支持 2.5GbE 局域网的思科 WAP581 Wireless-AC/N 双频无线接入点

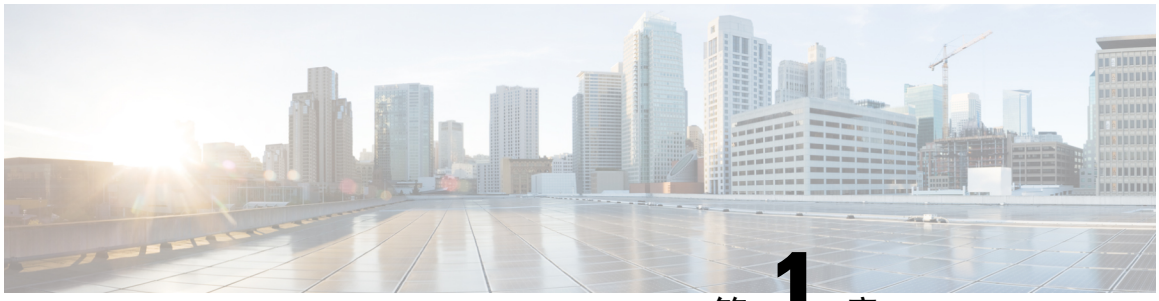
首次发布日期: 2016 年 11 月 23 日

上次修改日期: 2018 年 7 月 16 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883


Java 徽标是 Sun Microsystems, Inc. 在美国或其他国家/地区的商标或注册商标。

目录



第 1 章

使用入门

本章包含以下小节：

配置入门

本节介绍系统要求和如何访问基于 Web 的配置实用程序。

支持的浏览器

在开始使用该配置实用程序之前，请确保您的计算机安装有 Internet Explorer 9 或更高版本、Firefox 46 或更高版本、Chrome 49 或更高版本、Safari 5.0 或更高版本。

浏览器限制

- 如果使用 Internet Explorer 9，请配置以下安全设置：
  - 选择**工具**、**Internet 选项**，然后选择**安全**选项卡。
  - 接下来，选择**本地内联网**，然后选择**站点**。
  - 选择**高级**，然后选择**添加**。将 WAP 设备的内联网地址 `http://<ip-address>` 添加到本地内联网区域。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内联网区域。
- 如果管理站上有多个 IPv6 接口，则可以使用 IPv6 全局地址代替 IPv6 本地地址从浏览器访问 WAP 设备。

启动基于 Web 的配置实用程序

请按照以下这些步骤从您的计算机访问配置实用程序，来配置 WAP 设备：

1. 将 WAP 设备连接到您的计算机所在的网络（IP 子网）。WAP 设备的出厂默认 IP 地址配置为 DHCP。请确保您的 DHCP 服务器正在运行且可被访问。
2. 找到 WAP 设备的 IP 地址。
    1. 可通过使用思科 FindIT 网络发现实用程序来访问和管理 WAP 设备。通过此实用程序，可自动发现与计算机在同一本地网段中的所有受支持的思科设备。您可获取每个设备的静态视图，或启动产品配置实用程序来查看和配置设置。有关详细信息，请参阅http://www.cisco.com/go/findit。
    2. WAP 设备支持 Bonjour 功能，能够自动广播其服务并侦听其他支持 Bonjour 功能的设备所通告的服务。如果您有支持 Bonjour 功能的浏览器（例如安装 Bonjour 插件的 Microsoft Internet Explorer 或 Apple Mac Safari 浏览器），则无需知道 IP 地址即可找到您本地网络中的 WAP 设备。

        可从 Apple 网站下载适用于 Microsoft Internet Explorer 浏览器的完整 Bonjour 程序，下载网址为：http://www.apple.com/bonjour/.
    3. 访问路由器或 DHCP 服务器，查找 DHCP 服务器所分配的 IP 地址。有关详细信息，请参阅 DHCP 服务器说明。
3. 启动 Web 浏览器（例如 Microsoft Internet Explorer）。
4. 在地址栏中输入默认 DHCP 地址，然后按 **Enter** 键。
5. 输入默认用户名和密码：在**用户名**和**密码**字段中输入 `cisco`。
6. 单击**登录**。系统显示**无线接入点设置向导**。

根据“设置向导”说明完成安装。强烈建议您在首次安装时使用“设置向导”。有关详细信息，请参阅 使用无线接入点设置向导，第 2 页。

注销

默认情况下，如果配置实用程序在10分钟内无活动，将会注销。有关更改默认超时时间的说明，请参阅 管理，第 24 页。

要注销，请单击配置实用程序右上角的**注销**。

使用无线接入点设置向导

首次登录无线接入点（或重置为出厂默认设置后）时，系统会显示“无线接入点设置向导”，以帮助执行初始配置。请按照以下步骤完成向导：

注释 如果点击**取消**跳过向导，系统将显示**更改密码**页面。在该页面中，您可以更改默认的登录密码和用户名。有关详细信息，请参阅更改密码，第 5 页。

更改密码后必须重新登录：

步骤 1 在向导的**欢迎**页面点击**下一步**。

步骤 2 在**固件升级**窗口中，点击**升级**以升级固件。

注释 完成固件升级后，设备将自动重启并直接进入登录页面。

步骤 3 点击**跳过**。系统将显示**恢复配置**窗口。

步骤 4 选择要应用于设备的配置文件，然后点击**保存**。

注释 点击保存。设备**将应**用相关配置，然后自动重启并直接进入登录页面。

步骤 5 点击**跳过**。系统将显示**配置设备—IP 地址**窗口。

步骤 6 单击**动态 IP 地址 (DHCP)**（**建议**）从 DHCP 服务器接收 IP 地址，或单击**静态 IP 地址**手动配置 IP 地址。有关这些字段的说明，请参阅IPv4 配置。

步骤 7 单击**下一步**。此时会出现**集群设置 - 设置集群**窗口。有关集群设置的说明，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，请单击**新建集群名称**并指定新名称。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集群设置，请单击**请勿启用集群设置**。

或者，可以在**无线接入点位置**字段中输入位置以记录 WAP 设备的物理位置。

如果选中**加入现有集群**单选按钮，WAP将基于集群来配置其余设置。单击**下一步**并接受确认消息，以加入集群。单击**提交**加入集群。完成配置后，单击**完成**退出设置向导。

步骤 9 单击**下一步**。此时会出现**配置设备 - 设置系统日期和时间**窗口。

步骤 10 选择所在的时区，然后自动从 NTP 服务器设置系统时间或手动设置。有关这些选项的说明，请参阅时间，第 17 页。

步骤 11 单击**下一步**。此时会出现**配置设备 - 设置密码**窗口。

步骤 12 输入**新密码**，然后在**确认密码**字段中再次输入新密码。

注释 取消选中**密码复杂性**复选框可禁用密码安全规则。但是，思科强烈建议启用密码安全规则。有关密码的详情，请参阅 安全，第 31 页。

步骤 13 单击**下一步**。此时会出现“配置无线 1 - 为您的无线网络命名”窗口。

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**。此时会出现“配置无线 1 - 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，请参阅配置安全设置，第 47 页。

步骤 17 单击“下一步”。此时会出现“配置无线 1 - 为您的无线网络指定 VLAN ID”窗口。

步骤 18 为在无线网络中接收的流量选择 **VLAN ID**。

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

步骤 19 单击**下一步**。重复步骤 13 至步骤 18，配置无线 2 接口的设置。

步骤 20 单击**下一步**。此时会出现“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**下一步**。

如果单击**否**，则跳至步骤 29。

如果单击**是**，则会出现“启用网页认证 - 为您的访客网络命名”窗口。

步骤 22 指定**访客网络名称**。

步骤 23 单击**下一步**。此时会出现“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，请参阅配置安全设置，第 47 页。

步骤 25 单击**下一步**。此时会出现“启用网页认证 - 指定 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**。此时会出现“**启用网页**认证 - 启用重定向 URL”窗口。

步骤 28 选中**启用重定向 URL**，然后在**重定向 URL** 字段（包括 http://）中输入完全限定域名 (FQDN) 或 IP 地址。如果指定，系统会在身份验证后将访客网络用户重定向到指定的 URL。

步骤 29 单击**下一步**。此时会出现“摘要 - 确认您的设置”窗口。

步骤 30 检查已配置的设置。单击**返回**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**。您的设置已保存并出现确认窗口。

步骤 32 单击**完成**。

WAP 设备已成功配置。您需要使用新密码重新进行登录。

使用移动版无线接入点设置向导

首次使用便携式设备登录无线接入点（或将其重置为出厂默认设置）后，系统将显示移动版“无线接入点设置向导”以帮助执行初始配置。要使用向导配置无线接入点，请完成以下步骤：

注释 在出厂默认模式下，默认 SSID 为 **CiscoSB-Setup**。将您的便携式设备关联到具有该 SSID 且使用预共享密钥 **cisco123** 的无线接入点。启动浏览器，输入任意 IP 地址或域名。屏幕上将显示包含登录字段的网页。输入如下默认用户名和密码：**cisco**。单击**登录**。屏幕上将显示**无线接入点设置向导**。

步骤 1 在向导的**欢迎**页面上点击**下一步**。系统将显示**配置 IP 地址**窗口。

步骤 2 使用默认配置“动态 (DHCP)”（推荐）从 DHCP 服务器接收 IP 地址，或者点击**静态**手动配置 IP 地址。有关这些字段的说明，请参阅 **IPv4 配置**。

步骤 3 点击**下一步**。系统将显示**配置集群配置**窗口。

步骤 4 点击**跳过**。转到第 6 步。

步骤 5 要加入现有集群，请输入集群组名，然后单击**下一步**。屏幕上将显示包含集群信息的摘要页面。确认显示的数据，然后单击**提交**。

注释 如需创建新集群，请单击**创建**并输入集群名称，然后转至步骤 6。

步骤 6 在**配置设备 - 设置密码**窗口中输入新密码，然后在**确认密码**字段中重新输入该密码。

步骤 7 点击**下一步**。系统将显示**配置您的无线网络**窗口。

a) 输入用作默认无线网络的 SSID 的网络名称。

b) 输入安全密钥（默认的安全类型为“WPA2 个人 - AES”）

c) 输入要从无线网络接收流量的 VLAN ID。

注释 选中复选框以将相同的配置应用于 Radio 2，或者切换到另一个无线电选项卡并再次重复步骤 7 以进行配置。

步骤 8 点击**下一步**。系统将显示**设置网页认证**窗口。

步骤 9 点击**跳过**。转到第 12 步。

步骤 10 点击**是**。系统将显示**网页认证配置**窗口。

步骤 11 选择**无线电 1 (5 GHz)** 或**无线电 2 (2.4 GHz)**。

a) 指定访客网络名称。

b) 输入安全密钥（默认的安全类型为“WPA2 个人 - AES”）

c) 为访客网络指定 VLAN ID。

d) （可选）您可以使用完全限定域名 (FQDN) 指定重定向 URL，以便将通过验证的用户重定向到指定的 URL。

步骤 12 点击**下一步**。系统将显示**摘要**窗口

步骤 13 检查配置好的设置。点击**返回**可重新配置一项或多项设置。

步骤 14 确保数据正确无误，然后点击**提**交进行保存。

步骤 15 WAP 设备将成功完成配置。您需要使用新的密码重新登录。

更改密码

出于安全方面的考虑，您需要定期更改管理密码。当密码过期时间结束时，您将需要访问此页面。

默认情况下，系统会启用密码复杂性设置，“更改密码”页上会显示最低密码复杂性要求。新密码必须符合默认复杂性规则，或者可以禁用**密码复杂性**来暂时禁用该规则。有关详细信息，请参阅 安全，第 31 页。

要更改默认密码，请配置以下几项：

- **用户名** - 输入新的用户名。默认用户名为 cisco。

- **旧密码** - 输入当前密码（默认值为 cisco）。
- **新密码** - 输入新密码。
- **确认密码** - 再次输入新密码进行确认。
- **密码强度计** - 显示新密码的强度。
- **密码复杂性** - 默认情况下，系统会启用密码复杂性，并要求新密码符合以下复杂性设置：
  - 不同于用户名。
  - 不同于当前密码。
  - 最小长度为 8 个字符。
  - 包含至少三个字符类别的字符（大写字母、小写字母、数字和标准键盘上可用的特殊字符）。

注释 选中**禁用**可禁用密码复杂性规则。但是，强烈建议您启用密码复杂性规则。

TCP/UDP 服务

TCP/UDP 服务表显示在 WAP 上运行的协议和服务。

- **服务** - 服务名称。
- **协议** - 服务使用的底层传输协议（TCP 或 UDP）。
- **本地 IP 地址** - 连接设备的本地 IP 地址。“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** - 本地端口号。
- **远程 IP 地址** - 使用此服务的远程主机的 IP 地址。“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，此表仅显示状态为“活动”或“已建立”的连接。TCP 状态包括：
  - **正在监听** - 此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** - 已在 WAP 设备与服务器或客户端之间建立连接会话。
  - **等待时间** - 关闭序列已启动，WAP 设备在关闭连接之前等待系统定义的超时时间（通常为 60 秒）。

注释 可以修改或重新排列 TCP/UDP 服务表上的顺序。单击**刷新**可刷新屏幕并显示最新信息。

您还可以输入与服务、协议和其他详细信息相关的参数，以过滤显示的 TCP/UDP 服务。

单击**返回**可返回**使用入门**页。

系统状态

“系统状态”页显示硬件型号说明、软件版本和各种配置参数，如：

- **PID VID** - WAP 设备的硬件型号和版本。
- **序列号** - WAP 设备的序列号。
- **主机名** - 分配给 WAP 设备的主机名。
- **MAC 地址** - WAP 设备的 MAC 地址。
- **IPv4 地址** - WAP 设备的 IP 地址。
- **IPv6 地址** - WAP 设备的 IPv6 地址。
- **ETH0/PD 端口** - 显示以太网接口的状态。
- **ETH1 端口** - 显示 ETH1 接口的状态。
- **无线 1 (5GHz)** - 无线 1 接口启用或禁用 5GHz 模式。
- **无线 2 (2.4GHz)** - 无线 2 接口启用或禁用 2.4GHz 模式。
- **电源** - 系统可以通过电源适配器供电或通过以太网 (PoE) 接收供电，其中以太网供电包括来自供电设备 (PSE) 的 802.3.af 和 802.3at 的两个供电模式。

  当电源不足 (802.3af) 时，WAP 设备保留以下配置信息。

  - 禁用 Radio1(5GHZ)。
  - Radio2(2.4GHZ) 天线从 3x3 切换成 2x2，发射功率降至 18dBm。
  - ETH0/PD 端口的速度降至 1Gbps。
  - 关闭 ETH1 端口。

- **系统运行时间** - 自上次重启后的运行时间。
- **系统时间** - 当前系统时间。
- **固件版本（活动映像）** - 活动映像的固件版本。
- **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。

- **固件 MD5 校验和（非活动）** - 备份映像的校验和。

快速入门配置

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**页是启动时的默认窗口。

类别	链接名称（在页面上）	链接的页面
快速访问	设置向导	使用无线接入点设置向导，第 2 页
	更改帐户密码	添加用户，第 23 页
	备份/恢复配置	配置文件，第 107 页
	升级设备固件	固件，第 105 页
高级配置	无线设置	无线电，第 39 页
	管理设置	管理，第 24 页
	配置集群配置	为集群设置配置 WAP 设备，第 70 页
	局域网设置	IPv4 配置，第 11 页
	访客接入	访客接入，第 89 页
更多信息	控制面板	控制面板
	TCP/UDP 服务	TCP/UDP 服务，第 6 页
	查看系统日志	LED 显示，第 18 页
	流量统计信息	流量统计信息，第 100 页

有关设备的其他信息，可以通过以下方式访问产品支持页面或思科支持社区：

- 单击**支持**可访问产品支持页面。
- 单击**论坛**可访问思科支持社区页面。
- 点击**关于 FindIT 的详细信息**查看关于 FindIT 实用程序的信息。
- 点击**下载 FindIT** 下载 FindIT 实用程序。

窗口导航

使用导航按钮围绕 WAP 的图形用户界面移动。

配置实用程序页眉

配置实用程序页眉包含标准信息，在每页的顶部显示。页眉提供以下按钮：

按钮名称	说明
（用户）	登录 WAP 设备的用户帐户名称（Administrator 或 Guest）。出厂默认用户名为 **cisco**。
（语言）	将鼠标指针悬停在此按钮上，然后选择语言。出厂默认语言为英语。
	单击此按钮可注销配置实用程序。
	单击此按钮可显示 WAP 设备类型和版本号。
	单击此按钮可显示情境相关的在线帮助。可以使用UTF-8编码通过浏览器查看在线帮助。如果在线帮助显示乱码，请确认浏览器中的编码设置是否设置为 UTF-8。

导航窗格

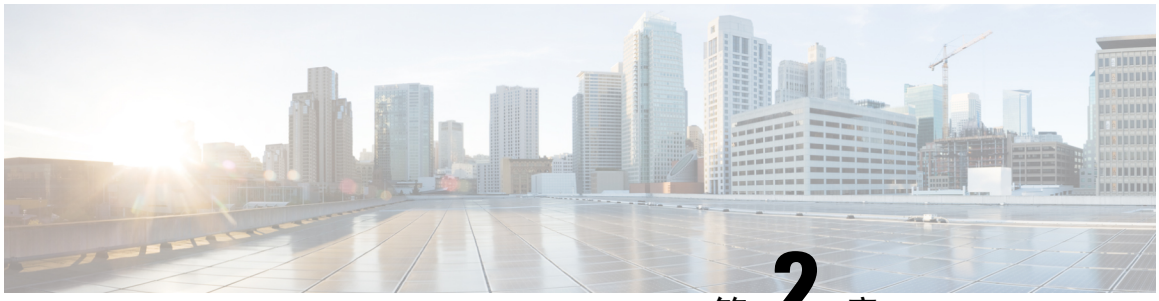
导航窗格或主菜单位于每个页面的左侧。导航窗格是 WAP 设备顶层功能的列表。如果主菜单项前面有一个箭头，选中此箭头可展开并显示每组子菜单。然后可以选择所需的子菜单项以打开关联页。

管理按钮

下表介绍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。
删除	删除表中的条目。
编辑	编辑现有条目。
刷新	用最新数据刷新当前页。

保存	保存设置或配置。
更新	将新信息更新到启动配置中。



第 2 章

系统配置

本章介绍如何配置全局系统设置和执行诊断。具体包括以下主题：

局域网

本节介绍如何在 WAP 设备上配置端口、VLAN、LLDP、IPv4 和 IPv6 设置。

IPv4 配置

使用“IPv4 设置”页配置 IPv4 地址。

步骤 1 依次选择**局域网 > IPv4 配置**。

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 (172.17.144.170) 的格式。

- **静态 IP 地址、子网掩码和默认网关** - 输入静态 IP 地址、子网掩码和默认网关。
- **域名服务器** - 选择以下选项之一：
  - **动态** - WAP 设备从局域网的 DHCP 服务器获取 DNS 服务器地址。

- **手动** - 在提供的字段中最多输入两个 IP 地址。

步骤 3 单击**保存**保存更改。

DHCP 自动配置设置

- **DHCP 自动配置选项** - 默认情况下，启用此选项。如果无线接入点使用的是出厂默认设置，则它会首先尝试使用 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，系统不会为用户提供任何服务。
  - 在经过“等待间隔”或配置文件完成 TFTP 上传后（以先到者为准），“DHCP 自动配置选项”会自动变为禁用状态。
  - 如果禁用 DHCP 客户端（即使用静态 IP 地址进行配置）或禁用“DHCP 自动配置选项”，自动配置过程会立即中止。

  DHCP 客户端会自动广播对 DHCP 选项 66 和 67 的请求。如果 DHCP 和“DHCP 自动配置选项”已启用，无线接入点在下次重启时，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。

注释 用户/思科上传的配置会覆盖自动配置，以确保用户/思科选择的配置文件具有更高优先级。如果在任何其他情况下重启无线接入点（如固件升级/重启操作），系统都将使用现有自动配置设置。

- **TFTP 服务器 IPv4 地址/主机名** - 如果配置 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。输入 IPv4 地址或主机名信息。如果使用主机名格式，则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。

- **配置文件名** - 如果指定配置文件名，而启动文件名不是从 DHCP 服务器收到的，那么无线接入点会在自动配置过程中从 TFTP 服务器检索指定的配置文件。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，则文件扩展名必须为 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。

- **等待间隔** - 如果已配置此设置，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服务。如果 TFTP 事务在此指定间隔内未完成初始化，则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。

- **状态日志** - 此字段用于显示自动配置完成或中止的原因。

IPv6 配置

使用“IPv6 设置”页配置 IPv6 地址，步骤如下：

步骤 1 依次选择**局域网 > IPv6 配置**。

步骤 2 配置以下参数：

- **IPv6 连接类型** - 选择以下选项之一：
  - **DHCPv6** - IPv6 地址由 DHCPv6 服务器指定。
  - **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。
- **IPv6 管理模式** - 选中**启用**启用 IPv6 管理模式。
- **IPv6 自动配置管理模式** - 选中**启用**启用 IPv6 自动地址配置功能。

  如果启用 IPv6 自动地址配置功能，WAP 设备会通过处理局域网端口接收的路由器通告识别其 IPv6 地址和网关。WAP 设备可拥有多个自动配置的 IPv6 地址。
- **静态 IPv6 地址** - 输入静态 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** - 输入静态地址的前缀长度，前缀长度为 0 至 128 之间的整数。默认值为 0。
- **静态 IPv6 地址状态** - 选择以下选项之一：
  - **运行** - IP 地址经验证为唯一地址，且可在局域网接口上使用。
  - **暂定** - 分配静态 IP 地址时，WAP 设备会自动启动重复地址检测 (DAD) 进程。此 IPv6 地址在网络上进行验证期间是暂定地址，不能用于传输或接收流量。
  - **空白（无值）** - 未分配 IP 地址。
- **IPv6 自动配置全局地址** - 列出已自动分配给设备的 IPv6 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** - 选择以下选项之一：
  - **动态** - 通过 DHCPv6 动态识别 DNS 服务器。
  - **手动** - 手动指定最多两个 IPv6 DNS 服务器。

端口设置

使用“端口设置表”查看和配置将 WAP 设备连接到局域网的端口的设置。

步骤 1 依次选择**局域网** > **更多** > **端口设置表**。

端口设置表显示局域网接口的以下状态和配置：

- **链路汇聚** - 启用链路汇聚组 (LAG)。
- **LAG 模式** - 包括以下选项：
  - **标准 LAG** - 如果两个以太网接口的协商速度不一致，则暂停后面的插件。
  - **BW 第一** - 如果两个以太网接口的协商速度不一致，则暂停速度较慢的接口。
  - **冗余和功率第一** - 将两个以太网接口的速度调整为相同速度以进行绑定。此为默认模式。

注释 WAP581 支持静态 LAG，不支持 LACP。确保 LAG 可用于 WAP581 设备。这有助于用户将 LAG 从默认模式切换为其他模式。

端口设置表包括接口（局域网）的以下状态和配置：

- **接口** - 指定局域网的接口
- **链路状态** - 显示当前端口链路状态。
- **端口速度** - 在查看模式中，会列出当前端口速度。在编辑模式中，如果“自动协商”已禁用，请选择一种端口速度，如 100 Mbps 或 10 Mbps。“自动协商”已启用时，仅支持 1000 Mbps 速度。
- **双工模式** - 在查看模式中，会列出当前端口的双工模式。在编辑模式中，如果“自动协商”已禁用，请选择**半双工**或**全双工**模式。
- **自动协商** - 如果已启用，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。如果已禁用，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。绿色以太网模式仅在端口启用自定协商时工作。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。

步骤 2 单击**保存**。

生成树协议

在“生成树协议”模式下，选中**启用**复选框以在思科 WAP 设备上启用 STP 模式。启用后，STP 可以帮助阻止交换环路。如果配置 WDS 链路，建议使用 STP。

VLAN 设置

使用“VLAN 配置”页查看和配置 VLAN 设置。

步骤 1 依次选择**局域网 > 更多 > VLAN 设置表**。

步骤 2 配置以下参数：

- **未标记 VLAN ID** - 对于未标记 VLAN ID，指定一个 1 至 4094 之间的数字。默认值为 1。在此字段中指定的 VLAN 上的流量在转发到网络时，不使用 VLAN ID 进行标记。
- **说明** - 相关 VLAN 的说明。
- **管理 VLAN** - 管理 VLAN 是用于通过 Telnet 或 Web GUI 访问设备的 VLAN。必须只有一个 VLAN 作为管理 VLAN。如果未将任何接口（有线或无线）分配到管理 VLAN，用户将没有能用于访问配置实用程序的接口。
- **VLAN** - 从下拉列表中选择（**未标记或已标记**）VLAN。

  默认情况下，WAP 设备上的所有流量都使用 VLAN 1（默认的未标记 VLAN）。这意味着在禁用未标记虚拟局域网、更改未标记流量 VLAN ID、使用 RADIUS 更改 VAP 或客户端的 VLAN ID 之前，不对任何流量进行标记。

步骤 3 单击**保存**。更改将保存到“启动配置”。

邻居发现

通过 Bonjour，可以使用组播域名服务器 (mDNS) 发现 WAP 设备及其服务。Bonjour 可向网络通告服务并对支持的服务类型进行查询答复，从而简化您业务环境中的网络配置。

WAP 设备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，客户端可以发现思科 WAP 设备以及网络中部署的其他产品。
- **管理用户接口** - 此服务可识别 WAP 设备中可用的管理接口（HTTP 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一个选项卡。

注释 系统管理员可以使用最新的 Internet Explorer 插件（思科 FindIT 工具）查看已启用 Bonjour 的 WAP。在 Bonjour 发现流程后，集群中的所有 WAP 设备在集群名称下显示。管理员应确保集群名称在网络中是唯一的。

Bonjour 在 IPv4 和 IPv6 中均可工作。

要通过 Bonjour 发现 WAP 设备，请执行以下步骤：

步骤 1 依次选择**局域网 > 邻居发现**。

步骤 2 选中**启用**启用 Bonjour。

步骤 3 单击**保存**。更改将保存到“启动配置”。

LLDP

链路层发现协议 (LLDP) 由 IEEE 802.1AB 标准定义，并允许 UAP 通告其系统名称、系统功能和电源要求。此信息可帮助识别系统拓扑并检测局域网中的不良配置。该无线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。

步骤 1 要配置 LLDP 设置，请依次选择**局域网 > LLDP**。

步骤 2 配置以下参数：

- **LLDP 模式** - 选中**启用**启用 LLDP。启用后，无线接入点会将 LLDP 协议数据单元发送给相邻设备。
- **传输间隔** - 传输每个 LLDP 消息之间间隔的秒数。有效范围为 5 至 32768 秒。默认值为 30 秒。
- **POE 优先级** - 从下拉列表中选择优先级（**严重**、**高**、**低或未知**）。当供电设备 (PSE) 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。

步骤 3 单击**保存**。

IPv6 隧道

WAP 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 路由器会将 IPv6 数据包封装到 IPv4 数据包中。

- **ISATAP 状态** - 选中**启用**可在设备上启用 ISATAP。
- **支持 ISATAP 的主机** - 输入 ISATAP 路由器的 IP 地址或 DNS 名称。默认值为 isatap。

- **ISATAP 查询间隔** - 输入 WAP 设备应向 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。有效范围为 120 至 3600 秒。默认值为 120 秒。
- **ISATAP 请求间隔** - 输入 WAP 设备应向 ISATAP 路由器发送路由器请求消息的频率。WAP 设备仅在没有活动 ISATAP 路由器时发送路由器请求消息。有效范围为 120 至 3600 秒。默认值为 120 秒。
- **ISATAP 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。
- **ISATAP 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。

注释 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”字段。这些是虚拟 IPv6 接口地址。

单击**保存**。

时间

系统时钟为消息日志提供网络同步的时间戳服务。系统时钟可以手动配置，也可以配置为从服务器获取时钟数据的网络时间协议 (NTP) 客户端。

使用“时间设置”页可手动或从预配置的 NTP 服务器配置系统时间。默认情况下，WAP 设备会配置为从预定义的 NTP 服务器列表获取其时间。

页面顶部会显示当前系统时间和**系统时钟源**选项。

自动通过 NTP 获取时间设置

要自动从 NTP 服务器获取时间设置，请按照以下步骤操作：

步骤 1 依次选择**系统配置 > 时间**。

步骤 2 在“系统时钟源”区域中，单击**网络时间协议 (NTP)**。

步骤 3 配置以下参数：

- **NTP 服务器（1 至 4）** - 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。
- **进行夏令时时间调整** - 选中以启用和配置以下字段：
  - **开始** - 选择夏令时开始的星期、日、月和时间。

- **结束** - 选择夏令时结束的星期、日、月和时间。
- **夏令时补偿** - 指定在夏令时开始和结束时时钟向前/向后拨动的分钟数。

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 依次选择**系统配置 > 时间**。
步骤 2 在“系统时钟源”区域中，选择**手动**。
步骤 3 单击**与 PC 同步时间**，从本地 PC 复制系统时间设置。
步骤 4 还可以配置以下字段：

- **系统日期** - 从下拉列表中选择当前年、月、日。
- **系统时间** - 选择当前的小时和分钟（24 小时制）。
- **时区** - 选择所在位置的时区。
- **进行夏令时时间调整** - 选中以启用和配置以下字段：
  - **开始** - 选择夏令时开始的星期、日、月和时间。
  - **结束** - 选择夏令时结束的星期、日、月和时间。
  - **夏令时补偿** - 指定在夏令时开始和结束时时钟向前/向后拨动的分钟数。

步骤 5 单击**保存**。更改将保存到“启动配置”。

注释 单击**与 PC 同步时间**，设备的系统时间将与 PC 相同。

通知

本节详细介绍启用和配置无线接入点通知的过程。

LED 显示

WAP 设备有两种类型的 LED：系统 LED 和以太网 LED。使用“LED 显示”页配置所有 LED。

要配置 LED 显示，请执行以下操作：

步骤 1 依次选择**通知 > LED 显示**。

步骤 2 选择**启用**启用 LED。选择**禁用**禁用 LED。选择**关联调度程序**并转到步骤 3。

步骤 3 从“关联调度程序LED显示”的下拉列表中选择配置文件名称。默认情况下，LED未关联任何配置文件。下拉选项中会显示在**无线 > 调度程序**页中配置的已配置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**。

日志设置

使用“日志设置”页将日志消息保存在永久内存中。也可以将日志发送到远程主机。

如果系统意外重启，则日志消息可用于诊断原因。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耗尽闪存（非易失性内存），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

步骤 1 依次选择**通知 > 日志设置**。

步骤 2 配置以下参数：

- **永久** - 选中**启用**将系统日志保存到非易失性内存中，以便在 WAP 设备重启时保留日志。最多可以保存 1000 条日志消息。达到 1000 条的限制时，最新的日志消息会覆盖最早的日志消息。清除此字段可将系统日志保存到易失性内存。系统重新启动时会删除易失性内存中的日志。
- **严重性** - 从用于过滤将保存在非易失性内存中的事件消息的下拉列表中选择严重性（**紧急**、**警报**、**严重**、**错误**、**警告**、**通知**、**信息或调试**）。所有其他消息都将保存在易失性内存中。
- **深度** - 输入可以存储在易失性内存中的最大消息数（最多为 1000 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。

步骤 3 单击**保存**。

远程日志服务器

内核日志是一个全面的系统事件（显示在“系统日志”中）和内核消息列表。

无法直接从配置实用程序查看内核日志消息。必须先设置远程日志服务器，才能接收和捕获日志。然后，可以配置 WAP 设备，以登录远程日志服务器。WAP 设备最多支持两台远程日志服务器。

系统日志消息的远程日志服务器集合提供以下功能：

- 允许从多个无线接入点集合系统日志消息。
- 存储消息历史记录的时间长于单个 WAP 设备。
- 触发脚本管理操作和警报。

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 依次选择**通知 > 日志设置**。

步骤 2 在“远程日志服务器表”中配置以下参数：

- **服务器 IPv4/IPv6 地址/名称** - 输入远程日志服务器的 IPv4 地址、IPv6 地址或主机名。

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

- **启用** - 选中**启用**启用远程日志服务器。然后，定义日志严重性和 UDP 端口。
- **日志严重性** - 选中事件必须将其发送到远程日志服务器的严重性。
- **UDP 端口** - 输入远程主机上系统日志进程的逻辑端口号。范围为 1 至 65535。默认端口为 514。

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

步骤 3 单击**保存**。更改将保存到“启动配置”。

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

如果已禁用远程日志服务器，单击**保存**可禁用远程日志记录。

查看系统日志

“查看系统日志”页显示设备上发生的系统事件的列表。系统会在重新启动时清除日志，也可以由管理员清除日志。最多可以显示1000个事件。根据需要从列表中删除较早的条目，为新事件释放空间。

要查看系统日志，请依次选择**通知 > 查看系统日志**。

系统将显示以下信息：

- **时间戳** - 事件发生时的系统时间。
- **严重性** - 事件的严重性级别。

- **服务** - 与事件关联的服务。
- **说明** - 事件说明。

可以过滤或重新排列“查看系统日志”中的设置。

单击**刷新**可刷新屏幕并显示最新信息。

单击**全部清除**可清除日志中的所有条目。

单击**下载**可下载日志中的所有条目。

邮件警报/邮件服务器/邮件配置

邮件警报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邮件警报的邮件地址。使用“邮件警报”页，可在发生特殊系统事件时将消息发送到已配置的邮件地址。

提示 请勿使用个人邮件地址。这会不必要地暴露个人邮件登录凭证。请使用单独的邮件帐户。另外，请注意，默认情况下，许多邮件帐户保留发送的所有邮件的副本。任何有权访问此邮件帐户的人都可以访问发送的邮件。查看邮件设置以确保其符合您的隐私策略。

要配置 WAP 设备以发送邮件警报，请执行以下步骤：

步骤 1 依次选择**通知 > 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** - 选中**启用**启用邮件警报功能。
- **邮件发件人地址** - 输入要显示为邮件发件人的邮件地址。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** - 输入发送预定邮件的频率（以分钟为单位）。范围为 30 至 1440 分钟。默认值为 30 分钟。
- **预定邮件严重性** - 从下拉列表中选择严重性（**紧急**、**警报**、**严重**、**错误**或**警告**），事件必须以“日志持续时间”指定的频率将其发送到配置的邮件地址。默认严重性为**警告**。
- **紧急邮件严重性** - 从下拉列表中选择严重性（**紧急**、**警报**、**严重**、**错误**、**警告**、**通知**、**信息或调试**），事件必须立即将其发送到配置的邮件地址。默认严重性为**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** - 输入出站 SMTP 服务器的 IP 地址或主机名。服务器地址必须是有效的 IPv4 地址或主机名。IPv4 地址应采用类似于 xxx.xxx.xxx.xxx (192.0.2.10) 的格式。

  主机名可以包含一个或多个标签，每个标签最多由 63 个字母数字字符组成。如果主机名包含多个标签，可用句点 (.) 分隔标签。整个标签和句点字串的长度不能超过 253 个字符。
- **数据加密** - 从出站邮件警报的下拉列表中选择安全模式（**无加密或 TLSv1**）。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** - 输入用于出站邮件的 SMTP 端口号。范围是从 0 至 65535 的有效端口号。默认端口为 465。
- **用户名** - 输入将用于发送这些邮件的邮件帐户的用户名。通常（但不一定），用户名是包含域的完整邮件地址（如 Name@example.com）。指定帐户将用作发件人的邮件地址。用户名可以包含 1 至 64 个字母数字字符。
- **密码** - 输入将用于发送邮件的邮件帐户的密码。密码可以包含 1 至 64 个字符。

步骤 4 在“邮件配置”区域中，配置邮件地址和主题行：

- **收件人邮件地址 1/2/3** - 最多可输入 3 个用于接收邮件警报的地址。每个邮件地址都必须为有效地址。
- **邮件主题** - 输入在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**保存**。

邮件警报示例

以下示例显示“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
```

以下示例显示常规日志邮件的样例格式。

```
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          Priority > Process 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
```

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**

使用“用户帐户”页最多可配置 4 个其他用户，并且可以更改用户密码。

添加用户

配置以下设置以添加新用户：

步骤 1 依次选择**系统配置 > 用户帐户**。

用户帐户表显示当前已配置的用户。用户 cisco 是在系统中预先配置的，具有读/写权限。

所有其他用户可以拥有只读访问权限，但没有读/写访问权限。

步骤 2 单击 添加新行。

步骤 3 选中新用户的复选框，并为新用户输入用户名。

步骤 4 输入“新密码”（0 至 127 个字符），然后在“确认新密码”字段中输入相同密码。

“密钥强度计”字段指示密码强度，如下所示：

- **红色** - 密码不满足最低复杂性要求。
- **橙色** - 密码满足最低复杂性要求，但密码强度较弱。
- **绿色** - 密码强度较强。

步骤 5 单击**保存**。

注释 要删除用户，请选择用户名并单击**删除**。要编辑现有用户，请选择用户名并单击**编辑**，然后单击**保存**以保存对配置所做的所有更改。

更改用户密码

要更改用户密码，请执行以下步骤：

步骤 1 依次选择**系统配置 > 用户帐户**。

用户帐户表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**（0 至 127 个字符），然后在**确认新密码**字段中输入相同密码。

“密钥强度计”指示密码强度，如下所示：

- **红色** - 密码不满足最低复杂性要求。
- **橙色** - 密码满足最低复杂性要求，但密码强度较弱。
- **绿色** - 密码强度较强。

步骤 4 单击**保存**。更改将保存到“启动配置”。

注释 如果更改密码，必须重新登录系统。

管理

使用“系统设置”页配置标识网络中 WAP 设备的信息。

要配置系统设置，请执行以下步骤：

步骤 1 依次选择**系统配置 > 管理**。

步骤 2 配置以下参数：

- **主机名** - 输入 WAP 设备的主机名。默认情况下，此名称是节点的完全限定域名 (FQDN)。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。其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 至 63 个字符。
- **系统联系人** - 输入 WAP 设备的联系人。系统联系人的长度为 0 至 255 个字符，可以包含空格和特殊字符。
- **系统位置** - 输入 WAP 设备的物理位置。系统位置的长度为 0 至 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”。

连接会话设置/HTTP/HTTPS 服务任务

使用“HTTP/HTTPS 服务”页可启用和配置基于 Web 的管理连接。如果对安全管理会话使用 HTTPS，还可以使用此页管理所需的 SSL 证书。

要配置 HTTP 和 HTTPS 服务，请执行以下步骤：

步骤 1 依次选择**系统配置 > 管理**。

步骤 2 在“全局设置”区域中配置以下参数：

- **最大会话数** - 输入可以同时使用的 Web 会话数，包括 HTTP 和 HTTPS。

  当用户登录 WAP 的配置实用程序时，系统会创建一个会话。在用户注销或会话超时过期之前此会话会一直保留。范围为 1 至 10 个会话。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** - 输入非活动用户保持登录的最长时间（以分钟为单位）。当达到配置的超时时间时，用户将自动注销。范围为 2 至 60 分钟。默认值为 10 分钟。

步骤 3 配置 HTTP 和 HTTPS 服务：

- **HTTP 服务器** - 启用或禁用通过 HTTP 的访问。默认情况下，HTTP 访问处于禁用状态。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** - 输入用于 HTTP 连接的逻辑端口号，范围为 1025 至 65535。HTTP 连接的默认端口号是已知 IANA 端口号 80。
  - **将 HTTP 重定向到 HTTPS** - 将 HTTP 端口上的管理 HTTP 访问尝试重定向到 HTTPS 端口。此字段仅在禁用 HTTP 访问时可用。
- **HTTPS 服务器** - 启用或禁用通过安全 HTTP (HTTPS) 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** - 输入用于 HTTPS 连接的逻辑端口号，范围为 1025 至 65535。HTTPS 连接的默认端口号是 IANA 端口号 443。
- **管理 ACL 模式** - 如果此模式已启用，则只能通过 Web 和 SNMP 访问指定 IP 主机。如果禁用此功能，任何人通过提供正确的 WAP 设备用户名和密码，都可以从任一网络客户端访问配置实用程序。

  注释 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，将失去对配置接口的访问权限。建议您为管理计算机指定一个静态 IP 地址，这样地址就不会随着时间而改变。

步骤 4 单击**保存**。

SSL 证书文件状态

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。

在“生成 SSL 证书”区域中，单击 **SSL 设置**，然后单击**生成**以生成 WAP 设备的证书。此程序应在 WAP 设备获取 IP 地址后完成，这样可以确保证书的公用名与 WAP 设备的 IP 地址匹配。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“SSL 证书文件状态”区域中，可以查看 WAP 设备上的当前证书。系统将显示以下内容：

- 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），可以将其下载到计算机上进行备份。在**传输 SSL 证书**（设备到 PC）区域中，选择 **HTTP/HTTPS** 或 **TFTP** 作为下载选项，然后单击**传输**。

- 如果选择 **HTTP/HTTPS**，请确认下载，然后浏览在网络中保存此文件的位置。
- 如果选择 TFTP，请输入为下载文件指定的文件名，以及要下载文件的 TFTP 服务器 IPv4 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**传输 SSL 证书**（PC 到设备）区域中，选择 **HTTP/HTTPS** 或 **TFTP** 作为上传选项，然后单击**传输**。

- 如果选择 HTTP/HTTPS，请浏览网络位置，选择文件，然后单击**传输**。
- 如果选择 TFTP，请输入“文件名”和“TFTP 服务器 IPv4 地址”，然后单击**传输**。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。

上传成功时系统会显示确认消息。

SNMP/SNMPv2c 设置

SNMP 定义用于记录、存储和共享网络设备相关信息的标准。SNMP 有助于网络管理、故障排除和维护。WAP 支持 SNMP，并且可以作为 SNMP 受管设备无缝集成到网络管理系统中。

使用“SNMP/SNMPv2c 设置”页启用 SNMP 并配置基本协议设置。

要配置通用 SNMP 设置，请执行以下步骤：

步骤 1 依次选择**管理 > SNMP 设置**。

步骤 2 选中**启用**启用 SNMP。

步骤 3 输入用于 SNMP 流量的 UDP 端口。默认值为 161。但是，可以进行配置，以便代理监听不同端口上的请求。有效范围为 1025 至 65535。

步骤 4 在“SNMPv2c 设置”区域中配置 SNMPv2c 设置：

- **只读社区** - 输入用于 SNMPv2 访问的只读社区名称。有效范围为 1 至 256 个字母数字和特殊字符。

  社区名称可以用作简单身份验证功能，限制网络中可以从 SNMP 代理请求数据的设备。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** - 输入用于 SNMP 设置请求的读写社区名称。有效范围为 1 至 256 个字母数字和特殊字符。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** - 所有工作站都可以通过 SNMP 访问 WAP 设备。
  - **用户定义** - 允许的用户定义 SNMP 请求集。

- **NMS IPv4 地址/名称** - 输入网络管理系统 (NMS) 的 IPv4 IP 地址、DNS 主机名或子网。

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

和社区名称一样，此设置也可提供有关 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，请以地址/掩码长度的形式输入一个或多个子网地址范围，其中地址是 IP 地址，掩码长度是掩码位数。地址/掩码和地址/掩码长度两种格式均受支持。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。

- **NMS IPv6 地址/名称** - 可以对受管设备执行、获取和设置请求的设备的 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。

注释　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。

步骤 5 在“SNMPv2c 陷阱设置”区域中配置 SNMPv2c 陷阱设置：

- **陷阱社区** - 输入与 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。有效范围为 1 至 60 个字母数字和特殊字符。
- **陷阱目标表** - 输入最多包含 3 个用于接收 SNMP 陷阱的 IP 地址或主机名的列表。选中此框，然后选择主机 IP 地址类型（IPv4 或 IPv6），最后添加主机名/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。您最多可以拥有 3 个 DNS 主机名。请确保选中**已启用**复选框，然后选择合适的主机 IP 地址类型。

步骤 6 单击**保存**。

SNMPv3 视图

SNMP MIB 视图是 MIB 分级结构中的视图子树系列。视图子树是通过位串掩码值的对象标识符 (OID) 子树值配对标识的。每个 MIB 视图是通过两组视图子树定义的，这些视图子树可包含在此 MIB 视图中或从 MIB 视图中排除。可以创建 MIB 视图以控制 SNMPv3 用户可以访问的 OID 范围。

WAP 设备最多支持 16 个视图。

本节总结了 SNMPv3 视图配置的关键准则。请在继续操作前阅读所有注释。

注释　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。

注释　默认情况下，view-all 和 view-none SNMPv3 视图在 WAP 设备中创建。这些视图无法删除或修改。

要添加和配置 SNMP 视图，请执行以下操作：

步骤 1 依次选择**管理** > **SNMPv3**

步骤 2 单击 以在 **SNMPv3 视图**表中创建一个新行，或选中现有视图的复选框，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 .1.3.6.1.2.1.1 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 3 单击**保存**。

注释 要删除视图，请在列表中选中相应视图，然后单击**删除**。

SNMPv3 组

通过 SNMPv3 组，可以将用户组合到具有不同授权和访问权限的组中。每组都与以下 3 个安全级别之一关联：

- noAuthNoPriv
- authNoPriv
- authPriv

通过将 MIB 视图关联到读取或写入访问权限组，可以分别控制对每组 MIB 的访问权限。

默认情况下，WAP 设备包含以下两组：

- **RO** - 使用身份验证和数据加密的只读组。此组中的用户使用 SHA 密钥或密码进行身份验证，并使用 DES 或 AES128 进行加密。必须定义 SHA、DES 和 AES128 密钥。默认情况下，此组的用户对默认的所有 MIB 视图具有读取访问权限。
- **RW** - 使用身份验证和数据加密的读/写组。此组中的用户使用 SHA 密钥或密码进行身份验证，并使用 DES 密钥或 AES128 进行加密。必须定义 SHA、DES 和 AES128 密钥。默认情况下，此组的用户对默认的所有 MIB 视图具有读写访问权限。

注释 不能删除默认组 RO 和 RW。WAP 设备最多支持 8 个组。

要添加和配置 SNMP 组，请按照以下步骤操作：

步骤 1 依次选择**管理 > SNMPv3**。

步骤 2 单击 将新行添加到 SNMPv3 组表。

步骤 3 选中新组的复选框，并配置以下参数

- **组名称** - 输入组的名称。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。
- **安全级别** - 从以下选项中选择组的安全级别：
  - **noAuthNoPriv** - 无身份验证和数据加密（无安全性）。
  - **authNoPriv** - 有身份验证，但无数据加密。使用此安全级别，用户可以发送使用 SHA 密钥或密码的 SNMP 消息进行身份验证，但不使用 DES 密钥或 AES128 进行加密。
  - **authPriv** - 有身份验证和数据加密。使用此安全级别，用户可以发送 SHA 密钥或密码进行身份验证并使用 DES 或 AES128 进行加密。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 SHA、DES 和 AES128 密钥或密码。
- **写入视图** - 从以下选项之一选择组的 MIB 的写入访问权限：
  - **view-all** - 此组可以创建、更改和删除 MIB。
  - **view-none** - 此组不能创建、更改或删除 MIB。
- **读取视图** - 从以下选项之一选择对组的 MIB 的读取访问权限：
  - **view-all** - 允许此组查看和读取所有 MIB。
  - **view-none** - 此组不能查看或读取 MIB。

步骤 4 单击**保存**将组添加到 SNMPv3 组表。

注释 要删除组，请在列表中选中相应组，然后单击**删除**。要编辑组，请在列表中选中相应组，然后单击**编辑**。

SNMPv3 用户

使用“SNMP 用户”页可定义用户、将安全级别关联到每个用户，以及为每个用户配置安全密钥。

可以从预定义或用户定义的组中将每个用户映射到 SNMPv3 组，（可选）还可以针对每个用户配置身份验证和加密。身份验证中仅支持 SHA 类型。对于加密，仅支持 DES 和 AES128 类型。WAP 设备中没有默认的 SNMPv3 用户，最多可以添加 8 个用户。

要添加 SNMP 用户，请执行以下步骤：

步骤 1 依次选择**管理 > SNMPv3**。

步骤 2 单击 将新行添加到 SNMPv3 用户表。

步骤 3 选中新行中的复选框，并配置以下参数：

- **用户名** - 输入用于标识 SNMPv3 用户的名字。用户名最多可包含 32 个字母数字字符。
- **组** - 输入要将用户映射到的组。默认组为 RW 和 RO。可以在“SNMP 组”页定义其他组。
- **身份验证类型** - 从以下选项中选择要用于来自用户的 SNMPv3 请求的身份验证类型：
  - **SHA** - 要求对来自此用户的 SNMP 请求进行 SHA 身份验证。
  - **无** - 不需要对来自此用户的 SNMPv3 请求进行身份验证。
- **身份验证密码** - 如果将 SHA 指定为身份验证类型，请输入密码，以使 SNMP 代理能够对此用户发送的请求进行身份验证。密码的长度必须为 8 至 32 个字符。
- **加密类型** - 从以下选项中选择应用于用户 SNMP 请求的加密/隐私类型：
  - **DES** - 对来自用户的 SNMPv3 请求使用 DES 加密。
  - **AES128** - 对来自用户的 SNMPv3 请求使用 AES128 加密。
  - **无** - 来自此用户的 SNMPv3 请求不需要隐私。
- **加密密码** - 如果将 DES 或 AES128 指定为加密类型，请输入用于对 SNMP 请求进行加密的密码。密码的长度必须为 8 至 32 个字符。

步骤 4 单击**保存**。系统将用户添加到 SNMPv3 用户列表中，并将所做更改保存到“启动配置”。

注释 要删除用户，请在列表中选择相应用户，然后单击**删除**。要编辑用户，请在列表中选择相应用户，然后单击**编辑**。

SNMPv3 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。

注释 SNMPv3 用户配置（请参阅 SNMPv3 用户页）应在配置 SNMPv3 目标之前完成。

WAP 设备最多支持 8 个目标。

要添加 SNMP 目标，请执行以下步骤：

步骤 1 依次选择**管理 > SNMPv3 目标**。

步骤 2 单击 将新行添加到表。

步骤 3 选中新行中的复选框，并配置以下参数：

- **IP 地址** - 输入用于接收目标的远程 SNMP 管理器的 IPv4 或 IPv6 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SNMPv3 用户 ， 第 29 页页。

步骤 4 单击**保存**。系统将用户添加到 SNMPv3 目标列表中，并将所做更改保存到“启动配置”。

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

安全

本节介绍如何在 WAP 设备上配置安全设置。

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，在无线接入点上配置虚拟无线接入点 (VAP) 时，可以配置用于控制无线客户端访问的安全方法。有关详细信息，请参阅无线电。“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，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，其他服务器则可以用作备份服务器。

注释 除了使用全局 RADIUS 服务器，还可以配置每个 VAP 以使用特定的 RADIUS 服务器组。请参阅网络。

配置全局 RADIUS 服务器

步骤 1 依次选择**安全** > **Radius 服务器**

步骤 2 配置以下参数：

- **服务器 IP 地址类型** - 选择 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** - 输入主全局 RADIUS 服务器的地址。第一个无线客户端尝试通过 WAP 设备进行身份验证时，WAP 设备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 或服务器 IPv6 地址 2** - 输入备份 IPv4 或 IPv6 RADIUS 服务器的地址。如果主服务器身份验证失败，则系统会尝试使用配置的备份服务器。
- **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。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** - 输入与已配置备份 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。
- **启用 RADIUS 帐务** - 用于对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量等。如果启用 RADIUS 记帐，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。

步骤 3 单击**保存**。

802.1x 请求方

通过 IEEE 802.1X 身份验证，WAP 设备可以获取对安全有线网络的访问权限。可以将此 WAP 设备作为有线网络中的 802.1X 请求方（客户端）。可配置使用 MD5 算法加密的用户名和密码，以允许 WAP 设备使用 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 验证方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。

要配置 802.1X 请求方设置，请按照以下步骤操作：

步骤 1 依次单击**安全 > 802.1X 请求方**。

步骤 2 在“802.1x 请求方”区域中，选中**启用**启用管理模式。

步骤 3 配置 802.1X 操作状态和基本设置：

- **EAP 方法** - 选择用于加密身份验证用户名和密码的算法。选项如下：
  - **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，可通过将其封装在 TLS 隧道内提供高于 MD5 的安全级别。
  - **TLS** - RFC 5216 中定义的传输层安全性，是可以提供高级别安全性的开放标准。

- **用户名** - 输入用户名。
- **密码** - 输入密码。

步骤 4 在“证书文件上传”区域中，可以将证书文件上传到 WAP 设备：

a) 选择 **HTTP** 或 **TFTP** 作为传输方式。
b) 如果选择 HTTP，请单击**浏览**选择文件。有关配置 HTTP 服务器设置的详细信息，请参阅连接会话设置/HTTP/HTTPS 服务任务。
c) 如果选择 **TFTP**，请输入文件名和 TFTP 服务器 IPv4 地址。
d) 单击**上传**。系统会显示一个确认窗口，后跟一个指示上传状态的进度条。

步骤 5 单击**保存**。

恶意无线接入点检测

恶意无线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无线接入点。恶意无线接入点存在安全威胁，因为进入网络的任何人会无意或恶意安装廉价的无线 WAP 设备，未经授权的用户可能会借此访问网络。

WAP 设备对所有信道执行射频扫描，以检测网络附近的所有无线接入点。如果检测到恶意无线接入点，系统会将其显示在“恶意无线接入点检测”页上。如果列为恶意的无线接入点是合法的，可以将其添加到“已知无线接入点列表”中。

注释 “已检测到的恶意无线接入点列表”和“受信任的无线接入点列表”可提供信息。无线接入点无法对列表中的无线接入点进行任何控制，也不能对通过射频扫描检测到的无线接入点应用任何安全策略。

如果启用恶意无线接入点检测，无线会定期从其工作信道切换以扫描同一频段内的其他信道。

查看恶意无线接入点列表

为了使恶意无线接入点检测功能正常工作，必须启用无线功能。对无线接口启用恶意无线接入点检测之前，应先启用无线接口。

要启用无线以收集有关恶意无线接入点的信息，请执行以下步骤：

步骤 1 依次选择**安全 > 恶意无线接入点检测**。
步骤 2 选中**启用**启用无线 1 和无线 2 的无线接入点检测。
步骤 3 单击**保存**。

“检测到的恶意无线接入点列表”表显示所有检测到的恶意无线接入点。“受信任的无线接入点列表”显示所有受信任的无线接入点。每个列表或恶意无线接入点列表显示以下设置：

- **MAC 地址** - 恶意无线接入点的 MAC 地址。
- **信标间隔** - 恶意无线接入点使用的信标间隔。信标帧由无线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。信标间隔在无线电，第 39 页页上设置。
- **类型** - 设备的类型。选项如下：
  - **无线接入点** - 在基础设施模式下支持 IEEE 802.11 无线网络架构的无线接入点恶意设备。
  - **临时** - 在临时模式下运行的恶意工作站。临时模式是 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)。
- **隐私** - 指示恶意设备上是否存在任何安全性。选项如下：
  - **关闭** - 安全模式关闭（无安全性）。
  - **开启** - 安全模式开启。
- **WPA** - 显示恶意无线接入点的 WPA 安全性处于开启还是关闭状态。
- **频段** - 恶意无线接入点上使用的 IEEE 802.11 模式，例如 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g。

  显示的数字表示相应的模式：
  - 2.4 表示 IEEE 802.11b、802.11g 或 802.11n 模式（或这些模式的组合）。
  - 5 表示 IEEE 802.11a 或 802.11n 模式（或这两种模式）。
- **信道** - 当前广播恶意无线接入点的信道。
- **速率** - 当前传输恶意无线接入点的速率（兆位/秒）。当前速率始终都是“支持的速率”字段中所示的速率之一。
- **信号** - 从恶意无线接入点发出的无线信号的强度。如果将鼠标指针悬停在这些条上，会出现用分贝 (dB) 表示强度的数字。
- **信标** - 自首次发现信标后从恶意无线接入点接收的信标总数。
- **上一个信标** - 从恶意无线接入点接收的上一个信标的日期和时间。
- **速率** - 恶意无线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。会列出所有支持速率，其中基本速率以粗体显示。速率集在无线电，第 39 页页中配置。

步骤 4 选中“无线接入点列表”，然后单击**移至受信任的无线接入点列表**，以将无线接入点移至**受信任的无线接入点列表**。如果无线接入点位于**受信任的无线接入点列表**中，请单击**检测到的恶意无线接入点列表**，以将该无线接入点移至**检测到的恶意无线接入点列表**。

步骤 5 单击**刷新**可刷新屏幕并显示最新信息。

保存受信任的无线接入点列表

要创建受信任的无线接入点列表并将其保存到文件中，请执行以下步骤：

步骤 1 选择**安全**，然后单击**恶意无线接入点检测**部分中的**查看恶意无线接入点列表...**。系统将显示**恶意无线接入点检测**页。

步骤 2 在**检测到的恶意无线接入点列表**中，对已知无线接入点单击**移至受信任的无线接入点列表**。受信任的无线接入点会移到受信任的无线接入点列表中。

步骤 3 在“下载/备份受信任的 AP 列表”区域中，选择**备份（从无线接入点到 PC**）。

步骤 4 单击**保存**。

列表包含已添加到已知无线接入点列表中的所有无线接入点的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。

导入受信任的无线接入点列表

可从保存的列表中导入已知无线接入点列表。该列表可以从其他无线接入点获取或从文本文件创建。如果接入点的 MAC 地址出现在受信任的无线接入点列表中，则系统不会将其检测为恶意接入点。

要从文件导入无线接入点列表，请执行以下步骤：

步骤 1 依次选择**安全 > 恶意无线接入点检测**。

步骤 2 在“下载/备份受信任的无线接入点列表”区域中，单击**下载（PC 到无线接入点**）。

步骤 3 在“源文件名”字段中，单击**浏览**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。各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 4 在“文件管理目标”字段中，选择是替换现有受信任的无线接入点列表还是将导入文件中的条目添加到受信任的无线接入点列表中。选项如下：

- **替换** - 导入列表并替换已知无线接入点列表的内容。
- **合并** - 导入列表并将导入文件中的无线接入点添加到已知无线接入点列表中当前显示的无线接入点。

步骤 5 单击**保存**。

导入完成后，系统刷新屏幕，并在已知无线接入点列表中显示导入文件中无线接入点的 MAC 地址。

配置密码复杂性

使用“密码复杂性”页修改用于访问配置实用程序的密码的复杂性要求。复杂密码可以提高安全性。

要配置密码复杂性要求，请按照以下步骤操作：

步骤 1 依次选择**安全 > 配置密码复杂性**。

步骤 2 选中**启用**启用密码复杂性。

步骤 3 配置以下参数：

- **密码最小字符类** - 输入必须在密码字符串中出现的最小字符类数。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** - 选中此项可使用户在当前密码过期后输入不同的密码。如果不选中，用户可以在密码到期时重新输入相同的密码。
- **最大密码长度** - 最大密码字符长度范围为 64 至 127。默认值为 64。
- **最小密码长度** - 最小密码字符长度范围为 0 至 32。默认值为 8。
- **密码过期支持** - 选中此项可使密码在配置的时间段后过期。
- **密码过期时间** - 输入新创建密码的有效期天数，范围为 1 至 365。默认值为 180 天。

步骤 4 单击**保存**。更改将保存到“启动配置”。

注释 **密码过期时间**结束时，您将需要访问更改密码页。

配置 WAP-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 预共享密钥或 WPA-PSK）作为安全方法，则可以在“WPA-PSK 复杂性”页上配置要在身份验证过程中使用的复杂性要求。较复杂的密钥可以提高安全性。

要配置 WPA-PSK 复杂性，请执行以下步骤：

步骤 1 依次选择**安全 > 配置 WPA-PSK 复杂性**。

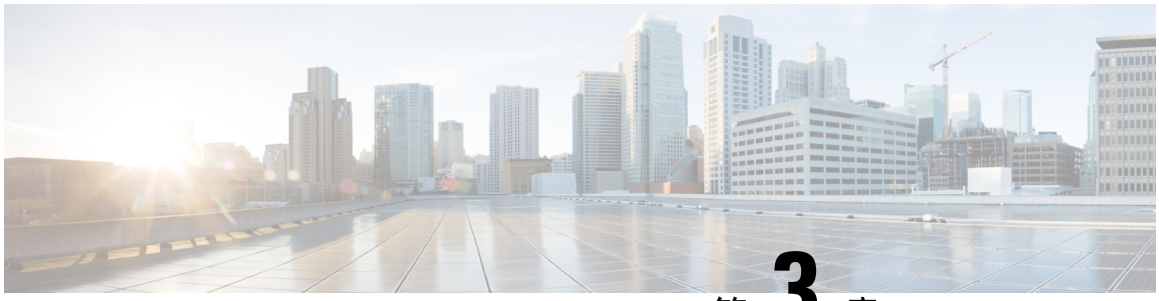
步骤 2 选中**启用**可使 WAP 设备根据配置的条件检查 WPA-PSK 密钥。如果禁用，则不使用任何配置的设置。默认情况下，系统会禁用“WPA-PSK 复杂性”。

步骤 3 配置以下参数：

- **WPA-PSK 最小字符类** - 选择必须在密钥字符串中出现的最小字符类数。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** - 选中**启用**可使用户在其当前密钥过期后配置不同的密钥。如果禁用，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** - 输入密钥长度值。最大密钥长度为 32 至 63 个字符。默认值为 63。
- **最小 WPA-PSK 长度** - 输入密钥长度值。最小密钥长度为 8 至 16 个字符。默认值为 8。

步骤 4 单击**保存**。



第 3 章

无线

本章介绍如何配置无线功能属性。具体包括以下主题：

无线电

无线电是创建无线网络的 WAP 的物理部分。WAP 上的无线设置控制无线的行为并确定 WAP 发出的无线信号的种类。

要配置无线功能设置，请执行以下步骤：

步骤 1 依次选择**无线 > 无线电**。

步骤 2 选择工作模式：

- **无线 1 (5G)** - 支持具有 4x4 MIMO 模式的 5G 无线。
- **无线 2 (2.4 G)** - 支持具有 3x3 MIMO 模式的 2.4G 无线。

步骤 3 在**每个接口的无线设置**区域中，选择要应用配置参数的无线接口。

步骤 4 在**基本设置**区域中，为所选无线接口配置以下参数：

注释 当地法规可能会禁止使用某些无线模式。某些模式在部分国家/地区不可用。

- **无线电** - 选中**启用**启用无线接口。
- **无线网络模式** - 无线使用的 IEEE 802.11 标准和频率。无线 2 的模式默认值是 802.11b/g/n，无线 1 的模式默认值是 802.11a/n/ac。请为每个无线选择一个可用的模式。

  无线 2 (2.4G) 支持以下无线模式：

- **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。
- **2.4 GHz 802.11n** - 仅以 2.4 GHz 频率运行的 802.11n 客户端可以连接到 WAP 设备。

无线 1 (5G) 支持以下无线模式：

- **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

- **无线频段选择**（**仅限 802.11n 和 802.11ac 模式**） - 802.11n 规范除允许使用传统 20 MHz 频段，也允许将共存的 20/40 MHz 频段用于其他模式。20/40 MHz 频段可提高数据速率，但会减少可用于其他 2.4GHz 和 5GHz 设备的频段。

  802.11ac 规范除了允许使用 20 MHz 和 40 MHz 频段，也允许使用 80 MHz 宽频段。

  将该字段设置为 20 MHz，以将无线频段选择的使用限制为 20 MHz 频段。对于 802.11ac 模式，将该字段设置为 40 MHz，以防止无线使用 80 MHz 无线频段选择。

- **主要频道**（**仅使用 20/40 MHz 带宽的 802.11n 模式**） - 可以将 40 MHz 频道视为由频率域中两个相邻的 20 MHz 频道组成。通常，将这两个 20MHz 频道分别称为主要频道和次要频道。主要频道用于传统客户端和仅支持 20MHz 频道带宽的 802.11n 客户端。

  请选择以下选项之一：

  - **高频** - 将主要频道设置为 40 MHz 频段中大于 20 MHz 频道。
  - **低频** - 将主要频道设置为 40 MHz 频段中小于 20 MHz 频道。默认选择“低频”。

- **信道** - 无线用于发送和接收的无线频谱部分。

  可用信道的范围由无线接口的模式和国家/地区代码的设置决定。如果选择“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。

- **调度程序** - 对于无线接口，请从列表中选择配置文件。

步骤 5 在**高级设置**区域中，配置以下参数：

- **DFS 支持** - 此字段仅在所选无线模式以 5GHz 频率运行时可用。

  对于在 5 GHz 频段中运行的无线，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 机制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，具体取决于无线接入点的国家/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。
- 如果无线接入点在启用 802.11h 的域中运行，则无线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无线接入点在信道中检测到雷达，则无线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，无线接入点在 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 链路中两个无线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。如果两个无线接入点在同一信道中运行，仅 WDS 可以正常工作。有关 WDS 的更多信息，请参阅“WDS 网桥”。

- **支持短保护间隔** - 仅当选定的无线模式包括 802.11n 时，此字段才可用。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。此项为默认选择。
  - **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），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。当模式为 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。

  注释 此设置不影响客户端与 WAP 设备进行关联的能力。

- **信标间隔** - 信标帧传输间隔。WAP 设备按规定的时间间隔发送这些信标帧，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 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 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。

  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等待接收的缓存数据。

  以信标为测量单位。例如，如果将其设置为 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。如果将其设置为 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 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。

默认情况下，分片功能是关闭的。除非怀疑存在无线电干扰，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。有效整数范围必须为 0 至 65535。默认值为 65535 个八位字节。

  RTS 阈值表示 MPDU 中的八位字节数，低于此阈值将不执行 RTS/CTS 握手。

  更改 RTS 阈值有助于通过 WAP 设备控制流量。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。

- **最大关联客户端数** - 允许在任何时间访问 WAP 设备的最大工作站数。可输入一个 0 至 200 之间的整数。默认值为 200 个工作站。

- **发射功率** - WAP 设备的发射功率电平的百分比值。

  默认值全功率 100% 可以向 WAP 设备提供最大的广播范围并减少所需的无线接入点数，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。此设置有助于减少无线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，中功率 25% 或低功率 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性能。

- **发送时间公平性模式** - 实施发送时间公平性 (ATF) 功能，以解决较慢数据传输限制较高速率数据传输的问题。

- **最大利用率阈值** - 输入在 WAP 设备禁止新客户端关联之前无线中允许的网络带宽利用百分比。有效整数范围为 0□ 至 100%。默认值为 0□。如果设置为 0，无论利用率为多少，都将允许所有新的关联。

- **固定组播速度** - 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。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无线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/组播速度限制** - 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，此功能处于禁用状态。在您启用此功能之前，以下字段处于禁用状态：

  - **速率限制** - 组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。

- **频谱分析模式** - 频谱分析模式状态可以是以下模式之一：
  - **专用频谱分析仪** - 在专用模式下，无线有超过 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。
  - **混合频谱分析仪** - 在混合模式下，客户端连接得到保证，但预期会整体降级。
  - **3+1 频谱分析** - 在 3+1 模式下，客户端连接到 3x3 链，而对 1x1 链进行频谱分析。
  - **已禁用** - 默认值为“已禁用”。
- **VHT 功能** - 此功能的目的是在 Broadcom 到 Broadcom 链接的 VHT 中启用/禁用 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）。802.11 ac PHY 支持 VHT 功能。

步骤 6 单击**配置 TSPEC**，并配置以下参数：

- **TSPEC 违规间隔** - 在“TSPEC 违规间隔”字段中，输入 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。输入一个 0 至 900 秒之间的时间。默认值为 300 秒。
- **TSPEC 模式** - 控制 WAP 设备中的整体 TSPEC 模式。默认情况下，TSPEC 模式是关闭的。选项如下：
  - **开启** - WAP 设备根据“无线”页中配置的 TSPEC 设置处理 TSPEC 请求。
  - **关闭** - WAP 设备忽略来自客户端工作站的 TSPEC 请求。
- **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** - 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** - 工作站可以发送和接收优先的语音流量，而无需使用经允许的 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** - 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** - 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 无线接入点不活动超时值** - 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。有效整数范围为 0 至 120 秒，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。有效整数范围为 0 至 120 秒，默认值为 30 秒。
- **TSPEC 传统 WMM 队列映射模式** - 选中“启用”以启用队列中作为 ACM 运行的混合传统流量。默认情况下，此模式是关闭的。

步骤 7 单击**确定**，然后单击**保存**。

网络

虚拟无线接入点 (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 设备中模拟多个无线接入点。此思科 WAP 设备最多支持四个 VAP。

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

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

允许使用的字符包括：

- 从 0x20 至 0x7E 的 ASCII 字符。
- 不允许使用结尾和前导空格 (ASCII 0x20)。

注释 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。此思科 WAP 设备支持 9 个活动虚拟局域网（其中 8 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 依次选择**无线 > 网络**。

步骤 2 在“无线电”字段中，单击应用 VAP 配置参数的无线接口（**无线 1** 或**无线 2**）。

步骤 3 如果 VAP0 是系统中配置的唯一 VAP，并且要添加 VAP，请单击 。然后，选中要添加的 VAP。

步骤 4 配置以下参数：

- **VLAN ID** - 指定要与 VAP 关联的 VLAN 的 VLAN ID。

  务必输入在网络中正确配置的 VLAN ID。如果 VAP 将无线客户端与配置不正确的 VLAN 相关联，则会造成网络问题。

  当无线客户端通过使用此 VAP 连接到 WAP 设备时，WAP 设备使用已配置 VLAN 标记来自无线客户端的所有流量，除非输入端口 VLAN ID 或使用 RADIUS 服务器将无线客户端分配给 VLAN。VLAN ID 的范围为 1 至 4094。

  如果将 VLAN ID 更改为与当前管理 VLAN ID 不同的 ID，则与此特定 VAP 关联的无线局域网客户端无法管理设备。可在 LAN 页验证非标记和管理 VLAN ID 的配置。有关详细信息，请参阅 IPv4 配置，第 11 页。

- **SSID 名称** - 输入无线网络的名称。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。

  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。保存此新设置后，您将需要重新连接到新 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。相反，必须在客户端上的无线连接实用程序中手动输入确切的网络名称，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。

  WMF - 无线组播转发提供一种有效的方法，可在无线设备上传输组播流量，也可以使用重复的单播或组播帧来克服 WLAN 上的组播传输问题。

- **安全性** - 选择访问 VAP 所需的身份验证类型。选项如下：
  - 无
  - 静态 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。有关配置无线安全设置的详细信息，请参阅配置安全设置。

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。

注释　静态 WEP 可用于不支持“WPA 个人”和“WPA 企业”的无线计算机或设备。要使用静态 WEP 设置安全性，请将无线配置为 802.11a 或 802.11b/g 模式。802.11n 模式限制将“静态”用作安全性。

- **客户端过滤器** - 指定是否将可访问此 VAP 的工作站限制为已配置的 MAC 地址全局列表。可以选择以下客户端过滤器类型之一：
  - **已禁用** - 不使用客户端过滤器。
  - **本地** - 使用在“客户端过滤器”页中配置的 MAC 身份验证列表。
  - **RADIUS** - 使用外部 RADIUS 服务器中的 MAC 身份验证列表。
- **信道隔离** - 选中此选项可启用信道隔离。

  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
- **频段切换** - 开启两个无线时，选中此选项可启用频段切换。它通过将支持双频段的客户端从 2.4 频段切换为 5 GHz 频段，有效利用 5 GHz 频段。
  - 其在每个 VAP 上配置，因此需要在两个无线上启用。
  - 不建议将频段切换用于时间敏感型语音或视频流量 VAP 上。
  - 频段切换时不会考虑无线的 802.11n 带宽。即使 5 GHz 无线刚好使用 20 MHz 带宽，无线接入点也会尝试将客户端切换到该无线。
- **调度程序** - 从列表中选择调度程序配置文件，VAP0 不能与调度程序配置文件关联。
- **访客接入实例** - 将 CP 实例与 VAP 相关联。关联的 CP 实例设置应用于尝试在 VAP 中验证身份的用户。为实例所要关联的每个 VAP 选择实例名称。

注释　VAP 可以在**访问控制** > **访客接入**页中与一个访客接入实例相关联。必须先配置**访客接入**实例。

步骤 5 单击**保存**。

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。此时建议更改 WAP 设备设置。

注释　要删除 VAP，请选中 VAP 并单击**删除**。要编辑 VAP，请选中 VAP 并单击**编辑**。要保存更改，请在完成后单击**保存**。

配置安全设置

本节介绍可在“网络”页上的 WAP 设备中配置的安全设置。有三个安全设置选项可供选择，分别为“无”、“WPA 个人”和“WPA 企业”。

无

如果选择**无**作为安全模式，则不需要在设备上进行其他安全设置。此模式表示不对 WAP 设备收发的数据进行加密。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无线接入点以加密数据。

“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。

以下参数可用于配置“静态 WEP”：

- **传输密钥索引** - 输入密钥索引列表。提供从 1 至 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** - 选择 64 位或 128 位作为密钥长度。
- **密钥类型** - 选择 ASCII 或 Hex 作为密钥类型。
- **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（如 @ 和 #）。
  - **十六进制** - 包括 0 至 9 的数字以及 A 至 F 的字母。
- 按照**所需字符数**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。
- **802.1X 身份验证** - 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”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”，则任何客户端都可以与 WAP 设备进行关联。

注释 即使允许关联客户端工作站，也无法确保该客户端工作站可以与 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”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，这样才能对无线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无线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（无线接入点和客户端）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密钥将数据传输至无线接入点。（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密钥对其传输的数据进行加密。这可以确保相邻无线接入点无法对其他无线接入点传输的数据进行解码。
- 无法在无线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。

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 个人”使用预共享密钥 (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”也称为 WPA-PSK。

此安全模式向后兼容支持最初的 WPA 的无线客户端。

要配置“WPA 个人”，请执行以下操作：

- **WPA 版本** - 从以下选项中选择客户端工作站类型：

- **WPA-TKIP** - 此网络具有仅支持原始 WPA 和 TKIP 安全协议的客户端工作站。请注意，根据 Wi-Fi 联盟的最新要求，不允许仅选择 WPA-TKIP。
- **WPA2-AES** - 网络上的所有客户端工作站都支持 WPA2 和 AES-CCMP 加密/安全协议。此版本可依据 IEEE 802.11i 标准提供最佳安全性。根据 Wi-Fi 联盟的最新要求，无线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原始 WPA，则选择两者。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 TKIP 密钥
  - 有效 AES-CCMP 密钥

- **PMF（保护管理帧）** - 为未加密 802.11 管理帧提供安全保障。当“安全模式”处于禁用状态时，PMF 设置为“无 PMF”且不可编辑（隐藏或灰色）。当“安全模式”设置为 WPA2-xxx 时，默认情况下，PMF 有能力且可编辑。它可以配置为以下三个复选框值。
  - **不需要**
  - **有能力**
  - **必需**

  注释 WiFi 联盟要求启用 PMF 并将其设置为“有能力（默认）”。当不兼容无线客户端遇到不稳定或连接问题时，可以将其禁用。

- **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 #）。
- **以明文显示密钥** - 如果启用，将显示键入的文本。如果禁用，输入时不隐藏文本。
- **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，请参阅配置 WAP-PSK 复杂性，第 36 页。
- **广播密钥刷新率** - 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 86400 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，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。

动态 VLAN 模式是默认启用的，它使 RADIUS 身份验证服务器可决定将哪个 VLAN 用于工作站。

以下参数用于配置“WPA 企业”：

- **WPA 版本** - 选择要支持的客户端工作站的类型。选项如下：
  - **WPA-TKIP** - 网络中有一些客户端工作站仅支持原始 WPA 和 TKIP 安全协议。请注意，根据 Wi-Fi 联盟的最新要求，不允许对无线接入点仅选择 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。此版本可依据 IEEE 802.11i 标准提供最佳安全性。根据 Wi-Fi 联盟的最新要求，无线接入点必须始终支持此模式。
- **启用预身份验证** - 如果仅选择 WPA2 或同时选择 WPA 和 WPA2 作为 WPA 版本，则可以对 WPA2 客户端启用预身份验证。

  如果您要 WPA2 无线客户端发送预身份验证数据包，请选中此选项。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无线接入点连接的漫游客户端的身份验证速度。

  如果已为 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 TKIP RADIUS IP 地址和 RADIUS 密钥
  - 有效 CCMP (AES) IP 地址和 RADIUS 密钥
- **PMF**（**保护管理帧**） - 为未加密 802.11 管理帧提供安全保障。当“安全模式”处于禁用状态或为 WEP 时，PMF 设置为**无 PMF** 且不可编辑（隐藏或灰色）。当“安全模式”设置为 **WPA2-xxx** 时，默认情况下，PMF **有能力**且可编辑。它可以配置为以下三个复选框值。
  - **不需要**
  - **有能力**
  - **必需**

  注释 WiFi 联盟要求启用 PMF，且默认设置为**有能力**。当不兼容无线客户端遇到不稳定或连接问题时，可以将其禁用。
- **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。但可以配置每个 VAP 以使用一组不同的 RADIUS 服务器。

  选中此选项可使用全局 RADIUS 服务器设置，取消选中此选项可对 VAP 使用单独的 RADIUS 服务器，并在相应的字段中输入 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。
- **服务器 IP 地址 2 或服务器 IPv6 地址 2** - 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** - 与已配置备份 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。
- **启用 RADIUS 记帐** - 可对特定用户消耗的资源进行跟踪和测量，例如系统时间、发送和接收的数据量等。如果启用 RADIUS 记帐，也会对主 RADIUS 服务器和所有的备份服务器启用此功能。
- **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 86400 秒。有效范围为 0 至 86400 秒。值 0 表示不刷新广播密钥。
- **会话密钥刷新率** - WAP 设备针对与 VAP 关联的每个客户端刷新会话（单播）密钥的间隔。有效范围为 30 至 86400 秒。值 0 表示不刷新会话密钥。

客户端过滤器

客户端过滤器可用于允许或拒绝列出的客户端工作站通过 WAP 设备进行身份验证。MAC 身份验证可在网络，第 44 页页配置。根据 VAP 配置，WAP 设备可能会参照外部 RADIUS 服务器中存储的客户端过滤器列表或在 WAP 设备中本地存储的客户端过滤器列表。

在 WAP 设备上本地配置客户端过滤器列表

WAP 设备仅支持一个本地客户端过滤器列表。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 个客户端地址添加到过滤器列表中。

要配置客户端过滤器，请按照以下步骤操作：

步骤 1 依次选择**无线 > 客户端过滤器**。

步骤 2 选择 WAP 设备使用过滤器列表的方式：

- **允许（只允许列表中的客户端）** - 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。
- **拒绝 (拒绝列表中的所有客户端)** - 仅拒绝列表中显示的工作站通过 WAP 设备访问网络。允许所有其他工作站访问。

注释　过滤器设置也适用于存储在 RADIUS 服务器上的客户端过滤器列表（如果存在）。

步骤 3 在此列表完成前一直输入 MAC 地址。单击 **关联客户端**旁边的箭头，然后它会显示关联客户端列表选择一个 MAC 地址，然后单击 **添加**。一条规则将会添加到 MAC 地址表中。关联客户端列表：

- **MAC 地址** - 关联无线客户端的 MAC 地址。
- **主机名** - 关联无线客户端的主机名。
- **IP 地址** - 关联无线客户端的 IP 地址。
- **网络 (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

步骤 4 单击 **保存**。

在 Radius 服务器上配置 MAC 身份验证

如果配置一个或多个 VAP 以使用客户端过滤器，则必须在 RADIUS 服务器上配置工作站列表。列表格式如下表所述。

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。	无密码

调度程序

无线和 VAP 调度程序可用来配置 VAP 的特定时间间隔规则或要使用的无线。

使用此功能方法是安排要运行的无线或只允许在工作时间访问 VAP，以确保安全并降低功耗。

WAP 设备最多支持 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。

调度程序配置文件配置

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。

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 依次选择**无线 > 调度程序**。

步骤 2 选中**启用**确保已启用“管理模式”。默认情况下，禁用此选项。

“调度程序运行状态”区域指示调度程序的当前运行状态：

- **状态** - 调度程序的运行状态（已启用或已禁用）。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。
  - **禁用管理模式** - 已禁用调度程序管理模式。
  - **系统时间已过时** - 系统时间已过时。
  - **受管模式** - 调度程序处于受管模式。

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。

配置文件规则配置

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以下参数（星期几、小时和分钟）。规则之间不能存在冲突；例如，可以配置一个在每个工作日启动的规则，再配置一个在每个周末启动的规则，但无法配置一个每天启动的规则，再配置一个周末启动的规则。

要配置配置文件规则，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 。

新规则将显示在**配置文件规则表**中。

步骤 3 选中**配置文件名称**前面的复选框，然后单击**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** - 设置启用无线或 VAP 的时间。时间采用 hh:mm 24 小时格式。范围为 <00-23>:<00-59>。默认值为 00:00。
- **结束时间** - 设置禁用无线或 VAP 的时间。时间采用 hh:mm 24 小时格式。范围为 <00-23>:<00-59>。默认值为 00:00。

步骤 6 单击**保存**。

注释 调度程序配置文件必须与无线接口或 VAP 接口关联才会生效。

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**。

QoS

服务质量 (QoS) 设置允许在处理差异化的无线流量时配置传输队列，进而优化吞吐量和增强性能。该流量可以是 VoIP、其他类型的音频、视频、流媒体以及传统的 IP 数据。

要在 WAP 设备上配置 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。

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 的默认值不应更改。更改这些值会影响提供的 QoS。

要配置 WAP 设备和 EDCA 参数，请执行以下步骤：

步骤 1 依次选择**无线 > QoS**。

步骤 2 选择无线接口（**无线 1 或无线 2**）。

步骤 3 从 EDCA 下拉列表中选择以下选项之一：

- **WFA 默认值** - 用 Wi-Fi 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 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、流媒体等时间敏感型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。会将时间敏感型视频数据自动发送到此队列中。
- **数据 2**（**尽力而为**） - 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间不敏感的批量数据（例如 FTP 数据）发送到此队列中。

步骤 4 选中**启用**启用 Wi-Fi 多媒体 (WMM) 扩展。

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

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

步骤 5 配置以下 EDCA 和工作站 EDCA 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 至 255。
- **最小争用窗口** - 输入用于确定重试传输故障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“最大争用窗口”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窗口的值。
- **最大争用窗口** - 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窗口大小之前，此值会一直成倍增加。

  达到最大争用窗口大小后，将一直重试，直至达到允许的最大重试次数。

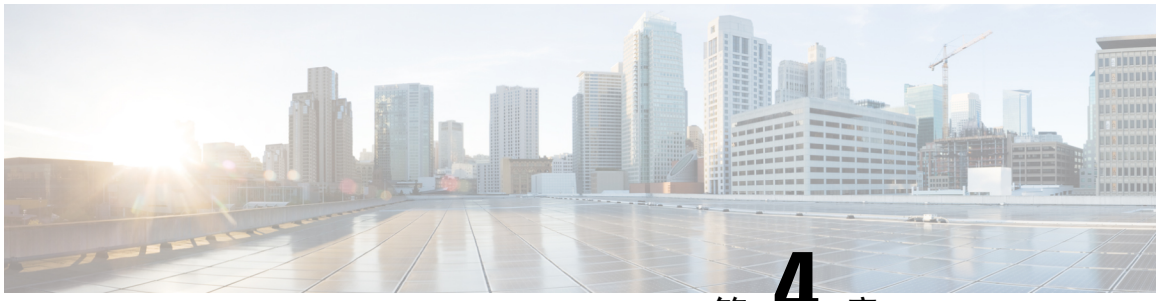
  有效值为 1、3、7、15、31、63、127、255、511 或 1023。此值必须大于最小争用窗口的值。
- **最大突发** - 仅适用于从 WAP 流向客户端工作站的流量的 WAP EDCA 参数。

  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 至 999。
- **TXOP 限制（仅工作站）** - TXOP 限制是一个工作站 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 6 配置以下更多设置：

- **无确认** - 选中**启用**以指定 WAP 设备不应将具有 QosNoAck 的帧确认为服务类别值。
- **非调度自动节能发送 (APSD)** - 选中**启用**启用 APSD。如果 VoIP 电话通过 WAP 设备访问网络，建议使用 APSD。

步骤 7 单击**保存**。



第 4 章

无线网桥

本章介绍如何配置“无线网桥”设置。具体包括以下主题：

无线网桥

无线分布式系统 (WDS) 可用于连接多个 WAP 设备。通过 WDS，WAP 设备可以相互进行无线通信。这可以为漫游客户端和管理多个无线网络提供无缝体验。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 设备可接受客户端关联并与无线客户端进行通信。WAP 设备通过在无线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 设备可用作多个无线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进行通信。所有其他无线接入点仅与中心 WAP 设备关联，然后中心 WAP 设备将数据包转发到相应的无线网桥以进行路由。

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

在 WAP 设备上配置 WDS 之前，请注意以下准则：

- 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：
  - 无线电
  - IEEE 802.11 模式
  - 频道带宽

- 频道（不建议使用“自动”模式）

在 802.11n 2.4 GHz 频段中进行桥接时，将“频道带宽”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 20MHz WAP 设备，工作带宽可以从 40 MHz 更改为 20 MHz。频道带宽不匹配会导致链路断开。

- 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。

配置 WDS 网桥

要配置 WDS 网桥，请执行以下步骤：

步骤 1 选择**无线网桥**。

步骤 2 单击 **WDS** 作为无线网桥模式。

步骤 3 选中**启用**以在 WDS 设置中启用 WDS 端口。

步骤 4 配置其余参数：

- **无线电** - 指定无线 ID（无线 1 [2.4 GHz] 或无线 2 [5GHz]）。
- **本地 MAC 地址** - 指定从其发送数据的当前或本地 WAP 设备的物理或 MAC 地址。
- **远程 MAC 地址** - 指定目标 WAP 设备的 MAC 地址。可以在“监控 > 控制面板 > 无线”页上查找 MAC 地址。
- **加密** - 选择要在 WDS 链路上使用的加密类型（**无**、**静态 WEP** 或 **WPA 个人**）。

  如果不担心 WDS 链路上的安全问题，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“WPA 个人”。在“WPA 个人”模式下，WAP 设备使用 WPA2-PSK 通过 WDS 链路进行 CCMP (AES) 加密。有关加密选项的详细信息，请参阅 WDS 链路中的 WPA/PSK，第 59 页。

步骤 5 最多对 4 个 WDS 接口重复上述步骤。

步骤 6 单击**保存**。

步骤 7 对连接到网桥的设备重复此程序。

注释 可以通过访问**监控** > **控制面板** > **无线**页来验证桥接链路是否开启。在接口状态表中，WDS(x) 状态应为**开启**。

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，请将 WEP 密钥长度指定为 64 位或 128 位。
- **密钥类型** - 如果启用 WEP，请选择 **ASCII** 或**十六进制** 作为 WEP 密钥类型。
- **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**十六进制**，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，所需字符数在此字段右边显示，并根据“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 网桥输入唯一共享密钥。还必须为 WDS 链路另一端的 WAP 设备输入此唯一的共享密钥。如果对于两个 WAP，此密钥不相同，它们之间将不能通信和交换数据。

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

工作组网桥

利用工作组网桥功能，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，WAP 设备可用作无线局域网中的无线工作站 (STA)。它可以在远程有线网络或关联无线客户端与使用工作组网桥模式连接的无线局域网之间桥接流量。

工作组网桥功能同时支持 STA 模式和无线接入点模式运行。WAP 设备可以在一个基本服务集 (BSS) 中作为 STA 设备运行，而在另一个 BSS 中作为 WAP 设备运行。如果启用“工作组网桥”模式，WAP 设备仅支持与其关联的无线客户端的 BSS 且 WAP 设备关联的另一个 BSS 作为无线客户端。

我们建议仅在 WDS 网桥功能无法用于对等 WAP 设备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。WDS 适用于桥接思科 WAP150 和思科 WAP361 设备。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。

注释 在 WAP 设备上启用“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，WAP 设备管理的 BSS 在 WAP 设备模式下运行时称为无线接入点接口，关联的 STA 称为下游 STA。另一个 WAP 设备（即与作为 STA 的 WAP 设备关联的设备）管理的 BSS 称为基础设施客户端接口，而另一个 WAP 设备称为上游无线接入点。

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

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

在 WAP 设备上配置**工作组网桥**之前，请注意以下准则：

- 所有加入工作组网桥的 WAP 设备必须拥有以下相同设置：
  - 无线电
  - IEEE 802.11 模式
  - 频道带宽
  - 频道（不建议使用“自动”模式）

  有关配置这些设置的详情，请参阅无线电，第 39 页（基本设置）。
- “工作组网桥”模式当前仅支持 IPv4 流量。
- 集群设置不支持“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 选择**无线网桥**。

步骤 2 单击**工作组**。

步骤 3 选择要应用配置参数的 WGB 端口。

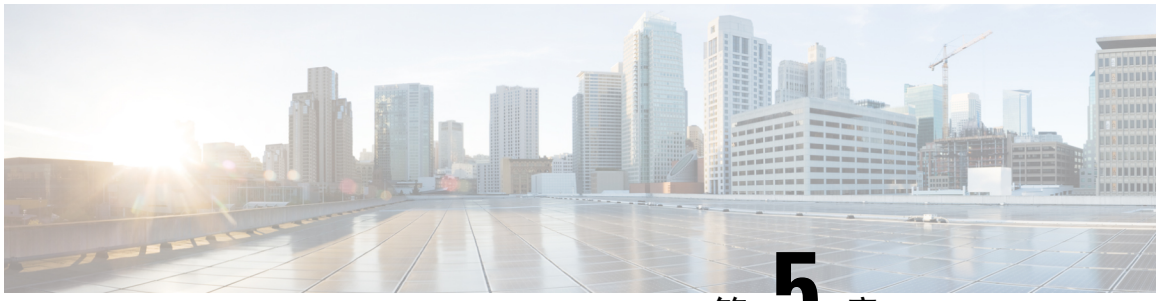
步骤 4 单击**编辑**为基础设施客户端接口（上行链路/下行链路）配置以下参数：

表 *1:* 基础设施客户端接口（上行链路/下行链路）

WGB 端口	**上行链路**	**下行链路**
已启用	选中该复选框以启用基础设施客户端接口。	选中该复选框以启用基础设施客户端接口。
无线电	指定无线 ID（无线 1 [2.4 GHz] 或无线 2 [5GHz]）。	指定无线 ID（无线 1 [2.4 GHz] 或无线 2 [5GHz]）。

WGB 端口	上行链路	下行链路
SSID	指定 BSS 的当前 SSID。 注释 SSID 扫描的 SSID 旁边有一个箭头。此功能在默认情况下禁用，仅在恶意无线接入点检测中的无线接入点检测（该功能在默认情况下也禁用）启用时启用。	无线接入点接口的 SSID 无需与基础设施客户端 SSID 相同。
加密	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。视图可为以下选项之一： • 无 • **静态 WEP** • **WPA 个人** • **WPA 企业**	用于身份验证的安全类型。选项如下： • 无 • **WPA 个人** • **静态 WEP**
连接状态	表示 WAP 是否已连接到上游 WAP 设备。	不适用 (N/A)
VLAN ID	指定与 BSS 关联的 VLAN。	使用与基础设施客户端接口中通告的相同 VLAN ID 配置无线接入点接口。
注释 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，指定一个静态 IP 地址。		
SSID 广播	指定 SSID 的广播是可用、已启用还是已禁用。	如果要广播下游 SSID，请选中此项。默认情况下，启用 SSID 广播。
客户端过滤器	不适用 (N/A)	请选择以下选项之一： • 已禁用 - 可访问上游网络的无线接入点 BSS 中的客户端组并不仅限于 MAC 地址列表中指定的客户端。 • 本地 - 可访问上游网络的无线接入点 BSS 中的客户端组仅限于本地定义的 MAC 地址列表中指定的客户端。 • RADIUS - 可访问上游网络的无线接入点 BSS 中的客户端组仅限于 RADIUS 服务器上的 MAC 地址列表中指定的客户端。
注释 如果选择“本地”或“RADIUS”，请参阅客户端过滤器了解创建客户端过滤器列表的说明。		

步骤 5 单击**保存**。关联的下游客户端现在可连接到上游网络。



第 5 章

快速漫游

本章介绍如何配置“快速漫游”设置。具体包括以下主题：

快速漫游

快速漫游（也称为 IEEE 802.11r 或快速 BSS 转换 [FT]）可以确保每次客户端设备从一个无线接入点漫游到另一个无线接入点时，不需要向 RADIUS 服务器重新进行身份验证，从而使客户端设备能够在实施 WPA2 企业安全性的环境中快速漫游。

快速转换漫游是对 IEEE 802.11 标准的修订，允许移动无线设备上的连续连接，以无缝方式快速安全地从无线接入点切换到其他受管无线接入点。为了确保语音质量和网络安全性，便携工作站必须能够在处理其他流量的无线接入点之间漫游时保持语音呼叫的安全性和低延迟性。

此设备支持 802.11r 中定义的 FBT（快速 BSS 转换），以实现 WPA2 企业安全性的快速切换。基于 WI-FI 企业的语音仅支持 802.11r 中定义的部分功能。快速 BSS 转换可减少漫游期间的延迟。

对每个 VAP 的每个无线都启用 FBT。

注释 在 VAP 上配置 FBT 之前，务必验证 VAP 是否已配置 WPA2 安全性并已禁用预身份验证和 MFP。

配置快速漫游

以下步骤是如何配置快速漫游的概括说明：

步骤 1 依次选择**快速漫游 > 漫游表**。

步骤 2 单击 将新行添加到漫游表。

步骤 3 配置以下参数：

- **启用** - 默认情况下选中此选项。
- **BSSID** - 选择要启用的 VAP（**2.4GVAP 0** 或 **5G VAP 0**）。
- **移动域** - 指定 FBT VAP 的移动域标识符 (MDID)。MDID 用于指示 ESS 内的一组无线接入点，这些无线接入点之间的 STA 可使用快速 BSS 转换服务。只有具有相同 MDID 并且位于相同 ESS 内的无线接入点之间才允许进行快速 BSS 转换。具有不同 MDID 或位于不同 ESS 的无线接入点之间不允许进行快速 BSS 转换。
- **FT 模式** - 快速转换协议允许移动站 (MS) 仅对域中的第一个无线接入点进行完全身份验证（支持 FT 协议的无线接入点组，并通过分发系统 [DS] 连接），并对同一域中的下一个无线接入点使用较短的关联程序。选择以下 FT 方式之一：
  - **通过空气** - 在“通过空气”方式中，移动站通过一个直接 802.11 链路与新无线接入点进行通信。
  - **通过 DS** - 在“通过 DS”方式中，MS 通过旧无线接入点与新无线接入点进行通信。
- **R0 密钥持有者** - 指定要在 Radius 访问请求消息中发送的 NAS 标识符。NAS 标识符用作 R0 密钥持有者 ID。
- **R1 密钥持有者** - 指定在身份验证器中命名 PMK-R1 持有者的 R1 密钥持有者 ID。
- **远程密钥持有者列表** - 从创建的下拉菜单中选择一个远程密钥持有者列表。

步骤 4 单击**保存**。

注释 要删除或修改漫游设置，请选择漫游设置，然后单击**删除**或**编辑**。

配置 FBT 设置后，单击**保存**以保存设置。更改某些设置可能会导致无线接入点停止并重启系统进程。如果出现这种情况，无线客户端将暂时断开连接。我们建议在 WLAN 流量低时更改无线接入点设置。

配置远程密钥持有者列表配置文件

要配置远程 R0 密钥持有者列表配置文件，请执行以下步骤：

步骤 1 依次选择**快速漫游 > 远程密钥持有者列表配置文件**。

步骤 2 单击 添加新配置文件，或单击**编辑**修改现有配置文件。系统将显示**远程密钥持有者列表配置文件**。

步骤 3 指定远程密钥持有者列表配置文件的名称。

步骤 4 配置以下参数。允许每个 VAP 最多配置 10 个条目的 R0 密钥持有者。

- **MAC 地址** - 输入目标的 VAP MAC 地址，即 R0 密钥持有者。系统将 RRB PULL 消息发送到此无线接入点 MAC 地址以获取 PMKR1 密钥。此 MAC 地址在所有 VAP 中必须唯一。
- **NAS ID** - 在启用 VAP 的目标 FBT 上配置的 NAS ID。
- **RRB 密钥** - 用于加密 RRM 协议消息的密钥。

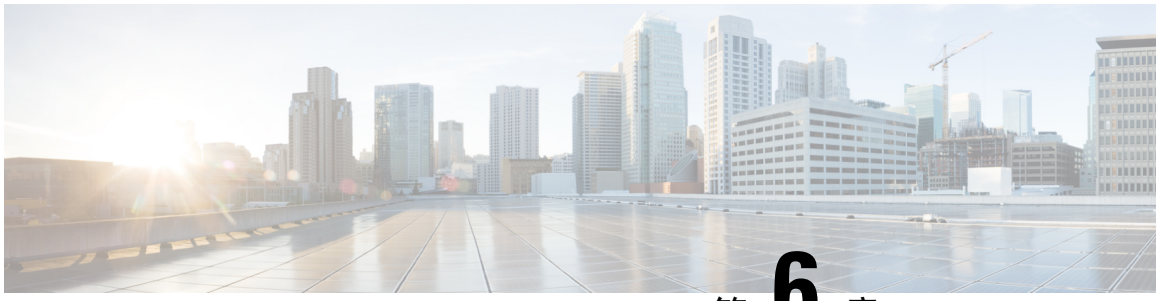
步骤 5 重复步骤 1 到 4，然后在“远程 R1 密钥持有者数据列表”中配置 R1 密钥持有者。允许每个 VAP 最多配置 10 个条目的 R1 密钥持有者。为每个 VAP 配置密钥持有者数据。

- **MAC 地址** - 目标的 VAP MAC 地址，即 R1 密钥持有者。系统在 RRB PUSH 消息中将 PMKR1 发送到此无线接入点 MAC 地址。此 MAC 地址在所有 VAP 中必须唯一。
- **R1 密钥持有者** - 在身份验证器中命名 PMK-R1 持有者的 R1 密钥持有者 ID。
- **RRB 密钥** - 用于加密 RRM 协议消息的密钥。

注释 配置“远程密钥持有者数据列表”设置后，可以单击**恢复**以恢复旧设置，或单击**保存**以保存该设置。单击**取消**可返回之前的**快速漫游**页。

复制或删除配置文件后，单击**保存**。

注意 为所选配置文件单击**导出**只会导出选定的配置文件。单击**导出**而不选择配置文件将**导出**所有配置文件。



第 6 章

集群设置

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：

集群设置概述

集群设置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。可使用集群设置创建无线设备的单个组或集群。WAP 设备集群化后，可以将无线网络作为单个实体进行查看、部署、配置操作并保证安全。创建无线集群后，集群设置还有助于无线服务间的信道规划，从而减少无线电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”配置集群设置或加入现有集群设置。如果不想使用“设置向导”，可以使用基于 Web 的配置实用程序。

管理无线接入点间的集群设置

集群设置在网络的同一子网中创建 WAP 设备的动态、可识别配置的集群或组。一个集群支持最多包含 16 个已配置 WAP581 设备的组，但同一集群中不能包含非 WAP581 型号。

通过集群设置，可以在同一子网或网络中管理多个集群，但这些集群作为单个独立实体进行管理。下表显示集群设置的无线服务限制：

表 *2:* 集群设置无线服务限制

组/集群类型	每个集群设置的 WAP 设备数	每个集群设置的活动客户端数	最大客户端数（活动和空闲）
思科 WAP581	16	960（用于双频 WAP581）	2048（用于双频 WAP581）

集群可以传播配置信息，如 VAP 设置、QoS 队列参数和无线参数。配置设备的集群设置时，如果其他设备加入集群，则将该设备的设置（无论这些设置是手动设置还是默认设置）传播到这些设备。

要组成一个集群，请确保满足以下先决条件或条件：

步骤 1 规划集群设置集群。确保要组成集群的两个或更多 WAP 设备属于同一型号。例如，思科 WAP581 设备只能与其他思科 WAP581 设备组成集群。

注释 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 设备的集群设置。有关详细信息，请参阅无线接入点。

步骤 4 确认所有 WAP 设备都引用相同的集群设置名称。有关详细信息，请参阅无线接入点。

集群设置协商

如果为集群设置启用并配置无线接入点，则无线接入点将每10秒定期发送一次通告来宣布其存在。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设置集群的形成和仲裁：

- 对于现有的集群设置集群，无论何时管理员更新任何集群成员的配置，都会将配置更改传播到所有的集群成员，并且配置的 WAP 设备可控制集群。
- 两个独立的集群设置集群加入一个集群时，则最近修改的集群将赢得配置仲裁，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。
- 如果集群设置模式下的 WAP 设备断开连接，不要立即从集群中将其删除。如果未删除设备，使其重新建立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。）

从集群设置中删除的 WAP 设备的运行

如果以前是集群成员的 WAP 设备断开与集群的连接，则适用以下指导原则：

- 与集群断开连接会阻止 WAP 设备接收最新运行配置设置。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设施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，具体取决于故障性质。

传播和不传播到集群设置无线接入点的配置参数

下表总结了可在组成集群的所有 WAP 设备之间共享和传播的配置：

表 *3:* 传播和不传播的配置参数

在集群设置中传播的通用配置设置和参数	
访问控制	密码复杂性
客户端 QoS	用户帐户
邮件警报	QoS
HTTP/HTTPS 服务（SSL 证书配置除外）	包括 TSPEC 设置的无线设置（部分情况例外）
日志设置	恶意无线接入点检测
客户端过滤器	调度程序
管理访问控制	SNMP 和 SNMPv3
网络	WPA-PSK 复杂性
时间设置	Umbrella
在集群设置中传播的无线配置设置和参数	
无线网络模式	
分片阈值	
RTS 阈值	
速率集	
信道	
保护	
固定组播速度	
广播或组播速度限制	

在集群设置中传播的通用配置设置和参数	
无线频段选择	
支持短保护间隔	
在集群设置中不传播的无线配置设置和参数	
信道	
信标间隔	
DTIM 周期	
最大工作站数	
发射功率	
在集群设置中不传播的其他配置设置和参数	
利用率阈值	端口设置
Bonjour	VLAN 和 IPv4
IPv6 地址	网桥
IPv6 隧道	数据包捕获

无线接入点

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

为集群设置配置 WAP 设备

要配置每个集群设置集群成员的位置和名称，请执行以下步骤：

步骤 1 依次选择**集群设置** > **无线接入点**。

默认情况下，“集群设置”在 WAP 设备中处于禁用状态。单击“启用”按钮，使“集群设置”按钮变为可见。

步骤 2 为每个集群设置集群成员配置以下参数：

- **无线接入点位置** - 输入 WAP 设备物理位置的说明，例如 Reception。此位置字段可选。有效范围为 1 至 64 个字母数字和特殊字符。
- **无线接入点优先级** - 输入基准无线接入点（集群控制器）选择的集群优先级。

- **要加入的集群名称** - 输入 WAP 设备要加入的集群的名称，例如 Reception_Cluster。集群名称不发送给其他 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设置，集群名称必须是唯一的。默认名称为 ciscosb-cluster。有效范围为 1 至 64 个字母数字和特殊字符。

  数字越大表示此无线接入点成为基准无线接入点的优先级越高。如果出现优先级平等的情况，优先级最低的 MAC 将成为基准。范围：0 至 255。默认值为 0。

- **集群 IP 协议** - 选择集群中的 WAP 设备与其他集群成员进行通信所用的 IP 版本。默认值为 IPv4。

- 如果选择 IPv6，集群设置可以使用链路本地地址、自动配置的 IPv6 全局地址和静态配置的 IPv6 全局地址。在使用 IPv6 时，确保集群中的所有 WAP 设备仅使用链路本地地址或仅使用全局地址。

  集群设置仅适用于使用相同类型 IP 寻址的 WAP 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。

该 WAP 设备开始在子网中搜索用相同集群名称和 IP 协议配置的其他 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。

步骤 3 配置集群管理地址：

集群管理地址 - 为了使用单个 IP 访问集群。可以使用集群 IPv4 地址选项配置集群。这是本节集群全局配置的一部分。可以由集群管理员以静态方式进行配置。集群 IP 管理地址应该是与集群无线接入点管理 IP 地址相同的子网的一部分。集群 IP 地址配置为基准无线接入点的管理接口的辅助 IP 地址。可使用集群 IP 地址访问基准无线接入点用户接口。当集群 IP 地址设置为基准 IP 的辅助 IP 地址时，其在管理 VLAN 上发送免费 ARP，以便在子网中建立新 IP 地址与 MAC 地址之间的映射。集群 IP 地址配置在所有集群无线接入点之间共享。

步骤 4 单击**保存**。

步骤 5 对要加入集群设置的其他 WAP 设备重复上述步骤。

固件管理

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

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** - 无线接入点物理位置的说明。
- **IP 地址** - 无线接入点的 IP 地址。
- **MAC 地址** - 无线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** - 无线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是否为无/已启动/已下载/成功/失败/Abort_admin/Abort_local/Dap_resigned。
- **固件传输进度条** - 显示固件下载的进度条。

要选择进行升级的集群成员，请执行以下步骤：

1. 在导航窗格中选择**集群设置** > **固件管理**。
2. 选择要升级的无线接入点的复选框。
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**。

要使用 TFTP 升级集群成员的固件，请执行以下步骤：

1. 选择 TFTP 作为传输方式。
2. 在“源文件名”字段中，输入映像文件的名称（1 至 256 个字符），应包含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。
3. 输入 TFTP 服务器 IPv4 地址，然后单击“开始升级”。

要使用 HTTP 进行升级，请执行以下步骤：

1. 选择 HTTP 作为传输方式。
2. 如果知道新文件的名称和路径，可在“新固件映像”字段中直接输入。

   否则，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。
3. 单击“开始升级”应用新固件映像。

注释 “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/正在进行/已完成/失败/Abort_admin/无）。

要停止从基准无线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”。

信道管理

使用“信道管理”页管理集群设置集群中 WAP 设备的信道。

如果启用信道管理，则 WAP 设备自动分配集群设置集群中的 WAP 设备使用的无线信道。自动信道分配可以减少互相干扰（或集群外的其他 WAP 设备的干扰），最大限度地提高 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，自动信道分配功能处于禁用状态。信道管理的状态（已启用或已禁用）会传播到集群设置集群中的其他设备。

配置高级设置

通过“高级”区域，可以自定义和制定集群设置的信道规划。

默认情况下，每小时自动重新分配一次信道，但仅在干扰可以减少 25% 或更多时执行。即使网络繁忙，也会重新分配信道。

默认设置可以满足需要实施信道管理的大多数情况。

可以通过配置以下设置更改高级设置：

- **更改信道阈值** - 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%。选择从 5% 至 75% 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。

- **重新分配信道间隔** - 计划实施自动更新的时间。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，这意味着系统会重新评估信道的使用情况并每小时应用一次生成的信道规划。

  如果更改这些设置，请单击**保存**。更改将保存到活动配置和“启动配置”。

  启用“自动信道分配”后，页面会显示信道分配表。

信道分配表

信道分配表按 IP 地址列出集群设置集群中的所有 WAP 设备。

该表提供以下有关信道分配的详细信息：

- **AP 位置** - WAP 设备的物理位置。
- **MAC 地址** - 无线的 MAC 地址。
- **IP 地址** - WAP 设备的 IP 地址。
- **无线频段** - WAP 设备进行广播所在的频段。

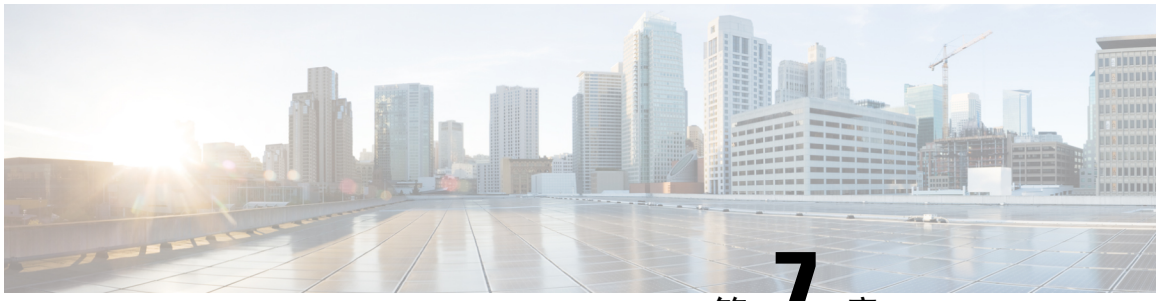
- **开启/关闭** - 显示 WAP 设备中无线功能的状态。部分 WAP 设备可能具有多个无线功能，而每个无线均显示在表中的单独一行中。无线状态是开启（工作）或关闭（不工作）。
- **当前信道** - 此 WAP 设备当前进行广播所在的无线信道。
- **建议信道（xx 小时之前）** - 即如果应用信道规划可为此 WAP 设备重新分配的无线信道。

为 WAP 设备进行选择时，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。

建议信道是在下次更新时分配到每个 WAP 设备的信道。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 设备分配到与其以前所用信道不同的信道，具体取决于规划结果。

刷新该页可查看新信道分配表。



第 7 章

访问控制

本章介绍如何在 WAP 设备上配置 ACL 和服务质量 (QoS) 功能。具体包括以下主题：

ACL

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

WAP 设备在每个 ACL 中最多支持 50 个 IPv4、IPv6 和 MAC ACL 以及最多 10 个规则。每个 ACL 支持多个接口。

IPv4 和 IPv6 ACL

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。IP ACL 可以将第 3 层和第 4 层流量分类。

注释 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 或服务类别。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

使用“ACL 规则”页配置 ACL 和规则，并将规则应用到指定接口。

要配置 ACL，请按照以下步骤操作：

步骤 1 依次选择**访问控制 > ACL**。

步骤 2 在 ACL 表中，单击 添加新行并创建 ACL。

步骤 3 输入 ACL 的名称。

步骤 4 从下拉列表中选择 ACL 类型（**IPv4**、**IPv6** 或 **MAC**）。

步骤 5 单击 并选择关联接口来应用 ACL，然后单击**确定**。如果要更改关联接口，可单击 **—** 删除所选接口，然后单击 选择新关联接口。

步骤 6 单击**更多**查看 ACL 的参数。

步骤 7 接下来，配置 ACL 的规则。对于 IPv4 ACL，请参阅 配置 IPv4 ACL，第 76 页。对于 IPv6 ACL，请参阅 配置 IPv6 ACL，第 78 页。对于 MAC ACL，请参阅 配置 MAC ACL，第 81 页。

步骤 8 单击**保存**保存所有更改。

配置 IPv4 ACL

要配置 IPv4 ACL，请执行以下步骤：

步骤 1 依次选择**访问控制 > ACL**。

步骤 2 单击 添加 ACL。

步骤 3 在“ACL 名称”字段中，输入该 ACL 的名称。该名称仅限于 31 个字母数字和特殊字符，中间不得有任何空格。

步骤 4 从“ACL 类型”列表中，选择 **IPv4** 作为 ACL 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 5 单击 并选择关联接口来应用 ACL。单击**确定**。如果要更改关联接口，可以单击 **—** 删除所选接口，然后单击 选择新关联接口。

步骤 6 单击**更多**查看配置参数。单击 添加规则并配置以下参数：

注释 如果未添加任何规则，DUT 将默认拒绝所有流量。

- **规则优先级** - 当 ACL 具有多个规则时，规则按优先级顺序应用于数据包或帧。数字越小意味着优先级越高。新规则的优先级将是所有显式规则中最低的。请注意，始终存在一个拒绝所有流量的隐式规则（优先级最低）。
- **操作** - 选择是**拒绝**还是**允许**该操作。默认操作为**拒绝**。

  如果选择**允许**，此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**，此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。

- **服务（协议）** - 根据“IP 协议”字段的值使用第 3 层或第 4 层协议匹配条件。可以选择以下选项之一：
  - **所有流量** - 允许符合规则条件的所有流量
  - **从列表中选择** - 选择以下协议之一：**IP**、**ICMP**、**IGMP**、**TCP** 或 **UDP**。
  - **自定义** - 输入从 0 至 255 的标准 IANA 分配协议 ID。选择此方法来识别“从列表中选择”中未列出的协议。
- **源 IPv4 地址** - 要求数据包的源 IP 地址与相应字段中定义的地址相匹配。
  - **任意** - 允许任意 IP 地址。
  - **单一地址** - 输入应用此条件的 IP 地址。
  - **地址/掩码** - 输入源 IP 地址通配符掩码。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** - 在规则的匹配条件中包含源端口。在数据报头中标识源端口
  - **所有流量** - 允许符合规则条件的所有流量。
  - **从列表中选择** - 选择与源端口关联的关键字进行匹配：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。
  - **自定义** - 输入 IANA 端口号以匹配数据报头中标识的源端口。端口范围为 0 至 65535 ，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
- **目标 IPv4 地址** - 要求数据包的目标 IP 地址与相应字段中定义的地址相匹配。
  - **任意** - 输入任意 IP 地址。
  - **单一地址** - 输入应用此条件的 IP 地址。
  - **地址/掩码** - 输入目标 IP 地址通配符掩码。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。
- **目标端口** - 在规则的匹配条件中包含目标端口。目标端口在数据报头中标识。
  - **任意** - 符合规则条件的任意端口。

- **从列表中选择** - 选择与目标端口关联的关键字进行匹配：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。
- **自定义** - 输入 IANA 端口号以匹配数据报头中标识的目标端口。端口范围为 0 至 65535，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

- **服务类型** - 根据特定服务类型匹配数据包。
  - **任意** - 任何类型的服务。
  - **从列表中选择** - 根据数据包的 DSCP 确保转发 (AS)、服务类别 (CS) 或加速转发 (EF) 值匹配数据包。
  - **DSCP** - 根据自定义 DSCP 值匹配数据包。如果选择此字段，请输入一个 0 至 63 之间的值。
  - **优先级** - 根据数据包的 IP 优先级值匹配数据包。如果选择此字段，请输入一个 0 至 7 之间的 IP 优先级值。
  - **ToS/掩码** - 输入 IP ToS 掩码值，以标识 IP ToS 数位值中用于与数据包的 IP ToS 字段值进行比较的数位位置。

    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 掩码中的零值数位表示 IP ToS 数位值中用于与数据包的 IP ToS 字段值进行比较的数位位置。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 数位值 0 和 IP ToS 掩码值 00。

步骤 7 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改 ACL，请选择 ACL，然后单击**删除**或**编辑**

要删除或修改规则，请在“规则配置”区域中选择规则，然后单击**删除**或**编辑**。

步骤 8 单击**保存**。

配置 IPv6 ACL

要配置 IPv6 ACL，请执行以下步骤：

步骤 1 依次选择**访问控制 > ACL**。

步骤 2 单击 添加 ACL。

步骤 3 在“ACL 名称”字段中，输入该 ACL 的名称。

步骤 4 从“ACL 类型”列表中，选择 **IPv6** 作为 ACL 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 5 单击 并选择关联接口来应用 ACL。接下来，单击**确定**。如果要更改关联接口，可以单击 **—** 删除所选接口，然后单击 选择新关联接口。

步骤 6 单击**更多**查看配置参数。单击 添加规则并配置以下参数：

注释 如果未添加任何规则，DUT 将默认拒绝所有流量。

- **规则优先级** - 当 ACL 具有多个规则时，规则按优先级顺序应用于数据包或帧。数字越小意味着优先级越高。新规则的优先级将是所有显式规则中最低的。可以单击向上或向下按钮更改其优先级。请注意，始终存在一个拒绝所有流量的隐式规则（优先级最低）。
- **操作** - 选择是**拒绝**还是**允许**该操作。默认操作为**拒绝**。

  如果选择**允许**，此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**，此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。
- **服务（协议）** - 根据“IP 协议”字段的值使用第 3 层或第 4 层协议匹配条件。可以选择以下选项之一：
  - **所有流量** - 允许符合规则条件的所有流量。
  - **从列表中选择** - 选择以下协议之一：**IPv6**、**ICMPv6**、**TCP** 或 **UDP**。
  - **自定义** - 输入从 0 至 255 的标准 IANA 分配协议 ID。选择此方法来识别“从列表中选择”中未列出的协议。
- **源 IPv6 地址** - 要求数据包的源 IP 地址与相应字段中定义的地址相匹配。
  - **任意** - 允许任意 IP 地址。
  - **单一地址** - 输入应用此条件的 IP 地址。
  - **地址/掩码** - 输入源 IP 地址通配符掩码。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** - 在规则的匹配条件中包含源端口。源端口在数据报头中标识。
  - **任意** - 允许任意源端口。
  - **从列表中选择** - 选择与源端口关联的关键字进行匹配：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。
  - **自定义** - 输入 IANA 端口号以匹配数据报头中标识的源端口。端口范围为 0 至 65535 ，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

- **目标 IPv6 地址** - 要求数据包的目标 IP 地址与相应字段中定义的地址相匹配。
  - **任意** - 输入任意 IP 地址。
  - **单一地址** - 输入应用此条件的 IP 地址。
  - **地址/掩码** - 输入目标 IP 地址通配符掩码。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。
- **目标端口** - 在规则的匹配条件中包含目标端口。目标端口在数据报头中标识。
  - **任意** - 符合规则条件的任意端口。
  - **从列表中选择** - 选择与目标端口关联的关键字进行匹配：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。
  - **自定义** - 输入 IANA 端口号以匹配数据报头中标识的目标端口。端口范围为 0 至 65535，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
- **流标签** - 指定 IPv6 数据包唯一的 20 位数字。
  - **任意** - 任何 20 位数。
  - **DSCP** - 根据自定义 DSCP 值匹配数字。
- **DSCP** - 根据数据包的 IP DSCP 值匹配数据包。
  - **任意** - 允许任意 DSCP 值。
  - **从列表中选择** - 从下拉列表中选择 DSCP 值。
  - **自定义** - 输入自定义 DSCP 值，范围为 0 至 63。

步骤 7 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改 ACL，请选择 ACL，然后单击**删除**或**编辑**。

要删除或修改规则，请在“规则配置”区域中选择规则，然后单击**删除**或**编辑**。

步骤 8 单击**保存**。

配置 MAC ACL

要配置 MAC ACL，请执行以下步骤：

步骤 1 依次选择**访问控制 > ACL**。

步骤 2 单击 添加 MAC ACL。

步骤 3 在“ACL 名称”字段中，输入用于标识该 ACL 的名称。

步骤 4 从列表中选择 **MAC** 作为 ACL 类型。MAC ACL 基于第 2 层标准控制访问。

步骤 5 单击 并选择关联接口来应用 ACL，然后单击**确定**。如果要更改关联接口，可以单击 **—** 删除所选接口，然后单击 选择新关联接口。

步骤 6 然后，单击**更多**查看配置参数。单击 添加规则并配置以下参数：

- **规则优先级** - 当ACL具有多个规则时，规则按其优先级顺序应用于数据包或帧。数字越小意味着优先级越高。新规则的优先级将是所有显式规则中最低的，可以单击向上或向下按钮更改其优先级。请注意，始终存在一个拒绝所有流量的隐式规则（优先级最低）。
- **操作** - 选择是**拒绝**还是**允许**该操作。默认操作为**拒绝**。

  如果选择**允许**，此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**，此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。
- **服务（ETH 类型）** - 选择此选项可将匹配标准与以太网帧头中的值进行比较。可以从下拉列表中选择 ETH 类型。
  - 任意 - 允许任意协议。
  - **从列表中选择** - 选择以下协议类型之一：**ARP**、**IPv4**、**IPv6**、**IPX**、**NetBIOS**、**PPPoE**。
  - **自定义** - 输入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。
- **源 MAC 地址** - 要求数据包的源 MAC 地址与相应字段中定义的地址相匹配。
  - **任意** - 允许任意源 MAC 地址。
  - **单一地址** - 输入要与以太网帧进行比较的源 MAC 地址。
  - **地址/掩码** - 输入源 MAC 地址掩码，指定源 MAC 中的哪些数位要与以太网帧进行比较。

    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。
- **目标 MAC 地址** - 要求数据包的目标 MAC 地址与相应字段中定义的地址相匹配。
  - **任意** - 允许任意目标 MAC 地址。
  - **单一地址** - 输入要与以太网帧进行比较的目标 MAC 地址。
  - **地址/掩码** - 输入目标 MAC 地址掩码，指定目标 MAC 中的哪些数位要与以太网帧进行比较

- **VLAN ID** - 要与以太网帧进行比较的 VLAN ID。
  - **任意** - 允许任意 VLAN ID。
  - **自定义** - 输入要与以太网帧进行比较的特定 VLAN ID。此字段位于 first/only 802.1Q VLAN 标记中。端口范围为 1 至 4094。
- **服务类别** - 指定服务 802.1p 用户优先级值的类别。
  - **任意** - 允许任意等级的服务。
  - **自定义** - 输入要与以太网帧进行比较的 802.1p 用户优先级。有效范围为 0 至 7。

步骤 7 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改 ACL，请选择 ACL，然后单击**删除**或**编辑**。要删除或修改规则，请在**规则配置**区域中选择规则，然后单击**删除**或**编辑**。

步骤 8 单击**保存**。

客户端 QoS

客户端服务质量 (QoS) 用于控制连接到网络的无线客户端，并管理所使用的带宽。客户端 QoS 可以通过使用访问控制列表 (ACL) 来控制流量，如 HTTP 流量或从特定子网流出的流量。ACL 是允许和拒绝条件的集合，也称为规则，可提供安全保障和阻止未经授权的用户，并允许授权用户访问特定资源。ACL 可以阻止未经授权的用户尝试访问网络资源。

流量分类

QoS 功能包含允许将流量分类为流的差分服务 (DiffServ) 支持。系统也根据定义的每跳行为对其进行一定的 QoS 处理。

基于 IP 的标准网络旨在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。对于典型的互联网应用（例如邮件和文件传输），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分类处理方式的策略映射进行关联。包含时间敏感型流量的类可以分配给策略映射。

配置 IPv4 流量分类

要添加并配置 IPv4 类映射，请执行以下步骤：

步骤 1 依次选择**客户端 QoS > 流量分类**。

步骤 2 单击 添加流量分类。

注释 最大类映射数为 50。

步骤 3 在**流量分类名称**文本框中，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 4 在**类类型**中，从列表中选择 **IPv4**。IPv4 流量分类仅适用于 WAP 设备中的 IPv4 流量。

步骤 5 配置以下参数：

- **源地址** - 要求数据包的源 IPv4 地址与相应字段中定义的 IPv4 地址相匹配。
  - **任意** - 要用作源地址的任意 IPv4 地址。
  - **单一地址** - 输入一个要应用此条件的 IPv4 地址。
  - **地址/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数位掩码，可指示目标 IP 地址中用于匹配数据包内容的部分。

    DiffServ 掩码 255.255.255.255 表示所有数位都重要，掩码 0.0.0.0 表示所有数位都不重要。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。

- **目标地址** - 要求数据包的目标 IPv4 地址与相应字段中定义的 IPv4 地址相匹配。
  - **任意** - 要用作目标地址的任意 IPv4 地址。
  - **单一地址** - 输入要应用此条件的 IPv4 地址。
  - **地址/掩码** - 输入目标 IP 地址掩码。

步骤 6 单击**更多**，并配置以下参数：

- **协议** - 基于 IPv4 数据包中的“IP 协议”字段值或 IPv6 数据包中的“下一个报头”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：
  - **所有流量** - 允许任意协议的所有流量。
  - **从列表中选择** - 与所选协议匹配：IP、ICMP、IGMP、TCP、UDP。
  - **自定义** - 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。

  注释 如果**协议**是“所有流量”，则**源地址**和**目标地址**不可选。

- **源端口** - 在规则的匹配条件中包含源端口。源端口在数据报头中标识。
  - **任意** - 允许任意端口作为源端口。
  - **从列表中选择** - 与源端口关联的关键字匹配：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。
  - **自定义** - 将数据报头中的源端口号与指定的 IANA 端口号进行匹配。端口范围为 0 至 65535，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

- **目标端口** - 在规则的匹配条件中包含目标端口。目标端口在数据报头中标识。
  - **任意** - 允许任意端口作为目标端口。
  - **从列表中选择** - 与源端口关联的关键字匹配：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。
  - **自定义** - 将数据报头中的源端口号与指定的 IANA 端口号进行匹配。端口范围为 0 至 65535，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

- **服务类型** - 指定在将数据包与类条件进行匹配时要使用的服务类型。
  - **任意** - 允许任意类型的服务作为匹配标准。
  - **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，范围为 0 至 63。
  - **IP 优先级**- 将数据包的 IP 优先级值与此字段中定义的 IP 优先级值进行匹配。IP 优先级范围为 0 至 7。
  - **IP TOS 数位** - 将 IP 报头中数据包的服务类型 (ToS) 数位用作匹配标准。IP TOS 数位值的范围为 00 至 FF。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 数位值中用于与数据包的 IP ToS 字段值进行比较的数位位置。

    IP ToS 掩码值是介于 00 至 FF 之间的两位十六进制数字。IP ToS 掩码中的非零值数位表示 IP ToS 数位值中用于与数据包的 IP ToS 字段值进行比较的数位位置。

步骤 7 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改类映射，请从列表中选择类映射名称，然后单击**删除**。如果类映射已附加到策略，则无法将其删除。

步骤 8 单击**保存**。

配置 IPv6 流量分类

要添加并配置 IPv6 类映射，请执行以下步骤：

步骤 1 依次选择**客户端 QoS > 流量分类**。

步骤 2 单击　添加流量分类。

注释　最大类映射数为 50。

步骤 3 在**流量分类名称**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 4 从列表中选择 **IPv6** 作为流量分类类型。IPv6 流量分类仅适用于 WAP 设备中的 IPv6 流量。

步骤 5 配置以下参数：

- **源地址** - 要求数据包的源 IPv6 地址与相应字段中定义的 IPv6 地址相匹配。
  - **任意** - 要用作源地址的任意 IPv6 地址。
  - **单一地址** - 输入要应用此条件的 IPv6 地址。
  - **地址/掩码** - 输入源 IPv6 地址的前缀长度。
- **目标地址** - 要求数据包的目标 IPv4 地址与相应字段中定义的 IPv4 地址相匹配。
  - **任意** - 要用作目标地址的任意 IPv6 地址。
  - **单一地址** - 输入要应用此条件的 IPv6 地址。
  - **地址/掩码** - 输入目标 IPv6 地址，并输入目标 IPv6 地址的前缀长度。

步骤 6 单击**更多**，并配置以下参数：

- **协议** - 基于 IPv4 数据包中的“IP 协议”字段值或 IPv6 数据包中的“下一个报头”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：
  - **所有流量** - 允许任意协议的所有流量。
  - **从列表中选择** - 与所选协议匹配：IP、ICMP、IGMP、TCP、UDP。
  - **自定义** - 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。
- **源端口** - 在规则的匹配条件中包含源端口。源端口在数据报头中标识。

  注释　如果**协议**是“所有流量”，则**源地址**和**目标地址**不可选。

  - **任意** - 允许任意端口作为源端口。
  - **从列表中选择** - 与源端口关联的关键字匹配：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。

- **自定义** - 将数据报头中的源端口号与指定的 IANA 端口号进行匹配。端口范围为 0 至 65535，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

- **目标端口** - 在规则的匹配条件中包含目标端口。目标端口在数据报头中标识。
  - 任意 - 允许任意端口作为目标端口。
  - **从列表中选择** - 与源端口关联的关键字匹配：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。
  - **自定义** - 将数据报头中的源端口号与指定的 IANA 端口号进行匹配。端口范围为 0 至 65535，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

- **IPv6 流标签** - 流标签由节点用来标记流中的数据包。
  - **任意** - IPv6 数据包特有的任意 20 位数字。
  - **用户定义** - 输入 IPv6 数据包特有的一个 20 位数字。此数字由终端站用于表示路由器中的 QoS 处理情况（范围为 0 至 FFFFF）。

- **服务类型** - 指定在将数据包与类条件进行匹配时要使用的服务类型。
  - **任意** - 允许任意类型的服务作为匹配标准。
  - **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，范围为 0 至 63

步骤 7 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改类映射，请从列表中选择类映射名称，然后单击**删除**。如果类映射已附加到策略，则无法将其删除。

步骤 8 单击**保存**。

配置 MAC 流量分类

要添加并配置 MAC 类映射，请执行以下步骤：

步骤 1 依次选择**客户端 QoS > 流量分类**。

步骤 2 单击　添加流量分类。

注释　最大类映射数为 50。

步骤 3 在“流量分类名称”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 4 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 5 **源地址** - 在规则的匹配条件中包含源 MAC 地址。

- **任意** - 要用作源地址的任意 MAC 地址。
- **单一地址** - 输入要与以太网帧进行比较的源 MAC 地址。
- **地址/掩码** - 输入源 MAC 地址掩码，指定目标 MAC 地址中的哪些数位要与以太网帧进行比较。

  对于 MAC 掩码中的每个数位位置，1 表示相应的地址位是高位，0 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 ff:ff:ff:ff:00:00 。MAC 掩码 ff:ff:ff:ff:ff:ff 可检查所有的地址位，用于匹配单个 MAC 地址。

步骤 6 **目标地址** - 在规则的匹配条件中包含目标 MAC 地址。

- **任意** - 要用作目标地址的任意 MAC 地址。
- **单一地址** - 输入要与以太网帧进行比较的目标 MAC 地址。
- **地址/掩码** - 输入目标 MAC 地址掩码，指定目标 MAC 地址中的哪些数位要与以太网帧进行比较。

步骤 7 单击**更多**，并配置以下参数：

- **协议** - 将匹配标准与以太网帧报头中的值进行比较。选择 EtherType 关键字或输入 EtherType 值以指定匹配标准：
  - **所有流量** - 允许任意协议的所有流量。
  - **从列表中选择** - 将数据报头中的 Ethertype 与所选协议类型进行匹配：Apple Talk、ARP、IPv4、IPv6、IPX、NETBIOS、PPPoE。
  - **自定义** - 将数据报头中的 Ethertype 与指定的自定义协议标识符进行匹配。此值可以是介于 0600 至 FFFF 之间的四位十六进制数。

  注释　如果**协议**是“所有流量”，则**源地址**和**目标地址**不可选。

- **服务类别** - 指定服务 802.1p 用户优先级值的类别。
  - **任意** - 允许任意等级的服务。

- **用户定义** - 输入要与以太网帧进行比较的 802.1p 用户优先级。有效范围为 0 至 7。

- **VLAN ID** - 要与以太网帧进行比较的 VLAN ID。
  - **任意** - 允许任意 VLAN ID。
  - **用户定义** - 输入要与以太网帧进行比较的特定 VLAN ID。此字段位于 first/only 802.1Q VLAN 标记中。端口范围为 1 至 4094。

步骤 8 单击**确定**。更改将保存到“启动配置”。

注释 要删除或修改类映射，请从列表中选择类映射，然后单击**删除**。如果类映射已附加到策略，则无法将其删除。

步骤 9 单击**保存**。

QoS 策略

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”页上的类定义。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 设备最多可容纳 50 个策略，每个策略中最多包含 10 个类。

要添加和配置策略映射，请执行以下步骤：

步骤 1 依次选择**客户端 QoS > QoS 策略**。

步骤 2 单击 添加 QoS 策略。在“QoS 策略名称”字段中，输入 QoS 策略的名称。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 可以选择之前创建的关联流量分类。

步骤 4 在“QoS 策略定义”区域中，为策略映射配置以下参数：

- **承诺速率** - 流量必须遵守的承诺速率 (Kbps)。范围为 1 至 1000000 Kbps。
- **承诺突发** - 流量必须遵守的承诺的突发大小（字节）。范围为 1 至 1600000Kbps。
- **操作** - 选择以下选项之一：
  - **发送** - 指定如果符合流量分类标准，将转发关联流量流的所有数据包。
  - **丢弃** - 指定如果符合流量分类标准，将丢弃关联流量流的所有数据包。
- **重新标记流量** - 使用 802.1p 报头优先级字段中的指定服务类别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 值是一个 0 至 7 之间的整数。
  - **重新标记 COS** - 网络流量可划分为多个优先级或服务类。CoS 值的范围为 0 至 7，其中 0 是最低优先级，7 是最高优先级。

- **重新标记 DSCP** - 根据提供的 QoS 指定应用于数据包的特定每跳行为 (PHB)。从下拉列表中选择值。
- **重新标记 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 优先级值是一个 0 至 7 之间的整数

步骤 5 单击**添加策略属性**。可以添加其他类映射，但此特定策略的类映射数的最大限值为 10。

步骤 6 单击**保存**。

注释 要删除或修改 QoS 策略，请从列表中选择 QoS 策略，然后单击**删除**或**编辑**。

QoS 关联

“QoS 关联”页提供对无线和以太网接口某些 QoS 方面的额外控制。

除控制一般的流量类别外，QoS 可用于配置通过 QoS 策略名称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，QoS 策略名称可用于建立可应用于每个无线客户端的一般微流定义和处理特性。

要配置 QoS 关联参数，请执行以下步骤：

步骤 1 依次选择**客户端 QoS** > **QoS 关联**。

步骤 2 单击 添加 QoS 关联。

步骤 3 从 **QoS 策略名称**下拉列表选择一个 QoS 策略名称。

步骤 4 配置以下参数：

- **速率限制（从无线接入点到客户端）** - 从 WAP 设备到客户端的最大允许传输速率（位/秒 [bps]）。有效范围为 0 至 1733Mbps。
- **速率限制（从客户端到无线接入点）** - 从客户端到 WAP 设备的最大允许传输速率（位/秒 [bps]）。有效范围为 0 至 1733Mbps。

步骤 5 单击**保存**。

注释 接口可以绑定 QoS 策略或 ACL，但不能同时绑定这两者。

访客接入

可以在 WAP 设备上配置默认 CP 实例。CP 实例是一组定义的实例参数。实例可以与一个或多个 VAP 关联。

使用无线客户端连接到 VAP 并访问任何 URL 时，Web 会将该 URL 劫持到“Web 门户区域设置”页，该页面可在“访问控制/访客接入”页中配置。

“Web 门户区域设置”定义劫持 GUI 页面的显示样式，访客组决定用户的用户名和密码。

要配置访客接入实例，请执行以下步骤：

步骤 1 编辑 **Web 门户区域设置表**以设计被劫持的 GUI 页面的显示。单击**预览**选项卡查看显示。

步骤 2 编辑**访客组表**，单击**总访客用户**数上的值链接添加用途，然后单击**保存**。

步骤 3 配置**访客接入实例表**，选择使用上述步骤配置的**访客组**和 **Web 门户区域设置**。

步骤 4 转到**无线** > **网络**以关联 VAP 访客接入并配置访客接入实例。

访客接入实例表

步骤 1 依次选择**访客接入** > **访客接入实例表**。

步骤 2 在**访客接入实例名称**字段中指定 CP 实例的名称。实例名称最多可包含 32 个字母数字字符。

步骤 3 “网页认证实例参数”区域再次显示，其中包含更多选项。配置以下参数：

- **协议** - 选择 HTTP 或 HTTPS 作为 CP 实例在验证过程中使用的协议。
  - **HTTP** - 在验证期间不使用加密。
  - **HTTPS** - 使用安全套接字层 (SSL)，它需要一个证书来提供加密。证书会在连接时提供给用户。
- **身份验证方法** - 选择用于验证客户端的 CP 的身份验证方法。选项如下：
  - **本地数据库** - WAP 设备使用本地数据库对用户进行身份验证。如果使用“本地数据库”设置，请配置以下参数。
    - **访客组名称** - 输入访客组的名称。
    - **空闲超时** - 输入空闲超时时间（分钟）。
    - **最大上传带宽** - 输入客户端在使用网页认证时可以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。范围为 0 至 1733 Mbps。默认值为 0。
    - **最大下载带宽** - 输入客户端在使用网页认证时可以接收流量的最大下载速度。此设置限制了用于从网络接收数据的带宽。范围为 0 至 1733 Mbps。默认值为 0。
    - **总访客用户** - 访客用户总数。
  - **RADIUS 身份验证** - 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。如果使用 RADIUS 身份验证设置，请配置以下参数。
    - **Radius IP 网络** - 从下拉列表中选择 Radius IP 网络（**IPv4 或 IPv6**）。

- **全局 RADIUS** - 选中**启用**启用全局 RADIUS。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 记帐** - 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 记帐，也会对主 RADIUS 服务器、所有备份服务器以及所有已配置服务器启用此功能。
- **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 或服务器 IPv6 地址 2 - 最多输入三个 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用服务器。
- **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 - 输入与已配置备份 RADIUS 服务器关联的 RADIUS 密钥。位于服务器 IP 地址 1 的服务器使用密钥 1，位于服务器 IP 地址 2 的服务器使用密钥 2，以此类推。

- **无身份验证** - 用户不需要通过数据库进行身份验证。
- **第三方凭证** - WAP 设备使用社交媒体上的凭证对用户进行验证。如果使用“已验证的第三方凭证”设置，请配置以下设置。
  - **已接受的凭证** - 选择 Facebook 或 Google 或者同时选择两者作为凭证验证信息来源。
  - **围墙花园** - 在选中**已接受的凭证**后，系统将自动设置相关的默认配置。

  注释　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*
- **Active Directory 服务** - WAP 设备使用远程 ADS 服务器上的数据库对用户进行验证。如果使用“已验证的 ADS”设置，请配置以下设置。
  - **Active Directory 服务器** - 点击　图标添加新的 ADS 服务器。您最多可以添加 3 台服务器。使用**箭头**调整服务器的位置和优先级。选择**垃圾桶**可删除配置。使用**测试**检查 ADS 服务器是否有效。

- **访客组** - 如果“身份验证方法”设置为“本地数据库”或“Radius身份验证”，请选择之前创建的访客组。允许属于一组的所有用户通过此门户访问网络。
- **重定向 URL** - 要启用 URL 重定向，请输入 URL（包括 http://）。范围为 0 至 256 个字符。

- **会话超时** - 输入 CP 会话的有效剩余时间（秒）。时间达到零后，系统将取消对客户端的身份验证。范围为 0 至 1440 分钟。默认值为 0。
- **Web 门户区域设置** - 从下拉列表中选择之前创建的 Web 门户区域设置。

步骤 4 单击**保存**。更改将保存到“启动配置”。

访客组表

在设备上，将每个本地用户分配给用户组，并将用户组分配给 CP 实例。组便于管理向用户指定 CP 实例。

名称为 Default 的用户组是内置用户组，无法删除。

要配置本地用户，请执行以下步骤：

步骤 1 依次选择**访客接入 > 访客组表**。

步骤 2 在“访客组设置”区域中配置以下参数：

- **访客组名称** - 指定新访客组的名称。默认访客组名称为 **Default**

步骤 3 配置以下参数：

- **空闲超时** - 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。范围为 0 至 1440 分钟。默认值为 60。此处配置的超时值优先于为 CP 实例配置的超时值，除非用户值设置为 0。设置为 0 时，系统将使用为 CP 实例配置的超时值。
- **最大上传带宽** - 输入客户端在使用网页认证时可以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。范围为 0 至 1733 Mbps。默认值为 0。
- **最大下载带宽** - 输入客户端在使用网页认证时可以接收流量的最大下载速度。此设置限制了用于从网络接收数据的带宽。范围为 0 至 1733 Mbps。默认值为 0。
- **总访客用户** - 显示访客用户总数。单击**总访客用户**上的值链接以显示**访客用户帐户**页。

步骤 4 单击**保存**。

访客用户帐户

要配置访客用户帐户，请执行以下步骤：

步骤 1 依次选择**访客接入 > 访客组表**。

步骤 2 单击**总访客用户**字段上的数字链接，在**访客用户帐户**页中显示**访客用户帐户表**。

步骤 3 单击 添加用户。

步骤 4 **访客用户名** - 输入新访客用户的名称。实例名称最多可包含 32 个字母数字字符。

步骤 5 **访客用户密码** - 输入密码。密码可以包含 8 至 64 个字母数字和特殊字符。

步骤 6 单击**保存**。

注释 可以单击**返回**按钮链接查看**访客接入**页。

要删除或修改访客用户，请选择访客用户，然后单击**删除**或**编辑**。

Web 门户自定义

CP 实例与 VAP 关联后，创建一个区域设置并将其映射到 CP 实例。用户访问与 CP 实例关联的 VAP 时，系统会显示身份验证页面。

使用“Web 门户自定义”页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。

步骤 1 依次选择**访客接入** > **Web 门户区域设置表**。

步骤 2 在此表中，单击**添加**以访问**网页认证自定义**页。要修改区域设置，请选中相应行，然后单击**编辑**或单击**删除**以删除。

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 门户区域设置名称** - 输入要指定给页面的 Web 区域设置名称。名称可以包含 1 至 32 个字母数字字符。

步骤 4 “网页认证 Web 区域设置参数”区域显示用于修改区域设置的其他选项。访客接入实例名称无法编辑。可编辑字段使用默认值进行填充。配置以下参数：

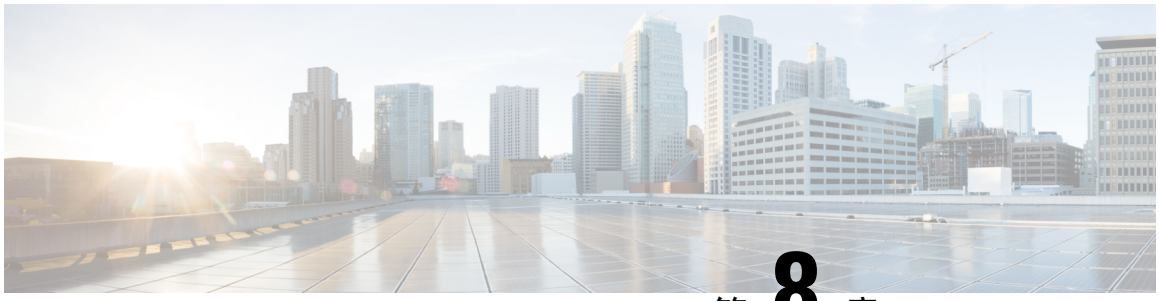
- **访客接入实例名称** - 显示访客接入实例的名称。
- **背景图像** - 单击**浏览**选择图像。可以单击**上传**以上传 CP 实例的图像。
- **徽标图像** - 单击**浏览**选择徽标图像。可以单击**上传**以上传徽标图像。
- **前景颜色** - 输入 6 位十六进制格式的前景颜色 HTML 编码。范围为 1 至 32 个字符。默认值为 #FFFFFF。
- **背景颜色** - 输入 6 位十六进制格式的背景颜色 HTML 编码。范围为 1 至 32 个字符。默认值为 #FFFFFF。
- **分隔符颜色** - 输入粗水平线的颜色 HTML 编码，用于将页眉与页面正文分开，采用 6 位十六进制格式。范围为 1 至 32 个字符。默认值为 #FFFFFF。
- **帐户图像** - 单击**浏览**选择图像。可以单击**上传**以上传帐户图像。
- **字体** - 从下拉列表中选择字体。显示所有文本时将使用此字体。
- **帐户提示** - 输入用户名。范围为 1 至 32 个字符。
- **用户名提示** - 用户名文本框的标签。范围为 1 至 32 个字符。

- **密码提示** - 用户密码文本框的标签。范围为 1 至 64 个字符。
- **按钮提示** - 用户单击此按钮上的标签可提交其用户名和密码进行身份验证。范围为 2 至 32 个字符。默认值为“连接”。
- **浏览器头提示** - 浏览器标题栏中显示的文本。范围为 1 至 128 个字符。默认值为“网页认证”。
- **门户标题提示** - 页眉中显示在徽标右侧的文本。范围为 1 至 128 个字符。默认值为“欢迎使用无线网络”。
- **帐户提示** - 页面正文中用户名和密码文本框下面的文本。范围为 1 至 256 个字符。默认值为“要开始使用此服务，请输入凭证，然后单击连接按钮”。
- **接受策略** -“接受使用政策”复选框中显示的文本。范围为 1 至 4096 个字符。默认值为“接受使用政策”。
- **接受提示** - 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。范围为 1 至 128 个字符。
- **无接受警告** - 当用户提交登录凭证而不选择“接受使用策略”复选框时，弹出窗口中显示的文本。范围为 1 至 128 个字符。
- **正在进行中提示** - 身份验证过程中出现的文本。范围为 1 至 128 个字符。
- **无效凭证提示** - 用户身份验证失败时出现的文本。范围为 1 至 128 个字符。
- **连接成功提示** - 客户端已向 VAP 进行身份验证时显示的文本。范围为 1 至 128 个字符。
- **欢迎提示** - 客户端连接到网络时显示的文本。范围为 1 至 256 个字符。
- **恢复** - 删除当前的区域设置。

步骤 5 单击**保存**。更改将保存到“启动配置”。

步骤 6 单击**预览**查看更新页面。

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**查看更改。



第 8 章

Umbrella

本章介绍如何配置**思科 Umbrella** 服务。其中包含以下主题：

思科 Umbrella

思科 Umbrella 是一款云安全平台，可针对互联网上的威胁提供第一道防线。它充当互联网与您的系统和数据之间的网关，用于阻止利用任何端口、协议或应用的恶意软件、僵尸网络和网络钓鱼。

此集成功能使用 Umbrella 帐户，透明地拦截 DNS 查询并将其重定向到 Umbrella。此设备将在 Umbrella 控制面板上显示为一台网络设备，可用于应用策略和查看报告。

步骤 1 选中该复选框可启用 Umbrella 功能。

步骤 2 在相应的字段中输入您从 **Umbrella** 网站获得的密码和 API 密钥

注释 登录到您的思科 Umbrella 并转至控制面板：导航至**管理 > 平台 API 密钥**以添加名称，并创建密码和密钥信息。

步骤 3 **在要绕过的本地域（可选）** 字段中输入您信任的域名，然后数据包将在不经过 Umbrella 的情况下到达目的地。

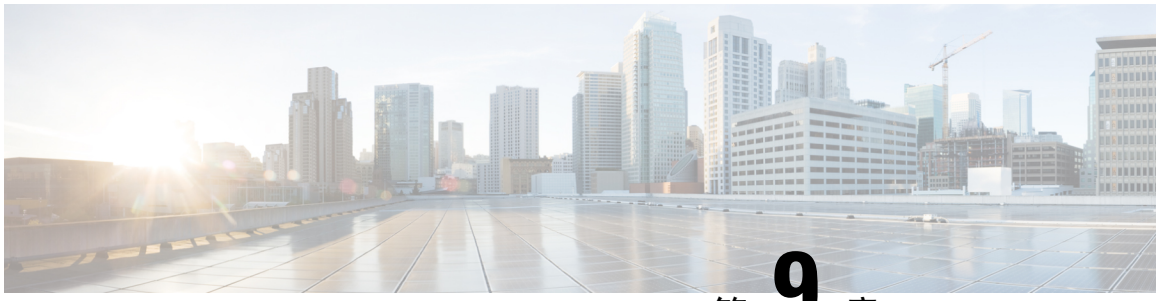
注释 对于所有内联网域和拆分 DNS 域，此步骤都是必需的。

步骤 4 在**设备标签（可选）** 字段中，输入标签名称以标记设备。

步骤 5 选中该复选框可启用 DNS 加密。

注释 DNSCrypt 用于保护 DNS 客户端与 DNS 解析器之间的 DNS 通信。它可以防御 DNS 攻击和监听等多种类型的攻击。默认设置为启用。

步骤 6 点击**保存**应用这些设置。在注册状态字段中可以查看注册状态。



第 9 章

监控

本章介绍如何显示 WAP 设备的状态和统计信息。具体包括以下主题：

控制面板

控制面板显示吞吐量状态，并提供可用于配置或监控网络设备的简单步骤。此页每30秒更新一次。

已连接客户端

当前与 WAP 设备关联的客户端总数。单击该方框可重定向到“客户端”页。

互联网/局域网/无线

页面右上角的圆形图标显示互联网、局域网和无线连接状态。

互联网

- **红色圆形** - 无互联网连接。
- **绿色圆形** - 互联网连接良好。

局域网

- **红色圆形** - 无有线连接。
- **绿色圆形** - 有线连接。

单击**局域网**链接可查看**局域网状态**页。

无线

- **红色圆形** - 所有无线都已禁用。
- **绿色圆形** - 至少一个无线正在工作。一个或两个无线已启用。

单击**无线**链接可查看**无线状态**页。

2.4G 无线吞吐量

此线形图显示 2.4G 无线吞吐量，并且每 30 秒更新一次。

- **上传** - 过去 30 秒传输的吞吐量。
- **下载** - 过去 30 秒接收的吞吐量。

单击**上传**或**下载**以不显示数据。

5G 无线吞吐量

此线形图显示 5G 无线吞吐量，并且每 30 秒更新一次。

- **上传** - 过去 30 秒传输的吞吐量。
- **下载** - 过去 30 秒接收的吞吐量。

单击**上传**或**下载**以不显示数据。

排名靠前的客户端

根据流量顺序，此条形图显示流量排名前 5 的客户端设备

- **上传** - 过去 30 秒传输的吞吐量。
- **下载** - 过去 30 秒接收的吞吐量。

单击**上传**或**下载**以不显示数据。

SSID 利用率

根据流量顺序，此饼图显示流量排名前 5 的 SSID

- 流量 - 传输和接收的总字节数。

网络使用情况

此线形图显示 eth 吞吐量

- **上传** - 过去 30 秒传输的吞吐量。
- **下载** - 过去 30 秒接收的吞吐量。

单击**上传**或**下载**以不显示数据。

快速访问

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。有关更多详细信息，请参阅 快速入门配置，第 8 页。

局域网状态

单击“局域网”圆圈可在局域网接口上显示以下配置和状态设置。

- **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 设备使用的域名服务器 1 的 IP 地址。
- **域名服务器 2** - WAP 设备使用的域名服务器 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 设备使用的 IPv6 DNS 服务器 1 的 IPv6 地址。
- **IPv6-DNS-2** - WAP 设备使用的 IPv6 DNS 服务器 2 的 IPv6 地址。

注释 这些设置适用于内部接口。单击**编辑**可更改任何以上设置。您将被重定向到**局域网**页。

单击**刷新**可刷新屏幕并显示最新信息。

单击**返回**可返回**控制面板**页。

无线状态

单击“无线”圆圈可显示无线功能接口，如：

- **无线功能** - 无线接口启用或禁用无线功能模式。
- **MAC 地址** - 与无线接口关联的 MAC 地址。
- **模式** - 无线接口使用的 802.11 模式 (a/b/g/n/ac)。
- **信道** - 无线接口使用的信道。
- **工作带宽** - 无线接口使用的工作带宽。

单击**编辑**可更改任何以上设置。您将被重定向到**无线电**页。

单击**刷新**可刷新屏幕并显示最新信息。

单击**返回**可返回**控制面板**页。

接口状态

接口状态表显示每个虚拟无线接入点 (VAP) 和每个无线分布式系统 (WDS) 接口的以下状态信息：

- **网络接口** - WAP 设备的无线接口。
- **名称 (SSID)** - 无线接口名称。
- **状态** - VAP 的管理状态（连接或中断）。
- **MAC 地址** - 无线接口的 MAC 地址。
- **VLAN ID** - 无线接口的 VLAN ID。
- **配置文件** - 任一关联调度程序配置文件的名称。
- **状态** - 当前状态（活动或非活动）。状态用于指示 VAP 是否与客户端交换数据。

流量统计信息

“流量统计信息”页显示以太网接口、虚拟无线接入点 (VAP) 和所有 WDS 接口的实时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 设备上次启动后的收发总数。如果重启 WAP 设备，则这些数字表示自重启以来的发送和接收总数。

要查看流量统计信息，请依次选择**监控** > **控制面板** > **快速访问** > **流量统计信息**。

系统将显示以下信息：

- **接口** - 以太网接口以及每个 VAP 和 WDS 接口的名称。每个 VAP 接口的名称均后跟 SSID（用括号括起）
- **数据包总数** - WAP 设备发送（在发送表中）或接收（在接收表中）的数据包总数。
- **字节总数** - WAP 设备发送（在发送表中）或接收（在接收表中）的字节总数。
- **已丢弃数据包总数** - WAP 设备发送（在发送表中）或接收（在接收表中）的已丢弃数据包总数。
- **已丢弃字节总数** - WAP 设备发送（在发送表中）或接收（在接收表中）的已丢弃字节总数。
- **错误数** - 与 WAP 设备上发送和接收的数据相关的错误总数。

注释 单击**刷新**可查看更新信息。

集群设置

此页显示集群成员和当前加入集群的 WAP 设备的流量。

排名靠前的 AP（按流量使用情况）

根据流量顺序，此条形图显示流量排名前 5 的 WAP 设备。

- **上传** - 传输的吞吐量。
- **下载** - 接收的吞吐量。

注释 单击**上传**或**下载**以不显示数据。

排名靠前的 AP（按客户端连接）

根据客户端连接数的顺序。此条形图显示排名前 5 的 WAP 设备。

信道分配表

信道分配表按 IP 地址列出集群设置集群中的所有 WAP 设备。

此表提供以下有关当前信道分配的详细信息：

- **AP 位置** - WAP 设备的物理位置。
- **无线信道** - 此 WAP 设备当前进行广播所在的无线信道。
- **IP 地址** - WAP 设备的 IP 地址。
- **流量（上传/下载）** - 客户端设备发送（上传）或接收（下载）的总字节数。
- **客户端连接数 (2.4G/5G)** - 连接到 WAP 设备的客户端数量。

客户端

客户端

“客户端”页显示与设备关联的客户端工作站。

关联客户端总数 - WAP 设备上的客户端总数。

客户端摘要

显示当前在设备上的 802.11 客户端类型的客户端摘要。

平均带宽

显示平均客户端带宽，以 Mbps 为单位。

- **上传** - 过去 30 秒传输的吞吐量。
- **下载** - 过去 30 秒接收的吞吐量。

注释 单击**上传**或**下载**以不显示数据。

最低信噪比 (SNR) 客户端

根据 SNR 列出信噪比最低的 5 个设备。

最低速客户端

根据速度顺序列出速度最低的 5 个设备。

关联客户端

- **客户端详细信息** - 关联无线客户端的主机名和 MAC 地址。
- **IP 地址** - 关联无线客户端的 IP 地址。
- **网络 (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。
- **模式** - 客户端上使用的 IEEE 802.11 模式，如 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g。
- **数据速率** - 当前传输数据速率。
- **信道** - 客户端当前与之相连的信道。信道可定义无线用于发送和接收的无线频谱部分。可使用“无线电”页设置信道。
- **流量（上传/下载）** - 客户端设备发送（上传）或接收（下载）的总字节数。
- **SNR (db)** - 以分贝 (dB) 为单位显示 SNR 强度。
- **吞吐量计** - 最后 30 秒的吞吐量/数据速率。

注释 可通过“客户端详细信息”、“网络 (SSID)”等为客户端排序。

可通过“客户端详细信息”、“网络 (SSID)”等过滤客户端。

集群设置客户端

- **客户端详细信息** - 关联无线客户端的 MAC 地址。IPv4 地址 - WAP 设备的 IP 地址。
- **IP 地址** - WAP 设备的 IP 地址。
- **网络 (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。
- **模式** - 客户端上使用的 IEEE 802.11 模式，如 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g。
- **数据速率** - 当前传输速率。

- **AP 位置** - WAP 设备的物理位置。
- **信道** - 当客户端当前连接的信道。信道可定义无线用于发送和接收的无线频谱部分。可使用“无线电”页设置信道。
- **流量（上传/下载）** - 客户端设备发送（上传）或接收（下载）的总字节数。
- **SNR (db)** - 以分贝 (dB) 为单位表示强度的数字。
- **吞吐量计** - 最后 30 秒的吞吐量/数据速率。

注释 可通过“客户端详细信息”、“网络 (SSID)”等排序和过滤客户端。

访客

“访客”页提供两个表。一个是“已通过身份验证的客户端”表，该表显示已在任何网页认证实例上进行身份验证的客户端。另一个是“身份验证失败的客户端”表，该表显示有关尝试在网页认证实例上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，请依次选择**监控 > 访客**。

系统将显示以下信息：

- **MAC** - 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。
- **VAP/无线 ID** - 与用户关联的 VAP 和无线。
- **网页认证 ID** - 与用户关联的网页认证实例的 ID。
- **超时** - CP 会话的有效剩余时间（秒）。时间达到零后，系统将取消对客户端的身份验证。
- **离开时间** — 客户端条目的有效剩余时间（秒）。当客户端从 CP 离开时，计时器启动。时间达到零后，系统将取消对客户端的身份验证。
- **上传/下载 (MB)** - WAP 设备从用户工作站传输和接收的字节数。
- **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“导出”可上传当前已通过身份验证/身份验证失败的客户端的消息。

注释 单击“导出”按钮之前，选择要上传的已通过身份验证或身份验证失败的客户端，然后单击**导出**。

第 10 章

管理

本章介绍如何配置“管理”设置和执行诊断。具体包括以下主题：

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。您也可以切换活动映像和非活动映像。

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

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。

注释 升级固件时，WAP 设备会保留现有配置设置。

切换固件映像

要切换 WAP 设备上运行的固件映像，请执行以下步骤：

步骤 1 依次选择**管理** > **固件**。

系统将显示产品 ID (PID VID) 以及活动和非活动固件版本。

步骤 2 单击**替换固件映像**。

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**继续。

此过程可能需要数分钟，在此期间不能访问 WAP 设备。进行映像交换时，不要断开 WAP 设备的电源。映像交换完成时，WAP 设备会重新启动。然后 WAP 设备恢复正常运行，使用和升级前相同的配置设置。

HTTP/HTTPS 升级

要使用 HTTP/HTTPS 进行升级，请执行以下步骤：

步骤 1 选择 **HTTP/HTTPS** 作为传输方式。

步骤 2 单击**浏览**并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**应用新固件映像。

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。此过程完成后，WAP 设备会重新启动并恢复正常运行。

步骤 4 要验证固件是否已成功升级，请登录基于 Web 的配置实用程序，打开“升级固件”页，然后查看活动固件的版本。

TFTP 升级

要使用 TFTP 升级 WAP 设备的固件，请执行以下步骤：

步骤 1 选择 **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 256 个字符），应包含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**升级**。

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。此过程完成后，WAP 设备会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，请登录配置实用程序，打开“升级固件”页，然后查看活动固件的版本。

配置文件

WAP 设备的配置文件采用 XML 格式，包含有关 WAP 设备设置的所有信息。可以将配置文件备份（上传）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，可以将其下载到 WAP 设备以修改配置。WAP 设备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 24 小时无任何修改，则会自动保存到镜像配置文件。镜像配置文件是过去启动配置的快照。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。

注释 您不仅可以将这些文件下载/上传到其他系统，还可以在WAP设备上将它们复制为不同的文件类型。

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 依次选择**管理 > 配置文件 > 下载/备份**。

步骤 2 选择**通过 TFTP** 或**通过 HTTP/HTTPS** 作为传输方式。

步骤 3 选择**备份（无线接入点到 PC**）将配置数据备份到 PC。

步骤 4 对于 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存储的路径，然后输入 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 对于 TFTP 备份，请输入 TFTP 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 24 小时无任何修改，则会自动保存到镜像配置文件。镜像配置是过去启动配置的快照。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/HTTPS 备份，系统会显示一个窗口，可用于浏览所需的文件保存位置。

下载配置文件

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

要将配置文件下载到 WAP 设备，请执行以下步骤：

步骤 1 依次选择**管理 > 配置文件 > 下载/备份**。

步骤 2 选择**通过 TFTP** 或**通过 HTTP/HTTPS** 作为传输方式。

步骤 3 选择**下载**（**PC 到无线接入点**）将配置数据备份到 PC。

步骤 4 对于 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存储的路径，然后输入 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**启动配置**或**备份配置**以将文件替换为下载的文件。

如果下载的文件覆盖了启动配置文件且通过了有效性检查，下载的配置将在 WAP 设备下次重新启动时生效。

步骤 6 单击**保存**开始升级或备份。对于 HTTP/HTTPS 下载，系统会显示一个窗口，可用于浏览以选择要下载的文件。

注意 下载配置文件时，请确保 WAP 设备电源不中断。如果在下载配置文件时发生断电，文件将会丢失，必须重新执行下载过程。

复制配置文件

可以在 WAP 设备文件系统内复制文件。例如，可以将备份配置文件复制为启动配置文件类型，以便下次启动 WAP 设备时使用。

要将文件复制为其他文件类型，请执行以下步骤：

步骤 1 依次选择**管理 > 配置文件 > 复制**。

步骤 2 在“复制来源”字段中，选择要复制的以下源文件类型之一：

- **启动配置** - 用于启动的配置文件。
- **备份配置** - WAP 设备中保存的备份配置文件。
- **镜像配置** - 如果启动配置至少 24 小时无任何修改，则会自动保存到镜像配置文件。镜像配置是过去启动配置的快照。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 在“复制到”字段中，选择正在复制的文件所要替换的文件类型。

步骤 4 单击**保存**开始复制过程。

清除配置文件

可以清除启动配置或备份配置文件。如果清除启动配置文件，备份配置文件将在下次重启 WAP 设备时变为活动文件。

要删除启动或备份配置文件，请执行以下步骤：

步骤 1 依次选择**管理 > 配置文件 > 清除**。

步骤 2 选择**启动配置**或**备份配置**。

步骤 3 单击**清除文件**。

步骤 4 单击**确定**。

重启

使用“重启”页重启 WAP 设备，或将 WAP 设备重置为出厂默认配置。要重启或重置 WAP 设备，请执行以下操作：

步骤 1 依次选择**管理 > 重启**。

步骤 2 要使用出厂默认配置文件重启 WAP 设备，请选中**恢复出厂默认设置**。任何自定义设置都将丢失。

步骤 3 单击**重启**。系统会显示一个窗口，提示您确认或取消重启。

步骤 4 单击**确定**进行重启。

计划重启

要在 WAP 设备上计划重启，请按照下列步骤操作：

步骤 1 选中**计划重启**复选框以启用计划重启功能。

步骤 2 计划重启有两个选项。

- **日期** - 设置重启设备的确切日期和时间。
- **发生时间** - 设置启用该功能后，重启发生的时间。

注释 对于**发生时间**，重启调度程序在设备重启后仍然有效。

步骤 3 单击**保存**。

第 11 章

故障排除

本章介绍如何通过多个 WAP 设备配置数据包捕获以进行故障排除。具体包括以下主题：

频谱智能

“频谱智能”页提供频谱分析仪功能的状态，并提供用于查看频谱数据的链接。以下页面介绍频谱分析仪的详细信息。

启用频谱分析模式 - 频谱分析模式为“专用频谱分析仪”或“混合频谱分析仪”或“3+1 频谱分析”。

步骤 1 依次选择**故障排除** > **频谱智能**

步骤 2 选择无线接口，然后单击**设置**按钮启动频谱智能。

步骤 3 单击**查看频谱数据**，查看有关**信道质量**和**非 WLAN 信道利用率**的详细信息。

查看频谱数据 - 当扫描模式设置为“专用频谱分析仪”或“混合频谱分析仪”或“3+1 频谱分析仪”时，系统将启动频谱查看器，无线状态为开启，且仅通过 IPv4 地址访问网页。

步骤 4 单击**停止**以禁用频谱分析模式状态。

数据包捕获

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

以下是两种数据包捕获方法：

- **本地捕获方法** - 捕获的数据包存储在 WAP 设备上的文件中。WAP 设备可以将此文件传输到 TFTP 服务器。此文件为 pcap 格式，可使用 Wireshark 进行检查。可以单击**在此设备上保存文件**来选择本地捕获方法。
- **远程捕获方法** - 捕获的数据包可以实时重定向到运行 Wireshark 的外部计算机。可以单击**传输到远程主机**来选择远程捕获方法。

  捕获的数据包可以实时重定向到 CloudShark，这是一个基于 Web 的数据包解码器和分析器网站。它与用于数据包分析的 Wireshark UI 类似。您可通过选中**流向 CloudShark** 来选择远程捕获方法。

WAP 设备可以捕获以下类型的数据包：

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

使用“数据包捕获”页可配置数据包捕获参数、启动本地或远程数据包捕获、查看当前数据包捕获状态，以及下载数据包捕获文件。

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 依次选择**故障排除 > 数据包捕获**。

步骤 2 确保已为“数据包捕获方法”选择**在此设备上保存文件**。

步骤 3 配置以下参数：

- **接口** - 输入数据包捕获的捕获接口类型：
  - **以太网** - 以太网端口中的 802.3 流量。
  - **无线 1/无线 2** - 无线接口中的 802.11 流量。
- **持续时间** - 输入捕获持续时间，单位为秒。范围为 10 至 3600。默认值为 60。
- **最大文件大小** - 输入允许的最大捕获文件大小，单位为 KB。范围为 64 至 4096。默认值为 1024。

步骤 4 数据包捕获有两种模式。

- **所有无线流量** - 捕获所有无线数据包。
- **流入/流出此无线接入点的流量** - 捕获从无线接入点发送或无线接入点接收的数据包。

步骤 5 单击**启用过滤器**。有三个复选框可用（**忽略信标**、**在客户端上过滤**、**在 SSID 上过滤**）。

- **忽略信标** - 启用或禁用对无线检测或传输的 802.11 信标的捕获。

- **在客户端上过滤** - 指定 WLAN 客户端过滤器的 MAC 地址。请注意，仅当在 802.11 接口上执行捕获时，客户端过滤器才处于活动状态。
- **在 SSID 上过滤** - 选择用于数据包捕获的 SSID 名称。

步骤 6 单击**保存设置**。更改将保存到“启动配置”。

步骤 7 单击**开始捕获**，然后单击**刷新**以获取包含以下数据的**数据包捕获状态**：

a) **当前捕获状态**
b) **数据包捕获时间**
c) **数据包捕获文件大小**

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

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

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 是免费提供的开源工具，可从 https://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 版本不适用于 WAP 设备。

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。

流到远程主机

要使用“流向远程主机”选项在 WAP 设备上启动远程捕获，请执行以下操作 :

步骤 1 依次选择**故障排除 > 数据包捕获**。

步骤 2 对于**数据包捕获方法**，单击**传输到远程主机**单选按钮。

步骤 3 在“远程捕获端口”字段使用默认端口 (2002)，或者如果使用的不是默认端口，请输入将 Wireshark 连接到 WAP 设备所需的端口号。端口范围为 1025 至 65530。

步骤 4 数据包捕获有两种模式。

- **所有无线流量** - 捕获传输的所有无线数据包。

- **流入/流出此无线接入点的流量** - 捕获从无线接入点发送或无线接入点接收的数据包。

步骤 5 接下来，选中**启用过滤器**。然后从以下选项中进行选择：

- **忽略信标** - 启用或禁用对无线检测或传输的 802.11 信标的捕获。
- **在客户端上过滤** - 指定 WLAN 客户端过滤器的 MAC 地址。请注意，仅当在 802.11 接口上执行捕获时，客户端过滤器才处于活动状态。
- **在 SSID 上过滤** - 选择用于数据包捕获的 SSID 名称。

步骤 6 如果要保存这些设置供以后使用，请单击**保存**。但是，为“数据包捕获方法”选择的“远程”不会保存。

步骤 7 单击**开始捕获**开始捕获。要停止捕获，请单击**停止捕获**。

流到CloudShark

要使用**流向 CloudShark** 选项在 WAP 设备上启动远程捕获，请执行以下操作：

步骤 1 选择**故障排除 > 数据包捕获**。

步骤 2 对于**数据包捕获方法**，请点击**流向 CloudShark** 单选按钮。

步骤 3 配置以下参数：

a) 接口 - 输入数据包捕获的捕获接口类型
b) 以太网 - 以太网端口中的 802.3 流量。
c) 无线电 1 (5GHz) / 无线电 2 (2.4GHz) - 无线电接口中的 802.11 流量
d) 持续时间 - 输入捕获持续时间（秒）。 CloudShark 无持续时间限制。默认值为 60
e) 最大文件大小 - 输入允许的最大捕获文件大小 (KB)。 此参数无大小限制。默认为 1024。

注释 CloudShark 有两种有效的帐户类型：“个人”和“企业”。“个人”和“企业”帐户类型一次可以上传的最大大小分别为 25 MB 和 150 MB。CloudShark 将根据帐户类型截断超出最大大小的部分。

f) CloudShark URL - 输入 CloudShark 的主机名。默认 URL：https://www.cloudshark.org
g) CloudShark API 密钥 - 输入您从 CloudShark 注册的有效 API 令牌

步骤 4 与 CloudShark 的通信使用 HTTPS 进行。如果要使用自签名的 SSL 证书，请选中是选项，然后点击**上传证书**上传您所签名的证书。

步骤 5 在“筛选表达式”字段中输入要捕获的协议。只有经过筛选的数据包才会传输到 CloudShark

步骤 6 有两种数据包捕获方法：

a) **所有无线流量** - 捕获所有无线数据包。
b) **发送到/来自该 AP 的流量** - 捕获从该 AP 发送的数据包或该 AP 接收的数据包。

步骤 7 点击**启用过滤器**。提供以下三个选项：

a) **忽略信标** - 允许或禁止捕获由无线电检测到或传输的 802.11 信标
b) **过滤客户端** - 指定无线局域网客户端过滤器的 MAC 地址。

注释　仅当在 802.11 接口中执行捕获时，客户端过滤器才处于活动状态。

c) **过滤 SSID** - 为数据包捕获选择一个 SSID 名称。

步骤 8 点击**保存**。更改将保存到“启动配置”。

步骤 9 点击**开始捕获**。在“数据包捕获”模式下，捕获的数据包实时传输到 CloudShark 网站。数据包捕获会在激活后继续执行，直到发生以下事件之一：

a) 捕获时间达到已配置的持续时间。

b) 捕获文件达到其最大大小。

c) 管理员停止捕获。

Wireshark

首先，下载 Wireshark 并将其安装到计算机上。可以从 https://www.wireshark.org/ 下载 Wireshark。

要启动 Microsoft Windows 版本的 Wireshark 网络分析程序，请按照以下步骤操作：

步骤 1 在计算机上启动 Wireshark 工具。

步骤 2 在菜单中，依次单击**捕获 > 选项**。系统将显示一个弹出窗口。

步骤 3 在“接口”字段，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 设备的端口号。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菜单，可用来从中选择接口。接口可以是以下类型之一：

Linux bridge interface in the wap device

```
--rpcap://[192.168.1.220]:2002/brtrunk
```

Wired LAN interface

```
-- rpcap://[192.168.1.220]:2002/eth0
```

VAP0 traffic on radio 1

```
-- rpcap://[192.168.1.220]:2002/wlan0
```

802.11 traffic

```
-- rpcap://[192.168.1.220]:2002/radio1
```

At WAP361, VAP1 ~ VAP7 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
```

At WAP150, VAP1 ~ VAP3 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3
```

最多可以同时跟踪 WAP 设备中的 4 个接口。但必须为每个接口单独启动一个 Wireshark 会话。要启动更多远程捕获会话，请重复 Wireshark 配置步骤。无需在 WAP 设备上进行任何配置。

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

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

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

以下是一些有用的显示过滤器的示例：

- 排除信标和 ACK/RTS/CTS 帧：

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

- 仅数据帧：

  wlan.fc.type == 2

- 特定 BSSID 的流量：

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

- 特定客户端收发的所有流量：

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

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

不在端口范围 58000-58004

出于性能和安全考虑，数据包捕获模式不会保存在 WAP 设备的 NVRAM 中。如果重置 WAP 设备，捕获模式会被禁用，届时您必须重新启用，才能恢复捕获流量。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（通常所有无线接入点每 100ms 发送一次）。虽然 Wireshark 支持信标帧的显示过滤器，但不支持捕获过滤器，无法阻止 WAP 设备将捕获的信标数据包转发到 Wireshark 工具。为减少捕获 802.11 信标对性能的影响，请禁用捕获信标模式。

数据包捕获文件下载

可以将捕获文件通过 TFTP 下载到配置的 TFTP 服务器，或通过 HTTP/HTTPS 下载到计算机。触发捕获文件下载命令后，捕获自动停止。

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

要使用 TFTP 下载数据包捕获文件，请执行以下步骤：

步骤 1 单击**下载至 TFTP 服务器**。

步骤 2 在提供的字段中，指定 TFTP 服务器 IPv4 地址。

步骤 3 如果不使用默认设置，请输入要下载的 TFTP 服务器文件名。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 4 单击**下载**。

使用 HTTP

要使用 HTTP 下载数据包捕获文件，请执行以下步骤：

步骤 1 单击**下载至此设备**。系统将显示确认弹出消息。

步骤 2 单击**确定**。随后会出现一个弹出窗口，请在其中选择一个用于保存文件的网络位置。

支持信息

此“支持信息”页显示 CPU 和 RAM 的状态。

要记录并显示 CPU/RAM 活动，请按照以下步骤操作：

步骤 1 依次选择**故障排除 > 支持信息**。

步骤 2 单击 **CPU** - 记录并显示 CPU 活动的设备。要停止记录，请再次单击 **CPU**。

步骤 3 单击 **RAM** - 记录并显示 RAM 活动的设备。要停止记录，请再次单击 **RAM**。

该图表显示 CPU/RAM 状态如下：

- 蓝线表示 CPU 活动。
- 红线表示 RAM 活动。
- 第一行图表每 1 秒更新一次。它将在 60 秒内显示 CPU/RAM 活动。
- 第二行图表每 5 秒更新一次。它将在 5 分钟内显示 CPU/RAM 活动。

步骤 4 单击**保存**。

下载 CPU/RAM 数据

使用“支持信息”页在选定的时间内下载 CPU/RAM 活动。可以向技术支持人员提供此文本文件，协助他们排除故障问题。要下载 CPU/RAM 数据，请执行以下操作：

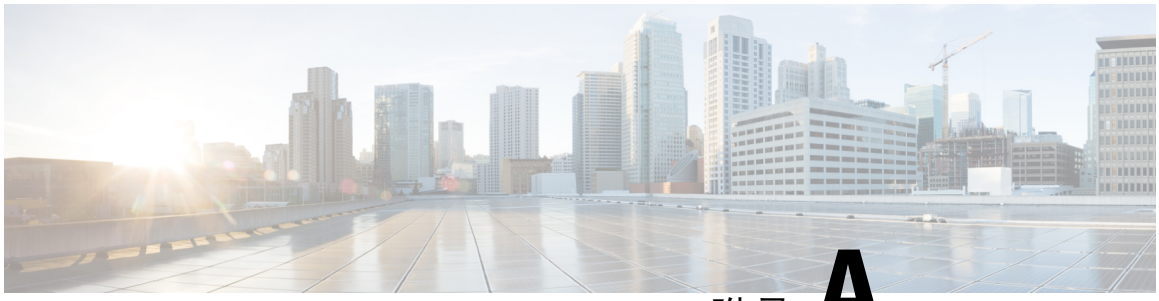
步骤 1 依次选择**故障排除 > 支持信息**。

步骤 2 在“下载数据”部分，选中**启用**启用下载。

步骤 3 选择要执行下载的时间：**今天**、**过去 7 天**、**过去 30 天**、**全部**、**自定义**。

步骤 4 使用 yyyy-mm-dd 完成**至**和**自**字段，然后使用 hh:mm:ss 设置时间。

步骤 5 单击**下载**以根据当前系统设置生成文件。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。



附录 A

取消身份验证消息原因代码

本附录包含以下部分：

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。系统配置>通知>查看系统日志。

有关更多信息，请参阅 取消身份验证原因代码表， 第 119 页。

取消身份验证原因代码表

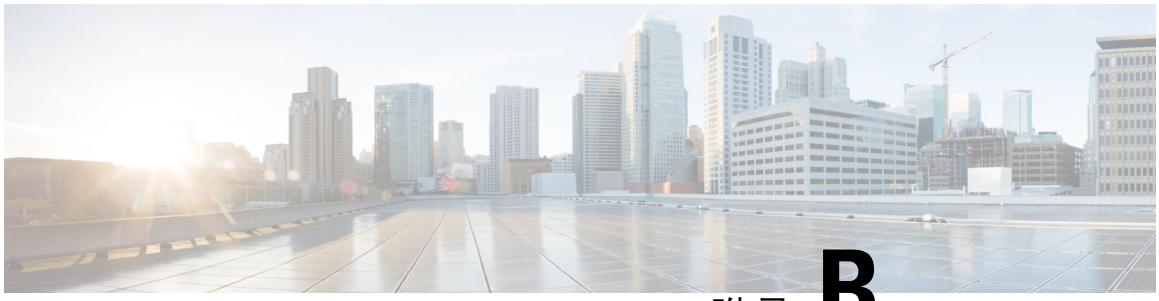
下表说明了取消身份验证原因代码。

表 4: 取消身份验证原因代码表

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

取消身份验证消息原因代码

原因代码	含义
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	保留
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



附录 B

快速索引

本附录包含以下部分：

快速索引

支持

思科支持社区	http://www.cisco.com/go/smallbizsupport
思科支持和资源	http://www.cisco.com/go/smallbizhelp
电话支持联系人名单	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
思科固件下载	http://www.cisco.com/go/smallbizfirmware 选择链接，可下载相应思科产品的固件。无需登录。
思科开源请求	如果希望接收在适用的免费/开源许可证（例如 GNU 宽松/通用公共许可证）下您有权获得的源代码副本，请将您的请求发送至：external-opensource-requests@cisco.com。 请在您的请求中提供思科产品名称、版本和 18 位参考号（例如：7XEEX17D99-3X49X08 1），此参考号可以在产品的开源文档中找到。
思科 WAP581 管理指南	http://www.cisco.com/go/500_wap_resources
思科电源适配器	http://www.cisco.com/go/wap_accessories

快速索引