频接口或以太网接口。

步骤 3 对于所选接口，配置以下参数：

- **ACL 类型 —** 选择针对进入 WAP 设备的流量所要应用的 ACL 的类型，可以是以下选项之一：
  - **IPv4 —** 检查与 ACL 规则匹配的 IPv4 数据包。
  - **IPv6 —** 检查与 ACL 规则匹配的 IPv6 数据包。
  - **MAC —** 检查与 ACL 规则匹配的第 2 层帧。
  - **无 —** 不检查进入 WAP 设备的流量。
- **ACL 名称 —** 选择针对进入 WAP 设备的流量所要应用的 ACL 的类型。

  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。

步骤 4 单击**“保存”**。更改将保存到“启动配置”。

ACL 状态

“ACL 状态”页面显示各种类型的 ACL 规则的详细信息。

要查看 ACL 状态，请选择“ACL”>“ACL 状态”。

系统将显示以下信息：

- **ACL 名称 —** ACL 的名称。
- **绑定的接口 —** ACL 所关联到的接口。

- **规则数量 —** ACL 所包含的规则的数量。
- **操作 —** ACL 将会采取的操作。
- **全部匹配 —** 显示 ACL 规则是否匹配所有数据包。

规则字段 — 显示 ACL 的详细设置。有关详情，请参阅 **ACL 规则**。

可以单击**"刷新"**刷新屏幕并显示最新信息。

10

SNMP

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：

- 通用
- 视图
- 组
- 用户
- 目标

通用

可以使用“常规”页启用 SNMP 和配置基本协议设置。

配置常规SNMP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”>“常规”**。

步骤 2 对于**“SNMP”**设置，选择**“已启用”**。默认情况下，禁用 SNMP。

步骤 3 指定用于 SNMP 流量的**“UDP 端口”**。

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：

- **只读社区 —** 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。

- **读/写社区 —** 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。

- **管理工作站 —** 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：

  - **全部 —** 不限制可以通过 SNMP 访问 WAP 设备的工作站集。
  - **自定义 —** 允许的 SNMP 请求集仅限于指定用户。

- **NMS IPv4 地址/名称 —** 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 (.) 分隔各个标签。整个标签和句点字串的长度不能超过 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 地址/名称 —** 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 (.) 分隔各个标签。整个标签和句点字串的长度不能超过 253 个字符。

步骤 5 配置 SNMPv2 陷阱设置：

- **Trap 社团 —** 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 目标表 —** 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**"主机 IP 地址类型"**（IPv4 或 IPv6），然后添加**"主机名/IP 地址"**。

  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**"已启用"**复选框，然后选择合适的**"主机 IP 地址类型"**。

  另请参阅前面步骤中有关主机名的注释。

步骤 6 单击**"保存"**。更改将保存到"启动配置"。

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。建议在断开连接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。

接入点最多支持 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，"全部查看"(view-all) 和"无视图"(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。

添加和配置SNMP视图

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"**>**"视图"**。

步骤 2 单击**"添加"**可以在"SNMPv3 视图"表中创建新行。

步骤 3 选中新行的复选框，然后单击**“编辑”**：

- **视图名称 —** 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。
- **类型 —** 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 .3.6.1.2.1.1 指定。
- **掩码 —** 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 单击**“保存”**。视图会添加到“SNMPv3 视图”列表中，所做的更改也保存到“启动配置”。

注 要删除视图，请在列表中选择相应视图，然后单击**“删除”**。

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

通过将管理信息库 (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，接入点包含以下两组：

- **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 接入点最多支持 8 个组。

添加和配置SNMP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"**>**"组"**。

步骤 2 单击**"添加"**可以在"SNMPv3 组"中创建新行。

步骤 3 选中新组的复选框，然后单击**"编辑"**。

步骤 4 配置以下参数：

- **组名称 —** 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。

- **安全等级 —** 设置组的安全等级，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。使用此安全等级，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。使用此安全等级，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 用户"页定义 MD5 和 DES 密钥/密码。

- **写入视图 —** 对此组的 MIB 的写入访问权限，可以是以下选项之一：
  - **"全部视图"(view-all) —** 此组可以创建、更改和删除 MIB。
  - **"无视图"(view-none) —** 此组不能创建、更改和删除 MIB。

- **读取视图 —** 对此组的 MIB 的读取访问权限：
  - **"全部视图"(view-all) —** 允许此组查看和读取所有 MIB。
  - **"无视图"(view-none) —** 此组不能查看或读取 MIB。

步骤 5 单击**"保存"**。组会添加到"SNMPv3 组"列表中，所做的更改也保存到"启动配置"。

注 要删除组，请在列表中选择相应组，然后单击**“删除”**。

用户

可以使用“SNMP 用户”页定义用户、将安全等级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。接入点中没有默认的 SNMPv3 用户，最多可以添加 8 个用户。

添加SNMP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”**>**“用户”**。

步骤 2 单击**“添加”**可以在“SNMPv3 用户”表中创建新行。

步骤 3 选中新行的复选框，然后单击**“编辑”**。

步骤 4 配置以下参数：

- **用户名 —** 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。
- **组 —** 用户映射到的组。默认组为 RW 和 RO。可以在“SNMP 组”页定义其他组。
- **验证类型 —** 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。
  - **无 —** 不需要对来自此用户的 SNMPv3 请求进行身份验证。
- **验证通行短语 —**（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。
- **加密类型 —** 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。

- 无 — 来自此用户的 SNMPv3 请求不需要隐私。

▪ **加密通行短语 —** （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 单击**"保存"**。用户会添加到"SNMPv3 用户"列表中，所做的更改也保存到"启动配置"。

注 要删除用户，请在列表中选择相应用户，然后单击**"删除"**。

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 接入点最多支持 8 个目标。

添加SNMP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">"目标"**。

步骤 2 单击**"添加"**。会在表中添加新行。

步骤 3 选中新行的复选框，然后单击**"编辑"**。

步骤 4 配置以下参数：

▪ **IP 地址 —** 输入用于接收目标的远程 SNMP 管理器的 IPv4 地址。

▪ **UDP 端口 —** 输入用于发送 SNMPv3 目标的 UDP 端口。

▪ **用户 —** 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 单击**"保存"**。用户会添加到"SNMPv3 目标"列表中，所做的更改也保存到"启动配置"。

注 要删除 SNMP 目标，请在列表中选择相应用户，然后单击**"删除"**。

11

网页认证

本章介绍网页认证 (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。您可以对 CP 验证进行配置，同时允许访客和已通过身份验证的用户进行访问。

授予访问权限前，必须根据已授权的 CP 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。

网页认证包含两个 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 WAP571/E 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（例如 WPA 或 WPA 企业）配置的其他 VAP 同时运行。

本章包括以下主题：

- 全局配置
- 本地组/用户
- 实例配置
- 实例关联
- Web 门户自定义
- 已验证的客户端

全局配置

通过“全局 CP 配置”页，可以控制网页认证功能的管理状态，并对影响 WAP 设备中配置的所有 CP 实例的全局设置进行配置。

配置 CP 全局设置

要配置 CP 全局设置，请执行以下步骤：

步骤 1 选择**“网页认证”>“全局配置”**。

步骤 2 配置以下参数：

- **网页认证模式 —** 在 WAP 设备上启用或禁用网页认证操作。
- **身份验证超时值 —** 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证，客户端可能需要刷新身份验证网页。默认的身份验证超时值为 300 秒。范围介于 60 至 600 秒之间。
- **其他 HTTP 端口 —** 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。
- **其他 HTTPS 端口 —** 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。

步骤 3 “网页认证配置计数器”区域显示只读的 CP 信息：

- **实例计数 —** 当前在 WAP 设备中配置的 CP 实例数。最多可以配置两个实例。
- **组计数 —** 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。
- **用户计数 —** 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 4 单击**“保存”**。更改将保存到“启动配置”。

本地组/用户

“本地组/用户”页用于管理本地组和用户。

每个本地用户都被指定给一个用户组。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 选择**“网页认证”>“本地组/用户”**。

步骤 2 在“本地组设置”区域中，配置以下参数：

- **网页认证组 —** 选择“创建”来创建新组。
- **组名称 —** 输入新组的名称。

步骤 3 单击**“添加组”**。更改将保存到“启动配置”。

要删除本地用户组，请执行以下步骤：

步骤 1 选择**“网页认证”>“本地组/用户”**。

步骤 2 在“本地组设置”区域中，选择要删除的组。

步骤 3 选中“删除组”选项。

步骤 4 单击**“删除组”**。更改将保存到“启动配置”。

您可以配置一个 CP 实例，来同时支持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。

在本地数据库中最多可配置 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 选择**“网页认证”>“本地组/用户”**。

步骤 2 在“本地用户设置”区域中，配置以下参数：

- **网页认证用户 —** 选择“创建”来创建新用户。
- **用户名 —** 输入新用户的名称。

步骤 3 单击“添加用户”。

步骤 4 “本地用户设置”区域再次出现，其中包含更多选项。配置以下参数：

- **用户密码 —** 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网页认证登录网络。
- **以明文显示密码 —** 如果启用，将显示键入的文本。如果禁用，输入时不隐藏文本。
- **超时退出值 —** 输入客户端取消与 WAP 设备的关联后，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 CP 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。
- **组名称 —** 选择指定的用户组。配置每个 CP 实例以支持特定的用户组。
- **最大上行带宽 —** 输入使用网页认证时客户端可传输流量的最大上传速度（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 1300 Mbps 之间。默认值为 0。
- **最大下行带宽 —** 输入使用网页认证时客户端可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 1300 Mbps 之间。默认值为 0。

步骤 5 单击**“保存用户”**。更改将保存到“启动配置”。

要删除本地用户，请执行以下步骤：

步骤 1 选择**“网页认证”>“本地组/用户”**。

步骤 2 在“本地用户设置”区域中，选择要删除的用户。

步骤 3 选中“删除用户”选项。

步骤 4 单击**“删除用户”**。更改将保存到“启动配置”。

实例配置

最多可以创建两个 CP 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，请转至网络页添加 VAP。

您是否需要添加新组或新用户？如果需要，请转至本地组/用户页添加组或用户。

创建 CP 实例并配置其设置

要创建 CP 实例并配置其设置，请执行以下步骤：

步骤 1 选择**“网页认证”>“实例配置”**。

步骤 2 从**“网页认证实例”**列表中选择**“创建”**。

步骤 3 在“实例名称”字段中输入 1 到 32 个字母数字字符的 CP 实例名称。

步骤 4 单击**“保存”**。

步骤 5 **“网页认证实例参数”区域再次出现，其中包含更多选项。**配置以下参数：

- **实例 ID —** 显示实例 ID。此字段是不可配置的。
- **管理模式 —** 启用和禁用 CP 实例。
- **协议 —** 选择在验证过程中是将 HTTP 还是 HTTPS 用作 CP 实例的协议。
  - **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。
- **验证 —** CP 用于验证客户端的身份验证方法：
  - **访客 —** 用户不需要通过数据库进行身份验证。
  - **本地 —** 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。**Active Directory 服务器 —** WAP 通过 `starttls` 命令使用 SSL\TLS 执行安全 LDAP 绑定，对 Active Director 中具有 sAMAccountName 属性的用户进行身份验证。

- **第三方凭证 —** WAP 设备能够对使用 Facebook 或 Google 帐户的用户进行身份验证。

- **社交媒体登录方法 —** WAP 设备能够通过 OAuth 协议对使用 Facebook 或 Google 帐户的用户进行身份验证。
  - **Facebook —** 启用或禁用“社交媒体登录”以使用 Facebook 帐户对客户端进行身份验证。
  - **Google —** 启用或禁用“社交媒体登录”以使用 Google 帐户对客户端进行身份验证。
- **Active Directory 服务器主机-1 —** 添加一台服务器并输入域控制器的 IP 地址。
- **Active Directory 服务器主机-2 —** 添加一台服务器并输入域控制器的 IP 地址。
- **Active Directory 服务器主机-3 —** 添加一台服务器并输入域控制器的 IP 地址。

注
- 可以添加多台服务器。接入点将按照主机-1 至主机-3的顺序对这些服务器进行测试。

- **Walled Garden 范围 —** 指定用户在登录 Web 门户页前可以访问的域的列表。列表项应使用逗号分隔，并且域可以包括星号 (*) 形式的通配符。

注
- 从概念构思到产品发布，思科将数据保护、隐私和安全要求融入到整个产品设计和开发过程。有关详细信息，请参阅 https://www.cisco.com/c/en/us/about/trust-center/gdpr.html

- 启用 Facebook 或 Google 登录时，“Walled Garden”（围墙花园）功能将自动激活，并会将下列域添加至该列表以进行身份验证。该域列表可以随 Facebook 或 Google 而更改，内容可能不是最新的。可以手动添加这些域。
  - **Facebook**：*.facebook.com、*.facebook.net、*.fbcdn.net
  - **Google**：*.googleapis.com、 apis.google.com、 accounts.google.com、*. googleusercontent.com、 ssl.gstatic.com、 fonts.gstatic.com
  - **Windows 10:** ww.msftconnecttest.com
- **重定向 —** 启用时，网页认证应将新通过身份验证的客户端重定向到已配置的 URL。如果禁用此选项，用户会在成功验证后看到特定于区域设置的欢迎页。
- **重定向 URL —** 如果启用“重定向”模式，输入新通过身份验证的客户端所重定向到的 URL （包括 http://）。范围介于 0 至 256 个字符之间。
- **超时退出值 —** 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量。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。

还会为每个用户配置超时退出值。请参阅本地组/用户页。除非此处配置的值设置为 0（默认值），否则在“本地用户”页上设置的超时退出值优先于此值。值 0 表示使用实例超时值。

- **会话超时值 —** 输入 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。
- **最大上行带宽 —** 输入使用网页认证时客户端可传输流量的最大上传速度 （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 1300 Mbps 之间。默认值为 0。
- **最大下行带宽 —** 输入使用网页认证时客户端可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 1300 Mbps 之间。默认值为 0。
- **用户组名称 —** 如果“验证”模式设置为“本地”或“RADIUS”，请将一个现有用户组指定给 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 网络 —** 选择 WAP RADIUS 客户端是否使用配置的 IPv4 或 IPv6 RADIUS 服务器地址。
- **全局 RADIUS —** 如果“验证”模式设置为“RADIUS”，请选中“启用”以使用默认全局 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，请参阅 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的字段中配置这些服务器。
- **RADIUS 帐务 —** 选中“启用”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 帐务，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。
- **服务器 IP 地址 1** 或 **服务器 IPv6 地址 1 —** 输入此 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。
- **服务器 IP 地址 (2 至 4)** 或 **服务器 IPv6 地址 (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。
- **密钥 1 —** 输入 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。

- **密钥 2** 至 **密钥 4 —** 输入与已配置的备份 RADIUS 服务器关联的 RADIUS 密钥。服务器 IP (IPv6) 地址 1 的服务器使用“密钥 1”，服务器 IP (IPv6) 地址 2 的服务器使用“密钥 2”，以此类推。
- **区域设置计数 —** 与实例关联的区域设置数量。在“Web 自定义预览”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。
- **删除实例 —** 选中以删除当前实例。

步骤 6 单击**“保存”**。更改将保存到“启动配置”。

实例关联

创建实例后，使用“实例关联”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。

将实例关联到 VAP

要将实例关联到 VAP，请执行以下步骤：

步骤 1 选择**“网页认证”>“实例关联”**。

步骤 2 选择要配置的无线射频。

步骤 3 为要与实例关联的每个 VAP 选择实例名称。

步骤 4 单击**“保存”**。更改将保存到“启动配置”。

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 CP 实例关联的 VAP 时，会看到身份验证页。

通过“Web 门户自定义”页，可以为网络中的不同区域设置创建唯一页面并自定义页面上的文本和图像。

配置 CP 身份验证页

创建并自定义 CP 身份验证页

要创建并自定义 CP 身份验证页，请执行以下步骤：

步骤 1 选择**“网页认证”>“Web 门户自定义”**。

步骤 2 从**“网页认证 Web 区域设置”**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。

步骤 3 在“网页认证 Web 区域设置参数”区域中，配置以下参数：

- **Web 区域设置名称 —** 输入要指定给页面的 Web 区域设置。名称可以包含 1 至 32 个字母数字字符。
- **网页认证实例 —** 选择该区域设置所关联的 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 4 单击**“保存”**。更改将保存到“启动配置”。

步骤 5 “网页认证 Web 区域设置参数”区域再次出现，其中包含用于修改区域设置的其他选项。“区域设置 ID”和“实例名称”字段无法编辑。可编辑字段使用默认值进行填充。

步骤 6 配置以下参数：

- **背景图像名 —** 选择作为页面背景显示的图像。可以单击**“上传/删除自定义图像”**以上传 CP 实例的图像。有关详情，请参阅上传和删除图像。
- **徽标图像名 —** 选择要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传到 WAP 设备，可以从列表中将其选中。
- **前景颜色 —** 输入 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。
- **背景颜色 —** 输入 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。
- **分隔符 —** 输入粗水平线的颜色 HTML 编码，用于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。
- **区域设置标签 —** 输入区域设置的说明性标签，包含 1 至 32 个字符。默认区域设置是“英语”。
- **区域设置 —** 输入区域设置的缩写，包含 1 至 32 个字符。默认值为“en”。

- **帐户图像 —** 选择显示在登录字段上方，用于表示已通过身份验证的登录用户的图像文件。
- **帐户标签 —** 指示用户输入用户名的文本。范围介于 1 至 32 个字符之间。
- **用户标签 —** 用户名文本框的标签。范围介于 1 至 32 个字符之间。
- **密码标签 —** 用户密码文本框的标签。范围介于 1 至 64 个字符之间。
- **按钮标签 —** 用户单击此按钮上的标签，可以提交其用户名和密码进行身份验证。范围介于 2 至 32 个字符之间，默认值为“连接”。
- **字体 —** 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。
- **浏览器标题 —** 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“网页认证”。
- **浏览器内容 —** 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“欢迎使用无线网络”。
- **内容 —** 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“要开始使用此服务，请输入您的凭证并单击连接按钮”。
- **接受使用政策 —** 显示在“接受使用政策”框中的文本。范围介于 1 至 4096 个字符之间。默认值为“接受使用政策”。
- **接受标签 —** 指示用户选中此复选框以确认阅读并接受“接受使用政策”的文本。范围介于 1 至 128 个字符之间。
- **未接受时显示的文本 —** 用户提交登录凭证但未选中“接受使用政策”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。
- **正在进行时显示的文本 —** 在身份验证期间显示的文本。范围介于 1 至 128 个字符之间。
- **被拒时显示的文本 —** 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。
- **欢迎标题 —** 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。
- **欢迎内容 —** 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。
- **删除区域设置 —** 删除当前区域设置。

步骤 7 单击**“保存”**。更改将保存到“启动配置”。

步骤 8 单击**“预览”**查看更新页面。

注 单击**“预览”**将显示已保存到“启动配置”的文本和图像。如果进行了更改，请单击**“保存”**，然后单击**“预览”**以查看更改。

上传和删除图像

用户开始访问与 CP 实例关联的 VAP 时，会出现身份验证页面。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

将二进制图形文件上传到 WAP 设备

要将二进制图形文件上传到 WAP 设备，请执行以下步骤：

步骤 1 在“Web 门户自定义”页，单击**“背景图像名”**、**“徽标图像名”**或**“帐户图像”**字段旁边的**“上传/删除自定义图像”**。

会出现“Web 门户自定义图像”页。

步骤 2 单击“浏览”以选择图像。

步骤 3 单击**“上传”**。

步骤 4 单击**“上一步”**返回“Web 门户自定义图像”页。

步骤 5 选择要配置的**“网页认证 Web 区域设置”**。

步骤 6 对于**“背景图像名”**、**“徽标图像名”**或**“帐户图像”**字段，选择新上传的图像。

步骤 7 单击**“保存”**。

步骤 8 要删除图像，请在“Web 门户自定义图像”页的**“删除 Web 自定义图像”**列表中将其选中，然后单击**“删除”**。无法删除默认图像。

已验证的客户端

“已验证的客户端”页提供两个表。一个是“已验证的客户端”表，与在任何网页认证实例上通过身份验证的客户端有关。另一个是“身份验证失败的客户端”表，其中列出有关尝试在网页认证进行身份验证但失败的客户端的信息。

要查看通过身份验证或未通过身份验证的客户端列表，请选择“网页认证”>“已验证的客户端”。系统将显示以下信息：

- **MAC 地址 —** 客户端的 MAC 地址。
- **IP 地址 —** 客户端的 IP 地址。
- **用户名 —** 客户端的网页认证用户名。
- **协议 —** 用户用于建立连接的协议（HTTP 或 HTTPS）。
- **验证 —** 用于在网页认证对用户进行身份验证的方法，可以是以下值之一：
  - **访客 —** 用户不需要通过数据库进行身份验证。
  - **本地 —** 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。
  - **Facebook —** WAP 设备使用 Facebook 帐户对用户进行身份验证。
  - **Google —** WAP 设备使用 Google 帐户对用户进行身份验证。
  - **Active Directory 服务 —** WAP 设备使用 Active Directory 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。
- **无线 ID —** 无线 ID。
- **网页认证 ID —** 与用户关联的网页认证实例的 ID。
- **会话超时 —** 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。

- **离开超时 —** 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。
- **已接收的数据包数 —** WAP 设备从用户工作站接收的 IP 数据包数。
- **已发送的数据包数 —** 从 WAP 设备发送到用户工作站的 IP 数据包数。
- **已接收的字节数 —** WAP 设备从用户工作站接收的字节数。
- **已发送的字节数 —** 从 WAP 设备发送到用户工作站的字节数。
- **失败时间 —** 身份验证失败的时间。包含显示失败时间的时间戳。

单击**“刷新”**以显示 WAP 设备中的最新数据。

12

集群配置

本章介绍如何通过多个 WAP 设备配置集群设置。

具体包括以下主题：

- 集群配置概述
- 接入点
- 会话
- 信道管理
- 无线相邻设备
- 集群固件升级

集群配置概述

集群配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。可以使用集群配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，集群配置还有助于无线服务间的信道规划，从而减少无线射频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“设置向导”配置“集群配置”或加入现有的集群配置。如果不想使用“设置向导”，可以使用基于 Web 的配置实用程序。

管理接入点间的集群配置

集群配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。集群支持最多包含 16 个已配置 WAP571/E 设备的组，但同一集群中不能包含非 WAP571/E 型号。

通过集群配置，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。下表显示集群配置的无线服务限制。

组/集群类型	每个集群配置的 WAP 设备数	每个集群配置的活动客户端数	最大客户端数（活动和空闲）
WAP571/E	16	960（仅限于双频 WAP571/E）	2048（仅限于双频 WAP571/E）

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）队列参数和无线射频参数。配置设备的集群配置时，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。

组成集群的先决条件或条件

要组成一个集群，请确保满足以下先决条件或条件：

步骤 1 计划集群配置集群。确保要组成集群的两个或更多 WAP 设备彼此兼容。例如，思科 WAP571/E 设备只能与其他思科 WAP571/E 设备组成集群。

注 强烈建议在所有集群化的 WAP 设备上运行最新的固件版本。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 设备的集群配置。请参阅接入点。

步骤 4 确认 WAP 设备全部引用相同的集群配置名称。请参阅接入点。

集群配置协商

如果为集群配置启用并配置接入点，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。

以下规则适用于集群配置集群的形成和仲裁：

- 对于现有的集群配置集群，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。
- 两个独立的集群配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。

- 如果集群配置模式下的 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。）

从集群配置中删除的 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。

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。

传播和不传播到集群配置接入点的配置参数

在集群配置中传播的通用配置设置和参数	
网页认证	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 设置的无线射频设置（有一些例外情况）
日志设置	恶意 AP 检测
MAC 过滤	调度程序
管理访问控制	SNMP General 和 SNMPv3
网络	WPA-PSK 复杂性

在集群配置中传播的通用配置设置和参数	
时间设置	无线组播转发
LED 显示	
LLDP （除 POE 优先级配置以外）	
Umbrella	

在集群配置中传播的无线射频配置设置和参数
模式
分片阈值
RTS 阈值
速率集
主信道
保护
固定组播速率
广播或多播速率限制
信道带宽
支持的较短保护间隔

在集群配置中不传播的无线射频配置设置和参数
信道
信标间隔
DTIM 周期
最大工作站数
发射功率

在集群配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	
数据包捕获	工作组网桥

接入点

通过“接入点”页，可以在 WAP 设备中启用或禁用集群配置、查看集群成员和配置成员位置及成员的集群名称。还可以单击成员的 IP 地址，在该设备中配置和查看数据。

为集群配置配置 WAP 设备

要配置每个集群配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**“集群配置”>“接入点”**。

默认情况下， “集群配置”在接入点中为禁用状态。此设置禁用时，会显示**“启用集群配置”**按钮。如果启用“集群配置”，则会显示**“禁用集群配置”**按钮。仅在“集群配置”禁用时可以编辑“集群配置”的选项。

此页右侧的图标指示是否启用“集群配置”，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“集群配置”，为每个“集群配置”集群成员配置以下信息。

- **位置 —** 输入接入点物理位置的说明，例如 Reception。此位置字段可选。
- **集群名称 —** 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集群配置，集群名称必须是唯一的。默认名称为 ciscosb-cluster。
- **集群 IP 版本 —** 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，集群配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。

集群配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 单击**“启用集群配置”**。

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配置配置一个或多个 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 对要加入集群配置的其他 WAP 设备重复上述步骤。

查看集群配置信息

启用集群配置时，接入点会自动与配置相同的其他 WAP 设备形成一个集群。在“接入点”页，表中会列出检测到的 WAP 设备并显示以下信息：

- **位置 —** 接入点物理位置的说明。
- **MAC 地址 —** 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，集群配置状态和 WAP 设备数量通过采用图表形式显示在页面右侧。

将接入点添加到集群配置

要将当前处于独立模式的新接入点添加到集群配置集群，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**“集群配置”>“接入点”**。

步骤 3 选择与为集群成员配置的名称相同的**“集群名称”**。

步骤 4 （可选）在**“位置”**字段中输入接入点物理位置的说明，例如 Reception。

步骤 5 单击**“启用集群配置”**。

此接入点自动加入集群配置。

从集群配置中删除接入点

要从集群配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，单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**“集群配置”>“接入点”**。

步骤 3 单击**“禁用集群配置”**。

该接入点的**“集群配置”**状态字段会显示**“禁用”**。

导航至特定设备的配置信息

集群配置集群中的所有 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，因为群集中任何 WAP 设备的管理 - 配置更改都会传播给其他成员。

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“接入点”页单击表中的 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

“会话 页”显示与集群配置集群中的 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 设备中的每个无线射频， “会话 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“状态”>“关联客户端”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，然后单击**“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。

要查看与集群相关联的会话，请选择**“集群配置”>“会话”**。

以下是对于具有集群配置的每个无线局域网客户端显示的数据。

- **AP 位置 —** 接入点的位置。

  位置来源于“管理” > “系统设置”页中指定的位置。

- **用户 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。

- **空闲 —** 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。

- **速率 —** 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。

  报告的速率是从接入点传输到客户端的最后一个数据包的速率。此值在基于接入点和客户端之间的信号质量的通告速率集中有所不同，并且广播帧或组播帧也以此速率进行发送。当接入点使用默认速率向 STA 发送广播帧时，对于 2.4 Ghz 无线射频，此字段将报告 1 Mbit/s；对于 5 Ghz 无线射频，此字段将报告 6 Mbit/s。空闲的客户端最可能报告较低的默认速率。

- **信号 —** 无线局域网客户端从接入点接收的无线射频 (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。

- **接收总数 —** 无线局域网客户端在当前会话期间接收的数据包总数。

- **发送总数 —** 在此会话期间传输到无线局域网客户端的数据包总数。

- **错误率 —** 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，请单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，请单击“信号”列标签。

信道管理

“信道管理”页显示集群配置集群中的 WAP 设备的当前和规划的信道分配。

如果启用信道管理，则接入点自动分配集群配置集群中的 WAP 设备使用的无线射频信道。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）传播到集群配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。

配置和查看集群配置成员的信道分配

要配置和查看集群配置成员的信道分配，请执行以下步骤：

步骤 1 在导航窗格中选择**“集群配置”>“信道管理”**。

在“信道管理”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，请单击**“开始”**。

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 设备的无线射频信道。如果启用信道管理，则不会将此集群的无线射频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集群配置集群中的 WAP 设备使用的无线射频信道，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。自动将无线射频信道策略设置为静态模式，并且对于“无线”>“无线射频”页的**“信道”** 字段不提供**“自动”**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，请单击**“停止”**。

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“当前信道分配”表和“建议信道分配”表。

当前信道分配表

“当前信道分配”表按 IP 地址列出集群配置集群中的所有 WAP 设备。

此表提供以下有关当前信道分配的详细信息。

- **位置 —** 设备的物理位置。
- **IP 地址 —** 接入点的 IP 地址。
- **无线射频 —** 无线射频的 MAC 地址。
- **频段 —** 接入点进行广播所在的频段。
- **信道 —** 此接入点当前进行广播所在的无线射频信道。
- **已锁定 —** 强行将接入点保留在当前信道。
- **状态 —** 显示设备中无线射频功能的状态。（部分 WAP 设备可能具有多个无线射频功能，而每个无线射频均显示在表中的单独一行中。）无线射频状态是 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。

单击**“保存”**更新锁定设置。锁定设备显示“当前信道分配”表和“建议信道分配”表的相同信道。锁定设备会保留其当前信道。

建议信道分配表

“建议信道分配”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。

对于集群配置中的每个 WAP 设备， “建议信道分配”表显示和“当前信道分配”表相同的位置、IP 地址和无线射频。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射频信道。

配置高级设置

通过“高级设置”区域，可以自定义和制定集群配置的信道规划。

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：

- **更改信道的条件是干扰降低至少 —** 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。

- **确定是否存在更好的信道集的时间间隔 —** 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，请单击**“保存”**。更改将保存到“活动配置”和“启动配置”。

无线相邻设备

对于集群中每个无线射频范围内的每个无线射频，“无线相邻设备”页最多可显示 20 个设备。（例如，如果 WAP 设备拥有两个无线射频，则集群中会显示 40 个设备。）“无线相邻设备”页还会区分集群成员和非集群成员。

“无线相邻设备”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，请选择**“集群配置”>“无线相邻设备”**。要查看在特定集群配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**“无线”>“恶意 AP 检测”**。

对于每个相邻接入点，显示以下信息：

- **显示相邻 AP —** 选择以下单选按钮之一以更改视图：
  - **在集群中 —** 仅显示属于集群成员的相邻 WAP 设备。
  - **不在集群中 —** 仅显示不属于集群成员的相邻 WAP 设备。
  - **全部 —** 显示所有的相邻 WAP 设备（集群成员和非成员）。

注 如果检测到的接入点也是集群成员，则仅默认 VAP (VAP0) 的 SSID 显示为“在集群中”。接入点中的非默认 VAP 显示为“不在集群中”。

- **集群 —** 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**“集群配置”>“接入点”**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。

  可以单击 IP 地址以查看有关特定 WAP 设备的更多详细信息。

- **邻居 —** 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。

邻居列表中每个 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。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。

查看集群配置成员的详细信息

要查看集群成员的详细信息，请在此页顶端单击成员的 IP 地址。

以下的设备详细信息出现在邻居列表下方。

- **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。
- **信道 —** 接入点当前进行广播所在的信道。
- **速率 —** 此接入点当前的传输速率 （兆位/秒）。当前速率始终都是“支持的速率”中所示速率之一。
- **信号 —** 从接入点检测到的无线射频信号的强度，以分贝 (dB) 为单位。
- **信标间隔 —** 接入点使用的信标间隔。
- **信标时间 —** 从此接入点接收的最后一个信标的日期和时间。

集群固件升级

集群提供集中的集群固件升级功能，通过此功能，可从基准接入点 （集群控制器）对集群中的接入点进行升级。集群固件升级仅可从基准接入点执行。

在“集群固件升级”页，表中会列出检测到的 WAP 设备并显示以下信息：

- **位置 —** 接入点物理位置的说明。

- **IP 地址 —** 接入点的 IP 地址。
- **MAC 地址 —** 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。
- **当前固件版本 —** 接入点的当前运行固件版本。
- **固件传输状态 —** 显示集群成员中的固件下载和验证的状态 （无/“已开始”[Started]/“已下载”[Downloaded]/“成功”[Success]/“失败”[Fail]/Abort_admin/Abort_local/Dap_resigned）。
- **固件传输进度条—** 显示固件下载的进度条。

选择进行升级的集群成员

要选择进行升级的集群成员，请执行以下步骤：

步骤 1 在导航窗格中选择**“集群配置”>“集群固件升级”**。

步骤 2 选择要升级的接入点相应的复选框。

步骤 3 单击**“保存”**。

要获得最新的集群固件升级状态，请执行以下步骤：

单击**“刷新”**。

使用 TFTP 升级集群成员的固件

要使用 TFTP 升级集群成员的固件，请执行以下步骤：

步骤 1 选择**“使用 TFTP 作为传输方式”**。

步骤 2 在**“源文件名”**字段中，输入映像文件的名称 （1 至 128 个字符），应包含所要上传的映像所在目录的路径。

例如，要上传位于 /share/builds/ap 目录下的 ap_upgrade.tar 映像，请输入：/share/builds/ap/ap_upgrade.tar

所提供的固件升级文件必须是 tar 文件。请勿尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不受支持。

文件名不能包含以下字符：空格、<、>、|、\、:, (,), &, ; , #, ?、 * 以及两个或两个以上连续的句点。

步骤 3 输入**“TFTP 服务器 IPv4 地址”**，然后单击**“开始升级”**。

使用 HTTP 进行升级

要使用 HTTP 进行升级，请执行以下步骤：

步骤 1 选择**“使用 HTTP 作为传输方式”**。

步骤 2 如果知道新文件的名称和路径，请在**“新固件映像”**字段中将其输入。否则，请单击**“浏览”**按钮，查找网络中的固件映像文件。

所提供的固件升级文件必须是 tar 文件。请勿尝试使用 bin 或其他格式的文件进行升级，这些类型的文件不受支持。

步骤 3 单击**“开始升级”**应用新的固件映像。

注 **“总体升级状态”**显示所有集群成员的总体升级状态 （“未初始化”[Not Initialized]/“正在进行”[In Progress]/“已完成”[Completed]/“失败”[Fail]/Abort_admin/无）。

要停止从基准接入点进行的集群成员升级，请执行以下步骤：

单击**“停止升级”**。

13

Umbrella

本章介绍如何在 WAP 设备上配置 Umbrella 功能。

具体包括以下主题：

- 思科 Umbrella 概述
- 配置 Umbrella

思科 Umbrella 概述

思科 Umbrella 是通过云交付的网络安全服务，不仅可实时提供洞察力来保护设备免受恶意软件攻击，还可实时提供漏洞保护。它可以使用不断演进的大数据和数据挖掘方法，对攻击做出前瞻性预测，同时进行基于类别的过滤。

思科 Umbrella 服务器可解析 DNS 查询并针对每个身份执行预先配置的安全过滤规则，从而将域标记为“恶意”使阻止的页面返回客户端，或者将域标记为“安全”使解析的 IP 地址返回客户端。

配置 Umbrella

要配置 Umbrella，请执行以下步骤：

步骤 1 在导航窗格中选择**“Umbrella”**。

步骤 2 配置以下参数：

- **启用 —** 在 WAP 设备上启用或禁用 Umbrella 功能。
- **API 密钥 —** 从“Umbrella 控制面板”获取 API 密钥：**“管理员”->“API 密钥”**。
- **API 密钥的密码 —** 只有在“Umbrella 控制面板”中创建 API 密钥后，才会显示 API 密钥的密码。

注

- 更改 API 密钥、API 密钥的密码和设备标签会触发重新注册，从而创建网络设备。
- **设备标签（可选）—** 用于描述设备或分配给设备的特定来源的文本标签。请确保它在您的组织中是唯一的。
- **要绕过的本地域（可选）—** 如果接入点已列入该列表，它会转发 DNS 查询。列表项应使用逗号分隔，并且域可以包括星号 (*) 形式的通配符。例如：*.cisco.com.*.
- **DNSCrypt —** 指定是否启用 DNSCrypt 功能。
- **注册状态 —** 注册状态具体显示如下：**“注册成功”**、**“正在注册”**或**“注册失败”**。

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。单击**“状态和统计信息”>“日志”** 即可查看日志消息。

- 取消身份验证原因代码表

取消身份验证原因代码表

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

原因代码	含义
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
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 WAP571/E 所带来的任何优势。

支持	
思科支持社区	www.cisco.com/go/smallbizsupport
思科 Small Business 支持中心 (SBSC) 电话支持联系人名单	www.cisco.com/go/sbsc
思科支持和资源	www.cisco.com/go/smallbizhelp
思科支持服务信息	www.cisco.com/go/sbs www.cisco.com/go/software （需要注册/登录）。
思科固件下载	www.cisco.com/go/smallbizfirmware 选择一个链接，可下载相应思科产品的固件。无需登录。 Cisco.com (www.cisco.com/go/software) （需要注册/登录）上的“下载”(Download) 区域提供了针对所有其他思科产品的软件和固件下载。
思科开源请求	www.cisco.com/go/smallbiz_opensource_request
思科合作伙伴中心 （需要合作伙伴登录）	www.cisco.com/web/partners/sell/smb
产品文档	
支持以太网供电 (PoE) 的思科 WAP571/E Wireless-AC/N 高级双频无线接入点快速入门指南和管理指南	http://www.cisco.com/go/500_wap_resources

B