用户手册

Allen-Bradley

Stratix 5100 无线接入点 / 工作组网桥

产品目录号 1783-WAPAK9、 1783-WAPEK9、 1783-WAPCK9、 1783-WAPZK9

重要用户须知

在安装、配置、操作或维护设备之前，请仔细阅读本文档及“其他资源”部分列出的文档，了解设备的安装、配置和操作信息。除了所有适用的规范、法律和标准的要求之外，用户还必须熟悉安装和接线说明。

安装、调节、投入使用、操作、装配、拆卸和维护等活动均要求由经过适当培训的人员遵照适用法规执行。

如果设备的使用方式与制造商指定的方式不同，则设备提供的保护功能可能会受到影响。

对于由于使用或应用此设备而导致的任何间接损失或连带损失，罗克韦尔自动化公司概不承担任何责任。

本手册中的示例和图表仅供说明之用。由于任何特定的安装都存在很多可变因素和要求，罗克韦尔自动化公司对于依据这些示例和图表所进行的实际应用不承担任何责任和义务。

对于因使用本手册中所述信息、电路、设备或软件而引起的专利问题，罗克韦尔自动化不承担任何责任。

未经罗克韦尔自动化公司的书面许可，禁止复制本手册的全部或部分内容。

在本手册中，在必要时我们使用注意事项来提醒您需要注意的安全问题。

	**警告：**指明在危险环境下可能导致爆炸进而造成人身伤害或死亡、财产损坏或经济损失的行为或情况的信息。
	**注意：**用于标识可能导致人员伤亡、物品损坏或经济损失的行为或情况。注意事项能帮助您发现危险情况、避免发生危险，并了解可能的后果。
重要事项	指明成功应用和理解产品的关键信息。

标签可能位于设备上或设备内，可提供特定警示。

	**电击危险：**位于设备 (例如，变频器或电机) 表面或内部的标签，提醒相关人员可能存在危险电压。
	**灼伤危险：**标签可能位于设备上或设备内 (例如驱动器或电机)，提醒人们表面可能存在危险的高温。
	**闪弧危险：**标签可能位于设备上或设备内 (例如电机控制中心)，提醒人们可能出现弧闪。闪弧可导致重伤或死亡。穿戴适当的个人防护设备 (PPE)。遵守安全工作规范和个人防护设备 (PPE) 的所有法规要求。

章节 3

Stratix 5100 设备管理器配置启动

章节 4

Stratix 5100 设备管理器参数定义

访问 **Logix Designer** 中的 **Stratix 5100** 无线接入点 / 工作组网桥

章节 5

章节 6

使用命令行界面配置 Stratix 5100 WAP

章节 7

管理 WAP 访问

章节 8

配置无线电设置

章节 9

配置 多个 SSID

章节 10

配置生成树协议

章节 11

将接入点配置为本地验证器

章节 12

配置密文组

章节 13

配置验证类型

章节 14

配置 WDS 和快速 安全漫游

章节 15

配置 RADIUS 和 TACACS+ 服务器

章节 16

配置 VLAN

章节 17

配置 QoS

章节 18

配置过滤器

章节 19

配置 CDP

章节 20

配置 SNMP

章节 21

配置工作组网桥模式、中继器模式和备用接入点

章节 22

配置系统消息记录

章节 23

故障处理

附录 A

协议过滤器

附录 B

支持的 MIB

附录 C

受众

本用户手册面向安装和管理 Stratix 5100™ 无线接入点和工作组网桥的联网专家。要使用本指南，您必须具备使用思科 IOS 软件的一些经验，熟悉无线局域网的原理和术语。

本用户手册涵盖了 支持 Stratix 5100 WAP，32 Mb 平台的思科 IOS 版本 15.2(4)JAZ 及更高版本。

用途

本用户手册为您提供了安装和配置接入点所需的信息。它给出了使用思科 IOS 软件命令 (这些命令已经创建或更改，可供接入点使用) 的步骤。它不提供关于这些命令的详细信息。

有关这些命令的详细信息，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges (Cisco Aironet 接入点和网桥的思科 IOS 命令参考)，思科 IOS 版本 15.2(4)JA、 15.2(2)JB、 15.2(2)JA、12.4(25d)JA 和 12.3(8)JEE。

重要事项	使用本手册配置 Stratix 5100 WAP 之前，必须执行站点调查。 射频 (RF) 站点调查是部署无线网络的第一步，也是确保正确运行的最重要步骤。站点调查是逐个任务依次执行的过程，检查员研究设施以了解射频行为，发现射频覆盖区域，检查射频干扰，并确定无线设备的适当位置。 有关站点调查的更多信息，请参见 思科无线站点调查常见问题解答。

本用户手册给出了 Stratix 5100 WAP 上罗克韦尔自动化基于 Web 的配置软件 (Stratix 5100 设备管理器) 的概览。它还给出了配置实例。

章节安排

本用户手册分成以下章节。

项目	描述
第 1 章 Stratix 5100 无线接入点 / 工作组网桥使用入门	给出了 Stratix 5100 无线接入点 / 工作组网桥的概览，包括其功能和网络配置
第 2 章安装 Stratix 5100 无线接入点 / 工作组网桥	给出了如何安装接入点的详细信息。
第 3 章 Stratix 5100 设备管理器配置启动	介绍了如何使用 Web 浏览器界面配置接入点。
第 6 章使用命令行界面配置 Stratix 5100 WAP	介绍了如何使用命令行界面 (CLI) 配置接入点。
第 7 章管理 WAP 访问	介绍了如何执行一次性操作管理接入点，例如，防止未授权访问接入点、设置系统日期和时间以及设置系统名称和提示。
第 8 章配置无线电设置	介绍了如何配置接入点无线电设备的设置，例如，无线电网络中的角色、发射功率、通道设置等。
第 9 章配置 多个 SSID	介绍了如何配置和管理接入点上的多个服务集标识符 (SSID) 和多个基本 SSID (BSSID)。可在接入点上配置多达 16 个 SSID 和多达 8 个 BSSID。
第 10 章配置生成树协议	描述了如何配置接入点、网桥或工作在网桥模式的接入点的生成树协议 (STP)。 STP 防止在用户网络中出现网桥循环。
第 11 章将接入点配置为本地验证器	介绍了如何配置接入点，令其充当无线局域网的本地 RADIUS 服务器。如果到主 RADIUS 服务器的 WAN 连接失败，接入点充当备用服务器对无线设备进行验证。
第 12 章配置密文组	介绍了如何配置使用验证密钥管理、有线等效加密 (WEP) 及包括 MIC、 CMIC、 TKIP、 CKIP 和广播密钥旋转在内的 WEP 功能所需的密文组。
第 13 章配置验证类型	介绍了如何配置接入点上的验证类型。客户端设备使用以下验证方法联网。
第 14 章配置 WDS 和快速 安全漫游	介绍了如何配置无线接入点参与 WDS，允许快速重关联漫游客户端服务，并参与无线电管理。
第 15 章配置 RADIUS 和 TACACS+ 服务器	介绍了如何启用和配置 RADIUS 和增强型终端访问控制器访问控制系统 (TACACS+)，使得可通过验证和授权过程提供详细的结算信息和灵活的管理控制。
第 16 章配置 VLAN	介绍了如何配置接入点与有线局域网上创建的 VLAN 交互。
第 17 章配置 QoS	介绍了如何通过 Web 浏览器界面配置和管理接入点上的 MAC 地址、 IP 和以太网类型过滤器。
第 18 章配置过滤器	介绍了如何通过 Web 浏览器界面配置和管理接入点上的 MAC 地址、 IP 和以太网类型过滤器。
第 19 章配置 CDP	介绍了如何配置接入点的思科发现协议 (CDP)。 CDP 是可在所有思科网络设备上运行的设备发现协议。
第 20 章配置 SNMP	介绍了如何配置接入点上的简单网络管理协议 (SNMP)。
第 21 章配置工作组网桥模式、中继器模式和备用接入点	介绍了如何将接入点配置为工作组网桥。
第 22 章配置系统消息记录	介绍了如何配置接入点上的系统消息记录。
第 23 章故障处理	给出了接入点基本问题的故障处理步骤。
附录 A 协议过滤器	列出了可在接入点上筛选的某些协议。
附录 B 支持的 MIB	列出了接入点对于该版软件支持的简单网络管理协议 (SNMP) 管理信息库 (MIB)。
附录 C 错误和事件消息	列出了 CLI 错误和事件消息，并给出每条消息的解释和建议的操作。

惯例

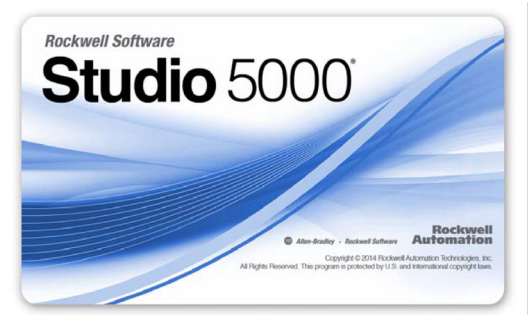
Stratix 5100 无线接入点 / 工作组网桥在本文档中称为 Stratix 5100 WAP、 WAP、接入点或工作组网桥。本出版物使用以下惯例来阐述指令和信息。

命令说明使用以下惯例：

- 方括号 ([ ]) 表示可选元素。
- 括号 ({ }) 对必选项进行分组，竖线 (|) 分隔可选元素。
- 方括号内的括号和竖线 ([{ | }]) 表示可选元素内的必选项。
- 以**屏幕**字体显示终端会话和系统。
- 斜体表示用户输入。

Studio 5000 环境

Studio 5000 工程和设计环境将工程和设计要素组合在一个通用的环境中。 Studio 5000 环境中的第一要素是 Logix Designer 应用程序。Logix Designer 应用程序是 RSLogix™ 5000 软件的换代产品，将继续作为 Logix 5000™ 控制器的编程产品，用于离散、过程、批次、运动控制、安全和基于驱动器的各种解决方案。



Studio5000 环境是未来罗克韦尔自动化工程设计工具和功能的基础。它是设计工程师开发控制系统全部元件所需的一站式软件。

其他资源

这些文档包含有关罗克韦尔自动化相关产品的附加信息。

资源	描述
http://www.Cisco.com	提供参考手册，例如， Configuration Professional Software User Manual (配置专业软件用户手册) 和 IOS CLI Reference Manual (IOS CLI 参考手册)。
使用 Cisco IOS Command-Line Interface Configuration Guide 15.3 (思科 IOS 命令行接口配置使用指南，第 15.3 版)	提供有关使用思科 IOS 命令行界面的全面信息。
Cisco IOS Security Command Reference for Release 12.3 (思科 IOS 安全命令参考，第 12.3 版)。	提供关于思科 IOS 安全命令的完整语法和用法信息。
http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html	与思科 ASA 系列有关的整套文档的位置。
Cisco IOS 15.2(4)JA Release Notes (思科 IOS 15.2(4)JA 版本说明)	适用于思科 IOS 版本 15.2(4)JA 的思科 Aironet 接入点和网桥的版本说明
Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges (思科 Aironet 接入点和网桥的思科 IOS 命令参考)	描述了用于配置和管理接入点、网桥及无线局域网的思科 IOS 命令。命令按字母顺序列出。

资源	描述
思科无线站点调查常见问题解答	提供有关如何进行站点调查的说明。射频 (RF) 站点调查是部署无线网络的第一步，也是实现有效站点配置的最重要步骤。
Industrial Automation Wiring and Grounding Guidelines (工业自动化布线和接地指南，出版号：1770-4.1)	提供安装罗克韦尔自动化工业系统的通用准则。
产品认证网站， http://www.ab.com	提供符合性声明、认证和其他认证的详细信息。

您可访问 http://www.rockwellautomation.com/literature/ 查看或下载以上出版物。如需订购技术文档的纸印本，请联系当地的 Allen-Bradley 分销商或罗克韦尔自动化销售代表。

罗克韦尔自动化支持

罗克韦尔自动化公司在网站上提供可帮助您使用其产品的技术信息。您可访问 http://www.rockwellautomation.com/support，获取技术和应用说明、示例代码和软件补丁包的链接。您也可访问支持中心 https://rockwellautomation.custhelp.com/ 获取软件更新，查找支持对话与支持论坛、技术信息、 FAQ，并登记参与产品通知更新。

此外，我们还提供多种安装、配置和故障处理支持计划。有关详细信息，请与本地分销商或罗克韦尔自动化销售代表联系，或者访问 http://www.rockwellautomation.com/services/online-phone。

Stratix 5100 无线接入点 / 工作组网桥使用入门

本章提供了 Stratix 5100 无线接入点 / 工作组网桥 (WAP) 的概览，包括其特性和网络配置。 Stratix 5100 无线接入点 / 工作组网桥在本文档中称为 Stratix 5100 WAP、 WAP、单元或接入点。

Stratix 5100 无线接入点 / 工作组网桥提供了一个安全、价格合理且易于使用的无线局域网解决方案，它将移动性和灵活性与联网专家需要的企业级功能完美结合在一起。凭借基于思科 IOS 软件的管理系统，Stratix 5100 WAP 可作为无线局域网收发器，其通过 Wi-Fi 认证并与以下标准兼容：

- 802.11a、 b、 g、 n
- 802.11b
- 802.11g
- pre-802.11n

Stratix 5100 WAP 提供双频段无线电装置 (2.4 GHz 和 5 GHz) 和外置天线。这些接入点与主流 802.11n 客户端具有完全的互操作性，并支持与其他接入点和无线控制器进行混合部署。

接入点作为无线和有线网络之间的连接点，或作为一个独立无线网络的中心点。在大型设施中，位于接入点无线电范围内的无线用户可以在整个设施内漫游，同时保持对网络无缝、不间断的访问。

Stratix 5100 WAP 支持高性能频谱智能技术，在为客户端提供服务时，在可部署的距离内以高可靠性保持三个空间流速率。无线接入点可实现出色的可靠性和整体无线性能。接入点为单机 (自发) 配置。

以下是 Stratix 5100 WAP 的一些特性。

- 2.4 GHz 和 5 GHz 802.11n 无线电装置，带双频段天线
- Wi-Fi 标准 802.11 a/b/g/n
- 3TX (发送) x 4RX (接收)
- 3 个空间流， 450 Mbps PHY 速率
- 吞吐量、转发和过滤性能扫描满足 3 个空间流， 450 Mbps 数据传输速率的要求
- 最大数据传输速率为 450 Mbps
- 提供工作组网桥 (WGB) 支持，将仅具备有线连接的客户端连接至无线网络
- 频带选择
- 思科波束成形技术用于.11ag 客户端、单空间流和双空间流客户端
- 根据 802.11n 标准，支持显式压缩波束成形 (ECBF) 技术的无线电硬件
- 外部天线
- CDP (思科发现协议)
- 处理子系统 (包括 CPU 和内存) 和支持的无线电硬件
  - 网络管理
  - 32 MB 非易失性内存
  - 安全功能
  - SNMP 社区
  - 网络配置
  - 安全
  - 安全外壳 (SSH)
- ClientLink 2.0 (128 个客户端)
- 视频流
- 非法 AP 检测

监管域

Stratix 5100 支持以下监管域。

- 1783-WAPAK9 (北美)
- 1783-WAPZK9 (澳大利亚 / 新西兰)
- 1783-WAPEK9 (欧盟)
- 1783-WAPCK9 (中国)

配置接入点

可使用以下方法配置和监视无线设备。

- 命令行界面 (CLI)
- Stratix 5100 WAP 设备管理器，基于浏览器的管理系统
- 简单网络管理协议 (SNMP)

管理选项

可通过以下接口使用无线设备管理系统。

- 一种通过 Web 浏览器使用的 Web 浏览器界面。

  有关 Web 浏览器界面的详细说明，请参见第 49 页的 “Stratix 5100 设备管理器配置启动 ”。

- 通过控制台端口或 Telnet 会话使用的思科 IOS 命令行接口 (CLI)。
- 有关 CLI 的更多信息，请参见第 195 页的 “ 使用命令行界面配置 Stratix 5100 WAP”。
- 简单网络管理协议 (SNMP). 第 459 页的 “ 配置 SNMP” 阐述了如何配置无线设备来实现 SNMP 管理。

漫游客户端设备

如果在无线局域网中有多个无线设备，则无线客户端设备可以从一个无线设备漫游到另一个无线设备。漫游功能取决于信号质量，而不是邻近度。当客户端的信号质量下降时，它漫游到接入点。

无线局域网用户有时担心客户端设备保持关联到一个远端接入点，而不是漫游到一个更近的接入点。但是，如果到远端接入点的客户端信号保持良好，且信号质量很高，则客户端不会漫游到一个更近的接入点。不断检查是否有更近的接入点，这使操作变得低效，而且附加的无线电流量会缩减无线局域网上的吞吐量。

通过使用思科集中式密钥管理 (CCKM) 和一个提供 WDS 的设备，客户端设备可以从一个接入点快速漫游到另一个接入点，速度如此之快，使得在语音或其他时间敏感应用中几乎感觉不到延迟。

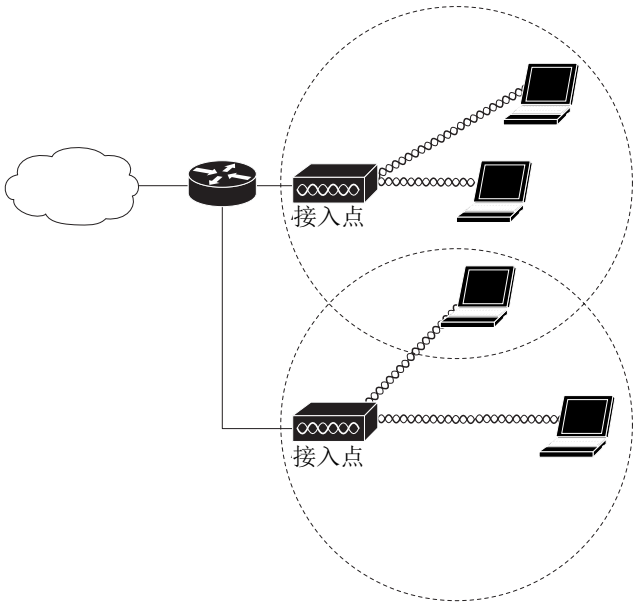
网络配置实例

本章节描述了接入点在公共无线网络配置中的作用。接入点的默认配置为一个连接至有线局域网的根单元，或作为无线网络中的中央单元。可将接入点配置为中继器接入点、网桥和工作组网桥。这些作用需要特定的配置。

根接入点

直接连接到有线局域网的接入点为无线用户提供一个连接点。如果有多个接入点连接到局域网，则用户可从一个设施区漫游到另一个设施区，而不会丢失与网络的连接。当用户移出一个接入点的范围时，它们会自动通过另一个接入点连接到网络 (关联)。漫游过程对用户而言是无缝且透明的。下图显示了在有线局域网上作为根单元的接入点。

图 1 - 在有线局域网上作为根单元的接入点



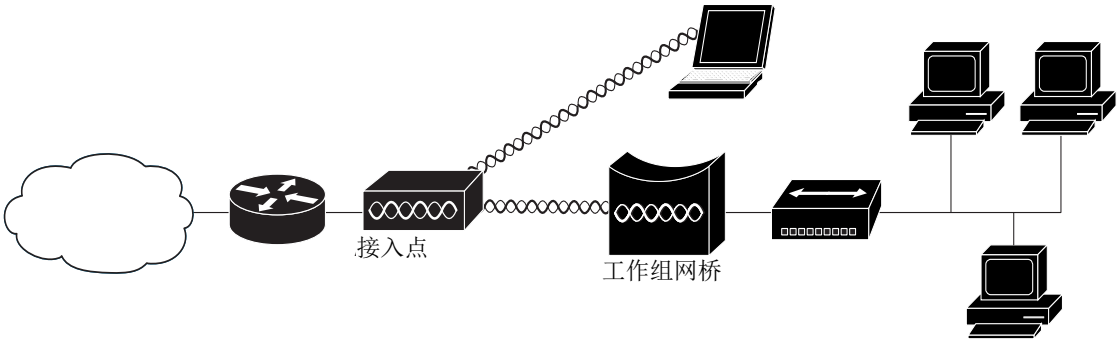
工作组网桥

可以将接入点配置为工作组网桥。在工作组网桥模式下，单元作为客户端关联到另一个接入点，并为连接到其以太网端口的设备提供一个网络连接。例如，如果您需要为一组网络打印机提供无线连接，您可将打印机连接到集线器或交换机，再将集线器或交换机连接到接入点以太网端口，并将接入点配置为工作组网桥。工作组网桥关联到网络上的一个接入点。

如果接入点有多个无线电设备，任何一个无线设备均可在工作组网桥模式下工作，但一次只有一个无线电设备是 WGB。

下图显示了配置为工作组网桥的接入点。有关将接入点配置为工作组网桥的信息，请参见第 473 页的 “ 工作组网桥模式 ” 和第 473 页的 “ 工作组网桥模式 ”。

图 2 - 作为工作组网桥的接入点



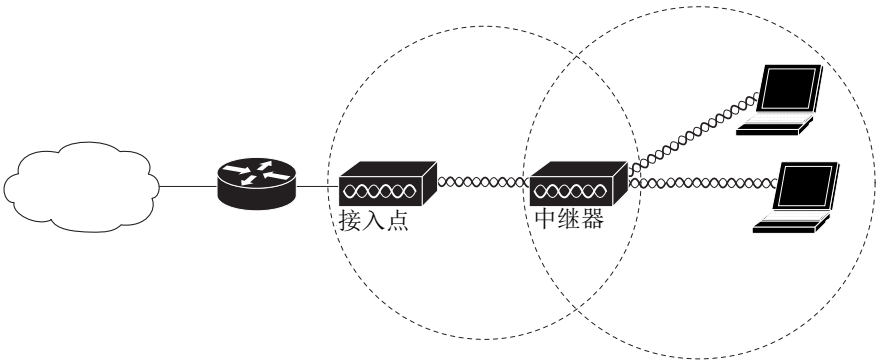
中继器接入点

可将接入点配置为一个独立的中继器，以扩展基础设施的范围或消除阻止无线电通信的障碍。中继器通过将数据包发送至另一个中继器或连接到有线局域网接入点，在无线用户和有线局域网之间转发流量。数据通过能为客户端提供最佳性能的路由进行发送。

有关如何将接入点设为中继器的说明，请参见第 473 页的 “ 配置工作组网桥模式、中继器模式和备用接入点 ”。

提示 非罗克韦尔自动化或思科制造的客户端设备与中继器接入点通信有困难。

图 3 - 作为中继器的接入点



网桥

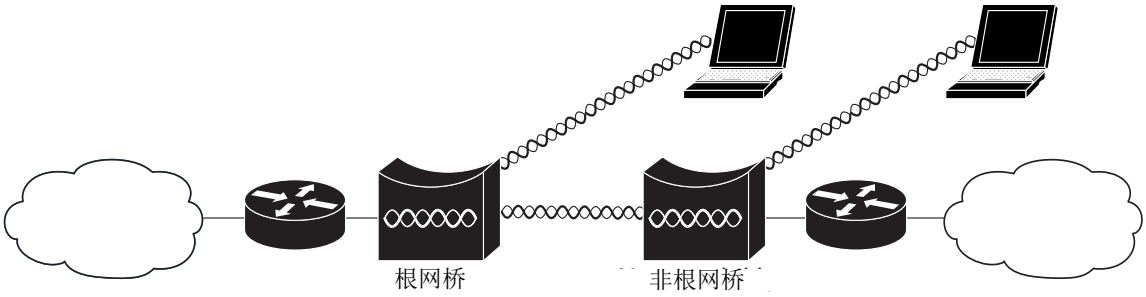
Stratix 5100 接入点可配置为根或非根网桥。当发挥这一作用时，接入点建立与非根网桥的无线链路。流量通过链路传送到有线局域网。作为根和非根网桥的接入点可配置为接受来自客户端的关联。

- 第 27 页的图 4 显示了配置为带客户端的根网桥的接入点。
- 第 27 页的图 4 显示了配置为根和非根网桥的两个接入点，两个接入点均接受客户端关联。

有关如何将接入点设为网桥的说明，请参见第 255 页的 “ 配置无线电设置 ”。

当在单点对多点配置中使用无线网桥时，吞吐量下降，具体取决于与根网桥关联的非根网桥的数目。在点对点链路中，最大吞吐量约为 25 Mbps。添加三个网桥，形成一个单点对多点网络，将吞吐量下降至约 12.5 Mbps。

图 4 - 作为带客户端的根和非根网桥的接入点



拆开 WAP 的包装

要拆开接入点的包装，按以下步骤操作：

1. 拆开包装，从装运箱中取出接入点和附属套件。
2. 将所有包装材料放回装运箱，保存以备后用。
3. 确认您已收到以下所列物品。
   - Stratix 5100 无线接入点 / 工作组网桥
   - 安装支架，含螺丝
   - 电源适配器
   - 4 根 Wi-Fi 天线
   - 控制台电缆

   如有任何物品丢失或损坏，请联系罗克韦尔自动化，具体参见本手册封底上的罗克韦尔自动化支持。

随 WAP 发货的物品

以下物品随 WAP 发货。

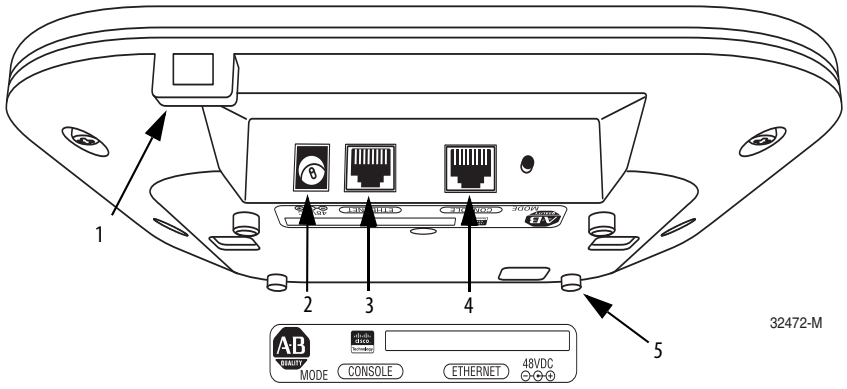
项目	描述
Stratix 5100 无线接入点 / 工作组网桥	1783-WAPAK9、 1783-WAPEK9、 1783-WAPCK9、 1783-WAPZK9
安装支架，含螺丝	AIR-AP-BRACKET-2
电源适配器	AIR-PWR-B 输入： 100…240 50/60 Hz VAC 输出： 48 V DC， 380 mA
4 根 Wi-Fi 天线	AIR-ANT2524DG-R
控制台电缆	思科零件号 72-3383-01. Rev. A2

安装 Stratix 5100 无线接入点 / 工作组网桥

本章给出了如何安装和配置 Stratix 5100 无线接入点 / 工作组网桥的基本说明。

端口和连接

端口和连接端位于接入点底部。



项目	描述
1	安全搭扣
2	电源连接
3	千兆以太网端口
4	控制台端口
5	安装支架

Stratix 5100 WAP 技术参数

下表列出了 Stratix 5100 无线接入点 / 工作组网桥的技术参数。

表 1 - Stratix 5100 无线接入点 / 工作组网桥技术参数

类别	技术参数
尺寸 (LxWxD)	22.04 x 22.04 x 4.67 cm (8.68 x 8.68 x 1.84 in)
重量	1.22 kg (2.7 lb)
工作温度	-20 ……
存储温度	-30 … 85 °C (-22 … 185 °F)
湿度	10 … 90% 无凝露
电源额定值	输入：100…240 50/60 Hz VAC 输出：48 V DC， 350 mA
天线	外部
合规性	符合 UL 2043 标准 (用于安装在建筑物的空气处理场所 (如吊顶上方) 中的产品)。
最大功率和通道设置	监管域中允许的最大功率和通道数。请参见思科 Aironet 轻型接入点的通道和最大功率设置。可在 Cisco.com 上下载本文档。

以太网电缆建议

对于 10/100 MB 设备，使用 CAT-5e 电缆时， Stratix 5100 WAP 能很好地运行；对于 1 GB 设备，我们建议使用 CAT-6a 电缆。

外部天线

Stratix 5100 无线接入点 / 工作组网桥在顶部有外置天线连接器和一个状态指示灯。天线坚固耐用，用于工业用途，可在医院、工厂、仓库和需要更大工作温度范围的其他场所使用。外置天线支持在符合 NEMA 标准的机壳内安装，可在最苛刻的环境下使用。

Stratix 5100 WAP 最多可配置四个外部双频偶极天线，并配有 2.4 GHz 和 5 GHz 双频无线电设备 (采用具有三个空间流的 3 x 4 多输入 / 多输出 (MIMO) 配置)。无线电设备和天线通过通用双频射频接口支持频段 2400 ... 2500 MHz 和 5150 ... 5850 MHz。

Stratix 5100 WAP 支持以下思科天线：

图 5 - 支持的思科天线

天线 (思科零件号)	天线增益 (dBi)		要在 CLI 接口中配置的天线增益参数 (dBi)		描述
	2.4 GHz	5 GHz	2.4 GHz	5 GHz	
AIR-ANT2524DG-R (随同产品发货)	2	4	4	8	双谐振灰色偶极天线
AIR-ANT2524 V4C-R	3	4	4	8	吊顶式双谐振全向天线(1)
AIR-ANT2544 V4M-R	4	4	8	8	双谐振全向天线 (1)
AIR-ANT2566P4W-R	6	6	8	8	双谐振定向天线 (1)

(1) 四件式 (4 根天线引线电缆)

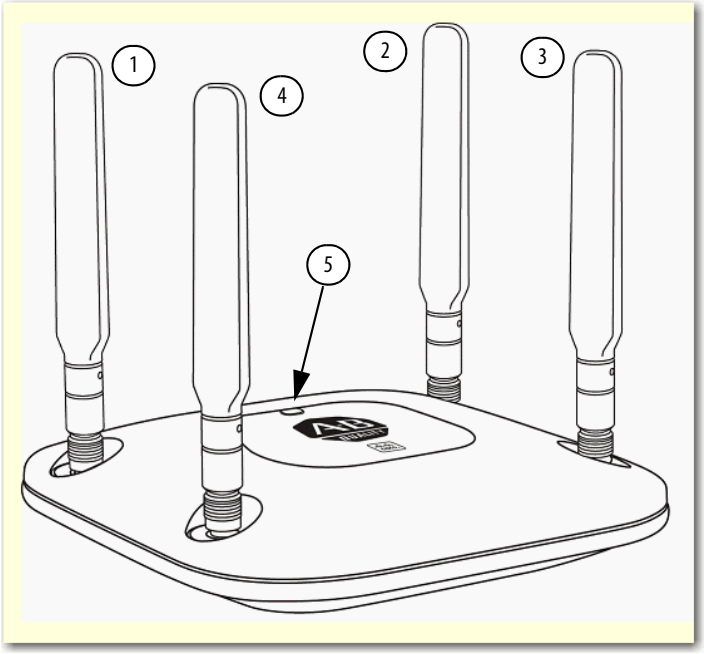
重要事项 该表提供了为获得低于适用监管限制的总输出功率等级 (eirp)，对设备进行初始配置时在命令行接口 (CLI) 中输入的每根天线的天线增益参数。不正确的配置可能导致输出功率等级 (eirp) 超出监管限制。

天线电缆延长建议

保持天线电缆布线尽可能短。思科提供低损耗 (LL) 和超低损耗 (ULL) 电缆，它们具有与 Times Microwave LMR-400 和 LMR-600 相同的特性。钻电缆孔时，应考虑连接器钻头规格，通常为 15.8750 毫米 (5/8 英寸)。

思科电缆上印有零件号 AIR-CAB (Aironet 电缆) 及电缆长度。例如，带有 RP-TNC 连接器、长度为 20 ft 的 LL 电缆为 Cisco AIR-CAB-020LL-R 电缆。这些重型黑色电缆并非 Plenum 等级电缆，主要应用于制造领域。

图 6 - 接入点 天线连接



1	天线连接器 A	4	天线连接器 D
2	天线连接器 B	5	状态指示灯
3	天线连接器 C		

Stratix 5100 WAP 最多可配置四个外部双频偶极天线，并配有 2.4 GHz 和 5 GHz 双频无线电装置 (采用具有三个空间流的 3 x 4 MIMO 配置)。无线电设备和天线通过通用双频射频接口支持频段 2400 ... 2500 MHz 和 5150 ... 5850 MHz。以下是外置双频段偶极子天线的特性：

- 在接入点的顶部有四个 RP-TNC 天线连接器
- 3 个发送和 4 个接收天线

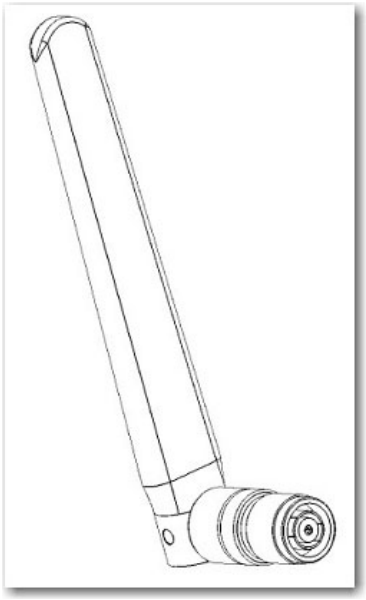
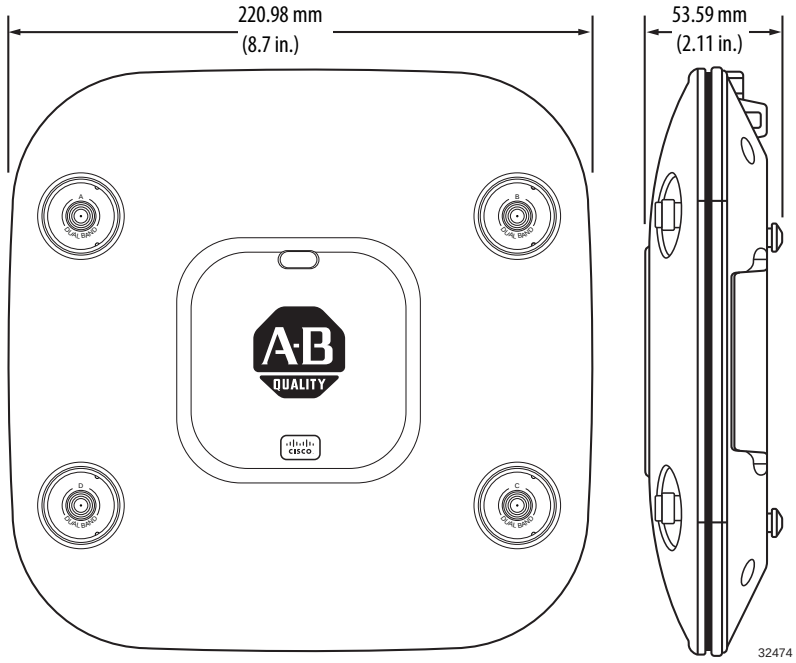


表 2 - 双频段偶极子天线 (AIR-ANT2524DG-R) 技术参数

参数	描述
天线类型	双频段偶极子
工作频率范围	2400…2500 MHz
标称输入阻抗	50 Ω
VSWR	小于 2:1
峰值增益 @ 2.4 GHz	2 dBi
峰值增益 @ 5 GHz	4 dBi
俯仰平面 3dB 波束宽度 @ 2.4 GHz	63°
俯仰平面 3dB 波束宽度 @ 5 GHz	39°
连接器类型	RP-TNC 插头
天线长度	168.5 mm (6.63 in.)
天线宽度	21 mm (0.83 in.)
天线罩长度	124 mm (4.88 in.)
重量	1.3 oz
工作温度	-20 ……
存储温度	-40 … 85 °C (-40 … 185 °F)

图 7 - Stratix 5100 WAP 尺寸



准备接入点

安装和部署接入点之前，要进行现场调查 (或使用现场规划工具) 来确定安装接入点的最佳位置。有关现场调查的更多信息，请参见 Cisco's Wireless Site Survey Frequently Asked Questions (思科无线现场调查常见问题)。

需要了解有关可用无线网络的下列信息：

- 接入点位置
- 接入点安装选项：吊顶下方、水平平面上或桌面上

  提示　可以在吊顶上方安装接入点，但是必须购买额外的安装零件。

  有关更多安装信息，请参见第 39 页的 " 安装接入点 "。

- 接入点电源选项：
  - 电源适配器，思科 AIR-PWR-B
  - PoE 馈电器 / 集线器

重要事项　为符合安全法规的要求，在建筑物的环境空间安装的接入点可使用 PoE 供电。

绘制显示接入点位置的现场地图，以便记录各个位置设备的 MAC 地址，并将这些地址返回给规划或管理无线网络的人员。

初始配置

第一次使用接入点 / 工作组网桥时，可使用以下方法。

- 控制台电缆和 CLI 命令。
- 通过 DHCP 获取 IP 地址，然后使用设备管理器。
- 当直接将 PC 连接至以太网端口时，将通过罗克韦尔自动化的 BOOTP 实用工具获取一个 IP 地址，然后使用设备管理器。

请参见第 52 页的 " 本地连接到 Stratix 5100 WAP 接入点 " 和第 195 页的 " 使用命令行界面配置 Stratix 5100 WAP"。

防止 WAP 损坏

为防止损坏 WAP，将设备连接到接入点时请遵循以下准则。

注意：关闭设备和无线接入点 / 工作组网桥的电源，直到完成所有连接为止。完成与接入点的所有连接前，不要开启设备。

可以在吊顶上方安装接入点，但是必须购买额外的安装零件。只有无法在吊顶下方安装时，才能将 Stratix WAP 安装在吊顶板上方。

安装 WAP

在水平表面上安装 Stratix 5100 WAP。

1. 拆开包装，从装运箱中取出接入点和附属套件。
2. 将所有包装材料放回装运箱，保存以备后用。
3. 确认您已收到以下所列物品。
   - 接入点
   - 安装支架
   - 电源适配器， Cisco AIR-PWR-B
   - 控制台电缆
   - 天线，请参见第 31 页的 “ 外部天线 ”

   如有任何物品丢失或损坏，请联系罗克韦尔自动化，请参见本手册封底上的罗克韦尔自动化支持。

安装该单元需要的其他物品：

- 防 ESD 的接线和腕带
- 以太网电缆
- 电源
- 安装螺丝
- 接地线

IDF 柜 (电信或其他电气设备)

在其他电气或电信设备附近安装 WAP 时，请将所有接线和金属远离天线，并且应避免将天线置于电气线路附近。请勿在天线 38 cm (15 in) 的近场区敷设电线或以太网，并且尽量不要在电气柜中安装 WAP。如果您的远程天线电缆来自电气柜，则当地的消防和安全法规可能要求您使用 Plenum 等级的电缆。请记住安装 WAP 的最佳位置为尽可能靠近用户的位置。

有关干扰的详细信息，请参见以下出版物：

- 20 Myths of Wi-Fi Interference (关于 Wi-Fi 干扰的 20 个误区)
- Wireless CleanAir Deployment Guide (无线 CleanAir 部署指南)

高海拔环境

虽然在技术参数表中未定义 Stratix 5100 WAP 适用的海拔高度，但它通过了执行 25 °C @ 4572 m (77 °F @ 15,000 ft) 非运行状态下高度测试后的功能检查。此外，它还完全通过了 40 °C @ 3000 m (104 °F @ 9843 ft) 运行状态下高度测试过程中的功能测试。测试组中的所有单元都至少与一个 WLAN 客户端相连，在整个运行状态下的高度测试过程中，通过不断的 ping 测试对连续运行的通信进行监测。

公共或分布式天线系统 (DAS)

由于 Stratix 5100 WAP 天线系统的双频特性以及其本身的关键功能 (如 ClientLink 2.0 波束成形)，所以不建议将 Stratix 5100 WAP 用于分布式天线系统 (DAS)。

对于任何 DAS 上的 Wi-Fi 部署，罗克韦尔自动化公司均不担保、不认同，也不提供射频支持。

DAS 供应商和系统集成商全权负责对 DAS 产品提供支持，确保足够的射频覆盖范围并解决与射频相关的所有问题。这一支持包括但不限于确保定位精度和射频覆盖范围，解决与射频相关的漫游问题和多路径问题以及满足客户的可扩展性要求。

DAS 供应商和系统集成商负责了解已部署的 DAS 系统是否满足客户所有 Wi-Fi 设备和 DAS 系统中应用的要求。本声明包括但不限于无线局域网语音通信 (Voice over WLAN, VoWLAN) 和医疗设备。

重要事项	虽然思科技术援助中心 (TAC) 和思科现场团队并不会针对用于 DAS 的思科 WLAN 中出现的射频问题提供支持，但根据客户与思科达成的支持协议，他们确实会为思科产品中的非射频相关的问题提供支持。罗克韦尔自动化公司不会对射频问题提供支持。

为接入点接地

由于接入点归为低压设备并且不包含内部电源，因此在室内安装时并非始终需要接地。但是，还请查阅当地和国家电气规范以确认是否需要接地。

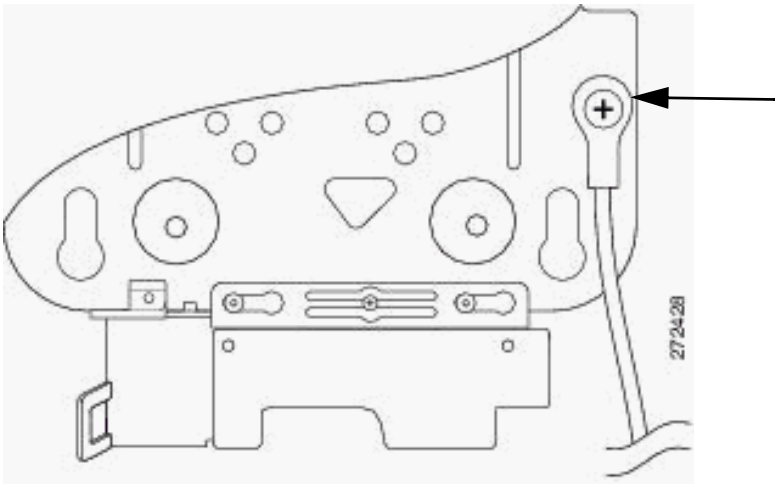
重要事项	将 WAP 安装到平面上之前，请确保将安装板接地。

根据以下步骤为接入点 / 网桥接地。

1. 找到尽可能接近接入点的合适的建筑物接地点。
2. 将用户提供的接地线连接至建筑物接地点。

   导线的最小长度为 2.5mm^2 (14 AWG)，假设电路长度为 1 ft (30.5 cm)。有关更多信息，请查阅当地电气规范。
3. 将接地线敷设到接入点。
4. 将接地线连接到合适的接地 O 形环接线片。
5. 将接地线压接或焊接到接线片上。
6. 将接地柱螺丝插入 O 形环接线片并将其安装到安装支架上。

图 8 - 将 0 型环接线片安装到接地柱



7. 使用十字螺丝刀拧紧接地螺丝。
8. 将接地柱螺丝插入 O 形环接线片并将其安装到安装支架上，如上图所示。

固定接入点

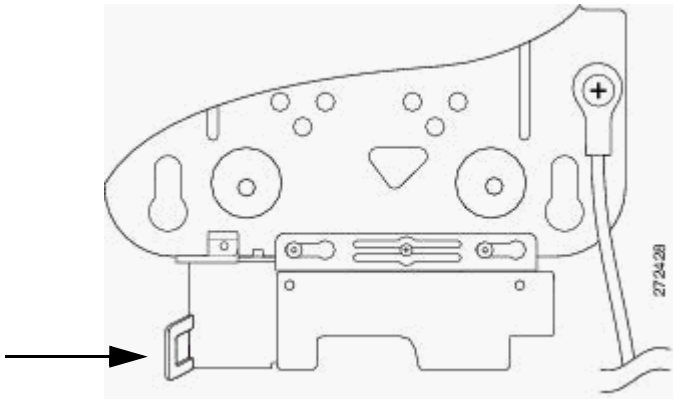
可以通过以下两种方式保护接入点：

- 用安全电缆将接入点连接到无法移动的物体。
- 用挂锁将其锁到安装板上。

将接入点固定到安装板上

使用挂锁 (用户提供) 和适配器电缆接入盖上的安全搭扣将接入点固定到安装板上。

图 9 - 安全搭扣



兼容的挂锁为 Master Lock 型号 120T 或 121T。安装支架上的电缆接入盖可盖住电缆区域 (包括电源端口、以太网端口、控制台端口和模式按钮)，以防止安装或拆卸电缆或激活模式按钮。

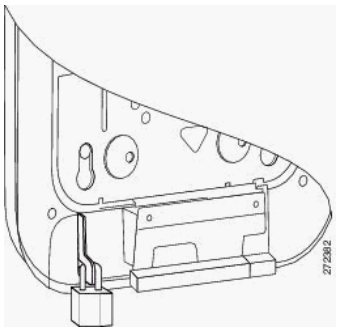
请按以下说明安装挂锁。

1. 将接入点安装到安装支架之后，将挂锁插入安全搭扣。

   提示　注意，如果将接入点安装到坚硬的吊顶上，则安装支架和吊顶之间的间隙会很小。用双手慢慢地将挂锁放入安装支架搭扣并固定。

2. 顺时针旋转挂锁并将锁柄与锁身对齐。
3. 抓住挂锁将其推向锁柄以将挂锁锁定。

图 10 - 装上挂锁。



安全电缆

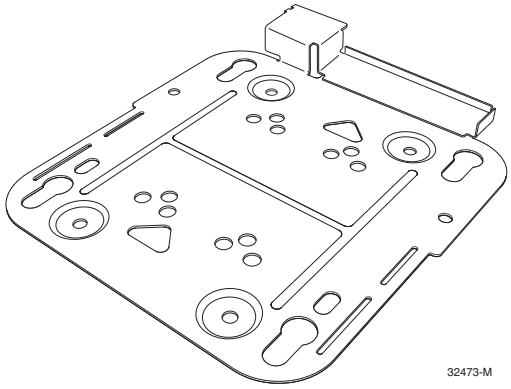
可通过将标准安全电缆 (例如 Kensington Notebook MicroSaver，型号 64068) 安装到接入点安全电缆插槽内来保护接入点。安全电缆适用于本文档所述的所有安装方式。

按照以下步骤安装安全电缆。

1. 将安全电缆缠绕在附近无法移动的物体上。
2. 将钥匙插入安全电缆锁。
3. 将安全电缆锁销插入接入点上的安全电缆插槽中。
4. 向右或向左旋转钥匙，将安全电缆锁固定到接入点上。
5. 取下钥匙。

安装接入点

Stratix 5100 WAP 标配一个矮型接入点安装支架：AIR-AP-BRACKET-1。该支架可在水平表面上齐平安装，或直接安装到天花板的龙骨上。



以下步骤介绍了如何使用安装支架 (AIR-AP-BRACKET-1) 在厚度 19.05 mm (3/4 in.) 的天花板上，或者使用相应的紧固件在更厚的胶合板上安装接入点。

提示 天线在竖直方向时接入点性能最好。

请按照以下步骤将接入点安装到坚硬的吊顶或墙壁上。

1. 将安装支架置于想要安装接入点的平面上。
2. 将安装支架作为模板来标记支架上安装孔 (1) 的位置。

图 11 - WAP 安装支架

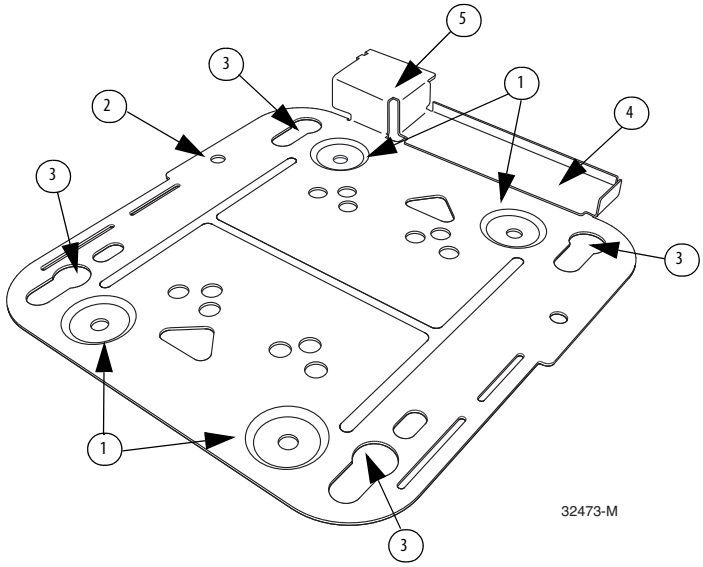


表 3 - 安装支架描述

1	壁式安装位置	4	电缆接入盖
2	接地柱	5	安全搭扣
3	接入点附件插槽		

提示　标记壁式安装的全部四个位置。确保安装牢固。使用合适的紧固件安装接入点并且使用的紧固件不能少于四个。

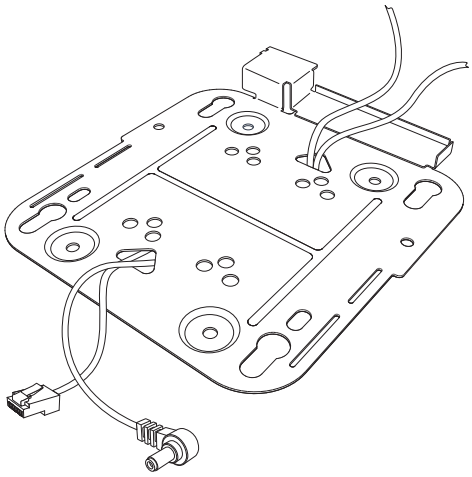
重要事项　采用吊顶安装方式时，切勿使用塑料墙锚或安装支架上的锁孔插槽进行安装。在坚硬的吊顶上安装接入点时，请使用四个至少能够承受 9 kg (20 lbs) 拔出力的紧固件。

3. 使用 3.4772 mm (0.1360 in) 钻头在标记的安装孔位置 (1) 钻出导向孔。

   提示　导向孔径根据要紧固的材料和厚度而定。对材料进行测试，确定最适合安装应用的孔径。

4. (可选) 在安装支架电缆接入盖附近下方钻出或切出电缆接入孔，孔的大小要足以容纳以太网电缆、建筑物接地线和电源电缆。
5. 将电缆拉入孔内大约 22.86 cm (9.00 in)。
6. 将电缆从一个通孔穿入，然后从另一个通孔穿出。

图 12 - 敷设以太网和电源电缆



7. (可选) 使用接地螺丝将建筑物接地线连接到安装支架上。

有关常规接地说明，请参见第 37 页的 “ 为接入点接地 ”。

8. 将安装支架的安装孔 (锯齿朝下) 放在导向孔上。
9. 将紧固件插入各个安装孔并拧紧。
10. 将以太网和电源电缆连接到接入点。
11. 将接入点支脚与安装板上大部分锁孔安装插槽对齐。
12. 放置正确时，电缆接入盖正好嵌入接入点连接器凹槽。
13. 将接入点轻轻地滑到安装支架锁孔插槽中，直到卡入到位。

Stratix 5100 接入点可在多种配置中安装，包括在坚固的天花板或墙壁、电气或网络盒以及吊顶和吊顶上方安装。 Stratix 5100 接入点配备了一个水平安装支架，该支架可用于在坚固的天花板或墙壁上安装以及需要在电气或网络盒上进行安装的应用。

接入点间距建议

如果您已拥有一台 Wi-Fi 设备 (如 WAP) 并且要在附近使用相同或不同通道的另一台 WAP，则两台 WAP 之间应保持 6 英尺 (2 米) 左右的距离。该建议距离的前提是两台设备在免执照共用频段工作，并且未发出超过 23 dB (即 200 mW) 射频能量。如果所用设备的功率更高，则距离也应更大。应避免 WAP 或不同 WAP 的天线聚集在一起，因为这样可能会降低性能。

如果有其他设备发射射频能量，请遵循以下说明。

1. 将各个设备移动或分隔至合理的距离。

如果各个设备在相同频率范围内运行，这就显得尤为重要；例如，跳频的早期 WAP 或刚好在低于或高于 2.4 Ghz 和 5 GHz 的频段运行的其他设备。

2. 检查是否存在干扰。
3. 在重载应用的情况下同时对两种设备进行测试。
4. 分别确定各个系统的特性，查看是否存在性能下降的情况。

在坚固的天花板或墙壁上安装接入点

以下步骤介绍了如何使用通用安装支架 (AIR-AP-BRACKET-2) 在厚度 19.05 mm (0.75 in.) 的天花板上，或者使用足够的紧固件在更厚的胶合板上安装接入点。

提示　当在水平表面如桌面或天花板上安装接入点时，接入点的性能最佳。对于如语音、位置和非法接入点检测等高级功能，强烈推荐在天花板上安装。

可通过以下网址 http://www.cisco.com/en/US/docs/wireless/access_point/mounting/guide/apmount.html#wp44461 获取更多安装信息。

支架和夹具

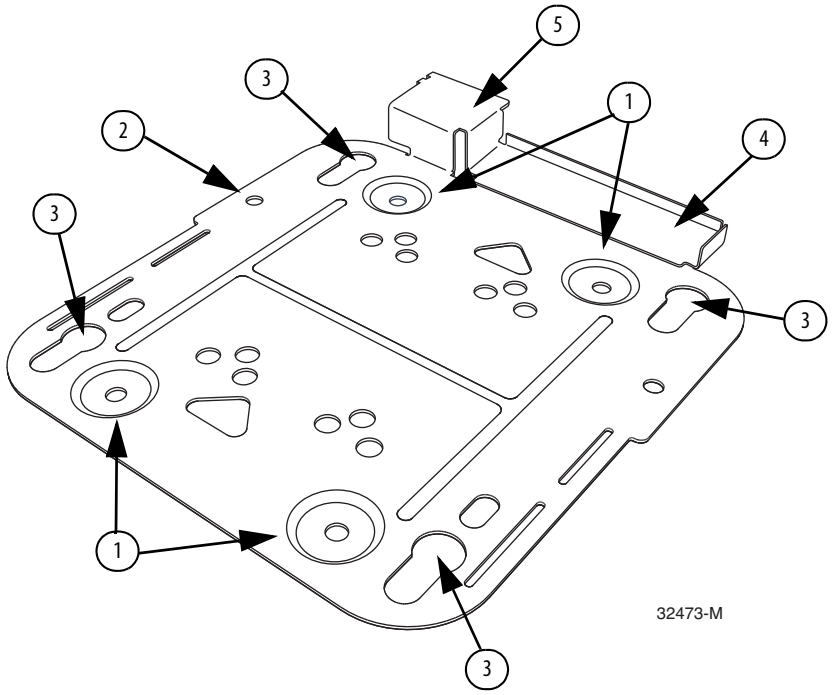
根据您的要求可提供不同的安装选件。支架由思科以及第三方公司提供。订货时，您可选择一个矮型或通用支架；在配置期间，两者在各自的括号中都显示零美元 ($0) 选项。

矮型 AIR-AP-BRACKET-1 (随同产品发货) 是进行天花板安装时使用最多的支架。

请按照以下步骤将接入点安装到坚硬的吊顶或墙壁上。

1. 将安装支架作为模板来标记支架上安装孔的位置。

图 13 - 安装支架的详细信息



1	壁式安装位置	4	电缆接入盖
2	接地柱	5	安全搭扣
3	接入点附件插槽		

提示 标记壁式安装的全部四个位置。确保安装牢固。使用合适的紧固件安装接入点并且使用的紧固件不能少于四个。

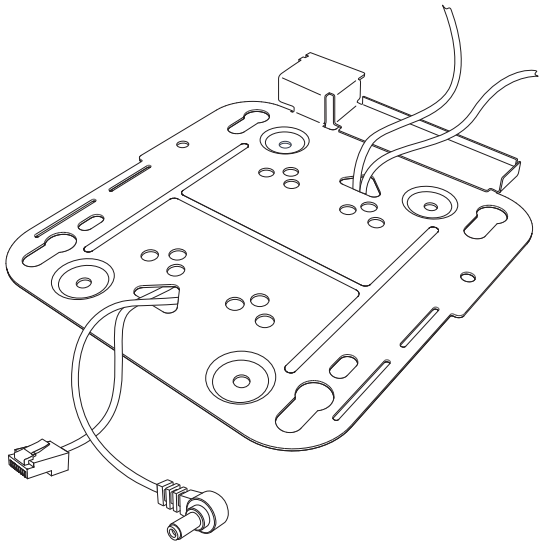
重要事项 采用吊顶安装方式时，切勿使用塑料墙锚或安装支架上的锁孔插槽进行安装。在坚硬的吊顶上安装接入点时，请使用四个至少能够承受 9 kg (20 lb) 拔出力的紧固件。

2. 使用 29 号钻头 (0.1360 in. [3.4772 mm]) 在标记的安装孔位置 (1) 钻出导向孔。

   提示 导向孔径根据要紧固的材料和厚度而定。思科建议您对材料进行测试，确定最适合安装应用的孔径。

3. (可选) 在安装支架电缆接入盖附近下方钻出或切出电缆接入孔，孔的大小要足以容纳以太网电缆、建筑物接地线和电源电缆。
4. 将电缆拉入孔内大约 9 in.。在将支架固定到天花板或墙壁之前，将以太网和电力电缆穿过支架。如下图所示，将电缆穿过主电缆通孔，然后穿过如所示的较小通孔。

图 14 - 敷设以太网和电源电缆



5. (可选) 使用接地螺丝将建筑物接地线连接到安装支架上。

   有关常规接地说明，请参见第 37 页的 “ 为接入点接地 ”。

6. 将安装支架的安装孔 (锯齿朝下) 放在导向孔上。
7. 将紧固件插入各个安装孔并拧紧。
8. 将以太网和电源电缆连接到接入点。
9. 将接入点支脚与安装板上大部分锁孔安装插槽对齐。

   放置正确时，电缆接入盖正好嵌入接入点连接器凹槽。

10. 将接入点轻轻地滑到安装支架锁孔插槽中，直到卡入到位。

将接入点安装到网络或电气盒

根据以下步骤将接入点安装到网络盒或电气盒上。

1. 将通用安装支架 (AIR-AP-BRACKET-2) 放在现有的网络或电气盒上，然后将支架安装孔对准盒子的孔。
2. 将安装支架固定就位，将一个 6 x 32 x 1/4 in. 的平头螺钉插入到每个安装孔，然后拧紧。
3. 将大约 9 in. 长的以太网和电力电缆穿过孔。

   在将支架固定到天花板之前，请将电缆穿过支架。将电缆穿过主电缆通孔，然后穿过如第 44 页的图 14 所示的较小通孔。

4. (可选) 使用接地螺丝将建筑物接地线连接到安装支架上。

   有关常规接地说明，请参见第 37 页的 “ 为接入点接地 ”。

5. 将以太网和电源电缆连接到接入点。
6. 将接入点的支脚与可选安装托架上的锁眼安装槽对准。
7. 将接入点滑到选配的安装支架上，直到卡入到位。

部署无线网络上的接入点

重要事项	该产品依靠建筑物的设施提供短路 (过流) 保护。确保保护装置的额定值不高于：120 V AC， 20 A (美国标准) (240 V AC， 16…20 A (国际标准))。 本产品需要短路 (过流) 保护，此保护应作为建筑安装的一部分进行提供。安装时必须在符合国家和当地布线规范。

安装接入点后，根据以下步骤在无线网络上部署接入点：

1. 接上电源线。
2. 将适配器 (带连接好的电源线) 插入 WAP。
3. 将电源线插入电源插座。
4. 观察接入点状态指示灯。

   有关状态指示灯的说明，请参见第 46 页的 “ 接入点状态指示灯 ”。

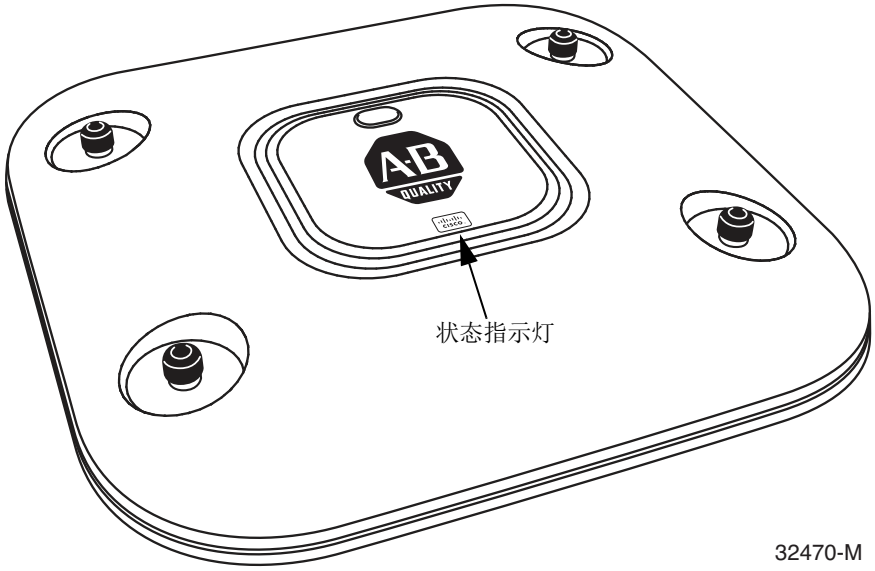
一旦使用控制台电缆完成接入点配置后，请参见第 52 页的 “ 本地连接到 Stratix 5100 WAP 接入点 ”。接入点将启动一个上电序列，可通过观察接入点指示灯进行确认。

如果状态指示灯未点亮，则接入点很有可能没有上电。

接入点状态指示灯

各单元间可能存在色彩强度和色调的微小差异。这一差异在状态指示灯制造商规范的正常范围内，并不是缺陷。

图 15 - 接入点状态指示灯



状态指示灯传达各种 WAP 状态。

Table 4 - 状态指示灯描述

消息类型	状态指示灯	描述
启动加载程序状态序列	绿色闪烁	正在对 DRAM 存储器进行测试
		DRAM 存储器测试完成
		正在对板进行初始化
		正在初始化非易失性内存的文件系统
		非易失性内存测试完成
		正在对以太网进行初始化
		以太网初始化完成
		正在启动思科 IOS
		初始化成功
连接状态	绿色	正常运行状态，但没有关联任何无线客户端
	蓝色	正常运行状态，已至少关联一个无线客户端
运行状态	红色闪烁	以太网链路未运行
启动加载程序警告	蓝色闪烁	正在恢复配置 (按住模式按钮 2…3 秒)
	红色	以太网故障或映像恢复。(模式按钮按下达 20…30 秒)
	绿色闪烁	正在恢复映像 (释放模式按钮)

Table 4 - 状态指示灯描述 (续)

消息类型	状态指示灯	描述
启动加载程序错误	红色	DRAM 存储器测试失败
	红色和蓝色闪烁	非易失性内存文件系统故障
	红色和熄灭闪烁	环境变量故障
		MAC 地址错误
		映像恢复期间以太网故障
		启动环境故障
		无思科映像文件
		启动故障
思科 IOS 错误	红色	软件故障；尝试断开并再次接通单元电源
	在蓝色、绿色、红色和熄灭之间循环	常规警告；线路电力不足

检查电源

通过检查馈电器，可确认接入点 / 网桥的电源是否可用。

- 电源状态指示灯
  - 绿色表示已给网桥接通输入电源。
  - 红色表示过电流或过电压错误情形 - 从馈电器上断开输入电源，检查所有同轴电缆接头是否出现短路，等待约 1 分钟，然后重新将输入电源连接至馈电器。如果状态指示灯再次变为红色，请联系技术支持人员获取援助。

    提示 馈电器大约需要 50 秒才能从过电流或过电压状态中恢复。

熄灭表示输入电源不可用 —— 确认已将电源模块连接至馈电器，且交流电源可用。

配置接入点

可使用 Stratix 5100 设备管理器对 WAP 执行配置过程。有关如何使用 Stratix 5100 设备管理器软件配置无线接入点 / 工作组网桥的说明，请参见第 49 页的 “Stratix 5100 设备管理器配置启动 ”。

备注：

Stratix 5100 设备管理器配置启动

本章介绍了 Stratix 5100 设备管理器和启动配置。 Web 浏览器界面是配置无线接入点 / 工作组网桥时所使用的界面。

设备管理器

设备管理器包含管理页面，可用于更改无线设备设置、升级固件并监控和配置网络上的无线设备。默认情况下，接入点无线电接口为禁用。在使用管理页面时，根据您所作的设置，当缺失配置参数时将会显示一些错误消息。当正确设置参数后才可继续。

以下是可使用设备管理器完成的任务的实例。

- 配置 VLAN。
- 分配 SSID 和广播 SSID。
- 确定 VLAN 到 SSID 的映射。
- 选择最优数据传输速率。
- 配置 EAP 验证，包括 EAP/RADIUS 服务器
- 分配加密模式。
- 使用无线 MAC 过滤器。
- 为过滤器检测 MAC (捕捉网络发现的 MAC 地址并导出到 MAC 过滤器列表)。

在 Easy Setup (简易设置) 页面中，您可快速配置接入点的基本参数。

提示 避免使用 CLI 和 Stratix 5100 WAP 设备管理器 (Web 浏览器) 同时配置无线设备。如果通过 CLI 配置无线设备， Web 浏览器界面会显示配置的不准确解析。但是，不准确并不一定意味着该无线设备配置错误。

准备事宜

在配置 Stratix 5100 WAP 之前，确保使用连接到与无线设备处于同一网络的计算机，并从您的网络管理员处获取下列信息。

- 接入点的系统名称 无线设备
- 无线电网络的无线服务集标识符 (SSID) (区分大小写)。
- 如果未连接到 DHCP 服务器，则提供无线设备唯一的 IP 地址 (例如， 172.17.255.115)。
- 如果无线设备与计算机不在同一子网中，则需要默认网关地址和子网掩码。
- 简单网络管理协议 (SNMP) 社区名称和 SNMP 文件属性 (如果使用了 SNMP)。
- 接入点 MAC 地址。 MAC 地址可在接入点底部的标签上找到 (例如， 00164625854c)。

登录到 Stratix 5100 WAP

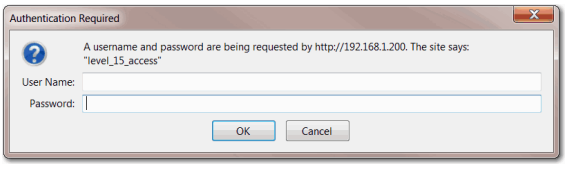
使用 WAP 的 IP 地址跳转到设备管理器。如果不知道接入点的 IP 地址，请参见第 55 页的 “ 登录到接入点 ”，了解为接入点分配 IP 地址的说明。

根据以下步骤以使用 Web 浏览器界面：

1. 打开浏览器。

   Web 浏览器界面与以下软件版本完全兼容。

   - Microsoft Internet Explorer 8.0 和 Firefox 27，基于 Windows 7
   - Microsoft Internet Explorer 6.0，基于 Windows 98、 2000 和 XP 平台
   - Netscape 7.0，基于 Windows 98、 2000、 XP 和 Solaris 平台
2. 在 address (地址) 域中，输入 Stratix 5100 WAP 的 IP 地址。
3. 输入用户名和密码，并单击 OK (确定)。



   将显示 Summary Status (概要状态) 主页。

获取和分配 IP 地址。

要浏览到 Stratix 5100 WAP 设备管理器的简易无线设备设置页，必须获取或分配无线设备 IP 地址。为您的网络管理员提供无线设备 介质访问控制 (MAC) 地址。您的网络管理员可使用 MAC 地址查询 DHCP 服务器来识别 IP 地址。接入点 MAC 地址位于接入点底部粘贴的标签上。

默认 IP 地址行为

当使用默认配置将 Stratix 5100 WAP 连接到局域网时，接入点将从 DHCP 服务器请求 IP 地址；如果没有接收到地址，将无限期持续发送请求。

本地连接到 Stratix 5100 WAP 接入点

如果需要本地配置接入点 (接入点不连接到有线局域网)，您可使用附带的控制台电缆 (DB-9 到 (RJ-45) 串行电缆) 连接计算机。

根据以下步骤连接到接入点控制台端口，以此打开 CLI：

1. 将控制台电缆 (RJ-45) 连接到 WAP。
2. 将控制台电缆的另一端 (DB-9) 连接到计算机上的串行端口。
3. 设置终端模拟器，使其与接入点进行通信。

   使用下列终端模拟器连接设置：9600 波特、 8 个数据位，无奇偶校验， 1 个停止位和无流量控制。如果 Xon/Xoff 流量控制不起作用，则不使用流量控制。
4. 连接后，按下回车键或输入 `en` 访问命令提示符。

   按下回车键将跳转到用户 exec 模式，并提示您输入密码，输入后将跳转到特权 EXEC 模式。
5. 当完成配置更改后，从接入点上拆下串行电缆。

更多详细信息，请参见第 195 页的 “ 使用命令行界面配置 Stratix 5100 WAP”。当使用 CLI 和控制台电缆完成初始配置后，您可登录到接入点，并开始使用 Stratix 5100 设备管理器。

默认 无线电设置

Stratix 5100 WAP 无线电装置被禁用，且未分配默认 SSID。这是为了防止非授权用户通过有默认 SSID 而无安全设置的接入点访问无线网络。必须先创建 SSID 后才能启用接入点无线电接口。

关于默认无线电设置的信息，请参见第 255 页的 “ 配置无线电设置 ”。

将 WAP 复位到默认设置

在初始设置过程中，如果需要重新开始，您可将接入点复位到出厂默认设置。

使用模式按钮将 WAP 复位到默认设置

根据以下步骤使用接入点 模式按钮，将接入点复位到出厂默认设置：

1. 断开接入点的电源 (外部电源的电源插座或 PoE 电源的以太网电缆)。
2. 按下并按住模式按钮，同时重新连接接入点的电源。
3. 按住模式按钮，直到状态指示灯变为琥珀色 (约 20...30 秒)，然后松开按钮。

   所有接入点设置都将恢复到出厂默认值。

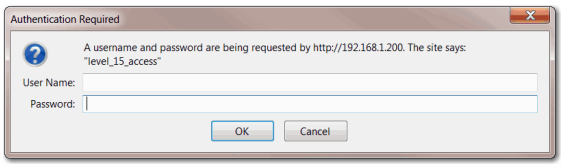
使用 GUI 复位到默认设置

复位到默认设置后，所配置的设备将恢复到其默认设置。需要输入 Stratix 5100 WAP 的用户名和密码进行登录，然后根据以下步骤将设备复位到默认设置。

根据以下步骤使用接入点 GUI 恢复到默认设置：

1. 打开 Internet 浏览器。
2. 在浏览器地址行中输入无线设备 IP 地址并按下回车键。

   将显示 Authentication Required (需要验证) 对话框。



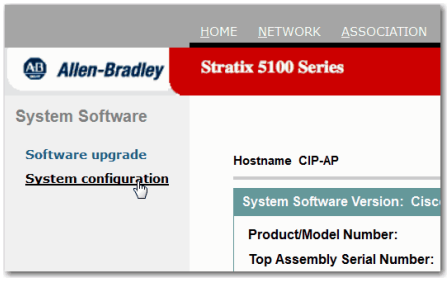
3. 在 User Name (用户名) 域中输入用户名。
4. 在 Password (密码) 域中输入无线设备密码并按下回车键。

将显示 Summary Status (概要状态) 页面。

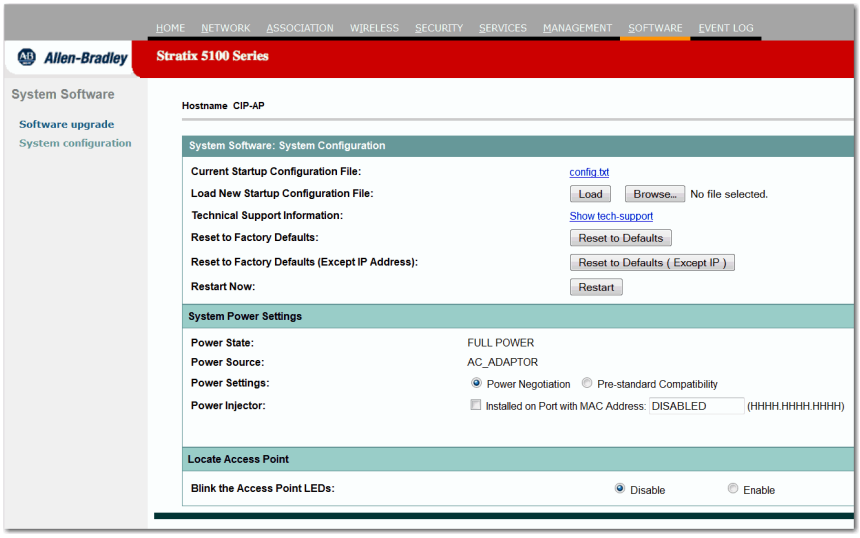
5. 在顶部菜单中，单击 Software (软件)。

将显示 System Software (系统软件) 画面。

6. 单击 System Configuration (系统配置)。



将显示 System Configuration (系统配置) 画面。



7. 单击 Reset to Defaults (复位到默认值) 将所有设置 (包括 IP 地址) 复位到出厂默认值。

您可使用 CLI 复位默认值，请参见第 203 页的 “ 使用 CLI 恢复默认设置 ”。

登录到接入点

用户可使用以下方法中的任一种登录到接入点。

- 图形用户界面 (GUI)
- Telnet (如果 AP 配置有 IP 地址)
- SSH (安全外壳) (如果 AP 上启用了该功能)
- 控制台端口

关于各种方法登录到接入点的信息：

- GUI，请参见第 51 页的 “ 登录到 Stratix 5100 WAP”。
- CLI，请参见第 202 页的 “ 访问 CLI”。
- 控制台端口，参见第 52 页的 “ 本地连接到 Stratix 5100 WAP 接入点 ”。

联机帮助

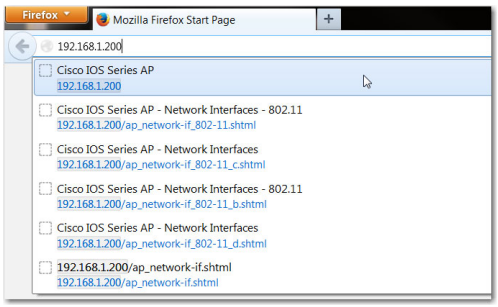
在 Web 浏览器界面中，单击页面顶部的帮助图标，以显示联机帮助。单击打印机图标打印您所在的页面。

帮助页面将在新浏览器页面中显示，使用主题下拉菜单显示帮助索引或常见配置任务的说明，例如，配置 VLAN。

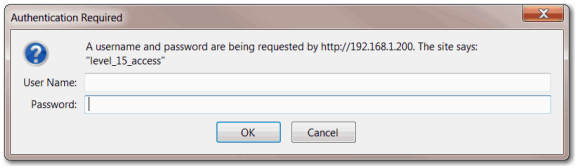
配置接入点的基本设置

在确定或分配无线设备 IP 地址后，您可浏览到 无线设备 Express Setup (简易设置) 页面执行初始配置。

1. 打开 Internet 浏览器。
2. 在浏览器地址行中输入 WAP 地址并按下回车键。



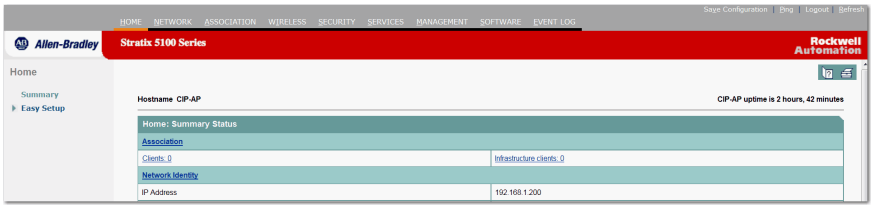
将显示 Enter Network Password (输入网络密码) 画面。



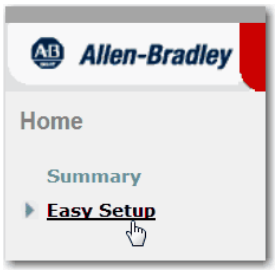
3. 单击 Tab 键跳过 Username (用户名) 域，前往 Password (密码) 域。
4. 输入密码 (区分大小写)：wirelessap.
5. 按下回车键。

将显示 Summary Status (概要状态) 页面。根据所使用的接入点型号，您的页面可能有所不同。

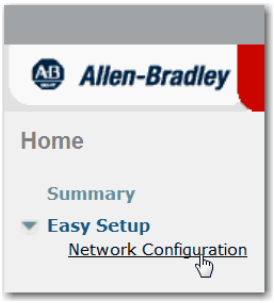
图 16 - Summary Status (概要状态) 页面



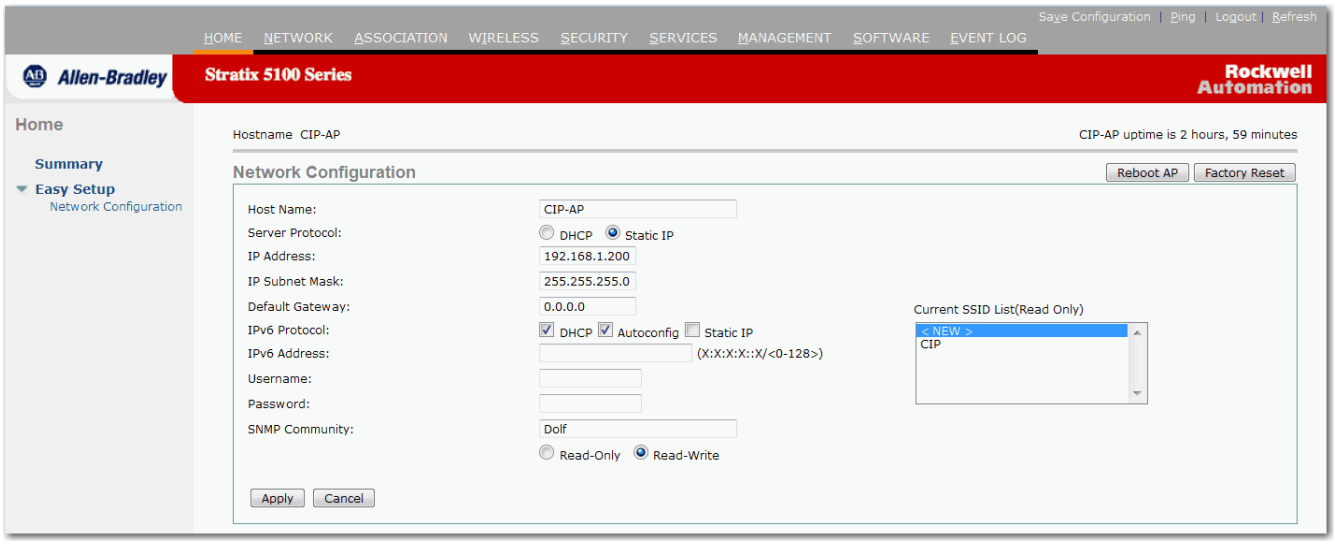
6. 单击 Easy Setup (简易设置)。



7. 将打开 Easy Setup (简易设置) 页，单击 Network Configuration (网络配置)。



8. 输入网络配置设置。



下表介绍了 Easy Setup (简易设置) 页面的网络配置设置。有关以下参数的详细信息，请参见第 78 页的 “ 简易设置网络配置页面 ”。

表 5 - 网络配置设置

参数	描述
Host Name	主机名称虽然不是关键设置，但有助于识别网络中的无线设备。主机名称将显示为管理系统页面中的标题。
Server Protocol	选择匹配网络 IP 地址分配方式的项目。
IP Address	使用该设置分配或更改无线设备 IP 地址。如果网络中启用了 DHCP，则将该域留空。
IP Subnet Mask	输入网络管理员提供的 IP 子网掩码，从而在局域网上识别 IP 地址。
Default Gateway	输入网络管理员提供的默认网关 IP 地址。如果启用了 DHCP，则将该域留空。
IPv6 Protocol	DCHP 自动配置 静态 IP
IPv6 Address	(X:X:X:X::X/<0-128>)
Username	想要使用该 WAP 的用户名。
Password	想要使用该 WAP 的密码。
SNMP Community	要使用简单网络管理协议 (SNMP)，输入社区名称。 SNMP 是一种应用层协议，支持在 SNMP 管理工作站和代理之间进行面向消息的通信。
Current SSID List	您已配置的 SSID 列表。

9. 输入无线电配置设置。

图 17 - Network Configuration (网络配置) 页面的无线电配置设置

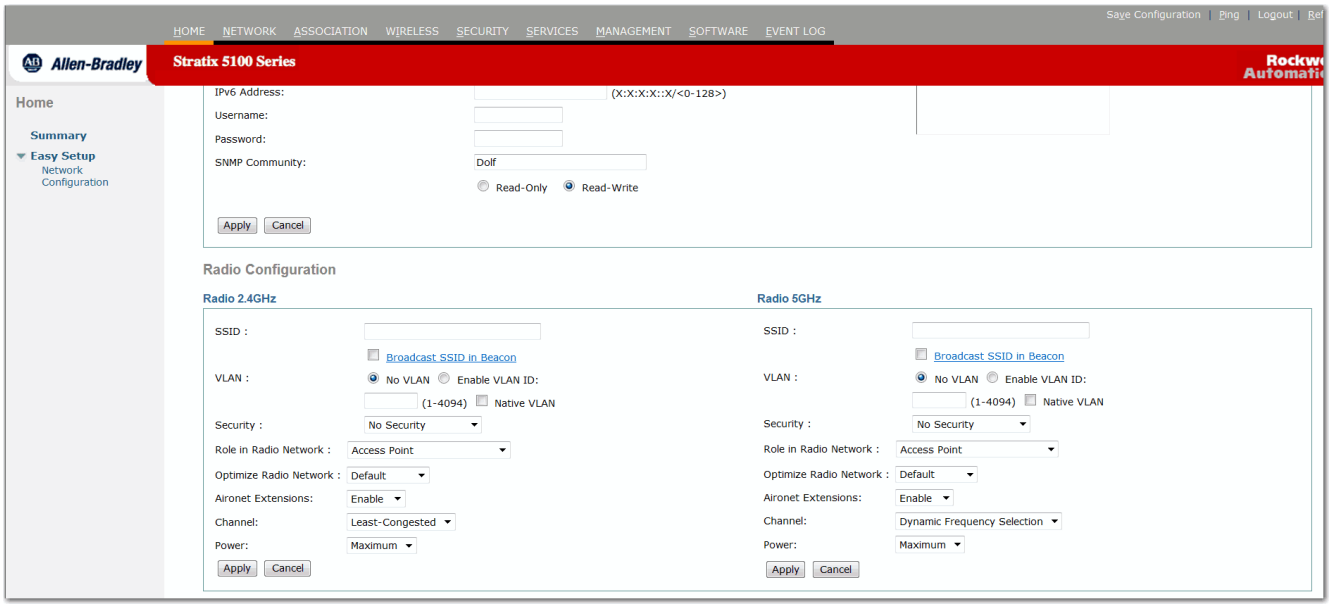


表 6 - 无线电配置设置

参数	描述
SSID	标识客户端设备关联设备必须使用的 SSID。
Broadcast SSID in Beacon	当设备处于根 AP 模式时，将激活该设置。当广播 SSID 时，如果网桥是根接入点，未指定 SSID 的设备可关联到该网桥。
Security	列出安全机制类型。
VLAN	选择一个 VLAN 设置。
Role in Radio Network (无线电网络中的角色)	
Access Point	如果无线设备连接到有线局域网，选择 Access Point (Root) (接入点 (根))。
Repeater	如果未连接到有线局域网，选择 Repeater (Non-root) (中继器 (非根))。
Root Bridge	与非根网桥建立链接。
Non-root Bridge	在该模式下，设备与根网桥建立链接。
Workgroup Bridge	指定 WAP 作为通过以太网集线器或交换机将其他思科接入点连接到以太网局域网网络的工作组网桥工作。
Universal Workgroup Bridge	指定 WAP 作为通过以太网集线器或交换机将任何其他接入点连接到以太网局域网网络的工作组网桥工作。
Scanner	指定接入点只能作为无线电扫描器工作，不接受来自客户端设备的关联。
Spectrum	指定 AP 作为专用型 RF 频谱传感器，与 Cisco Spectrum Expert 软件配合使用。
Optimize Radio Network for	使用该设置选择无线设备无线电的预配置设置，或者无线设备无线电的自定义设置。 选项有 default (默认)、 range (范围) 和 throughput (吞吐量)。

表 6 - 无线电配置设置

参数	描述
Aironet Extensions	如果在无线局域网上只有罗克韦尔自动化 WAP 或思科 Aironet 设备，而设备作为接入点或工作组网桥工作，或设备作为中继器工作，则选择 Enable (启用)。
Channel	通道号 / 频率 最不拥挤 当选择 Least congested (最不拥挤) 时， WAP 将自行决定哪个通道是最佳通道。
Power	最大值 比功率等级 (dBm)

10. 单击 Apply (应用) 保存设置

更多关于参数的无线电配置，请参见以下链接：

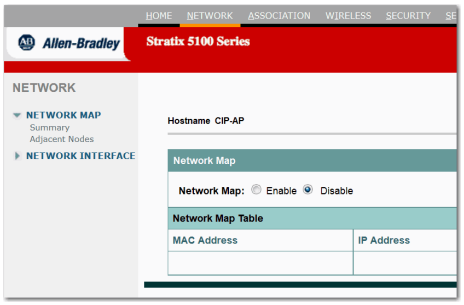
- 第 78 页的 “ 简易设置网络配置页面 ”
- 第 86 页的 “Network Interface Summary (网络接口概览) 页面 ”

启用网络上的无线电装置

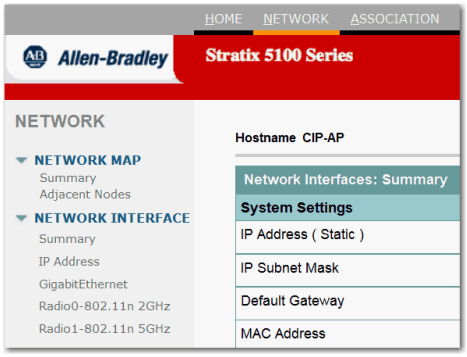
除了在 Easy Setup (简易设置) 页面设置参数之外，还必须跳转到无线电设置页面启用无线电装置。

1. 在顶部菜单中，单击 Network (网络)。

   将显示 Network Summary (网络概要) 页面。

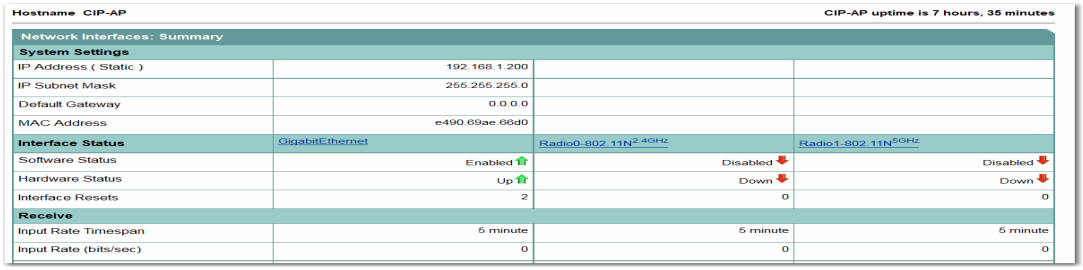


2. 单击 Network Interface (网络接口)。



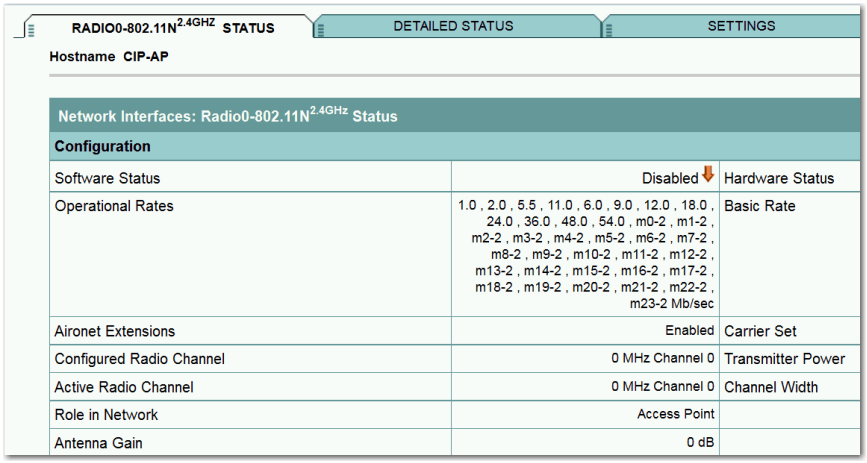
3. 单击 Summary (概要)。

将显示 Network Interfaces Summary (网络接口概要) 页面。



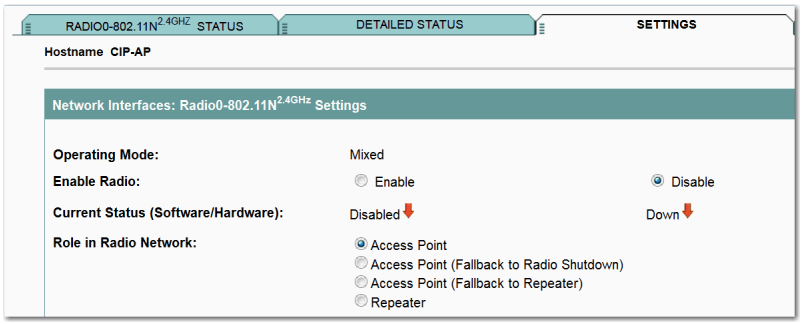
4. 单击想要配置的无线电接口。

将显示 Radio Status (无线电状态) 页面。

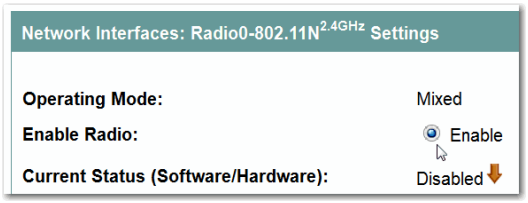


5. 单击 Settings (设置) 选项卡。

将显示 Radio Settings (无线电设置) 页面。



6. 选中 Enable (启用)。



7. 单击 Apply (应用)。

提示 您的接入点现在正在运行，但需要进行额外配置，以符合网络运行和安全要求。

默认情况下不创建 SSID，因此，在您启用 SSID 之前，接入点无法接受无线客户端。

VLAN

如果在无线局域网上使用 VLAN，并为 VLAN 分配 SSID，您可使用 Express Security (快速安全机制) 页面的四种安全设置中的任意一种创建多个 SSID。但如果没有在无线局域网上使用 VLAN，则能够在 Easy Setup (简易设置) 页面中分配给 SSID 的安全选项将受到限制，并将链接到加密设置和验证类型。

在没有 VLAN 的情况下，可为接口应用相关加密设置 (密文)，例如，2.4 GHz 无线电，但无法在该接口上使用多种加密设置。

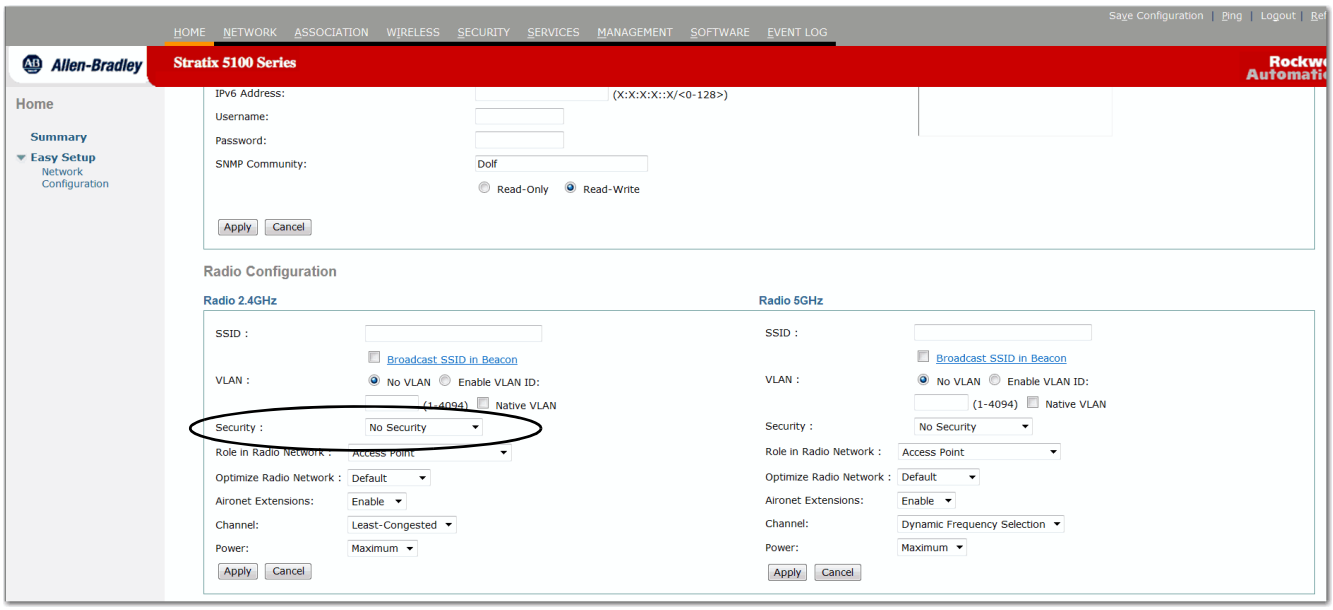
例如，当创建使用静态 WEP 的 SSID 并禁用了 VLAN 时，将无法创建更多使用 WPA 验证的 SSID，这是因为它们使用不同的加密设置。如果发现一个 SSID 的安全设置与另一个 SSID 冲突，您可删除一个或多个 SSID 来消除冲突。

配置安全

在分配了 WAP 的基本设置后，必须配置安全设置，以防止对网络进行非法访问。由于属于无线电设备，无线设备可跨越工作地点的物理障碍进行通信。

使用 Easy Setup (简易设置) 页面创建唯一的 SSID 并为其分配四种安全类型之一。

图 18 - Easy Setup (简易设置) — 无线电安全设置



Easy Set-up (简易设置) 页面的安全类型

下表介绍了可在 Easy Setup Network Configuration (简易设置 — 网络配置) 页面中为 SSID 分配的四种安全类型。

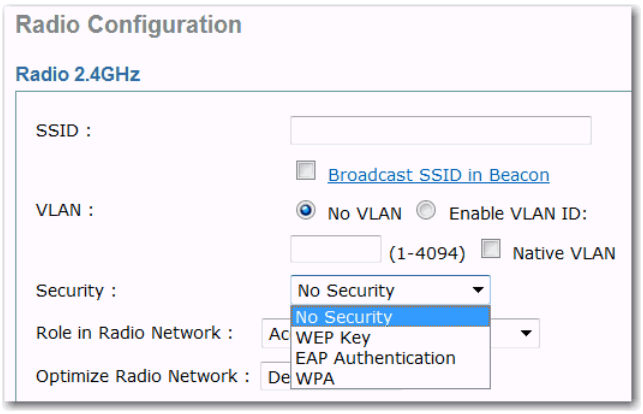


表 7 - Easy Set-up Security Setup (简易安全性设置) 页面上的安全类型

安全类型	描述	启用的安全功能
No Security (无安全性)	这是最不安全的一个选项。仅限对在公共场所中使用的 SSID 使用该选项，并将其分配给限制访问您的网络的 VLAN。	无
WEP Key (WEP 密钥)	该选项比 No Security (无安全性) 选项安全一些。 **警告：**静态 WEP 密钥很容易受到攻击。WEP 安全机制是一种传统方法，现已不再使用。	强制输入 WEP。由于该 SSID 不具备与无线设备密钥匹配的 WEP 密钥，客户端设备无法使用其进行关联。
EAP Authentication (EAP 验证)	该选项启用 802.1X 验证，例如， LEAP、 PEAP、 EAP-TLS、 EAP-FAST、 EAP-TTLS、 EAP-GTC、 EAP-SIM 和其他基于 802.1X/EAP 的产品 该设置使用强制加密、 WEP、开放式验证 + EAP、网络 EAP 验证、无密钥管理以及 RADIUS 服务器验证端口 1645。 您必须为网络上的验证 RADIUS 服务器输入 IP 地址和共享密钥 (服务器验证端口 1645)。因为 802.1X 验证提供动态加密密钥，因此，无需输入 WEP 密钥。 如果网络中没有 RADIUS 服务器，则应考虑使用接入点作为本地验证服务器，请参见第 307 页的 " 将接入点配置为本地验证器 "。	强制 802.1X 验证。使用该 SSID 关联的客户端设备必须执行 802.1X 验证。 如果将无线电客户端配置为使用 EAP-FAST 验证，则也可配置开放式验证 + EAP。如果未配置使用开放式验证 + EAP，则将显示下列 GUI 警告消息： 注意：网络 EAP 仅用于 LEAP 验证。如果将无线电客户端配置为使用 EAP-FAST 验证，则也可配置开放式验证 + EAP。 如果使用的是 CLI，则将显示该警告消息： SSID 配置警告：[SSID]：如果无线电客户端使用的是 EAP-FAST，则必须配置使用开放式验证 + EAP。
WPA	Wi-Fi 保护访问 (WPA) 允许无线访问通过验证服务器的服务对照数据库验证的用户，然后使用比 WEP 更强的算法加密它们的 IP 通信。 该设置使用加密密文、 TKIP、开放式验证 + EAP、网络 EAP 验证、强制密钥管理 WPA 和 RADIUS 服务器验证端口 1645。 当使用 EAP 验证时，您必须为网络上的验证 RADIUS 服务器输入 IP 地址和共享密钥 (服务器验证端口 1645)。	强制 WPA 验证。使用该 SSID 关联的客户端设备必须支持 WPA。 如果将无线电客户端配置为使用 EAP-FAST 验证，则必须配置开放式验证 + EAP。如果未配置使用开放式验证 + EAP，则将显示下列 GUI 警告消息： 注意：网络 EAP 仅用于 LEAP 验证。如果将无线电客户端配置为使用 EAP-FAST 验证，则必须配置开放式验证 + EAP。 如果使用的是 CLI，则将显示该警告消息： SSID 配置警告：[SSID]：如果无线电客户端使用的是 EAP-FAST，则必须配置使用开放式验证 + EAP。

简易设置 — 网络配置 — 安全限制

由于 Easy Setup (简易设置) 页面用于进行简单的基本网络配置和安全配置，此处的选项仅是无线设备安全功能的一个子集。如果选择了 No VLAN (无 VLAN) 选项，可配置一次静态 WEP 密钥。如果选择了 Enable VLAN (启用 VLAN)，则禁用静态 WEP 密钥。

关于配置安全功能的详细信息，请参见第 110 页的 “Security (安全) 页面 ”。

在使用 Easy Setup (简易设置) 页面时，请记住以下限制：

表 8 - Easy Setup (简易设置) 页面安全设置限制

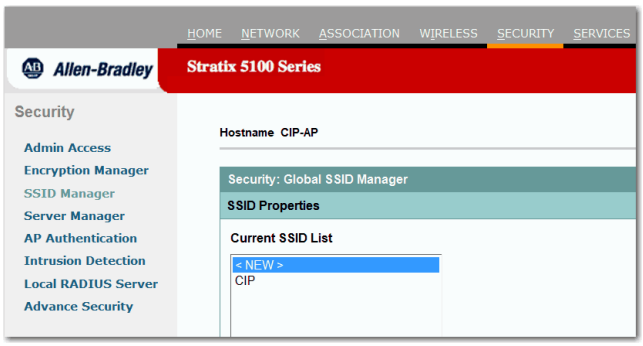
您无法	注
编辑 SSID。	但可删除 SSID 然后重新创建。
分配 SSID 到特定的无线电接口。	将创建 SSID 并分别被应用到各个无线电接口。要将同一 SID 分配给两个无线电接口，可使用 Security SSID Manager (安全 SSID 管理器) 页面 或 Easy Setup (简易设置) 页面。
配置多个验证服务器。	要配置多个验证服务器，可使用 Security Server Manager (安全服务器管理器) 页面。
将 SSID 分配给无线设备上已配置的 VLAN。	要将 SSID 分配给现有 VLAN，可使用 Security SSID Manager (安全 SSID 管理器) 页面。
在同一 SSID 上配置验证类型组合 (例如，MAC 地址验证与 EAP 验证)。	要配置验证类型组合，可使用 Security SSID Manager (安全 SSID 管理器) 页面。

从 Security (安全) 菜单创建 SSID

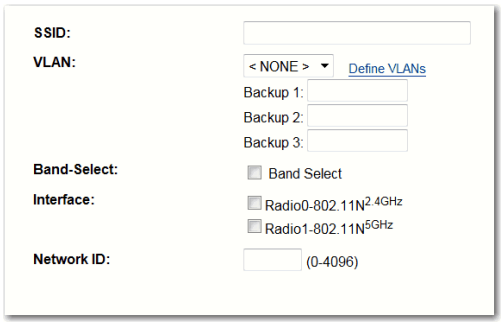
根据以下步骤使用 Security (安全) 菜单创建 SSID。您还可在 Easy Setup (简易设置) 页面中定义 SSID。

- 关于命名惯例的详细信息，请参见第 115 页的 “SSID Manager (SSID 管理器) 页面 ”。
- 关于如何使用 CLI (命令行接口) 创建 SSID 的信息，请参见第 204 页的 “ 安全 CLI 配置示例 ”。

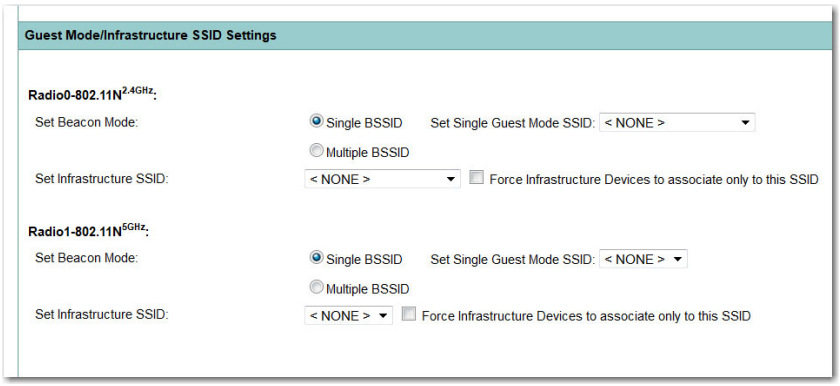
1. 在顶部菜单中，单击 Security (安全)。
2. 从左侧菜单中单击 SSID Manager (SSID 管理器)。



3. 单击 NEW (新建) 并在 SSID 输入域中输入 SSID。



- SSID 最多包含 32 个字母数字字符。
- 关于命名惯例的详细信息，请参见第 115 页的 “SSID Manager (SSID 管理器) 页面 ”。

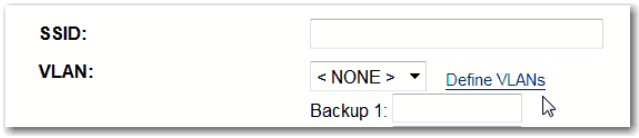


4. 要在无线设备信标中广播 SSID，选中 Broadcast SSID in Beacon (在信标中广播 SSID) 复选框。

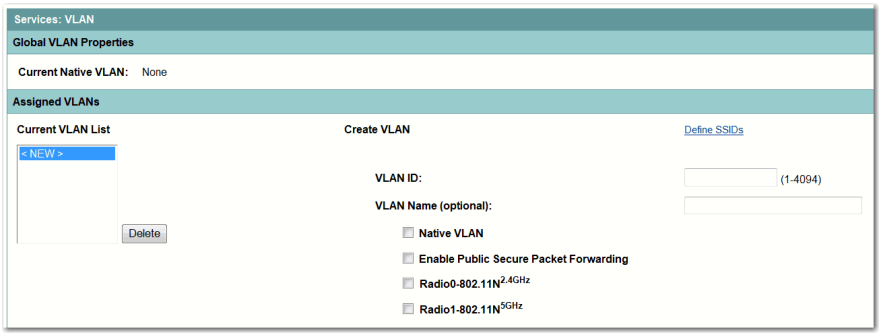
   只有当设备处于根 AP 模式时，才会激活该设置。当广播 SSID 时，如果网桥是根接入点，未指定 SSID 的设备可关联到该网桥。当 SSID 要被访客或公共场所的客户端设备使用时，该选项很有用。如果不广播 SSID，客户端设备将无法关联到接入点，除非其 SSID 匹配该 SSID。信标中只能有一个 SSID。

   如果未指定 SSID，设备将通过发送广播消息，来搜索要关联的接入点。该设置允许未指定 SSID 的设备关联到该接入点

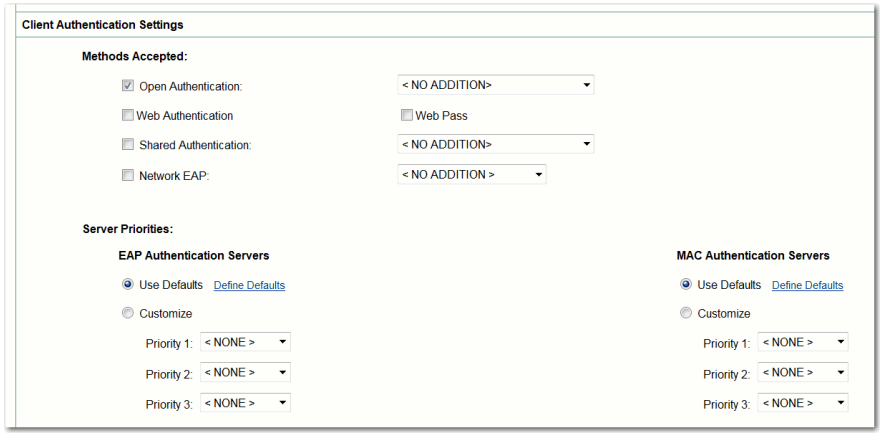
5. (可选) 为 VLAN 分配 SSID。
   a. 单击 Define VLANS (定义 VLAN)。



   b. 选择 NEW (新建)。
   c. 输入 VLAN 编号 (1...4094)。
   d. 选择一个无线电，然后单击 Apply (应用)。



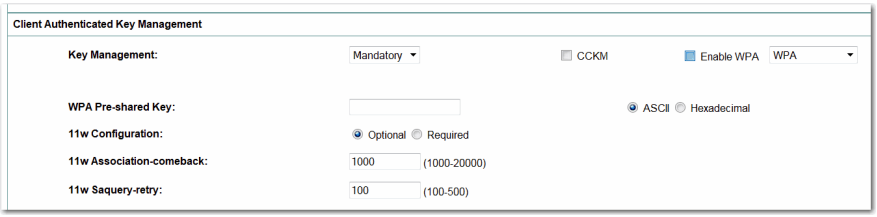
6. (可选) 选中 Native VLAN (本征 VLAN) 复选框，将 VLAN 标记为本征 VLAN。
7. 选择客户端的验证方法。



8. 选择服务器优先级。

9. 如果需要的话，选择 MAC 验证服务器。
10. 定义密钥管理。

提示 如果未在无线局域网上使用 VLAN，则分配给多个 SSID 的安全选项存在限制。更多详细信息，请参见第 409 页的“配置 VLAN”。



11. 单击 Apply (应用)。

    SSID 将出现在页面顶部的 SSID 表中。

启用 HTTPS 实现安全浏览

您可启用 HTTPS 来保护与接入点 Web 浏览器界面的通信。 HTTPS 使用安全套接字层 (SSL) 协议保护 HTTP 浏览器会话。

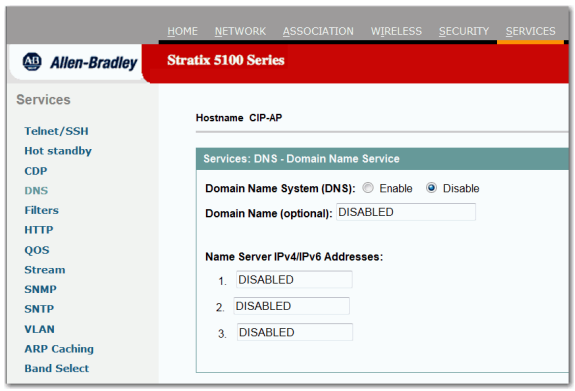
当启用 HTTPS 后，浏览器可能会丢失与接入点的连接。如果丢失连接，可在浏览器地址行中更改 URL，将 http://*IP* 地址改为 https://*IP* 地址，然后重新登录到接入点。

启用 HTTPS 后，每次浏览不具备完全限定域名 (FQDN) 的设备时，大多数浏览器会提示进行验证。要避免验证提示，完成以下说明的步骤 2 至步骤 9，为接入点创建 FQDN。但如果不想创建 FQDN，可跳转到步骤 10。

根据以下步骤创建 FQDN 并启用 HTTPS。

1. 跳转到 Services (服务) > DNS。

图 19 - DNS 页面



2. 选择 Enable (启用) 域名系统。
3. 在 Domain Name (域名) 域中输入域名。

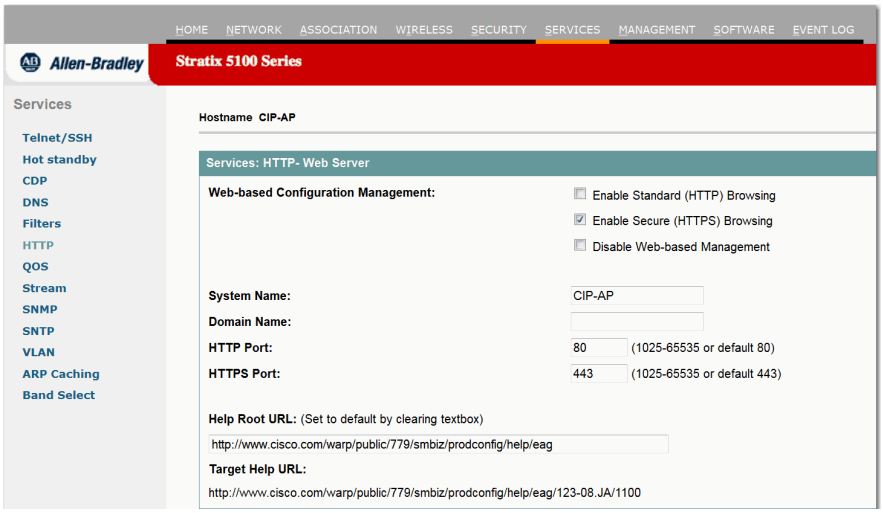
   例如，在罗克韦尔自动化公司，域名为 rockwellautomation.com。
4. 在 Name Server IP Addresses (域名服务器 IP 地址) 中，输入至少一个 DNS 服务器 IP 地址。
5. 单击 Apply (应用)。

   接入点 FQDN 是系统名称和域名的组合。例如，如果系统名称为 ap1100，域名为 company.com，则 FQDN 为 ap1100.company.com。
6. 在 DNS 服务器上输入 FQDN。

   这样， DNS 服务器可将友好型 AP 名称映射到正确的 IP 地址。这是 DNS 的一个重要步骤，因为 DNS 服务器必须知晓 AP 的名称，以便将友好型名称正确翻译为可正确连接的 IP。

   提示 如果没有 DNS 服务器，您可通过动态 DNS 服务注册接入点 FQDN。在互联网上搜索动态 DNS，查找收费的 DNS 服务。
7. 浏览到 Services: HTTP Web Server (服务：HTTP Web 服务器) 页面。

图 20 - Services: HTTP Web Server (服务： HTTP Web 服务器) 页面

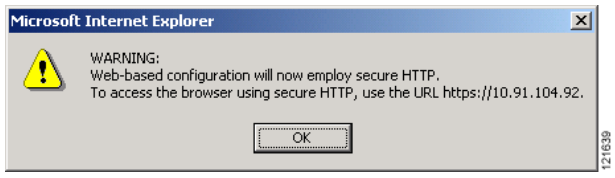


8. 单击 Enable Secure (HTTPS) Browsing (启用安全 (HTTPS) 浏览) 复选框并单击 Apply (应用)。
9. 输入域名并单击 Apply (应用)。

提示 虽然您可同时启用标准 HTTP 和 HTTPS，我们建议您只启用其中一个。

将显示警告页面，声称您需要使用 HTTPS 浏览接入点。页面还将提示您将浏览接入点所使用的 URL 从 *http* 更改为 *https*。

图 21 - HTTPS 警告页面



10. 单击 OK (确定)。

浏览器地址行中的地址从：

http://*IP* 地址更改为 https://*IP* 地址。

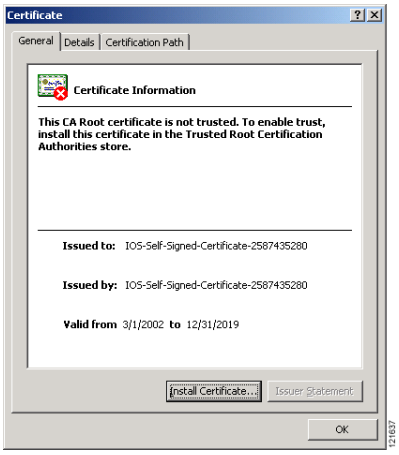
将显示另一个警告页面，声称接入点安全证书有效，但并非来自已知来源。但您可放心接受证书，因为相关站点是您自己的接入点。

图 22 - 证书警告页面

11. 要接受证书并继续，单击 View Certificate (查看证书)。

    要不接受证书并继续，单击 Yes (是)，将跳转到步骤 17。

图 23 - 证书页面



12. 在 Certificate (证书) 对话框中，单击 Install Certificate (安装证书)。

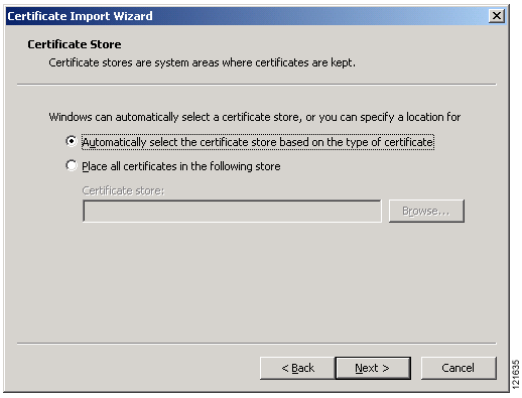
将显示 Microsoft 页面 Certificate Import Wizard (证书导入向导)。

图 24 - Certificate Import Wizard (证书导入向导) 页面

13. 单击 Next (下一步)。

    将显示 Certificate Storage Area (证书存储区域) 对话框，询问证书保存位置。我们建议您使用系统的默认存储区域。

图 25 - 证书存储区域页面



14. 单击 Next (下一步) 接受默认存储区域。

    将显示一个对话框，声称您已成功导入证书。

图 26 - 证书完成页面

15. 单击 Finish (完成)。

    将显示最终的安全警告。

图 27 - 证书安全警告

16. 单击 Yes (是)。

    将显示另一个页面，声称安装已成功完成。

图 28 - 成功导入页面

17. 单击 OK (确定)。

    将显示接入点登录对话框，必须重新登录接入点。

CLI 配置示例

本例显示了相当于第 67 页的 " 启用 HTTPS 实现安全浏览 " 中所列步骤的 CLI 命令。

在本例中，接入点系统名称为 ap1100，域名为 company.com， DNS 服务器的 IP 地址为 10.91.107.18。

```
AP# configure terminal
AP(config)# hostname ap1100
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

关于本例中使用的命令的完整说明，请参见 Using the Cisco IOS Command-Line Interface Configuration Guide 15.3 (思科 IOS 命令行接口配置使用指南第 15.3 版)。

删除 HTTPS 证书

启用 HTTPS 时，接入点将自动生成证书。但如果需要更改接入点的完全限定域名 (FQDN)，或者在启用 HTTPS 后需要添加 FQDN，您可删除证书。根据以下步骤删除证书。

1. 浏览到 Services (服务) > HTTP 页面。
2. 取消选中 Enable Secure (HTTPS) Browsing (启用安全 (HTTPS) 浏览) 复选框以禁用 HTTPS。
3. 单击 Delete Certificate (删除证书)。
4. 重新启用 HTTPS。

   接入点将使用新的 FQDN 生成新的证书。

禁用 Web 浏览器界面

要完全禁止使用 Web 浏览器界面，在 Services: HTTP-Web Server (服务：HTTP-Web 服务器) 页面中选中 Disable Web-Based Management (禁用基于 Web 的管理) 复选框，并单击 Apply (应用)。

要重新启用 Web 浏览器界面，输入该 CLI 全局配置命令。

```
ap(config)# ip http server
```

备注：

Stratix 5100 设备管理器参数定义

本章定义了设备管理器中每个页面的参数设置。

设备管理器系统管理选项卡

在最初配置了接入点的 IP 地址并登录后，则在主页上显示这些信息。主页提供了关联工作站、系统事件和端口状态的概览。主页还提供了到各页面的多个链接，这些页面给出详细信息。

System Management (系统管理) 选项卡提供了查看和保存配置信息的统一方法。在每个系统管理主题左侧显示一个展开菜单。

提示 请记住，当在 Web 浏览器中单击 Back (后退) 返回到上一页时，软件不保存您所作的任何更改。仅在单击 Apply (应用) 后才会应用更改。

图 29 - Stratix 5100 设备管理器主页

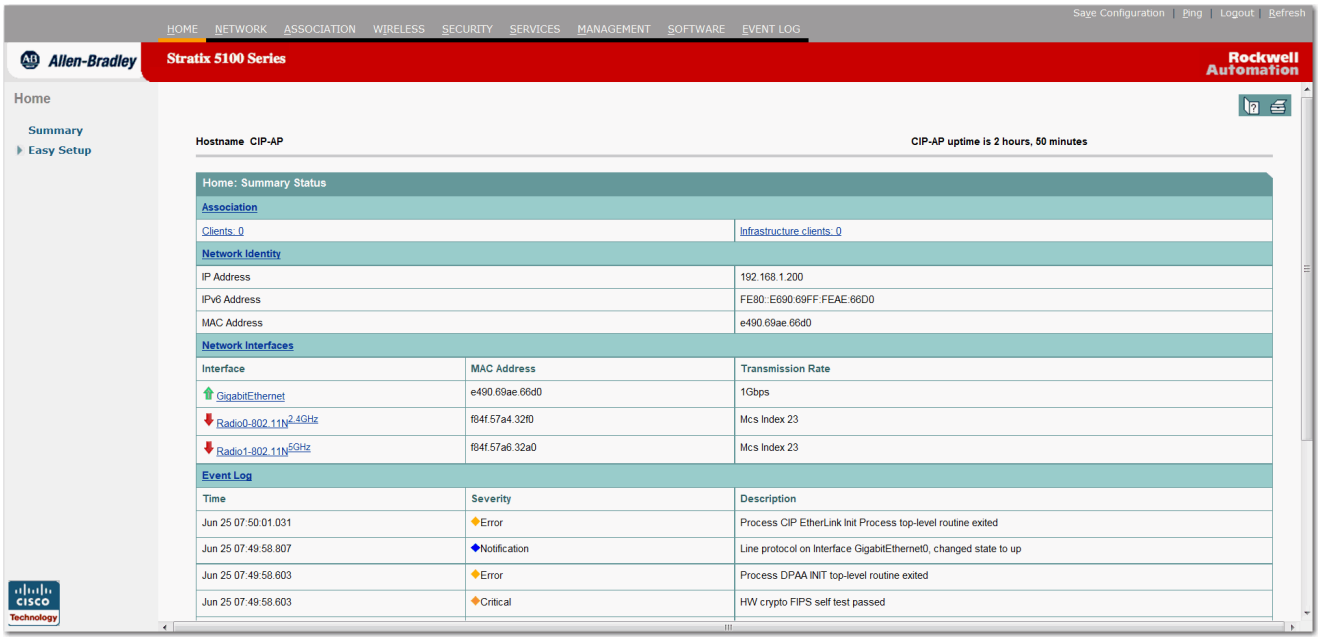


表 9 - Stratix 5100 设备管理器系统管理选项卡描述

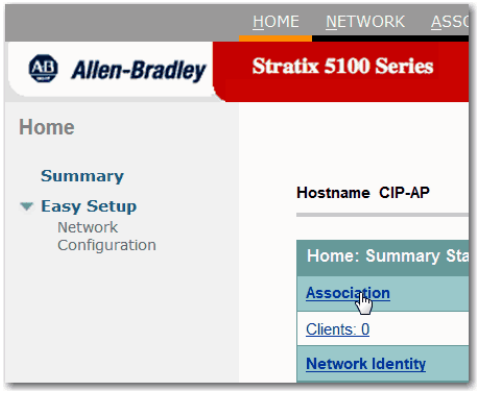
项目	描述
Home	Home-Summary (主页 - 概要) 页面为无线设备状态页面提供关联到无线电设备的无线电设备数信息、以太网和无线电接口状态以及最近的无线电设备活动列表。
Network	Summary (概要) 页面提供以太网、无线电接口的状态和统计信息。 Network Interface (网络接口) 提供接口总览，以及到每个接口配置页面的链接。 有关详细信息，请参见第 85 页的 “Network (网络) 页面 ”。
Association	提供无线局域网上所有设备的列表，列出其系统名称、网络角色和父级客户端关系。 有关详细信息，请参见第 103 页的 “Association (关联) 页面 ”。
Wireless	提供无线域服务器 (WDS) 概要。 有关详细信息，请参见第 104 页的 “Wireless (无线) 页面 ”。
Security	可访问安全服务，例如，管理访问和 SSID 管理器。 有关详细信息，请参见第 110 页的 “Security (安全) 页面 ”。
Services	可访问其他可用服务，例如， HTTP 和 QOS。 有关详细信息，请参见第 134 页的 “Services (服务) 页面 ”。

表 9 - Stratix 5100 设备管理器系统管理选项卡描述 (续)

项目	描述
Management	这是您管理 guest 用户帐户和 WebAuth 的地方。在 WebAuth 中，您可自定义 Login (登录) 页面的外观 (如果启用了 Web Authentication (Web 验证))。 有关详细信息，请参见第 163 页的 "Management (管理) 页面 "。
Software	可访问软件升级和配置。 有关详细信息，请参见第 165 页的 "Software (软件) 页面 "。
Event Log	创建无线设备事件日志并提供到配置页面的链接，您可在其中选择要捕获的事件、设置事件严重性等级和通知方式。 • 在 Summary (概要) 页面中， Time (时间) 列显示以系统运行时间或挂钟时间表示的事件时间。 • 每个页面右上角显示自启动或复位以来，以累计天数、小时数、分钟数和秒数表示的当前系统运行时间。 • Severity (严重性) 列标注事件的严重程度。严重性选项有 Emergency (紧急)、 Alert (报警)、 Critical (关键)、 Error (错误)、 Warning (警告)、 Notification (通知)、 Information (信息) 或 Debugging (调试)。 参见第 170 页的 "Event Log (事件日志) 页面 "，查看各种类型的严重性等级和描述。 • Description (描述) 列是事件的简要说明。

简易设置网络配置页面

导航栏上的简易设置功能列出了网络配置的基本设置，包括系统名称、IP 地址以及在无线电网络中的角色。



Easy Setup (简易设置) 页面上的网络配置设置

这是 Easy Setup (简易设置) 下的 Network Configuration (网络配置) 页面。 Easy Setup (简易设置) 包含了 Network (网络) 页面的参数缩写版本。

图 30 - 网络配置简易设置

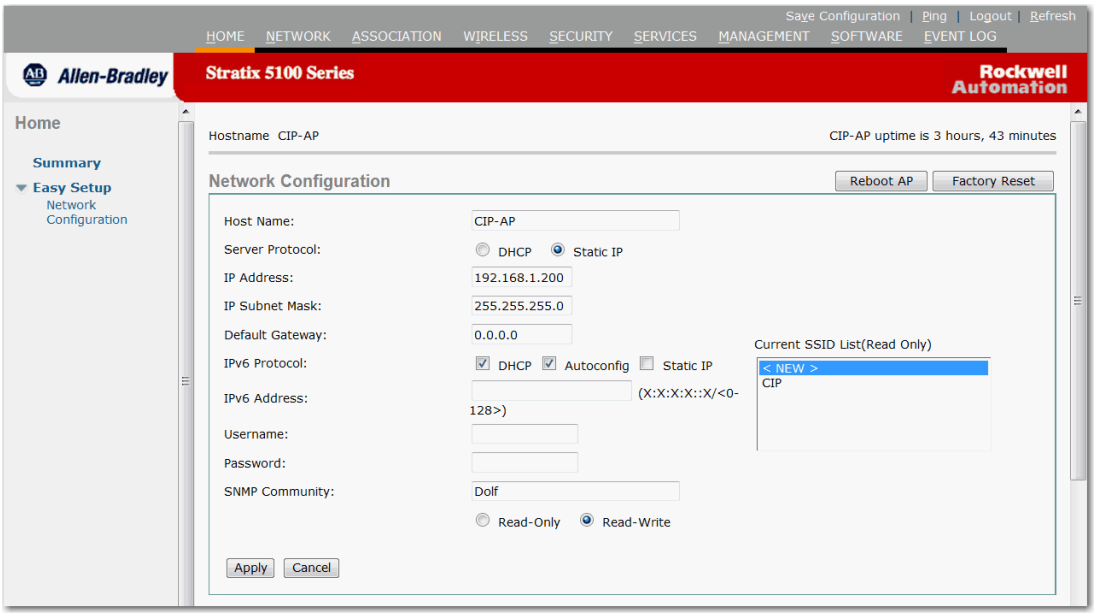


表 10 - 网络配置参数描述

参数	描述
Host Name	主机名称虽然不是关键设置，但有助于识别网络中的无线设备。主机名称将显示为管理系统页面中的标题。 系统名称最多可使用 32 个字符。但当无线设备识别为客户端设备时，它只使用系统名称的前 15 个字符。如果需要让客户端用户清楚区分无线设备，则确保系统名称的前 15 个字符是唯一的。 **警告：**当更改系统名称时，无线设备复位无线电通信，导致相关客户端设备解除关联并断开。
Server Protocol	选择匹配网络 IP 地址分配方式的项目。 • DHCP—— 由网络 DHCP 服务器自动分配 IP 地址。 • Static IP (静态 IP)—— 无线设备使用您在 IP 地址域中输入的静态 IP 地址。
IP Address	使用该设置分配或更改无线设备 IP 地址。如果网络中启用了 DHCP，则将该域留空。 如果在使用 Web 浏览器界面或基于有线局域网的 Telnet 会话配置无线设备时更改了无线设备 IP 地址，将丢失到无线设备的连接。如果丢失了连接，将使用新的 IP 地址重新连接到无线设备。 • 如果未启用 DHCP，则在该域中输入的 IP 地址将成为设备的 IP 地址。 • 如果启用了 DHCP，则该域仅当服务器以设备的 IP 地址响应时提供 IP 地址。 按照第 53 页的 " 使用 GUI 复位到默认设置 " 或第 203 页的 " 使用 CLI 恢复默认设置 " 中的步骤操作。
IP Subnet Mask	输入网络管理员提供的 IP 子网掩码，从而在局域网上识别 IP 地址。 • 如果未启用 DHCP，则该域是子网掩码。 • 如果启用了 DHCP，该域仅在服务器响应 DHCP 请求时才提供子网掩码，否则留空。
Default Gateway	输入网络管理员提供的默认网关 IP 地址。如果启用了 DHCP，则将该域留空。
IPv6 Protocol	确定 IP 地址的分配方式，例如， DHCP、静态和自动分配。 互联网协议 (IP) 定义了计算机如何在网络上通信。支持 IPv6。 DCHP 自动配置 静态 IP
IPv6 Address	地址的值，例如， FE80::E690:69FF:FEAE:66D0 (X:X:X:X::X/<0-128>)
Username	想要使用该 WAP 的用户名。

表 10 - 网络配置参数描述 (续)

参数	描述
Password	想要使用该 WAP 的密码。
SNMP Community	• 要使用简单网络管理协议 (SNMP)，输入社区名称。 SNMP 是一种应用层协议，支持在 SNMP 管理工作站和代理之间进行面向消息的通信。当启用 SNMP 时，该社区名称将自动显示在授权用户列表中，供查看和更改管理系统。 • SNMP 社区字符串的作用类似于用户名，用于 SNMP 中的验证、隐私和授权服务。为该社区选择只读或读 / 写属性。 – 只读指示接入点只允许 SNMP 读访问。使用该选项，您将无法更改接入点配置设置。 – 读写指示接入点允许 SNMP 读和写访问。使用该设置，您可更改接入点配置。
Current SSID List	• 您已配置的 SSID 列表。

如果要在 CLI 中设置基本配置参数，请参见第 195 页的 “ 使用命令行界面配置 Stratix 5100 WAP”。

Easy Setup (简易设置) 页面上的无线电配置设置

此页包含关于 GigabitEthernet 和 Radio-802.11b、 Radio-802.11a 或 Radio-802.11g 接口的状态信息，具体信息取决于在接入点上安装的无线电装置。以下是来自 Network (网络) > Network Interface (网络接口) 的无线电设置的参数缩写。

图 31 - Network Configuration (网络配置) 页面上的无线电配置设置

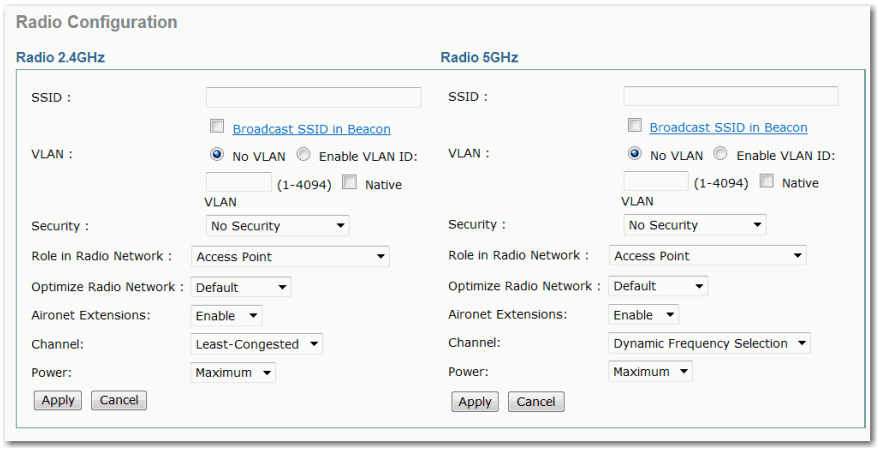


表 11 - 无线电配置参数描述

参数	描述
SSID	在信标中广播 SSID 标识客户端设备关联设备必须使用的 SSID。要启用无线电接口，必须先创建 SSID。SSID 帮助客户端设备区分临近区域的多个无线网络。 在该文本域中，不得使用这些字符：TAB、 ?、 $、 +、 !、 # 和 ;。
Security	• 无安全防护 • WEP 密钥 • EAP 验证 • WPA
VLAN	选择一个 VLAN 设置。 • VLAN 如果在无线局域网上使用 VLAN 并为 VLAN 分配 SSID，您可使用 Express Security (快速安全机制) 页面中四种安全设置的任意一种创建多个 SSID。但是，如果没有在无线局域网上使用 VLAN，则您分配给 SSID 的安全选项将受到限制，原因是 Express Security (快速安全机制) 页面的加密设置和验证类型是关联的。在没有 VLAN 的情况下，可为接口应用相关加密设置 (WEP 与密文)，例如， 2.4 GHz 无线电，但无法在该接口上使用多种加密设置。 • 无 VLAN 如果未使用 VLAN，则选择该设置。 • 启用 VLAN ID 如果要指定绑定 SSID 的虚拟以太网局域网识别号，则选择该设置。 • 本征 VLAN 如果希望该 VLAN ID 成为本征 VLAN，则选择该设置。
Access Point	如果无线设备连接到有线局域网，选择 Access Point (Root) (接入点 (根))。 根设备；接受来自客户端的关联，并将来自客户端的无线通信桥连到无线 LAN。该设置可应用于各种接入点。 指定设备作为连接到主以太网局域网网络的接入点运行。在该模式下，允许无线客户端设备关联到接入点。

表 11 - 无线电配置参数描述 (续)

参数	描述
Repeater	如果未连接到有线局域网，选择 Repeater (Non-root) (中继器 (非根))。 非根设备；接受来自客户端的关联，并将来自客户端的无线通信桥连到连接到无线局域网的根接入点。该设置可应用于各种接入点。 当禁用以太网端口时，无线设备成为中继器，并关联到附近的根接入点。您不必指定回退中继器关联的根接入点；中继器将自动关联到提供最佳无线电连接的根接入点。
Root Bridge	与非根网桥建立链接。 在该模式下，设备还接受客户端的关联，并且，它将直接连接到主以太网局域网网络。该模式不支持无线客户端关联。
Non-root Bridge	在该模式下，设备与根网桥建立链接。 指定设备作为非根网桥进行操作，连接到远程局域网网络，且必须使用无线接口与思科 Aironet 根网桥关联。
Workgroup Bridge	指定 WAP 作为通过以太网集线器或交换机连接到小型有线以太网局域网网络的工作组网桥工作。 在工作组网桥模式下， WAP 作为客户端关联到其他接入点，为连接到以太网端口的设备提供网络连接。工作组网桥必须关联到网络上的思科 Aironet 接入点。当将一个无线电接口配置为工作组网桥时，将自动禁用另一个无线电接口。
Universal Workgroup Bridge	提供了一种将 Stratix 5100 WAP 配置为工作组网桥 (WGBs) 并关联到非思科接入点的方法。此外，该功能还让 WGB 能够持续运行在 World 模式。
Scanner	指定接入点只能作为无线电扫描器工作，不接受来自客户端设备的关联。作为扫描器，接入点收集无线电数据，并将其发送给网络上的 WDS 接入点。 仅当与网络上的 WLSE 设备配合使用时才支持该选项。
Spectrum	指定 AP 作为专用型 RF 频谱传感器，与 Cisco Spectrum Expert 软件配合使用。
Optimize Radio Network for	使用该设置选择无线设备无线电的预配置设置，或者无线设备无线电的自定义设置。 选项有默认、范围和吞吐量。
Aironet Extensions	如果在无线局域网上只有罗克韦尔自动化 WAP 或思科 Aironet 设备，而设备作为接入点或工作组网桥工作，或设备作为中继器工作，则选择 Enable (启用)。要使用负载平衡、消息完整性检查 (MIC) 或临时密钥完整性协议 (TKIP) 等功能，必须将该设置设为 Enable (启用)。
Channel	• 2.4 GHz – 最不拥挤 – 通道号 / 频率 • 5 GHz – 动态频率选择 – 通道号 / 频率
Power	• 2.4 GHz – 最大比功率等级 (dBm) • 5 GHz – 最大比功率等级 (dBm)

Easy Setup (简易设置) 页面上的安全配置设置

您可为 Stratix 5100 WAP 配置有限数目的安全参数。有四种选择：

- No Security (无安全功能)
- WEP Key (WEP 密钥)
- EAP Authentication (EAP 验证)
- WPA

使用 Security (安全) 页面查看和配置接入点的安全设置。

您还可使用 CLI 配置安全，请参见第 204 页的 “ 安全 CLI 配置示例 ”。

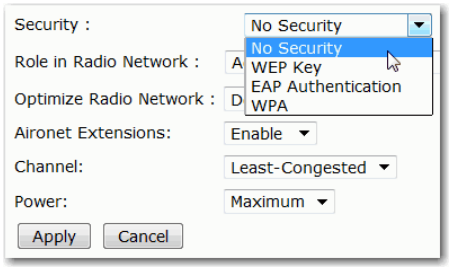
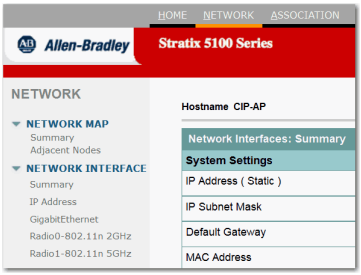


表 12 - Easy Set-up Security Setup (简易安全设置) 页面上的安全性类型

安全类型	描述	启用的安全功能
No Security	这是最不安全的一个选项。仅限对在公共场所中使用的 SSID 使用该选项，并将其分配给限制访问您的网络的 VLAN。	无
WEP Key	该选项比 No Security (无安全功能) 选项安全一些。 **警告：**静态 WEP 密钥很容易受到攻击。WEP 安全机制是一种不应再使用的传统方法。	强制输入 WEP。由于该 SSID 不具备与无线设备密钥匹配的 WEP 密钥，客户端设备无法使用其进行关联。
EAP Authentication	该选项启用 802.1X 验证，例如， LEAP、 PEAP、 EAP-TLS、 EAP-FAST、 EAP-TTLS、 EAP-GTC、 EAP-SIM 和其他基于 802.1X/EAP 的产品。 该设置使用强制加密、 WEP、开放式验证 + EAP、网络 EAP 验证、无密钥管理以及 RADIUS 服务器验证端口 1645。 您必须为网络上的验证 RADIUS 服务器输入 IP 地址和共享密钥 (服务器验证端口 1645)。因为 802.1X 验证提供动态加密密钥，因此，无需输入 WEP 密钥。 如果网络中没有 RADIUS 服务器，则应考虑使用接入点作为本地验证服务器，请参见第 49 页的 “Stratix 5100 设备管理器配置启动 ”。	强制 802.1X 验证。使用该 SSID 关联的客户端设备必须执行 802.1X 验证。 如果将无线电客户端配置为使用 EAP-FAST 验证，则也可配置开放式验证 + EAP。如果未配置使用开放式验证 + EAP，则将显示下列 GUI 警告消息： 警告：网络 EAP 仅用于 LEAP 验证。如果将无线电客户端配置为使用 EAP-FAST 验证，则也可配置开放式验证 + EAP。 如果使用的是 CLI，则将显示该警告消息： SSID 配置警告：[SSID]：如果无线电客户端使用的是 EAP-FAST，则必须配置使用开放式验证 + EAP。
WPA	Wi-Fi 保护访问 (WPA) 允许无线访问通过验证服务器的服务对照数据库验证的用户，然后使用比 WEP 更强的算法加密它们的 IP 通信。 该设置使用加密密文、 TKIP、开放式验证 + EAP、网络 EAP 验证、强制密钥管理 WPA 和 RADIUS 服务器验证端口 1645。 当使用 EAP 验证时，您必须为网络上的验证 RADIUS 服务器输入 IP 地址和共享密钥 (服务器验证端口 1645)。	强制 WPA 验证。使用该 SSID 关联的客户端设备必须支持 WPA。 如果将无线电客户端配置为使用 EAP-FAST 验证，则必须配置开放式验证 + EAP。如果未配置使用开放式验证 + EAP，则将显示下列 GUI 警告消息： 警告：网络 EAP 仅用于 LEAP 验证。如果将无线电客户端配置为使用 EAP-FAST 验证，则必须配置开放式验证 + EAP。 如果使用的是 CLI，则将显示该警告消息： SSID 配置警告：[SSID]：如果无线电客户端使用的是 EAP-FAST，则必须配置使用开放式验证 + EAP。

Network (网络) 页面

Network (网络) 页面包含关于网络地图和相邻节点的信息。Network Interface (网络接口) 页面给出了 GigabitEthernet 和 Radio-802.11b、Radio-802.11a 或 Radio-802.11g 接口的状态，具体状态取决于在接入点上安装的无线电装置。



为网络地图功能选择 Enable (启用) 或 Disable (禁用)。若选择 Enable (启用)，最好在离开该页面前返回默认设置 Disable (禁用)，因为发现网络所需的时间会大大提高系统负载。

图 32 - Network Map (网络映射)

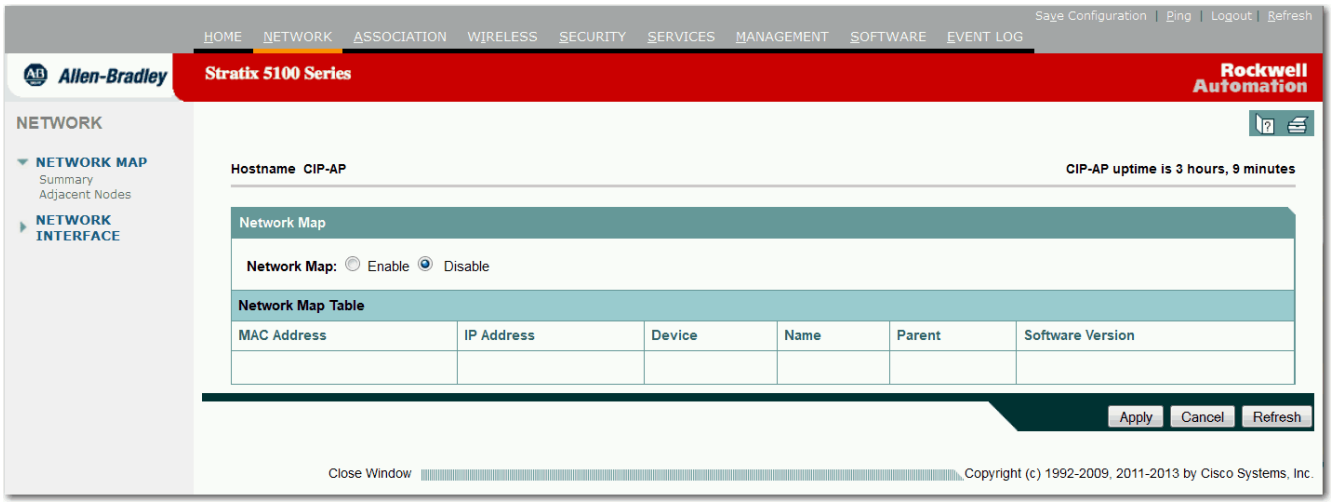


表 13 - Stratix 5100 网络映射参数描述

项目	描述
Network Map	
Summary	Network Map (网络映射) 页面提供无线网络上各设备的信息。Network Map (网络映射) 页面不列出局域网上的有线设备。如果需要查看局域网上的有线设备，请参见第 103 页的 "Association (关联) 页面 "。选择 Enable (启用) 查看网络映射。如果选择了 Enable (启用)，在离开页面之前，切回 Disable (禁用)，因为搜索网络时会大大增加系统负载。
MAC Address	制造商为设备分配的唯一标识符。
IP Address	端口的 IP 地址。
Device	设备类型 (客户端、接入点、网桥等)。
Name	赋予该设备的名称。
Software Version	设备上当前运行的软件版本。
Radio	指定无线电为 802.11a 或 802.11b。

表 13 - Stratix 5100 网络映射参数描述 (续)

项目	描述
Channel	指定无线电使用的通道。
Age (hrs)	指定接入点在临近接入点列表中的保留时长，不活动时间超过该时长将被从列表中删除。
SSID	标识客户端设备关联设备必须使用的 SSID。 SSID 帮助客户端设备用于识别临近的多个无线网络。
Adjacent Nodes	这是接入点在临近接入点列表中的保留时长，不活动时间超过该时长将被从列表中删除。 AP 寿命超时 1…1000 小时

Network Interface Summary (网络接口概览) 页面

网络接口

- 概览
- IP 地址
- 千兆以太网
- Radio0-802.11n 2.4 GHz
- Radio1-802.11n 5 GHz

Summary (概览) 页面包含关于 GigabitEthernet 和 Radio-802.11b、Radio-802.11a 或 Radio-802.11g 接口的状态信息，具体信息取决于在接入点上安装的无线电装置。

图 33 - Network Interface Summary (网络接口概览) 页面

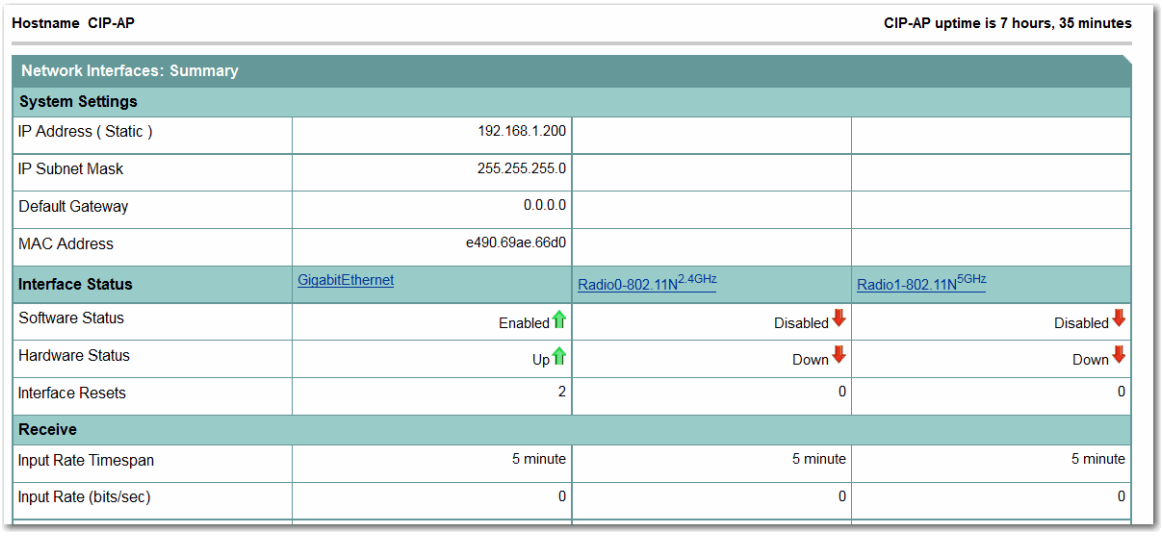


表 14 - 系统设置参数描述

系统设置	描述
IP Address (DHCP) / IP Address (Static)	接入点的 IP 地址。 IP 地址可使用 DHCP 动态分配，或静态指定。
IP Subnet Mask	IP 子网掩码用于标识子网，以便在局域网上识别 IP 地址。
Default Gateway	在此显示默认互联网网关的 IP 地址。
MAC Address	介质访问控制地址是制造商分配给网络接口的唯一标识符。
Interface Status	GigabitEthernet、 Radio0-802.11N$^{2.4\ GHz}$ 和 Radio0-802.11N$^{5\ GHz}$ 的状态。
Software Status	指示 GigabitEthernet、 Radio-802.11b、 Radio-802.11a 或 Radio-802.11g 接口是被操作员启用还是禁用。
Hardware Status	指示 GigabitEthernet、 Radio-802.11a、 Radio-802.11b 或 Radio-802.11g 接口的线路协议是上行还是下行。
Interface Resets	接口被完全重置的次数。
Input Rate Timespan	输入速率时间跨度
Input Rate (bits/sec)	在指定输入速率时间跨度内每秒钟发送的平均位数。
Input Rate (packets/sec)	在指定输入速率时间跨度内每秒钟发送的平均数据包数。
Time Since Last Input	自从上次从接口成功接收数据包以来的时间 (小时、分钟和秒格式)。知晓该时间有助于确定接口的负载，从而帮助定位网络问题。
Total Packets Input	系统接收到的无错数据包总数。
Total Bytes Input	系统接收到的无错字节总数。
Broadcast Packets	系统接收到的广播数据包总数。
Total Input Errors	发生的与输入相关的错数总数，包括超短帧、超长帧、无缓冲区、 CRC、帧、超限和忽略计数等错误。
Overrun Errors	因输入速率超过接收器的数据处理能力，而使接收器硬件无法将接收到的数据发送到硬件缓冲区的次数。
Ignored Packets	因接口硬件的内部缓冲区不足，而使接收到的数据包被接口忽略的数量。广播风暴和噪声会导致被忽略的次数增加。
Throttles	可能因缓冲区或处理器过载，而使端口上的接收器被禁用的次数。
Output Rate Timespan	输出速率的时间跨度。
Output Rate (bits/sec)	在指定输出速率时间跨度内每秒钟发送的平均位数。
Output Rate (packets/sec)	在指定输出速率时间跨度内每秒钟发送的平均数据包数。
Time Since Last Output	自从上次接口成功发送数据包以来的时间 (小时、分钟和秒格式)。知晓该时间有助于确定接口的通信负载，从而帮助定位网络问题。
Total Packets Output	系统发送的消息总数。
Total Bytes Output	系统发送的字节总数，包括数据和 MAC 封装。
Total Output Errors	致使无法检查从接口最终传输出去的数据包的各种错误总数。

表 14 - 系统设置参数描述 (续)

系统设置	描述
Last Output Hang	自上一次接口因传输耗时太长重置以来，所经过的小时数、分钟数和秒钟数 (或从未有)。 如果 Time Since Last Input (自上次输入以来的时间)、 Time Since Last Output (自上次输出以来的时间) 或 Last Output Hang (上次输出重置) 域中的小时数超过 24 小时，将显示天数和小时数。
Lost Parent Counts (Repeater Mode Only)	• 无信标 中继器停止从父级接入点接收信标的次数。父级接入点可能不在范围内。平均重试水平 • 未验证 中继器从父级接入点收到未验证数据包的次数。 • 解除关联 中继器从父级接入点收到解除关联数据包的次数。 • 时基丢失 中继器的时基广播更改为一个过大的量的次数。父级接入点可能已重启。 • 主机请求 中继器和父级接入点之间的链接的重启次数。操作员更改了分配的父级接入点。 • 找到更好的父接入点 因当前父级接入点信号变弱，中继器切换到新的父级接入点的次数。
Association Statistics (Repeater Mode Only)	如果未将中继器分配给父级接入点，请记下这些统计信息。 • SSID 不匹配 中继器接收到不匹配所请求的 SSID 的信标或探测响应的次数。 • 非指定 AP 中继器从未在父级接入点列表中配置的父级接入点接收到响应的次数。 • 速率不匹配 中继器从不支持所请求速率的父级接入点接收到响应的次数。 • 隐私不匹配 中继器从不支持所请求隐私设置的父级接入点接收到响应的次数。 • 验证被拒次数 中继器从包含不成功状态的父级接入点接收到验证响应的次数。 • 关联超时 中继器未从父级接入点接收到关联请求响应的次数。

Network Interface IP Address (网络接口 IP 地址) 页面

使用此页来确定配置服务器协议，并确定 IP 地址、 IP 子网掩码和默认网关的 IP 地址。

图 34 - 网络接口 IP 地址

表 15 - IP 地址参数描述

参数	描述
Configuration Server Protocol	根据匹配网络的 IP 地址分配方法设置该参数。如果网络服务器使用 IP 地址自动分配，则选择 DHCP。如果分配固定 IP 地址，则选择 Static IP (静态 IP)。如果需要兼容旧 DHCP 服务器，则选择 Disable DHCP Address Binding (禁用 DHCP 地址绑定)。通常无需选中该复选框。如果选中该复选框，将不会向 DHCP 服务器发送客户端标识符。 DHCP 服务器需要使用客户端标识符来发布一致的 IP 地址。 注意：如果将接入点配置为 DHCP 服务器，则其将为子网中的设备分配 IP 地址。子网中的设备可与其他设备通信，但无法跨子网通信。如果需要跨子网传送数据，则必须分配一个默认路由器。
IP Address	使用该设置分配或更改接入点的 IP 地址。如果网络未启用 DHCP，则在该域中输入的 IP 地址将成为接入点的 IP 地址。如果启用了 DHCP，则无法修改该域。
IP Subnet Mask	输入 IP 子网掩码来标识子网，以便在局域网上识别 IP 地址。如果未启用 DHCP，该域将是子网掩码。如果启用了 DHCP，则无法修改该域。
默认网关 IP 地址	输入网络的默认网关的 IP 地址。如果启用了 DHCP，则无法修改该域，除非选择了 Override DHCP Default Gateway (覆盖 DHCP 默认网关)。
覆盖 DHCP 默认网关	该设置可用于更改 DHCP 服务器协商的默认网关。启用该功能可停止到接入点的通信；因此，我们建议直接使用 DHCP 服务器所分配的网关，不要改动。

Network Interface GigabitEthernet Status (网络接口 GigabitEthernet 状态) 页面

使用此页面查看 GigabitEthernet 接口的状态。

图 35 - Network Interface GigabitEthernet Status (网络接口 GigabitEthernet 状态) 页面

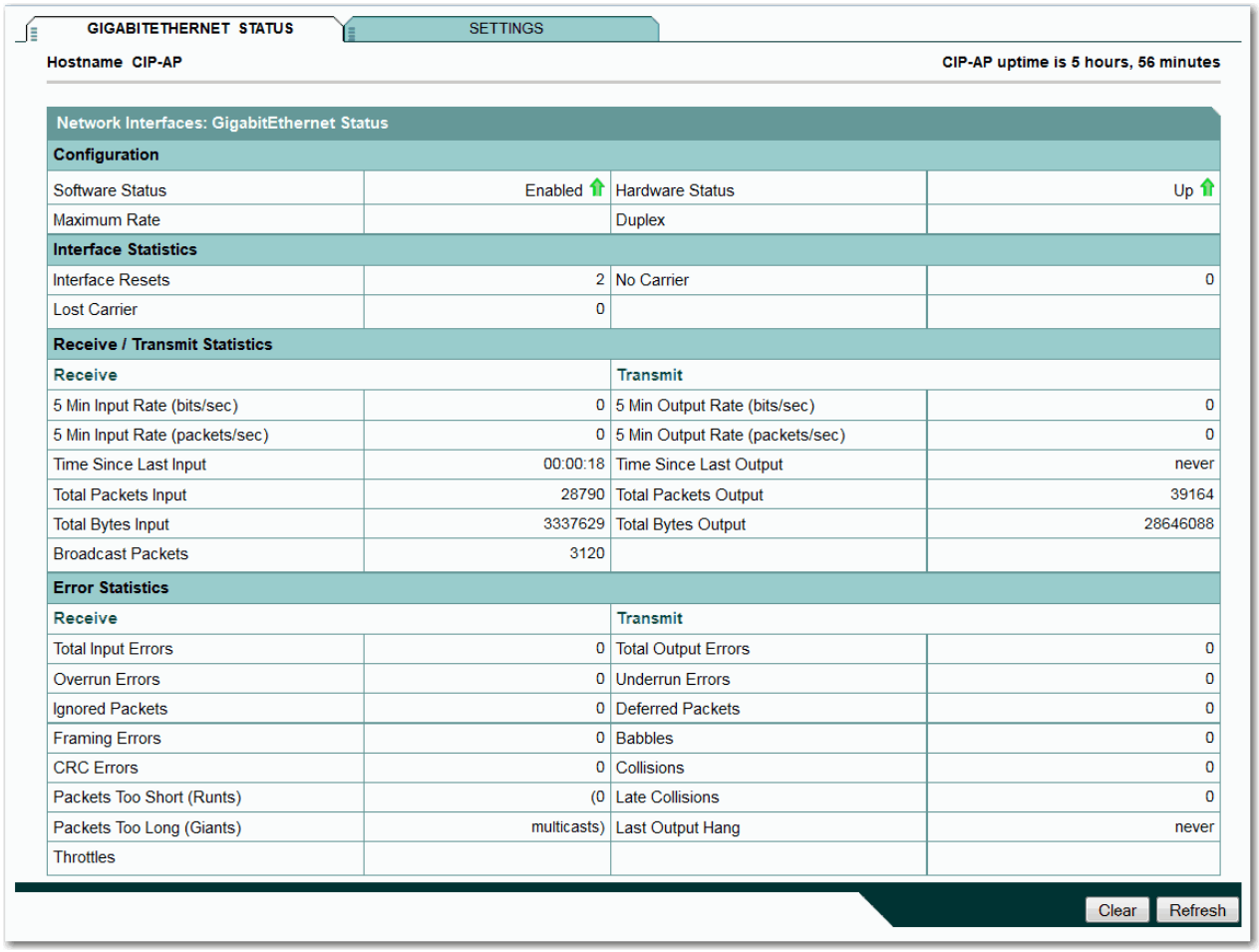


表 16 - 千兆以太网状态参数描述

参数	描述
Configuration	
Software Status	指示接口被操作员启用还是禁用。
Hardware Status	指示接口的线路协议是上行还是下行。
Maximum Rate	以太网接口的速率设置：10 Mbps、 100 Mbps 或 1Gbps。
Duplex	以太网接口的双工设置：半双工或全双工。
Interface Statistics	
Interface Resets	接口被完全重置的次数。
No Carrier	传输期间发生运营商不存在的次数。
Lost Carrier	传输期间发生运营商丢失的次数。

表 16 - 千兆以太网状态参数描述 (续)

参数	描述
Receive Statistics	
5 min Input Rate (bits/sec)	在过去 5 分钟里平均每秒钟发送的位数。
5 min Input Rate (packets/sec)	在过去 5 分钟里平均每秒钟发送的数据包数。
Time Since Last Input	自从上次从接口成功接收数据包以来的时间 (小时、分钟和秒格式)。知晓该时间有助于确定接口的通信负载，从而帮助定位网络问题。
Total Packets Input	系统接收到的无错数据包总数。
Total Bytes Input	系统接收的字节总数，包括数据和 MAC 封装。
Broadcast Packets	系统接收到的广播数据包总数。
Transmit Statistics	
5 min Output Rate (bits/sec)	在过去 5 分钟里平均每秒钟发送的位数。
5 min Output Rate (packets/sec)	在过去 5 分钟里平均每秒钟发送的数据包数。
Time Since Last Output	自从上次接口成功发送数据包以来的时间 (小时、分钟和秒格式)。知晓该时间有助于确定接口的通信负载，从而帮助定位网络问题。
Total Packets Output	系统发送的消息总数。
Total Bytes Output	系统发送的字节总数，包括数据和 MAC 封装。
Error Statistics/Receive	
Total Input Errors	发生的与输入相关的错数总数，包括超短帧、超长帧、无缓冲区、 CRC、帧、超限和忽略计数等错误。
Overrun Errors	因输入速率超过接收器的数据处理能力，而使接收器硬件无法将接收到的数据发送到硬件缓冲区的次数。
Ignored Packets	因接口硬件的内部缓冲区不足，而使接收到的数据包被接口忽略的数量。广播风暴和噪声会导致被忽略的次数增加。
Framing Errors	不正确地接收到有 CRC 错误和非整数 8 位字节的数据包数。这些错误因以太网冲突或故障而发生在局域网中。
CRC Errors	由原始局域网工作站或远端设备生成的循环冗余校验和与从接收数据计算得到的校验和不匹配。这些错误指示局域网接口或局域网总线本身存在噪声或传输问题。大量的 CRC 错误通常会导致冲突或传输不良数据。
Packet too Short (Runts)	因小于介质的最小数据包大小而被丢弃的数据包数。例如，任何小于 64 字节的以太网数据包都将视为超短帧。
Packet too Long (Giants)	因大于介质的最大数据包大小而被丢弃的数据包数。例如，任何大于 1,518 字节的以太网数据包都将视为超长帧。
Throttles	可能因缓冲区或处理器过载，而使端口上的接收器被禁用的次数。
Error Statistics/Transmit	
Total Output Errors	致使无法检查最终传输数据包的各种错误总数。
Underrun Errors	发射器运行速率快于路由器处理能力的次数。
Deferred Packets	长时间延期的数据包数。
Babbles	发送 Jabber 时间超时次数。

表 16 - 千兆以太网状态参数描述 (续)

参数	描述
Collisions	由于以太网冲突而重新发送的数据包数 (仅适用于半双工模式)。
Late Collisions	后期冲突数。该冲突通常是因为局域网铺设的过长而造成，比如，以太网或收发器电缆太长，使用的级联多端口收发器太多，或工作站之间使用了多个中继器。
Last Output Hang	自上一次接口因传输耗时太长重置以来，所经过的小时数、分钟数和秒钟数 (或从未有)。当 Time Since Last Input (自上次输入以来的时间)、Time Since Last Output (自上次输出以来的时间) 或 Last Output Hang (上次输出重置) 域中的小时数超过 24 小时，将显示天数和小时数。

网络接口： GigabitEthernet 设置

您可使用该设置页面定义物理设置和 AP 验证。

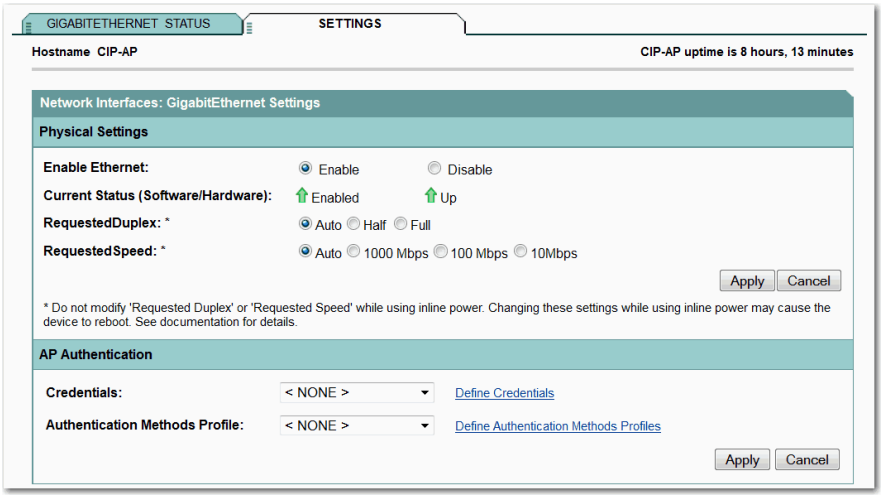


表 17 - 千兆以太网参数描述

参数	描述
Physical Settings	
Enable Ethernet	启用 禁用
Current Status	启用 上行
Requested Duplex	以太网接口的双工设置： Auto (自动)、 Half (半双工) 和 Full (全双工)。 **重要事项：** 当使用内部电源时，不要修改请求的双工。使用内部电源时更改这些设置可能导致设备重启。
Requested Speed	自动 1000 Mbps 100 Mbps 10 Mbps **重要事项：** 当使用内部电源时，不要修改请求的速度。使用内部电源时更改这些设置可能导致设备重启。
AP Authentication	
Credentials	选择凭证或单击 Define Credentials (定义证书) 跳转到 AP Authentication (AP 验证)，您可在此定义所需的证书。
Authentication Methods Profile	选择配置文件或单击 Authentication Methods Profile (验证方法配置文件) 跳转到 AP Authentication (AP 验证)，您可在此定义所需的配置文件。

网络接口： Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 状态

Radio Status (无线电状态) 和 Detailed Status (详细状态) 页面提供了当前无线电接口配置和统计数据的概览。

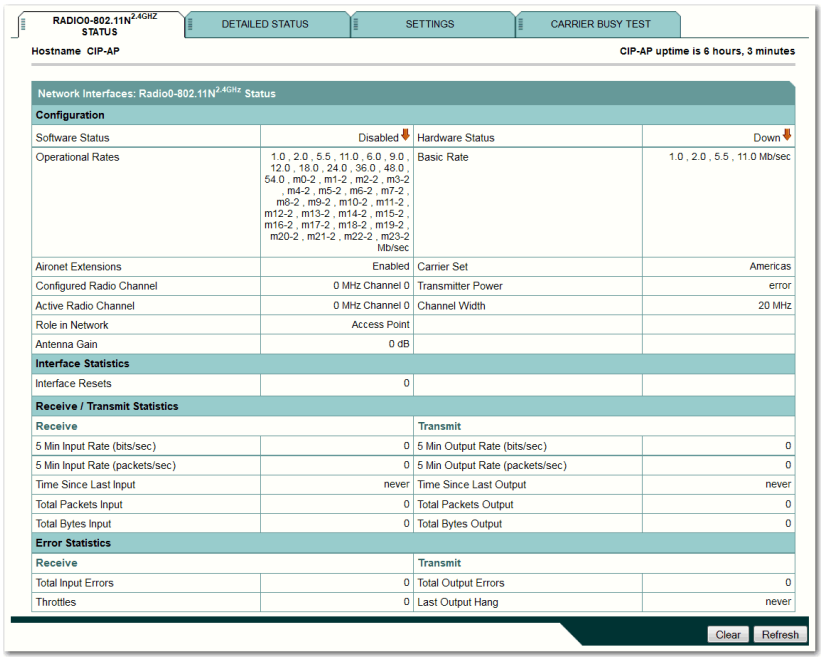


表 18 - 无线电接口配置和统计信息参数描述

参数	描述
Configuration	
Software Status	指示接口被操作员启用还是禁用。
Operational Rates	设备用于传输数据的数据传输速率 (以 Mb/s 表示)。设备始终尝试以所选的最高速率发送数据。如果发生阻碍或干扰，设备将逐级下降到能够传输数据的最高速率。
Aironet Extensions	如果需要与非思科 /Aironet 产品兼容，则取消选择 Aironet Extensions (Aironet 扩展)。禁用该选项将限制接入点的多个高级功能，例如， MIC 和 TKIP。
Carrier Set	指示接入点工作的法定域。运营商设置限制了可用的频率和功率等级。
Current Radio Channel	802.11b、 802.11a 或 802.11g 无线的当前通道和频率。
Transmitter Power	无线传输的功率等级。默认功率设置为法定域所允许的最高发送功率。
Hardware Status	指示接口的线路协议是上行还是下行。通常，如果启用了 Software Status (软件状态)， Hardware Status (硬件状态) 将为上行。如果启用了 Software Status (软件状态)，而 Hardware Status (硬件状态) 为下行，则将出错。
Basic Rate	启用单播和多播时所有数据包在该速率下传输。必须至少将一个数据传输速率设置为基本速率。
Role in Network	接入点 (根) 模式下的 Stratix 5100 将无线客户端连接到有线网络。 工作组网桥模式下的 Stratix 5100 变为根 AP 的无线客户端，用于通过无线链接连接一个或多个有线客户端。
Antenna Gain	可查看天线增益状态。您可使用 Web 界面设置增益 (Radio Interface - Detailed Settings (无线接口 - 详细设置))。

表 18 - 无线电接口配置和统计信息参数描述 (续)

参数	描述
Interface Statistics	
Interface Resets	接口被完全重置的次数。
Receive Statistics	
5 min Input Rate (bits/sec)	在过去 5 分钟里平均每秒钟接收的位数。
5 min Input Rate (packets/sec)	在过去 5 分钟里平均每秒钟接收的数据包数。
Time Since Last Input	自从上次接口成功发送数据包以来的小时数、分钟数和秒钟数。知晓该时间有助于确定接口的通信负载，从而帮助定位网络问题。
Total Packets Input	系统接收到的无错数据包总数。
Total Bytes Input	系统接收的字节总数，包括数据和 MAC 封装。
Transmit Statistics	
5 min Output Rate (bits/sec)	在过去 5 分钟里平均每秒钟发送的位数。
5 min Output Rate (packets/sec)	在过去 5 分钟里平均每秒钟发送的数据包数。
Time Since Last Output	自从上次接口成功发送数据包以来的时间 (小时、分钟和秒格式)。知晓该时间有助于确定接口的通信负载，从而帮助定位网络问题。
Total Packets Output	系统发送的消息总数。
Total Bytes Output	系统发送的字节总数，包括数据和 MAC 封装。
Error Statistics	
Total Input Errors	发生的与输入相关的错数总数，包括超短帧、超长帧、无缓冲区、 CRC、帧、超限和忽略计数等错误。
Total Output Errors	致使无法检查最终传输数据包的各种错误总数。
Last Output Hang	自上一次接口因传输耗时太长重置以来，所经过的小时数、分钟数和秒钟数 (或从未有)。当 Time Since Last Input (自上次输入以来的时间)、 Time Since Last Output (自上次输出以来的时间) 或 Last Output Hang (上次输出重置) 域中的小时数超过 24 小时，将显示天数和小时数。
Throttles	可能因缓冲区或处理器过载，而使端口上的接收器被禁用的次数。

详细状态

该页面显示了接口的详细状态信息。

图 36 - 接口详细状态

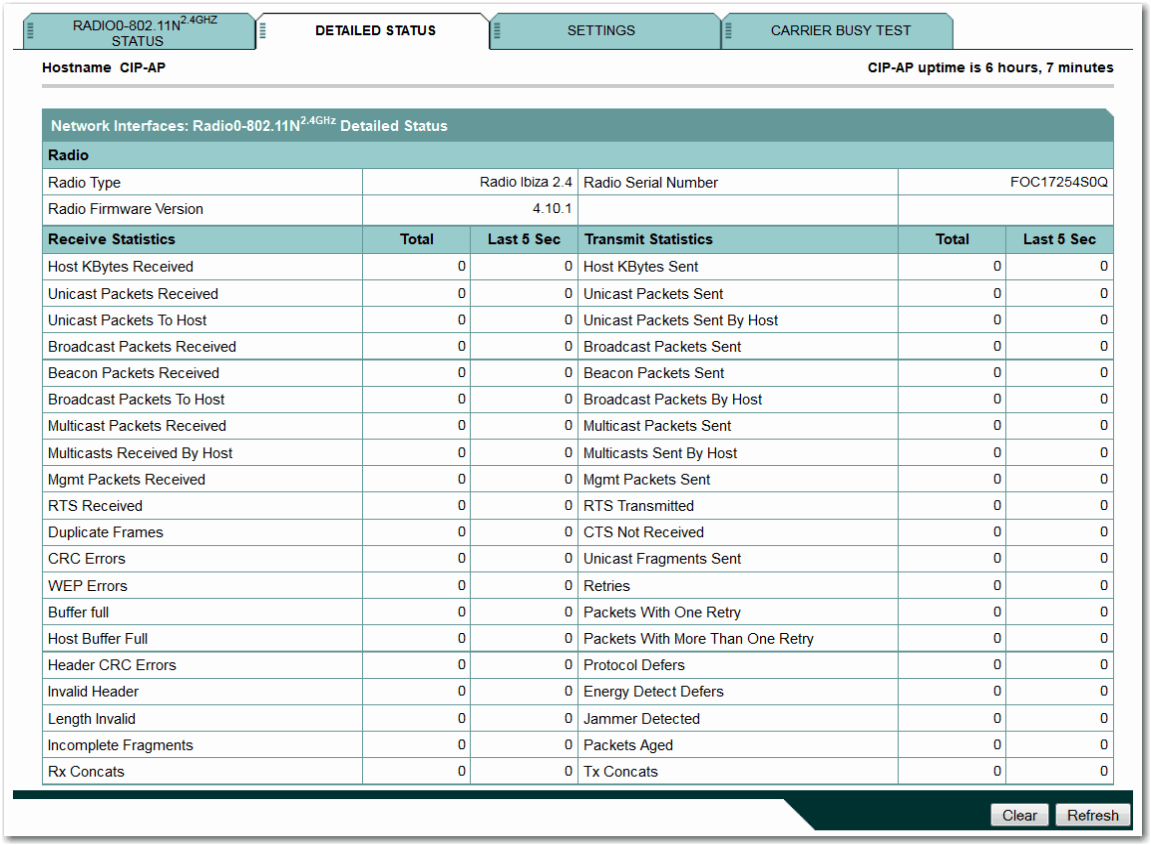


表 19 - 网络接口： Radio0-802.11N2.4 GHz 和 5 GHz 详细状态

参数	描述
Radio	
Radio Type	列出接口和序列号。
Radio Firmware Version	WAP 上安装的当前固件版本。
Receive/Transmit Statistics	
Host Kilobytes Received/Sent	服务器发送和接收的千字节数。
Unicast Packets Received/Sent	点对点通信中接收 / 发送的单播数据包数。
Unicast Packets Sent To Host/By Host	由服务器接收 / 发送的单播数据包数。
Broadcast Packets Received/Sent	由接入点接收 / 发送的广播数据包数。
Beacon Packets Received/Sent	由接入点接收 / 发送的信标数据包数。
Broadcast Packets To Host/By Host	由服务器接收 / 发送的广播数据包数。
Multicast Packets Received/Sent	• 接收的数据包数 (向一组节点发送)。 • 发送的数据包数 (向一组节点发送)。

表 19 - 网络接口： Radio0-802.11N2.4 GHz 和 5 GHz 详细状态 (续)

参数	描述
Multicasts Received/Sent By Host	由服务器接收 / 发送的多播数据包数。
Mgmt Packets Received/Sent	由接入点接收 / 发送的管理数据包数。
RTS Received/Transmitted	接入点接收的旨在响应 RTS 帧的 CTS 帧数。
Duplicate Frames	带有序列控制域，指示接收到重复帧的次数。
CTS Not Received	未被接入点接收到的 CTS 帧数。
CRC Errors	显示带 CRC 错误的数据包数。
Unicast Fragments Sent	接入点已发送的帧的片段数。
WEP Errors	因接入点无法解密或未加密而被丢弃的帧数。
Retries	尝试发送数据包的次数。
Buffer full	发送到发送设备的消息，要求暂停传输，直到缓冲区中的数据已被处理。
Packets With One Retry	一次重试发送的数据包数。
Host Buffer Full	发送到发送设备的消息，要求暂停传输，直到缓冲区中的数据已被处理。
Packets With More Than One Retry	多次重试发送的数据包数。
Header CRC Errors	接收到的表头 CRC 错误的数量。
Protocol Defers	发送的协议延期数量。
Invalid Header	接收到的无效表头数量。
Energy Detect Defers	发送的能量检测延期数量。
Length Invalid	接收到的长度无效的数据包数。
Jammer Detected	检测到的拥堵设备的数量。
Incomplete Fragments	接收到的片段数据包数量。
Rx/Tx Contacts	接收和发送

Network Interface Radio Settings (网络接口无线电设置) 页面

Setting (设置) 页面提供了待配置接口的详细参数设置。这些参数与 Easy Setup (简易设置) 页面中部分重复。

图 37 - Interface Settings (接口设置) 页面

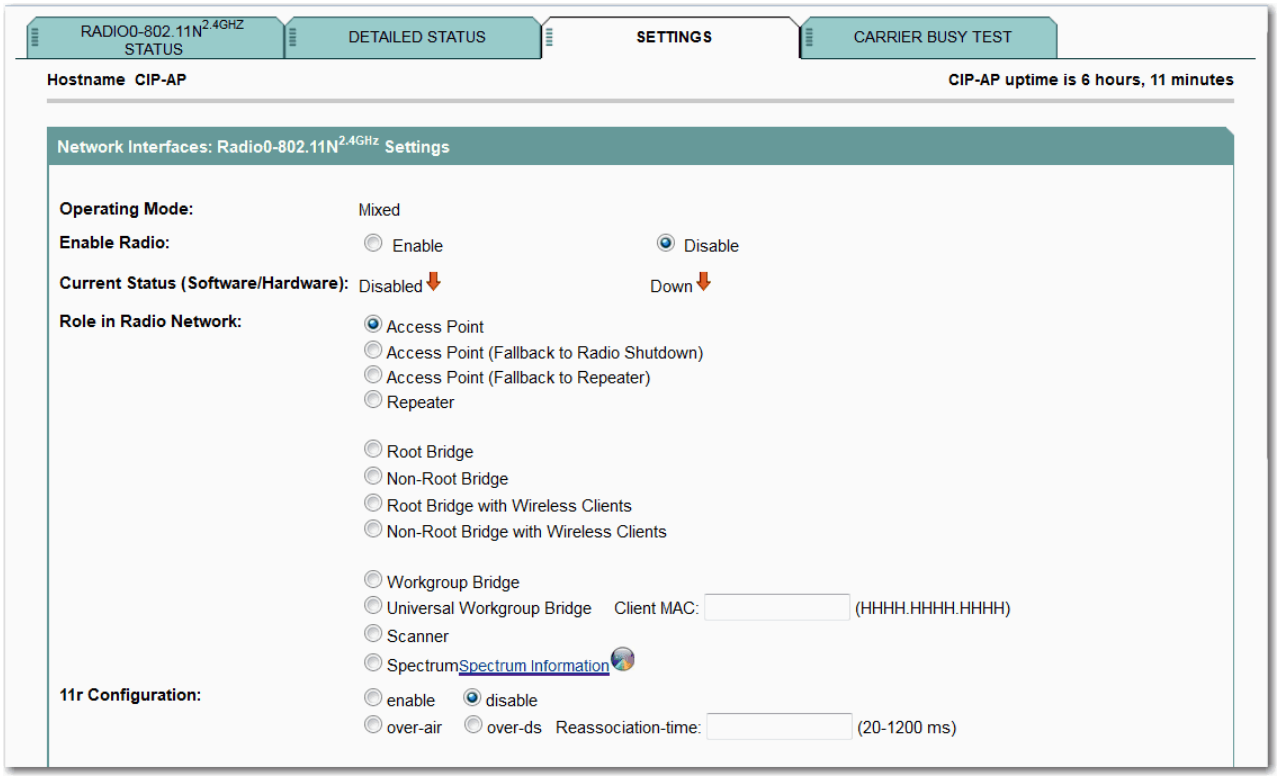


表 20 - Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 设置描述

参数	描述
Operating Mode	该值指示无线是否支持多种协议，例如， 802.11b、 802.11g 或 802.11n。 混合模式下的无线电装置同时支持多个客户端。
Enable Radio	用于启用无线电。您可在简易设置页中设置一些参数，但要启用无线电，需要跳转到该页面。 通过 Network (网络) > Network Interface (网络接口) > Radio0-802.11n 2 GHz (或 Radio0-802.11n 5 GHz) > Settings (设置) 启用无线电。

表 20 - Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 设置描述（续）

参数	描述
Current Status	该值来自于上方的单选按钮。如果将无线电设为启用，该值将相应变化。 • 软件状态 — 上行 / 下行 / 禁用 • 硬件状态 — 上行 / 下行 / 重置
Role in Radio Network	用于选择无线电网络中的角色。选项有： • 接入点 • 中继器 • 根网桥 • 非根网桥 • 安装 • 工作组网桥 • 扫描器 • 频谱 更多详细信息，请参见第 82 页的 “ 无线电配置参数描述 ”。
11r Configuration	配置 802.11r 协议，以支持快速漫游。需要在网络中启用 WDS • 启用 • 禁用 • Over-air • Over-ds • 重新关联时间：(20…1200 ms)

图 38 - Interface Settings (接口设置) 页面 (续)

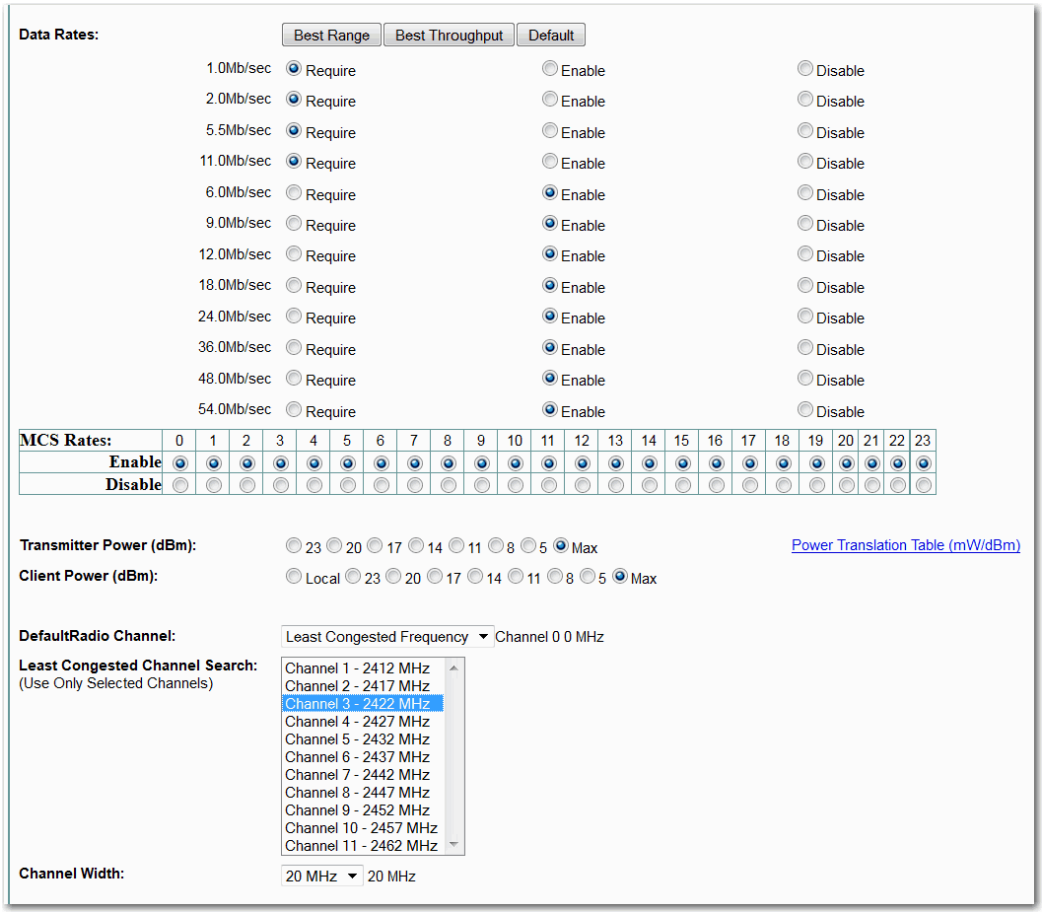


表 21 - Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 设置描述

参数	描述
Data Rates	• 默认 • 最佳范围 • 最佳吞吐量 • 1.0、 2.0、 5.5、 11.0、 6.0、 9.0、 12.0、 18.0、 24.0、 36.0、 48.0 和 54.0 Mbps • 需要、启用、禁用
MCS (802.11n) Rates	0…23 启用 禁用
Transmitter Power (dBm)	指定发射器功率设置 (dBm)。 2.4 和 5 GHz 无线的功率值不同。它们也会因场所和通道不同而异。
Client Power (dBm)	指定无线客户端用于与 AP 通信的功率设置。客户端根据该设置和本地配置值选择实际的发送功率等级。 2.4 和 5 GHz 无线的功率值不同。它们也会因场所和通道不同而异。
Default Radio Channel	最不拥挤通道搜索 (仅使用所选的通道)
Channel Width	20 MHz / 40 MHz

图 39 - Interface Settings (接口设置) 页面 (续)

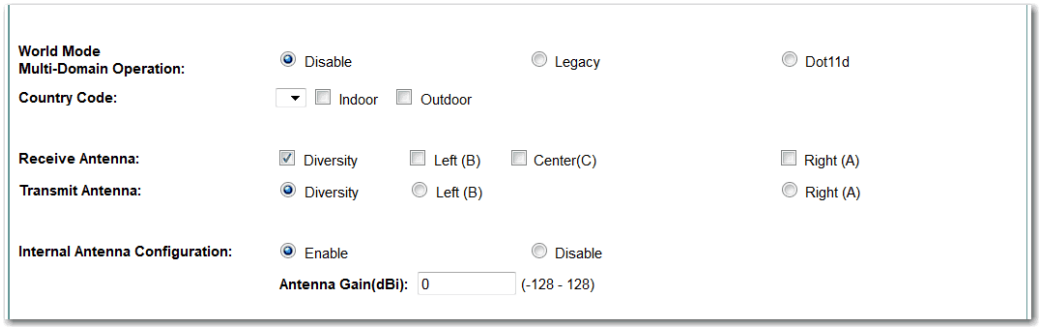
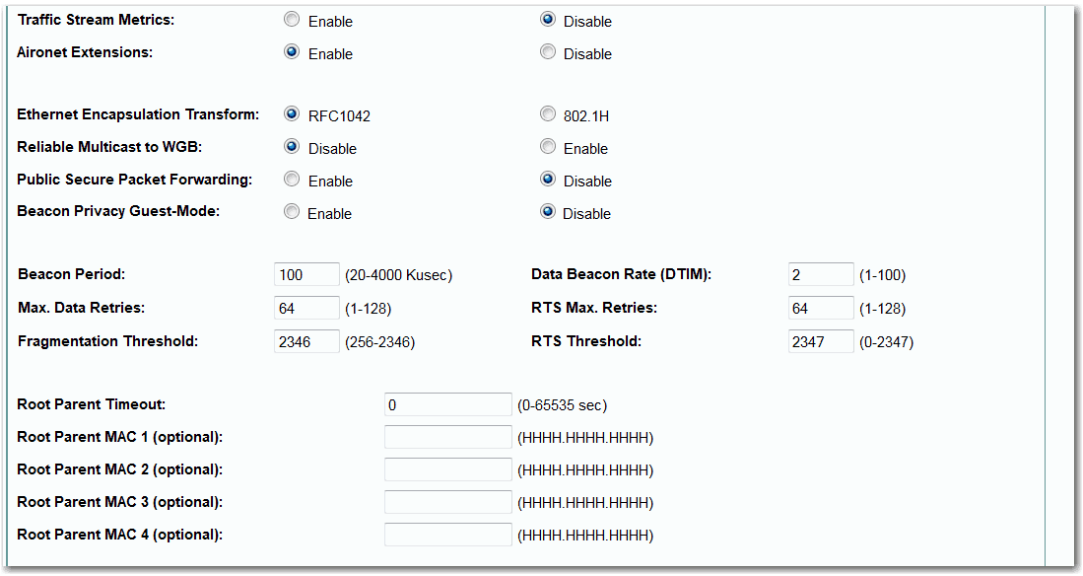


表 22 - Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 设置描述 (续)

World Mode Multi-Domain Operation	禁用 旧式 Dot11d
Country Code	国家代码、室内、室外 国家代码仅在 World Mode (世界模式) 配置为 802.11d 时可用。
Receive Antenna	分集 左 (B) 中 (C)
Transmit Antenna	分集 左 (B)
Internal Antenna Configuration	启用 禁用 天线增益 (dBi)：(-128…128)

图 40 - Interface Settings (接口设置) 页面 (续)



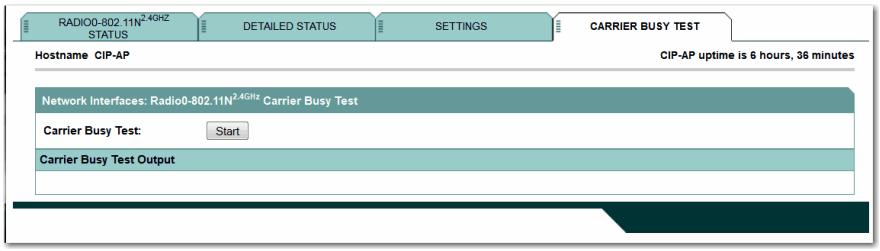
警告：下面的无线电设置是高级设置，通常禁止修改。

表 23 - Radio0-802.11n 2 GHz 和 Radio1-802.11n 5 GHz 设置描述 (续)

Traffic Stream Metric	启用 禁用
Aironet Extension	启用 禁用
Ethernet Encapsulation Transform	RFC1042 802.1H
Reliable Multicast to WGB	启用 禁用
Public Secure Packet Forwarding	启用 禁用
Beacon Privacy Guest-Mode	启用 禁用
Beacon Period	20…4000 Kusec
Data Beacon Rate (DTIM)	1…100
Max. Data Retries	1…128
RTS Max. Retries	1…128
Fragmentation Threshold	256…2346
RTS Threshold	0…2347
Root Parent Timeout	0…65535 s
Root Parent MAC 1…4 (optional)	HHHH.HHHH.HHHH

载波忙碌测试

您可执行载波忙碌测试，以检查无线通道上的无线电活动。在载波忙碌测试期间，无线设备断开无线网络设备的所有关联达 4 秒，同时执行载波测试，然后显示测试结果。该测试会干扰用户流量。



Association (关联) 页面

在 Association (关联) 页面中可查看与 AP (在根 AP 模式下) 或父 AP (在工作组网桥模式下) 关联的客户端信息。

图 41 - Association (关联) 页面

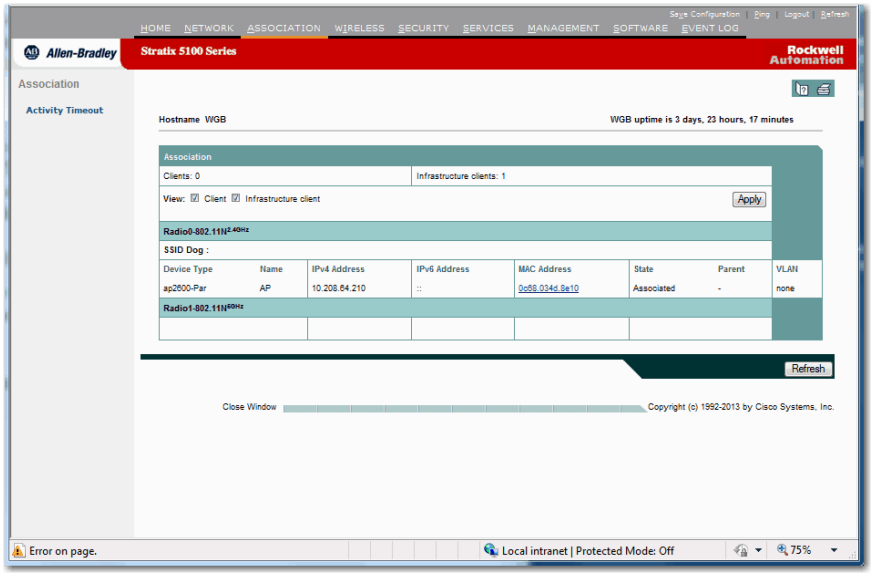


表 24 - Association (关联) 页面参数描述

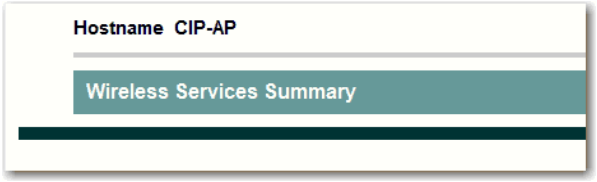
参数	描述
SSID	名称
Device Type	设备类型。
Name	显示设备的名称。
IP Address	客户端的 IP 地址。
State	客户端的状态可以是 Associated (已关联) 或 Association Processing (关联处理中)。
Parent	定义父级无线客户端设备。

表 24 - Association (关联) 页面参数描述 (续)

参数	描述
VLAN	标识 VLAN 是否已被分配给该客户端。
MAC Address	介质访问控制 (MAC) 地址是制造商分配给网络接口的唯一标识符。如果单击 MAC Address (MAC 地址) 链接，将跳转到 Association: Station View - Client (关联：工作站视图 — 客户端) 画面。
Activity Timeout	在该页面中，可指定接入点跟踪不活动设备的秒数。 • 设备类别 指定思科 Aironet 设备类别。 • 默认 (可选) 1…100000 s 指定当设备关联并提出零刷新率或不提出刷新率时，接入点使用的活动超时值。 • 最大值 (可选) 指定不管设备在关联时提出多大的刷新率，设备所允许的最大活动超时值。 • 网桥 — 网桥名称。 • 客户端工作站 — 客户端工作站名称。 • 中继器 — 中继器名称。 • 工作组网桥 — 工作组网桥名称。 • 未知 (非思科设备)— 未知设备的名称。

Wireless (无线) 页面

Wireless (无线) 页面提供无线服务概览。您可访问 AP 无线服务和 WDS/WNM 常规设置。



AP

在无线局域网中提供无线域服务 (WDS) 的接入点保持无线局域网中具有 CCKM 功能的客户端设备的凭证缓存。当具有 CCKM 功能的客户端从一个接入点漫游到另一个接入点时， WDS 将客户端凭证转发到新的接入点。在客户端和新的接入点之间仅传送两个数据包，大大缩短了重关联时间。

图 42 - 无线 AP 服务概览

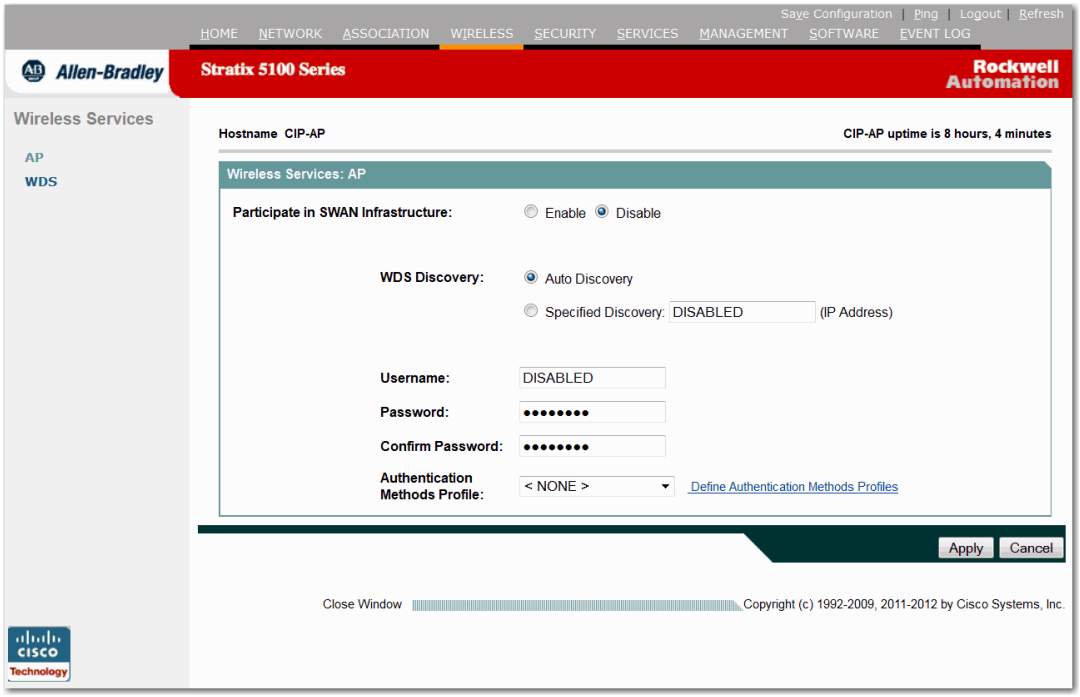
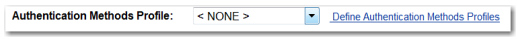


表 25 - Wireless AP (无线 AP) 页面参数描述

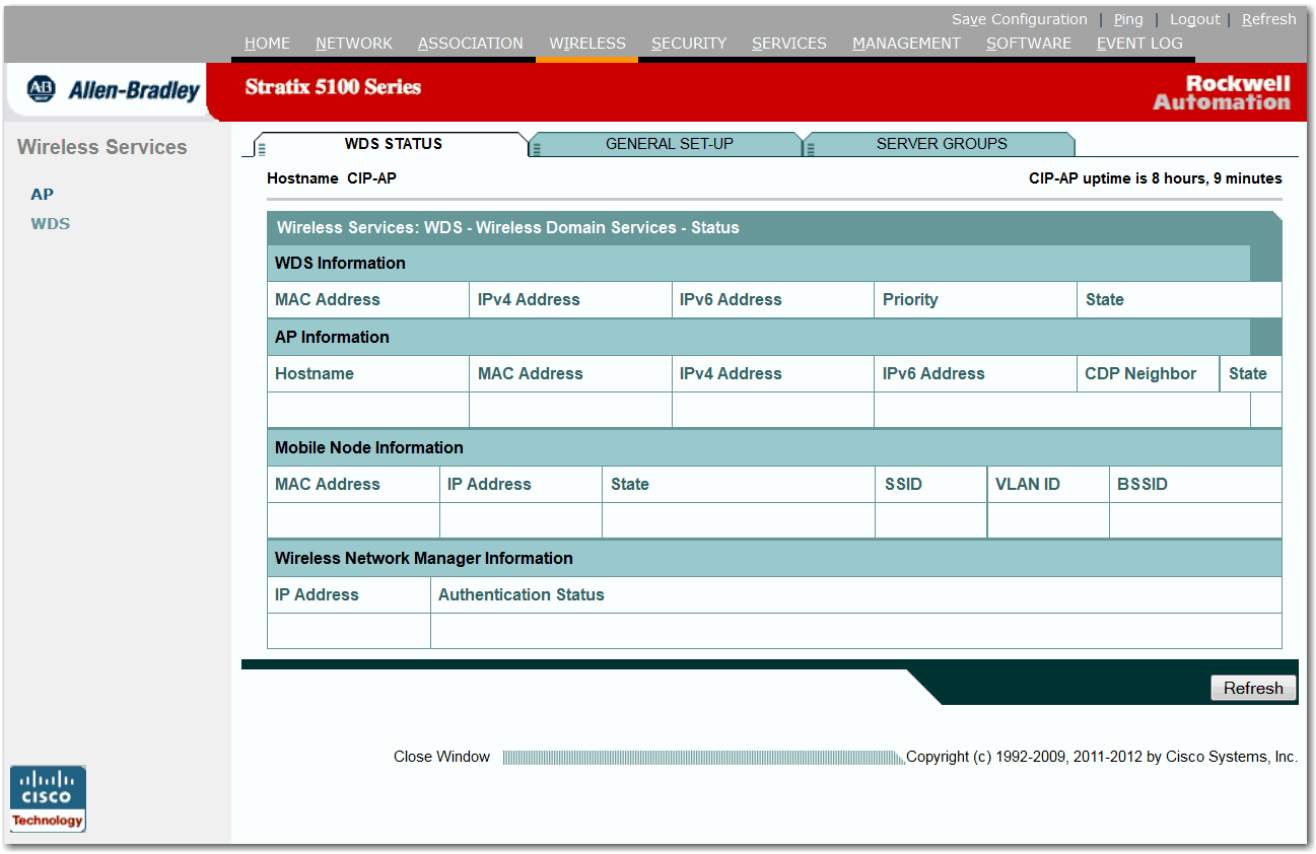
参数	描述
Participate in SWAN Infrastructure	启用 禁用
WDS Discovery	自动发现 指定发现 (IP 地址)
Username	参与者用户名
Password	参与者密码
验证方法配置文件	 Define Authentication Methods Profile (定义验证方法配置文件) 链接将跳转到 Security > AP Authentication (安全 > AP 验证)。更多信息，请参见第 110 页的 “Security (安全) 页面 ”。

WDS

当在网络上配置无线域服务时，无线局域网上的接入点使用启用 WDS 功能的接入点，为客户端设备提供快速、安全的漫游以及参与无线电管理。使用以下参数确定接口是否用作无线域服务 (WDS)。

有关详细的配置信息，请参见第 353 页的 “ 配置 WDS 和快速 安全漫游 ”。

图 43 - WDS (无线域服务) Status (WDS 状态) 页面



该页面提供了已设置的无线域服务的状态总览。

表 26 - 无线 WSD/WNM 常规设置页面参数描述

参数	描述
WDS Information	
MAC Address	介质访问控制 (MAC) 地址是制造商分配给网络接口的唯一标识符。
IP Address	尝试注册此无线域的接入点的 IP 地址。
Priority	显示此 WDS 候选者的一个优先级编号，范围为 1…255。具有最高优先级编号的候选 WDS 成为活动 WDS。
State	显示接入点状态 (注册与否)。

表 26 - 无线 WSD/WNM 常规设置页面参数描述 (续)

参数	描述
AP Information	
MAC Address	介质访问控制 (MAC) 地址是制造商分配给网络接口的唯一标识符。
IP Address	客户端 / 中继器的 IP 地址。
CDP Neighbor	CDP 邻居的 IP 地址，通过此地址直接连接接入点的以太网端口。
State	显示客户端 / 中继器的状态 (注册与否)。
Mobile Node Information	
MAC Address	介质访问控制 (MAC) 地址是制造商分配给网络接口的唯一标识符。
IP Address	客户端 / 中继器的 IP 地址。
State	显示客户端 / 中继器的状态 (注册与否)。
SSID	指定关联至 VLAN 的 SSID。
VLAN ID	指定与 SSID 绑定的虚拟以太网局域网识别号。除了数字 ID 之外，您还可为 VLAN 分配一个名称。
BSSID	指定基本服务器组标识符的 MAC 地址。基本服务器组是一组相互通信的工作站。
Wireless Network Manager Information	
IP Address	包含为所浏览的接入点配置使用的无线域服务的 IP 地址。
Authentication Status	用于验证无线局域网上的基础设施设备 (例如，接入点) 的服务器。

图 44 - WDS and WNM General Set-up (WDS 和 WNM 常规设置) 页面

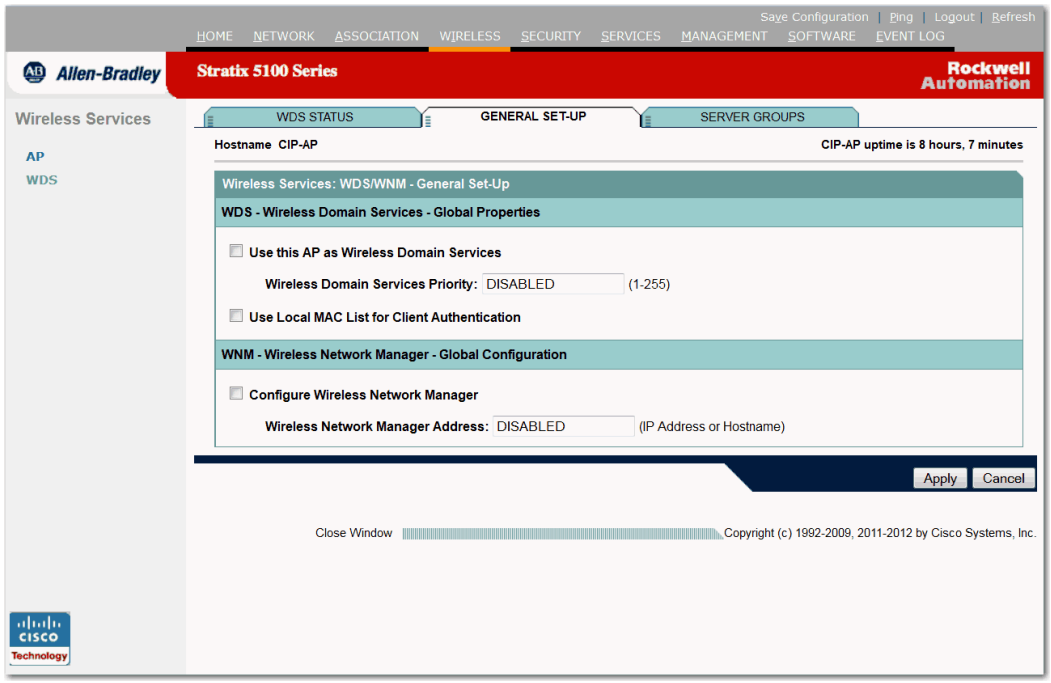
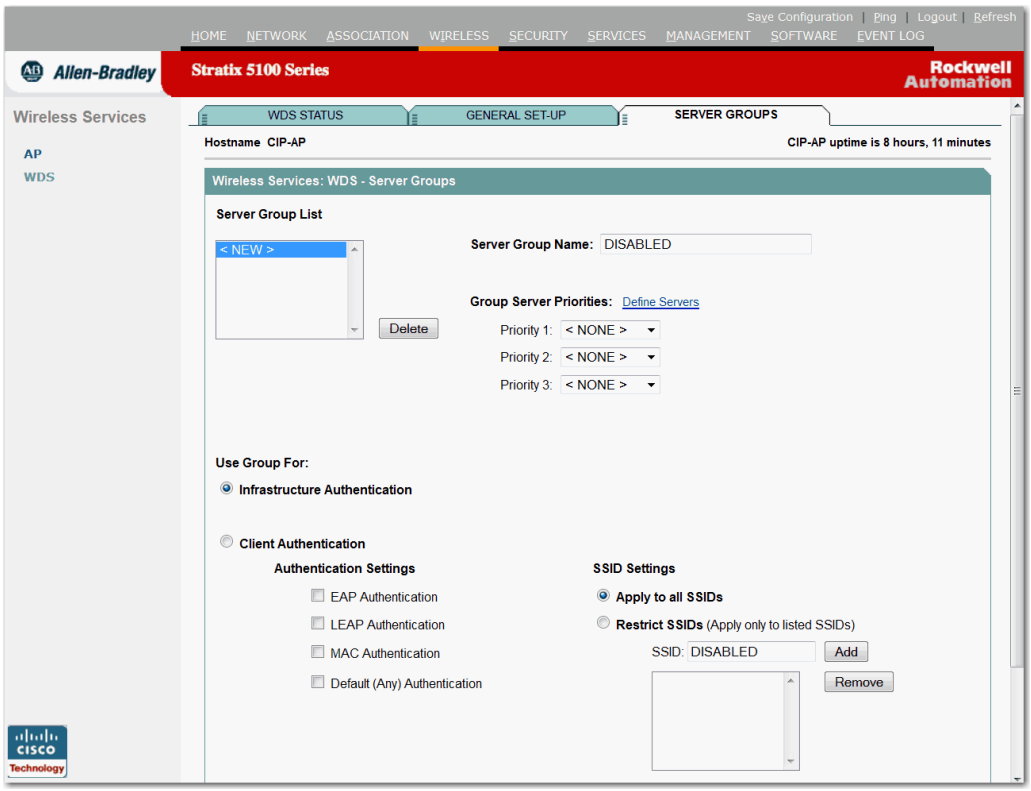


表 27 - Wireless WSD/WNM General Setup (无线 WSD/WNM 常规设置) 页面参数描述

参数	描述
WDS - Wireless Domain Services - Global Properties	
Use this AP as Wireless Domain Services	如果要使用 AP 作为无线域服务，则选中该复选框。 如果想要该接入点成为 WDS，以便使用支持 CCKM 的客户端快速安全漫游，或想要该接入点将统计信息转发到 WNM 供 WLSE 收集，则选中该复选框。 如果想要将接入点用作 WDS 或候选 WDS，则应使用该页面将接入点配置为 WDS。对于您的 WDS，应选择此类接入点： • 具备良好的物理安全保护，可防止被盗。 • 服务较少的客户端设备，因为接入点的 WDS 负载会降低关联客户端设备的性能。
Wireless Domain Services Priority	设置 WDS 优先级：该候选 WDS 的 1...255。 编号最高的候选 WDS 接入点将成为代理 WDS 接入点。如果将接入点配置为备用 WDS，则为想要用作主 WDS 的接入点分配最高优先级，为备用 WDS 分配较低的优先级。 如果主 WDS 发生故障，则有最高优先级的备用 WDS 将成为活动 WDS。
Use Local MAC List for Client Authentication	要使用 WDS 设备上配置的本地列表中的 MAC 地址验证客户端设备，选中该复选框。 如果未选中该复选框，则 WDS 设备将使用 Server Groups (服务器组) 页面中指定的 MAC 地址验证服务器，根据 MAC 地址来验证客户端。 选择 Use Local MAC List for Client Authentication (使用本地 MAC 列表进行客户端验证) 复选框不会强制客户端设备执行基于 MAC 的验证。它为基于服务器的 MAC 地址验证提供了一个本地备选方案。

图 45 - WDS Server Groups (WDS 服务器组) 页面



该页面允许您设置可由 WDS 无线接入点使用的验证服务器。如果希望将接入点用作 WDS 或候选 WDS，您需要按如下进行配置。

在此处设置服务器组之前，必须至少在一个服务器上的 Security (安全) > Server Manager (服务器管理器) 选项卡上进行配置。

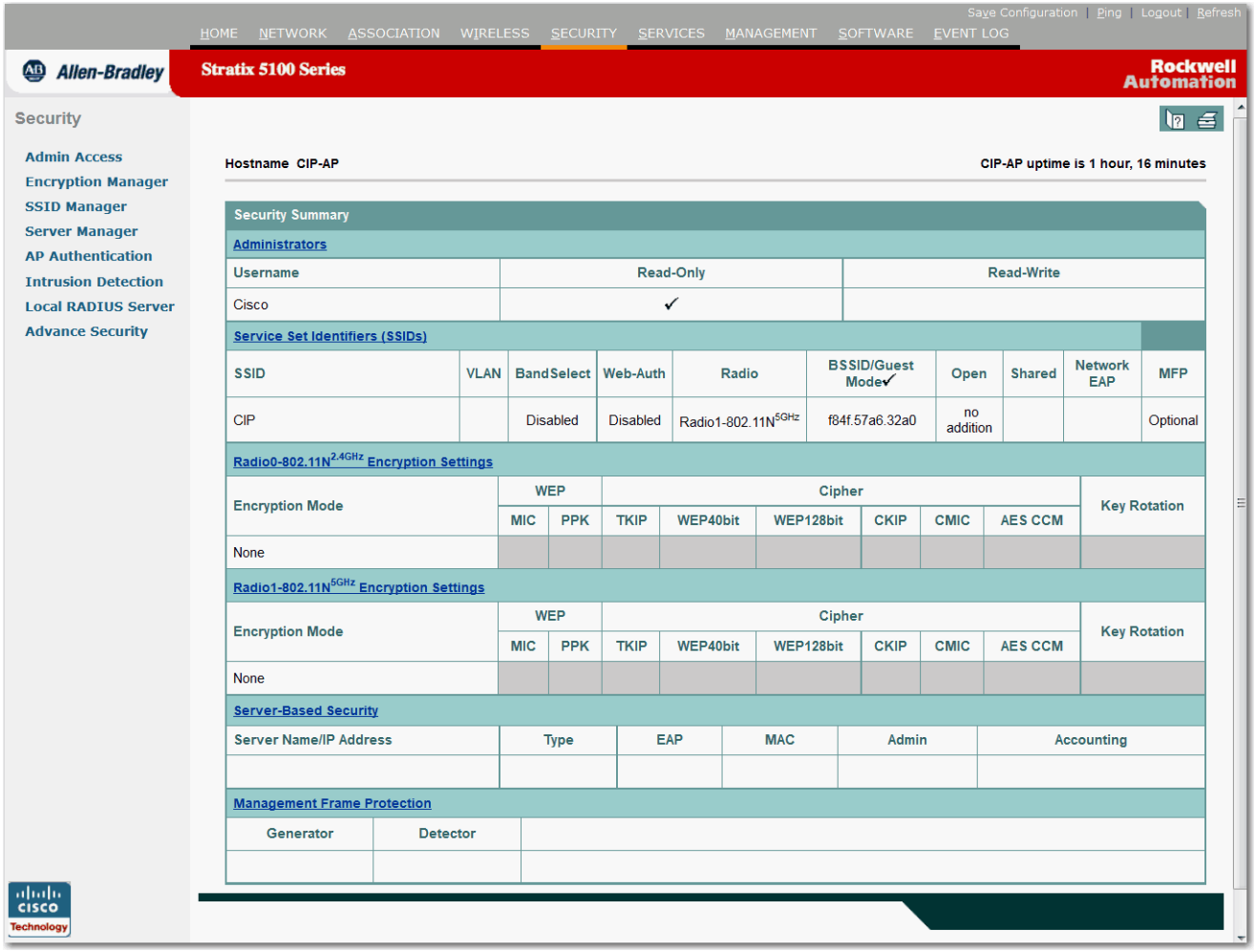
表 28 - 无线服务器组参数描述

参数	描述
Server Group List	单击选择要编辑的服务器。
Server Group Name	输入唯一的组名。
Group Sever Priorities	设置用于架构和客户端验证的服务器的优先级。
Define Servers	单击 Define Servers (定义服务器) 跳转到 Security>Server Manager (安全 > 服务器管理) 页面，您可在此配置服务器。
Infrastructure Authentication/ Client Authentication	选择用于验证服务器组的设备。在基础架构设备中选择，例如，接入点、使用 EAP 验证的客户端、使用 LEAP 验证的客户端、使用基于 MAC 验证的客户端或使用任何验证类型的客户端。如果将 Any Authentication (任何验证) 设置为默认组，则当没有其他适用的客户端验证组 (EAP、 LEAP 或 MAC) 时，将应用该设置。
SSID Settings	默认情况下，服务器组应用到所有 SSID。 要针对特定的 SSID 列表定义该设置，单击 Restrict SSIDs (限制 SSID)。 单击 Add (添加) 添加所需的 SSID。

Security (安全) 页面

使用 Security (安全) 页面配置安全设置，以防止对网络的未授权访问。由于 WAP 属于无线电设备，它可在工作现场的物理边界外通信。Security Summary (安全概要) 页面提供了安全设置及到其他安全页面的链接的快照。

图 46 - Security Summary (安全概要) 页面



Security Summary (严重性概要) 页面中的链接	描述
Administrators	关于到 Admin Access (管理访问) 的链接，请参见 第 112 页的 “Admin Access (管理员访问) 页面 ”。
Service Set Identifiers (SSIDs)	关于到 SSID Manager (SSID 管理器) 的链接，请参见 第 115 页的 “SSID Manager (SSID 管理器) 页面 ”。
Radio0-802.11N2.4 GHz Encryption Settings	关于到 Encryption Manager (加密管理器) 的链接，请参见 第 113 页的 “Encryption Manager (加密管理器) 页面 ”。
Radio1-802.11N 5 GHz Encryption Settings	关于到 Encryption Manager (加密管理器) 的链接，请参见 第 113 页的 “Encryption Manager (加密管理器) 页面 ”。
Server-Based Security	关于到 Server Manager (服务器管理器) 的链接，请参见 第 118 页的 “Server Manager (服务器管理器) 页面 ”。
Management Frame Protection	到 Intrusion Detection (入侵检测) 的链接，请参见 第 126 页的 “ 入侵检测 ”。

表 29 - 安全概要参数描述

参数	描述
Username	活动用户的用户名。
Read-Only	指定用户是否只具有只读权限。
Read-Write	指定用户是否具有读 / 写权限。
SSID	指定客户端设备用于与接入点关联的唯一标识符。
VLAN	指定当前分配的 VLAN。
SSID	唯一标识符
Band Select	启用时，将允许双频带客户端无线电装置切换到不拥挤的 5 GHz 频带。
Web-Auth	指定是否为客户端启用 Web 验证。
Radio	指定使用哪种无线电。
BSSID/Guest Mode	指定附加于该 SSID 的 BSSID/ 访客模式。
Open/Shared/Network EAP	指定要使用的验证方法。 • 开放式验证允许任何设备进行验证和尝试与接入点通信。 • 共享验证将向任何试图与接入点通信的设备发送未加密的质询字符串。 • 网络 EAP 使用 EAP 与网络上兼容 EAP 的服务器交互，为无线客户端设备提供验证。
Management Frame Protection (MFP)	可对管理帧进行保护，检测发起拒绝服务攻击的攻击者。此类攻击包括：让网络充斥关联和探测、插入伪接入点以及通过攻击 QoS 和无线电测量帧影响网络性能。该链接可跳转到 Intrusion Detection (入侵检测) 页面。

Admin Access (管理员访问) 页面

Admin Access (管理员访问) 页面为管理员提供关于安全、验证和用户列表的信息。

图 47 - 安全管理员访问

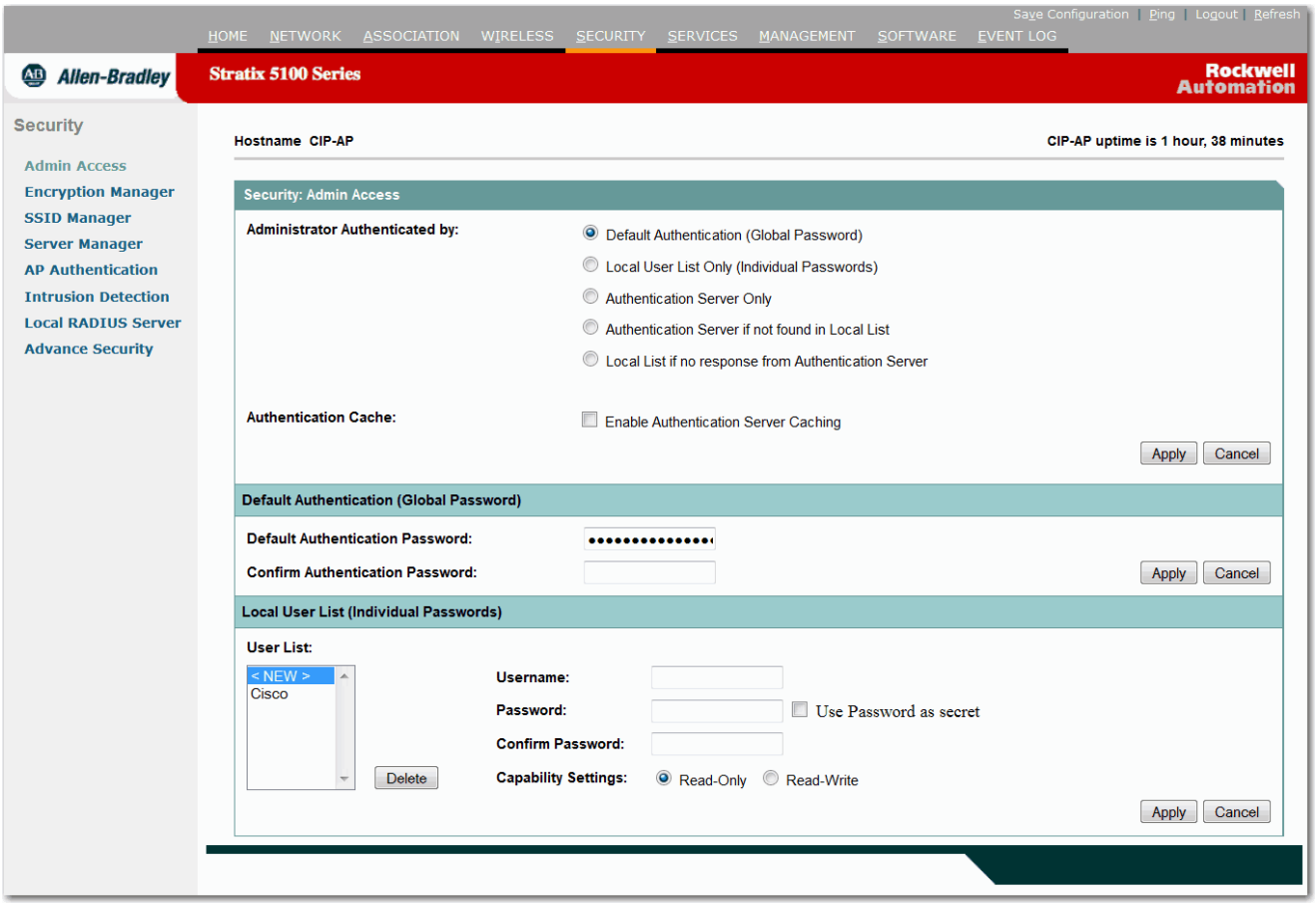


表 30 - 安全管理访问参数描述

参数	描述
Administrator Authenticated by	• 默认验证 (全局密码) • 仅本地用户列表 (单独密码) • 仅验证服务器 • 如果未在本地列表中找到，使用验证服务器 • 如果验证服务器没有响应，使用本地列表
Authentication Cache	启用验证服务器缓存
Default Authentication	默认验证密码 (全局密码) 指定进入特权 exec (管理员) 模式的密码。
Local User List	• 用户名 • 密码 • 使用密码作为保密密码：以便进入特权 exec (管理员) 模式。 • 功能设置：只读 / 读写

Encryption Manager (加密管理器) 页面

该页面允许您选择加密和解密无线电信号的加密模式和参数。

图 48 - 加密管理器参数说明

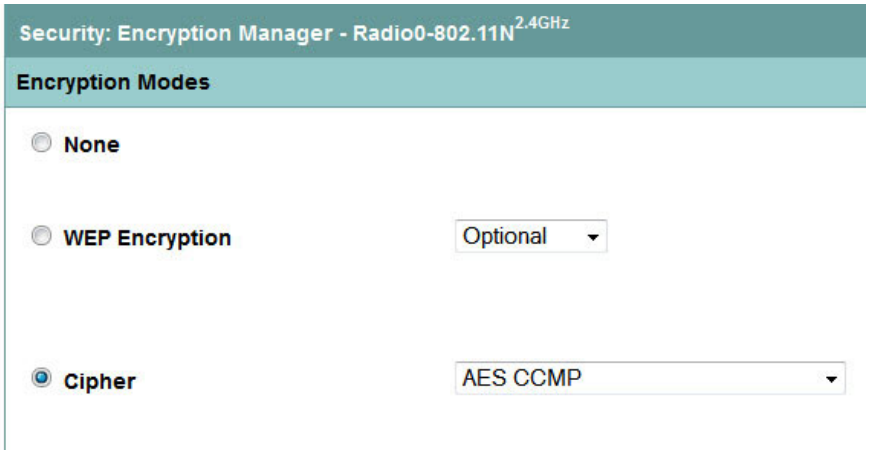


图 49 - 安全加密管理器

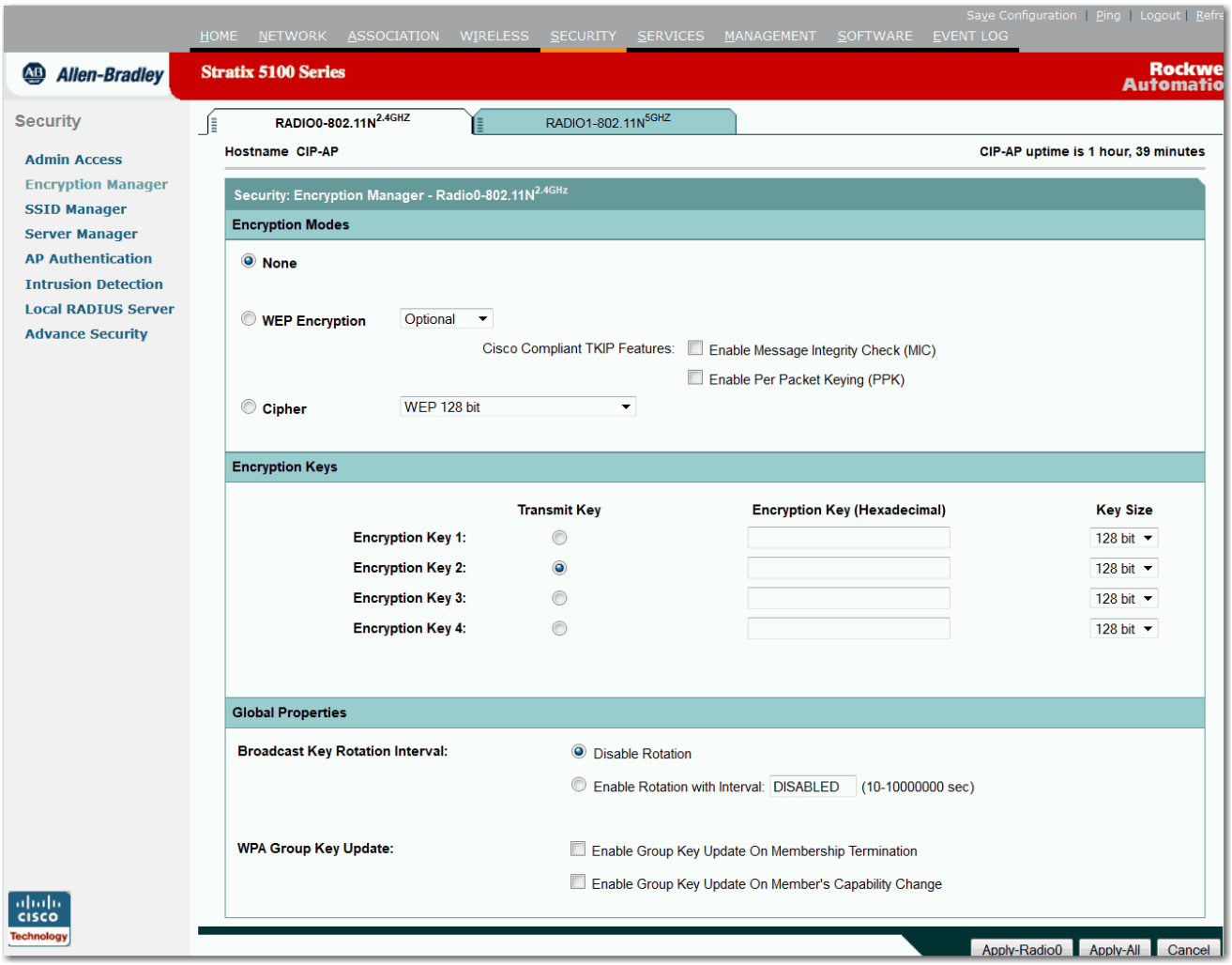


表 31 - 安全加密管理器参数描述

参数	描述
Encryption Modes	指示客户端与网桥通信时是否使用数据加密。
None	不在无线电接口上启用加密。
WEP Encryption	选择 Optional (可选) 或 Mandatory (强制)。如果是可选，则客户端设备在有 WEP 或无 WEP 时，都可与该接入点或网桥通信。如果是强制，客户端设备与接入点通信时必须使用 WEP。未使用 WEP 的网桥不允许通信。 WEP 是一种 802.11 标准加密算法，最初用于无线 LAN。但基本 WEP 构造存在缺陷，攻击者耗费一定精力仍可窃取隐私。 **不建议使用** WEP 作为 WLAN 安全方法。要正确运行，需要将思科 802.11n 无线电装置配置为不加密或 AES-CCMP 加密。
Cipher	密文组是一组加密和完整性算法，用于保护无线局域网上的无线电通讯。您必须使用密码组来启用 Wi-Fi 保护访问 (WPA) 或思科集中密钥管理 (CCKM)。使用下拉菜单在 AES、 TKIP、 CKIP、 CMIC 和 WEP 间选择。AES CCMP 安全性最高，建议使用该方式。 AES-CCMP 是一种对称分组密文，可使用 128、 192 和 256 位密钥加密和解密数据。 AES-CCMP 优于 WEP 加密，在 IEEE 802.11i 标准中定义。 WEP 密码组安全性最差，不建议使用。
Transmit Key	该参数仅用于 WEP，且**不建议使用**。单击 Transmit Key (发送密钥)，选择该网桥要使用的 WEP 密钥。每次只能选择一个密钥。设置的所有密钥都可用于接收数据。 在关联到接入点或网桥的客户端设备上，也必须在相同密钥槽中输入选为密钥的发送密钥，但不必在客户端设备上将其选为发送密钥。
Encryption Key 1-4	在其中一个 Encryption Key (加密密钥) 域中输入 WEP 密钥。对于 40 位加密，输入 10 个十六进制数字；对于 128 位加密，输入 26 个十六进制数字。十六进制数字是以数字 0-9、小写字母 a-f 以及大写字母 A-F 构成的一组字符。 WEP 密钥可包含这些字符的任意组合。 WEP 密钥不区分大小写。 最多可输入四组 WEP 密钥。在关联到接入点或网桥的客户端设备上，也必须在相同密钥槽中输入选为密钥的发送密钥，但不必在客户端设备上将其选为发送密钥。 如果配置了四组 WEP 密钥，并选择 WEP 密钥 2 作为发送密钥，则客户端设备上的 WEP 密钥 2 必须包含相同内容。如果客户端设备上设置了 WEP 密钥 4，但未选择作为发送密钥，则无需在接入点上设置 WEP 密钥 4。
Key Size	为每个密钥选择 40 位或 128 位加密。
Global Properties	广播密钥旋转间隔：禁用旋转或以一定间隔启用旋转 (10…10000000 s)
Broadcast Key Rotation Interval	让接入点生成尽可能随机的组密钥，并定期更新所有具有密钥管理功能的工作站。广播密钥旋转不适用于静态 WEP 客户端。该功能使得组密钥仅对当前活动的成员保持私密。但如果网络频繁漫游，则可能会产生一些系统开销。
WPA Group Key Update	选中相应复选框，以确定接入点更改组密钥并将其分配给启用 WPA 的客户端设备的频率。 • 在成员资格结束时启用组密钥更新 • 在成员功能更改时启用组密钥更新

SSID Manager (SSID 管理器) 页面

使用 SSID Manager (SSID 管理器) 页面将 SSID 分配给特定的无线电接口。

图 50 - SSID 管理器

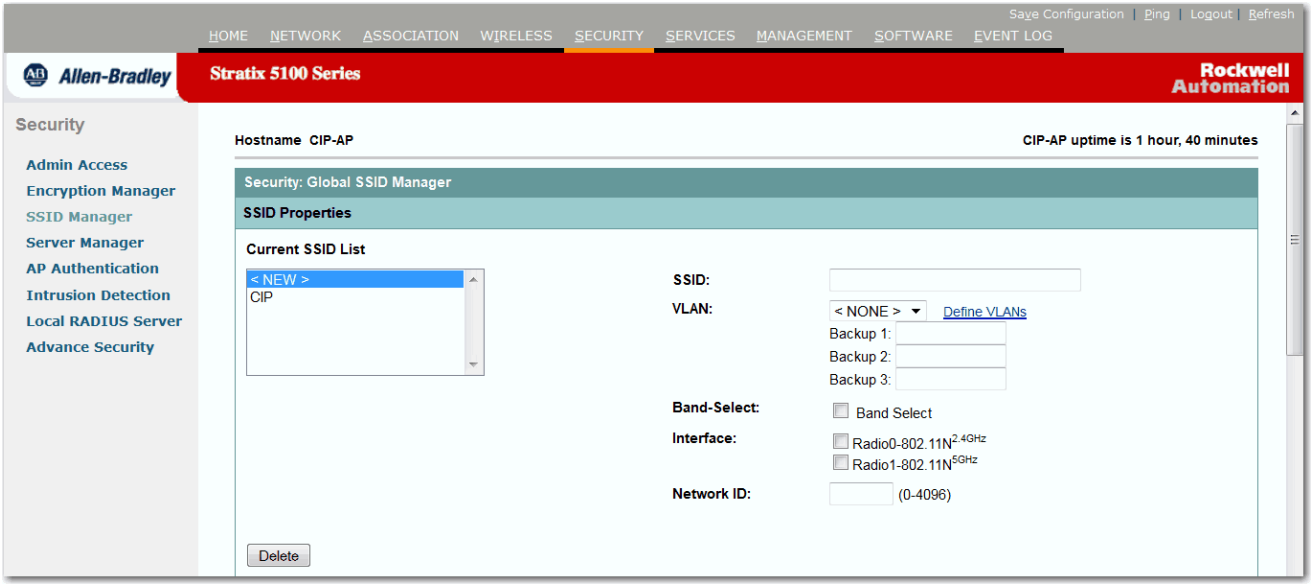


表 32 - SSID 管理器参数描述

参数	描述
Current SSID List	输入客户端设备用于与接入点关联的唯一标识符。 SSID 帮助客户端设备用于识别临近的多个无线网络。 SSID 可以是任意字母数字，可输入 2...32 个字符，且区分大小写。
SSID	服务集标识符 (SSID) - 也称为无线电 SSID - 是客户端用于关联无线网络的唯一标识符。最多可添加 16 个 SSID。 不允许使用下列六个字符：+、]、 /、 "、 TAB 和末尾空格。此外，下列三个字符不得作为第一个字符：!、 # 和 ;。 SSID 参数区分大小写。
VLAN	使您能够将 SSID 关联到已配置的 VLAN。 VLAN 是一种按功能、项目团队或应用进行逻辑分段的交换网络，而不是根据物理或地理位置来分段。例如，特定工作组团队使用的所有工作站和服务器都可连接到相同的 VLAN，不管它们以何种物理连接方式连接到网络，或者它们是否可与其他团队组合。
Define VLANs	将可跳转到 Services > VLAN (服务 > VLAN) 页面。如果在单击该链接之前未应用配置更改，则更改将丢失。在该页面中，您可设置默认 VLAN，并分配当前 VLAN 及其 ID 和信息。例如，企业用户可使用不同的 VLAN 来隔离员工通信与访客通信，并将这些通信组进一步与高层人员相隔离。可将来往于不同安全等级的无线客户端分割到具有不同安全策略的 VLAN 中。
Band-select	频带选择可将无线客户端 (具有双频带功能， 2.4 和 5 GHz) 切换到不那么拥挤的 5 GHz 无线电频带上工作。
Interface	选择要启用的无线电接口。该 SSID 保持为不活动，直到为某个无线电接口启用它。
Network ID	网络 ID

表 32 - SSID 管理器参数描述 (续)

参数	描述
Client Authentication Settings and Methods Accepted	**开放式验证** 选中该复选框选择开放式验证。 开放式验证允许任何设备进行验证和尝试与接入点通信。 要进行安全验证，必须使用附加方法，例如， EAP 或 WPA/WPA2 预共享密钥。 在选择开放式验证后，您可从下列列表中选择要使用的附加方法。下拉菜单中的选项有： • MAC 验证 • EAP • MAC 验证与 EAP • MAC 验证或 EAP，或使用可选的 EAP 要启用 EAP，必须在该页面或 Server Manager (服务器管理器) 页面中设置 EAP 验证服务器。要启用 MAC 验证，必须本地输入 MAC 地址，或在 Advanced Security (高级安全) 页面中选择 Authentication Server Only (仅验证服务器) 选项。选择 Optional EAP (可选 EAP)，则可关联客户端和可选 EAP 客户端，并通过两种验证方法中的任一种进行验证。 虽然接入点可使用开放式验证 + EAP 方法来验证无线客户端设备，接入点无法使用 EAP 来验证另一个接入点。也就是说，接入点必须使用开放式验证、共享验证或网络 EAP 验证方法来相互验证。 **共享验证** 选中 Shared Authentication (共享验证) 复选框选择共享验证。由于存在安全缺陷，不建议使用共享密钥验证。而应使用开放式验证 + EAP 或 WPA/WPA2 预共享密钥。 接入点将向任何试图与接入点通信的设备发送未加密的质询字符串。请求验证的设备加密质询文本，并将其发回接入点。如果质询文本加密正确，接入点允许请求设备进行验证。 但是，未加密的质询和加密的质询均可被监控，因此，入侵者可通过比较未加密的和加密的文本串来猜测 WEP 密钥，致使接入点易受到攻击。由于存在这一缺陷，共享密钥验证的安全性不如开放式验证。仅一个 SSID 可使用共享验证。在选择共享验证后，您可从下列列表中选择要使用的方法。选项有 MAC Authentication (MAC 验证)、 EAP 或 MAC Authentication and EAP (MAC 验证和 EAP)。 **网络 EAP** 选中 Network EAP (网络 EAP) 复选框选择网络 EAP。设备使用可扩展验证协议 (EAP) 与网络上兼容 EAP 的服务器交互，为无线客户端设备提供验证。客户端设备使用动态 WEP 密钥与网络进行验证。在选择 Network EAP (网络 EAP) 后，您可选择 MAC Authentication (MAC 验证)。 要与支持 LEAP 验证方法的思科客户端设备配合工作，必须使用 Network EAP (网络 EAP)。通常使用开放式验证 + EAP，而不使用更安全的方法。
Server Priorities	确定将如何在该 SSID 上使用特定 RADIUS 服务器。在 EAP and MAC Authentication Server (EAP 和 MAC 验证服务器) 区域中，您可选择默认设置，或者通过下拉菜单自定义优先级。如果单击启用了使用默认设置，单击 Define Defaults (定义默认设置) 链接将跳转到 Server Manager (服务器管理器) 页面。
Authenticated Key Management	WPA 和 CCKM 是验证密钥管理解决方案。 Wi-Fi 保护访问 (WPA) 依赖于 IEEE 802.11i 标准的版本。 WPA 支持 TKIP 和 WEP 加密算法，与现有验证系统简单集成时，可使用 802.1X 和 EAP。 WPA 密钥管理使用加密方法组合来保护客户端设备和接入点之间的通信。 WPA 密钥管理当前支持两种互斥的验证密钥管理类型：WPA 和 WPA-PSK。如果验证密钥管理为 WPA，则客户端和验证服务器将使用 EAP 验证方法 (例如， EAP-TLS) 并生成成对主密钥 (PMK) 进行相互验证。如果验证密钥管理方式为 WPA-PSK，则将直接使用预共享密钥作为 PMK。 使用思科集中密钥管理 (CCKM)，已验证客户端设备可从一个接入点漫游到另一个接入点，重新关联期间不会有任何可以察觉到的延迟。网络中的接入点可提供无线域服务 (WDS)，并为子网中启用 CCKM 的客户端设备创建安全凭证缓存。 当启用 CCKM 的客户端设备漫游到新的接入点时，凭证的 WDS 缓存可显著缩短重新关联所需的时间。要为 SSID 启用 CCKM，还必须启用网络 EAP 验证。当为 SSID 启用 CCKM 和 Network EAP (网络 EAP) 后，使用 LEAP、 EAP-FAST、 PEAP/GTC、 MSPEAP 和 EAP-TLS 的客户端设备可使用 SSID 进行验证。要为 SSID 启用 WPA，必须还启用开放式验证或网络 -EAP 或者两者都启用。启用 CCKM 或 WPA 前，必须先使用密文组选项中的一种设置 SSID 的 VLAN 的加密方式。
Key Management	使用下拉菜单选择执行密钥管理属于强制还是可选操作。您可为无线电 802.11b 或 802.11g 同时选择 CCKM 和 WPA 验证密钥管理。对于无线电 802.11a，只能选择一种密钥管理。
WPA Pre-shared Key	要支持使用 WPA 密钥管理的客户端设备，必须在接入点上配置预共享密钥。输入密钥并指定输入十六进制还是 ASCII 字符。 如果使用十六进制，则必须输入 64 个十六进制字符，以完成 256 位密钥。如果使用 ASCII，则必须至少输入 8 个字母、数字或符号，接入点将为您扩展密钥。您最多可输入 63 个 ASCII 字符。
IDS Client MFP	在该 SSID 上启用客户端 MFP，以保护客户端和 AP 之间的无线管理通信。
AP Authentication	凭证用于将接入点与网络进行验证。它与客户端验证不同。

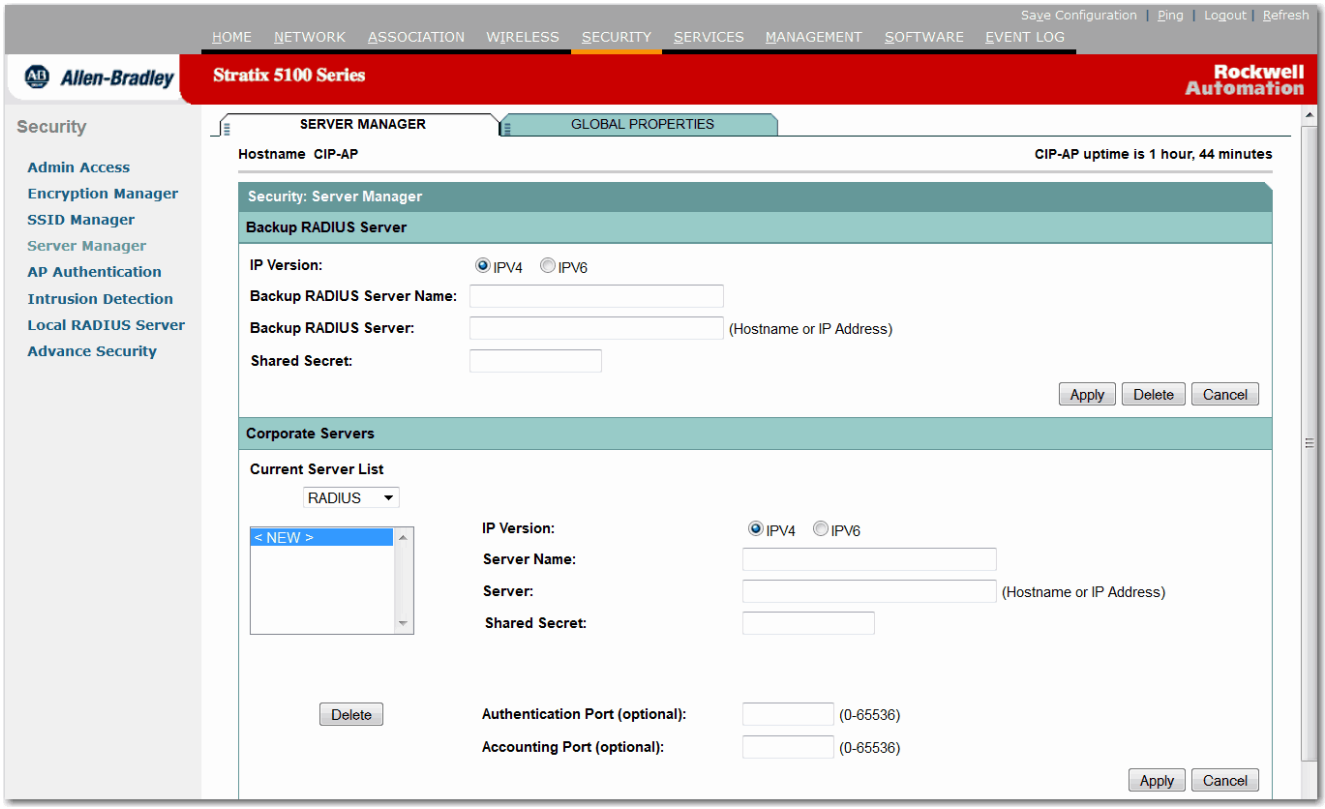
表 32 - SSID 管理器参数描述 (续)

参数	描述
凭证	使用下拉菜单指定 SSID 的凭证配置文件。 定义凭证 如果需要定义凭证，单击链接跳转到 AP Authentication - General Setup (AP 验证 — 常规设置) 页面，您可在此创建用户名和密码，或匿名 ID 和凭证的信任点。
Authentication Methods Profile	当接入点连接到网络时，接入点和网络验证设备进行协商，就两种设备共同支持的验证方法达成一致，以完成验证。验证方法配置文件用于限制接入点同意使用的验证类型。使用下拉菜单指定 SSID 的证书配置文件。
Define Authentication Methods Profile	如果需要定义验证方法配置文件，单击该链接跳转到 AP Authentication - General Setup (AP 验证 — 常规设置) 页面。
Accounting Settings Enable Accounting	指示是否要让该服务器记录客户端与接入点关联的使用数据。一些使用数据可用于记帐或使用追踪。
Accounting Server Priorities	您可使用下拉菜单选择使用默认设置或自定义优先级。如果选择启用了使用默认设置，单击 Define Defaults (定义默认设置) 链接将跳转到 Server Manager (服务器管理器) 画面。
General Settings Advertise Extended Capabilities of this SSID	包括无线配置服务 (WPS) 信息元素中的 SSID 名称和功能。
Advertise Wireless Provisioning Services (WPS) Support	在 WPS 信息元素中启用 WPS 功能标记。
Advertise this SSID as a Secondary Broadcast SSID	在 WPS 信息元素中包含 SSID 名称和功能。
Enable IP Redirection on this SSID	在配置 SSID 的 IP 重定向时，接入点将关联到该 SSID 的客户端设备发送过来的所有数据包重定向到特定的 IP 地址。您可重定向使用该 SSID 关联的客户端设备的所有数据包，或者仅重定向原先定向到特定 TCP 或 UDP 端口的数据包。当将接入点配置为仅重定向指向特定端口的数据包时，接入点重定向使用该 SSID 的客户端的数据包，丢弃使用该 SSID 的客户端的所有其他数据包。
IP Address	输入用于重定向数据包的目标 IP 地址。
IP Filter	在启用 IP 重定向并输入 IP 地址后，单击 Define Filter (定义过滤器) 跳转到 IP Filters (IP 过滤器) 页面，您可在此指定用于重定向的适当 TCP 或 UDP 端口。如果未指定 TCP 或 UDP 端口，接入点将重定向从客户端设备接收到的所有数据包。
Association Limit (optional)	特定 SSID 最多可关联的客户端数量。该限值可防止接入点过载，有助于为关联的客户端提供适当的服务水平。
EAP Client (optional)	思科建议使用 AP 验证，不要使用 EAP 客户端来将接入点验证到网络。
Username	指示当中继器接入点与父级接入点关联时或当热备用接入点与受监控的接入点关联时，网络 EAP 验证使用的用户名。
Password	指示当中继器接入点与父级接入点关联时或当热备用接入点与受监控的接入点关联时，网络 EAP 验证使用的密码。注意：不允许使用下列字符：TAB、 ?、 $、 + 和 [。
Multiple BSSID Beacon Settings Multiple BSSID Beacon	如果要将 SSID 包括在信标中，选择 Set SSID as Guest Mode (设置 SSID 作为访客模式) 复选框。要延长使用该 SSID 的节能客户端的电池续航时间，选择 Set Data Beacon Rate (DTIM) (设置数据信标速率 (DTIM)) 复选框，输入 SSID 的信标速率。信标速率决定了接入点发送包含交付通信指示器消息 (DTIM) 的信标的频率。当客户端设备接收到包含 DTIM 的信标时，它们通常会被唤醒，检查未决的数据包。 DTIM 之间的间隔越长，客户端睡眠时间越长，从而更节能。相反地， DTIM 周期越短，接收数据包的延时越短，但客户端会被频繁唤醒，使用更多的电池电源。 更多步骤信息，请参见第 289 页的 " 配置 多个 SSID"。
Guest Mode/Infrastructure SSID Settings Set Beacon Mode	单击选择单条或多条接入点信标消息。从下拉菜单中，指示启用了客户端，但没有任何 SSID 关联到该访问点的访客模式。 详细步骤信息，请参见第 289 页的 " 配置 多个 SSID"。
Set Infrastructure SSID	当接入点处于中继模式时，将使用该 SSID 关联父级接入点。如果要强制基础架构设备只与该 SSID 关联，则通过下拉菜单选中复选框。

Server Manager (服务器管理器) 页面

在 Server Manager (服务器管理器) 页面中可以输入验证服务器的设置。网络上的 RADIUS/TACACS+ 服务器使用 EAP 来提供无线客户端设备的验证服务。

图 51 - 服务器管理器



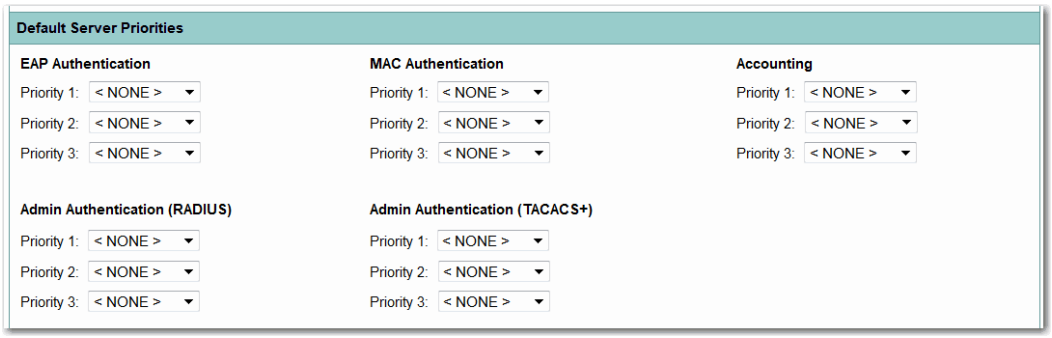


表 33 - 安全：服务器管理器参数描述

参数	描述
Backup RADIUS Server	输入作为本地 RADIUS 服务器的接入点的主机名称或 IP 地址。当主 RADIUS 服务器未响应时，无线局域网上的其他接入点使用该备用验证器。
Shared Secret	输入本地 / 备用 RADIUS 服务器使用的共享密钥。设备上的共享密钥必须与本地 / 备用服务器上的共享密钥相匹配。
Corporate Servers Current Server List	标识当前可用的服务器。
Server	输入服务器的名称或 IP 地址。
Shared Secret	输入 RADIUS/TACACS+ 服务器使用的共享密钥。设备上的共享密钥必须与 RADIUS/TACACS+ 服务器上的共享密钥相匹配。
Authentication Port (optional)	输入 RADIUS/TACACS+ 服务器用于验证的端口号。思科 RADIUS 服务器 (访问控制服务器 [ACS]) 的端口设置为 1645，许多 RADIUS 服务器的端口设置为 1812。查看您的服务器的产品文档，查找正确的端口设置。
Accounting Port (optional)	输入 RADIUS 服务器用于结算的端口号。思科 RADIUS 服务器 (访问控制服务器 [ACS]) 的端口设置为 1646，许多 RADIUS 服务器的端口设置为 1813。查看您的服务器的产品文档，查找正确的结算端口设置。
Default Server Priorities EAP Authentication	按所需的优先级顺序选择用于 EAP 验证的服务器。
MAC Authentication	以所需的优先级顺序选择用于 MAC 验证的服务器。
Accounting	以所需的优先级顺序选择用于结算的服务器。
Admin Authentication (RADIUS)	以所需的优先级顺序选择用于 RADIUS 管理验证的服务器。
Admin Authentication (TACACS+)	以所需的优先级顺序选择用于 TACACS 管理验证的服务器。

服务器管理器全局属性

Server Manager Global Properties (服务器管理全局属性) 页面提供关于您正在使用的服务器及这些服务器的全局位置的详细信息。

图 52 - 服务器管理器全局属性

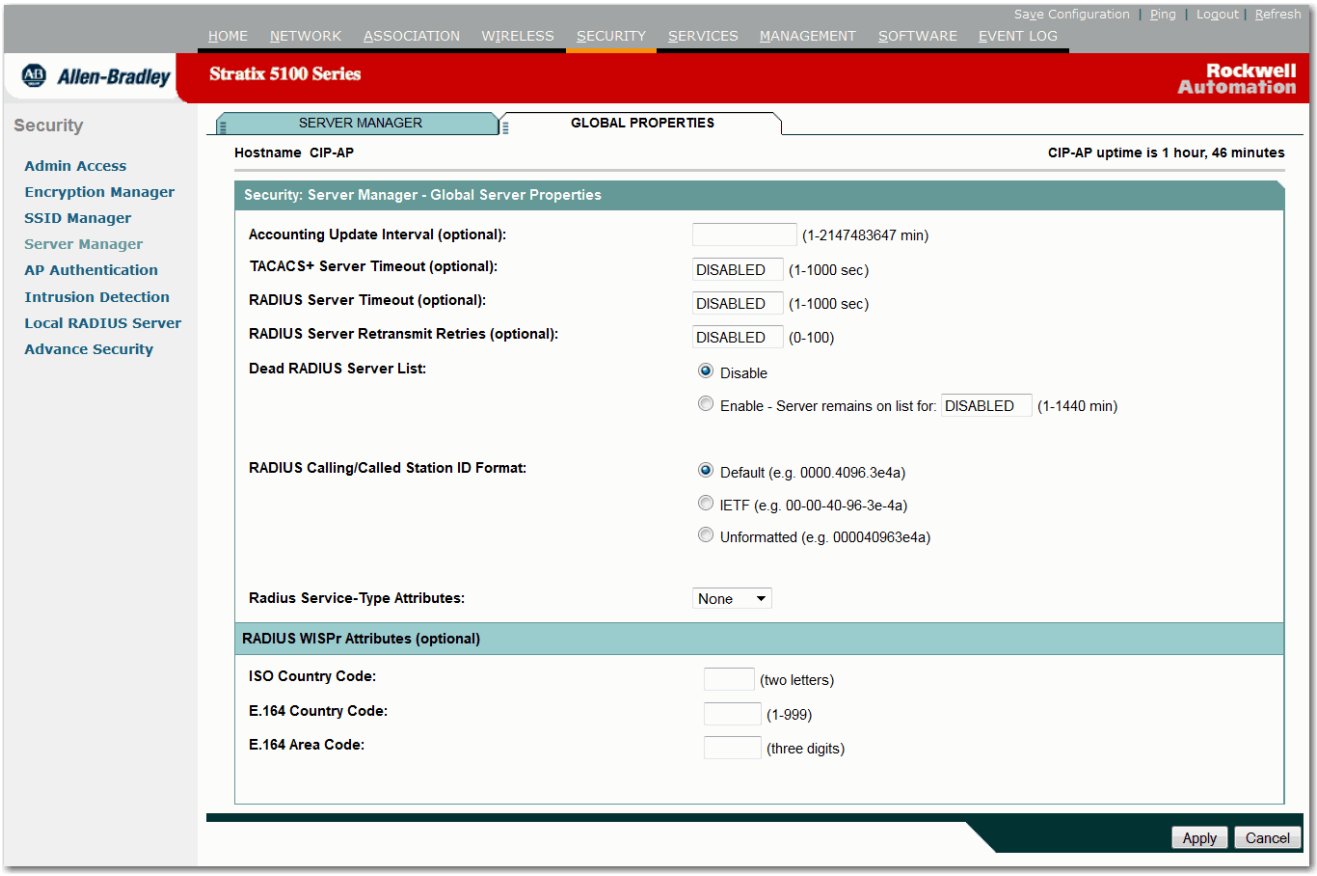


表 34 - 服务器管理器全局属性参数描述

参数	描述
Accounting Update Interval (optional)	1…2147483647 分钟
TACACS+ Server Timeout (optional)	1…1000 秒
RADIUS Server Timeout (optional)	1…1000 秒
RADIUS Server Retransmit Retries (optional)	0…100
Dead RADIUS Server List	启用 —— 服务器在列表中保留 1…1440 分钟 禁用

表 34 - 服务器管理器全局属性参数描述

参数	描述
RADIUS Calling/Called Station ID Format	默认 示例：0000.4096.3e4a IETF 示例：00-00-40-96-3e-4a 无格式 示例：000040963e4a
RADIUS Service-Type Attributes	登录 框架化
RADIUS WISPr Attributes (optional)	ISO 国家代码 (2 个字母) E.164 1…999 国家代码 E.164 三位区域代码

AP 验证

按照惯例， dot1x 验证器 / 客户端关系始终分别是网络设备与 PC 客户端的关系，因为个人计算机用户都必须进行验证，以获取网络访问权限。但是，无线网络为传统的验证器 / 客户端关系引入了独特的挑战。

首先，接入点可能位于公共场所，因此有可能被拔下，网络连接也可能被外部人员使用。其次，当将一个工作组网桥或中继器接入点集成到无线网络中时，中继器接入点必须采用和客户端一样的方法执行与根级接入点的验证。如果使用 EAP 验证替代预共享密钥，需要在 WGB 或中继器上配置验证凭证。

必须先创建并配置凭证配置文件，然后将凭证应用于接口或 SSID。凭证用于验证连接至网络的接入点。

图 53 - AP 验证

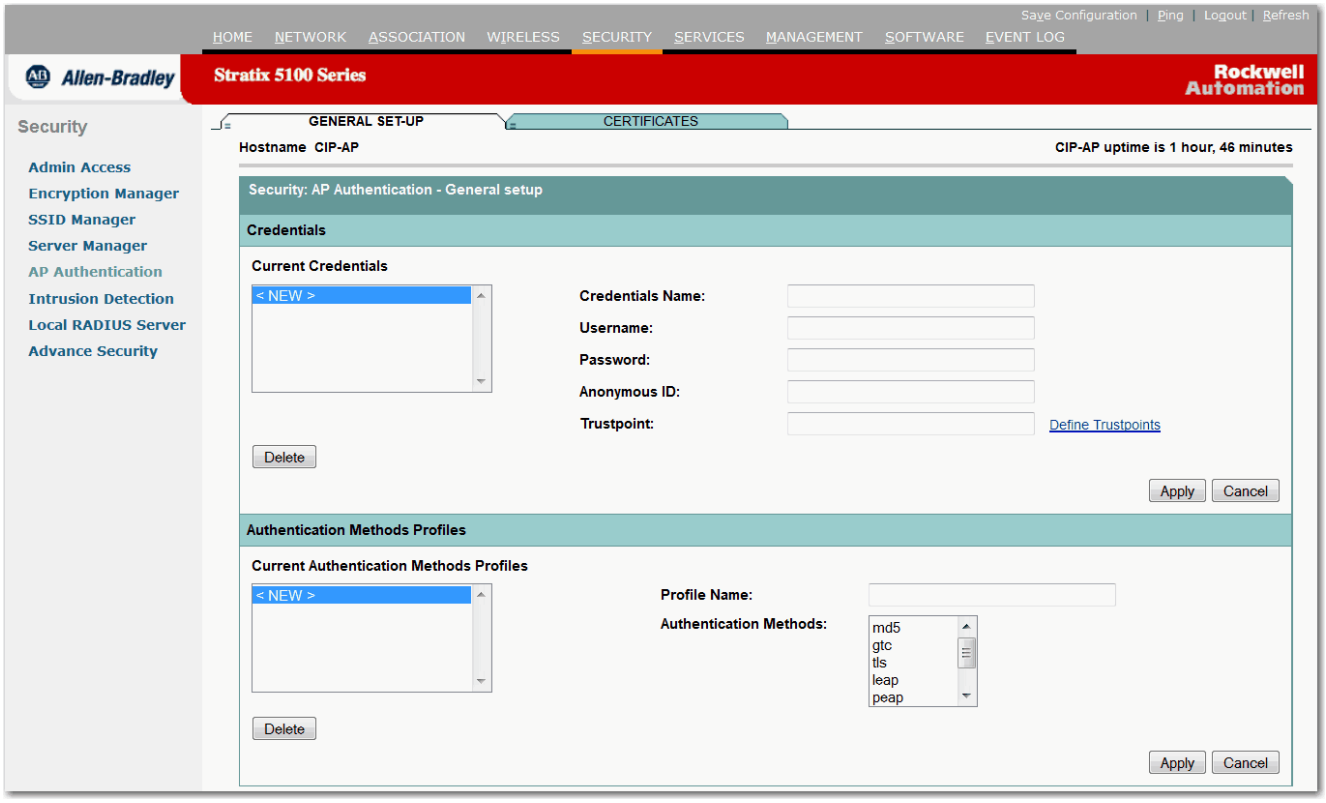


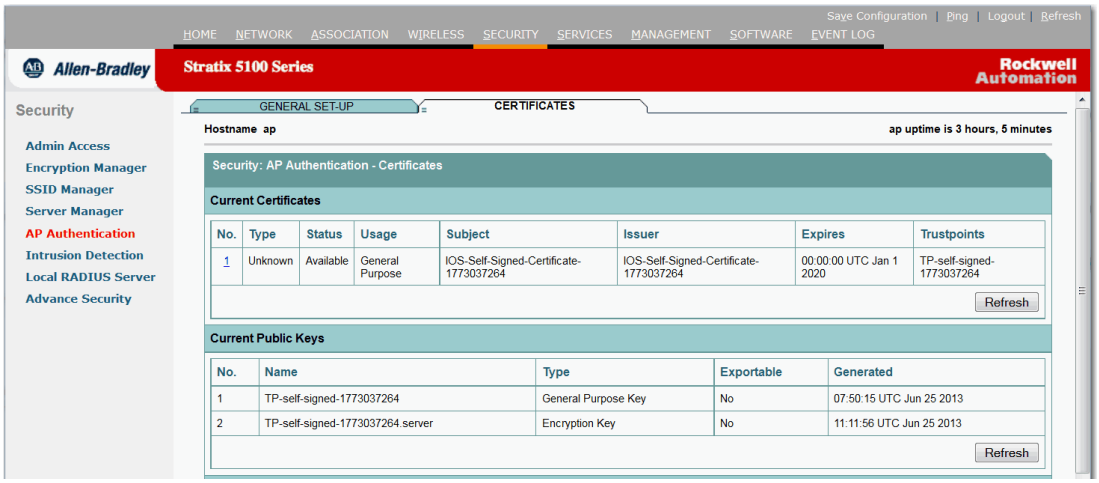
表 35 - AP 验证常规设置参数描述

参数	描述
Current Credentials	如果要添加 dot1x 凭证配置文件，选择 <NEW> (新建)。
Credentials Name	如果添加新的配置文件，输入 dot1x 凭证配置文件的名称。如果选择现有配置文件，您可更改名称。
Username	输入身份验证用户 ID。
Password	输入验证密码。
Anonymous ID	输入要使用的匿名身份。根据网络验证要求，您可配置匿名 ID，而不使用用户名和密码。
Trustpoint	通过信任点管理路由器证书和关联 CA 证书。输入默认 pki-trustpoint。如果网络验证需要，输入信任点。
Define Trustpoints	如果需要定义信任点，单击该链接跳转到 AP Authentication - Certificates (AP 验证 — 证书) 页面，您可在此配置信任点的参数。
Authentication Methods Profile	凭证配置文件以相同的方式应用到接口或 SSID。当接入点连接到网络时，接入点和网络验证设备进行协商，就两种设备共同支持的验证方法达成一致，以完成验证。 验证方法配置文件用于限制接入点同意使用的验证类型。如果要限制用于与网络验证的验证类型，则定义验证方法配置文件，并将其分配给相关的 SSID 或 GigabitEthernet 接口。 该限制措施可防止网络验证服务器和接入点协商诸如 LEAP 等验证方法，而不是更安全的验证方法，如 EAP-FAST。
Current Authentication Methods Profile	如果要添加验证方法配置文件，选择 <NEW> (新建)。
Profile Name	如果添加新的配置文件，输入验证方法配置文件的名称。如果选择现有配置文件，您可更改名称。
Authentication Methods	选择接入点与网络验证时需要使用的验证方法。通过选择强验证方法，您可防止接入点准许较弱的验证方法。 例如，如果 RADIUS 服务器支持 EAP-FAST 和 LEAP，在某些配置下，服务器一开始可配置 LEAP，而不是更安全的方法。如果未在该参数中定义首选方法列表，可选择 LEAP，而不使用更优的 EAP-FAST。

AP 验证证书

此页面列出了当前可用的证书和公钥。您还可以配置信任点参数。

图 54 - AP 验证证书



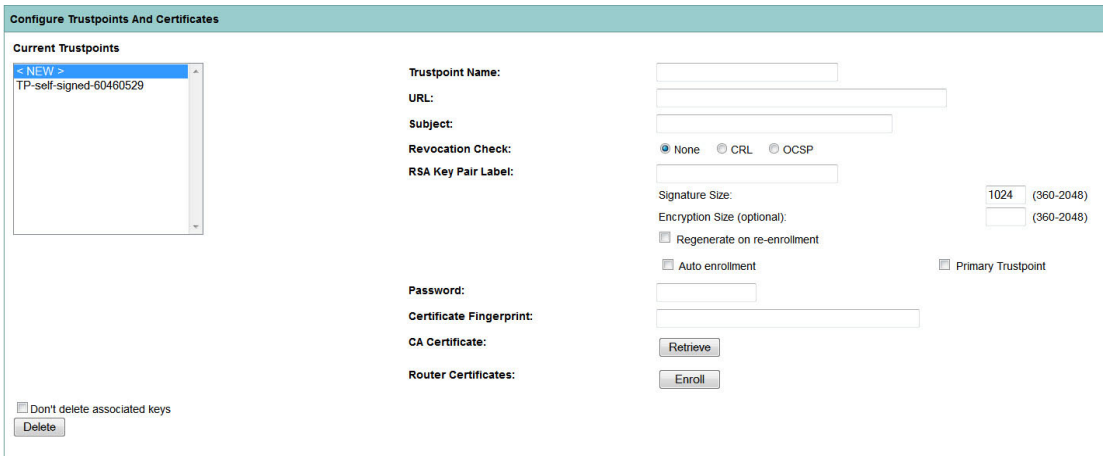


表 36 - 证书页面属性参数描述

参数	描述
Certificates	接入点上当前安装的证书列表。
Current Public Keys	可用的公共密钥列表。
Current Trustpoints	接入点认证操作当前使用的证书颁发机构。 • CA Certificate 在定义信任点后，单击 Retrieve (提取) 按钮下载证书认证机构证书。 • Router Certificates 在成功提取 CA 证书后，单击 Enroll (注册) 按钮注册带 CA 的接入点证书。将向 CA 发送证书注册请求，并安装接收到的证书。操作将立即执行，或花费一些时间，具体取决于 CA 设置。例如，一些 CA 被设置为立即发布证书，而一些则需要人工干预，从而导致证书发布时间推延。 • Don't delete associated keys 当删除信任点时，关联的 RSA 密钥也将被删除。如果要确保密钥完好，则必须在删除之前选中该选项。
Trustpoint Name	分配的唯一名称，用于定义或分组证书认证机构的详情。
URL	CA 的注册 URL (因供应商不同而异)。
Subject	所请求的 X.509 证书中主题域的详情。
Revocation Check	指定是否对收到的证书执行证书更新检查。对于 EAP-TLS，将该项设为 None (否)。
RSA Key Pair Label	用于标识证书 RSA 密钥的可选名称。
Signature/Encryption Size	RSA 密钥所需的位数。位数越多越安全。
Regenerate on Enroll	如果选中了该选项，当在证书认证机构中注册证书时，将生成 RSA 密钥。
Auto-enroll	在配置信任点时自动注册证书。无需专门下载 CA 证书，然后再注册路由器证书，这些过程都是自动完成的。
CA Certificate	在定义信任点后，单击 Retrieve (提取) 按钮下载证书认证机构证书。
Router Certificates	在成功提取 CA 证书后，单击 Enroll (注册) 按钮注册带 CA 的接入点证书。将向 CA 发送证书注册请求，并安装接收到的证书。操作将立即执行，或花费一些时间，具体取决于 CA 设置。例如，一些 CA 被设置为立即发布证书，而一些则需要人工干预，从而导致证书发布时间推延。
Don't delete associated keys	当删除信任点时，关联的 RSA 密钥也将被删除。如果要确保密钥完好，则必须在删除之前选中该选项。
Current Trustpoints	• CA 证书 在定义信任点后，单击 Retrieve (提取) 按钮下载证书认证机构证书。 • 路由器证书 在成功提取 CA 证书后，单击 Enroll (注册) 按钮注册带 CA 的接入点证书。将向 CA 发送证书注册请求，并安装接收到的证书。操作将立即执行，或花费一些时间，具体取决于 CA 设置。例如，一些 CA 被设置为立即发布证书，而一些则需要人工干预，从而导致证书发布时间推延。 • 不删除关联密钥 当删除信任点时，关联的 RSA 密钥也将被删除。如果要确保密钥完好，则必须在删除之前选中该选项。

入侵检测

管理帧保护可用于识别发起拒绝服务攻击、通过关联和嗅探导致网络洪泛、插入非法接入点或通过攻击 QoS 和无线电测量帧影响网络性能的恶意行为。

图 55 - 入侵检测：管理帧保护

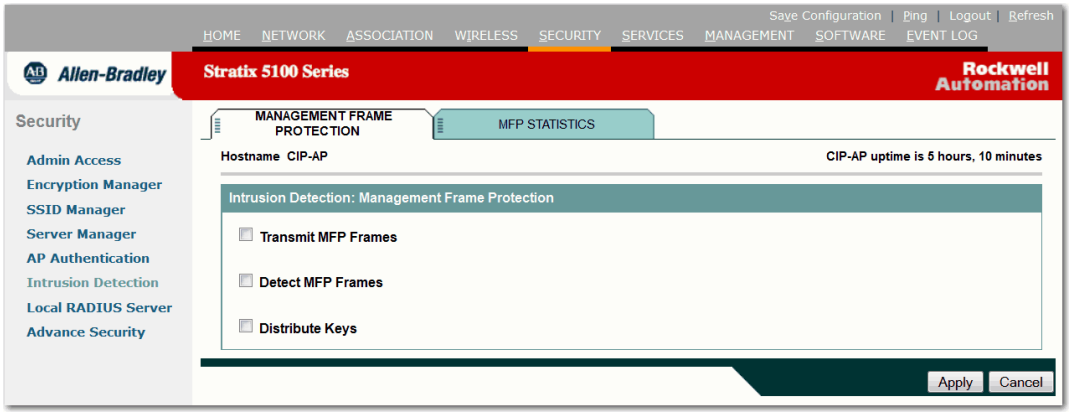


图 56 - 入侵检测：MFP 统计数据

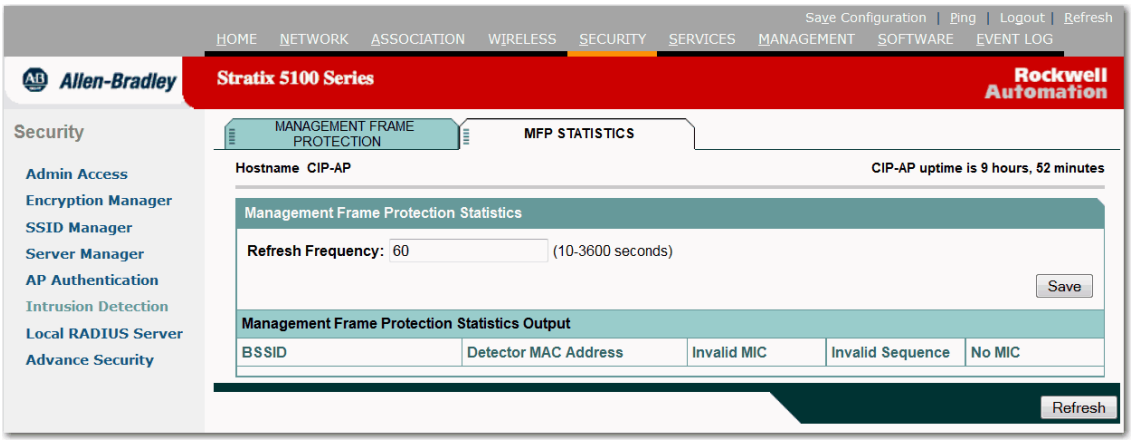


表 37 - Intrusion Detection (入侵检测) 页面参数描述

参数	描述
Transmit MFP Frames	启用时，接入点为每个帧通过添加消息完整性检查信息元素 (MIC IE)，实现对管理帧的保护。任何复制、修改或重发帧的尝试都将导致 MIC 失效，致使任何被配置为检测 MFP 帧的接收接入点报告该不一致。接入点必须是发送 MFP 帧的 WDS 的成员。如果不是，将在该页面中显示一条警告消息。
Detect MFP Frames	当启用 MFP 检测时，接入点将验证从网络中其他接入点接收到的每个管理帧。它确保 MIC IE 存在 (当发起方配置为发送 MFP 帧时) 并匹配管理帧的内容。 接入点必须是检测 MFP 帧的 WDS 的成员。如果不是，将在该页面中显示一条警告消息。
Distribute Keys	必须至少将网络中的一个 WDS 配置为向网络中的 MFP 发生器 (保护器) 和 MFP 检测器 (验证器) 发布签名密钥。发生器需要用它创建 MIC IE，检测器需要用它验证 MIC IE。 如果接入点不是 WDS，则不显示该复选框。

本地 RADIUS 服务器

通常使用一个外部 RADIUS 服务器来验证用户。在某些情况下，这不是一个可行的解决方案。在这些情况下，接入点可以充当 RADIUS 服务器。在此，根据在接入点中配置的本地数据库对用户执行验证。这就是所谓的本地 RADIUS 服务器功能。此外，您也可令网络中的其他接入点使用某个接入点上的本地 RADIUS 服务器功能。

图 57 - Local RADIUS Server Statistics (本地 RADIUS 服务器统计数据) 页面

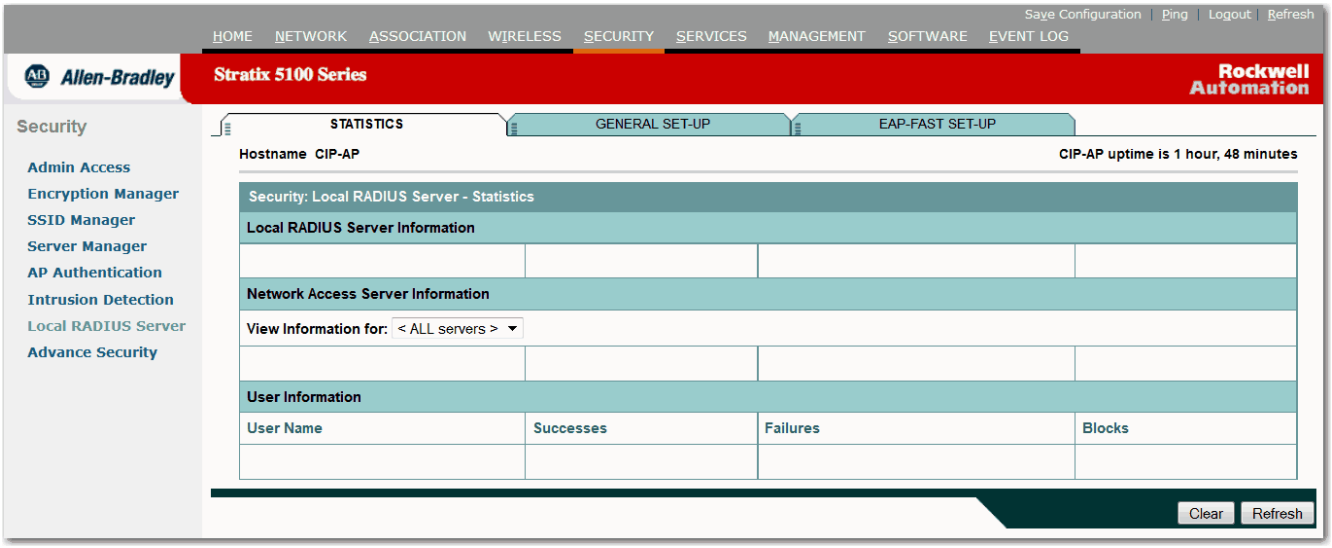


表 38 - Local RADIUS Server Statistics (本地 RADIUS 服务器统计) 信息页面参数描述

参数	描述
Blocks	验证忽略次数，当某个用户多次验证失败时，该用户名将被阻止，验证将被忽略。
Failures	该名用户验证失败次数，通常是由于密码错误。
Network Access Server xx.xx.xx.xx	选择要查看的网络接入服务器。网络接入服务器是配置为使用本地 RADIUS 服务器作为备用认证器的接入点。
Successes	验证成功次数。
User Name	显示活动用户的用户名。

图 58 - Local RADIUS Server General Set-up (本地 RADIUS 服务器常规设置) 页面

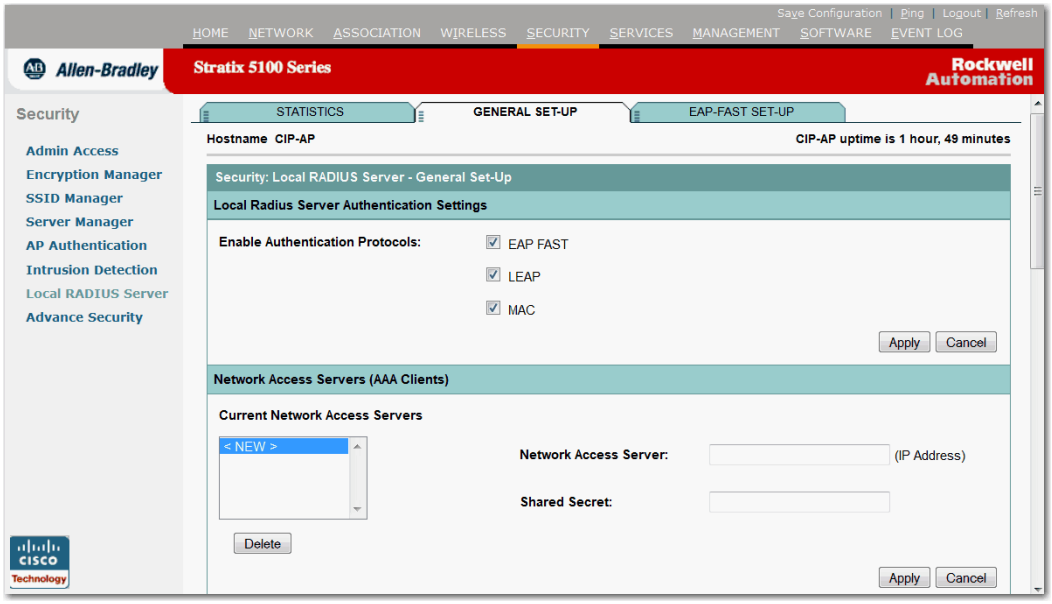
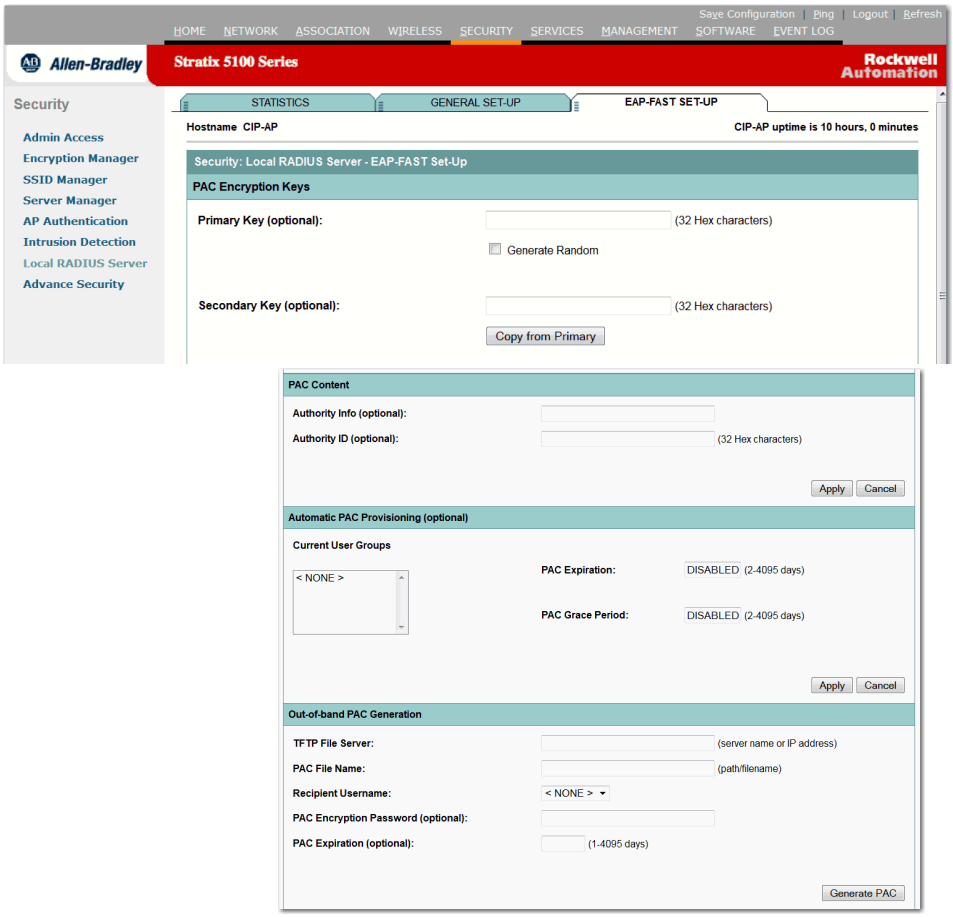


表 39 - Local RADIUS Server General Set-up (本地 RADIUS 服务器常规设置) 页面参数描述

参数	描述
Enable Authentication Protocols	EAP FAST LEAP MAC
Network Access Server (AAA Clients)	当前网络访问服务器 网络访问服务器 (IP 地址) 共享密文
Individual Users	当前用户 用户名：文本或 NT Hash 密码 组名 仅 MAC 验证
User Groups	当前用户组 组名 会话超时 (可选)：1…4294967295 s 锁定前允许的验证失败时间 (可选)：1…4294967295 s 锁定时间 (可选)：无限或间隔 1…4294967295 s VLAN ID (可选) SSID (可选)

图 59 - Local RADIUS Server EAP-Fast Set-up (本地 RADIUS 服务器 EAP 快速设置) 页面



提示　EAP-FAST 验证的默认设置适用于大多数无线局域网。但是，您可根据网络要求自定义凭证超时值、权限 ID 和服务器密钥。

表 40 - Local RADIUS Server EAP-Fast Set-up (本地 RADIUS 服务器 EAP-Fast 设置) 页面参数描述

参数	描述
PAC Encryption Keys	• 主密钥 (可选)：32 个十六进制字符；随机生成 • 辅助密钥 (可选)：32 个十六进制字符；从主密钥复制
PAC Content	• 颁发机构信息 (可选) • 颁发机构 ID (可选)， 32 个十六进制字符
Automatic PAC Provisioning (optional)	当前用户组 • PAC 到期时间：2…4095 天 • PAC 宽限期：2…4095 天
Out-of- PAC Generation	• TFTP 文件服务器：服务器名称或 IP 地址 • PAC 文件名：路径 / 文件名 • 接收方用户名 • PAC 加密密码 (可选) • PAC 到期时间 (可选)：1…4095 天

高级安全

您可设置接入点采用 MAC 与 EAP 相结合的验证方法来验证客户端设备，请参见第 115 页的 “SSID Manager (SSID 管理器) 页面 ”。当启用此功能时，与使用 802.11 开放式验证的接入点关联的客户端设备首先尝试 MAC 验证。

- 如果 MAC 验证成功，则客户端设备加入网络。
- 如果 MAC 验证失败，则接入点等待客户端设备尝试 EAP 验证。

图 60 - MAC Address Authentication (MAC 地址验证) 页面

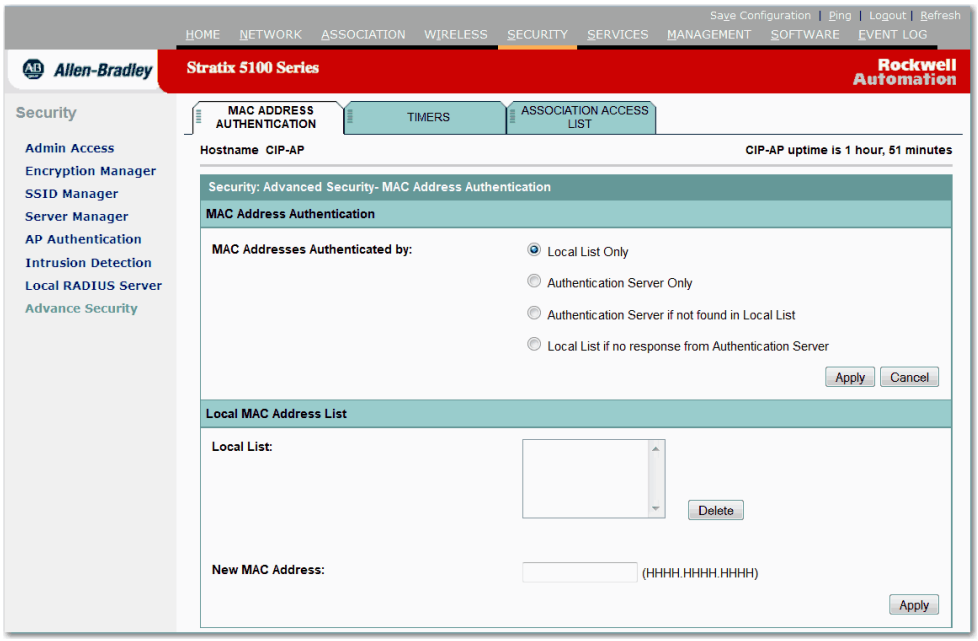


表 41 - MAC Address Authentication (MAC 地址验证) 页面参数描述

参数	描述
MAC Addresses Authenticated by	仅本地列表 • 如果要将验证信息保存在接入点中，选择 Local List Only (仅本地列表) 并输入 MAC 地址。 仅验证服务器 • 如果要将验证信息保存在服务器上，选择 Authentication Server Only (仅验证服务器) 选项。 如果未在本地列表中找到，使用验证服务器 • 如果要先尝试 MAC 验证列表，然后再自动尝试验证服务器列表，选择 Authentication Server if not found in Local List (如果本地列表中未找到，则使用验证服务器)。如果验证成功，客户端将加入到网络中。 如果验证服务器没有响应，使用本地列表 • 如果选择 Authentication Server Only (仅验证服务器) 或 Authentication Server if not found in Local List (如果本地列表中未找到，则使用验证服务器)，需要在 Server Manager (服务器管理器) 页面中至少选择一种 MAC 验证。
Local MAC Address List	本地列表 • 本地列表中显示 MAC 地址。 MAC 地址将保留在管理系统中，直到将其删除。要从列表中删除 MAC 地址，选择地址然后单击 Delete (删除)。 新建 MAC 地址：HHHH.HHHH.HHHH • 如果需要输入新的 MAC 地址，则输入地址，并以句点分隔三个四字符组，例如，40.9612.3456。 • 为确保过滤器正确操作， MAC 地址中的字母均使用小写输入。单击 Apply (应用) 将 MAC 地址存入管理系统中。还必须在 SSID Manager (SSID 管理器) 页面中启用 MAC 地址验证。您可导览到 Association (关联) 页面，确认是否已关联和验证预配置的客户端。

图 61 - Timers (计时器) 页面

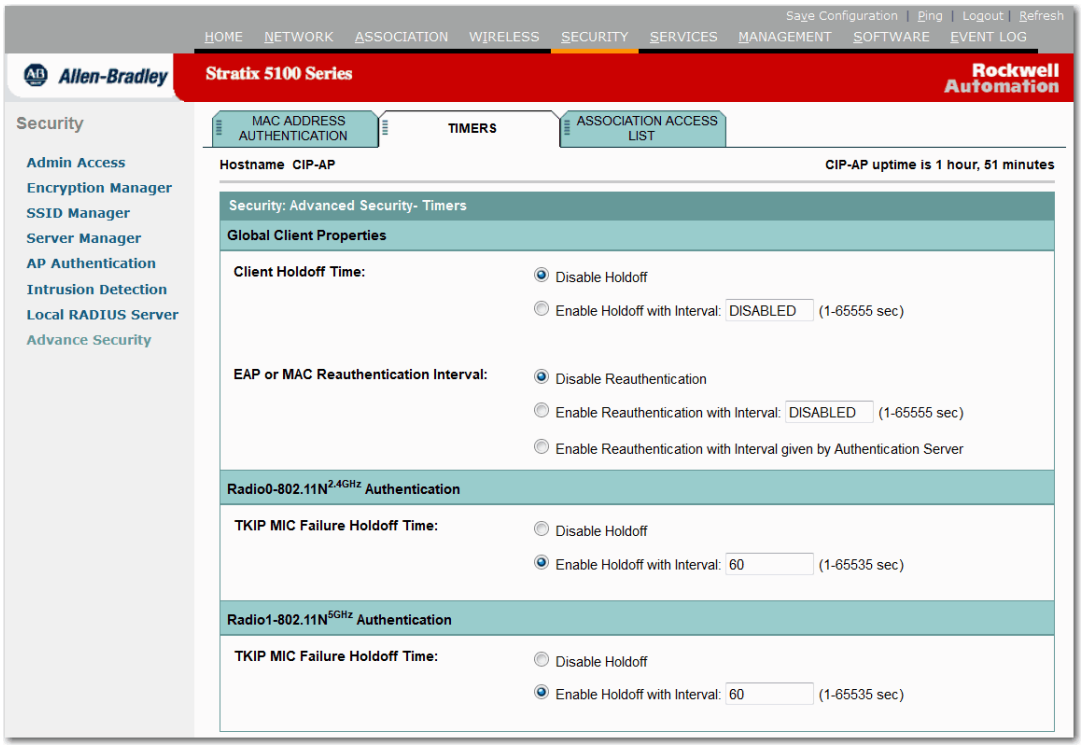


表 42 - Timers (计时器) 页面参数描述

参数	描述
Global Client Properties	客户端保持时间 禁用保持 启用保持，间隔为：1…65555 s
EAP or MAC Reauthentication Interval	禁用重新验证 (启用重新验证，间隔为：1…65555 s 以验证服务器给定的间隔启用重新验证
Radio0-802.11N2.4 GHz Authentication	TKIP MIC 故障保持时间 禁用保持 启用保持，间隔为：1…65535 s
Radio1-802.11N2.4 GHz Authentication	TKIP MIC 故障保持时间 禁用保持 启用保持，间隔为：1…65535 s
Association Access List Page Parameter Descriptions	通过 MAC 地址访问列表过滤客户端关联 定义过滤器：该链接将跳转到 Services (服务) 页面的 MAC Address Filters (MAC 地址过滤器)。

图 62 - Associated Access list (关联的访问列表) 页面

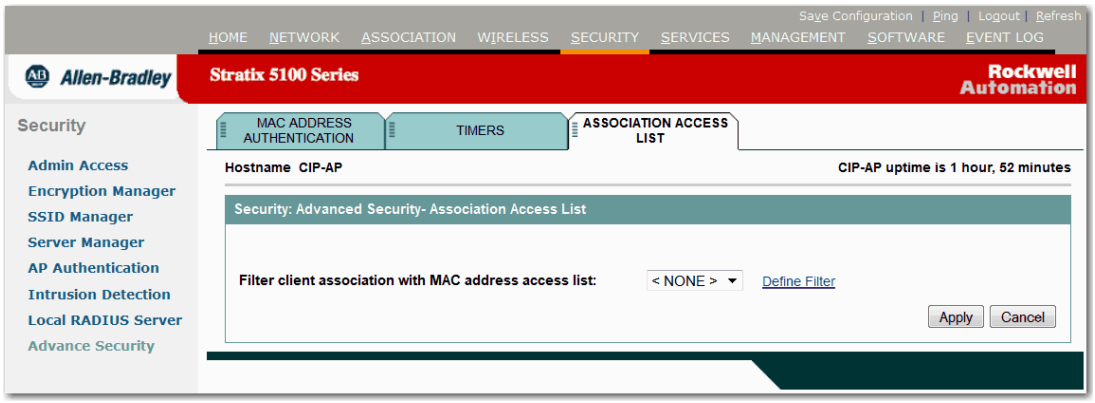


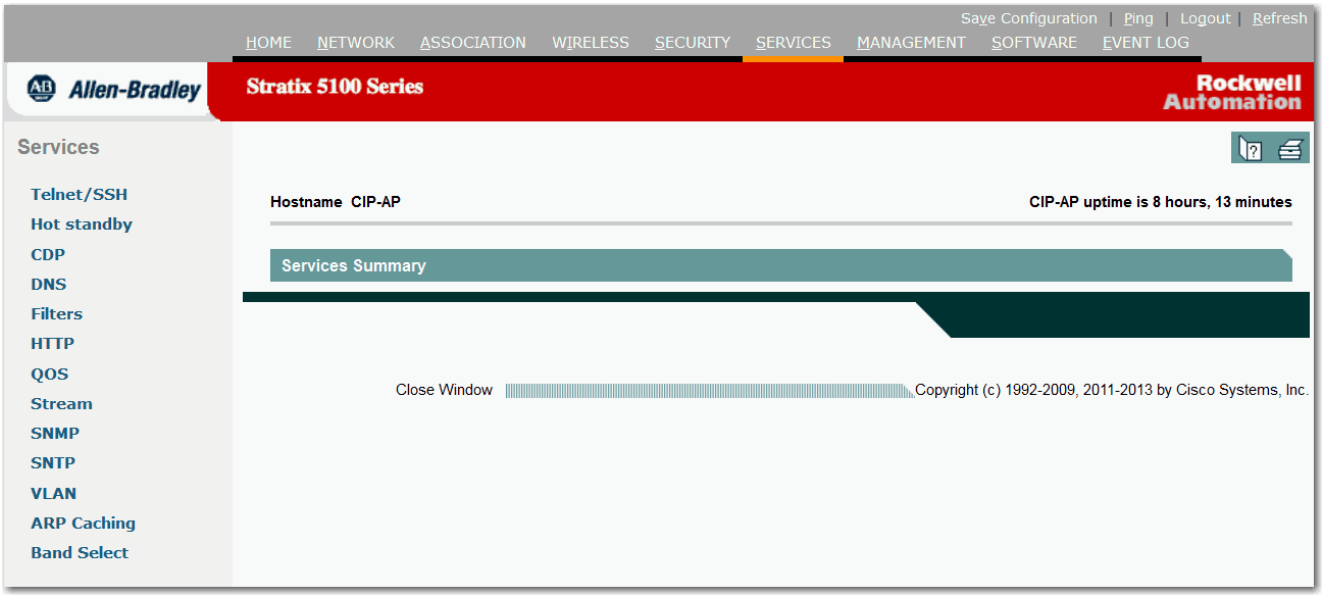
表 43 - 关联访问列表页面参数描述

参数	描述
通过 MAC 地址访问列表过滤客户端关联	选择一个过滤器。
Define Filter	该链接将跳转到 Service>Filter (服务 > 过滤器)，您可在此配置过滤器。

Services (服务) 页面

概览部分给出了当前启用或禁用的主服务列表。您可以单击任意链接进入该页面并更改配置。

图 63 - Services (服务) 页面



Telnet/SSH

图 64 - Telnet/SSH 页面

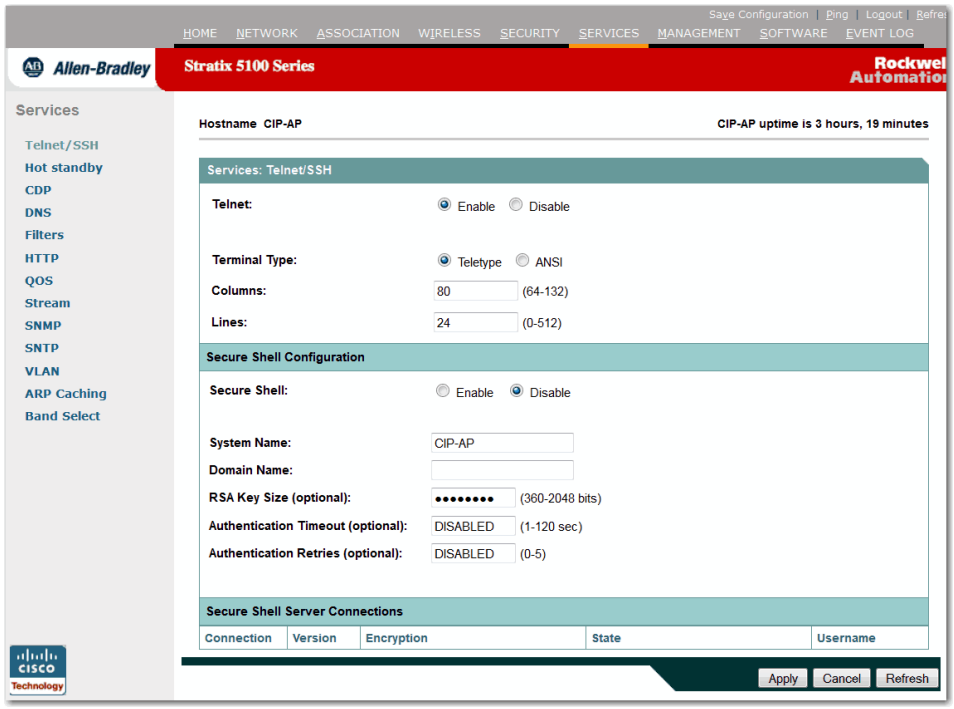


表 44 - Telnet/SSH 页面参数描述

参数	描述
Telnet/SSH…	• Telnet 启用或禁用。选择 Enabled (启用) 让 Telnet 访问管理系统。 • 终端类型 Teletype 或 ANSI。首选设置为 ANSI，它可提供图形功能，如反白显示按钮和下划线链接。并不是所有终端仿真器都支持 ANSI，因此，默认设置为 Teletype。 • 列 64…132 定义终端仿真器的显示宽度，范围为 64…132 字符。调整该值，实现终端仿真器的最优显示。 • 行 0…512 定义终端仿真器的显示高度，范围为 16…50 字符。调整该值，实现终端仿真器的最优显示。
Secure Shell Configuration	在 安全外壳 (SSH) 之前，安全功能仅限 Telnet 安全功能。有了安全外壳，思科 IOS 软件验证便可使用更强大的加密。 安全外壳 • 启用或禁用。 • 如果要启用安全外壳 (SSH) 功能，以使用标准的加密机制提供到接入点的安全远程连接，则选择 Enabled (启用)。 系统名称 • 接入点的主机系统名称。 域名 • 接入点的主机域。生成 SSH 密钥时需要。 RSA 密钥位数 (可选) • 为接入点生成的 RSA 密钥对长度。 验证超时 (可选)：1…120 秒 • 在 SSH 协商阶段，接入点等待客户端响应的时间。 验证重试次数 (可选)：0…5 • 在接口重置之前， SSH 协商尝试的次数。
安全外壳服务器连接	它显示 SSH 服务器连接状态。 • 连接 SSH 会话使用唯一的编号标识。 • 版本 SSH 客户端支持的协议版本号。 • 加密 SSH 客户端使用的加密类型。 • 状态 SSH 会话的进程。 • 用户名 该会话验证所用的登录用户名。

Hot Standby (热备用) 页面

图 65 - Hot Standby (热备用) 页面

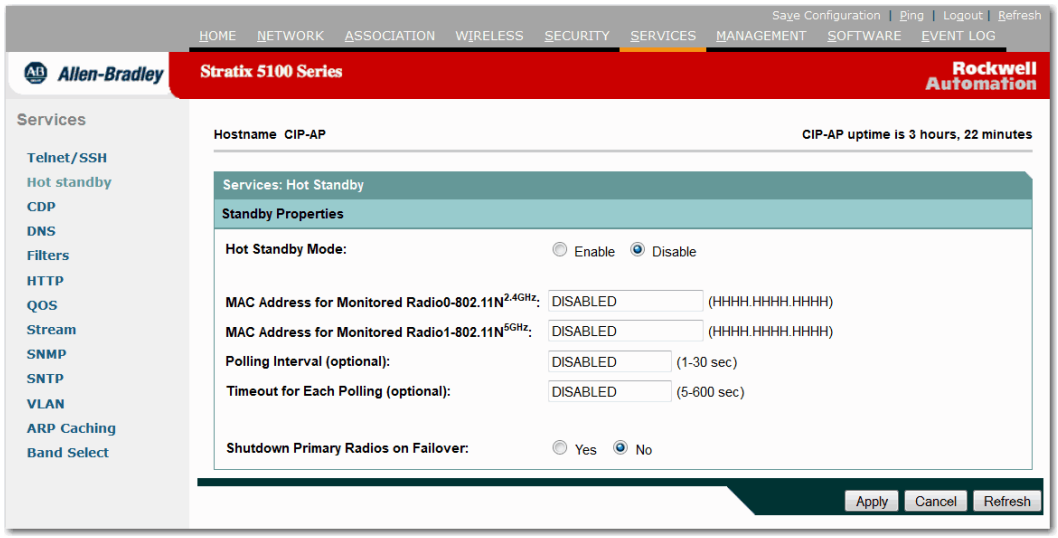


表 45 - Hot Standby (热备用) 页面参数描述

参数	描述
Hot Standby Mode	启用热备用即指定该设备作为另一个接入点的备用设备。备用设备将被置于其所监控的接入点附近，其配置与被监控设备完全相同。备用设备通过以太网和无线电定期查询被监控接入点。如果被监控设备未能响应，备用接入点将进入联机状态，在网络中取代被监控设备的位置。 当启用热备用时，将显示 Standby Status (备用状态) 域。该域显示热备用的当前状态，按下 Refresh (刷新) 可更新状态。
MAC Address for Monitored Radio0-802.11N2.4 GHz	被监控 802.11 b/g/n 无线电装置的 MAC 地址为：HHHH.HHHH.HHHH 被监控设备的 MAC 地址。
MAC Address for Monitored Radio1-802.11N5 GHz	被监控 802.11a/n 无线电装置的 MAC 地址为：HHHH.HHHH.HHHH 被监控设备的 MAC 地址。
Polling Interval (optional)	备用设备发送到被监控接入点的每次轮询之间的秒数。
Timeout for Each Polling (optional)	备用设备需要等待的秒数，在此之后，如果被监控接入点仍未能响应，将认定被监控设备发生故障。
Shutdown Primary Radios on Failover	如果要配置备用接入点，使其在备用单元激活时向被监控接入点发送 Dumb Device Protocol (DDP) 消息，以禁用被监控接入点的无线电装置，则选择 Yes (是)。该功能将阻止关联到被监控接入点的客户端设备保持与故障设备的关联。

注意：与备用接入点关联的客户端在热备用设置过程中丢失连接。

CDP 页面

思科发现协议 (CDP) 是一种运行在所有思科网络设备上的设备发现协议。每台设备向多播地址发送标识消息，每台设备监视其他设备发送的消息。 CDP 数据包中的信息用于网络管理软件。使用 CDP 页调节设备的 CDP 设置。

图 66 - CDP 页面

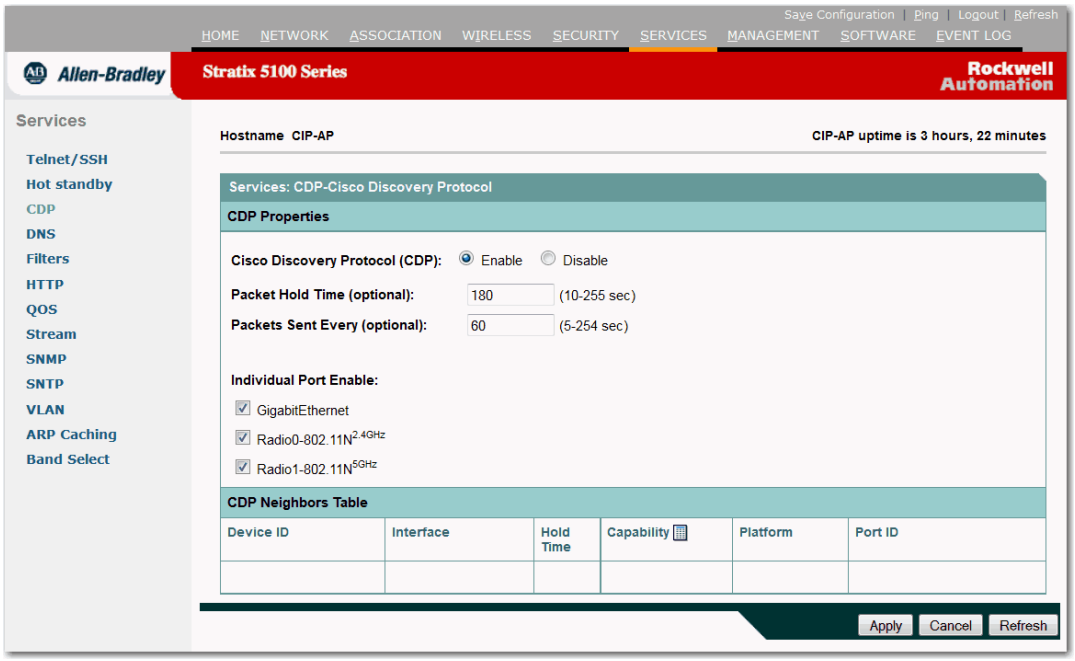


表 46 - CDP 页面参数描述

参数	描述
Cisco Discovery Protocol (CDP)	选择 Disabled (禁用) 禁用设备上的 CDP ； 选择 Enabled (启用) 启用设备上的 CDP。 CDP 默认已启用。
Packet Hold Time (optional)	其他启用 CDP 的设备认为 CDP 信息有效所需的秒数。如果其他设备在此时间内未从设备接收到另一个 CDP 数据包，设备很可能已经脱机。默认值为 180。数据包保持时间始终应大于 Packets Sent Every (数据包发送间隔) 域中的值。

表 46 - CDP 页面参数描述 (续)

参数	描述
Packets Sent Every (optional)	设备发送的各 CDP 数据包之间的秒数。默认值为 60。该值应小于数据包保持时间。
Individual Port Enable	• 以太网 当选择后，设备通过其以太网端口发送 CDP 数据包，并监控以太网是否有另一个设备的 CDP 数据包。 • 接入点无线电选项 当选择后，设备通过其内部无线电端口发送 CDP 数据包，并监控内部无线电装置是否有另一个设备的 CDP 数据包。 注意：提供 MIB 文件配合 CDP 使用。文件名为 CISCO-CDP-MIB.my，您可在此下载 MIB 文件： http://www.cisco.com/public/mibs/v1/CISCO-CDP-MIB-V1SMI.my。
CDP Neighbors Table	该区域显示所发现的设备类型。特别是显示以下这些值。 • 设备 ID 设备的已配置 ID、 MAC 地址或序列号。 • 接口 所使用的本地接口协议的编号和类型。 • 保持时间 当前设备保持来自发送路由器的 CDP 广告的剩余秒数，此后它将被丢弃。 • 功能 CDP 邻居表中所列的设备类型。对于路由器，可能值为 R，透明网桥为 T，网桥为 B，交换器为 S，主机为 H，IGMP 设备为 I，中继器为 r。如果单击计算器图像，可看到带有功能代码图例的弹出窗口。 • 平台 设备的产品编号。 • 端口 ID 设备的协议和端口号。

DNS 页面

在该页面中决定是否启用或禁用 DNS (域名系统)。 DNS 是一个命名服务器，它允许您连接到一个设备，而无需知道其 IP 地址，但可通过给定的名称对此设备进行访问。因此，在给 WAP 命名，并分配了要使用的 DNS 服务器后，您需要确保 DNS 服务器拥有 WAP 记录。如需了解使用 DNS 的更多信息，请参见第 67 页的 “ 启用 HTTPS 实现安全浏览 ”。

图 67 - DNS 页面

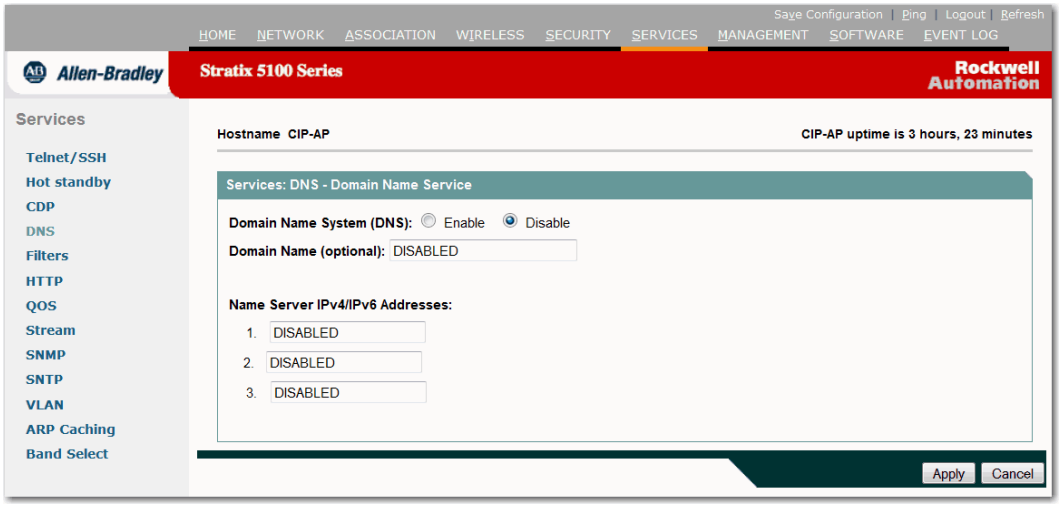


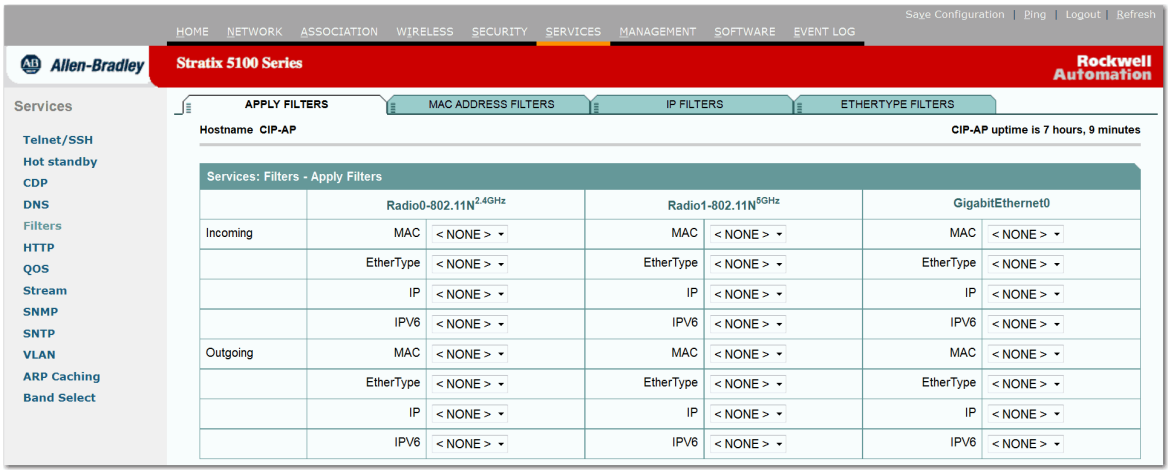
表 47 - DNS 页面参数描述

参数	描述
Domain Name System (DNS)	在此选择启用或禁用 DNS。如果启用 DNS，至少需要输入一个域名服务器。
Domain Name (optional)	如果网络使用域名系统 (DNS)，输入网络的 IP 域的名称。输入类似于 mycompany.com。
域名服务器 IP 地址	输入网络中最多三个域名服务器的 IP 地址。

Filters (过滤器) 页面

协议过滤器用于阻止或允许通过接口使用特定的协议。您可设置单个协议过滤器或过滤器组。该基本页面允许您对传入和传出以太网和 802.11b 无线电接口应用过滤器。必须在应用之前创建过滤器 协议过滤器通常称为访问控制列表 (ACL)。

图 68 - Filters (过滤器) 页面



在此 Apply Filters (应用过滤器) 页面上启用之前，不会应用在 MAC Address (MAC 地址)、 IP Filters (IP 过滤器) 或 Ethertype Filters (以太网类型过滤器) 页面上设置的任何过滤器。

小心地应用过滤器。过滤器配置错误会导致您被锁定，无法访问接入点。如果发生这种情况，恢复方法是通过控制台端口访问 (如果可用)，或将接入点复位到默认配置。

表 48 - 应用过滤器页面参数描述

参数	描述
Incoming	从下拉菜单中选择要启用的 MAC、以太网类型和 IP 协议过滤器集。
Outgoing	从下拉菜单中选择要启用的 MAC、以太网类型和 IP 协议过滤器集。

如需了解将 WAP 复位到默认配置的更多信息，请参见第 53 页的 “ 将 WAP 复位到默认设置 ”。

MAC Address Filters (MAC 地址过滤器) 页面

使用该页面允许或禁止向特定的 MAC 地址来回转发单播或多播数据包。您可创建一个过滤器，允许通过除指定地址外的所有 MAC 地址的流量，或者阻止除指定地址外的所有 MAC 地址的流量。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

图 69 - MAC Address Filters (MAC 地址过滤器) 页面

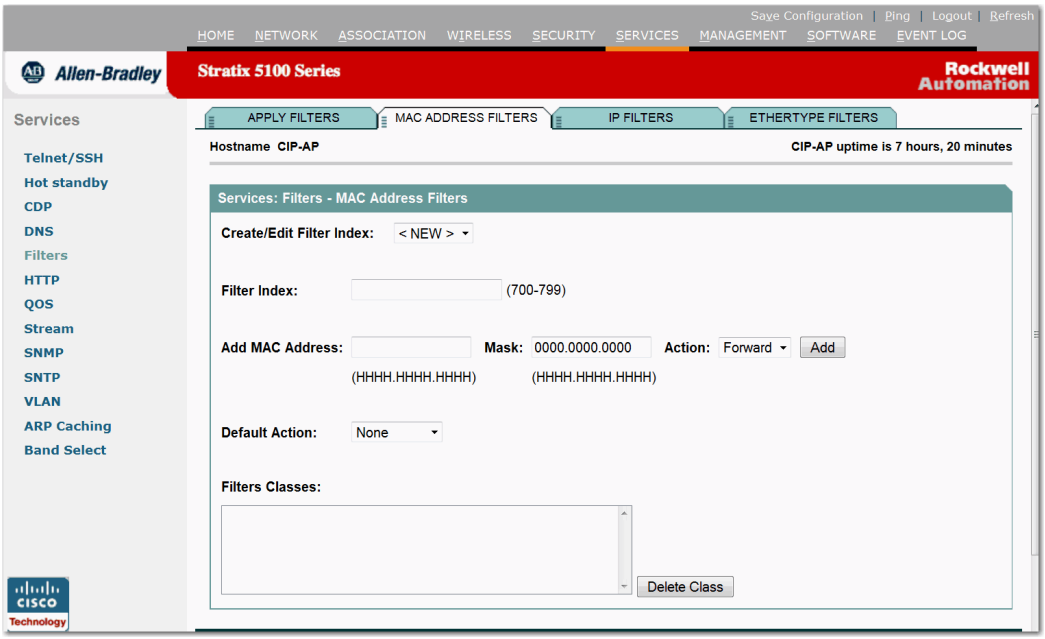


表 49 - MAC Address Filters (MAC 地址过滤器) 页面参数描述

参数	描述
Create/Edit Filter Index	如果要创建新的 MAC 地址过滤器，确保选择 <NEW> (新) (默认值)
Filter Index	使用 700…799 之间的数字给过滤器命名。您所分配的数字将用于创建过滤器的访问控制列表 (ACL)。
Add MAC Address	输入目标 MAC 地址，它是以句点分隔的三个四字符组，例如， 0040.9612.3456。 为确保过滤器正确操作， MAC 地址中的字母均使用小写输入。 如果您打算阻止除了指定允许的地址外的所有 MAC 地址的通信，则将 MAC 地址置于允许的 MAC 地址列表中。
Mask	输入 MAC 地址的掩码。输入掩码，它是以句点分隔的四个三字符组，例如， 112.334.556.778。输入掩码的方法取决于版本。 输入 255.255.255.255 作为掩码将导致接入点接受所有 IP 地址。如果输入 0.0.0.0，则接入点将查找与您在 IP Address (IP 地址) 域中的输入完全匹配的 IP 地址。在该域中输入的掩码其行为方式与在 CLI 中输入的完全相同。

表 49 - MAC Address Filters (MAC 地址过滤器) 页面参数描述 (续)

参数	描述
Action	选择 Forward (转发) 或 Block (阻止)。单击 Add (添加)。MAC 地址将显示在 Filters Classes (过滤器类别) 域中。
Default Action	与任何一个过滤器类别都不匹配的数据包将根据默认操作中的设置进行处理。 选择 Forward All (全部转发) 或 Block All (全部阻止)。过滤器的默认操作必须至少与其中一个过滤器地址的操作相反。例如，如果输入了多个地址，并选择 Block (阻止) 作为所有这些地址的操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。 单击 Apply (应用)，将过滤器保存到接入点上，但它并未被启用，需要在 Apply Filters (应用过滤器) 页面中应用后才会启用。
Filters Classes	要从 Filters Classes (过滤器类别) 列表中删除 MAC 地址，选择该类别，然后单击 Delete (删除)。

IP Filters (IP 过滤器) 页面

使用该页面创建或编辑协议过滤器。 IP 过滤器阻止或允许通过接入点的以太网和无线电端口使用 IP 地址 (ES)、 IP 协议和 TCP/UDP 端口。您可以创建一个过滤器，允许通过除指定地址外的所有地址的流量，也可阻止除指定地址外的所有地址的流量。您可以创建包含一种、两种或所有三种 IP 过滤方法的元素的过滤器。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

图 70 - IP Filters (IP 过滤器) 页面

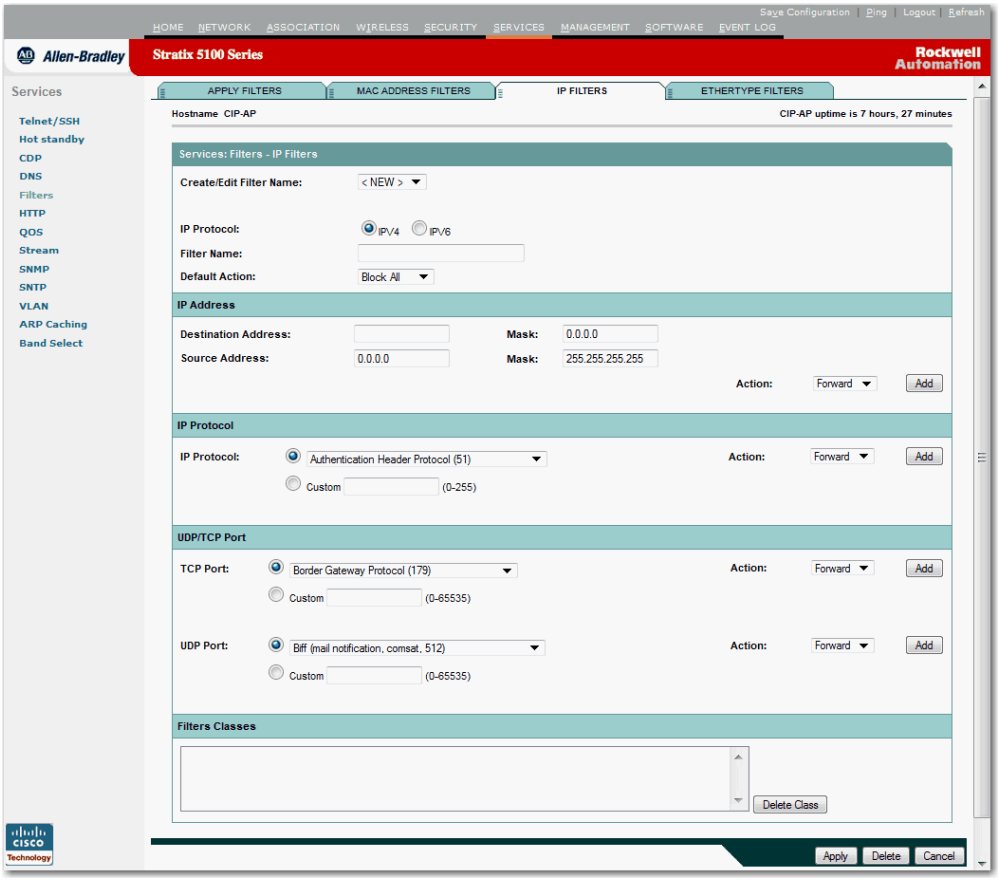


表 50 - IP Filters (IP 过滤器) 页面参数描述

参数	描述
Create/Edit Filter Name	如果要创建新过滤器，确保从 Create/Edit Filter (创建 / 编辑过滤器) 下拉菜单中选择 <NEW> (新) (默认值)。 要编辑现有过滤器，选择 Create/Edit Filter (创建 / 编辑过滤器) 下拉菜单中选择过滤器名称。
IP Protocol	IPv4 IPV6
Filter Name	输入新过滤器的描述性名称。

表 50 - IP Filters (IP 过滤器) 页面参数描述 (续)

参数	描述
Default Action	与任意一个过滤器类别匹配的数据包将根据默认操作中的设置进行处理。 选择 Forward All (全部转发) 或 Block All (全部阻止) 作为过滤器的默认操作。过滤器的默认操作必须至少与其中一个过滤器地址的操作相反。 例如，如果创建了一个包含 IP 地址、IP 协议和 TCP/UDP 端口的过滤器，并选择 Block (阻止) 作为它们的操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。
Destination Address	此处用于识别要过滤的目标 IP 地址。 如果您打算阻止除了指定允许的地址外的所有 MAC 地址的通信，则将计算机地址置于允许地址列表中，以免丢失与接入点的连接。
Source Address	此处用于识别要过滤的源 IP 地址。 如果您打算阻止除了指定允许的地址外的所有 MAC 地址的通信，则将计算机地址置于允许地址列表中，以免丢失与接入点的连接。
Mask	输入目标 IP 地址的掩码。输入掩码，它是以句点分隔的四个三字符组，例如， 112.334.556.778。 • 如果输入 255.255.255.255 作为掩码，接入点将接受任何 IP 地址。 • 如果输入 0.0.0.0，则接入点将查找与您在 IP Address (IP 地址) 域中的输入完全匹配的 IP 地址。 在该域中输入的掩码其行为方式与在 CLI 中输入的完全相同。
IP Protocol	可在此处过滤 IP 协议。从下列菜单中选择一种公共协议，或单击 Custom (自定义) 然后在 Custom (自定义) 域中输入现有 ACL 的编号。 输入 ACL 编号，范围：0…255。
TCP Port	可在此处过滤 TCP 协议。从下拉菜单中选择一种公共端口协议，或选择 Custom (自定义) 单选按钮，然后在其中一个 Custom (自定义) 域中输入现有协议的编号。 输入一个 0…65535 之间的协议编号。
UDP Port	可在此处过滤 UDP 协议。选择一种通用公共端口协议，或选择 Custom (自定义) 单选按钮，然后在其中一个 Custom (自定义) 域中输入现有协议的编号。 输入一个 0…65535 之间的协议编号。
Filters Classes	协议将显示在页面的该区域中。 要从 Filters Classes (过滤器类别) 列表中删除协议，选择该协议，然后单击 Delete (删除)。

Ethertype Filters (以太网类型过滤器) 页面

以太网类型过滤器阻止或允许通过接入点的以太网和无线电端口使用特定的 L3 协议。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

图 71 - Ethertype Filters (以太网类型过滤器) 页面

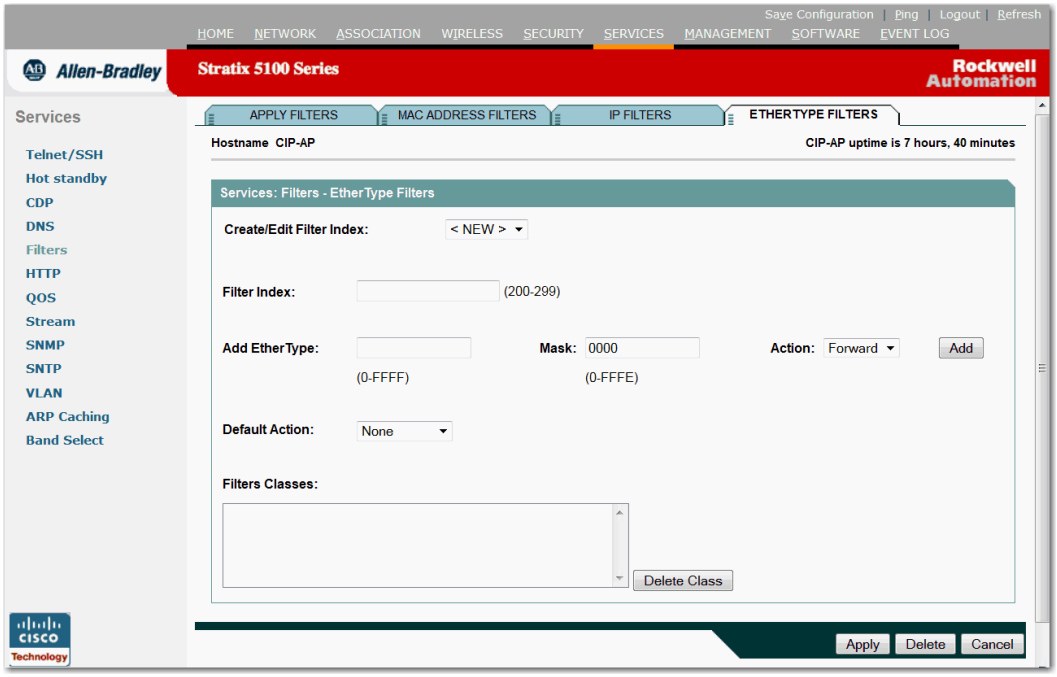


表 51 - Ethertype Filters (以太网类型过滤器) 页面参数描述

参数	描述
Create/Edit Filter Index	如果创建新过滤器，确保在 Create/Edit Index (创建 / 编辑索引) 菜单中选择 <NEW> (新) (默认值)。 要编辑现有过滤器，选择 Create/Edit Index (创建 / 编辑索引) 菜单中选择过滤器编号。
Filter Index	使用 200…299 之间的数字给过滤器命名。 您所分配的数字将用于创建过滤器的访问控制列表 (ACL)。
Add Ethertype	此处用于识别以太网类型编号，并输入以太网类型的掩码。
Default Action	与任何一个过滤器类别都不匹配的数据包将根据默认操作中的设置进行处理。您可选择 Forward All (全部转发) 或 Block All (全部阻止)。 过滤器的默认操作必须至少与其中一个过滤器中以太网类型的操作相反。 例如，如果输入了多个以太网类型，并选择 Block All (全部阻止) 作为所有这些地址的操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。
Filters Classes	显示您已配置的当前过滤器列表。

HTTP 页面

使用 Web Server (Web 服务器) 页面允许浏览到基于 Web 的管理体系文件，并输入定制网络系统的管理设置。

图 72 - HTTP 页面

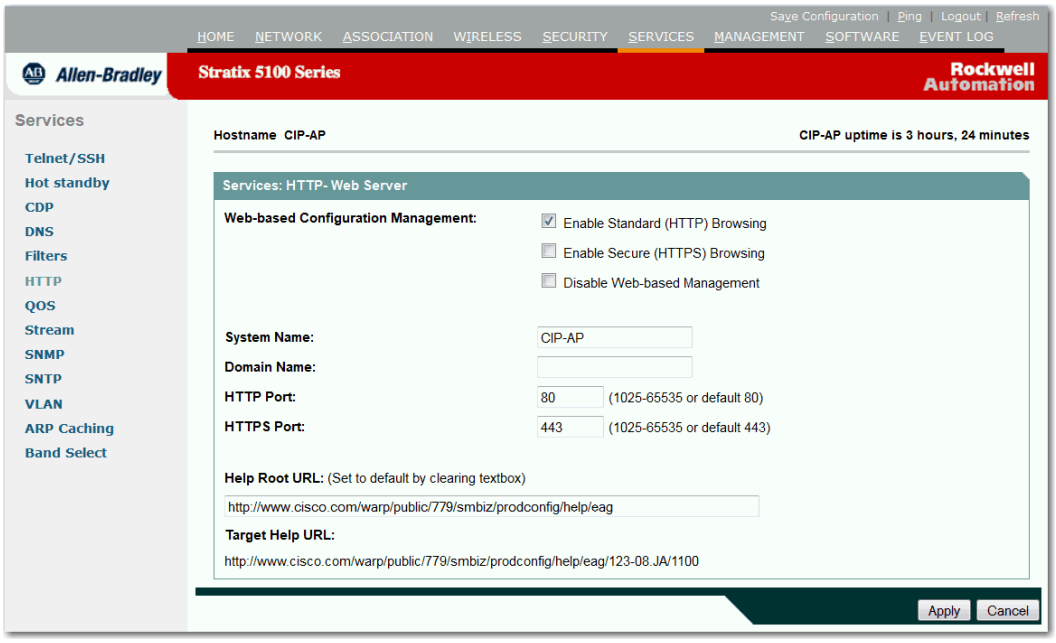


表 52 - HTTP 页面参数描述

参数	描述
Web-based Configuration Management	选中 Enable Standard (HTTP) Browsing (启用标准 (HTTP) 浏览) 以允许管理系统进行非安全浏览。 选中 Enable Secure (HTTPS) Browsing (启用安全 (HTTPS) 浏览) 以允许管理系统进行安全 (SSL) 浏览。 建议两者都选。选择 Disable Web-based Management (禁用基于 Web 的管理) 以阻止管理系统进行浏览。在该模式下，接入点只能通过控制台和 Telnet/SSH 接口访问。 当首次启用 HTTPS 时，将生成自签名证书，并将其保存在接入点中。证书基于您当前的系统名称和域名创建。 证书将在每次后续访问呈现给浏览器，以建立 SSL 连接。证书可安装在您的浏览器中，或在每次访问时批准。 如果证书中的主机名称和域名与 URL 中不匹配，浏览器中将显示一条警告。为避免该警告，在浏览接入点时，系统名称和域名必须与完全限定域名相匹配，而不是 IP 地址。 如果更改了系统名称或域名，选择 Delete Existing SSL Certificate (删除现有 SSL 证书)。这将生成一个新证书。
System Name (or Host Name)	显示在管理系统页和 Association (关联) 页面标题中的系统名称，用于帮助识别网络中的设备。系统名称保存在自签名证书中，该证书用于建立安全浏览器连接。
Domain Name	网络的 IP 域名 (例如， mycompany.com)。域名保存在自签名证书中，该证书用于建立安全浏览器连接。

表 52 - HTTP 页面参数描述 (续)

参数	描述
HTTP Port	该设置决定了设备提供给非安全 Web 访问的端口。使用您的系统管理员提供的端口设置。默认值为 80。
HTTPS Port	该设置决定了设备提供给安全 (SSL) Web 访问的端口。使用您的系统管理员提供的端口设置。默认值为 443。
Target Help URL	显示帮助文件的完整 URL，包括附加版本号和型号。

QoS Policies (QoS 策略) 页面

该页面允许您配置接入点的服务质量 (QoS)。通过此功能，您可对某些流量提供优先处理。在不使用 QoS 时，接入点为每个数据包 (无论数据包的内容和大小) 提供尽力服务。它发送数据包时不提供关于可靠性、延迟界限或吞吐量的任何保证。

图 73 - QoS Policy (QoS 策略) 页面

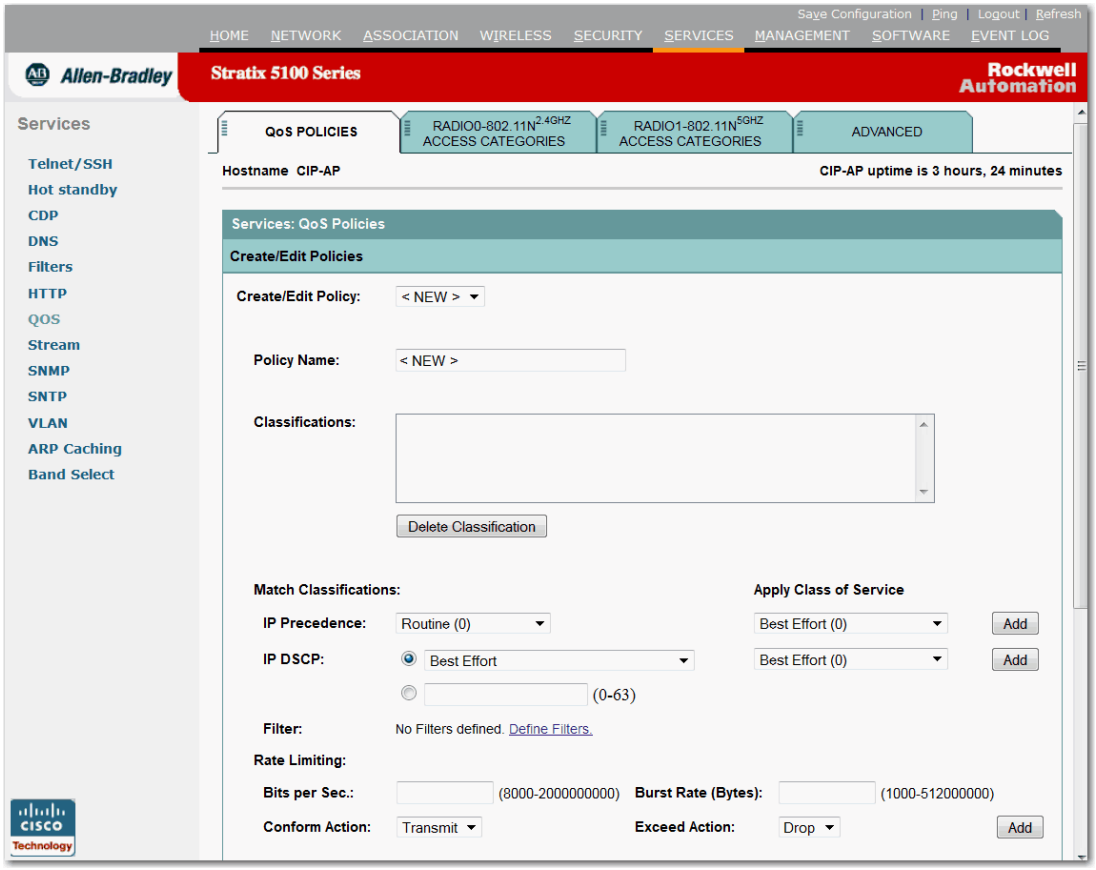


表 53 - QoS Policies (QoS 策略) 页面参数描述

参数	描述
Create/Edit Policies	如果输入新策略，确保在 Create/Edit Policy (创建 / 编辑策略) 菜单中选择 <NEW> (新) (默认值)。要编辑现有策略，选择 Create/Edit Policy (创建 / 编辑策略) 菜单中选择策略名称。当前的选择为 WMM 或 Spectralink，应将这两者之一填入 Policy Name (策略名称) 域中。
Policy Name	输入附加到输入或输出接口的策略名称。如果在 Create/Edit Policy (创建 / 编辑策略) 域中选择现有策略，将自动填入策略名称。
Classifications	类别是通过检查数据包中的域，区分各种通信的过程。将提供适合指定策略名称的类别。在帧或数据包中指定想要用于分类进入的通信的域。
Match Classifications	指定通信分类标准，例如， IP 优先级、 DSCP 和过滤器。

表 53 - QoS Policies (QoS 策略) 页面参数描述 (续)

参数	描述
IP Precedence	RFC791 中定义了八种 IP 优先级值。选择其中一种作为匹配标准。
IP DSCP	RFC2474 中定义的 IP DSCP (差分服务代码点)。选择 IP DSCP 值作为匹配标准。
IP Protocol 119	该协议用于匹配 SpectraLink 语音协议。
Apply Class of Services	确定服务类别，以便接入点将其应用于与 Filter (过滤器) 菜单中所选的过滤器相匹配的数据包。单击 Class of Service (服务类别) 旁边的 Add (添加)。
Filter	如果设置了过滤器，您可为数据包分配匹配所选过滤器的优先级。 从 Filter (过滤器) 下拉菜单中，选择想要包括在策略中的过滤器。例如，您可为包括 IP 电话 MAC 地址的 MAC 地址过滤器分配高优先级。 您可使用 Define Filters (定义过滤器) 链接跳转到 Services > Filters (服务 > 过滤器)，您可在此配置过滤器。 注意：QoS 中使用的访问列表不影响接入点的数据包转发决策。
Rate Limiting	位 / 秒：8000…2000000000 突发速率 (字节)：1000…512000000 确认操作：发送 超时操作：丢弃
Apply Policies to Interface/VLANs	在创建和应用 QoS 策略后，您可将策略分配给这两种接口的流入或流出的通信。
Incoming	使用下拉菜单选择为 GigabitEthernet 和 802.11 无线电接口流入的通信分配的策略。
Outgoing	使用下拉菜单选择为从 GigabitEthernet 和 802.11 无线电接口出站的通信分配的策略。

QoS：Radio (QoS：无线电) 页面

此页面允许您定义每种流量接入类别的载波侦听多路访问 (CSMA) 参数。这些参数影响不同服务类别的数据包交付方式。

请参见第 148 页的 “QoS Policies (QoS 策略) 页面 ”，确定您想要的服务等级。

由于会影响无线电特性，因此修改这些参数时务必小心。若要恢复到默认值，请参见第 53 页的 “ 将 WAP 复位到默认设置 ”。

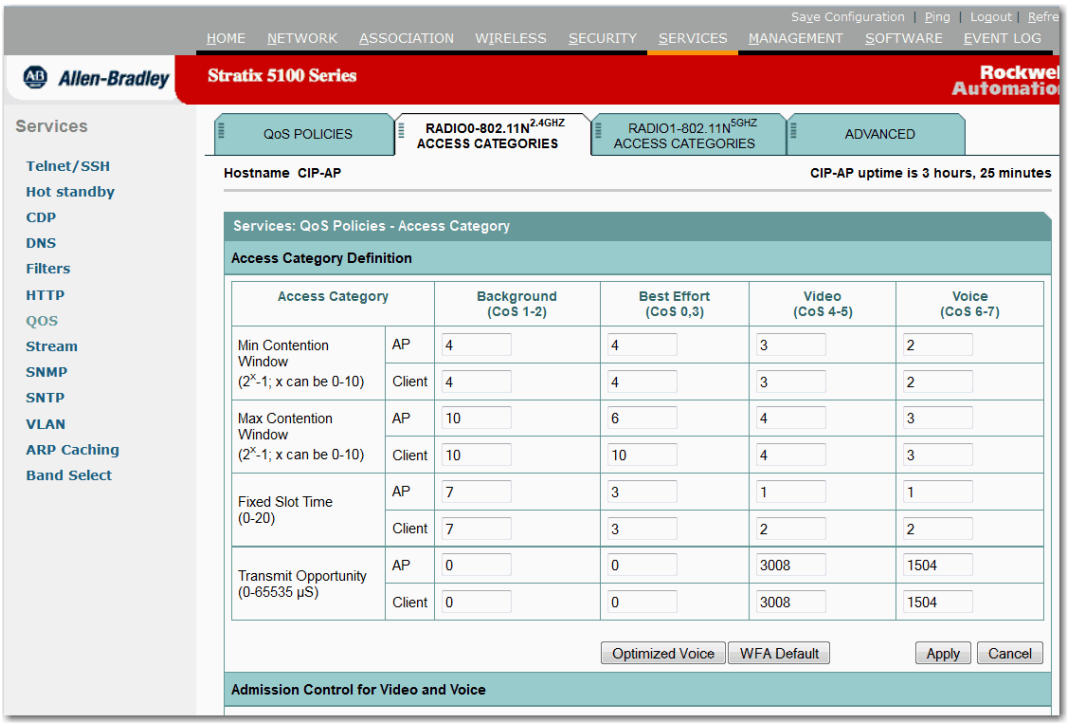


表 54 - Access Category Definition (访问类别定义) 页面参数描述

参数	描述
Min Contention	对于每个访问类别，输入最小争用窗口值。通道访问通过给高优先级通信类别分配较小的争用窗口值来排定优先级。如果通道忙碌或传输发生冲突，节点将在 0 至当前争用窗口最小值之间随机选择一个值。
Max Contention	对于每个访问类别，输入最大争用窗口值。每次发生冲突时，最小争用窗口值将翻倍，直到达到最大值。如果争用窗口值较小，可缩短访问延时，但会增大冲突可能性。
Fixed Slot Time	为每个访问类别输入固定时隙。通道访问通过给高优先级通信类别分配较小的固定时隙值来严格排定优先级。每次接收到数据包后，访问类别中的通信必须等待该固定时隙数，才会继续随机回退。

表 54 - Access Category Definition (访问类别定义) 页面参数描述 (续)

参数	描述
Transmit Opportunity	输入一段时间 (单位：微秒)，符合条件的发射器可在期间通过正常回退过程发送一组未决数据包。 较大的值可让客户端有更多的时间控制通道，使其在该访问类别实现更高的吞吐量，代价是所有访问类别的访问时间会延长。
Admission Control	Admission Control (接纳控制) 复选框控制客户端是否使用访问类别。当启用某个访问类别的接纳控制时，关联到接入点的视频和声音客户端必须完成 WMM 接纳控制过程后才能使用该访问类别。
Optimized Voice	如果单击该选项，将发生下列变化。 • Access Category Definition (访问类别定义) 的值经更改后可优化语音。 • 用户优先级 5 和 6 的数据包处理更改为低延时。 参见 Services (服务) > Stream (通信流) > Packet Handlings per User Priority (按照用户优先级处理数据包) • 在该无线电装置上启用无偿探测响应 (GPR)。 参见 Network Interfaces (网络接口) > Radio1-802.11A > Setting (设置)。
WFA Default	单击该按钮将以上各域恢复到默认值。
Admission Control for Video and Voice	视频 (CoS 4-5)：启用接纳控制 语音 (CoS 6-7)：启用接纳控制
Max Channel Capacity (%)	默认最大通道能力为 75%，范围为 0...100%。如果通道没有呼叫，可将该参数设为 0%。否则，确定占用通道的声音呼叫的百分比。
Roam Channel Capacity (%)	默认漫游通道能力为 6%，范围为 0...100%。确定呼叫可漫游到蜂窝或另一个蜂窝的通道的百分比。

图 74 - QOS Advanced (QOS 高级) 页面

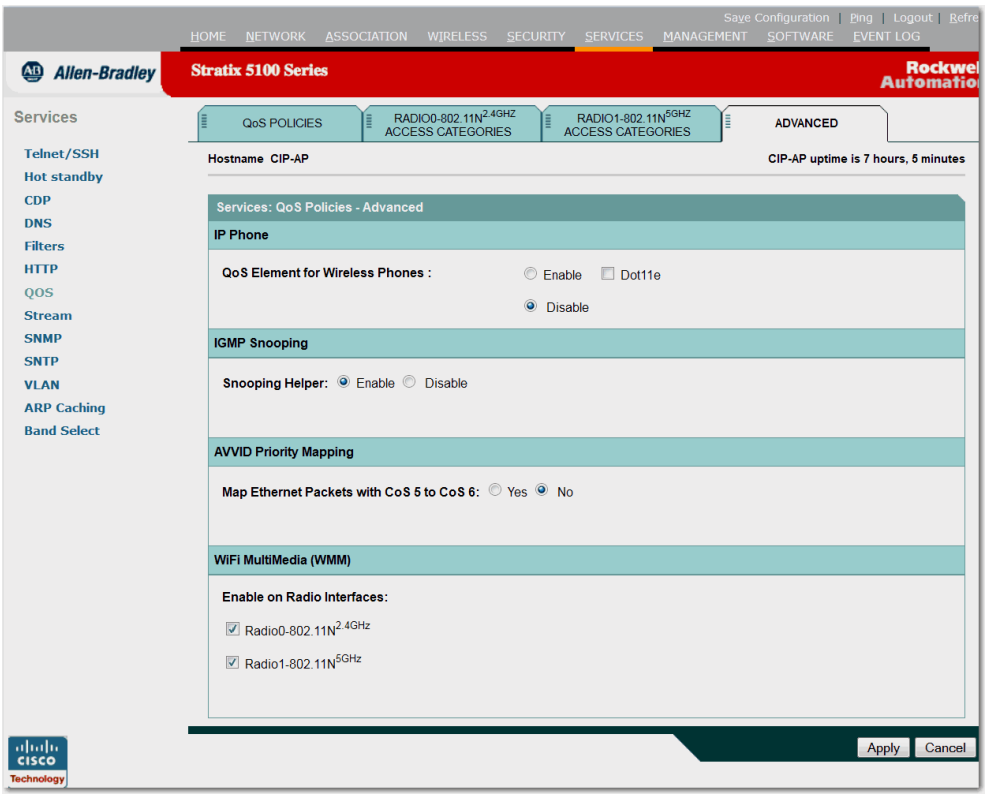


表 55 - QoS Policies Advanced (QoS 策略高级选项) 页面参数描述

参数	描述
IP Phone QoS Element for Wireless Phones	如果启用了该功能，将为一些无线电话供应商客户端提供动态语音分类符，为所有语音数据包提供最高优先级。此外，还将启用 QoS 基本服务集 (QBSS)，以推广信标和探测响应帧中的通道负载信息。一些 IP 电话使用 QBSS 元素根据通信负载确定要关联的接入点。
Dot11e	单击 Dot11e 使用最新版 QBSS 负载 IE。如果未单击 Dot11e，则将使用以前的 QBSS 负载 IE 版本。
IGMP Snooping Snooping Helper	当在交换机上启用了互联网组成员协议 (IGMP) 监听时，客户端从一个接入点漫游到另一个接入点时，客户端的多播会话将被丢弃。当启用了接入点的 IGMP 监听助手时，每次客户端关联或重新关联到接入点时，接入点将代表客户端向网络基础设施发送常规 IGMP 查询。如此，当客户端漫游时，多播流将得以维持。 监听助手默认为启用。要禁用，单击 Disable (禁用) 选项并单击 Apply (应用)。
AVVID Priority Mapping	将带 CoS 5 的以太网数据包映射到 CoS 6 如果网络基于思科 AVVID 规范，单击 Yes (是)。该映射操作将优先处理包括优先级 5 (视频) 的语音数据包。
WiFi MultiMedia (WMM)	在无线电接口上启用 Wi-Fi 多媒体 (WMM) 是 IEEE 802.11e 无线局域网标准关于服务质量 (QoS) 的一个组件。其专门支持优先级标签和排队。 当启用 QoS 时，接入点默认使用 WMM 模式。解除选中无线电接口复选框，以禁用特定无线电接口的 WMM。

Stream (通信流) 页面

Stream (通信流) 页面设置通信流服务的用户优先级，在页面中可增大或减少数据传输速率。

图 75 - Stream (通信流) 页面

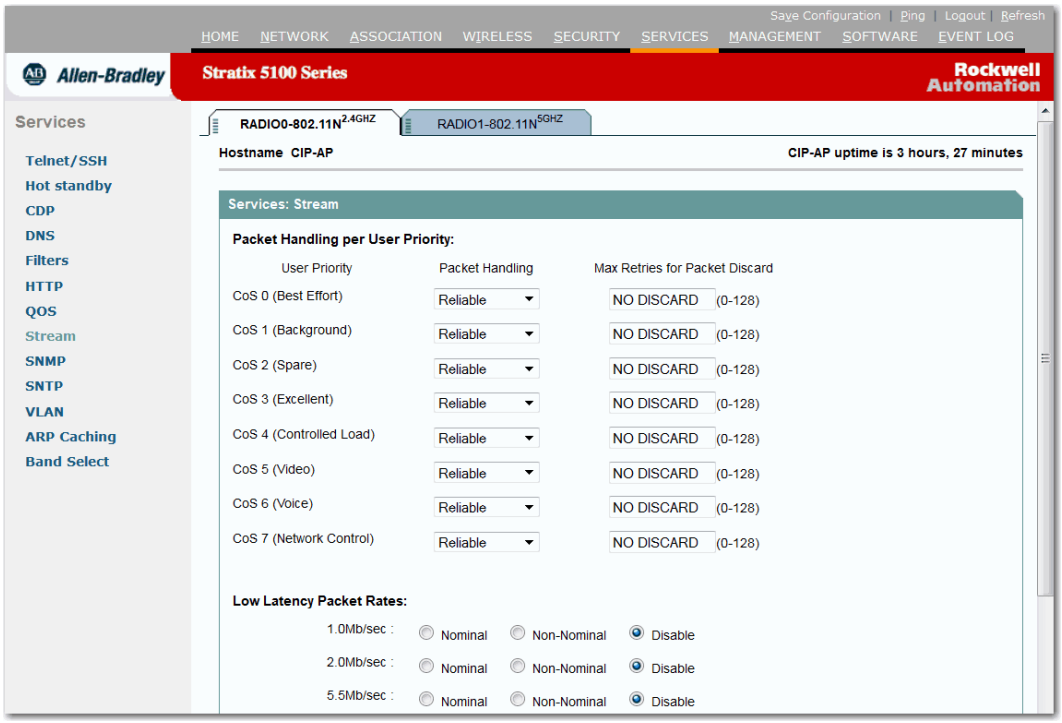


表 56 - Stream (通信流) 页面参数描述

参数	描述
Packet Handling per User Priority	选择用于通信流服务的用户优先级。对于所列的每种用户优先级，使用下拉菜单选择数据包处理描述符为 Reliable (可靠) 或 Low Latency (低延时)。然后确定丢弃数据包的最大重试次数。
Low Latency Packet Rates	低延时数据包速率通过减小数据传输速率增大覆盖范围，通过增大指定用户优先级的数据传输速率增强调用能力。

SNMP 页面

SNMP 是一种应用层协议，支持在 SNMP 管理工作站和代理之间进行面向消息的通信。该页面配置与网络管理员的简单网络管理协议 (SNMP) 工作站一起使用的接入点。

除了启用 SNMP 外，还必须输入一个 SNMP 社区。 SNMP 社区字符串的使用方法和用户名类似，它用于 SNMP 内部的验证、保密和授权服务。当在 Express Setup (快速设置) 页面上输入 SNMP 社区名称时，通过只读或读 / 写功能关联社区。

图 76 - SNMP 页面

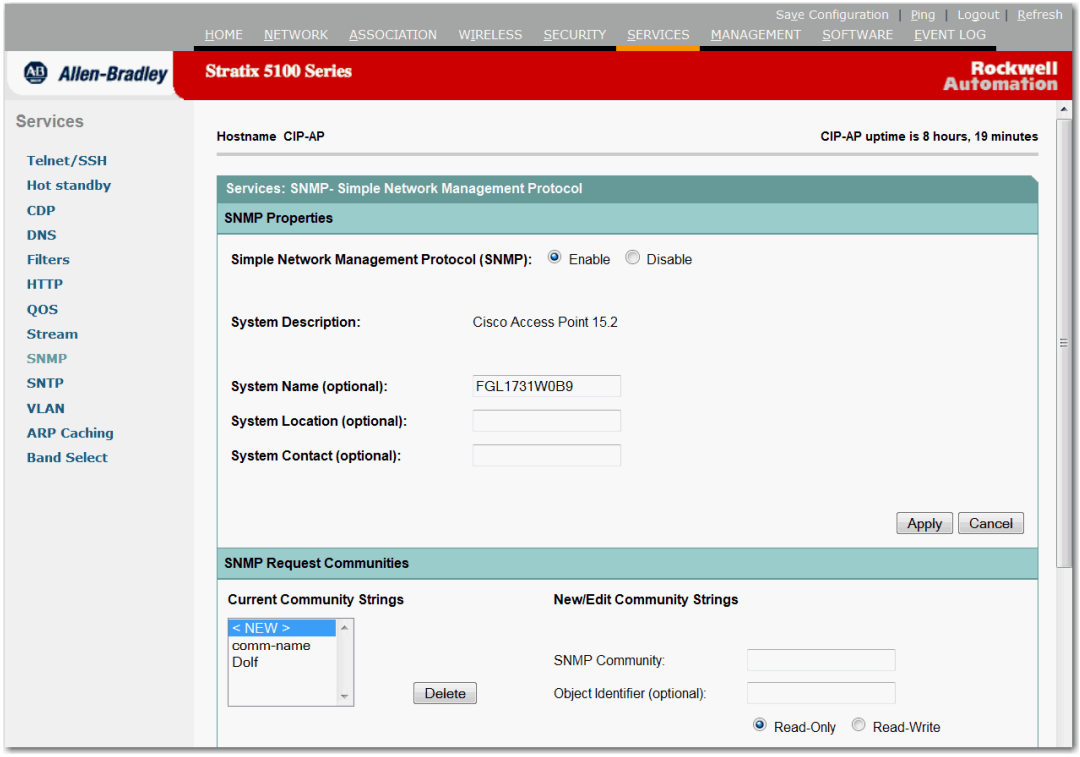


表 57 - SNMP 页面参数描述

参数	描述
Simple Network Management Protocol (SNMP)	要将 SNMP 用于设备，必须启用该设置。除了启用 SNMP 之外，还必须输入 SNMP 社区字符串。
System Description	在页面底部列出系统的设备类型和当前固件版本。
System Name (optional)	设备的名称。当使用 SNMP 与设备通信时，该域中的名称将作为设备名称被告给您的 SNMP 管理工作站。
System Location (optional)	设备物理位置，例如，建筑物名称或房间。
System Contact (optional)	设备系统管理员的姓名。

表 57 - SNMP 页面参数描述 (续)

参数	描述
SNMP Request Communities	该区域仅当在页面顶部的 Simple Network Management Protocol (SNMP) (简单网络管理协议) 域中选择了 Enabled (启用) 并单击 Apply (应用) 后才会启用。
Current Community String	如果要添加新的社区字符串，确保在列表中高亮显示 <NEW> (新) (默认值)。SNMP 社区字符串作为嵌入式密码，用于对访问 MIB 对象进行认证。将显示当前定义的社区字符串。您可高亮显示任何想要删除的字符串，然后单击 Delete (删除)。
New/Edit Community Strings	• SNMP 社区 当在 Current Community Strings (当前社区字符串) 列表中选择要编辑的社区字符串后，将显示该社区字符串的 SNMP 社区值。SNMP 社区字符串作为嵌入式密码，用于对访问 MIB 对象进行认证。 • 对象标识符 当在 Current Community Strings (当前社区字符串) 列表中选择要编辑的社区字符串后，将显示该社区字符串的对象标识符，或为社区字符串输入新的对象标识符。对象标识符为可选域，用于限制用户可通过社区字符串访问的 SNMP MIB 对象范围。
Read-only/Read-Write	Read-only (只读) 选项赋予授权的管理工作站对除社区字符串之外的所有对象的读权限，但没有写权限。Read/Write (读写) 选项赋予授权的管理工作站对所有对象的读写权限，但不允许访问社区字符串。

图 77 - SNMP Trap Community

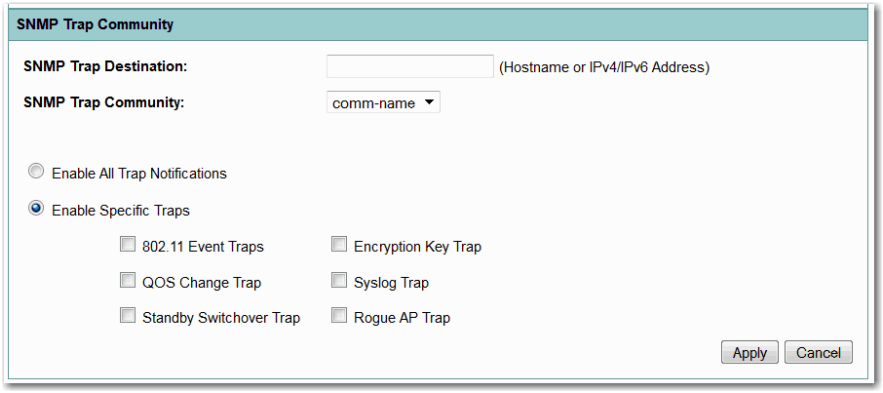


表 58 - SNMP 陷阱社区参数描述

参数	描述
SNMP Trap Community	该区域仅当在页面顶部的 Simple Network Management Protocol (SNMP) (简单网络管理协议) 域中选择了 Enabled (启用) 并单击 Apply (应用) 后才会启用。
SNMP Trap Destination	SNMP 管理工作站的 IP 地址。如果网络使用 DNS，输入解析为 IP 地址的主机名称。

表 58 - SNMP 陷阱社区参数描述 (续)

参数	描述
SNMP Trap Community	SNMP 社区字符串向陷阱目标标识发送方。在陷阱目标地址记录由设备发送的陷阱之前，它需要使用该字符串。
Enable All Trap Notifications	选择此选项启用接入点上可用的所有通知。
Enable Specific Traps	启用此选项指定要发送的通知。 • 802.11 Event Traps 启用客户端验证失败、客户解除验证和客户端解除关联的陷阱。 • Encryption Key Trap 启用关于 WEP 加密密钥设置更改的陷阱。 • QoS Change Trap 启用关于 8 个流量等级定义更改的陷阱。 • Syslog Trap 当发生某种严重性等级 (由事件日志配置页面创建) 的事件日志时启用陷阱发送。 • Standby Switchover Trap 当在待机模式下将接入点切换到活动模式时启用陷井发送。 • Rogue AP Trap 当无线电客户端报告非法接入点时启用陷井发送。

SNTP 页面

简单网络时间协议由网络时间协议 (NTP) 改编而来，用于同步因特网中的计算机时钟。在该页面上，可以配置 NTP 参数。

图 78 - SNTP 页面

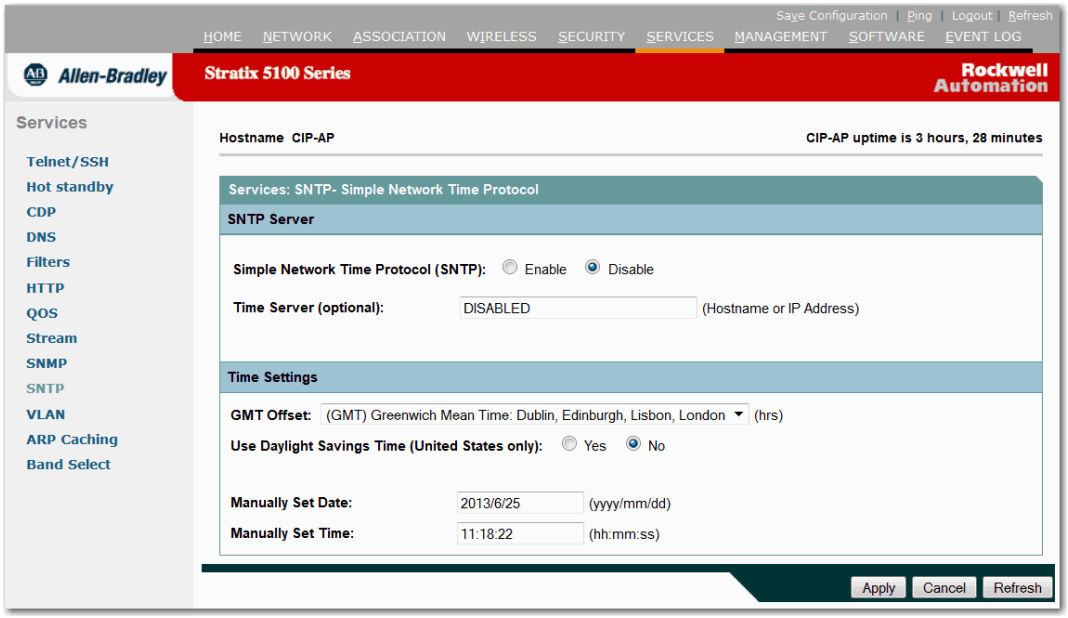


表 59 - SNTP 页面参数描述

参数	描述
Simple Network Time Protocol (SNTP)	如果网络使用 SNTP，选择 Enable (启用)。如果要关闭 SNTP，选择 Disable (禁用)。 当启用 SNTP 时，将显示 SNTP Status (SNTP 状态) 域。该域指示 SNTP 已同步还是未同步。单击 Refresh (刷新) 更新该状态。
Time Server (optional)	如果网络有默认的时间服务器，输入服务器的 IP 地址或主机名称。
Time Settings	• GMT 偏移量 GMT Offset (GMT 偏移量) 下拉菜单列出了相对于格林尼治标准时间 (GMT) 的世界时区。选择接入点所工作的时区。 • 使用夏令时 (仅限美国) 选择 Yes (是)，接入点将自动调节夏令时。 • 手动设置日期 输入当前日期，覆盖时间服务器的值，或没有可用的服务器时，设置日期。在输入日期时，使用斜杠分隔年、月、日。例如， 2001 年 2 月 17 日，可输入 2001/02/17。 • 手动设置时间 输入当前时间，覆盖时间服务器的值，或没有可用的服务器时，设置时间。在输入时间时，使用冒号分隔小时、分钟和秒钟。例如，您可输入 18:25:00，代表下午 6:25。

VLAN 页面

VLAN 是一种按功能、项目团队或应用进行逻辑分段的交换网络，而不是根据物理或地理位置来分段。例如，特定工作组团队使用的所有工作站和服务器都可连接到相同的 VLAN，不管它们以何种物理连接方式连接到网络，或者它们是否可与其他团队组合。您可以使用软件来重新配置网络，而无需以物理的方式拔下和移动设备或导线。

可将 VLAN 视为存在于定义的交换机组内的广播域。 VLAN 由通过一个桥接域连接的多个终端系统 (主机或网络设备 (如网桥和路由器) 组成。在各网络设备段上支持桥接域；例如，在各段之间运行桥接协议的局域网交换机，其中，每个 VLAN 都有一个独立的组。

VLAN 的基本无线组件包括一个接入点和一个通过无线技术与之关联的客户端。从根本上而言，配置接入点连接到特定 VLAN 的关键是通过配置其 SSID 识别该 VLAN。由于 VLAN 通过 VLAN ID 进行标识，因此，当接入点上的 SSID 配置为识别特定 VLAN ID 后，建立到此 VLAN 的连接。完成此连接后，具有相同 SSID 的关联无线客户端设备可以通过接入点访问 VLAN。 VLAN 处理与客户端之间往来数据的方式与其处理有线连接往来数据的方式相同。

图 79 - VLAN 页面

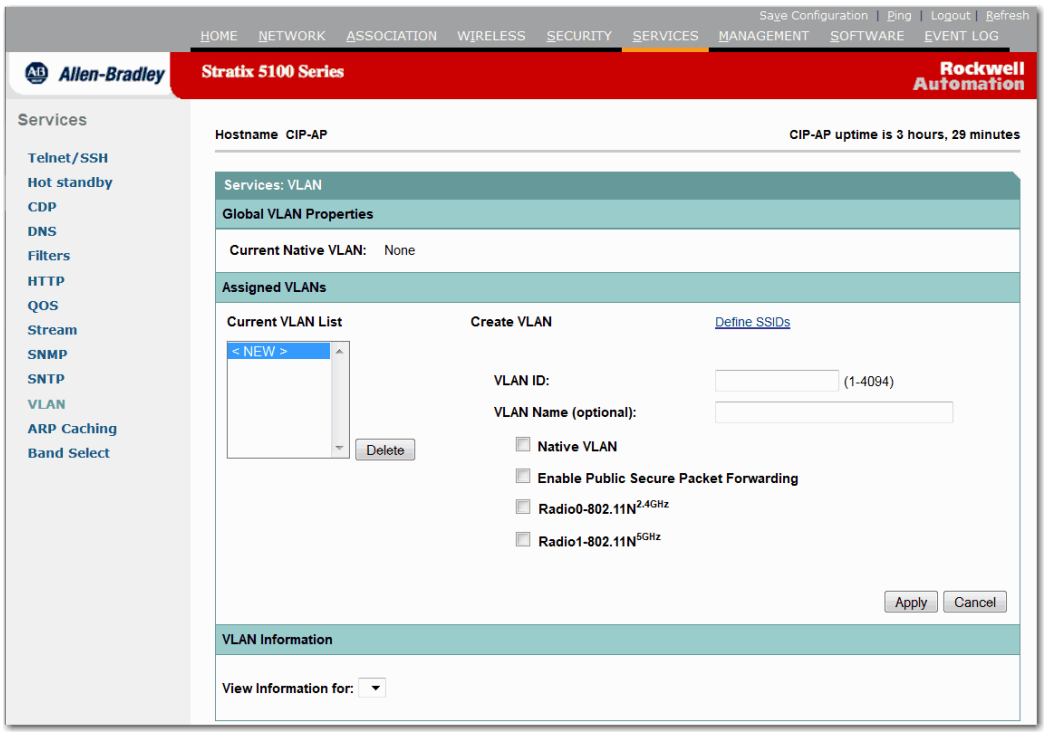


表 60 - VLAN 页面参数描述

参数	描述
Global VLAN Properties	Current Native VLAN (当前的本征 VLAN) 指定作为本征 VLAN 的 VLAN。选中 VLAN ID 域下方的复选框。
Assigned VLANs	当前 VLAN 列表 从该列表中选择 VLAN，将显示该 VLAN 的 VLAN ID 和 SSID。您可单击 Delete (删除) 删除 VLAN，或单击 Define SSIDs (定义 SSID) 跳转到 SSID Manager (SSID 管理器) 页面。
Create VLAN	如果要添加 VLAN，可使用该区域创建 VLAN 并为其分配 SSID。
VLAN ID	指定与 SSID 绑定的虚拟以太网局域网识别号。除了数字 ID 之外，您还可为 VLAN 分配一个名称。
VLAN Name (optional)	除了数字 ID 之外，您还可为 VLAN 分配一个名称。VLAN 名称最多可包含 32 个 ASCII 字符。接入点将使用表格保存各 VLAN 名称和 ID 对。
Native VLAN	802.1q 干线交换机端口上的无标签 VLAN。
Public Secure Packet Forwarding	公共安全数据包转发可阻止关联到相同 AP 的客户端之间进行通信。
Radio0-802.11N 2.4 GHz	在 2.4 GHz 无线接口上启用 VLAN。
Radio1-802.11N 5 GHz	在 5 GHz 无线接口上启用 VLAN。
VLAN Information	使用下拉菜单显示已创建的 VLAN 列表。高亮显示列表中的 VLAN 后，可查看已接收以太网数据包、已发送以太网数据包、已接收无线数据包和已发送无线数据包的值。

ARP Caching (ARP 缓存) 页面

接入点上的 ARP 缓存通过停止接入点处客户端设备的 ARP 请求减少无线局域网的流量。除了将 ARP 请求转发至客户端设备外，接入点代表关联客户端设备响应请求。

当禁用 ARP 缓存时，接入点通过无线电端口将所有 ARP 请求转发至关联客户端，然后由 ARP 请求指向的目标客户端进行响应。当启用 ARP 缓存时，接入点响应关联客户端 的 ARP 请求，不将请求转发至客户端。当接入点收到不在缓存中的 IP 地址的 ARP 请求时，接入点将丢弃该请求，而不转发请求。

图 80 - ARP Caching (ARP 缓存) 页面

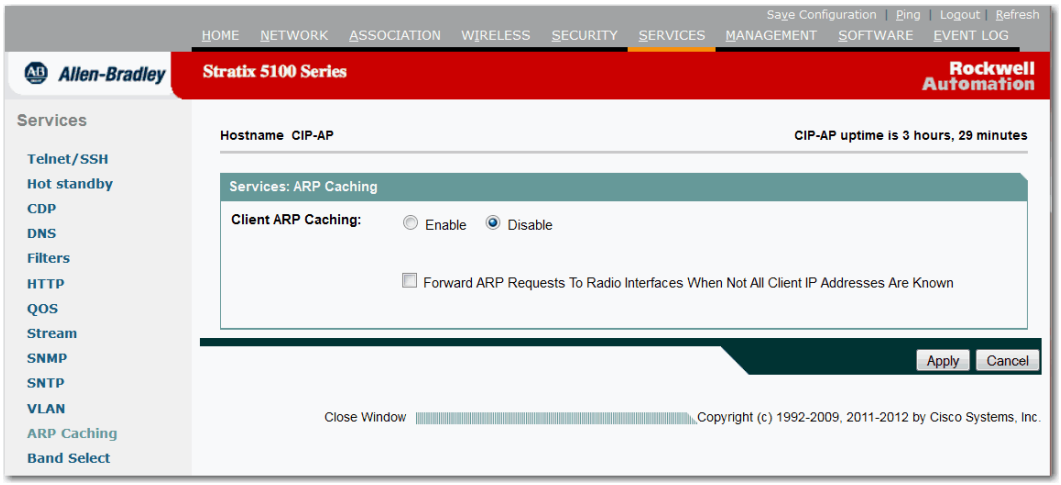


表 61 - ARP Caching (ARP 缓存) 页面参数描述

参数	描述
Client ARP Caching	单击相应的单选按钮启用或禁用客户端 ARP 缓存。
Forward ARP Requests to Radio Interfaces When Not All Client IP Addresses Are Known	当非思科客户端设备关联到接入点且不传送数据时，接入点将无法知晓客户端 IP 地址。如果您的无线局域网中经常出现这种情况，您可选中该复选框。在这种情况下，接入点代表已知 IP 地址的客户端进行响应，但对于指向未知客户端的任何 ARP 请求，将通过其无线电端口进行转发。当接入点知道所有关联客户端的 IP 地址时，它将丢弃不是指向其关联客户端的 ARP 请求。

Band Select (频段选择) 页面

频段选择允许将可执行双频段 (2.4 和 5 GHz) 操作的客户端无线电设备转移到接入点上较不拥塞的 5 GHz 无线频段。2.4 GHz 频段通常拥塞。由于三个非重叠通道的 802.11b/g 限制，该频段上的客户端通常会受到来自蓝牙设备、微波炉和无绳电话的干扰以及其他接入点的共用通道干扰。为了对抗这些干扰源并提高整个网络的性能，您可配置接入点上的频段选择。

频段选择的原理是调节对客户端的嗅探响应。它通过延迟 2.4 GHz 通道上客户端的嗅探响应，使客户端更倾向于使用 5 GHz 通道。

您可全局或针对某个特定的 SSID 启用频段选择。当您希望对某个选定的客户端组 (例如，时间敏感型语音客户端) 禁用该功能时，这非常有用。

重要事项 只能由具有资质的网络工程师修改这些设置。

图 81 - Band Select (频段选择) 页面

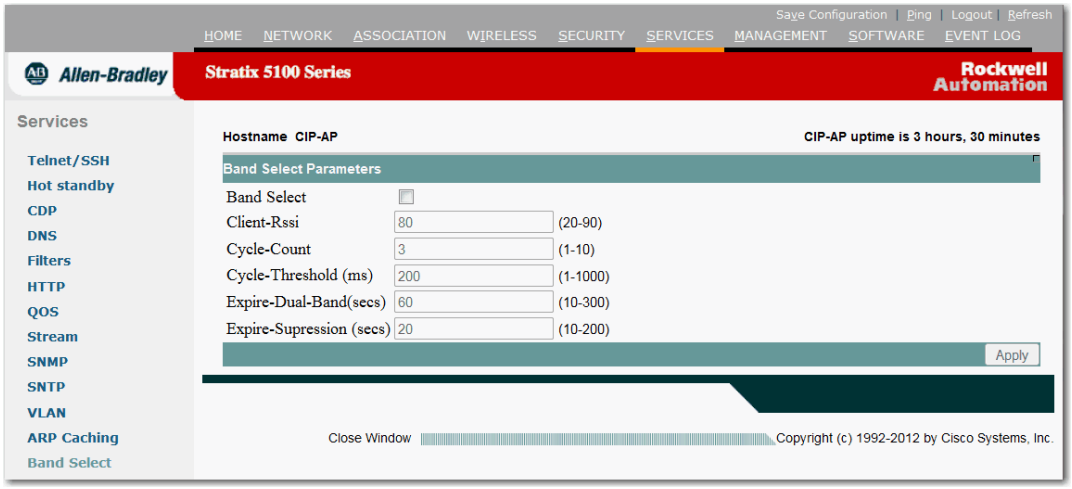


表 62 - Band Select (频带选择) 页面参数描述

参数	描述
Band Select	启用 / 禁用
Client-Rssi	20…90 RSSI 是接收信号强度指标。它显示无线客户端的信号强度 (dBm)。
Cycle-Count	1…10 循环计数用于设置新客户端的抑制循环数。默认循环计数为 2

表 62 - Band Select (频带选择) 页面参数描述 (续)

参数	描述
Cycle-Threshold	1…1000 ms
Expire-Dual-Band	10…300 s 设置用于消除之前已知的双频带客户端的到期时间。默认值为 60 秒。在此时间之后，客户端将变为新的客户端，并受到探测响应抑制。
Expire-Suppression	10…2000 s 设置用于消除之前已知的 802.11b/g 客户端的到期时间。默认值为 20 秒。在此时间之后，客户端将变为新的客户端，并受到探测响应抑制。

Management (管理) 页面

在 Management (管理) 页面中，您可管理来宾用户帐户。在该页面上，企业可通过创建一个 Web 验证页面创建来宾无线用户访问。

例如，如果用户希望登录允许来宾访问的网络，则用户将导览至一个带有 Wi-Fi 使用条款和条件声明的网页。一旦来宾接受条款并输入密码 (如有必要)，他们即可访问网络。

图 82 - Management (管理) 页面

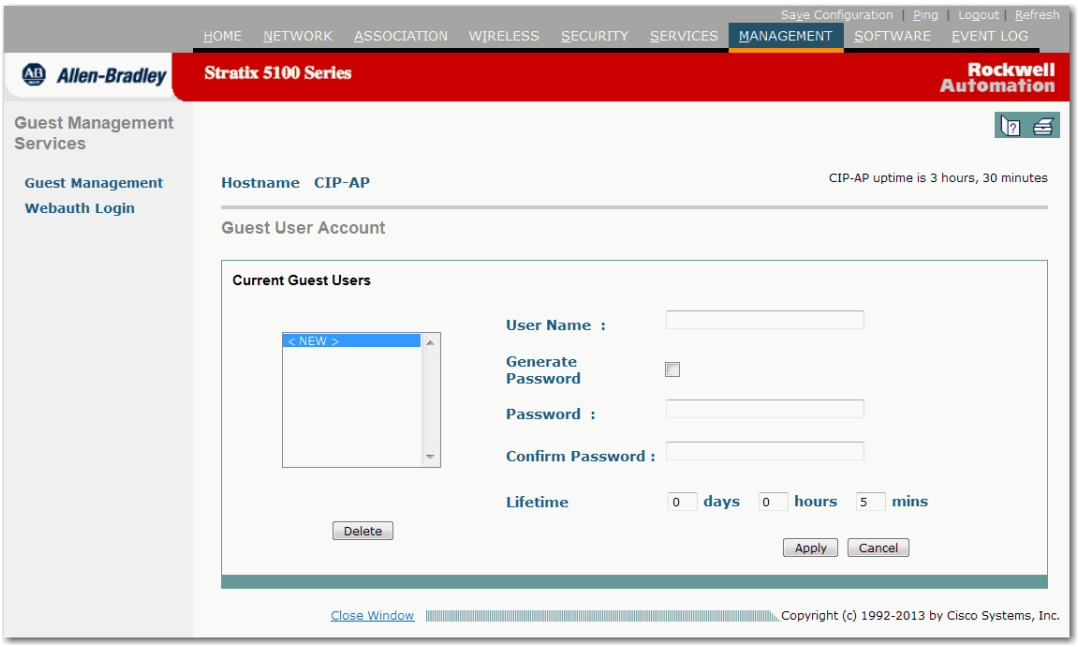


表 63 - Management (管理) 页面参数描述

参数	描述
Current Guest Users	当前访客用户
User Name	用户名
Generate Password	生成密码
Password	密码
Confirm Password	确认密码
Lifetime	日 / 小时 / 分钟

Webauth 登录

该页面可以自定义 Login (登录) 页面的外观。如果在 SSID 上开启了 “Web Authentication”(Web 验证)，当 Web 用户第一次访问无线网络时，将呈现 Login (登录) 页面。

图 83 - Webauth 登录页面

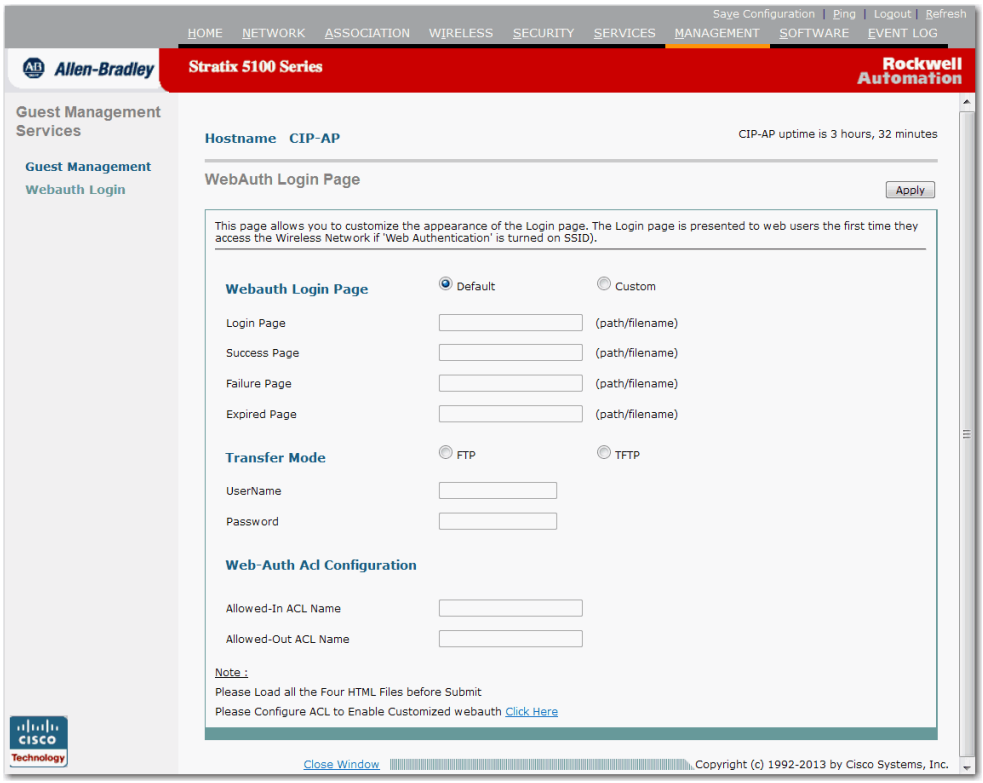


表 64 - Webauth Login (Webauth 登录) 页面参数描述

参数	描述
Webauth Login Page	登录页面 成功页面 失败页面 过期页面
Transfer Mode	FTP TFTP Username Password
Web-Auth ACL Configuration	准入 ACL 名称 准出 ACL 名称

Software (软件) 页面

Software (软件) 页面提供了思科 IOS 软件的版本信息。

图 84 - Software (软件) 页面

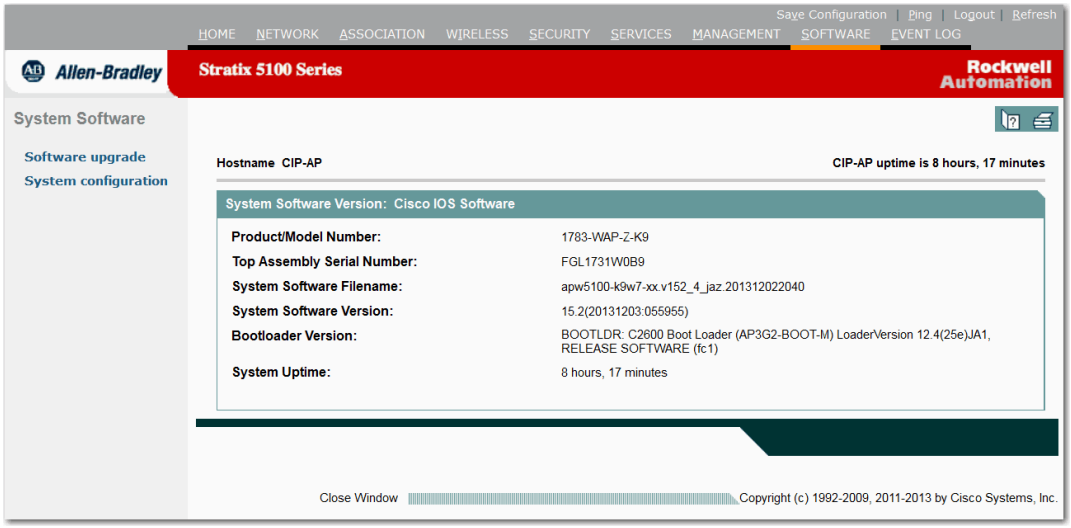


表 65 - Software (软件) 页面参数描述

参数	描述
Product/Model Number	接入点的型号。
Top Assembly Serial Number	接入点的序列号。
System Software Filename	系统上安装的软件文件。
System Software Version	接入点上运行的思科 IOS 软件的版本。
Bootloader Version	安装的引导加载程序的版本。系统映像更改时，引导加载程序并不更改。
System Uptime	接入点上电的日数、小时数和分钟数。

Software Upgrade HTTP (软件升级 HTTP) 页面

HTTP 升级需要将映像加载到接入点存储器。如果没有足够的系统内存执行 HTTP 升级，将导致升级失败。如果升级失败，在禁用无线电接口、关闭高内存使用率功能 (如 WDS) 并重启系统后，尝试使用 TFTP 升级或重新执行 HTTP 升级。

图 85 - Software Upgrade HTTP (软件升级 HTTP) 页面

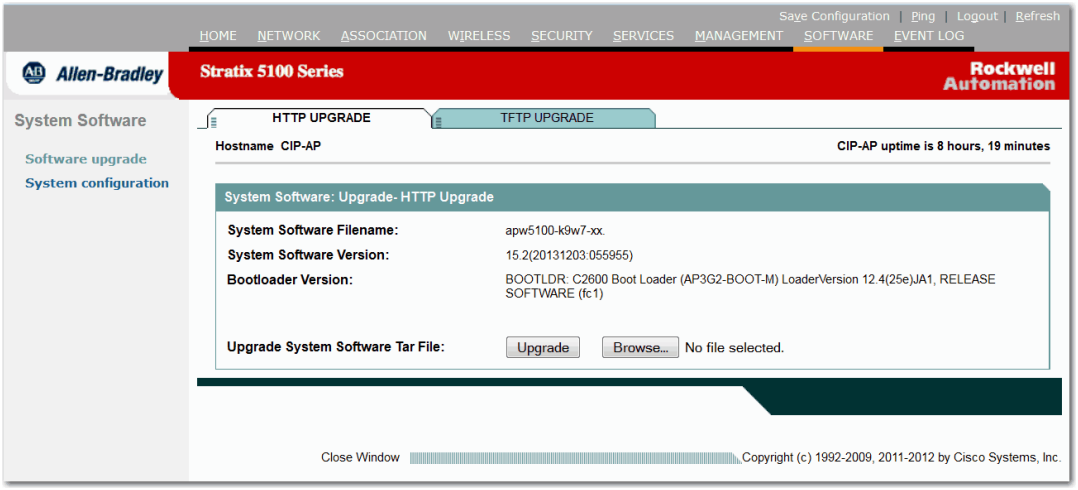


表 66 - Software HTTP Upgrade (软件 HTTP 升级) 页面参数描述

参数	描述
System Software Filename	系统上安装的软件文件。
System Software Version	接入点上运行的思科 IOS 软件的版本。
Bootloader Version	安装的引导加载程序的版本。系统映像更改时，引导加载程序并不更改。
Upgrade System Software Tar File	要安装新版思科 IOS 软件，按以下步骤操作。 1. 插入新系统软件 tar 文件正确的路径和文件名。 2. 跳转到 Cisco.com 并下载适合本地驱动器的最新系统软件版本。 3. 单击 Browse (浏览)，找到新系统软件文件。 4. 单击 Upgrade (升级) 将文件复制到接入点。 升级可能需要几分钟，并可能导致接入点重启。

Software Upgrade TFTP (软件升级 TFTP) 页面

使用 Software Upgrade TFTP (软件升级 TFTP) 页面通过 TFTP 服务器升级无线 AP。 (您需要提供 TFTP 服务器) 这允许 WAP 连接至用户提供的 TFTP 服务器，并下载软件的新版本，然后升级。

您需要输入 TFTP 的 IP 地址或 DNS 名称，然后输入要安装软件升级版本的路径 / 文件名。

图 86 - Software Upgrade TFTP (软件升级 TFTP) 页面

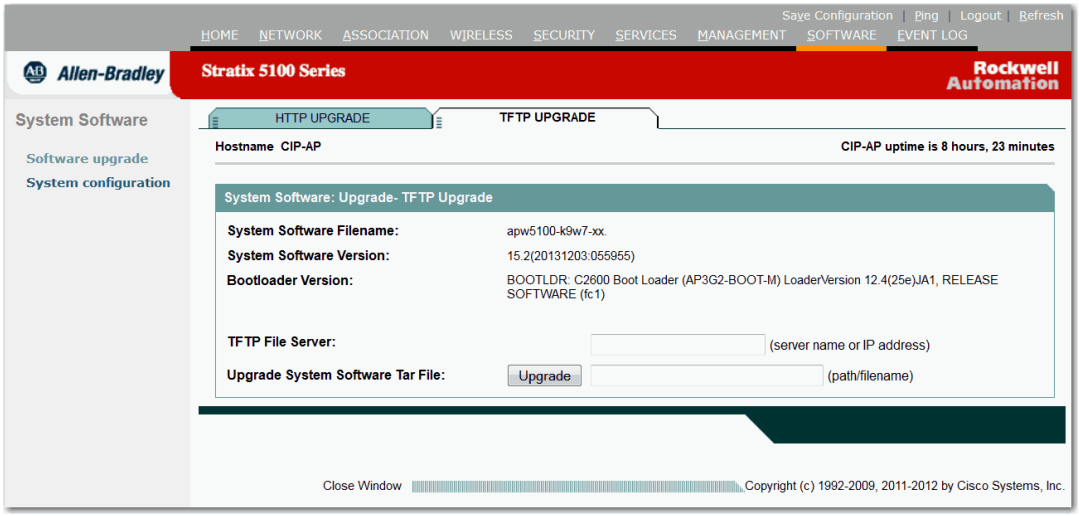


表 67 - TFTP 升级参数描述

参数	描述
System Software Filename	系统上安装的软件文件。
System Software Version	接入点上运行的思科 IOS 软件的版本。
Bootloader Version	安装的引导加载程序的版本。系统映像更改时，引导加载程序并不更改。
TFTP File Server	这是 TFTP 服务器的 IP 地址。 TFTP 是提供文件的服务器。
Upgrade System Software Tar File	要安装新版思科 IOS 软件，按以下说明操作。 1. 插入新系统软件 tar 文件正确的路径和文件名。 2. 跳转到 Cisco.com 并下载适合本地驱动器的最新系统软件版本。 3. 单击 Browse (浏览)，找到新系统软件文件。 4. 单击 Upgrade (升级) 将文件复制到接入点。 升级可能需要几分钟，并可能导致接入点重启。

System Configuration (系统配置) 页面

在此页面中可以找到系统配置信息。在该页面上，可以加载新的配置文件、拉取显示技术信息、复位设备以及调整 PoE 设置。

图 87 - System Configuration (系统配置) 页面

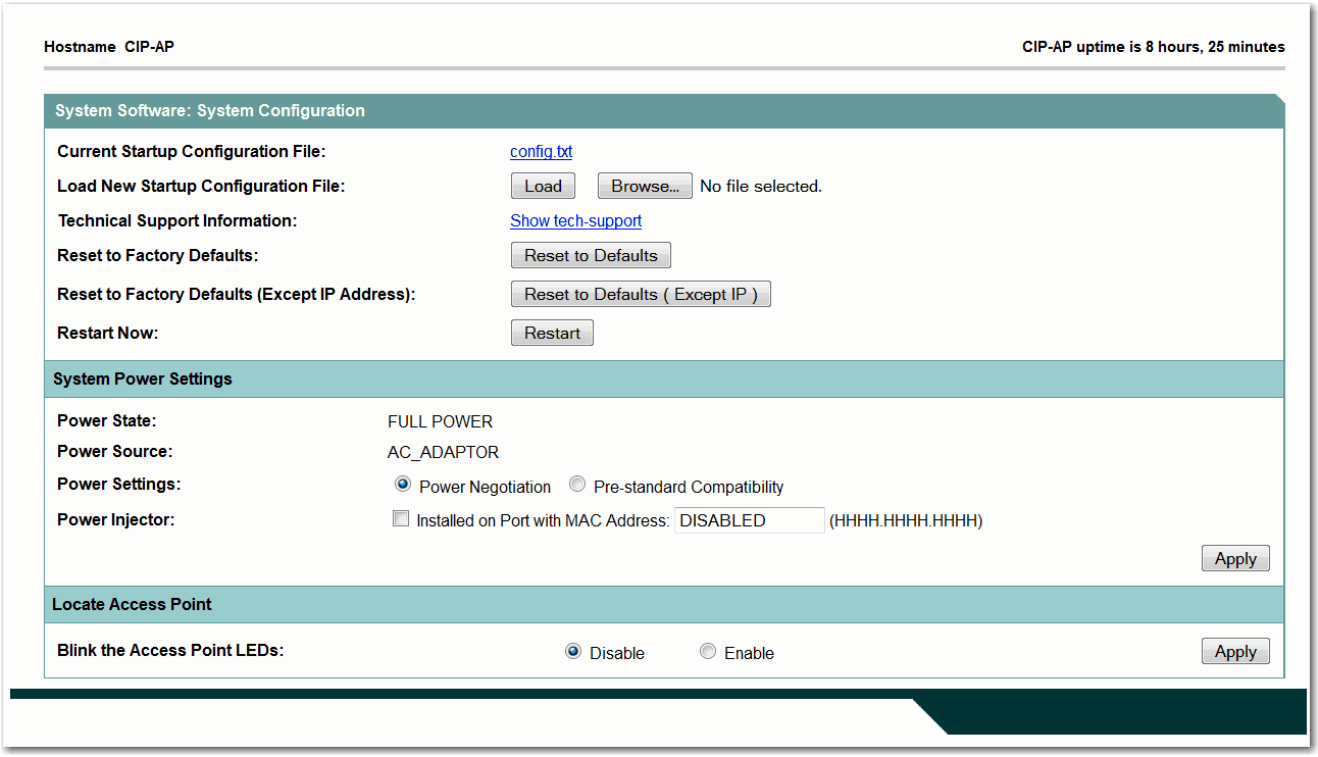


表 68 - 软件系统配置参数描述

参数	描述
Current Startup Configuration File	右击该链接，将 config.txt 文件保存到本地硬盘驱动器。随后您便可根据自己的需要编辑文件和配置接入点。 使用 Load New Startup Configuration File (加载新启动配置文件) 功能将新文件上传到要使用相同配置的接入点。
Load New Startup Configuration File	浏览到使用 Current Startup Configuration File (当前的启动配置文件) 功能保存 config.txt 文件的位置。 单击 Load (加载) 将新文件上传到要使用相同配置的接入点。当新配置加载后，接入点将重启。
Technical Support Information	show-tech 命令能够提供大量系统信息，对于确定产品故障原因很有帮助。您的技术支持员工对设备进行故障处理将需要这些信息。 右击该链接，将技术支持信息保存到本地硬盘驱动器。随后您便可将这些信息通过电子邮件发送给技术支持员工，以帮助他们配置您的接入点。
Reset to Factory Defaults	将所有接入点设置恢复到出厂默认值。 IP 地址将被设为 DHCP。 单击 Reset to Defaults (恢复到默认值) 将导致接入点重启。接入点的默认密码为 wirelessap。

表 68 - 软件系统配置参数描述 (续)

参数	描述
Reset to Factory Defaults (Except IP Address)	将所有接入点设置恢复到默认值，但固定 IP 地址保持其配置设置不变。 单击 Reset to Defaults (Except IP) (恢复到默认值 (IP 地址除外)) 将导致接入点重启。接入点的默认密码为 wirelessap。
Restart Now	单击 Restart (重启) 重启系统，无需查找和拔下接入点。 只有在从断电或雷暴导致的网络问题恢复后，才需要重启冷引导。
System Power Settings	支持思科智能电源管理的接入点提供该功能。一些接入点支持低电量模式，以防止旧供电设备 (PSE) 上出现过载状况。
Table	确认电源和交换机状态，并确保设备已配置。
Power State	显示接入点的电源模式。警告状态指示 PSE 无法提供足够的电源，或馈电器未正确配置。 关于如何纠正该问题的说明，请参见 " 系统电源设置 "。
Power Source	显示接入点检测到的电源。
Power Settings	选择 Power Negotiation (电源协商) 或 Pre-standard Compatibility (预置标准兼容性)。使用电源协商设置，让设备与支持思科智能电源管理的 PSE 协商内部电源，或在使用思科 Aironet 馈电器时进行协商。 如果使用非思科交换机，则无需更改电源设置。
Power Injector	当在不支持思科智能电源管理的思科 PSE 之前连接了馈电器，则必须选中 Installed on Port with MAC Address (安装在以下 MAC 地址的端口上) 复选框。确保交换机端口的 MAC 地址显示在 MAC address (MAC 地址) 域中。如果思科交换机支持智能电源管理协商，则取消选中 Installed on Port with MAC Address (安装在以下 MAC 地址的端口上)。
Locate Access Point	使接入点状态指示灯闪烁。 单击 Enable (启用)，让接入点上的状态指示灯闪烁，以便找到特定的设备。

Event Log (事件日志) 页面

在该页面上可以查看事件日志。在 CLI 中，该命令显示正在登录。

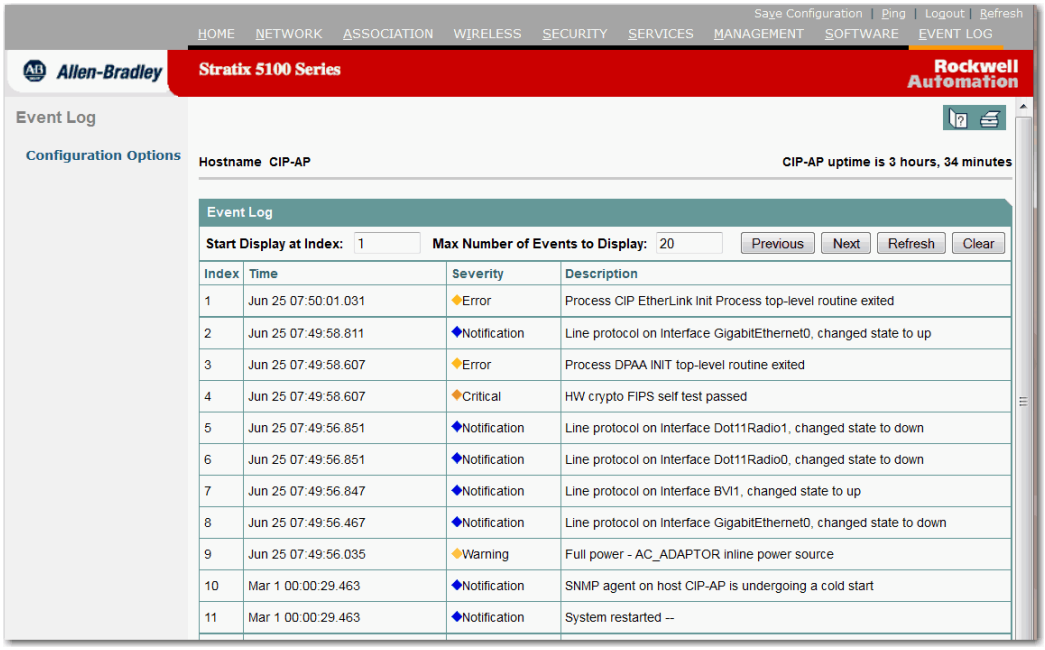


表 69 - Event Log (事件日志) 页面参数描述

参数	描述
Start Display at Index	输入要从哪条事件开始查看事件日志。
Max Number of Events to Display	输入想要在事件日志中显示的事件数量。
Index	事件在事件日志中从旧到新的顺序号。

表 69 - Event Log (事件日志) 页面参数描述 (续)

参数	描述
Time	显示连同事件一起记录的时间戳。显示格式可在 Event Log: Configuration Options (事件日志：配置选项) 页面中选择。时间戳显示格式取决于事件发生时所选择的时间戳格式。支持三种时间戳格式。 • 系统运行时间 事件发生时系统的运行时长。时长最开始以秒数显示，然后逐渐增加到分、日和周。例如， 1w0d 表示一周零天。 • 全球标准时间 事件发生时的 UTC 时间。该时间以 Month dd hh:mm:ss.usec 加三字母时区 (UTC) 格式记录。要确保时间戳正常工作，必须设置系统时钟。 • 当地时间 事件发生时当地时区的时间。该时间以 Month dd hh:mm:ss:usec 加三字母时区格式记录。要确保时间戳正常工作，必须设置系统时钟。
Severity	下表列出了事件的严重性。 **严重性** / **描述** 紧急 (严重性等级 0) / 系统不可使用。 警报 (严重性等级 1) / 需要立即执行操作。 严重 (严重性等级 2) / 当前状况严重。 错误 (严重性等级 3) / 记录到错误状况。 警告 (严重性等级 4) / 警告消息指示潜在的错误状况。 通知 (严重性等级 5) / 仍可正常操作，但可能导致严重状况。 信息 (严重性等级 6) / 信息消息提供正常活动的例行信息，不指示错误。 调试 (严重性等级 7) / 提供调试消息。
Description	错误事件的描述。 显示在接入点事件日志中的无线 MAC 地址。当客户端从一个接入点 (例如，接入点 A) 漫游到另一个接入点 (接入点 B) 时，将在接入点 A 的事件日志中显示一条消息，声明客户端已漫游到接入点 B。事件消息中显示的 MAC 地址是接入点 B 无线电装置的 MAC 地址，而不是接入点 B 的以太网端口的 MAC 地址。

有关该错误消息的更多信息，请参见第 531 页的 “ 错误和事件消息 ”。

Configuration Options (配置选项) 页面

这些设置允许您确定所记录的不同事件的通知方式以及要发生的记录级别。

图 88 - Configuration Options (配置选项) 页面

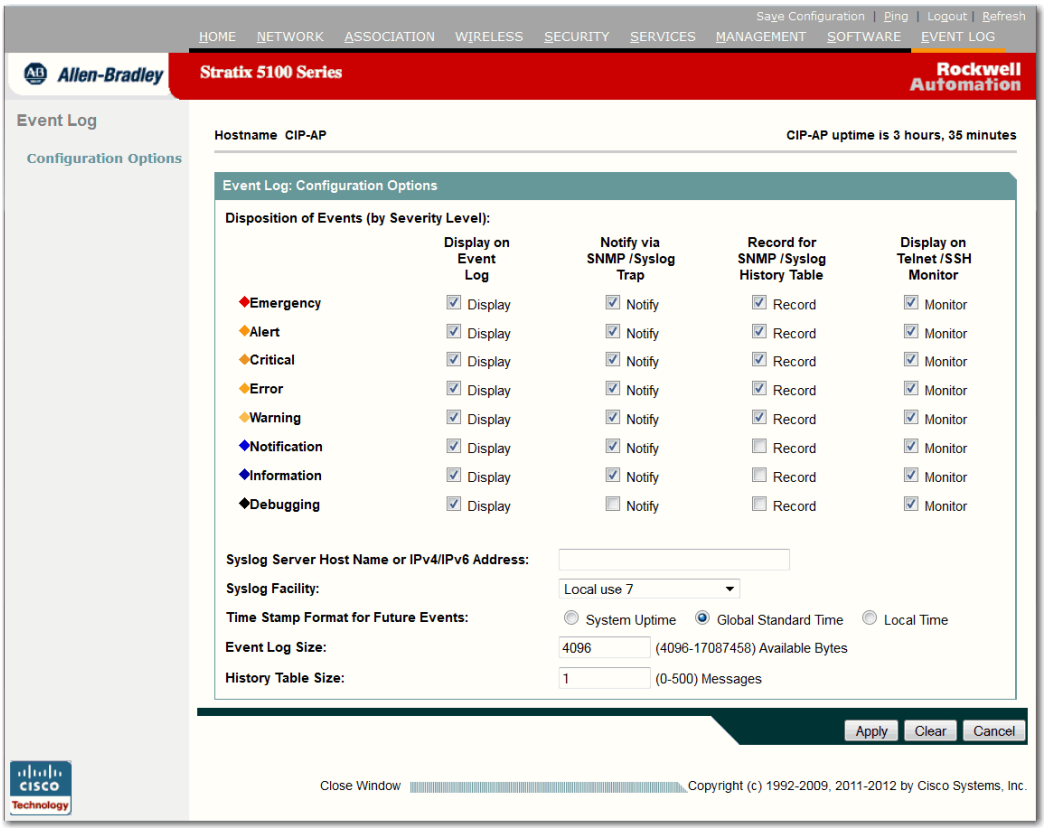


表 70 - 事件日志配置参数描述

参数	描述
Disposition of Events (by Severity Level)	当选择一个严重性等级时，也将选择所有更高优先级的严重性等级。
Display on Event Log	确定各种严重性等级下的事件是否要显示在事件日志中，要显示的在复选框中打上复选标记。事件日志中显示的事件将出现在事件日志页面。
Notify via SNMP/Syslog Trap	确定各种严重性等级下的事件发生时，是否要通过 SNMP/Syslog 陷阱通知。如果要通知，在复选框中打上复选标记。
Record for SNMP/Syslog History Table	确定各种严重性等级事件是否要记录到 SNMP/Syslog 历史表中。如果要记录事件，在复选框中打上复选标记。
Display on Telnet/SSH Monitor	确定各种严重性等级事件是否要显示在 Telnet/SSH 监视器上。如果要在监视器上显示事件，在复选框中打上复选标记。

表 70 - 事件日志配置参数描述 (续)

参数	描述
Time Stamp Format for Future Events	选择保存事件时间戳信息使用的时间格式。支持三种时间戳格式，如下所述。 • 系统运行时间 事件发生时系统的运行时长。该时间最开始以秒数显示，然后逐渐增加到分数、日数和周数。例如， 1w0d 表示一周零天。 • 全球标准时间 事件发生的 UTC 时间以 Month dd hh:mm:ss.usec 加 3 字母时区 (UTC) 格式记录。要确保时间戳正常工作，必须设置系统时钟。 • 当地时间 事件发生的当地时间以 Month dd hh:mm:ss.usec 加 3 字母时区格式记录。要确保时间戳正常工作，必须设置系统时钟。
Event Log Size	确定创建用于记录命令的缓冲区大小。分配给日志的内存越大，可供交换机数据包使用的内存就越小。
History Table Size	确定接入点历史表中最多可保存的 syslog 消息数量。

备注：

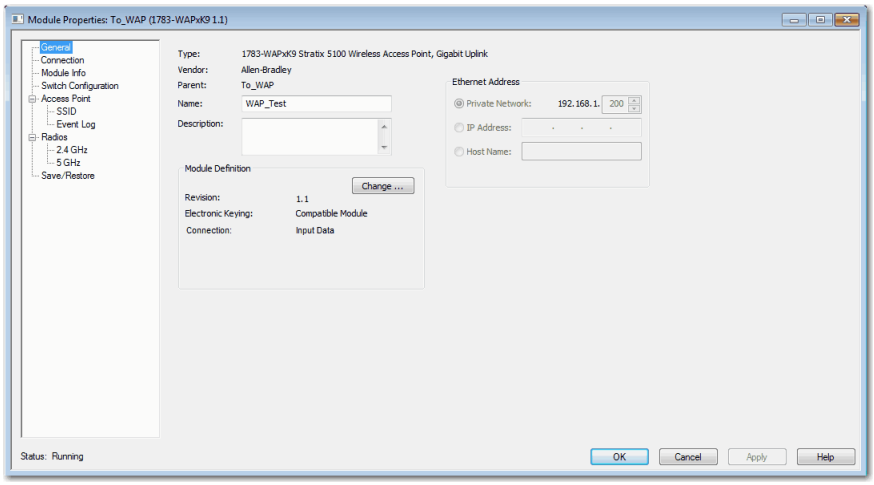
访问 Logix Designer 中的 Stratix 5100 无线接入点 / 工作组网桥

本章提供有关基本接入点 / 工作组网桥参数的信息，您可通过这些参数在 Logix Designer 中配置和查阅状态信息。

General (常规) 对话框

General (常规) 对话框提供各种信息，如名称、以太网地址和版本。

图 89 - General (常规) 对话框



General (常规) 对话框包含以下参数。

表 71 - 常规参数描述

参数	描述
Type	显示正在创建模块的类型和描述 (只读)。
Vendor	显示正在创建模块的供应商 (只读)。
Parent	显示父模块的名称 (只读)。如果模块位于本地机架，则显示 “Local”(本地)。
Name	输入模块的名称。 名称必须符合 IEC 1131-3 标准。这是必填域，因此必须填写；否则，在退出该对话框时会收到错误消息。 如果检测到名称重复或输入的字符无效，会显示错误消息。如果超过软件允许的最大名称长度，额外字符将被忽略。
Description	输入关于模块的描述，最多 128 个字符。请在该域使用任何可打印字符。如果超出字符最大长度，软件将忽略任何额外字符。

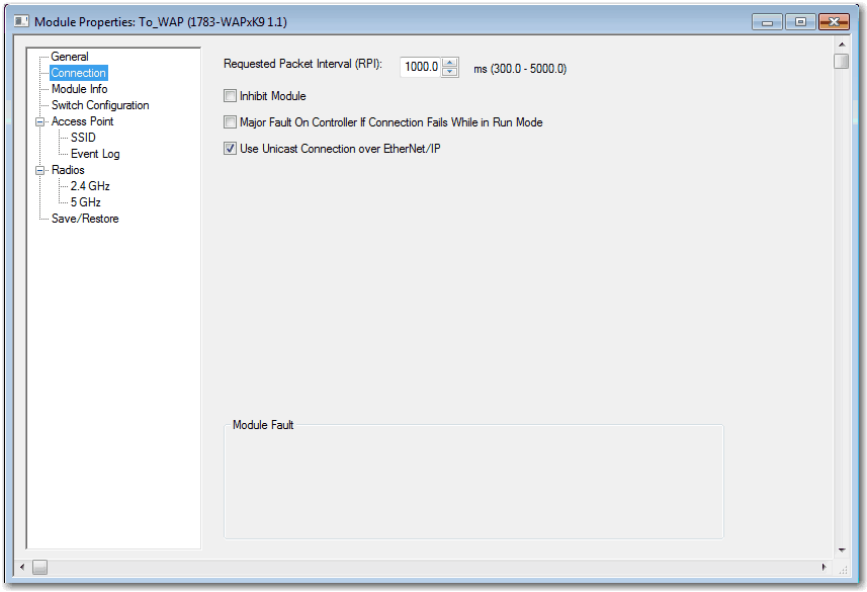
表 71 - 常规参数描述 (续)

参数	描述
Ethernet Address	输入唯一的 IP 地址，以识别网络上的模块。 IP 地址可标识 IP 网络 (或连接的网络系统) 上的每个节点。网络上的每个 TCP/IP 节点必须拥有唯一的 IP 地址。 IP 地址是互联网协议网络上的每个节点的 32 位标识号。这些地址表示为四组 8 位数字 (数字范围为 0 … 255)，使用小数点分隔。 IP 地址由网络 ID 部分和主机 ID 部分构成。网络被分类为 A、 B、 C 或其他。网络类别决定了 IP 地址的格式。 可从其小数点 IP 地址的首个整数区分 IP 地址的类别。 • 同一物理网络上的每个节点必须拥有相同类别的 IP 地址和相同的网络 ID。 • 同一网络上的每个节点必须拥有不同的主机 ID，即唯一的 IP 地址。 IP 地址的首个八位字节不能是 127，或大于 223 的数字。如果输入任何这些值，并试图使用 Set (设置) 按钮下载该配置，将显示错误消息，同时值不会发送到模块。 例如， 32 位 IP 地址： 00000011 00000000 00000000 00000001 被写入为 3.0.0.1。 可从其小数点 IP 地址的首个整数区分 IP 地址的类别，步骤如下： **首个整数的范围** **类别** 0...127 A 128...191 B 192...223 C 224...255 其他 请联系网络管理员或网络信息中心，向模块分配一个唯一的 IP 地址。 在线时， IP 地址无法更改。
Revision	接入点的固件版本。
Electronic Keying	在初始模块配置期间，为您的模块选择其中一个匹配选项。 **精确匹配** 下面所描述的所有参数必须匹配，否则插入的模块将拒绝连接。 **兼容模块** 您必须满足以下条件，否则插入的模块将拒绝连接： 模块类型、产品目录号和主要版本必须匹配。 物理模块的次要版本必须等于或高于软件中指定的版本。 **禁用匹配** 控制器不采用任何匹配功能。 更改 RPI 和电子匹配选择可能会导致模块的连接损坏，从而导致数据丢失。 **警告：** 使用该选项时要格外小心；如果使用不当，该选项可能会导致人员受伤或死亡、财产损坏或经济损失。
Connection	您可选择随时更改模块定义，无需删除现有模块和创建新模块。配置文件将尝试提交新设置的所有配置数据。无法提交的任何配置数据都将被设为默认值。一旦应用新的设置，这些设置便成为基本设置，之前的所有数据格式配置都将丢失。 请注意：借助组合模块，需要在执行输入之前解决存在的系统问题。输入连接将需要生成只用于配置输入的部分配置数据类型。 **输入** 生成输入和配置数据类型和标签。如果建立该连接，其便拥有配置；并分享输入。 **输出** 生成输入、输出和配置数据类型和标签。如果建立该连接，其便拥有配置和输出；并分享输入。

Connection (连接) 对话框

在 Connection (连接) 对话框中，您可通过连接更新数据，也可禁用或启用与模块的连接。

图 90 - Connection (连接) 对话框



Connection (连接) 对话框包含以下参数。

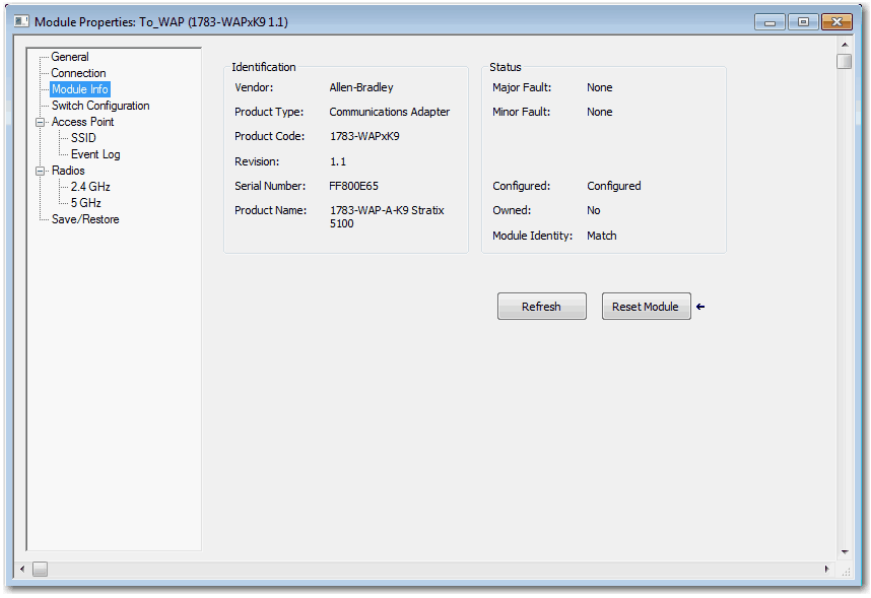
表 72 - 连接参数描述

参数	描述
Requested Packet Interval (RPI)	请求信息包间隔 (RPI) 设置确定了数据通过连接更新的时间段 (单位：ms)。 RPI 控制呈灰色显示，因为每个控制器都可有其自己单独的 RPI 设置。
Inhibit Module	禁用模块 禁用或启用到模块的连接。禁用模块可能会导致到模块的连接损坏。禁用模块可能会导致到模块的连接损坏，进而导致数据丢失。
Major Fault	如果模块连接失败，则可能会导致控制器严重故障。
Use Unicast	如果当前版本的模块支持单播，且模块路径的任何部分通过 EtherNet/IP，则启用。
Module Fault	连接请求错误 —— 控制器尝试建立到模块的连接，但发生错误。连接未建立。 服务请求错误 —— 控制器尝试从模块请求服务，但发生错误。服务没有成功执行。 模块配置无效 —— 模块中的配置无效。 (该错误通常由电子匹配传递失败引起。) 电子匹配不一致 —— 电子匹配功能启用，软件和模块之间的部分匹配信息不同。

模块信息对话框

在 Module Information (模块信息) 对话框中，可查看状态并复位接入点。

图 91 - Module Information (模块信息) 对话框



Module Information (模块信息) 对话框包含以下参数。

表 73 - 模块信息参数描述

项目	描述
Type	显示正在创建模块的类型和描述 (只读)。
Identification	显示模块的： • 供应商 • 产品类型 • 产品代码 • 版本 • 序列号 • 产品名称
Revision	选择模块的次要版本号。要更改版本，请通过单击 Change (更改) 按钮来访问 Module Definition (模块定义) 对话框。 版本分为主要版本和次要版本。主要版本静态显示在该对话框上；可从 Select Module Type (选择模块类型) 对话框编辑该值。 主要版本用于指示模块的接口版本。次要版本用于指示固件版本。
Change...	单击该按钮，访问 Module Definition (模块定义) 对话框，在此处可更改定义模块定义的值、电子匹配和次要版本。
Faults	严重和轻微故障状态
Configured	指示模块是否已经过配置。
Owned	显示控制器当前是否连接到模块。

表 73 - 模块信息参数描述 (续)

项目	描述
Match	与 General (常规) 选项卡上指定的内容一致。 为确保匹配条件成立，以下各项必须一致： • 供应商 • 模块类型 (特定供应商的产品类型和产品代码组合) • 主版本 与 General (常规) 选项卡上指定的内容不一致。
Refresh	使用模块中的新数据刷新对话框。
Reset Module	通过模拟断电重启将模块返回到其上电状态。  **警告：** 重置模块会导致与所有模块的连接关闭，使您无法再进行控制。

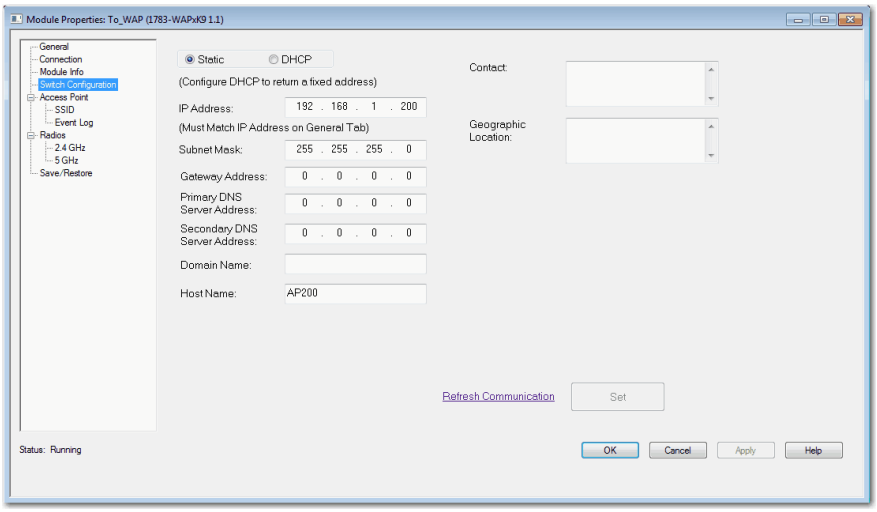
Switch Configuration (交换机配置) 对话框

在 Switch Configuration (交换机配置) 对话框中，可对接入点进行配置。可以配置的参数包括：如 IP 地址、服务器地址和主机名称。

IP 地址可以手动分配 (静态)，也可以由动态主机配置协议 (DHCP) 服务器自动分配。默认设置为 Static (静态)。

建议选择 Static (静态) 并为交换机手动分配 IP 地址。此后，如需访问交换机，则可随时使用该 IP 地址。

图 92 - Switch Configuration (交换机配置) 对话框



Switch Configuration (交换机配置) 对话框包括这些信息。

表 74 - 交换机配置参数描述

项目	描述
Static	手动输入接入点 / 工作组网桥的 IP 地址、子网掩码和网关。默认设置为静态。
DHCP	接入点自动从 DHCP 服务器获取 IP 地址、默认网关和子网掩码。只要接入点未重新启动，就会继续使用分配的 IP 信息。
IP Address	输入接入点的 IP 地址。 交换机的 IP 地址是 32 位标识号。它表示为使用句点分隔的 4 个八位字节 (xxx.xxx.xxx.xxx)。将每个八位字节设为介于 0…255 之间。 该值必须与 Express Setup (快速设置) 期间在设备管理器中输入的 IP 地址以及 General (常规) 选项卡上的地址匹配。 如果为交换机重新配置的是不同的 IP 地址，则单击 Set (设置) 后将失去与交换机的通信。要更正此问题，必须返回到 Express Setup (快速设置) 和 General (常规) 选项卡，设置新的 IP 地址，然后下载到控制器。 IP 地址不应低于 0.1.0.0 或介于 224.0.0.0 和 255.255.255.255 之间。 请联系网络管理员或网络信息中心，向接入点分配一个唯一的 IP 地址。

表 74 - 交换机配置参数描述 (续)

项目	描述
Subnet Mask	为接入点输入相应的子网掩码。 子网掩码是一个 32 位数字。将每个八位字节设为介于 0…255 之间。 默认值为 255.255.255.0。 该值必须与 Express Setup (快速设置) 期间在设备管理器中输入的子网掩码匹配。
Gateway Address	(可选) 输入网关的 IP 地址。 网关是接入点与其他网络或子网络上的设备进行通信所使用的路由器或其他网络设备。 网关 IP 地址应同接入点 IP 地址在同一子网中。接入点 IP 地址和默认网关 IP 地址不可相同。
Primary DNS Server Address	输入主域名系统 (DNS) 服务器的地址。 将每个八位字节设为介于 0…255 之间。首个八位字节不能是 127，或大于 223 的数字。
Secondary DNS Server Address	(可选) 输入网关的 IP 地址。 网关是交换机与其他网络或子网络上的设备进行通信所使用的路由器或其他网络设备。 网关 IP 地址应同接入点 IP 地址在同一子网中。接入点 IP 地址和默认网关 IP 地址不可相同。
Domain Name	输入模块所属的域名。域名包括由句点分隔的一系列名称标签，例如 rockwellautomation.com。域名长度限值为 48 个字符，并限制为只使用 ASCII 字母 a… z、数字 0…9、句点和连字符。
Host Name	为计算机输入唯一的主机名称。 主机名称是其所在域内唯一的计算机名称。其始终是全名的第一个元素，包括其所在域和顶级域名后缀，从而可在互联网上创建唯一的计算机名称。例如，如果一个交易网站是 www.trading.com，主机名称是 www，这在网络上并不唯一，但在交易域内却是唯一的。 此外，主机名称也指完全限定域名 (FQDN)，或在本例中为 www.trading.com。两种命名方法一般可交替使用。
Contact	输入接入点的联系人信息，最多 200 个字符。该功能是可选功能。 联系人信息可包含字母数字字符、特殊字符和回车。
Geographic Location	输入接入点的地理位置，最多 200 个字符。该功能是可选功能。 地理位置可包含字母数字字符、特殊字符和回车。
Refresh Communication	单击以用模块的新数据刷新对话框。 在离线模式下， Refresh (刷新) 按钮不可用。

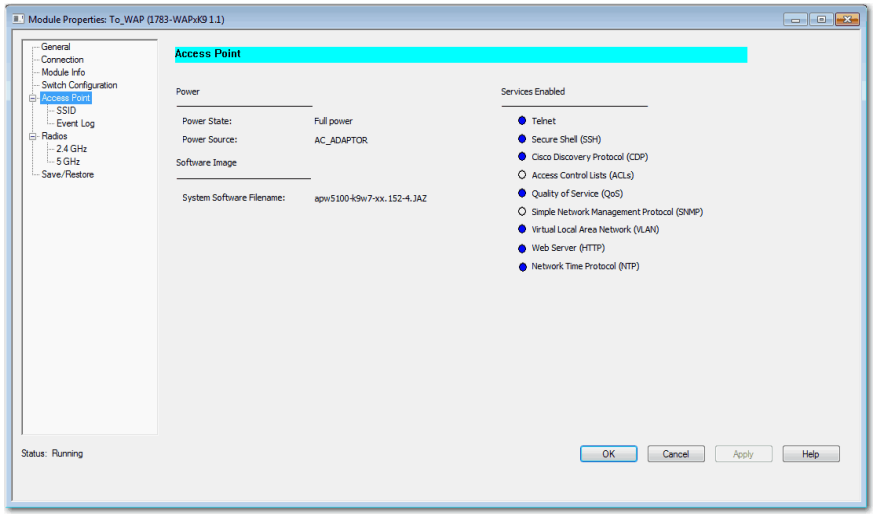
Access Point (接入点) 对话框

可使用该对话框查看有关无线接入点的信息。您可在 Access Point (接入点) 对话框上查看以下内容。

- 接入点的电源模式。
- 接入点检测到的电源。
- 在接入点中启用的服务。
- 上传到交换机的固件文件名和版本。

数据仅在模块在线时显示。

图 93 - Access Point (接入点) 对话框



接入点参数

Access Point (接入点) 对话框包含这些参数。

表 75 - 接入点参数描述

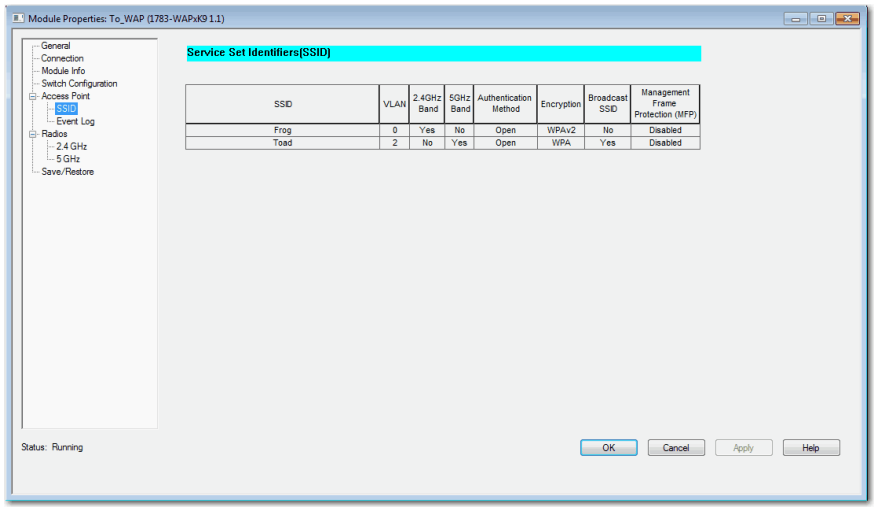
参数	描述
Power State	接入点的电源模式：电源充足、电源不足
Power Source	接入点检测到的电源。交流适配器以太网供电 (PoE)
System Software Filename	交换机中上传的固件文件名。
Services Enabled	当前启用或禁用的主服务。当指示器蓝色时启用服务。 • Telnet • 安全外壳 (SSH) • 思科发现协议 (CDP) • 访问控制列表 (ACL) • 服务质量 (QoS) • 简单网络管理协议 (SNMP) • 虚拟局域网 (VLAN) • Web 服务器 (HTTP) • 网络协议 (NTP)

Service Set Identifiers (SSID)(服务集标识符 (SSID)) 对话框

使用该对话框显示有关 SSID 的消息。您可在 SSID 对话框上查看以下内容。

- 与无线电装置关联的 SSID
- 与 SSID 关联的 VLAN
- 用于 SSID 的验证方法
- 用于 SSID VLAN 的加密模式
- 接入点是否广播 SSID
- 用于 SSID 的管理帧保护；数据仅在模块在线时显示。

图 94 - Service Set Identifiers (SSID)(服务集标识符 (SSID)) 对话框



Service Set Identifiers (SSID)(服务集标识符 (SSID)) 对话框包含以下参数。

表 76 - 服务集标识符 (SSID) 参数描述

参数	描述
SSID	用于与无线电关联的唯一标识符。
VLAN	与 SSID 关联的 VLAN。
2.4GHz Band	指示 2.4 GHz 频段是否针对 SSID 启用。
5GHz Band	指示 5 GHz 频段是否针对 SSID 启用。
Authentication Method	SSID 用于网络验证的验证方法。这包括开放式验证、共享式验证和 EAP 验证
Encryption	SSID 的 VLAN 加密模式。 • WPA • WPAv1 • WPAv2
Broadcast SSID	指示 SSID 是否是广播。
Management Frame Protection2 (MFP)	SSID 的管理帧保护设置。 • 禁用 • 可选 • 需要

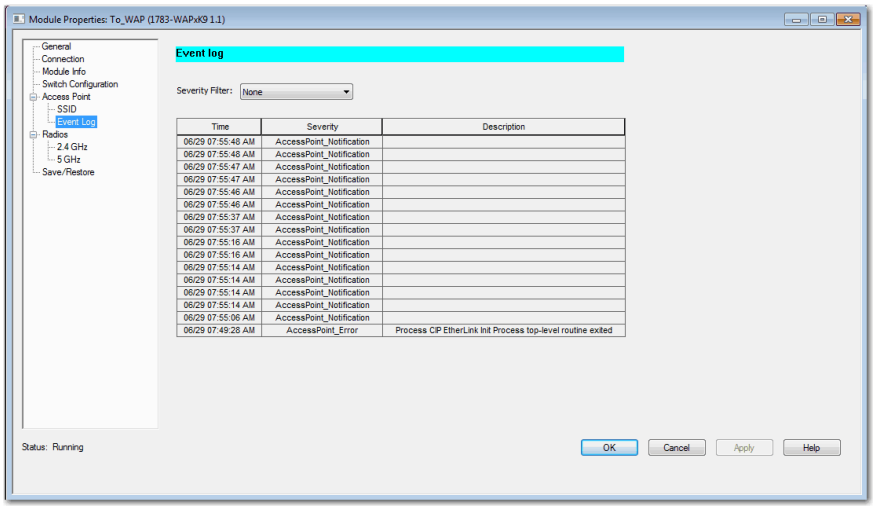
Event Log (事件记录) 对话框

Event (事件) 对话框显示事件记录。可在 Event Log (事件记录) 对话框上执行以下操作。

- 选择要查看事件的严重性或查看所有记录的事件。
- 事件发生时查看。
- 查看事件的严重性。
- 查看事件描述。

数据仅在模块在线时显示。

图 95 - Event Log (事件记录) 对话框



Event Log (事件记录) 对话框包含以下参数。

表 77 - 事件记录参数描述

参数	描述
Severity Filter	使用该参数可选择显示在事件记录表中的事件严重性。 • AccessPoint_Emergency —— 系统不可使用 • AccessPoint_Alert —— 需要立即执行操作 • AccessPoint_Critical —— 当前状况严重 • AccessPoint_Error —— 记录到错误状况 • AccessPoint_Warning —— 指示潜在的错误状况 • AccessPoint_Notification —— 仍可正常操作，但可能导致严重状况 • AccessPoint_Informational —— 信息消息提供正常活动的例行信息；不指示错误 • AccessPoint_Debugging —— 提供调试消息 • None —— 显示所有事件
Time	时间戳连同时间一起记录。
Severity	事件的严重性。 • AccessPoint_Emergency • AccessPoint_Alert • AccessPoint_Critical • AccessPoint_Error AccessPoint_Warning • AccessPoint_Notification • AccessPoint_Informational • AccessPoint_Debugging None
Description	错误事件的描述。

Radios (无线电) 对话框

使用该对话框显示有关 Stratix 5100 中所包含无线电的概要信息。Stratix 5100 包含同步双频段无线电装置 (2.4 GHz 和 5 GHz)。可在 Radios (无线电) 对话框上查看以下信息。

- 无线电装置描述。
- 与无线电装置关联的 MAC 地址。
- 无线电装置启动并持续运行的时间。
- 软件和硬件状态。
- 数据仅在模块在线时显示。

Radios (无线电) 对话框包含以下参数。

表 78 - 无线电对话框参数描述

参数	描述
Radio (GHz)	双频段无线电。 Stratix 5100 包含 2.4 GHz 和 5 GHz 无线电装置。
Description	无线电描述。
MAC Address	与无线电关联的 MAC 地址
Uptime	自网络管理系统开始运行的时间。
Software Status	接口的管理状态。 • 上行 • 下行 • 测试 • 未知 • 休眠 • 不存在 • 底层停机
Hardware Status	指示接口的线路协议是启用还是禁用。

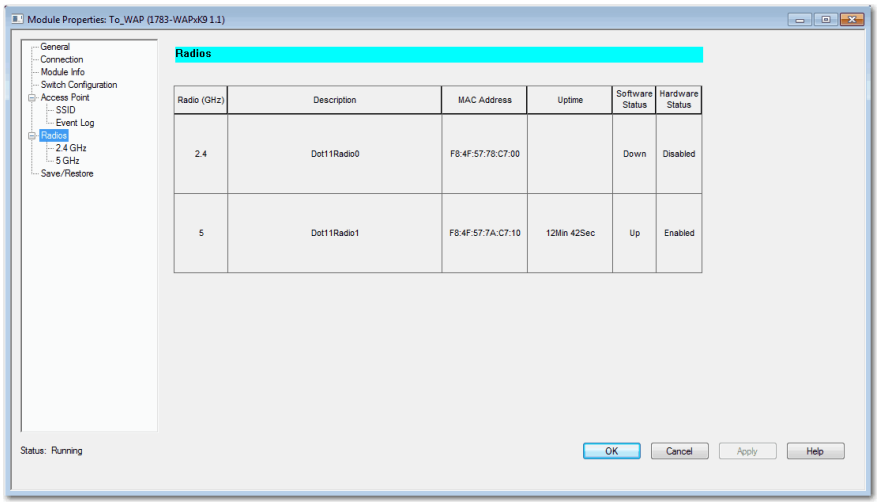
2.4 GHz 或 5 GHz Radio (无线电) 对话框

可使用该对话框查看有关 2.4 GHz 或 5 GHz 波段无线电装置的信息。可在 2.4 GHz 或 5 GHz Radio (无线电) 对话框中执行以下操作。

- 查看当前与无线电装置关联的活动无线客户端和网桥的数量。
- 查看用于发送数据的功率级别和数据传输速率。
- 查看无线电装置的作用和客户端设备的类型。
- 查看 IP 地址、 MAC 地址、客户端设备状态以及客户端发送和接收的数据包数量。
- 打开 Diagnostic (诊断) 对话框，可查看无线电装置各速率的计数和统计数据。

数据仅在模块在线时显示。

图 96 - 2.4 GHz 或 5 GHz Radio (无线电) 对话框



2.4 GHz 或 5 GHz Radio (无线电) 对话框包含以下参数。

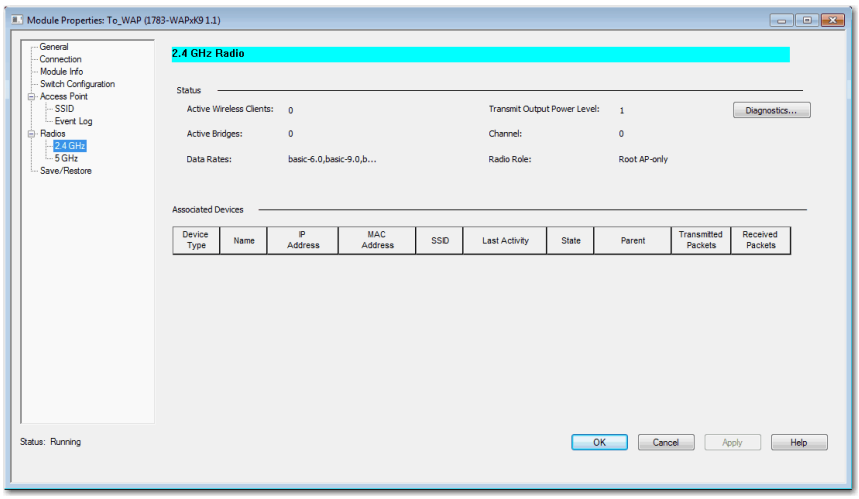
表 79 - 2.4 GHz 或 5 GHz 无线电装置参数描述

参数	描述
Active Wireless Clients	当前与该接口上的设备关联的无线客户端数量。
Active Bridges	当前与该接口上的设备关联的网桥数量。
Data Rates	设备用于发送数据的速率。 • 默认 • 最佳范围 • 最佳吞吐量 • 1.0、2.0、5.5、11.0、6.0、9.0、12.0、18.0、24.0、36.0、48.0 和 54.0 Mbps • 需要、启用、禁用
Transmit Output Power Level	用于发送数据的功率级别。功率级别取决于频带。 最大值为： • 2.4 GHz 频带： 22dBm • 5 GHz 频带： 14dBm
Channel	当前工作频率通道。

表 79 - 2.4 GHz 或 5 GHz 无线电装置参数描述 (续)

参数	描述
Radio Role	确定无线电的作用。 • 非根网桥 • 带无线客户端的非根网桥 • 中继器 • 根接入点 • 仅根 AP • 根网桥 • 带无线客户端的根网桥 • 扫描器 • 工作组网桥
Diagnostic	打开 Diagnostic (诊断) 对话框，可查看无线电装置各速率的计数和统计数据。该对话框提供了用于监控和诊断接入点工作的信息。
Device Type	设备类型。 0：未知 1：WGB 客户端 2：WGB 3：客户端 4：中继器 5：网桥名称
Name	设备的名称。
IP Address	客户端设备的 IP 地址。
MAC Address	客户端设备的 MAC 地址。
SSID	用于与无线电关联的唯一标识符。
Last Activity	设备上一次活动的时间。
State	客户端设备的状态。 • 0：关联 — 处理 • 1：EAP — 关联 • 2：MAC — 关联 • 3：关联
Parent	父无线客户端设备的名称。
Transmitted Packets	发送到客户端的数据包数量。
Received Packets	从客户端接收的数据包数量。

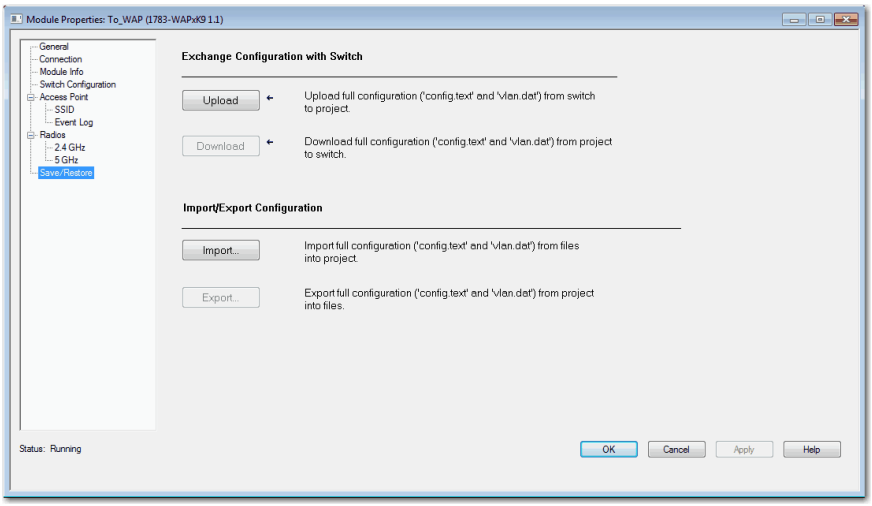
图 97 - 2.4 GHz 或 5 GHz Radio (无线电) 对话框对话框



Save/Restore (保存 / 恢复) 对话框

Save (保存) 和 Restore (恢复) 对话框可向接入点上传项目或从接入点下载项目。

图 98 - Save/Restore (保存 / 恢复) 对话框



Save/Restore (保存 / 恢复) 对话框包含以下参数。

表 80 - 保存 / 恢复参数描述

项目	描述
Exchange Configuration with Switch	**上传** 在线时，将交换机的全部设置上传到项目。这包括 config.text 和 vlan.dat 文件。在离线模式下上传不可用。 **下载** 在线时，将项目的全部设置下载到交换机。这包括 config.text 和 vlan.dat 文件。在离线模式下下载不可用。
Import/Export Configuration	**导入** 在线时，将来自计算机本地存储文件的交换机配置导入到项目文件。这包括 config.text 文件和 vlan.dat 文件 当出现 Import (导入) 对话框时： 1. 输入包含想导入内容的 config.text 文件 (和完整路径) 的名称。 2. 单击 Import (导入)。 Import (导入) 对话框重新显示。 3. 输入想导入的 vlan.dat 文件 (和完整路径) 的名称。 4. 单击 Import (导入)。 系统将两个文件导入到项目中。 交换机配置文件在 Projects Samples (项目示例) 目录下提供。如果想将交换机远程复位到其开箱即用默认值，请将文件导入到项目，并下载到交换机。 **导出** 在线时，将交换机配置数据从项目导出到文件。当显示 Export (导出) 对话框时，根据以下步骤操作。 1. 输入 config.text 文件 (和完整路径) 的名称。 2. 单击 Export (导出)。 Export (导出) 对话框重新显示。 3. 输入 vlan.dat 文件 (和完整路径) 的名称。 4. 单击 Export (导出)。 系统将内容导出到两个文件中。 在离线模式下导出不可用。

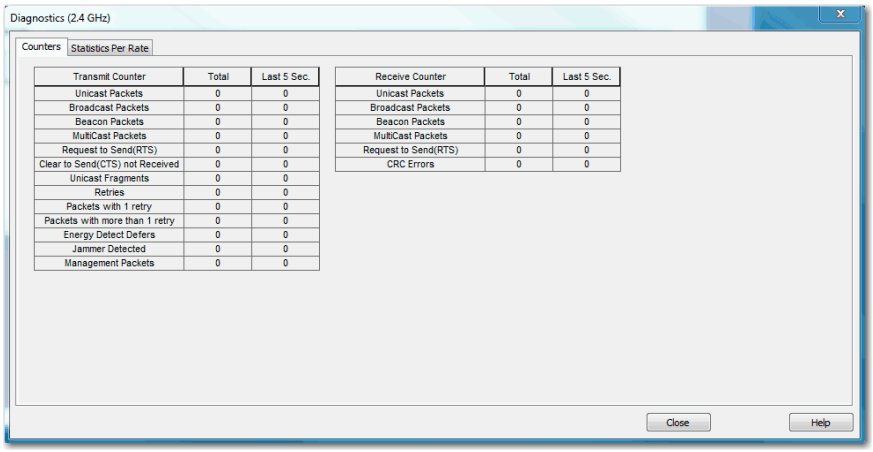
Counters (计数) 对话框

使用该对话框，可查看有关最近 5 秒钟内以及累计接收和发送的数据包信息。该对话框和 Statistics Per Rate (速率统计数据) 对话框提供用于监控和诊断接入点工作的实用信息。

可在 Counters (计数) 对话框上查看以下信息：

- 由接入点发送 / 接收的单播、广播、信标和多播数据包
- 由接入点发送 / 接收的请求发送 (RTS) 和清除发送 (CTS)
- 接入点尝试发送数据包的次数
- 由于另一个无线电装置正在发送而导致的延期数据包
- 检测到干扰源，但被忽略
- 带 CRC 错误的数据包

数据仅在模块在线时显示。



Counters (计数) 对话框包含以下参数。

表 81 - 计数器参数描述

参数	描述
Transmit Counter	发送统计数据。
Receive Counter	接收统计数据
Total	客户端发送或接收数据包的总数。
Last 5 Sec.	最近 5 秒内发送或接收的数据包数量。
Unicast Packets	由接入点发送 / 接收的单播数据包数。
Broadcast Packets	由接入点发送 / 接收的广播数据包数。
Beacon Packets	由接入点发送 / 接收的信标数据包数。
Multicast Packets	由接入点发送 / 接收的多播数据包数。
Request to Send (RTS)	由接入点发送 / 接收的 RTS 次数。
Clear to Send (CTS) not Received	RTS 已发送但响应中却未收到 CTS 的次数。

表 81 - 计数器参数描述 (续)

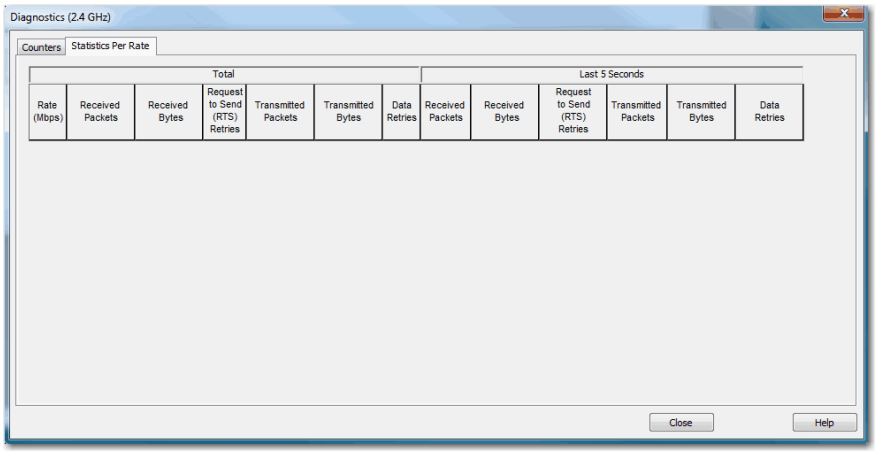
参数	描述
Unicast Fragments	发送的全部或部分碎片数据包的数量。
Retries	接入点尝试发送数据包或 RTS 的次数。
Packets with 1 retry	接入点仅一次重试发送数据包的次数。
Packets with more than 1 retry	接入点多次重试发送数据包的次数。
Energy Detect Defers	由于能量检测电路指示另一个无线电装置正在发送而导致数据包延期发送的次数。
Jammer Detected	检测到持续时间超过法定 802.11 数据包的干扰源次数。干扰源被忽略，且重复传输。
Management Packets	由接入点发送的管理数据包数。
CRC Errors	带 CRC 错误的数据包数。

Statistics Per Rate (速率统计数据) 对话框

使用该对话框，可查看有关最近 5 秒钟内以及累计接收和发送的数据包信息。该对话框和 Counters (计数) 对话框提供用于监控和诊断接入点工作的实用信息。

可在 Statistics Per Rate (速率统计数据) 对话框上查看以下内容。

- 用于发送数据的速率
- 接收到的数据包和字节数
- 接入点尝试发送请求发送 (RTS) 的次数
- 从接入点发送的数据包和字节数



数据仅在模块在线时显示。

表 82 - 速率统计参数描述

参数	描述
Total	客户端发送或接收数据包的总数。
Last 5 Seconds	最近 5 秒内发送或接收的数据包数量。
Rate (Mbps)	用于发送数据的速率。速率单位为兆比特 / 秒。
Received Packets	正在接收的数据包数。
Received Bytes	正在接收的字节数。
Request to Send (RTS) Retries	接入点尝试发送 RTS 数据包的次数。
Transmitted Packets	从接入点发送的数据包数量。
Transmitted Bytes	从接入点发送的字节数量。
Data Retries	接入点尝试发送数据包的次数。

模块定义的数据类型

下表列出和说明了 Stratix 5100 无线接入点中由模块定义的数据类型。下表包含用于输入的信息，使用 “I” 指示。

表 83 - 模块定义数据类型： AB:STRATIX_5100_1PORT:I:0

成员名称	类型	默认显示样式
Fault	DINT	二进制
Radio2_4GHzEnabled	BOOL	十进制
Radio5GHzEnabled	BOOL	十进制
Radio2_4GHzUptime	DINT	十进制
Radio5GHzUptime	DINT	十进制
ClientsConnected	INT	十进制
WorkGroupBridgesConnected	INT	十进制
UnicastPacketsSent	DINT	十进制
UnicastPacketsReceived	DINT	十进制
CRCErrors	DINT	十进制
TotalPacketsMoreThan1Retry	DINT	十进制
TotalRetries	DINT	十进制
SSIDsDefined	INT	十进制
PortGiConnected	BOOL	十进制
PortGiSpeed	DINT	十进制
PortGiFullDuplex	BOOL	十进制

备注：

使用命令行界面配置 Stratix 5100 WAP

本章介绍了可用于配置无线设备的思科 IOS 命令行界面 (CLI)。

思科 IOS 命令模式

思科 IOS 用户界面分为多种不同模式。可使用哪些命令取决于您当前所处的模式。在命令提示符位置输入问号 (?)，可获取各命令模式的可用命令列表。

当在无线设备上启动会话时，便进入用户模式，通常称为用户 EXEC 模式。在用户 EXEC 模式下，可使用的命令是思科 IOS 命令的一个子集。例如，大多数用户 EXEC 命令都是一次性命令，如 show 命令 (显示当前配置状态) 和 clear 命令 (清除计数器或界面)。当无线设备重启时，用户 EXEC 命令不会被保存。

要访问所有命令，必须进入特权 EXEC 模式。通常，要进入特权 EXEC 模式，必须输入密码。必须在进入特权 EXEC 模式后，才能再从该模式进入全局配置模式。

您可使用以下配置模式更改正在运行的配置：全局、界面和命令行。如果保存了配置，将在无线设备重启后保存和使用这些命令。要访问各种配置模式，必须以全局配置模式启动。从全局配置模式中，可进入界面配置模式和命令行配置模式。

下表介绍了主要的命令模式、如何访问各种模式、该模式中的提示符以及如何退出模式。表中的示例使用主机名称 ap。

表 84 - 命令模式

模式	访问方法	提示符	退出方法	关于该模式
用户 EXEC	开始与无线设备的会话。	ap>	输入 logout 或 quit。	使用该模式： • 更改终端设置 • 执行基本测试 • 显示系统信息
特权 EXEC	在用户 EXEC 模式下时，输入 enable 命令。	ap#	输入 disable 退出。	使用该模式显示设备配置、诊断和调试信息。使用密码保护对该模式的访问。
全局配置	在特权 EXEC 模式下时，输入 configure 命令。	ap(config)#	要退出特权 EXEC 模式，输入 exit 或 end，或按下 Ctrl-Z。	使用该模式配置要应用到整个无线设备的参数。
接口配置	在全局配置模式下时，输入 interface 命令 (带特定的接口)。	ap(config-if)#	要退出全局配置模式，输入 exit。要返回到特权 EXEC 模式，按下 Ctrl-Z 或输入 end。	使用该模式配置以太网和无线电接口的参数。 • 802.11n 2.4 GHz 无线电方式为 radio 0 • 802.11n 5 GHz 无线电方式为 radio 1

获取帮助

您可在系统提示符处输入问号 (?)，以显示各种命令模式可用的命令列表。您还可获取各个命令的关联关键字和参数，表中也对此进行了介绍。

表 85 - 帮助概要

命令	用途
帮助	在任何命令模式下可获取帮助系统的简要描述。

abbreviated-command-entry?	获取以特定字符串开头的命令列表。
	例如：
	`ap# di?`
	`dir disable disconnect`

abbreviated-command-entry<Tab>	填写部分命令名称。
	例如：
	`ap# sh conf<tab>`
	`ap# show configuration`

表 85 - 帮助概要 (续)

命令	用途
?	列出特定命令模式的所有可用命令。 例如： `ap> ?`
command ?	列出命令的相关关键字。 例如： `ap> show ?`
command keyword ?	列出关键字的相关参数。 例如： `ap(config)# cdp holdtime ?` <10-255> 接收器必须保留该数据包的时长 (s)

缩写命令

您必须输入足够多的字符，以便无线设备以唯一名称识别命令。下例显示了如何输入 show configuration 特权 EXEC 命令：

```
ap# show conf
```

使用命令的 No 和 Default 格式

大多数配置命令还具有 no 格式。通常，可使用 no 格式禁用功能或反转命令的操作。例如， no shutdown 界面配置命令反转界面的关机操作。使用不带关键字 `no` 的命令可启用已禁用的功能，或启用默认禁用的功能。

配置命令还有 default 格式。命令的 default 格式将命令设置返回到其默认值。默认情况下，大多数命令为禁用，因此， default 格式与 `no` 格式的效果相同。但一些命令默认为启用，并将变量设为特定的默认值。在这种情况下， default 命令将启用命令，并将变量设为默认值。

了解 CLI 消息

下表列出了使用 CLI 配置无线设备时可能遇到的一些错误消息。

表 86 - CLI 错误消息

错误消息	含义	如何获取帮助
% Ambiguous command: show con	没有输入足够多的字符，无线设备无法识别命令。	输入命令，后跟一个问号 (**?**)，命令和问号之间留一个空格。 将显示可随命令一块输入的关键字。
% Incomplete command.	没有输入该命令所必需的所有关键字或值。	输入命令，后跟一个问号 (**?**)，命令和问号之间留一个空格。 将显示可随命令一块输入的关键字。
% Invalid input detected at '^' marker.	输入的命令不正确。脱字符号 (^) 标记错误点。	输入问号 (**?**)，以显示该命令模式下的所有可用命令。 将显示可随命令一块输入的关键字。

命令历史

CLI 提供您所输入的命令的历史或记录。当需要重新调用较长或复杂的命令或输入 (包括访问列表) 时，该功能很有用。您可根据自己的需要自定义命令历史功能。

更改命令历史缓冲区大小

默认情况下，无线设备将十行命令行记录到历史缓冲区中。在特权 EXEC 模式下可输入此命令，更改无线设备在当前终端会话期间记录的命令行数：

```
ap# terminal history[size number-of-lines]
```

范围为 0...256。

在命令行配置模式下输入该命令，配置无线设备在特定行上所有会话的记录的命令行数：

```
ap(config-line)# history [size number-of-lines]
```

范围为 0...256。

重新调用命令

要从历史缓冲区中重新调用命令，可执行下表中所列的操作之一。

表 87 - 调用命令操作和结果

操作[1]	结果
按下 Ctrl-P 或向上箭头键。	从最后使用的命令开始，调用历史缓冲区中的命令。重新按键序列，按顺序调用更早的命令。
按下 Ctrl-N 或向下箭头键。	在使用 Ctrl-P 或向上箭头键调用命令后，返回到历史缓冲区中更近期的命令。重新按键序列，按顺序调用更近期的命令。
显示历史	在特权 EXEC 模式下，列出刚输入的最后几个命令。显示的命令数量取决于 terminal history 全局配置命令和 history 命令行配置命令的设置。

(1) 仅兼容 ANSI 的终端 (例如， VT100) 上可使用箭头键。

禁用命令历史功能

命令历史功能已自动启用。

- 要在当前终端会话期间禁用该功能，输入 terminal no history 特权 EXEC 命令。
- 要禁用命令行的命令历史，输入 no history 命令行配置命令。

使用编辑特性

本节介绍了可用于操控命令行的编辑特性。

启用和禁用编辑功能

增强编辑模式已自动启用，但您可禁用它。

要在当前终端会话中重新启用增强编辑模式，在特权 EXEC 模式下输入该命令：

```
ap# terminal editing
```

要重新配置特定的命令行以启用增强编辑模式，在命令行配置模式下输入该命令：

```
ap(config-line)# editing
```

要全局禁用增强编辑模式，在命令行配置模式下输入该命令：

```
ap(config-line)# no editing
```

使用按键编辑命令

下表显示了编辑命令行所需的按键。

表 88 - 通过按键编辑命令

功能	按键(1)	用途
在命令行中移动进行更改或修正。	Ctrl-B 或向左箭头键	将光标向后移一个字符。
	Ctrl-F 或向右箭头键	将光标向前移一个字符。
	Ctrl-A	将光标移动到当前行的开头。
	Ctrl-E	将光标移动到当前行的末尾。
	Esc B	将光标向后移一个单词。
	Esc F	将光标向前移一个单词。
	Ctrl-T	将光标左侧的字符与光标位置的字符调换。
调用缓冲区中的命令，将它们粘贴到命令行中。无线设备将您删除的最后十条命令存储在缓冲区中。	Ctrl-Y	调用缓冲区中的最近的一条命令。
	Esc Y	调用缓冲区中的下一条命令。 缓冲区只包含您删除或剪切的最后 10 条命令。如果按下 Esc Y 多次，可循环到缓冲区中的第一条命令。
用于在写错或想要更改时删除条目。	Delete 或退格	删除光标左侧的一个字符。
	Ctrl-D	删除光标处的字符。
	Ctrl-K	删除从光标到命令行末尾之间的所有字符。
	Ctrl-U 或 Ctrl-X	删除从光标到命令行开头之间的所有字符。
	Ctrl-W	删除光标左侧的一个字符。
	Esc D	删除从光标到单词末尾之间的字符。
大写或小写单词，或大写一组字母。	Esc C	大写光标处的字符。
	Esc L	将光标处的单词变为小写。
	Esc U	将光标到单次末尾之间的字母变为大写。
将特定按键指定为可执行命令，例如，作为快捷键。	Ctrl-V 或 Esc Q	
当终端屏幕无法全部显示时，滚动行或屏幕画面。 当输出的行数过多以至于无法在终端屏幕中完全显示时，将显示 More 提示符 (包括 show 命令输出)。当看到 More 提示符时，可使用 Return 和 空格键显示更多信息。	Return	向下滚动一行。
	SPACE	向下滚动一个屏幕画面。
如果无线设备突然向屏幕发送一条消息，则重新显示当前的命令行。	Ctrl-L 或 Ctrl-R	重新显示当前的命令行。

(1) 仅兼容 ANSI 的终端 (例如， VT100) 上可使用箭头键。

编辑换行的命令行

您可使用命令的 wraparound 功能，在屏幕上扩展单行命令行。当光标到达右边界时，命令行向左平移十个空格。您无法看到命令行的前十个字符，但可向后滚动，查看命令开头的语法。

要向后滚动到命令条目的开头，重复按下 Ctrl-B 或向左箭头键。您还可按下 Ctrl-A 立即移动到命令行的开头。

仅兼容 ANSI 的终端 (例如， VT100) 上可使用箭头键。

在本例中， `access-list global configuration` 命令条目扩展一行。当光标第一次到达行末尾时，行向左平移十个空格，重新显示。美元符号 `$` 指示行已被向左滚动。每次光标到达行末尾时，行重新向左平移十个空格。

```
ap(config)# access-list 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1

ap(config)# $ 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1.20 255.25

ap(config)# $t tcp 131.108.2.5 255.255.255.0
131.108.1.20 255.255.255.0 eq

ap(config)# $108.2.5 255.255.255.0 131.108.1.20
255.255.255.0 eq 45
```

在完成输入后，按下 Ctrl-A 检查完整的语法，然后再按下 Return 键执行命令。行末尾的美元符号 ($) 指示行已向右滚动：

```
ap(config)# access-list 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1$
```

软件假设终端屏幕宽度为 80 列。如果宽度不同，可使用 terminal width 特权 EXEC 命令设置终端宽度。

使用自动换行及命令历史功能重新调用和修改之前的复杂命令条目。关于重新调用之前的命令条目的信息，请参见第 200 页的 “ 使用按键编辑命令 ”。

搜索和过滤 show 和 more 命令的输出

您可搜索和过滤 show 和 more 命令的输出。如果您需要整理大量输出或者排除不想看见的输出，该命令很有用。

要使用该功能，输入 show 或 more 命令，然后再接 管道符 (|)，关键字 begin、 include 或 exclude 之一以及想要搜索或滤除的表达式：

```
command | {begin | include | exclude} regular-expression
```

表达式区分大小写。例如，如果输入 | exclude output，则将不显示包含 output 的行，但将显示包含 Output 的行。

下列显示了如何只在输入显示中显示表达式中包含 protocol 的行：

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

访问 CLI

您可使用 Telnet 或 安全外壳 (SSH) 打开无线设备 CLI。

使用 Telnet 打开 CLI

根据以下步骤使用 Telnet 打开 CLI。这些步骤适用于运行 Microsoft Windows 且带 Telnet 终端应用程序的计算机。查看计算机操作说明，了解适用于您的操作系统的详细说明。

1. 单击 Start (开始) > Programs (所有程序) > Accessories (附件) > Telnet

   如果 Telnet 不在 Accessories (附件) 菜单中，单击 Start (开始) > Run (运行)，在输入框输入 Telnet，然后按下回车键。
2. 当显示 Telnet 页面后，单击 Connect (连接)，选择 Remote System (远程系统)。
3. 在 Host Name (主机名称) 框中，输入无线设备 IP 地址，然后单击 Connect (连接)。
4. 在出现用户名和密码提示时，输入您的管理员用户名和密码。

   默认用户名为空，默认密码为 wirelessap。默认启用密码也是 wirelessap。用户名和密码区分大小写。

使用安全外壳打开 CLI

安全外壳协议是一种为联网设备提供安全远程连接的协议。安全外壳 (SSH) 是一个通过加密整个会话提供安全登录会话的软件包。 SSH 具有强加密验证、强加密和完整性保护功能。关于 SSH 的详细信息，请访问 SSH Communications Security, Ltd 的主页：http://www.ssh.com/。

当验证设备后， SSH 可通过强力加密提供比 Telnet 更出色的远程连接安全性。本版本支持 SSH 第 1 版和第 2 版。

关于设置无线设备进行 SSH 访问的详细说明，请参见第 243 页的 “ 配置接入点使用安全 外壳 ”。

使用 CLI 恢复默认设置

注意：在复位默认设置或重新加载软件之前，不得删除任何系统文件。

如果要将接入点恢复到默认设置，可使用以下命令。

```
write erase
erase startup-config
```

在特权 EXEC 模式下，可使用 CLI 根据以下步骤将接入点 / 网桥的配置恢复到出厂默认值：

1. 输入 `write erase` 或 `erase startup-config?`
2. 输入 `write default-config`。
3. 当出现下列 CLI 消息时，输入 `Y`：

   ```
   Erasing the nvram filesystem will remove all
   configuration files! Continue? [confirm].
   ```

4. 当出现下列 CLI 消息时输入 reload：

   ```
   Erase of nvram: complete. This command reloads the
   operating system.
   ```

5. 当出现下列 CLI 消息时，输入 `Y`：

   ```
   Proceed with reload? [confirm].
   ```

注意：避免损坏配置，不要中断启动过程。等待接入点 / 网桥安装模式状态指示灯开始闪烁绿色后，再执行 CLI 配置更改。

在接入点 / 网桥重启后，您可使用设备管理器或 CLI 重新配置接入点：

默认情况下，接入点被配置为从 DHCP 接收 IP 地址。要显示接入点 / 网桥的 IP 地址，可使用 `show interface bvi1` 命令。

安全 CLI 配置示例

本节中的示例显示了等效于使用 Security (安全性) 菜单中各种安全类型创建 SSID 的 CLI 命令。本节包含以下配置示例：

示例 1：无安全性

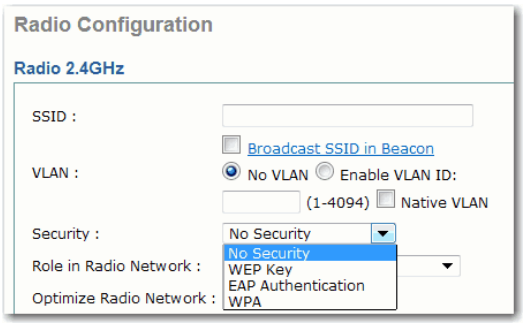
本例显示了一部分配置，使用 Security (安全性) 页面创建一个名为 `no_security_ssid` 的 SSID，将 SSID 包含在信标中，将其分配给 VLAN 10，并选择 VLAN 10 作为本征 VLAN。

提示　以下示例并不是完整配置，仅显示了配置在 CLI 中的样例。

```
!
dot11 ssid no_security_ssid
authentication open
VLAN 10 :
!
interface Dot11Radio1
 no ip address
 no ip route-cache
!
ssid no_security_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
```

```
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
```

关于设备管理器的说明，请参见第 62 页的 “ 配置安全 ”。



示例 2：使用 WPA 与预共享密钥 (WPA2-PSK)

本例显示了一部分配置，使用 Security (安全性) 页面创建一个名为 wpa2_psk_ssid 的 SSID。其操作是将 SSID 排除在信标外，将 SSID 分配给 VLAN 20, 使用预共享密钥与 AES 加密配置 WPA2 密钥管理。

```
ssid wpa2_psk_ssid
      VLAN 20 :
      authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 06345F2247590C48544541
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
encryption vlan 20 mode ciphers aes-ccm
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
```

```
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

   ssid wpa2_psk_ssid
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
encryption vlan 20 mode ciphers aes-ccm
 !
 ssid wpa2_psk_ssid
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.20
 encapsulation dot1Q 20
```

```
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
bridge-group 20 spanning-disabled
```

关于设备管理器的更多信息，请参见第 64 页的 “ 简易设置 — 网络配置 — 安全限制 ”。

示例 3：WPA 和 EAP

本例显示了一部分配置，使用 Security (安全性) 页面：

- 创建名为 wpa_ssid 的 SSID
- 配置 WPA 密钥管理与 EAP
- 从信标中排除 SSID
- 将 SSID 分配给 VLAN 40

```
dot11 ssid wpa_ssid
    VLAN 40 :
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
 !
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 40 mode ciphers tkip
 !
     ssid wpa_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
```

```
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
    ssid wpa_ssid
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
!
```

```
ip radius source-interface BVI1

radius-server host 10.91.104.92 auth-port 1645
acct-port 1646 key 7 091D1C5A4D5041

!
```

关于设备管理器的说明，请参见第 62 页的 “ 配置安全 ”。

使用 CLI 分配 IP 地址

当将无线设备连接到有线局域网时，无线设备将使用自动创建的网桥虚拟接口 (BVI) 链接到网络。网络将不追踪无线设备独立的 IP 地址、以太网和无线电端口，而是使用 BVI。

当使用 CLI 给无线设备分配 IP 地址时，必须给 BVI 分配地址。在特权 EXEC 模式下，根据以下步骤为无线设备 BVI 分配 IP 地址：

1. 进入全局配置模式，配置终端。

   ```
   configure terminal
   ```

2. 进入 BVI 的界面配置模式。

   ```
   interface bvil
   ```

3. 为 BVI 分配 IP 地址和地址掩码。

   ```
   ip address address mask
   ```

   提示 如果使用 Telnet 会话连接到无线设备，当给 BVI 分配新的 IP 地址时，将丢失到无线设备的连接。如果需要继续使用 Telnet 配置无线设备，使用新的 IP 地址打开另一个连接至无线设备的 Telnet 会话。

关于设备管理器的说明，请参见第 55 页的 “ 登录到接入点 ”。

使用 终端应用程序会话访问 CLI

根据以下步骤使用终端应用程序访问 CLI。这些步骤适用于运行 Microsoft Windows 且带 Telnet 终端应用程序的计算机。查看计算机操作说明，了解适用于您的操作系统的详细说明。

1. 单击 Start (开始) > Programs (所有程序) > Accessories (附件) > Telnet

   如果 Telnet 不在 Accessories (附件) 菜单中，单击 Start (开始) > Run (运行)，在输入框输入 Telnet，然后按下回车键。

2. 当显示 Telnet 页面后，单击 Connect (连接)，选择 Remote System (远程系统)。
3. 在 Host Name (主机名称) 框中，输入无线设备 IP 地址，然后单击 Connect (连接)。

提示 您还可使用终端程序，如 PuTTY。 PuTTY 是一种 SSH 和 telnet 客户端。可从 http://www.putty.org/ 下载应用程序。

配置 802.1X 请求者

按照惯例， `dot1x` 验证器 / 客户端关系始终分别是网络设备与个人计算机客户端的关系，因为个人计算机用户都必须进行验证，以获取网络访问权限。但是，无线网络为传统的验证器 / 客户端关系引入了独特的挑战。

首先，接入点可能位于公共场所，因此有可能被拔下，网络连接也可能被外部人员使用。其次，当中继器接入点被集成到无线网络中时，必须以与客户端相同的方式在根接入点上进行验证。

请求者分两个阶段进行配置：

- 创建和配置凭证配置文件
- 将凭证应用到接口或 SSID

您可以任意顺序完成这两个阶段，但必须在请求者运行之前完成配置。

创建凭证配置文件

在特权 EXEC 模式下，根据以下步骤创建 802.1X 凭证配置文件。

关于设备管理器的信息，请参见第 122 页的 “AP 验证 ”。

1. 进入全局配置模式，配置终端。

   ```
   configure terminal
   ```

2. 创建 dot1x 凭证配置文件，进入 dot1x 凭证配置子模式。

   ```
   dot1x credentials profile
   ```

3. 输入要使用的匿名身份。该操作是可选操作。

   ```
   anonymous-id description
   ```

4. (可选) 输入凭证配置文件的描述。

   ```
   description description
   ```

5. 输入身份验证用户 ID。

   ```
   username username
   ```

6. 输入凭证的未加密密码。
   - 0，后面跟随未加密密码。
   - 7，后面跟随隐藏密码。当应用之前保存的配置时，将使用隐藏密码。
   - LINE—— 未加密 (明文) 密码。未加密密码即明文密码。您可输入 0，后面跟明文密码，或省略 0 并输入明文密码。

   ```
   password {0 | 7 | LINE}
   ```

7. (可选，仅适用于 EAP-TLS) —— 输入默认的 pki-trustpoint。

   ```
   pki-trustpoint pki-trustpoint
   ```

8. 返回到特权 EXEC 模式。

   ```
   end
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running config startup-config
   ```

使用 dot1x creden 命令的 no 格式来否定参数。

下例创建了一个名为 *test* 的凭证配置文件，用户名为 *Rockwell*，未加密密码为 *wirelessap*。

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End
with CTRL-Z.
ap1240AG(config)# dot1x credentials test
ap1240AG(config-dot1x-creden)#username Rockwell
ap1240AG(config-dot1x-creden)#password wirelessap
ap1240AG(config-dot1x-creden)#exit
ap1240AG(config)#
```

将凭证配置文件应用到上行设备所使用的 SSID

如果在无线网络中有一个工作组网桥或中继器接入点，并在根接入点上使用 802.1X 请求者，则必须将 802.1X 请求者凭证应用到工作组网桥或中继器，用于关联和验证到根接入点的 SSID。

在特权 EXEC 模式下，根据以下步骤将凭证应用到上行设备所使用的 SSID。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入 802.11 SSID。

SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。第一个字符不能包含 !、# 或 ; 字符。字符 +、]、/、"、TAB 和结尾空格也是无效的 SSID 字符。

```
dot11 ssid ssid
```

3. 输入预配置凭证配置文件的名称。

   ```
   dot1x credentials profile
   ```

4. 退出 dot1x 凭证配置子模式

   ```
   end
   ```

5. 将您的输入保存到配置文件中。该操作是可选操作。

   ```
   copy running config startup-config
   ```

下列将凭证配置文件 test 应用到中继器接入点上的 `ssid testap1`。

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line. End
with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

创建和应用 EAP 方法配置文件

您可选择配置 EAP 方法列表，以便请求者识别特定的 EAP 方法。参见第 351 页的 “ 为 802.1X 请求者创建并应用 EAP 方法配置文件 ”。

管理 WAP 访问

本章介绍了如何管理无线设备。

禁用模式按钮

您可使用 [no] boot mode-button 命令，禁用带控制台端口的接入点的模式按钮。该命令可防止密码恢复，还可防止未授权的用户获得接入点 CLI 的访问权限。

重要事项　该命令禁用密码恢复。在输入该命令后，如果遗忘了接入点特权 EXEC 模式的密码，则需要联系 Cisco 技术支持中心 (TAC)，以重新获取对接入点 CLI 的访问。

默认情况下，模式按钮为启用状态。在特权 EXEC 模式下，根据以下步骤禁用接入点模式按钮。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 禁用接入点模式按钮。

   ```
   no boot mode-button
   ```

3. 不必保存配置。

   ```
   end
   ```

您可在特权 EXEC 模式下执行 show boot 或 show boot mode-button 命令，查看模式按钮的状态。该状态不出现在运行配置中。以下给出了 show boot 和 show boot mode-button 命令的典型响应。

```
ap#show boot
BOOT path-list: flash:/c1200-k9w7-mx-
v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
     buffer size: 32768

ap#show boot mode-button
on
ap#
```

只要知道特权 EXEC 密码，便可使用 boot mode-button 命令将模式按钮恢复到常规运行状态。

防止对接入点的未授权访问

您可防止未授权用户重新配置无线设备和查看配置信息。通常，您希望网络管理员有权访问无线设备，同时限制本地网络中通过终端或工作站连接的用户进行访问。

要防止对无线设备的未授权访问，可配置以下安全功能之一：

- 多组用户名和密码，它们保存在本地的无线设备上。用户需要输入这些用户名和密码才能访问无线设备。您也可为每个用户名和密码组分配特定的特权级别 (只读或读 / 写)。
- 默认用户名为空，默认密码为 `wirelessap`。用户名和密码区分大小写。
- 关于 CLI 的更多信息，请参见第 220 页的 “ 配置用户名和密码组合 ”。

  提示 TAB (制表符)、 ?、 $、 + 和 [属于无效的密码字符。

- 用户名和密码组集中保存在安全服务器的数据库中。

  更多信息，请参见第 223 页的 “ 通过 RADIUS 控制接入点访问 ”。

  更多信息，请参见第 62 页的 “ 配置安全 ”。

特权 EXEC 命令的访问保护

有一种简单的方法对网络中的终端进行访问控制，即使用密码并分配特权级别。密码保护可限制对网络或网络设备的访问。特权级别定义了用户登录网络设备后可发出哪些命令。

如需了解本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Security Command Reference for Release 12.3 (思科 IOS 安全命令参考，第 12.3 版)。

默认密码和特权级别配置

下表给出了默认密码和特权级别配置。

表 89 - 默认密码和特权级别

功能	默认设置
用户名和密码	默认用户名为空，默认密码为 *wirelessap*。
启用密码和特权级别	默认密码为 *wirelessap*。默认级别为 15 (特权 EXEC 级别)。密码在配置文件中经过加密。
启用密文密码和特权级别	默认启用密码为 *wirelessap*。默认级别为 15 (特权 EXEC 级别)。密码经加密后写入到配置文件中。
命令行密码	默认密码为 *wirelessap*。密码在配置文件中经过加密。

设置或更改静态启用密码

启用密码可控制对特权 EXEC 模式的访问。 `no enable password` 全局配置命令可删除启用密码，但使用该命令时要极其小心。如果删除了启用密码，则 EXEC 模式将被锁定。

在特权 EXEC 模式下，根据以下步骤设置或更改静态启用密码。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 定义用于访问特权 EXEC 模式的新密码或更改现有密码。

   ```
   enable password password
   ```

默认密码为 *wirelessap*。

对于 *password*，可指定 1...25 个字母数字字符组成的字符串。该字符串不能以数字开头，区分大小写，可使用空格，但会忽略前导空格。

提示　　TAB (制表符)、?、$、+ 和 [属于无效的密码字符。

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

启用密码未加密，且可读入到无线设备配置文件中。

本例介绍了如何将启用密码更改为 *l1u2c3k4y5*。该密码未加密，并提供对级别 15 的访问 (传统的特权 EXEC 模式访问)：

```
AP(config)# enable password l1u2c3k4y5
```

通过加密保护启用密码和启用密文密码

要提供附加的安全保护层级，特别是跨网络的密码或保存在简单文件传输协议 (TFTP) 服务器中的密码，您可使用 `enable password` 或 `enable secret` 全局配置命令。两种命令的作用相同，就是说您可创建一个加密密码，如果用户要访问特权 EXEC 模式 (默认) 或您指定的任何特权级别，就必须输入该密码。

建议使用 `enable secret` 命令，因为它使用了改进型加密算法。

如果配置了 `enable secret` 命令，其优先级将高于 `enable password` 命令，且两个命令无法同时起效。

在特权 EXEC 模式下，根据以下步骤配置启用密码和启用密文密码的加密。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 定义用于访问特权 EXEC 模式的新密码或更改现有密码。

   ```
   enable password [level level] {password |
   encryption-type encrypted-password}
   ```

   或

   ```
   enable secret [level level] {password | encryption-
   type encrypted-password}
   ```

   定义密文密码，其使用不可逆的加密方法进行保存。

   - (可选) `level` 的范围为 0 至 15。级别 1 是常规用户 EXEC 模式特权。默认级别为 15 (特权 EXEC 模式特权)。
   - 对于 `password`，可指定 1...25 个字母数字字符组成的字符串。该字符串不能以数字开头，区分大小写，可使用空格，但会忽略前导空格。默认情况下未定义密码。
   - (可选) 对于 `encryption-type`，仅提供类型 5，即思科专有加密算法。如果您要指定加密类型，则必须提供加密密码 —— 即从另一个接入点配置中复制的加密密码。

     提示 如果指定了加密类型，则输入明文密码时，将无法重新进入特权 EXEC 模式。您无法使用任何方法恢复丢失的加密密码。

3. (可选) 在定义密码时或写配置文件时加密密码。

   ```
   service password-encryption
   ```

   加密可防止配置文件中的密码被读取。

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

如果启用密码和启用密文密码都已定义，用户必须输入启用密文密码。

使用 `level` 关键字定义特定特权级别的密码。在指定级别并设定密码后，只将密码给予需要访问该级别的用户。使用 `privilege level` 全局配置命令指定各级别可访问的命令。更多信息，请参见第 222 页的 “ 配置多个特权级别 ”。

如果启用了密码加密，则将应用到所有密码，包括用户名密码、验证密钥密码、特权命令密码以及控制台及虚拟终端命令行密码。

- 要消除密码和级别，使用 `no enable password [level level]` 或 `no enable secret [level level]` 全局配置命令。
- 要禁用密码加密，使用 `no service password-encryption` 全局配置命令。

本例说明了如何为特权级别 2 配置加密密码 *1FaD0$Xyti5Rkls3LoyxzS8*：

```
AP(config)# enable secret level 2 5
$1$FaD0$Xyti5Rkls3LoyxzS8
```

配置用户名和密码组合

您可配置多组用户名和密码，它们保存在本地的无线设备上。这些用户名和密码会被分配给命令行或接口，用户需要输入它们后才能访问无线设备。如果定义了特权级别，您还可为每组用户名和密码分配特定的特权级别 (及相关权限和特权)。

在特权 EXEC 模式下，根据以下步骤创建需要登录用户名和密码且基于用户名的验证系统。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入每个用户的用户名、特权级别和密码。

   ```
   username name [privilegelevel] {password
   encryption-type password}
   ```

- 对于 name，指定一个单词作为用户 ID。不允许使用空格和引号。
- (可选) 对于 level，指定获得访问权限后拥有的特权级别。其范围为 0...15。

  级别 15 赋予特权 EXEC 模式访问权限。级别 1 赋予用户 EXEC 模式访问权限。
- 对于 encryption-type，输入 0 即指定在后面添加一个不加密密码。
- 输入 7 即指定后面添加一个隐藏密码。
- password 用于指定用户要访问无线设备前必须输入的密码。

  密码必须由 1...25 个字符组成，中间可加入空格，且必须是 username 命令中的最后一个指定选项。

3. 启用登录时执行本地密码检查。根据第 2 步中指定的用户名进行验证。

   ```
   login local
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要禁用特定用户的用户名验证，可使用 no username name 全局配置命令。
- 要禁用密码检查且允许无密码连接，使用 no login 命令行配置命令。

提示 您必须至少配置一个用户名，且必须已设置 login local 命令，以打开到无线设备的 Telnet 会话。如果没有输入唯一的用户名，您可能会被锁定在无线设备之外。

配置多个特权级别

默认情况下，思科 IOS 软件有两种密码安全性模式：用户 EXEC 和特权 EXEC。每种模式最多可配置 16 个层级的命令。通过配置多个密码，您可允许不同用户组分别访问特定的命令。

例如，如果希望许多用户都可访问 `clear line` 命令，可分配级别 2 安全性，然后将级别 2 密码广泛分配给这些用户。但如果希望严格限制对 `configure` 命令的访问，可为其分配级别 3 安全性，只将该密码分配给有限的用户组。

设置命令的特权级别

在特权 EXEC 模式下，根据以下步骤为命令模式设置特权级别。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 设置命令的特权级别。
   - 对于 *mode*，输入 `configure` 表示全局配置模式，输入 `exec` 表示 EXEC 模式，输入 `interface` 表示接口配置模式，或输入 `line` 表示命令行配置模式。
   - *level* 的范围为 0...15。级别 1 是常规用户 EXEC 模式特权。级别 15 是**启用**密码所允许的访问级别。
   - *command* 用于指定您想要限制访问的命令。

   ```
   privilege mode level level command
   ```

3. 指定特权级别的启用密码。

- *level* 的范围为 0...15。级别 1 是常规用户 EXEC 模式特权。
- 对于 *password*，可指定 1...25 个字母数字字符组成的字符串。该字符串不能以数字开头，区分大小写，可使用空格，但会忽略前导空格。默认情况下未定义密码。

提示　TAB (制表符)、?、$、+ 和 [属于无效的密码字符。

```
enable password level level password
```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   第一条命令提供密码和访问级别配置。第二条命令提供特权级别配置。

   ```
   show running-config
   ```

   或

   ```
   show privilege
   ```

6. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

当为某条命令设置特权级别时，语法是该命令子集的所有命令都将被设为该级别。例如，如果将 `show ip route` 命令设为级别 15，则 `show` 命令和 `show ip` 命令将被自动设为特权级别 15，除非单独为其设置不同的级别。

要将给定的命令恢复到默认的特权，可使用 `no privilege` *`mode`* `level` *`level command`* 全局配置命令。

本例介绍了如何给 `configure` 命令设置特权级别 14，并定义 *`SecretPswd14`* 作为密码，而用户必须输入该密码才能使用级别 14 命令：

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

登录和退出特权级别

在特权 EXEC 模式下，根据以下步骤登录和退出特定的特权级别：

1. 登录特定的特权级别。

   level 的范围为 0...15。

   ```
   enable level
   ```

2. 退出特定的特权级别。

   level 的范围为 0...15。

   ```
   disable level
   ```

通过 RADIUS 控制接入点访问

本节介绍了如何使用远程验证拨号用户服务 (RADIUS) 控制管理员对无线设备的访问。关于配置无线设备使其支持 RADIUS 的完整说明，请参见第 377 页的 “ 配置 RADIUS 和 TACACS+ 服务器 ”。

RADIUS 在验证和授权过程中提供详细的结算信息和灵活的管理控制。RADIUS 可通过 AAA 命令加速，同时只能通过 AAA 命令启用。

如需了解本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Security Command Reference for Release 12.3 (思科 IOS 安全命令参考，第 12.3 版)。

默认配置

默认情况下， RADIUS 和 AAA 被禁用。

为防止安全性失效，您不可使用 SNMP 通过网络管理应用程序配置 RADIUS。启用后， RADIUS 可验证通过 CLI 或 HTTP (设备管理器) 访问无线设备的管理员。

配置 RADIUS 登录验证

要配置 AAA 验证，您可定义一个命名验证方法列表，然后将该列表应用到不同接口。方法列表定义验证类型以及执行的顺序；要让定义的验证方法得以执行，必须先将其应用到特定的接口。唯一的例外是默认方法列表。除了已经过明确定义的命名方法列表，默认的方法列表将自动应用到所有其他接口。

方法列表描述了验证用户时的顺序以及调用的验证方法。您可指定一个或多个安全性协议用于验证，从而确保当初始方法失败时可使用备用验证系统。软件使用列出的第一种方法来验证用户；如果该方法未能响应，软件将选择列表中的第二种验证方法。

该过程将持续，直至通过所列验证方法顺利通信，或者定义的所有方法都被排除。如果验证在该循环的任一点失败 —— 即安全服务器或本地用户名数据库拒绝用户访问 —— 验证过程将停止，且不再尝试其他验证方法。

在特权 EXEC 模式下，根据以下步骤配置登录验证。该过程必须执行。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 创建登录验证方法列表。

   ```
   aaa authentication login {default | list-name}
   method1 [method2...]
   ```

   - 当 `login authentication` 命令中没有指定命名列表时，如果要创建默认列表，可使用 default 关键字，**并在后面输入默认情况下使用的方法。**默认方法列表将自动应用到所有接口。
   - *`list-name`* 用于指定一个字符串，以命名刚创建的列表。
   - *`method1`*... 用于指定验证算法尝试使用的方法。附加验证方法仅在前一种方法返回错误时才会使用 (而不是失败)。

选择以下其中一种方法：

- 本地

  使用本地用户名数据库进行验证。您必须将用户名信息输入到数据库中。使用 `username password` 全局配置命令。

- `radius`

  使用 RADIUS 验证。在使用该验证方法之前，您必须先配置 RADIUS 服务器。更多信息，请参见第 380 页的 “ 识别 RADIUS 服务器主机 ”。

4. 进入命令行配置模式，应用验证列表。

   `line [console | tty | vty] line-number [ending-line-number]`

5. 将验证列表应用到命令行或命令行组。
   - 如果指定了 `default`，则将使用通过 `aaa authentication login` 命令创建的默认列表。
   - *`list-name`* 指定通过 `aaa authentication login` 命令创建的列表。

   `login authentication {default | list-name}`

6. 返回到特权 EXEC 模式。

   `end`

7. 确认您的输入。

   `show running-config`

8. (可选) 将您的输入保存到配置文件中。

   `copy running-config startup-config`

- 要禁用 AAA，使用 `no aaa new-model` 全局配置命令。
- 要禁用 AAA 验证，使用 `no aaa authentication login {default | list-name} method1 [method2...]` 全局配置命令。
- 要禁用登录时的 RADIUS 验证或返回到默认值，使用 `no login authentication {default | list-name}` 命令行配置命令。

定义 AAA 服务器组

您可配置无线设备来使用 AAA 服务器组，将现有服务器主机集合在一起进行验证。您可选择一个已配置服务器主机的子集，然后将它们用于特定的服务。服务器组使用全局服务器主机列表，其中包含所选服务器主机的 IP 地址。

如果服务器的每个主机条目有唯一的标识符 (IP 地址和 UDP 端口号组合)，则服务器组也可包含同一服务器的多个主机条目，从而将不同的端口单独定义为提供特定的 AAA 服务的 RADIUS 主机。如果在同一 RADIUS 服务器上为相同服务 (例如，结算) 配置了两个不同的主机条目，则配置的第二个主机条目将作为第一个条目的故障切换备用条目。

您可使用 `server` 组服务器配置命令将特定服务器关联到已定义的服务器组。您可通过 IP 地址识别服务器，也可使用可选的 `auth-port` 和 `acct-port` 关键字识别多个主机实例或条目。

在特权 EXEC 模式下，根据以下步骤定义 AAA 服务器组，并将特定的 RADIUS 服务器与之关联。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 指定远程 RADIUS 服务器主机的 IP 地址或主机名称。

   ```
   radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
   ```

   - (可选) 使用 `auth-port port-number` 指定验证请求的 UDP 目标端口。
   - (可选) 使用 `acct-port port-number` 指定结算请求的 UDP 目标端口。
   - (可选) 使用 `timeout seconds` 指定无线设备在重新发送之前等待 RADIUS 服务器回复的时间间隔。其范围为 1...1000。该设置将忽略 `radius-server timeout` 全局配置命令设置。如果未使用 `radius-server host` 命令设置超时，将使用 `radius-server timeout` 命令的设置。
   - (可选) 使用 `retransmit retries` 指定当服务器未响应或响应迟缓时，重新向服务器发送 RADIUS 请求的次数。其范围为 1...1000。如果未使用 `radius-server host` 命令设置重新发送值，则将使用 `radius-server retransmit` 全局配置命令的设置。

- (可选) 使用 `key string` 指定无线设备和 RADIUS 服务器上运行的 RADIUS daemon 之间使用的验证和加密密钥。

  提示 密钥属于文本字符串，它必须与 RADIUS 服务器上使用的加密密钥相匹配。始终将密钥配置为 radius-server host 命令的最后一项。前导空格将被忽略，但密钥中间和末尾可使用空格。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

要配置无线设备来识别与单个 IP 地址关联的多个主机条目，可在必要时多次输入该命令，确保每个 UDP 端口号各不相同。无线设备软件将根据您指定的顺序搜索主机。设置特定 RADIUS 主机使用的超时、重新发送和加密密钥值。

4. 使用一个组名定义 AAA 服务器组。

   该命令将无线设备置于服务器组配置模式。

   ```
   aaa group server radius group-name
   ```

5. 将特定 RADIUS 服务器关联到定义的服务器组。对 AAA 服务器组中的每个 RADIUS 服务器重复该步骤。

   组中的每个服务器都必须在步骤 2 中预先定义。

   ```
   server ip-address
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. 确认您的输入。

   ```
   show running-config
   ```

8. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

9. 启用 RADIUS 登录验证。

   更多信息，请参见第 224 页的 “ 配置 RADIUS 登录验证 ”。

   - 要删除指定的 RADIUS 服务器，使用 `no radius-server host hostname | ip-address` 全局配置命令。
   - 要从配置列表中删除服务器组，使用 `no aaa group server radius group-name` 全局配置命令。
   - 要删除 RADIUS 服务器的 IP 地址，使用 `no server ip-address` 服务器组配置命令。

在本例中，将无线设备配置为识别两组不同的 RADIUS 组服务器 (*group1* 和 *group2*)。 Group1 在同一 RADIUS 服务器上有两个配置了相同服务的不同主机条目。第二个主机条目作为第一个条目的故障切换备用条目。

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646

AP(config)# aaa group server radius group1

AP(config-sg-radius)# server 172.20.0.1 auth-port
1000 acct-port 1001

AP(config-sg-radius)# exit

AP(config)# aaa group server radius group2

AP(config-sg-radius)# server 172.20.0.1 auth-port
2000 acct-port 2001

AP(config-sg-radius)# exit
```

配置用户特权访问和网络服务的 RADIUS 授权

使用 AAA 授权限制提供给用户的服务。启用 AAA 授权后，无线设备使用用户配置文件 (保存在本地用户数据库或安全服务器中) 中提取的信息来配置用户会话。当用户配置文件中的信息允许时，用户被授予访问所请求服务的权限。

您可使用 `aaa authorization` 全局配置命令以及 `radius` 关键字设置相关参数，限制用户网络访问特权 EXEC 模式。

`aaa authorization exec radius local` 命令用于设置这些授权参数。

- 如果已使用 RADIUS 执行验证，则使用 RADIUS 进行特权 EXEC 访问验证。
- 如果未使用 RADIUS 执行验证，则使用本地数据库。

提示　对于已通过 CLI 登录的验证用户，即使配置过授权，也会绕过授权。

在特权 EXEC 模式下，根据以下步骤为特权 EXEC 访问和网络服务指定 RADIUS 授权：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置无线设备，对所有网络相关服务请求执行用户 RADIUS 授权。

   ```
   aaa authorization network radius
   ```

3. 配置无线设备执行用户 RADIUS 授权，确定用户是否有特权 EXEC 访问权限。

   `exec` 关键字可返回用户配置文件信息 (例如， `autocommand` 信息)。

   ```
   aaa authorization exec radius
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

   要禁用授权，使用 `no aaa authorization {network | exec} method1` 全局配置命令。

显示 RADIUS 配置

要显示 RADIUS 配置，使用 `show running-config` 特权 EXEC 命令。

使用 TACACS+ 控制接入点访问

本节介绍了如何使用终端访问控制器访问控制系统加强版 (TACACS+) 控制管理员对无线设备的访问。

关于配置无线设备使其支持 TACACS+ 的完整说明，请参见第 377 页的 “ 配置 RADIUS 和 TACACS+ 服务器 ”。

TACACS+ 在验证和授权过程中提供详细的结算信息和灵活的管理控制。TACACS+ 可通过 AAA 命令加速，同时只能通过 AAA 命令启用。

如需了解本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Security Command Reference for Release 12.3 (思科 IOS 安全命令参考，第 12.3 版)。

默认配置

默认情况下， TACACS+ 和 AAA 被禁用。

为防止安全性失效，您不可使用 SNMP 通过网络管理应用程序配置 TACACS+。启用后， TACACS+ 可验证通过 CLI 或 HTTP (设备管理器) 访问无线设备的管理员。

配置 TACACS+ 登录验证

要配置 AAA 验证，您可定义一个命名验证方法列表，然后将该列表应用到不同接口。方法列表定义执行的验证类型以及执行顺序；要让定义的验证方法得以执行，必须先将其应用到特定的接口。

唯一的例外是默认方法列表。除了已经过明确定义的命名方法列表，默认的方法列表将自动应用到所有其他接口。定义的方法列表将优先于默认方法列表。

方法列表描述了验证用户时的顺序以及调用的验证方法。您可指定一个或多个安全性协议用于验证，从而确保当初始方法失败时可使用备用验证系统。软件使用列出的第一种方法来验证用户；如果该方法失败，软件将选择列表中的第二种验证方法。

该过程将持续，直至通过所列验证方法顺利通信，或者定义的所有方法都被排除。如果验证在该循环的任一点失败 —— 即安全服务器或本地用户名数据库拒绝用户访问 —— 验证过程将停止，且不再尝试其他验证方法。

在特权 EXEC 模式下，根据以下步骤配置登录验证。该过程必须执行。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 创建登录验证方法列表。

   ```
   aaa authentication login {default | list-name}
   method1 [method2...]
   ```

   - 当 `login authentication` 命令中**没有**指定命名列表时，如果要创建默认列表，可使用 default 关键字，**并在后面输入默认情况下使用的方法**。默认方法列表将自动应用到所有接口。
   - *`list-name`* 用于指定一个字符串，以命名刚创建的列表。
   - *`method1...`* 用于指定验证算法尝试使用的方法。附加验证方法仅在前一种方法返回错误时才会使用 (而不是失败)。

   选择以下其中一种方法：

   - 本地

     使用本地用户名数据库进行验证。您必须将用户名信息输入到数据库中。使用 `username` *`password`* 全局配置命令。

   - `tacacs+`

     使用 TACACS+ 验证。在使用该验证方法之前，您必须先配置 TACACS+ 服务器。

4. 进入命令行配置模式，应用验证列表。

   ```
   line [console | tty | vty] line-number [ending-
   line-number]
   ```

5. 将验证列表应用到命令行或命令行组。
   - 如果指定了 `default`，则将使用通过 `aaa authentication login` 命令创建的默认列表。
   - *list-name* 指定通过 `aaa authentication login` 命令创建的列表。

   ```
   login authentication {default | list-name}
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. 确认您的输入。

   ```
   show running-config
   ```

8. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要禁用 AAA，使用 `no aaa new-model` 全局配置命令。
- 要禁用 AAA 验证，使用 `no aaa authentication login {default | list-name} method1 [method2...]` 全局配置命令。
- 要禁用登录时的 TACACS+ 验证或返回到默认值，使用 `no login authentication {default | list-name}` 命令行配置命令。

配置特权 EXEC 访问和网络服务的 TACACS+ 授权

使用 AAA 授权限制提供给用户的服务。启用 AAA 授权后，无线设备使用用户配置文件 (保存在本地用户数据库或安全服务器中) 中提取的信息来配置用户会话。当用户配置文件中的信息允许时，用户被授予访问所请求服务的权限。

您可使用 `aaa authorization` 全局配置命令以及 `tacacs+` 关键字设置相关参数，限制用户网络访问特权 EXEC 模式。

`aaa authorization exec tacacs+ local` 命令用于设置这些授权参数。

- 如果已使用 TACACS+ 执行验证，则使用 TACACS+ 进行特权 EXEC 访问验证。
- 如果未使用 TACACS+ 执行验证，则使用本地数据库。

提示　对于已通过 CLI 登录的验证用户，即使配置过授权，也会绕过授权。

在特权 EXEC 模式下，根据以下步骤为特权 EXEC 访问和网络服务指定 TACACS+ 授权：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置无线设备，对所有网络相关服务请求进行用户 TACACS+ 授权。

   ```
   aaa authorization network tacacs+
   ```

3. 配置无线设备进行用户 TACACS+ 授权，确定用户是否有特权 EXEC 访问权限。

   `exec` 关键字可返回用户配置文件信息 (例如， `autocommand` 信息)。

   ```
   aaa authorization exec tacacs+
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要禁用授权，使用 `no aaa authorization {network | exec} method1` 全局配置命令。

显示 TACACS+ 配置

要显示 TACACS+ 服务器统计数据，可使用 `show tacacs` 特权 EXEC 命令。

配置以太网速度和双工设置

您可为无线设备分配以太网端口速度和双工设置。我们建议您为无线设备以太网端口的速度和双工设置都使用默认设置 `auto`。当无线设备从交换机接收内部电源时，如果对速度或双工设置的更改会重置以太网链路，则将重启无线设备。

如果未将连接无线设备的交换机端口设置为 `auto`，您可将无线设备端口更改为 `half` 或 `full`，以纠正双工不匹配，这样便不会重置以太网链路。但是，如果从 `half` 或 `full` 改回 `auto`，链路将被重置；如果无线设备从交换机接收内部电源，无线设备将重启。

重要事项	无线设备以太网端口的速度和双工设置必须与连接无线设备的端口的以太网设置相匹配。 如果更改了连接无线设备的端口的设置，也必须更改无线设备以太网端口设置，以使两者相匹配。

默认情况下，以太网速度和双工被设为 auto。在特权 EXEC 模式下，根据以下步骤配置以太网速度和双工。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入配置接口模式。

   ```
   interface gigabitEthernet0
   ```

3. 配置以太网速度。我们建议您**使用默认设置** auto。

   ```
   speed {10 | 100 | 1000 | auto}
   ```

4. 配置双工设置。我们建议您**使用默认设置** auto。

   ```
   duplex {auto | full | half}
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. 确认您的输入。

   ```
   show running-config
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

为本地验证和授权配置接入点

您可将无线设备配置为以本地模式执行 AAA，以无服务器的方式运行 AAA。无线设备随后处理验证和授权。在该配置中，没有提供结算功能。

提示　您可将无线设备配置为 802.1x 客户端设备的本地验证器，作为主服务器的备用设备，或者在没有 RADIUS 服务器的网络上提供验证服务。

关于如何将无线设备配置为本地验证器的详细说明，请参见第 307 页的 " 将接入点配置为本地验证器 "。

在特权 EXEC 模式下，根据以下步骤配置无线设备为本地 AAA。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 设置登录验证，使用本地用户名数据库。

   default 关键字将本地用户数据库验证应用到所有接口。

   ```
   aaa authentication login default local
   ```

4. 配置用户 AAA 授权，通过检查本地数据库确定是否允许用户运行 EXEC 外壳。

   ```
   aaa authorization exec local
   ```

5. 配置与网络相关的所有服务请求的用户 AAA 授权。

   ```
   aaa authorization network local
   ```

6. 进入本地数据库，建立基于用户名的验证系统。

   对每个用户重复该命令。

   - 对于 *name*，指定一个单词作为用户 ID。不允许使用空格和引号。
   - (可选) 对于 *level*，指定获得访问权限后拥有的特权级别。范围为 0...15。级别 15 赋予特权 EXEC 模式访问权限。级别 0 赋予用户 EXEC 模式访问权限。
   - 对于 *encryption-type*，输入 0 即指定在后面添加一个不加密密码。输入 7 即指定后面添加一个隐藏密码。
   - *password* 用于指定用户要访问无线设备前必须输入的密码。密码必须由 1...25 个字符组成，中间可加入空格，且必须是 username 命令中的最后一个指定选项。

   提示 TAB (制表符)、?、$、+ 和 [属于无效的密码字符。

   ```
   username name [privilegelevel] {password
   encryption-type password}
   ```

7. 返回到特权 EXEC 模式。

   ```
   end
   ```

8. 确认您的输入。

   ```
   show running-config
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要禁用 AAA，使用 no aaa new-model 全局配置命令。要禁用授权，使用 no aaa authorization {network | exec} *method1* 全局配置命令。

配置验证缓存和配置文件

使用验证缓存和配置文件功能，接入点可为用户缓存验证 / 授权响应，这样便不需要向 AAA 服务器发送后续的验证 / 授权请求。

提示　在接入点上，仅管理员验证支持该功能。

在思科 IOS 版本 12.3(7) 及更高版本中，下列命令支持该功能：

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

关于思科 IOS 命令 CLI 列表，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide (思科 Aironet 接入点和网桥思科 IOS 命令参考手册)。

下面是一个配置实例，接入点被配置为在启用验证缓存的情况下使用 TACACS+ 进行管理员验证。该实例基于 TACACS 服务器，但可将接入点配置为使用 RADIUS 进行管理员验证：

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7
01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port
1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache
tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache
tac_admin group tac_admin
aaa accounting network acct_methods start-stop
group rad_acct
```

```
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-
11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/
779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7
```

```
105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req
format %h
radius-server host 192.168.134.229 auth-port 1645
acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

配置接入点提供 DHCP 服务

默认情况下，接入点被配置为从网络中的 DHCP 服务器接收 IP 设置。您还可将接入点配置为用作 DHCP 服务器，为有线和无线局域网设备分配 IP 设置。

提示　如果将接入点配置为 DHCP 服务器，则其将为子网中的设备分配 IP 地址。子网中的设备可与其他设备通信，但无法跨子网通信。如果需要跨子网传送数据，则必须分配一个默认路由器。默认路由器的 IP 地址必须与作为 DHCP 服务器的接入点处于相同子网中。

关于与 DHCP 命令和选项相关的命令的详细信息，请参见 Configuring DHCP in the Cisco IOS IP Configuration Guide, Release 12.3 (思科 IOS IP 配置中 DHCP 配置指南，第 12.3 版)。

设置 DHCP 服务器

在特权 EXEC 模式下，根据以下步骤将接入点配置为提供 DHCP 服务，并指定默认路由器。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 从无线设备分配的地址范围中排除无线设备 IP 地址。分四组字符输入 IP 地址，例如， 10.91.6.158。

   无线设备假定 DHCP 地址池子网中的所有 IP 地址都可用于分配给 DHCP 客户端。您必须指定 DHCP 服务器不得分配给客户端的 IP 地址。

   (可选) 要输入排除地址范围，先输入范围下限地址，后面紧跟范围上限地址。

   ```
   ip dhcp excluded-address low_address [ high_address ]
   ```

3. 针对无线设备为响应 DHCP 请求分配的 IP 地址池创建一个名称，并进入 DHCP 配置模式。

   ```
   ip dhcp pool pool_name
   ```

4. 为地址池分配子网编号。无线设备分配该子网中的 IP 地址。

   (可选) 为地址池分配子网掩码，或指定比较地址前缀的位数。前缀是另一种分配网络掩码的方式。前缀长度必须以斜杠 (/) 作为前导字符。

   ```
   network subnet_number
   [ mask | prefix-length ]
   ```

5. 配置由无线设备分配的 IP 地址的租期时长。
   - 天数，配置租期时长天数
   - (可选) 小时数，配置租期时长小时数
   - (可选) 分钟数，配置租期时长分钟数
   - 无限，将租期时长设置为无限长

   ```
   lease { days [ hours ] [ minutes ] | infinite }
   ```

6. 指定子网中 DHCP 客户端的默认路由器的 IP 地址。至少需要一个 IP 地址；但最多可在一个命令行中指定八个地址。

   ```
   default-router address [address2 ... address 8]
   ```

7. 返回到特权 EXEC 模式。

   ```
   end
   ```

8. 确认您的输入。

   ```
   show running-config
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用这些命令的 no 形式恢复到默认设置。

本例描述了如何将无线设备配置为 DHCP 服务器、排除一个 IP 地址范围并分配默认路由器：

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1
172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

监视和维护 DHCP 服务器接入点

您可使用 show 和 clear 命令监视和维护 DHCP 服务器接入点。

show 命令

在 Exec 模式下，输入本表中的命令，显示作为 DHCP 服务器的无线设备的信息。

表 90 - 显示 DHCP 服务器命令

命令	用途
show ip dhcp conflict [*address*]	在特定 DHCP 服务器中记录的所有地址冲突列表。输入无线设备 IP 地址，显示无线设备记录的冲突。
show ip dhcp database [*url*]	提供 DHCP 数据库的最近活动。 可在特权 EXEC 模式下使用该命令。
show ip dhcp server statistics	提供关于服务器统计数据和收发消息的计数信息。

clear 命令

在特权 EXEC 模式下，使用本表中的命令清除 DHCP 服务器变量。

表 91 - 清除 DHCP 服务器命令

命令	用途
clear ip dhcp binding { *address* | * }	删除从 DHCP 数据库绑定的自动地址。指定该地址参数可清除特定 (客户端) IP 地址的自动绑定。指定一个星号 (*) 可清除所有自动绑定。
clear ip dhcp conflict { *address* | * }	从 DHCP 数据库中清除地址冲突。指定该地址参数可清除特定 IP 地址的冲突。指定一个星号 (*) 可清除所有地址的冲突。
clear ip dhcp server statistics	将所有 DHCP 服务器计数器复位为 0。

调试命令

要启用 DHCP 服务器调试，可在特权 EXEC 模式下使用此命令：

```
debug ip dhcp server { events | packets | linkage }
```

使用命令的 no 形式禁用无线设备 DHCP 服务器的调试。

配置接入点使用安全外壳

本节介绍了如何配置安全外壳 (SSH) 功能。

如需了解本节中使用的命令的完整语法和用法信息，请参见 Cisco IOS Security Command Reference for Release 12.3 *(* 思科 IOS 安全命令参考，第 12.3 版 *)* 中的安全外壳命令。

了解 SSH

SSH 是一种协议，提供到第 2 层或第 3 层设备的安全远程连接。SSH 有两个版本：SSH 第 1 版和 SSH 第 2 版。该版软件同时支持两种 SSH 版本。如果未指定版本号，接入点默认使用第 2 版。

当验证设备后， SSH 可通过强力加密提供比 Telnet 更出色的远程连接安全性。SSH 功能包括一个 SSH 服务器和一个 SSH 集成客户端。客户端支持以下用户验证方式：

- RADIUS

  参见第 223 页的 “ 通过 RADIUS 控制接入点访问 ”。

- 本地验证和授权

  参见第 234 页的 “ 为本地验证和授权配置接入点 ”。

配置 SSH

关于配置 SSH 和显示 SSH 设置的完整信息，请参见以下出版物：

- Cisco IOS Security Configuration Guide for Release 12.3 (思科 IOS 安全配置指南 (版本 12.3))
- 在运行思科 IOS 的路由器和交换器上配置安全外壳

配置客户端 ARP 缓存

您可配置无线设备，使其为相关客户端设备保留 ARP 缓存。在无线设备上保留 ARP 缓存可减轻无线局域网上的通信负载。默认情况下， ARP 缓存被禁用。

在无线设备上保留 ARP 缓存可停止无线设备中客户端设备的 ARP 请求，从而减轻无线局域网上的通信负载。无线设备不向客户端设备转发 ARP 请求，而是代表关联客户端设备响应请求。

当禁用 ARP 缓存后，无线设备通过无线电端口将所有 ARP 请求转发到关联客户端，并由客户端给出响应。当启用 ARP 缓存后，无线设备响应关联客户端的 ARP 请求，而不将请求转发到客户端。当无线设备接收到不属于缓存中的 IP 地址的 ARP 请求时，无线设备将丢弃该请求，也不转发该请求。在其信标中，无线设备包括一个信息元素，用于提醒客户端设备可安全忽略广播消息，从而延长电池寿命。

可选 ARP 缓存

如果客户端设备关联的是非思科设备接入点，也不传递数据，则无线设备无法知晓客户端 IP 地址。如果您的无线局域网中经常出现这种情况，您可启用可选 ARP 缓存。当 ARP 缓存为可选时，无线设备代表客户端进行响应 (无线设备已知晓 IP 地址)，但对于指向未知客户端的任何 ARP 请求，将通过其无线电端口进行转发。当无线设备知道所有关联客户端的 IP 地址时，它将丢弃不是指向其关联客户端的 ARP 请求。

配置 ARP 缓存

在特权 EXEC 模式下，根据以下步骤配置无线设备为关联客户端保留 ARP 缓存：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 在无线设备上启用 ARP 缓存。
   - (可选) 仅对无线设备已知其 IP 地址的客户端设备使用 `optional` 关键字启用 ARP 缓存。

   ```
   dot11 arp-cache [ optional ]
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

本例显示了如何在接入点配置 ARP 缓存：

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

管理系统时间和日期

您可使用简单网络时间协议 (SNTP) 自动管理无线设备上的系统时间和日期，或在无线设备上手动设置时间和日期。

关于本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference (思科 IOS 配置基本命令参考和思科 IOS IP 和 IP 路由命令参考)。

简单网络时间协议 (SNTP) 是一种仅限于客户端的简化型 NTP。SNTP 只能从 NTP 服务器接收时间；它无法用于为其他系统提供时间服务。SNTP 通常可提供与准确时间不超过 100 毫秒误差的时间，但不提供 NTP 的复杂过滤和统计机制。

您可配置 SNTP 向配置的服务器请求并接受数据包，或接受任何来源的 NTP 广播数据包。当有多个来源发送 NTP 数据包时，将选用最佳层级的服务器。

如果多个服务器具有相同的层级，将优先选用配置的服务器，而不是广播服务器。如果多个服务器同时满足这两项标准，则将选用第一个发送时间数据包的服务器。如果 SNTP 停止从当前选择的服务器上接收数据包，或发现更优的服务器 (根据以上标准)，则将只选择新的服务器。

配置 SNTP

默认情况下禁用 SNTP。要在接入点上启用 SNTP，可在全局配置模式下使用以下命令中的一种或两种同时使用：

表 92 - SNTP 命令

命令	用途
`sntp server {address | hostname} [version number]`	配置 SNTP，从 NTP 服务器请求 NTP 数据包。
`sntp broadcast client`	配置 SNTP，接受来自任何 NTP 广播服务器的 NTP 数据包。

为每个 NTP 服务器输入 `sntp server` 命令一次。必须将 NTP 服务器配置为响应来自接入点的 SNTP 消息。

如果您同时输入 `sntp server` 命令和 `sntp broadcast client` 命令，则接入点将接受广播服务器的时间，而不是配置的服务器的时间 (假如两个服务器的层级相同)。要显示关于 SNTP 的信息，可使用 `show sntp` EXEC 命令。

手动配置时间和日期

如果没有其他时间源，您可在系统重启后手动配置时间和日期。在下一次重启系统之前，时间将保持精确。我们建议您仅将手动配置作为最后的手段。如果有供无线设备同步的外部源，则无需手动设置系统时钟。

设置系统时钟

如果网络上有提供时间服务的外部源，例如， NTP 服务器，则无需手动设置系统时钟。

在特权 EXEC 模式下，根据以下步骤设置系统时钟。

1. 可使用以下格式之一手动设置系统时钟：
   - 使用 `hh:mm:ss` 按小时 (24 小时制)、分钟和秒钟格式指定时间。指定的时间相对于配置的时区。
   - 使用 `day` 指定月中日期。
   - 使用 `month` 指定月份。
   - 使用 `year` 指定年份 (无缩写)。

   `clock set hh:mm:ss day month year`

   或

   `clock set hh:mm:ss month day year`

2. 确认您的输入。

   ```
   show running-config
   ```

3. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

本例给出了如何将系统时钟手动设置为 2001 年 7 月 23 日，下午 1:32。

```
AP# clock set 13:32:00 23 July 2001
```

显示时间和日期配置

要显示时间和日期配置，使用 `show clock [detail]` 特权 EXEC 命令。

系统时钟将保留一个权威标志，显示时间是否为权威时间 (即精确时间)。如果系统时钟是通过定时源 (例如， NTP) 设置的，则将设置该标志。如果时间不是权威时间，则仅作为参考显示。在时钟显示权威时间并设置权威标志之前，当对等方的时间无效时，标志会阻止对等方根据其来同步时钟。

`show clock` 之前的符号含义如下：

- * 时间不是权威时间。
- (空白) 时间是权威时间。
- . 时间是权威时间，但 NTP 未同步。

配置时区

在特权 EXEC 模式下，根据以下步骤手动配置时区。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 设置时区。

   无线设备以通用协调时间 (UTC) 保持内部时间，因此，该命令仅用于显示用途以及手动设置时间的情况。

   - 对于 *zone*，输入当标准时间生效时要显示的时区名称。默认值为 UTC。
   - 对于 *hours-offset*，输入相对于 UTC 的小时偏移量。
   - (可选) 对于 *minutes-offset*，输入相对于 UTC 的分钟偏移量。

   ```
   clock timezone zone hours-offset [minutes-offset]
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

`clock timezone` 全局配置命令中的 *`minutes-offset`* 变量用于当地时区与 UTC 的偏差为一小时的百分比的情形，例如，加拿大大西洋省份 (AST) 一些区域的时区为 UTC-3.5，其中，3 表示 3 小时，.5 表示 50%。在这种情况下，应使用的命令为：

```
clock timezone AST -3 30?
```

要将时间设为 UTC，可使用 `no clock timezone` 全局配置命令。

配置夏令时

在特权 EXEC 模式下，根据以下步骤为相关区域配置在每年某周的特定一天开始和结束夏令时。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置在每年指定的日期开始和结束夏令时。

   默认情况下禁用夏令时。如果指定 `clock summer-time` *`zone`* `recurring` 时不带参数，则将默认采用美国夏令时规则。

   - 对于 *`zone`*，指定当夏令时生效时要显示的时区名称 (例如，PDT)。
   - (可选) 使用 *`week`* 指定月份中的第几周 (1...5 或 last)。
   - (可选) 使用 *`day`* 指定周中的哪一天 (Sunday、 Monday...)。
   - (可选) 使用 *`month`* 指定月份 (January、 February...)。
   - (可选) 使用 *`hh:mm`* 按小时和分钟格式 (24 小时制) 指定时间。
   - (可选) 使用 *`offset`* 指定夏令时期间要增加的分钟数。默认值为 60。

     ```
     clock summer-time zone recurring [week day month
     hh:mm week day month hh:mm [offset]]
     ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

`clock summer-time` 全局配置命令的第一部分指定夏令时开始时间，第二部分指定结束时间。所有时间都是相对于当地时区。开始时间相对于标准时间。结束时间相对于夏令时时间。如果开始月份在结束月份之后，系统将假定您处于南半球。

本例显示了如何指定从 4 月第一个周日的 02:00 开始夏令时，并在 10 月最后一个周日 02:00 结束夏令时：

```
AP(config)# clock summer-time PDT recurring 1
Sunday April 2:00 last Sunday October 2:00
```

如果您所在区域中的夏令时不遵循循环模式，则在特权 EXEC 模式下，按以下步骤操作 (配置下一次夏令时的准确日期和时间)。

1. 进入全局配置模式。

```
configure terminal
```

2. 配置第一个日期作为夏令时开始时间，第二个日期作为结束时间。

   默认情况下禁用夏令时。

   - 对于 *zone*，指定当夏令时生效时要显示的时区名称 (例如，PDT)。
   - (可选) 使用 *week* 指定月份中的第几周 (1...5 或 last)。
   - (可选) 使用 *day* 指定周中的哪一天 (Sunday、 Monday...)。
   - (可选) 使用 *month* 指定月份 (January、 February...)。
   - (可选) 使用 *hh*:*mm* 按小时和分钟格式 (24 小时制) 指定时间。
   - (可选) 使用 *offset* 指定夏令时期间要增加的分钟数。默认值为 60。

```
clock summer-time zone date [month date year hh:mm
month date year hh:mm [offset]]
```

   或

```
clock summer-time zone date [date month year hh:mm
date month year hh:mm [offset]]
```

3. 返回到特权 EXEC 模式。

```
end
```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

`clock summer-time` 全局配置命令的第一部分指定夏令时开始时间，第二部分指定结束时间。所有时间都是相对于当地时区。开始时间相对于标准时间。结束时间相对于夏令时时间。如果开始月份在结束月份之后，系统将假定您处于南半球。

要禁用夏令时，使用 `no clock summer-time` 全局配置命令。

本例显示了如何设置在 2000 年 10 月 12 日 02:00 开始夏令时，在 2001 年 4 月 26 日 02:00 结束夏令时：

```
AP(config)# clock summer-time pdt date 12 October
2000 2:00 26 April 2001 2:00
```

定义 HTTP 访问

默认情况下，端口 80 用于 HTTP 访问，端口 443 用于 HTTPS 访问。用户也可自定义这些值。

使用这些命令定义 HTTP 访问。

```
ip http port <port number>
ip http secure-port <port number>
```

配置系统名称和提示符

您可配置用于识别无线设备的系统名称。默认情况下，系统名称和提示符为 `ap`。

如果未配置系统提示符，将使用系统名称的前 20 个字符作为系统提示符。将附加一个大于符号 (>)。每当系统名称更改时，提示符将会相应更新，除非使用 `prompt` 全局配置命令手动配置提示符。

关于本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference (思科 IOS 配置基本命令参考和思科 IOS IP 和 IP 路由命令参考)。

默认系统名称和提示符配置

默认接入点系统名称和提示符为 ap。

配置系统名称

在特权 EXEC 模式下，根据以下步骤手动配置系统名称。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 手动配置系统名称。

   默认设置为 ap。

   注意：当更改系统名称时，无线设备的无线信号将重置，关联的客户端设备将解除关联，然后快速重新关联。

   系统名称最多可使用 63 个字符。但当无线设备将自身识别为客户端设备时，则只使用系统名称的前 15 个字符。如果必须让客户端用户清楚区分不同接入点，则确保系统名称的前 15 个字符是唯一的。

   ```
   hostname name
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

在设置系统名称时，也可将其用作系统提示符。

要恢复到默认主机名称，使用 no hostname 全局配置命令。

了解 DNS

DNS 协议控制域名系统 (DNS)，它是一个将主机名称映射到 IP 地址的分布式数据库。当在无线设备上配置 DNS 时，在所有 IP 命令 (例如， ping、 telnet、 connect) 及相关的 Telnet 支持操作中，可使用主机名称代替 IP 地址。

IP 定义了一种层级式命名方案，以便通过位置或域识别设备。域名由以句点 (.) 作为分隔符的区段组合在一起。例如， Cisco Systems 是一个商业组织， IP 以 com 域名进行标识，因此其域名为 reckwellautomation.com。该域中的特定设备 (例如，文件传输协议 (FTP) 系统) 被标识为 ftp.cisco.com。

为跟踪域名， IP 定义了域名服务器的概念，它保留了映射到 IP 地址的名称的缓存 (或数据库)。要将域名映射到 IP 地址，必须先标识主机名称，指定存在于网络中的域名服务器，并启用 DNS。

默认 DNS 配置

下表显示了默认 DNS 配置。

表 93 - 默认 DNS 配置

功能	默认设置
DNS 启用状态	禁用。
DNS 默认域名	未配置。
DNS 服务器	未配置域名服务器地址。

设置 DNS

在特权 EXEC 模式下，根据以下步骤设置无线设备使用 DNS。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 定义软件用于补足不合规主机名称 (无句点分隔符的域名) 的默认域名。

   不要包括用于分隔不合规名称与域名的开头句点。

   在启动时并未配置域名；但如果无线设备配置来自于 BOOTP 或动态主机配置协议 (DHCP) 服务器，则将由 BOOTP 或 DHCP 服务器设置默认域名 (如果服务器配置了该信息)。

   ```
   ip domain-name name
   ```

3. 指定一个或多个用于域名和地址解析的域名服务器地址。

   最多可指定六个域名服务器。各服务器之间用空格分隔。第一个指定的服务器为主服务器。无线设备先向主服务器发送 DNS 查询请求。如果查询失败，则将查询备用服务器。

   ```
   ip name-server server-address1 [server-address2 ... server-address6]
   ```

   (可选) 在无线设备上启用基于 DNS 的主机名称 —— 地址转换功能。默认情况下禁用该功能。

   如果网络设备需要连接网络中不是由您控制名称指定的其他设备，您可使用全球互联网命名方案 (DNS) 动态分配可唯一标识设备的设备名称。

   ```
   ip domain-lookup
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

   (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

如果使用无线设备 IP 地址作为其主机名称，则将使用 IP 地址，不进行 DNS 查询。如果配置的主机名称中不包含句点 (.)，则在执行 DNS 查询将名称映射到 IP 地址之前，将在主机名称后附加一个句点和默认域名。

默认域名是由 `ip domain-name` 全局配置命令设置的值。如果主机名称中有句点 (.)，思科 IOS 软件将不在主机名称后附加默认域名，而是直接查找 IP 地址。

- 要删除域名，可使用 `no ip domain-name name` 全局配置命令。
- 要删除域名服务器地址，可使用 `no ip name-server server-address` 全局配置命令。
- 要在无线设备上禁用 DNS，可使用 `no ip domain-lookup` 全局配置命令。

显示 DNS 配置

要显示 DNS 配置信息，可使用 `show running-config` 特权 EXEC 命令。当在无线设备上配置了 DNS 时， `show running-config` 命令有时会显示服务器 IP 地址，而不是服务器名称。

配置无线电设置

本章描述了如何配置无线设备的无线电设置。

启用无线电接口

无线设备无线电默认情况下处于禁用状态。

重要事项　从思科 IOS 版本 12.3(8)JA 开始，不再提供 SSID。您必须先创建一个 SSID，然后才能启用无线电接口。

在特权 EXEC 模式下，根据以下步骤启用接入点无线电。

1. 进入全局配置模式。
   ```
   configure terminal
   ```
2. 输入 SSID。

   SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。
   ```
   dot11 ssid ssid
   ```
3. 进入无线电接口的接口配置模式。
   ```
   interface dot11radio {0 | 1}
   ```
   - 802.11n 2.4 GHz 无线电装置是无线电 0。
   - 802.11n 5 GHz 无线电装置是无线电 1。
4. 将在步骤 2 中创建的 SSID 分配给相应的无线电接口。
   ```
   ssid ssid
   ```
5. 启用无线电端口。
   ```
   no shutdown
   ```
6. 返回到特权 EXEC 模式。
   ```
   end
   ```
7. (可选) 将您的输入保存到配置文件中。
   ```
   copy running-config startup-config
   ```
   使用关闭命令禁用无线电端口。

配置无线电网络中的角色。

Stratix 5100 无线接入点 / 工作组网桥在无线电网络中具有以下角色。

- 接入点
- 接入点 (关闭无线电作为后备)
- 接入点 (中继器模式作为后备)
- 工作组网桥
- 中继器
- 根网桥
- 非根网桥
- 带无线客户端的根网桥
- 带无线客户端的非根网桥
- 通用工作组网桥
- 扫描器

当使用 AES-CCM TKIP 配置通用工作组网桥时，非根设备必须使用 TKIP 或 AES-CCM TKIP 作为密文关联到根设备。如果它仅配置了 AES-CCM，则非根设备不与根关联。该配置导致根和非根设备之间的多播密码不匹配。

您也可以为根接入点配置后备角色。当其以太网端口被禁用或断开与有线局域网的连接时，无线设备将自动采用后备角色。有两种可能的后备角色：

- 中继器

  当禁用以太网端口时，无线设备成为中继器，并关联到附近的根接入点。您无需指定后备中继器要关联的根接入点；中继器自动关联到提供最佳无线电连接的根接入点。

- 关闭

  无线接入点 / 工作组网桥关闭其无线电，解除所有客户端设备的关联。

在特权 EXEC 模式下，根据以下步骤设置无线设备的无线电网络角色和后备角色。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4-Ghz 无线电装置是接口 0。
   - 802.11n 5-GHz 无线电装置是接口 1。

   ```
   interface dot11radio { 0 | 1 }
   ```

3. 设置无线设备角色。
   - 将角色设为根接入点、工作组网桥或带 / 不带无线客户端的非根网桥、中继器接入点、或扫描器。网桥模式无线电装置支持点对点及单点对多点配置方式。
   - 当其中一个无线电装置被配置为中继器时，将关闭以太网端口。每个接入点只有一个无线电装置可被配置为工作组网桥或中继器。
   - 当将接入点配置为中继器时， `dot11radio 0|1 antenna-alignment` 命令可用。
   - (可选) 选择根接入点后备角色。如果无线设备以太网端口被禁用或从有线局域网断开连接，则无线设备可以关闭其无线电端口或成为一个与任意相邻的根接入点关联的中继器接入点。

   ```
   station-role


   non-root {bridge | wireless-clients}
   ```

```
repeater （中继器）


root {access-point | ap-only | [bridge | wireless-
clients] | [fallback | repeater | shutdown]}


scanner （扫描器）


workgroup-bridge {multicast | mode <client |
infrastructure>| universal <Ethernet client MAC
address>}
```

4. 返回到特权 EXEC 模式。

```
end
```

5. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

提示　当您在无线电网络中启用网桥 / 工作组网桥角色，并使用 no shut 命令启用接口时，只有在另一端的接入点或网桥上的设备正常工作时，才显示接口的物理状态和软件状态。否则，仅显示设备的物理状态。只有位于另一端的设备已配置且正常工作时，才显示此设备的软件状态。

通用工作组网桥模式

当配置通用工作组网桥角色时，您必须包括客户端 MAC 地址。如果工作组网桥出现在网桥表上，且不是一个静态条目，则此网桥只能与此 MAC 地址关联。如果验证失败，工作组网桥与其 BVI MAC 地址关联。在通用工作组网桥模式下，工作组网桥使用以太网客户端的 MAC 地址与思科和非思科根设备关联。通用工作组网桥是透明的，不进行管理。

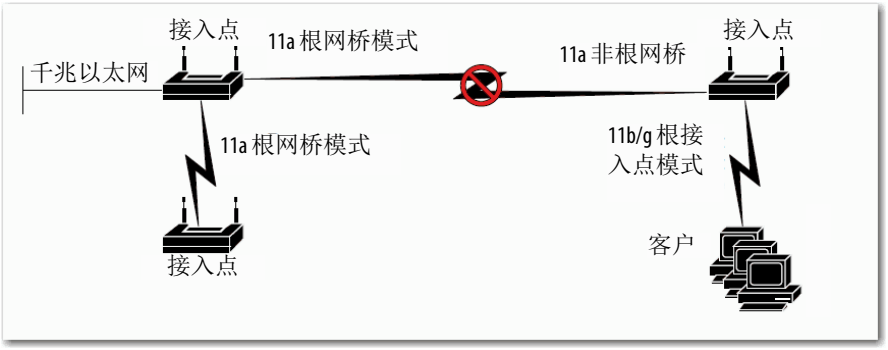
重要事项 通用工作组网桥仅支持一个有线客户端。

您可以启用恢复机制，并通过禁用以太网客户端来重新管理工作组网桥，使得通用工作组网桥使用自己的 BVI 地址关联至接入点。

配置双无线电后备

双无线电后备功能允许您配置接入点，从而当将接入点连接至网络基础设施的非根网桥链路发生故障时，根接入点链路 (客户端通过其连接至接入点) 将会关闭。关闭根接入点链路会导致客户端漫游到另一个接入点。没有此功能时，客户端保持连接到接入点，但不能从网络收发数据。

图 99 - 双无线电后备



无线电追踪

您可以配置接入点来追踪或监视其中一个无线电装置的状态。若被追踪的无线电装置出现故障或被禁用，接入点关闭另一个无线电装置。若被追踪的无线电装置出现，接入点启用另一个无线电装置。

- 若要追踪无线电装置 0，输入以下命令：

```
# station-role root access-point fallback track d0
shutdown
```

- 若要追踪无线电装置 1，输入以下命令：

```
# station-role root access-point fallback track d1
shutdown
```

千兆以太网追踪

当接入点的以太网端口被禁用或断开与有线局域网的连接时，您可配置接入点后备。

提示　千兆以太网跟踪不支持中继器模式。

使用以下命令在无线电接口配置模式中配置千兆以太网追踪的 802.11n 接入点：

```
# station-role root fallback shutdown
```

MAC 地址追踪

您可通过其 MAC 地址追踪另一个无线电装置的客户端接入点，将角色为根接入点的无线电装置配置为启用或停用。如果客户端解除与接入点的关联，根接入点无线电装置停用。如果客户端重新关联至接入点，根接入点无线电装置又再度启用。

当客户端是连接至上游有线网络的非根网桥接入点时， MAC 地址追踪极为有用。

例如，若要追踪 MAC 地址为 12:12:12:12:12:12 的客户端，输入以下命令：

```
# station-role root access-point fallback track
mac-address 12:12:12:12:12:12 shutdown
```

配置无线电数据传输速率

您可使用数据传输速率设置来选择无线设备用于传输数据的数据传输速率。速率单位为兆比特 / 秒。无线设备总是尝试使用设为 “ 启用 ” 的最高数据传输速率传送。如果存在障碍物或干扰，无线设备下降至允许数据传输的最高速率。您可将每个数据传输速率设为三种状态之一：

- Basic (基本)(GUI 将基本速率标为 “ 必需 ”)

  允许以该速率传输所有的数据包，包括单播和多播。至少一个以上无线设备的数据传输速率必须设为 Basic (基本)。

- 启用

  无线设备仅以该速率发送单播数据包；以设为 Basic (基本) 的其中一种数据传输速率发送多播数据包。

- 禁用

  无线设备不以该速率发送数据。

提示 必须至少将一种数据传输速率设为 “ 基本 ”。

您可以使用数据传输速率设置来设置接入点，为特定数据传输速率的客户端设备提供服务。

例如，要将 2.4 GHz 无线电装置设为仅用于 11 Mbps 服务，将 11 Mbps 速率设为 Basic (基本)，并将其他数据传输速率设为 Disabled (禁用)。

- 要将 2.4 GHz， 802.11g 无线电装置设为仅为 802.11g 客户端设备提供服务，将所有正交频分复用 (OFDM) 数据传输速率 (6、 9、 12、 18、 24、 36、 48、 54) 设为 Basic (基本)。

- 要将 5 GHz 无线电装置设为仅用于 54 Mbps 服务，将 54 Mbps 速率设为 Basic (基本)，将其他数据传输速率设为 Disabled (禁用)。

您可以配置无线设备自动设置数据传输速率，以优化范围或吞吐量。在 2.4-GHz 无线电装置上，范围设置将 1.0 数据传输速率配置为 “ 基本 ”，将其他数据传输速率设为 “ 支持 ”。在 5-GHz 无线电装置上，范围设置将 6.0 数据传输速率配置为 “ 基本 ”，将其他数据传输速率设为 “ 支持 ”。

范围设置允许接入点通过降低数据传输速率来扩大覆盖范围。因此，如果有一个客户端不能连接到接入点，而其他客户端可以，原因之一可能是该客户端不位于接入点的覆盖区域内。在这种情况下，范围选项有助于扩大覆盖范围，提高客户端连接到接入点的能力。

但是，允许客户端在远离 AP 时以最低数据传输速率进行通信会严重降低其他客户端的性能。在大多数情况下不建议使用范围选项。

通常需要在吞吐量和覆盖范围之间取得折衷。当信号质量下降 (可能由于与接入点的距离) 时，速率重新向下调整，以保持链路 (但以较低的数据传输速率)。相反，当信号质量下降到不足以保持所配置的高数据传输速率时，或漫游至具有充足覆盖范围的另一个接入点 (如果存在) 时，配置了较高吞吐量的链路速率将会下降。

例如，必须根据无线项目可用的资源确定两者 (吞吐量与范围) 之间的平衡，这是众多设计决策之一：

- 用户传送的流量类型
- 所希望的服务级别
- RF 环境质量

当输入吞吐量作为数据传输速率设置时，无线设备将所有数据传输速率设为 “ 基本 ”。

接入点以最高基本速率发送多播和管理帧

运行最新思科 IOS 版本的接入点以所配置的最高基本速率发送多播和管理帧，这是一种会导致可靠性问题的情况。

因为多播帧不在 MAC 层重新发送，因此，蜂窝边缘的站点可能无法成功接收它们。如果目标是可靠接收，则可以低数据传输速率发送多播。如果要求支持高数据传输速率多播，则缩小蜂窝尺寸，禁止所有较低的数据传输速率。

根据您的具体要求，可以采取以下措施：

- 如果需要以最大的可靠性发送多播数据，且对大多播带宽没有需求，则配置一个单一的基本速率，该速率低到足以到达无线蜂窝的边缘。
- 如果需要以某个特定的数据传输速率发送多播数据，以实现特定的吞吐量，则将该速率配置为最高基本速率。您还可设置一个较低的基本速率，以覆盖非多播客户端。

在特权 EXEC 模式下，根据以下步骤配置无线电数据传输速率。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。

   2.4 GHz N 无线电装置为无线电 0， 5 GHz N 为无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 请参见速度命令和用途描述。

表 94 - 速度命令和用途描述

命令	用途
speed **802.11n 2.4 GHz 无线电装置：** {[1.0] [11.0] [12.0] [18.0] [2.0] [24.0] [36.0] [48.0] [5.5] [54.0] [6.0] [9.0] [basic-1.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-5.5] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] [m16-23] [m16.] [m17.] [m18.] [m19.] [m20.] [m21.] [m22.] [m23.] [ofdm] [only-ofdm] | range | throughput} **802.11n 5 GHz 无线电装置：** {[12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [6.0] [9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] [m16-23] [m16.] [m17.] [m18.] [m19.] [m20.] [m21.] [m22.] [m23.] | range | throughput}	将每个数据传输速率设为 " 基本 " 或 " 启用 "，或输入范围来优化范围，或输入吞吐量来优化吞吐量。 输入 1.0、2.0、5.5、6.0、9.0、11.0、12.0、18.0、24.0、36.0、48.0 和 54.0，在 802.11g, 2.4 GHz 无线电装置上设置启用这些数据传输速率。 输入 6.0、9.0、12.0、18.0、24.0、36.0、48.0 和 54.0，在 5 GHz 无线电装置上设置启用这些数据传输速率。 要在 802.11g，2.4 GHz 无线电装置上将这些数据传输速率设为 " 基本 "，输入以下命令：basic-1.0、basic-2.0、basic-5.5、basic-6.0、basic-9.0、basic-11.0、basic-12.0、basic-18.0、basic-24.0、basic-36.0、basic-48.0 和 basic-54.0 **提示**　客户端必须支持您选择的基本速率，否则无法关联到无线设备。如果 802.11g 无线电装置的基本数据传输速率选择 12 Mbps 或更高值，则 802.11b 客户端设备不能关联到无线设备 802.11g 无线电装置。 要在 5 GHz 无线电装置上将这些数据传输数据设为 " 基本 "，输入以下命令：basic-6.0、basic-9.0、basic-12.0、basic-18.0、basic-24.0、basic-36.0、basic-48.0 和 basic-54.0。 • (可选) 输入范围和吞吐量自动优化无线电范围和吞吐量。当输入范围时，无线设备将最低的数据传输速率设为 " 基本 "，将其他速率设为 " 启用 "。当输入吞吐量时，无线设备将所有数据传输速率设为 " 基本 "。 • (可选) 在 802.11g 无线电装置上，输入速度吞吐量 ofdm 将所有 OFDM 速率 (6、9、12、18、24、36 和 48) 设为 " 基本 "(必需)，将所有 CCK 速率 (1、2、5.5 和 11) 设为 " 禁止 "。该设置禁用 802.11b 的保护机制，并为 802.11g 客户端提供最大吞吐量。但是，它会阻止 802.11b 客户端关联到接入点。 • (可选) 输入默认值，将数据传输速率设为出厂默认设置 – 在 802.11n 2.4 GHz 无线电装置上，默认选项将速率 1.0、2.0、5.5 和 11.0 设为 " 启用 "。 – 在 802.11n 5 GHz 无线电装置上，默认选项将速率 6.0、12.0 和 24.0 设为 " 启用 "。 两个 802.11n 无线电装置的默认 MCS 设置均为 0-23。

4. 返回到特权 EXEC 模式。

```
end
```

5. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

使用 no 格式的速度命令从配置中删除一个或多个数据传输速率。本例显示了如何从配置中删除数据传输速率 basic-2.0 和 basic-5.5：

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

配置 MCS 速率

调制编码方案 (MCS) 是 PHY 参数规范，包括调制顺序 (BPSK、QPSK、16-QAM、64-QAM) 和 FEC 编码速率 (1/2、2/3、3/4、5/6)。MCS 在 802.11n 无线电装置中使用，它定义了 32 个对称设置 (每个空间流 8 个)：

- MCS 0–7
- MCS 8–15
- MCS 16–23
- MCS 24–31

MCS 是一项重要设置，因为它提供了潜在的更大的吞吐量。高吞吐量数据传输速率为 *MCS*、*带宽* 和 *保护间隔* 的函数。 802.11 a、 b 和 g 无线电装置使用 20 MHz 通道宽度。下表显示了基于 MCS、保护间隔和通道宽度的潜在数据传输速率。

提示 2.4 GHz 无线电装置不支持 40 MHz 通道宽度。

表 95 - 基于 MCS 设置、保护间隔和通道宽度的数据传输速率

MCS 索引	保护间隔 = 800 ns		保护间隔 = 400 ns	
	20 Mhz 通道宽度的数据传输速率 (Mbps)	40 Mhz 通道宽度的数据传输速率 (Mbps)	20 Mhz 通道宽度的数据传输速率 (Mbps)	40 Mhz 通道宽度的数据传输速率 (Mbps)
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300
16	19.5	40.5	21.7	45
17	39	81	43.3	90
18	58.5	121.5	65	135
19	78	162	86.7	180
20	117	243	130	270
21	156	324	173.3	360

表 95 - 基于 MCS 设置、保护间隔和通道宽度的数据传输速率 (续)

MCS 索引	保护间隔 = 800 ns		保护间隔 = 400 ns	
22	175.5	364.5	195	405
23	195	405	216.7	450

传统速率为：
5 GHz：6、 9、 12、 18、 24、 36、 48 和 54 Mbps
2.4 GHz：1、 2、 5.5、 6、 9、 11、 12、 18、 24、 36、 48 和 54 Mbps

MCS 速率使用速度命令进行配置。本例显示了 802.11n 5 GHz 无线电装置的一项速度设置：

```
interface Dot11Radio0
   no ip address
   no ip route-cache
   !
   ssid 1250test
   !
   speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0
   36.0 48.0 54.0 m0. m1. m2. m3. m4. m8. m9. m10. m11.
   m12. m13. m14. m15. m16. m17. m18. m19. m20. m21.
   m22. m23.
```

配置无线电发射功率

无线电发射功率基于在接入点中安装的无线电装置类型以及其运行所在的监管域。

使用下表确定发射功率，以及 mW 和 dBm 之间的转换关系。

表 96 - mW 和 dBm 之间的转换

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

在特权 EXEC 模式下，根据以下步骤设置接入点无线电装置上的发射功率。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。

   2.4 GHz 802.11n 无线电类型为 0；5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 将 2.4 GHz 无线电装置或 5 GHz 无线电装置的发射功率设为监管域允许的其中一个功率等级。

   ```
   power local
   ```

以下选项可用于 2.4 GHz 802.11n 无线电装置 (单位：dBM)：

```
{ 4 | 7 | 10 | 13 | 16 | 19 | 22 }
```

以下选项可用于 5 GHz 802.11n 无线电装置 (单位：dBM)：

```
{ 5 | 8 | 11 | 14 | 17 | 20 | 23 }
```

提示 确保电源设置与您监管域的设置相匹配。

提示 802.11g 无线电装置以高达 100 mW 的发射功率提供 1、 2、 5.5 和 11 Mbps 的数据传输速率。但是，对于 6、 9、 12、 18、 24、 36、 48 和 54 Mbps 数据传输速率， 802.11g 无线电装置的最大发射功率是 30 mW。

4. 返回特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的功率命令将功率设置恢复为最大值 (默认设置)。

限制关联客户端设备的功率等级

您还可限制关联至无线设备的客户端设备的功率等级。当客户端设备关联至无线设备，无线设备将最大功率等级设置发送至客户端。

提示　思科 AVVID 文档使用动态功率控制 (DTPC) 这个术语来表示限制所关联的客户端设备的功率等级。

在特权 EXEC 模式下，根据以下步骤指定关联至无线设备的所有客户端设备允许的最大功率设置。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。

2.4 GHz 无线电方式为 radio 0， 5 GHz 无线电方式为 radio 1。

```
interface dot11radio {0 | 1}
```

3. 设置关联至无线设备的客户端设备的最大功率等级。
   - 将功率等级设为 local，表示将客户端功率等级设为接入点的功率等级。
   - 将功率等级设为 `maximum`，表示将客户端功率设为所允许的最大功率。

     提示　您的监管域所允许的设置可能与此处所列设置不同。

   ```
   power client
   ```

以下选项可用：

```
{local | <-127 - 127> | maximum}
```

4. 返回特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 `no` 格式的客户端功率命令禁用所关联客户端的最大功率等级。必须启用 Aironet 扩展来限制关联客户端上的功率等级。默认情况下启用 Aironet 扩展。

配置无线电通道设置

无线设备无线电的默认通道设置为最不拥塞；启动时，无线设备扫描并选择最不拥塞的通道。但是，为了在站点调查后实现最一致的性能，我们建议您为每个接入点分配一个静态通道设置。无线设备上的通道设置对应于监管域中可用的频率。有关您的监管域中允许的频率，请参见接入点硬件安装指南。

提示 在射频干扰会导致客户端偶尔断开与无线网络的连接的场所，将无线接口设为在另一个通道上运行可避免干扰。

每个 2.4 GHz 通道覆盖 22 MHz。通道 1、 6 和 11 的带宽不重叠，因此，您可在同一邻近区域设置多个接入点，而不会造成干扰。

5 GHz 无线电装置在频率范围 5180 - 5825 MHz 内工作。通道数取决于监管域，范围为 5 - 21。每个通道覆盖 20 MHz，通道带宽稍有重叠。为实现最佳性能，对紧挨的无线电装置使用不相邻的通道 (例如，44 和 48)。

提示 同一邻近区域内的接入点太多，出现无线电拥塞，吞吐量降低。详尽的站点调查可以确定实现最大无线电覆盖范围和最高吞吐量的最佳接入点位置。请参见最新的产品规范。

由于它们经常改变，本文档不对通道设置进行描述。有关接入点或网桥通道设置的最新信息，请参见最新的产品规范。

802.11n 通道宽度

802.11n 协议允许您使用 40 MHz 通道宽度，它包含 2 个连续不重叠的通道 (例如，5 GHz 通道 44 和 48)。2.4 GHz 无线电装置不支持 40 MHz 通道宽度。

其中一个 20 Mhz 通道称为控制通道。传统客户端和 20 Mhz 802.11n 客户端使用控制通道。只能在该通道上发送信标。第 2 个 20 Mhz 通道称为扩展通道。 40 Mhz 站点同时使用该通道和控制通道。

40 Mhz 通道被指定为通道及扩展通道，例如， 1,1。在本例中，控制通道是通道 1，扩展通道高于控制通道。

在特权 EXEC 模式下，根据以下步骤设置无线设备通道宽度。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入 5 GHz 无线电接口的接口配置模式。

   ```
   interface dot11radio 1
   ```

3. 设置无线设备无线电的通道。
   - 使用 `width` 选项指定一个要使用的带宽。

   该选项包含三个可用设置：20， 40-above 和 40-below。选择 20 将通道宽度设为 20 MHz。选择 40-above 将通道宽度设为 40 Mhz，扩展通道高于控制通道。选择 40-below 将通道宽度设为 40 MHz，扩展通道低于控制通道。

   ```
   channel
   {frequency | least-congested | width [20 | 40-above
   | 40-below] | dfs}
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

Dynamic Frequency Selection (动态频率选择)

出厂时配置了 5 GHz 无线电装置的接入点计划在北美、欧洲使用，如今符合要求无线电设备使用动态频率选择 (DFS) 来检测雷达信号以及避免干扰雷达信号的规范。当接入点在某个通道上检测到雷达时，其将避免使用该通道 30 分钟。配置为在其他监管域中使用的无线电装置不使用 DFS。

提示　由于 DFS 操作可能对客户端流量产生长时干扰，建议传输关键数据时避免使用 DFS 通道。

当启用了 DFS 的 5 GHz 无线电装置在第 271 页的表 97 列出的 15 个通道之一上工作时，接入点自动使用 DFS 设置工作频率。当启用了 DFS 时，接入点为雷达信号监视其工作频率。

如果接入点在通道上检测到雷达信号，则执行以下步骤：

- 阻止通道上的新传输操作。
- 刷新节能客户端队列。
- 广播 802.11h 通道切换公告。
- 解除剩余客户端设备的关联。
- 如果参与 WDS，将一个 DFS 通知发送至离开此频率的活动 WDS 设备。
- 随机选择一个不同的 5 GHz 通道。
- 如果所选的通道是第 271 页的表 97 中的其中一个，则对新通道扫描雷达信号达 60 秒。
- 如果新通道上没有雷达信号，则启用信标，并接受客户端关联。

- 如果参与 WDS，将新工作频率的 DFS 通知发送至活动 WDS 设备。

提示 根据监管要求，在某些地区不能手动选择启用了 DFS 的 5 GHz 无线电通道。在这种情况下，接入点将随机选择一个通道。

下表列出了需要 DFS 的通道和频率。

表 97 - 要求使用 DFS 的通道

通道	MHz	通道	MHz	通道	MHz
52	5260	104	5500	124	5620
56	5280	108	5520	128	5640
60	5300	112	5560	132	5660
64	5320	116	5580	136	5680
100	5500	120	5600	140	5700

为实现自动操作， DFS 需要在列出的通道中进行随机通道选择。未列出的通道不需要随机选择，可手动配置。

在第 271 页的表 97 中列出的任何一个通道上发送信息之前，接入点无线电装置执行通道可用性检查 (CAC)。 CAC 是一次长达 60 秒的扫描，扫描是否在通道上存在雷达信号。在接入点控制台上显示以下示例消息，这些消息给出 CAC 扫描的开始和结束时间：

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning
frequency 5500 MHz for 60 seconds

*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan
complete on frequency 5500 MHz
```

当在第 271 页的表 97 中列出的任何一个 DFS 通道上工作时，除执行 CAC 外，接入点还连续监视通道是否存在雷达信号。如果检测到雷达，接入点在 200 ms 内停止转发数据包，并广播 5 个包括 802.11h 通道切换公告的信标，指示接入点开始使用的通道号。下例显示了在检测到雷达时，在接入点控制台上显示的消息：

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on
frequency 5500 MHz
```

当在通道上检测到雷达时，将连续 30 分钟不使用该通道。接入点在非易失性存储区中为在最近的 30 分钟内检测到雷达的每个通道保存一个标志。 30 分钟后，清除相应通道的标志。如果在清除标志之前重启动接入点，则在初始化通道时，将非占用时间复位到 30 分钟。

提示　某些 5 GHz 通道的最大合法发射功率比其他通道高。当接入点随机选择一个功率受限的 5 GHz 通道时，接入点自动降低发射功率，以符合该通道的功率限制。

提示　我们建议您使用 `world-mode dot11d country-code configuration interface` 命令为启用了 DFS 的无线电装置配置一个国家代码。

IEEE 802.11h 协议要求接入点在信标和探测响应中包含国家信息元素 (IE)。但是，默认情况下 IE 中的国家代码为空白。您可使用 world-mode 命令来填入国家代码 IE。

DFS 通道上的雷达检测

当接入点在 DFS 通道上检测到雷达时，接入点在其闪存中创建一个文件。该文件基于 802.11a 无线电序列号，包含检测到雷达的通道号。这是期望行为，因此您不能删除该文件。

CLI 命令

以下小节描述了应用于 DFS 的 CLI 命令。

确认启用了 DFS

使用 `show controllers dot11radio1` 命令确认启用了 DFS。该命令还包括需要均匀扩频的指示以及在检测雷达之前处于非占用周期的通道。

本例显示了启用了 DFS 的通道执行 `show controller` 命令后的一个输出行。上一段中列出的指示用粗体显示：

```
ap#show controller dot11radio1
!
interface Dot11Radio1
Radio AIR-RM1251A, Base Address 011.9290ec0, BBlock
version 0.00, Software version 6.00.0
Serial number FOCO83114WK
Number of supported simultaneous BSSID on
Dot11Radio1: 8
Carrier Set: Americas (OFDM) (US )
Uniform Spreading Required: Yes
```

```
Current Frequency: 5300 MHz Channel 60 (DFS enabled)

Current Frequency: 5300 MHz Channel 60 (DFS
enabled)

Allowed Frequencies: 5180(36) 5200(40) 5220(44)
5240(48) *5260(52) *5280(56) *53

00(60) *5320(64) *5500(100) *5520(104) *5540(108)
*5560(112) *5580(116) *5660(13

2) *5680(136) *5700(140) 5745(149) 5765(153)
5785(157) 5805(161)

* = May only be selected by Dynamic Frequency
Selection (DFS)


Listen Frequencies: 5170(34) 5190(38) 5210(42)
5230(46) 5180(36) 5200(40) 5220(4

4) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64)
5500(100) 5520(104) 5540(108) 55

60(112) 5580(116) 5600(120) 5620(124) 5640(128)
5660(132) 5680(136) 5700(140) 57

45(149) 5765(153) 5785(157) 5805(161) 5825(165)


DFS Blocked Frequencies: none

Beacon Flags: 0; Beacons are enabled; Probes are
enabled

Current Power: 17 dBm

Allowed Power Levels: -1 2 5 8 11 14 15 17

Allowed Client Power Levels: 2 5 8 11 14 15 17

...
```

配置通道

使用 channel 命令配置通道。修改接口命令的目的仅在于让您选择一个特定的通道号以及启用 DFS。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入 802.11a 无线电装置的配置接口

   ```
   interface dot11radio1
   ```

3. 输入通道 < 编号 >：
   可用的通道号为：36、 40、 44、 48、 149、 153、 157、 161、 165、 5180、 5200、 5220、 5240、 5745、 5765、 5785、 5805 或 5825。

   提示　　这与 A 域 (美国 / 加拿大) 有关。

   要使用 DFS 通道，输入 dfs 和以下其中一个频带来使用选定通道上的动态频率选择：

   1 - 5.150...5.250 GHz

   2 - 5.250...5.350 Ghz

   3 - 5.470...5.725 GHz

   4 - 5.725...5.825 GHz

如果尝试配置一个只能由 dfs 选择的通道，显示以下消息：

```
This channel number/frequency can only be used by
Dynamic Frequency Selection (DFS)
```

4. 返回特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入

   ```
   show running-config
   ```

6. (可选) 将输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

下例选择了通道 36，并将该通道配置成使用频带 1 上的 DFS：

```
ap#configure terminal
ap(config)interface dot11radio1
ap(config-if) channel 36
ap(config-if)
```

阻止 DFS 选择通道

如果监管域在某些特定场所限制您可使用的通道 —— 例如，室内或户外，您可以阻止通道组，防止在启用了 DFS 时接入点选择这些通道。使用以下配置接口命令阻止通道组，禁止供 DFS 选择：

```
[no] dfs band [1] [2] [3] [4] block
```

1、 2、 3 和 4 选项指定阻止的通道：

- 1 - 指定频率 5.150...5.250 GHz。

  该频率组也称为 UNII-1 频带。
- 2 - 指定频率 5.250...5.350 GHz。

  该频率组也称为 UNII-2 频带。
- 3 - 指定频率 5.470...5.725 GHz。
- 4 - 指定频率 5.725...5.825 GHz。

  该频率组也称为 UNII-3 频带。

本例显示了如何防止接入点在 DFS 期间选择频率 5.150...5.350 GHz：

```
ap(config-if)# dfs band 1 2 block
```

本例显示了如何为 DFS 取消阻止频率 5.150...5.350：

```
ap(config-if)# no dfs band 1 2 block
```

本例显示了如何为 DFS 取消阻止所有频率：

```
ap(config-if)# no dfs band block
```

设置 802.11n 保护间隔

802.11n 保护间隔是数据包之间的间隔，单位为纳秒。提供两种设置：短 (400 ns) 和长 (800 ns)。短保护间隔的性能略好，但在有很多反射和多径信号的环境中会出现问题。

在特权 EXEC 模式下，根据以下步骤设置 802.11n 保护间隔。

1. 进入全局配置模式。

   ```
   configure terminal
   ```
2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4 GHz 无线电装置为无线电 0
   - 802.11n 5 GHz 无线电装置是无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 输入一个保护间隔。
   - `any` 允许使用短 (400 ns) 或长 (800 ns) 保护间隔
   - `long` 只允许使用长 (800 ns) 保护间隔

   ```
   guard-interval {any | long}
   ```
4. 返回到特权 EXEC 模式。

   ```
   end
   ```
5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

配置发送和接收天线

您可以选择无线设备用于接收和发送数据的天线。

选项	描述
a-antenna	使用天线 A
ab-antenna	使用天线 A 和 B
abc-antenna	使用天线 A、 B 和 C
abcd-antenna	使用天线 A、 B、 C 和 D

在特权 EXEC 模式下，根据以下步骤选择无线设备用于接收和发送数据的天线。

1. 进入全局配置模式。

   ```
   configure terminal
   ```
2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4 GHz 无线电装置为无线电 0
   - 802.11n 5 GHz 无线电装置是无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```
3. 输入一个 -128...128 dB 的值，指定固定到设备的天线的合成增益。

   如有必要，可使用小数值，例如， 1.5。

   ```
   gain dB
   ```
4. 选择要使用的天线：

   ```
   antenna {a-antenna | ab-antenna | abc-antenna |
   abcd-antenna}
   ```

为获得最佳性能，请不要使用该设置，除非连接一个非标准外接天线或禁用一个损坏的天线端口。当使用 AP 时，将天线端口标记为 A、B、 C、 D。

5. 返回特权 EXEC 模式。

   ```
   end
   ```
6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

启用和禁用无偿探测响应

无偿探测响应 (GPR) 有助于支持蜂窝和 WLAN 工作方式的双模电话节省电池电量。 5 GHz 无线电装置上提供 GPR，默认情况下为禁用。您可配置两项 GPR 设置：

- 周期

  该设置确定 GRP 传输的时间间隔，单位为 Kusec，范围为 10...255 (与信标周期类似)。

- 速度

  速度是用于发送 GPR 的数据传输速率。选择一个较长的周期可减少由 GPR 消耗的射频带宽量，同时电池续航时间可能缩短。选择较高的传输速度也会减少消耗的带宽量，但会缩小蜂窝规模。

在特权 EXEC 模式下，根据以下步骤启用 GPR 并设置其参数。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入 5 GHz 无线电接口的接口配置模式。

   ```
   interface dot11radio {1}
   ```

3. 使用默认周期 (10 Kusec) 和速度 (6.0 Mbps) 启用无偿探测响应功能。

   ```
   probe-response gratuitous
   {period | speed}
   ```

4. (可选) 输入一个范围为 10 - 255 的值。默认值为 10

   ```
   period Kusec
   ```

5. (可选) 设置响应速度，单位为 Mbps。默认值为 6.0。

   ```
   speed
   {[6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0 ]
   [54.0] }
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

当您不想使用默认值时，可单独或组合配置可选参数，如下例所示：

```
(config-if)# probe-response gratuitous period 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30
speed 12.0
```

使用 no 格式的命令禁用 GPR 功能。

禁用和启用 Aironet 扩展

默认情况下，无线设备使用 Aironet 扩展来检测客户端设备的功能，并支持需要在无线设备和所关联客户端之间进行特殊交互的功能。必须启用 Aironet 扩展来支持以下功能：

- 负载平衡

  无线设备根据用户数量、误码率和信号强度等因素，使用 Aironet 扩展将客户端设备引导到提供与网络最佳连接的接入点。

- 消息完整性校验 (MIC)

  MIC 是一个附加 WEP 安全功能，可防止对加密数据包的攻击，即位翻转攻击。在无线设备和所有关联客户端设备上实施的 MIC 将数个字节添加到每个数据包中，以防止数据包被篡改。

- 思科密钥完整性协议 (CKIP)

  思科的 WEP 密钥置换技术基于由 IEEE 802.11i 安全任务组提供的早期算法。基于标准的算法 TKIP 不要求启用 Aironet 扩展。

- 中继器模式

  您必须在中继器接入点及关联的根接入点上启用 Aironet 扩展。

- 世界模式 (仅传统设备)

  启用了传统世界模式的客户端设备允许从无线设备接收载波设置信息，并自动调整其设置。 802.11d 世界模式操作不需要使用 Aironet 扩展。

- 限制关联客户端设备的功率等级

  当客户端设备关联至无线设备时，无线设备将允许的最大功率等级设置发送给客户端。

禁用 Aironet 扩展后，上述列出的功能也将被禁用，但这有时会提高非思科客户端关联至无线设备的能力。

默认情况下启用 Aironet 扩展。在特权 EXEC 模式下，根据以下步骤禁用 Aironet 扩展。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。2.4 GHz 无线电装置为无线电 0，而 5 GHz 无线电装置为无线电 1。
   - 802.11n 2.4 GHz 无线电装置为无线电 0
   - 802.11n 5 GHz 无线电装置是无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 禁用 Aironet 扩展。

   ```
   no dot11 extension aironet
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 `dot11 extension aironet` 命令启用 Aironet 扩展 (若被禁用)。

配置以太网封装变换方法

当无线设备接收的数据包不是 802.3 数据包时，无线设备必须使用封装变换方法将数据包格式化为 802.3。有两种变换方法：

- 802.1H —— 该方法为思科 Aironet 无线产品提供了出色性能。
- RFC 1042 —— 使用该设置来验证与非思科 Aironet 无线设备是否有良好的互操作性。 RFC 1042 由其他无线设备制造商使用，它是默认设置。

在特权 EXEC 模式下，根据以下步骤配置封装变换方法。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4 GHz 无线电装置为无线电 0
   - 802.11n 5 GHz 无线电装置是无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 将封装变换方法设为 RFC 1042 (`rfc1042`，默认设置) 或 802.1h (`dot1h`)。

   ```
   payload-encapsulation
   rfc1042 | dot1h
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

启用和禁用到工作组网桥的可靠多播

从接入点到工作组网桥设置的可靠多播消息将多播消息可靠地发送至约 20 个思科 Aironet 工作组网桥 (关联到无线设备)。默认设置为禁用，其降低了多播发送的可靠性，允许更多的工作组网桥关联至无线设备。

该模式下的接入点和网桥不将工作组网桥视为客户端设备，而是类似于接入点或网桥的基础设施设备。将工作组网桥视为基础设施设备表示无线设备可靠地将多播数据包 (包括地址解析协议 (ARP) 数据包) 发送至工作组网桥。

可靠多播发送的性能成本，即将每个多播数据包的副本发送到每个工作组网桥 —— 限制了可关联至无线设备的基础设施设备数量，包括工作组网桥。为将可与无线设备保持无线电链接的工作组网桥的数量增至 20 个以上，无线设备必须降低将多播数据包发送至工作组网桥的可靠性。随着可靠性的下降，无线设备不能确认多播数据包是否到达目标工作组网桥，因此处于无线设备覆盖范围边缘的工作组网桥会丢失 IP 连接。当将工作组网桥视为客户端设备时，性能提高，但可靠性会降低。

提示 固定工作组网桥使用此功能。移动工作组网桥可能会在无线设备覆盖区域的一些位置不接收多播数据，并且会丢失与无线设备的通信，即便它们仍与无线设备关联。

在特权 EXEC 模式下，根据以下步骤配置封装变换方法。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入 2.4 GHz 无线电接口的接口配置模式。

   ```
   interface dot11radio { 0 }
   ```

3. 允许将可靠多播消息发送到工作组网桥

   ```
   infrastructure-client
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的命令禁止将可靠多播消息发送至工作组网桥。

启用和禁用公共安全数据包转发

公众安全数据包转发 (PSPF) 防止关联至接入点的客户端设备与关联至接入点的其他客户端设备意外共享文件或通信。它为客户端设备提供因特网访问能力，但不提供局域网的其他功能。该功能对如安装在机场或在大学校园里的公共无线网络非常有用。

提示　为防止在关联到不同接入点的客户端之间进行通信，必须在连接了无线设备的交换机上设置保护端口。有关设置保护端口的说明，请参见第 283 页的 " 配置保护端口 "。

要通过 CLI 命令启用或禁用无线设备上的 PSPF，请使用网桥组。您可以在本文档中找到关于网桥组及其执行指令的详细说明：

- 请参见 Cisco IOS Bridging and IBM Networking Configuration Guide (思科 IOS 桥接和 IBM 联网配置指南) 中的 " 配置透明网桥 " 部分。

您还可以通过 Web 浏览器界面启用和禁用 PSPF。 PSPF 设置位于 Radio Settings (无线电设置) 页面。

默认情况下禁用 PSPF。在特权 EXEC 模式下，根据以下步骤启用 PSPF。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4 GHz 无线电装置为无线电 0
   - 802.11n 5 GHz 无线电装置是无线电 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 启用 PSPF。

   ```
   bridge-group group port-protected
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的命令禁用 PSPF。

配置保护端口

为防止关联至无线局域网的不同接入点的客户端设备之间进行通信，您必须在连接了无线设备的交换机上设置保护端口。

在特权 EXEC 模式下，根据以下步骤将交换机上的一个端口定义为保护端口。

1. 进入全局配置模式。

   `configure terminal`

2. 进入接口配置模式，并输入要配置的交换机端口的类型和数量，例如 `gigabitethernet0/1`。

   `interface` *`interface-id`*

3. 将接口配置成保护端口。

   `switchport protected`

4. 返回到特权 EXEC 模式。

   `end`

5. 确认您的输入。

   `show interfaces` *`interface-id`* `switchport`

6. (可选) 将您的输入保存到配置文件中。

   `copy running-config startup-config`

要禁止保护端口，使用 `no switchport protected` 接口配置命令。

配置信标周期和 DTIM

信标周期是接入点信标之间的时间间隔，单位为千微秒 (Kμs)。一个 Kμs 等于 1,024 微秒。数据信标速率通常是信标周期的倍数，它确定信标包含交付传输指示消息 (DTIM) 的频率。 DTIM 告知节能客户端设备有一个数据包正等待它们获取。

例如，如果信标周期设为 100 (其默认设置)，且数据信标速率设为 2 (其默认设置)，则无线设备每 200 Kμs 发送一个包含 DTIM 的信标。一个 Kμs 等于 1,024 微秒。

默认信标周期为 100，默认 DTIM 为 2。在特权 EXEC 模式下，根据以下步骤配置信标周期和 DTIM。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 802.11n 2.4 GHz 无线电类型为 0。
   - 802.11n 5 GHz 无线电类型为 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 设置信标周期。输入一个单位为 Kμs 的值。

   ```
   beacon period value
   ```

4. 设置 DTIM。输入一个单位为 Kμs 的值。

   ```
   beacon dtim-period value
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

配置 RTS 阈值和重试次数

RTS 阈值确定无线设备在发送数据包之前发布发送请求 (RTS) 的数据包大小。在有很多客户端设备与无线设备关联的区域，或在客户端相距很远以及只能检测无线设备而不能相互检测的区域，低 RTS 阈值设置极为有用。可输入一个范围为 0...2347 字节的设置。

最大 RTS 重试次数是无线设备停止通过无线电尝试发送数据包之前发布 RTS 的最大次数。输入一个 1...128 之间的数值。

所有接入点和网桥的默认 RTS 阈值是 2347，默认的最大 RTS 重试设置是 32。在特权 EXEC 模式下，根据以下步骤配置 RTS 阈值和最大 RTS 重试次数。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 设置 RTS 阈值。输入一个范围为 0...2347 的 RTS 阈值。

   ```
   rts threshold value
   ```

4. 设置最大 RTS 重试次数。输入一个 1...128 之间的设置。

   ```
   rts retries value
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的命令将 RTS 设置复位到默认值。

配置最大数据重试次数

最大数据重试次数设置确定无线设备在放弃并丢弃数据包之前尝试发送数据包的次数。

默认设置为 32。在特权 EXEC 模式下，根据以下步骤配置最大数据重试次数。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 设置最大数据重试次数。输入一个 1...128 之间的设置。

   ```
   packet retries value
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的命令将设置复位到默认值。

配置分段阈值

分段阈值确定数据包片段的大小 (作为多个片段发送而不是作为一个块发送)。在通信质量不佳或存在大量无线电干扰的区域使用较低的设置。

默认设置为 2338 字节。在特权 EXEC 模式下，根据以下步骤配置分段阈值：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio {0 | 1}
   ```

3. 设置分段阈值。
   - 对于 2.4 GHz 无线电装置，输入一个 256...2346 字节之间的设置。
   - 对于 5 GHz 无线电装置，输入一个 256...2346 字节之间的设置。

   ```
   fragment-threshold value
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用 no 格式的命令将设置复位到默认值。

执行载波载波忙碌测试

您可以执行载波忙碌测试，以检查无线通道上的无线电活动。在载波忙碌测试期间，无线设备断开无线网络设备的所有关联达 4 秒，同时执行载波测试，然后显示测试结果。

在特权 EXEC 模式下，输入以下命令执行载波忙碌测试：

```
dot11 interface-number carrier busy
```

对于 *interface-number*，输入 `dot11radio 0` 在 2.4 GHz 无线电装置上运行测试，或输入 `dot11radio 1` 在 5 GHz 无线电装置上运行测试。

使用 `show dot11 carrier busy` 命令显示载波忙碌测试结果。

配置 ClientLink

思科 ClientLink (请参见波束成形) 是一种智能波束成形技术，它用于将射频信号引导到 802.11a/g 设备，可将性能提高 65%，覆盖率提高达 27%，并减少覆盖空洞。

思科 ClientLink 有助于延长现有 802.11a/g 设备在混合客户端网络中的使用寿命。这对于迁移到 802.11n 并希望确保网络上的所有客户端 (无论哪种类型) 都具备所需的带宽和吞吐量的机构而言十分有利。

使用 CLI 配置 ClientLink

要启用 ClientLink，在 802.11n 无线电接口的接口配置模式下输入该 CLI 命令：

```
beamform ofdm
```

ClientLink 配置选项不通过 GUI 提供。默认情况下禁用 ClientLink。

调试无线电功能

使用 `debug dot11` **特权执行**命令开始调试无线电功能。使用以下命令的 **no** 格式来停止调试操作。命令语法为：

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map
| syslog | virtual-interface}
```

警告：启用调试模式会严重影响性能，甚至完全中断通信。只有在技术支持人员的指导下才能使用。

表 98 - `debug dot11` 命令的语法

语法	激活对象
事件	激活所有无线电相关事件的调试
`packets`	激活已接收和已发送的无线电数据包的调试
`forwarding`	激活无线电转发数据包的调试
`mgmt`	激活无线电接入点管理活动的调试
`network-map`	激活无线电关联管理网络图的调试
`Syslog`	激活无线电系统日志的调试
`virtual interface`	激活无线电虚拟接口的调试

本例显示了如何开始调试所有无线电相关的事件：

```
AP# debug dot11 events
```

本例显示了如何开始调试无线电系统日志：

```
AP# debug dot11 syslog
```

本例显示了如何停止调试所有无线电相关事件：

```
AP# no debug dot11 events
```

提示　命令的默认值为不启用调试。

配置 多个 SSID

本章描述了如何配置和管理接入点上的多个服务集标识符 (SSID) 。

了解多个 SSID

SSID 是无线网络设备用于建立和保持无线连接的唯一标识符。一个网络或子网中的多个接入点可以使用相同的 SSID。SSID 区分大小写，最多可包含 32 个字母数字字符。不得在 SSID 中包含空格。

您可在接入点上配置多达 16 个 SSID，并给每个 SSID 分配不同的配置设置。所有 SSID 均同时激活；也就是说，客户端设备可使用任何一个 SSID 与接入点关联。以下是可分配给每个 SSID 的设置：

- VLAN
- 客户端验证方法

  提示 有关客户端验证类型的详细信息，请参见第 341 页的 “ 配置验证类型 ”。

- 使用 SSID 的客户端关联的最大数目
- 使用 SSID 的 RADIUS 流量结算
- 来宾模式
- 工作组网桥或中继器模式下的验证配置文件 (用户名和密码)
- 重定向从客户端设备接收的数据包

如果您希望接入点允许来自未在配置中指定 SSID 的客户端设备的关联，可创建一个 来宾 SSID。接入点在其信标中包括来宾 SSID。如果来宾模式被禁用，则不在信标消息中广播 SSID。如果不希望没有预配置 SSID 的客户端连接到无线网络，则禁用来宾 SSID 功能。

有关如何配置来宾模式 SSID 和禁止来宾模式 SSID 的信息，请参见第 290 页的 “ 创建全局 SSID”。

如果接入点是一个中继器或用作中继器父节点的根接入点，则可创建一个在中继器模式下使用的 SSID。可为中继器模式 SSID 分配一个验证用户名和密码，使中继器像客户端设备一样对用户网络进行验证。

如果用户网络使用 VLAN，可将一个 SSID 分配给一个 VLAN，将使用此 SSID 的客户端设备归在该 VLAN 组。

重要事项	SSID、 VLAN 和加密方案以一一对应的方式相互映射；一个 SSID 可以映射到一个 VLAN，一个 VLAN 可以映射到一个加密方案。当使用全局 SSID 配置时，您无法配置一个具有两种不同加密方案的 SSID。例如，您不能将带 TKIP 的北方 SSID 应用到接口 dot11 0，将带 WEP128 的北方 SSID 应用于接口 dot11 1。

配置多个 SSID

以下章节包含多个 SSID 的配置信息：

默认 SSID 配置

对于思科 IOS 版本 12.3(7)JA 及更高版本，没有默认 SSID。

创建全局 SSID

您可以配置全局 SSID 或将其配置用于某个特定的无线电接口。当使用 `dot11 ssid` 全局配置命令创建 SSID 时，可使用 `ssid` 配置接口命令将 SSID 分配给特定的接口。

当在全局配置模式下创建了一个 SSID 后，`ssid` 配置接口命令将 SSID 连接至接口，但不进入 ssid 配置模式。但是，如果尚未在全局配置模式下创建 SSID， `ssid` 命令将 CLI 置于新 SSID 的 SSID 配置模式。

在特权 EXEC 模式下开始操作时，请根据以下步骤创建一个全局 SSID。创建 SSID 后，可将其分配给特定的无线电接口。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 创建一个 SSID，然后进入新 SSID 的 SSID 配置模式。

   SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。

   - 第一个字符不能包含 !、 # 或 ; 字符。
   - +、]、 /、 "、制表符和尾随空格对 SSID 而言是无效字符。

   ```
   dot11 ssid ssid-string
   ```

3. (可选) 设置在中继器模式下接入点用于验证网络的验证用户名和密码。

4. (可选) 设置中继器接入点用于关联到根接入点或其他中继器的 SSID 用户名和密码。

   ```
   authentication client
   username username
   password password
   ```

5. (可选) 启用该 SSID 的 RADIUS 结算功能。

   对于 *list-name*，指定结算方法列表。

   ```
   accounting list-name
   ```

6. (可选) 将 SSID 分配给用户网络上的 VLAN。

   将使用 SSID 关联的客户端设备归到该 VLAN 组。您只能将一个 SSID 分配给一个 VLAN。

   ```
   vlan vlan-id
   ```

7. (可选) 指定作为接入点来宾模式 SSID 的 SSID。

   接入点在其信标中包括 SSID，允许来自未指定 SSID 的客户端设备的关联。

   ```
   guest-mode
   ```

8. 该命令控制接入点和网桥相互关联时使用的 SSID。根接入点只允许通过基础设施 SSID 关联一个中继器接入点。

   根网桥只允许通过基础设施 SSID 关联一个非根网桥。中继器接入点和非根网桥使用该 SSID 与根设备关联。

   接入点和网桥 GUI 要求为中继器配置基础设施 SSID，而非根网桥的角色。为工作组网桥角色配置基础设施 SSID 并非强制操作。但是，如果使用 CLI 配置设备角色，则不必配置基础设施 SSID，除非在无线电设备上配置了多个 SSID。如果在无线电设备上配置了多个 SSID，则必须使用 `infrastructure-ssid` 命令指定非根网桥用于连接至根网桥的 SSID。

   无论存在一个还是多个 SSID，当没有配置基础设施 SSID 时，中继器不与网桥关联。

   ```
   infrastructure-ssid [optional]
   ```

9. 进入要分配给 SSID 的无线电接口的接口配置模式。

   ```
   interface dot11radio { 0 | 1 }
   ```

   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

10. 将在步骤 2 中创建的全局 SSID 分配给无线电接口。

    ```
    ssid ssid-string
    ```

11. 返回到特权 EXEC 模式。

    ```
    end
    ```

12. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

重要事项	可使用 `ssid` 命令验证选项配置每个 SSID 的验证类型。请参见第 307 页的 " 将接入点配置为本地验证器 "，了解关于配置验证类型的说明。

使用命令的 no 格式禁用 SSID 或禁用 SSID 功能。

本例显示了如何：

- 命名 SSID。
- 将使用该 SSID 关联的客户端设备的最大数目设为 15。
- 将 SSID 分配给一个 VLAN。
- 将 SSID 分配给一个无线电接口。

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

查看全局配置的 SSID

使用以下命令查看全局配置的 SSID 的配置详情：

```
AP# show running-config ssid ssid-string
```

使用 RADIUS 服务器限制 SSID

为防止客户端设备使用未经授权的 SSID 关联到接入点，您可创建一个客户端必须在 RADIUS 验证服务器上使用的授权 SSID 列表。

SSID 授权过程由以下步骤组成。

1. 客户端设备使用在接入点上配置的任何 SSID 关联至接入点。
2. 客户端开始 RADIUS 验证。
3. RADIUS 服务器返回允许客户端使用的 SSID 列表。接入点检查列表中是否有与客户端所用 SSID 相匹配的 SSID。有三种可能结果：
   a. 如果客户端用于关联到接入点的 SSID 与 RADIUS 服务器返回的允许列表中的一个条目相匹配，则在完成所有验证要求后，允许客户端访问网络。
   b. 如果接入点没有在允许的 SSID 列表中找到客户端的匹配项，则接入点解除与客户端的关联。
   c. 如果 RADIUS 服务器未返回客户端的任何 SSID (无列表)，则管理员尚未配置列表，且允许客户端关联，并尝试进行验证。

您必须以思科 VSA 的格式使用来自 RADIUS 服务器 的 SSID 列表。因特网工程任务组 (IETF) 草案标准规定了一种使用供应商特定属性 (属性 26) 在接入点和 RADIUS 服务器之间传送供应商特定信息的方法。

供应商特定属性 (VSA) 允许供应商支持并不通用的个人扩展属性。思科 RADIUS 工具使用规范中建议的格式支持一个供应商相关选项。思科供应商 ID 为 9，支持的选项为供应商类型 1，即 `cisco-avpair`。Radius 服务器为每个客户端提供 0 个或多个 SSID VSA。

在本例中，以下 AV 对将 SSID batman 添加到某个用户的允许 SSID 列表中：

```
cisco-avpair= ”ssid=batman”
```

有关配置接入点识别和使用 VSA 的说明，请参见第 395 页的 “ 配置接入点进行供应商专有 RADIUS 服务器通信 ”。

配置多个基本 SSID

接入点 802.11a、 802.11g 和 802.11n 无线电支持多达 8 个基本 SSID (BSSID)，这一点与 MAC 地址类似。您可使用多个 BSSID 为每个 SSID 分配唯一的 DTIM，并在信标中广播多个 SSID。较大的 DTIM 值可延长使用 SSID 的节能客户端设备的电池寿命，并广播多个 SSID，使来宾更易于访问用户无线局域网。

当添加或删除多个 BSSID 时，无线局域网上配置为根据接入点 MAC 地址关联至某个特定接入点的设备 (如客户端设备、中继器、热备用单元、或工作组网桥) 会丢失关联。当添加或删除多个 BSSID 时，检查配置为关联到某个特定接入点的设备的关联状态。如有必要，重新配置已解除关联的设备，以使用新的 BSSID MAC 地址。

多个 BSSID 的配置要求

要配置多个 BSSID，接入点必须满足以下最低要求：

- VLAN 必须已配置
- 接入点必须包含一个支持多个 BSSID 的无线电装置。

  为确定无线电装置是否支持多个基本 SSID，输入 `show controllers radio_interface` 命令。如果结果包含以下行，则无线电装置支持多个基本 SSID：

  ```
  Number of supported simultaneous BSSID on
  radio_interface: 16
  ```

使用多个 BSSID 的准则

当配置多个 BSSID 时，请记住以下准则：

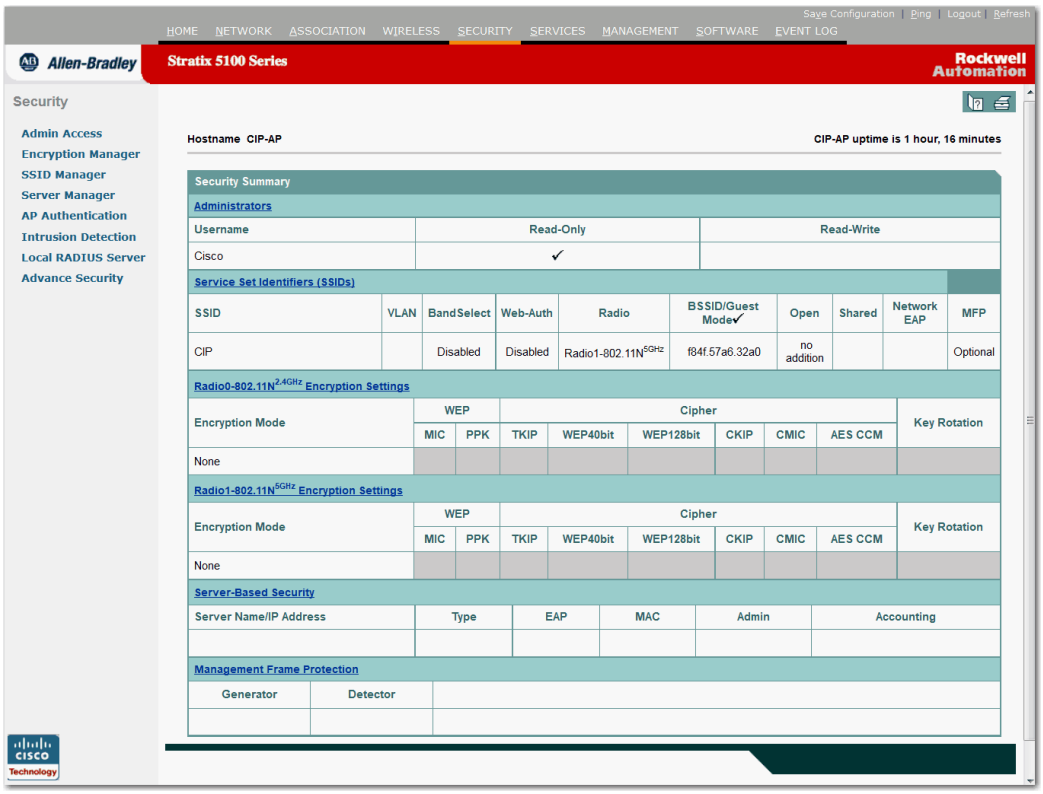
- 当启用多个 BSSID 时，不支持分配了 RADIUS 的 VLAN。
- 当启用 BSSID 时，接入点自动将一个 BSSID 映射到每个 SSID。不能手动将 BSSID 映射到特定的 SSID。
- 在接入点上启用多个 BSSID 时， SSIDL IE 不包含 SSID 列表；它仅包含扩展功能。
- 任何 Wi-Fi 认证客户端设备可使用多个 BSSID 关联到接入点。
- 可在参与 WDS 的接入点上启用多个 BSSID。

配置多个 BSSID

根据以下步骤配置多个 BSSID。

1. 单击 Security (安全)。

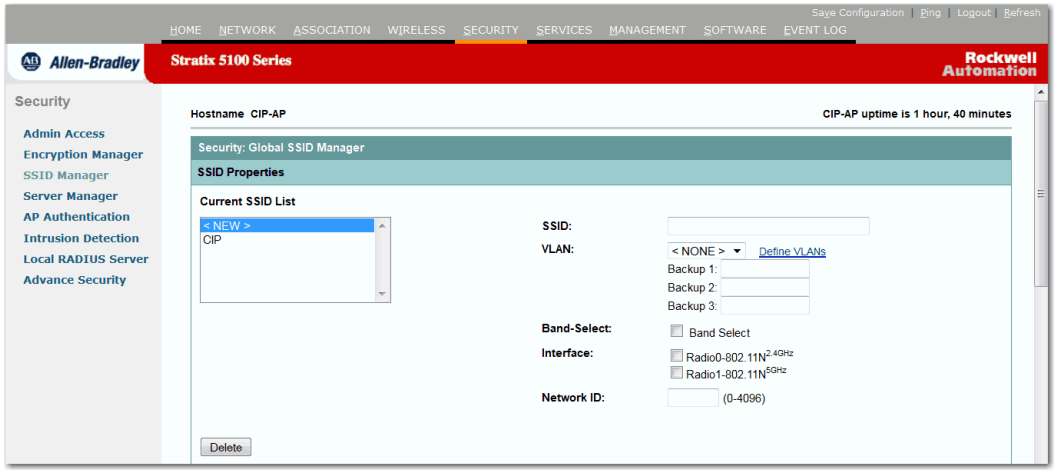
   显示 Security summary (安全概要) 页面。



   如果使用 CLI 而不是 GUI，请参见第 298 页的 “CLI 配置示例 ”中列出的 CLI 命令。

2. 从左侧菜单中单击 SSID Manager (SSID 管理器)。

   显示 SSID Manager (SSID 管理器) 页面。



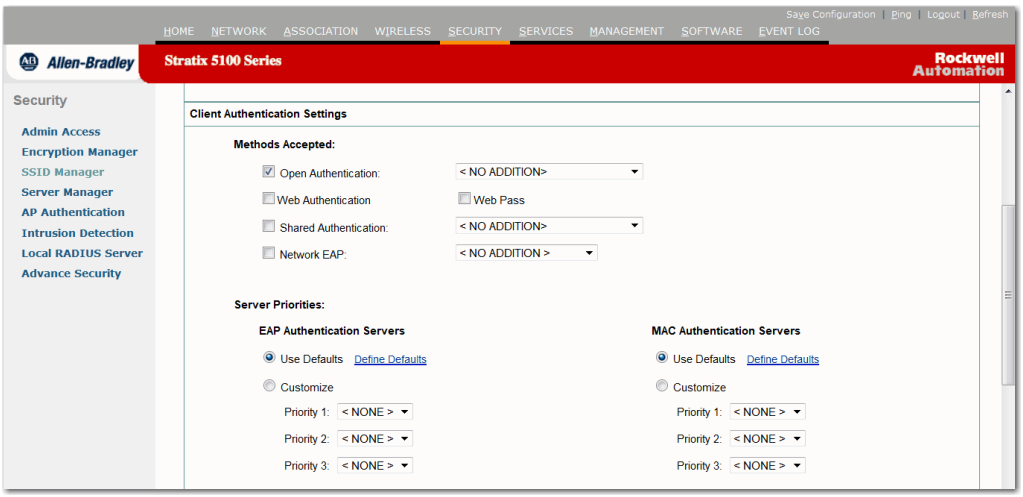
3. 在 SSID 域中输入 SSID 名称。
4. 从 VLAN 下拉菜单中选择分配给 SSID 的 VLAN。

5. 选择启用了 SSID 的无线电接口。

   该 SSID 保持为不活动，直到为某个无线电接口启用它。

6. 在 Network ID (网络 ID) 域中输入 SSID 的网络 ID。

7. 在页面的 Authentication Settings (验证设置)、 Authenticated Key Management (验证密钥管理) 和 Accounting Settings (结算设置) 区域将验证、验证密钥管理和结算设置分配给 SSID。



   BSSID 支持 SSID 所支持的所有验证类型。

8. (可选) 在 Multiple BSSID Beacon Settings (多个 BSSID 信标设置) 区域，选中 Set SSID as Guest Mode (将 SSID 设为来宾模式) 复选框，在信标中包含 SSID。

9. (可选) 要延长使用该 SSID 的节能客户端的电池寿命，选中 Set Data Beacon Rate (DTIM) (设置数据信标速率) 复选框，并输入一个 SSID 的信标速率。

   信标速率决定接入点发送包含传输流量指示消息 (DTIM) 的信标的频率。

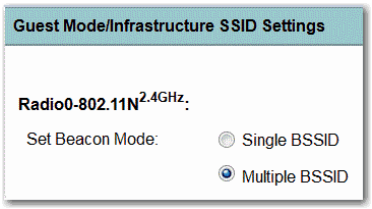
   当客户端设备接收包含一个 DTIM 的信标时，它们通常会被唤醒检查待处理的数据包。 DTIM 之间的间隔越长，客户端睡眠时间越长，从而更节能。相反地， DTIM 周期越短，接收数据包的延时越短，但客户端会被频繁唤醒，使用更多的电池电源。

   默认信标速率是 2。这表示每隔一个信标包含一个 DTIM。

10. 输入范围为 1...100 的信标速率。

    提示　增大 DTIM 周期计数将延迟多播数据包的传送。由于多播数据包已进行缓冲，DTIM 周期计数较大可能导致缓冲区溢出。

11. 在 Guest Mode/Infrastructure SSID Settings (来宾模式 / 基础设施 SSID 设置) 区域，选择 Multiple BSSID (多个 BSSID)。



12. 单击 Apply (应用)。

CLI 配置示例

本例显示了用于启用无线电接口上的多个 BSSID 的 CLI 命令，创建一个名为 *visitor* 的 SSID，将该 SSID 指定为 BSSID，指定将该 BSSID 包含在信标中，设置该 BSSID 的 DTIM 周期，以及将 SSID *visitor* 分配给无线电接口：

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(config-if)# ssid visitor
```

可使用 `dot11 mbssid` 全局配置命令同时启用所有无线电接口 (支持多个 BSSID) 上的多个 BSSID。

显示已配置的 BSSID

使用 `show dot11 bssid` 特权 EXEC 命令显示 SSID 和 BSSID 或 MAC 地址之间的关系。本例显示了命令输出结果：

```
AP1230#show dot11 bssid
Interface     BSSID           Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

分配 SSID 的 SSID 的 IP 重定向

当配置 SSID 的 IP 重定向时，接入点将关联至该 SSID 的客户端设备发送的所有数据包重定向到一个特定的 IP 地址。 IP 重定向主要在为手持式设备服务的无线局域网上使用，这些手持设备使用一个中央软件应用程序，并静态配置为与某个特定 IP 地址进行通信。

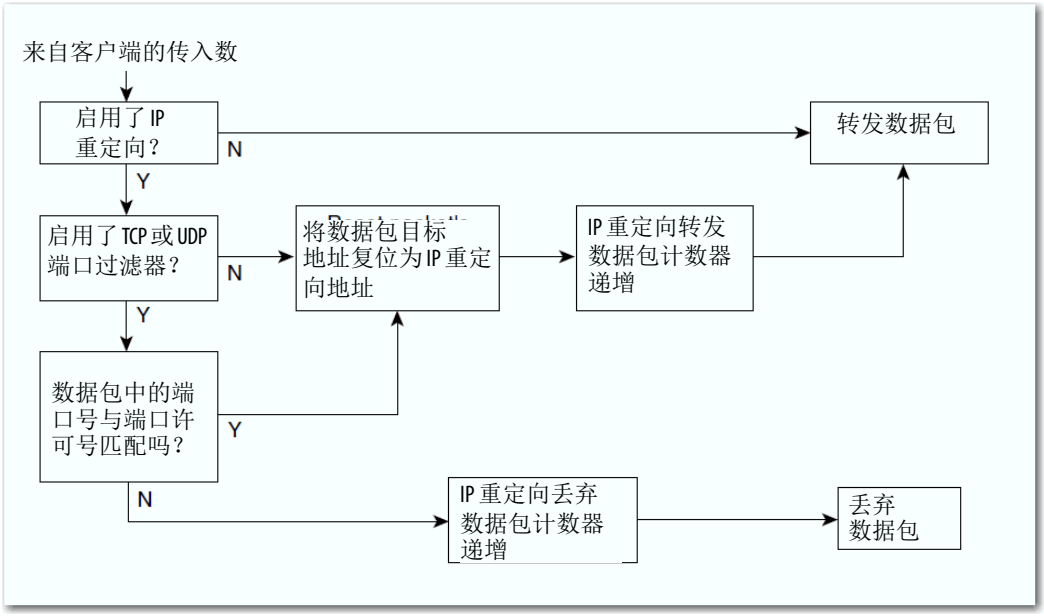
例如，零售商店或仓库的无线局域网管理员可配置条形码扫描器的 IP 重定向。他们使用相同的扫描器应用程序，并将数据发送给同一个 IP 地址。

您可重定向来自使用 SSID 关联的客户端设备的所有数据包，或仅重定向发往特定 TCP 或 UDP 端口 (如在访问控制列表所定义) 的数据包。将接入点配置为仅重定向发往特定端口的数据包时，接入点重定向来自客户端的数据包，并丢弃来自使用 SSID 的客户端的所有其他数据包。

提示 当执行从接入点到使用 IP 重定向 SSID 关联的客户端设备的 ping 测试时，将来自客户端的应答数据包重定向到指定的 IP 地址，不由接入点接收。

下图显示了在接入点收到通过 IP 重定向 SSID 关联的客户端的数据包时发生的过程流。

图 100 - IP 重定向的过程流



使用 IP 重定向的准则

当使用 IP 重定向时，请牢记以下准则：

- 接入点不重定向从客户端设备收到的广播、单播、或多播 BOOTP/DHCP 数据包。
- 传入数据包的现有 ACL 过滤器的优先级高于 IP 重定向。

配置 IP 重定向

在特权 EXEC 模式下，根据以下步骤配置 SSID 的 IP 重定向。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入特定 SSID 的配置模式。

   ```
   dot11 ssid ssid-string
   ```

3. 输入 IP 地址的 IP 重定向配置模式。输入十进制 IP 地址，如本例所示：10.91.104.92

   如果没有指定定义重定向 TCP 或 UDP 端口的访问控制列表 (ACL)，则接入点重定向从客户端设备接收的所有数据包。

   ```
   ip redirection host ip-address
   ```

4. (可选) 指定一个用于数据包重定向的 ACL。

   仅重定向发送至 ACL 中定义的特定 UDP 或 TCP 端口的数据包。接入点丢弃与 ACL 中定义的设置不匹配的所有已接收数据包。**in** 参数指定将 ACL 应用于接入点的传入接口。

   ```
   ip redirection host ip-address access-group acl in
   ```

本例显示了如何在不应用 ACL 的情况下配置 SSID 的 IP 重定向。接入点重定向从关联至 SSID 信标的客户端设备接收的所有数据包。

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config ssid)# ip redirection host 10.91.104.91
AP(config ssid-redirect)# end
```

本例显示了如何仅为发送到 ACL 中指定的特定 TCP 和 UDP 端口的数据包配置 IP 重定向。当接入点接收来自使用 SSID `robin` 命令关联的客户端设备的数据包时，其重定向发送至特定端口的数据包，并丢弃所有其他数据包。

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config ssid)# ip redirection host 10.91.104.91
access-group redirect-acl in
AP(config ssid)# end
```

在 SSIDL IE 中包括 SSID

接入点信标可以只发布一个广播 SSID。但是，您可在接入点信标中使用 SSIDL 信息元素 (SSIDL IE)，提醒接入点上的客户端设备还存在其他 SSID。当指定在 SSIDL IE 中包含 SSID 时，客户端设备检测到该 SSID 可用，并且检测到通过该 SSID 关联所需的安全设置。

重要事项	在接入点上启用多个 BSSID 时， SSIDL IE 不包含 SSID 列表；它仅包含扩展功能。

在特权 EXEC 模式下，根据以下步骤在 SSIDL IE 中包含 SSID。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入特定 SSID 的配置模式。

   ```
   dot11 ssid ssid-string
   ```

3. 在发布接入点扩展功能的接入点信标中包含 SSIDL IE (如 802.1x)，并支持微软无线规范服务 (WPS)。

   使用发布选项在 SSIDL IE 中包含 SSID 名称和功能。使用 wps 选项在 SSIDL IE 中设置 WPS 功能标志。

   ```
   information-element ssidl [advertisement] [wps]
   ```

   使用 no 格式的命令禁用 SSIDL IE。

配置生成树协议

本章介绍了如何在接入点 / 网桥上配置生成树协议 (STP)。

重要事项 STP 仅当接入点处于网桥模式时才可用。

生成树协议 (STP)

STP 是第二层链路管理协议，可在提供路径冗余的同时防止网络中出现环路。为了使第二层以太网络正常工作，任何两个站点之间只能存在一个活动路径。对于无法检测到是连接到单网段 LAN 还是多网段 LAN 的终端站而言，生成树操作是透明的。

在创建容错互联网网络时，网络中的所有节点之间必须有一个无环路径。生成树算法计算通过第 2 层网络的最佳无环路径。无线接入点 / 网桥和交换机等基础设施设备会定期发送和接收称为桥接协议数据单元 (BPDU) 的生成树帧。设备不会转发这些帧，但会使用它们构建无环路路径。

终端站之间存在多个活动路径会导致网络中出现环路。如果网络中存在环路，终端站可能会接收到重复消息。基础设施设备也可能在多个第二层接口获取终端站 MAC 地址。上述情况会造成网络不稳定。

STP 定义了带根网桥的树，它在第 2 层网络中可实现从根到所有基础架构设备的无环路径。

提示　在关于 STP 的探讨中，使用术语“根”来描述两个概念：一是网络上用作生成树中心点的网桥，它被称为根网桥；另一种是每个网桥上的端口，提供到根网桥的最高效路径，它被称为根端口。

这些含义与无线电网络设置中包括根和非根选项的角色无关。如果一个网桥在无线电网络设置中的角色为根网桥，并不一定表示它会成为生成树中的根网桥。在本章中，生成树中的根网桥被称为生成树根。

STP 会强制冗余数据路径进入备用 (被阻) 状态。如果生成树中的网段失效且存在冗余路径，生成树算法将重新计算生成树拓扑并激活备用路径。

当网桥中的两个接口都是环的一部分时，将由生成树端口优先级和路径开销设置决定要置于转发状态或阻止状态的接口。端口优先级值代表接口在网络拓扑中的位置以及位置是否良好，以便于传送流量。路径开销值代表介质速度。

接入点 / 网桥既支持基于 VLAN 的生成树 (PVST)，也支持无 VLAN 的单个 802.1q 生成树。接入点 / 网桥无法运行 802.1s MST 或 802.1d 通用生成树，它们可将多个 VLAN 映射到单实例的生成树中。

接入点 / 网桥可为其上配置的每个活动的 VLAN 维持独立的生成树实例。网桥 ID 由网桥优先级和接入点 / 网桥的 MAC 地址组成，与每个实例相关联。对于每个 VLAN，带最小接入点 / 网桥 ID 的接入点 / 网桥将成为该 VLAN 的生成树根。

配置 STP 功能

STP 仅当接入点处于网桥模式时才可用。完成以下主要步骤，在接入点 / 网桥上配置 STP。

1. 如有必要，为网桥组分配接口和子接口。
2. 为每个网桥组启用 STP。
3. 设置每个网桥组的 STP 优先级。

默认 STP 配置

默认情况下禁用 STP。下表列出了启用 STP 时的默认 STP 设置。

表 99 - 启用 STP 时的默认 STP 值

设置	默认值
Bridge priority (网桥优先级)	32768
Bridge max age (网桥最大寿命)	20
Bridge hello time (网桥问候时间)	2
Bridge forward delay (网桥转发延时)	15
Ethernet port path cost (互联网端口路径开销)	19
Ethernet port priority (以太网端口优先级)	128
Radio port path cost (无线端口路径开销)	33
Radio port priority (无线端口优先级)	128

默认情况下，接入点 / 网桥上的无线电和以太网接口以及本征 VLAN 将被分配给网桥组 1。当启用 STP 并为网桥组 1 分配优先级后，将在无线电和以太网接口以及主 VLAN 上启用 STP，这些接口将采用分配给网桥组 1 的优先级。您可为子接口创建网桥组，并为这些网桥组分配不同的 STP 设置。

配置 STP 设置

在特权 EXEC 模式下，根据以下步骤在接入点 / 网桥上配置 STP。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电或以太网接口或子接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   千兆以太网接口为 0。

   ```
   interface { dot11radio number | gigabitEthernet number }
   ```

3. 将接口分配给网桥组。您可使用 1...255 之间的数字给网桥组编号。

   ```
   bridge-group number
   ```

4. 取消该命令，将自动禁用网桥组的 STP。当输入 bridge *n* protocol ieee 命令时，将启用该接口的 STP。

   ```
   no bridge-group number spanning-disabled
   ```

5. 返回到全局配置模式。

   ```
   exit
   ```

6. 为网桥组启用 STP。对于使用网桥组命令创建的网桥组，必须在每个网桥组上启用 STP。

   ```
   bridge number protocol ieee
   ```

7. (可选) 向网桥组分配优先级。优先级越低，网桥成为生成树根的可能性越大。

   ```
   bridge number priority priority
   ```

8. 返回到特权 EXEC 模式。

   ```
   end
   ```

9. 确认您的输入。

   ```
   show spanning-tree bridge
   ```

10. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

显示生成树状态

要显示生成树状态，可使用下表中的一个或多个特权 EXEC 命令。

表 100 - 显示生成树状态的命令

命令	描述
show spanning-tree	关于网络生成树的信息。
show spanning-tree blocked-ports	该网桥上被阻挡端口列表。
show spanning-tree bridge	该网桥的状态和配置。
show spanning-tree active	仅活动接口上的生成树信息。
show spanning-tree root	生成树根节点信息概要。
show spanning-tree interface *interface-id*	指定接口的生成树信息。
show spanning-tree summary [totals]	端口状态概要或 STP 状态区域显示的总行数。

关于 `show spanning-tree` 特权 EXEC 命令的其他关键字的信息，请参见出版物 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges (思科 Aironet 接入点和网桥的思科 IOS 命令参考)。

将接入点配置为本地验证器

本章描述了如何将接入点配置为本地验证器，以作为小型无线局域网的独立验证器或提供备用验证服务。作为本地验证器，接入点为多达 50 个客户端设备执行 LEAP、 EAP-FAST、和 基于 MAC 的验证。

本地验证

很多可通过 802.1x 验证提高安全性的小型无线局域网不能访问 RADIUS 服务器。在很多使用 802.1x 验证的无线局域网上，接入点依靠一个在远端位置安装的 RADIUS 服务器来对客户端设备进行验证，验证流量必须通过 WAN 链路。如果 WAN 链路发生故障，或因某种原因接入点无法访问 RADIUS 服务器，即使它们希望完全在本地执行操作，客户端设备也无法访问无线网络。

为了在 WAN 链路或服务器出现故障时提供本地验证服务或备用验证服务，您可将接入点配置为充当本地验证服务器。通过使用 LEAP、EAP-FAST、或基于 MAC 的验证，接入点可对多达 50 个无线客户端设备进行验证。接入点每秒最多执行 5 次验证。

您需要手动配置本地验证器接入点的客户端用户名和密码，因为其数据库不与主 RADIUS 服务器同步。此外，还可指定一个 VLAN 及客户端允许使用的 SSID 列表。

提示 如果无线局域网仅包含一个接入点，则可将接入点配置为 802.1x 验证器和本地验证器。但是，当接入点验证客户端设备时，与本地验证器接入点关联的用户将察觉到性能下降。

当接入点无法到达主服务器时，可将接入点配置为使用本地验证器；或当没有 RADIUS 服务器时，将接入点配置为使用本地验证器或作为主验证器。当将本地验证器配置为主服务器的备用设备时，接入点定期检查到主服务器的链接，并在恢复到主服务器的链接时，自动停止使用本地验证器。

重要事项　用作验证器的接入点包含无线局域网的详细验证信息，因此，可以物理方式将其固定，确保其配置安全。

配置本地验证器

将接入点配置为本地验证器时请遵守以下指南。

- 使用一个不需服务大量客户端设备的接入点。当接入点用作验证器时，关联的客户端设备的性能会下降。
- 通过物理方式固定接入点，保护其配置安全。

配置概览

完成以下四个主要步骤设置本地验证器。

1. 在本地验证器上，创建一个授权使用验证器对客户端设备进行验证的接入点列表。使用本地验证器的每个接入点都是网络访问服务器 (NAS)。

   如果本地验证器接入点也为客户端设备提供服务，则必须输入本地验证器接入点，将其作为 NAS。当客户端关联至本地验证器接入点时，接入点自行对客户端进行验证。
2. 在本地验证器上，创建用户组，并配置要应用于每个组的参数 (可选)。
3. 在本地验证器上，创建一个本地验证器已被授权进行验证的列表，该列表可包含多达 50 个 LEAP 用户、 EAP-FAST 用户或 MAC 地址。

   您无需指定本地验证器要执行的验证类型。它将自动对用户数据库中的用户执行 LEAP、 EAP-FAST、或 MAC 地址验证。
4. 在使用本地验证器的接入点上，将本地验证器作为 RADIUS 服务器输入。

   如果本地验证器接入点还为客户端设备提供服务，则必须在本地验证器配置中将本地验证器作为 RADIUS 服务器输入。当客户端关联至本地验证器接入点时，接入点自行对客户端进行验证。

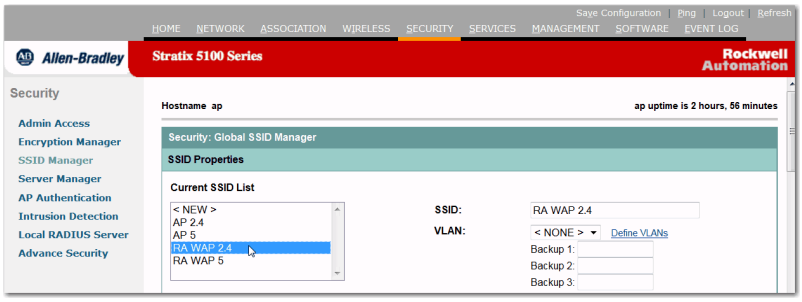
配置 / 启用本地 MAC 验证

使用两种模式的 MAC 验证。一种是仅 MAC 验证，其中 MAC 地址验证作为开放式验证、共享密钥验证或网络 EAP 验证的补充。第二种是 MAC 验证与 EAP 验证共存。该模式结合了 MAC 地址验证和 EAP，对设备或用户进行验证。每种方法的第一步都是配置 SSID。

配置 SSID

根据以下步骤配置 SSID。

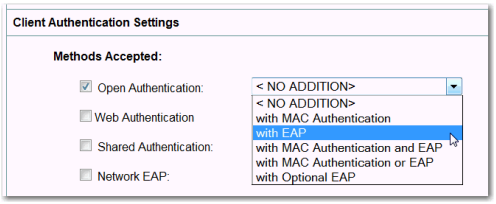
1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中，单击 SSID Manager (SSID 管理器) 转至 SSID Manager (SSID 管理器) 页面。
3. 在当前的 SSID 列表中，为 MAC 验证选择 SSID。



如果需要创建一个新的 SSID，继续执行步骤 4。否则，跳至步骤 7。

4. 从 Current SSID List (当前 SSID 列表) 中选择 <NEW>。
5. 在 SSID 文本域中输入 SSID 名称。
6. 从 VLAN 下拉列表中，选择该 SSID 要使用的 VLAN。

   若 VLAN 未启用，选择 <NONE>。
7. 在 Authentication Methods Accepted (接受的验证方法) 下，选择在该 SSID 上要使用的验证类型。

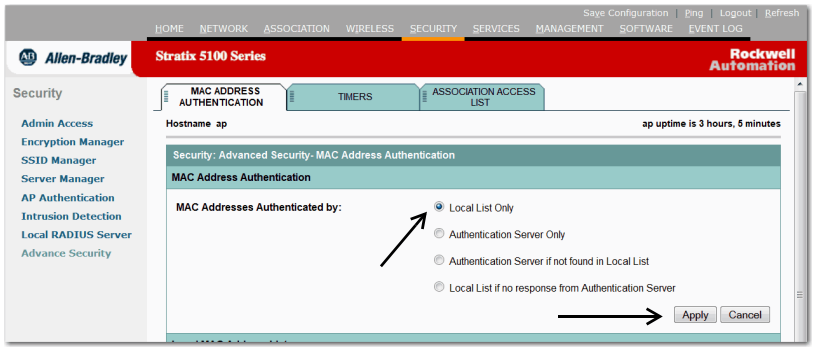


8. 单击 Apply (应用) 创建 SSID。

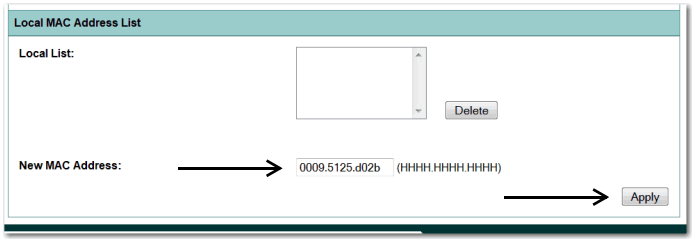
创建本地 MAC 地址列表

SSID 现已配置完成，随后可以创建本地 MAC 地址列表。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中，单击 Advanced Security (高级安全)。
3. 单击 MAC Address Authentication (MAC 地址验证) 选项卡跳转到 MAC Address Authentication (MAC 地址验证) 页面。



4. 位由参数进行验证的 MAC 地址选择 Local List Only (仅本地列表)。
5. 单击页面上 MAC Address Authentication (MAC 地址验证) 部分的 Apply (应用)。
6. 转至 Local MAC Address List (本地 MAC 地址列表) 区域，在 New MAC Address (新 MAC 地址) 参数中输入授权的 MAC 地址。

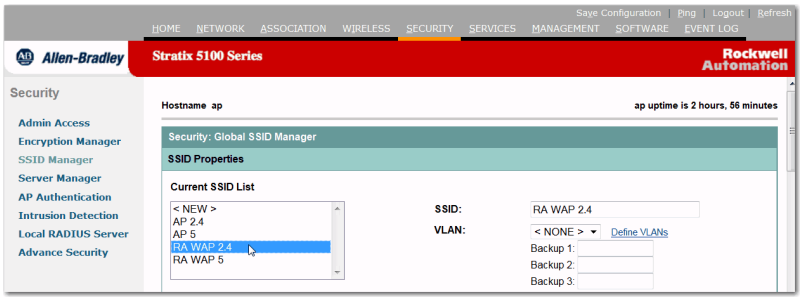


7. 单击页面上 Local MAC Address List (本地 MAC 地址列表) 部分的 Apply (应用)。

通过 RADIUS 服务器创建和启用 MAC 验证

您必须首先配置 SSID。完成以下步骤配置 SSID。

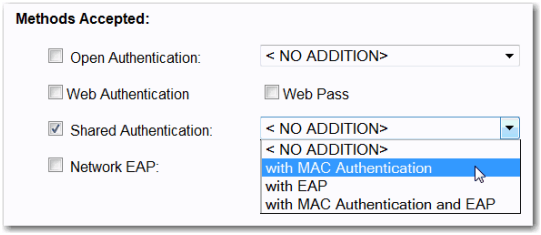
1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中单击 SSID Manager (SSID 管理器)。
3. 在当前的 SSID 列表中，为 MAC 验证选择 SSID。



如果需要创建一个新的 SSID，继续执行步骤 4。否则，跳至步骤 7。

4. 从 Current SSID List (当前 SSID 列表) 中选择 <NEW>。
5. 在 SSID 文本域中输入 SSID 名称。
6. 在 VLAN 列表中选择该 SSID 要使用的 VLAN。

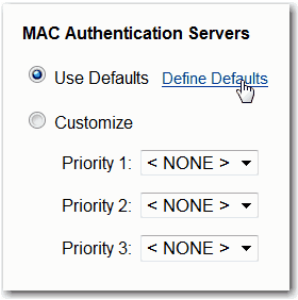
   若 VLAN 未启用，选择 <NONE>。
7. 在 Authentication Methods Accepted (接受的验证方法) 下，选择在该 SSID 上要使用的验证类型。
8. 使用下拉菜单选择 MAC Authentication (MAC 验证)，也可选择 MAC 与 EAP 验证，或者 MAC 或 EAP 验证中任选其一。



9. 使用 EAP 和 MAC 验证服务器部分确定在该 SSID 上使用特定的 RADIUS 服务器的方式。

   您可使用下拉菜单选择使用默认设置或自定义优先级。

   如果单击启用默认值，单击 Define Defaults (定义默认值) 链接转到 Server Manager (服务器管理器) 页。在该页面上配置 RADIUS 服务器。

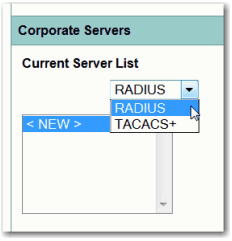


10. 单击 Apply (应用)。

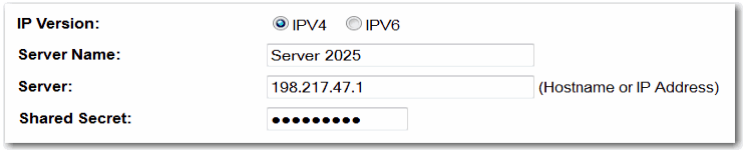
添加 RADIUS 服务器

SSID 现已配置完成，随后可以添加 RADIUS 或 TACACS+ 服务器。完成以下步骤添加 RADIUS 服务器。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中单击 Server Manager (服务器管理器)。
3. 从 Current Server List (当前服务器列表) 下拉菜单中，选择 MAC 验证要使用的服务器。

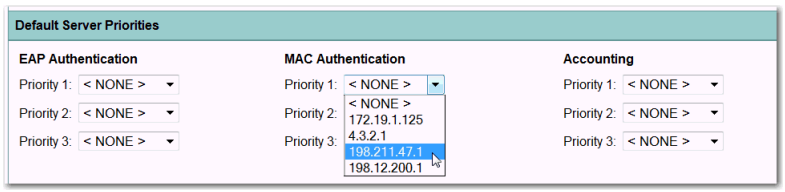
   如果需要创建一个新服务器，继续执行步骤 4 步骤 4。否则跳至步骤 11。
4. 从 Current Server List (当前服务器列表) 中选择 <NEW>。
5. 使用下拉菜单选择 RADIUS 服务器作为服务器类型。
6. 在 Server (服务器) 文本域中输入服务器主机名或 IP 地址。

7. 在 Shared Secret (共享密钥) 文本域中，输入由指定的服务器所使用的与设备上的密钥相匹配的共享密钥。
8. (可选) 在 Authentication Port (验证端口) 参数中输入服务器用于执行验证的端口号。

   例如，思科 RADIUS 服务器 (访问控制服务器 [ACS]) 的端口设置为 1645，而很多 RADIUS 服务器的端口设置为 1812。

9. 从 Default Server Priorities (默认服务器优先级) 区域，确定要分配给每个服务器的优先级。
10. 为该服务器选择优先级 1、 2 或 3。

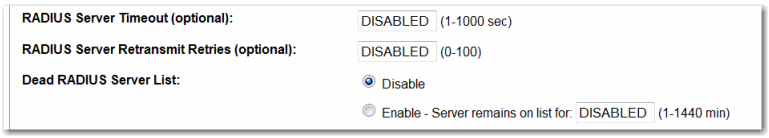


11. 单击 Apply (应用) 添加服务器。

    步骤 步骤 12 至 步骤 16 是可选任务，可跳过这些步骤以加快设置。

12. 单击 Global Properties (全局属性) 选项卡。
13. 在 Accounting Updates Interval (结算更新间隔) 域中，指定要执行结算更新的时间间隔。

14. 在 TACACS+ Server Timeout (TACACS+ 服务器超时) 域中，指定接入点在重新发送请求之前等待 TACACS+ 请求应答的时间 (单位：秒)。
15. 在 RADIUS Server Timeout (RADIUS 服务器超时) 域中，指定接入点在重新发送请求之前等待 RADIUS 请求应答的时间 (单位：秒)。



16. 在 RADIUS Server Retransmit Retries (RADIUS 服务器重传重试次数) 域中，指定接入点放弃之前将每个 RADIUS 请求发送到服务器的次数。

    如果将多个 RADIUS 服务器配置用于 MAC 验证，则启用 Dead Server List (停机服务器列表) 选项。

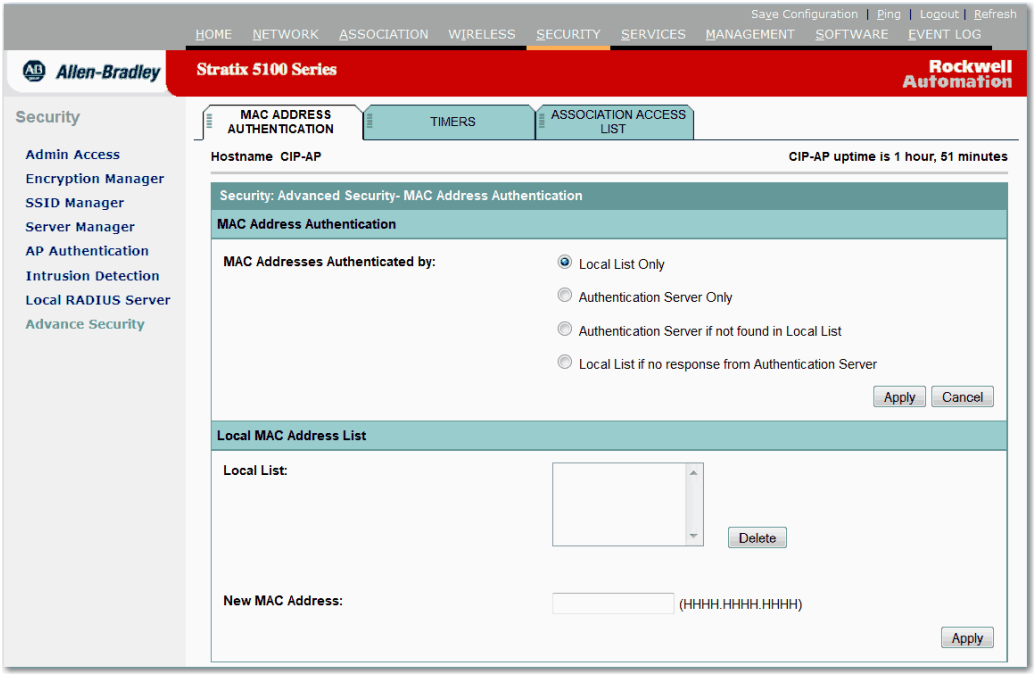
    a. 指定当接入点尝试执行 RADIUS 服务器验证时，跳过未应答的 RADIUS 服务器的时长。
    b. 在 Server remains on list for (服务器保留在列表的时间) 文本域中输入该时长。

17. 单击 Apply (应用)。

设置 MAC 验证方法

在添加 RADIUS 服务器后，可设置 MAC 验证方法。完成以下步骤设置 MAC 验证方法。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中，单击 Advanced Security (高级安全)。
3. 单击 MAC Address Authentication (MAC 地址验证) 选项卡。



4. 如果要将 RADIUS 服务器与本地列表结合使用，则在 Local List (本地列表) 中未找到时选择 Authentication Server (验证服务器)。
5. 单击 MAC Address Authentication (MAC 地址验证) 区域中的 Apply (应用)。

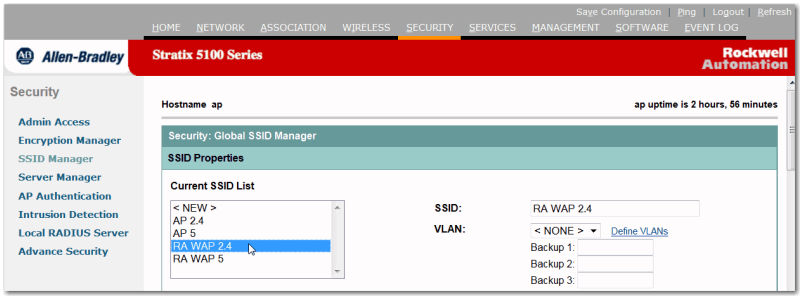
   然后完成步骤 6 至步骤 9。否则，为由参数进行验证的 MAC 地址选择 Authentication Server Only (仅验证服务器)，然后跳至步骤 9。
6. 转至 Local MAC Address List (本地 MAC 地址列表) 区域，在 New MAC Address (新 MAC 地址) 参数中输入授权的 MAC 地址。
7. 单击页面中的 Local MAC Address List (本地 MAD 地址列表) 部分的 Apply (应用)，将该 MAC 地址添加到本地列表中。
8. 如果需要将多个 MAC 地址添加到本地列表中，重复步骤 4 和 5，直到完成该列表。
9. 单击 MAC Address Authentication (MAC 地址验证) 区域中的 Apply (应用)。

配置网络 EAP

设备使用可扩展验证协议 (EAP) 与用户网络上兼容 EAP 的 RADIUS 服务器交互，为无线客户端设备提供验证。

要配置网络 EAP，必须首先配置 SSID。根据以下步骤配置 SSID。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中单击 SSID Manager (SSID 管理器)。
3. 在当前的 SSID 列表中，选择 SSID 作为 EAP 验证类型。

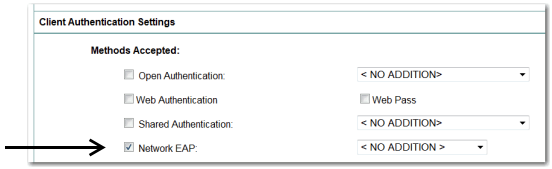


如果需要创建一个新 SSID，继续执行步骤 4。否则跳至步骤 7。

4. 从 Current SSID List (当前 SSID 列表) 中选择 <NEW>。
5. 在 SSID 文本域中输入 SSID 名称。
6. 从 VLAN 下拉列表中，选择该 SSID 要使用的 VLAN。

   若 VLAN 未启用，选择 <NONE>。您可使用 Define VLANs (定义 VLAN) 链接转到 Services > VLAN (服务 > VLAN)，并配置 VLAN。

7. 在 Authentication Methods Accepted (接受的验证方法) 下，选中 Network EAP (网络 EAP) 复选框。



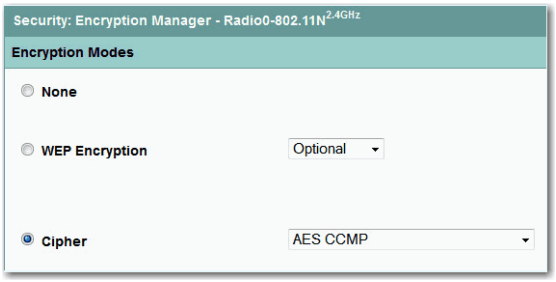
8. 单击 Apply (应用) 创建 SSID。

SSID 现已配置完成，随后必须配置加密。完成以下步骤配置加密。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中单击 Encryption Manager (加密管理器)。
3. 从 Set Encryption Mode and Keys for VLAN (设置 VLAN 的加密模式和密钥) 下拉菜单中，选择与上文所添加的 SSID 相对应的 VLAN。

   当启用 VLAN 后，将显示该 VLAN 下拉菜单。如果不存在 VLAN，则加密设置应用于所有 SSID。若 VLAN 未启用，选择 <NONE>。

4. 在 Encryption Mode (加密模式) 区域，单击 Cipher (密文) 启用 AES CCMP 加密。



加密现已配置完成，随后必须添加一个 RADIUS 或 TACACS+ 服务器。完成以下步骤添加 RADIUS 服务器。

1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中单击 Server Manager (服务器管理器)。
3. 在 Current Server List (当前服务器列表) 中，选择 EAP 验证要使用的服务器。

   如果需要创建一个新的服务器，继续执行步骤 4。否则，跳至步骤 10。
4. 从 Current Server List (当前服务器列表) 中选择 <NEW>。
5. 在 Server (服务器) 文本域中输入服务器主机名或 IP 地址。
6. 使用下拉菜单选择 RADIUS 或 TACACS+ 服务器。
7. 在 Shared Secret (共享密钥) 文本域中，输入由指定的服务器所使用的与设备上的密钥相匹配的共享密钥。
8. 在 Authentication Port (验证端口) 参数中输入服务器用于执行验证的端口号。

   思科 RADIUS 服务器 (访问控制服务器 [ACS]) 的端口设置为 1645，许多 RADIUS 服务器的端口设置为 1812。
9. 输入 RADIUS 服务器用于结算的端口号。

   思科 RADIUS 服务器 (访问控制服务器 [ACS]) 的端口设置为 1646，许多 RADIUS 服务器的端口设置为 1813。查看您的服务器的产品文档，查找正确的结算端口设置。
10. 使用下拉菜单确定要分配给每个服务器的优先级。
11. 单击 Apply (应用) 添加服务器。

    步骤 步骤 12 至 步骤 17 是可选任务，可跳过这些步骤以加快设置。
12. 单击 Global Properties (全局属性) 选项卡。
13. 在 Accounting Updates Interval (结算更新间隔) 域中，指定要执行结算更新的时间间隔。

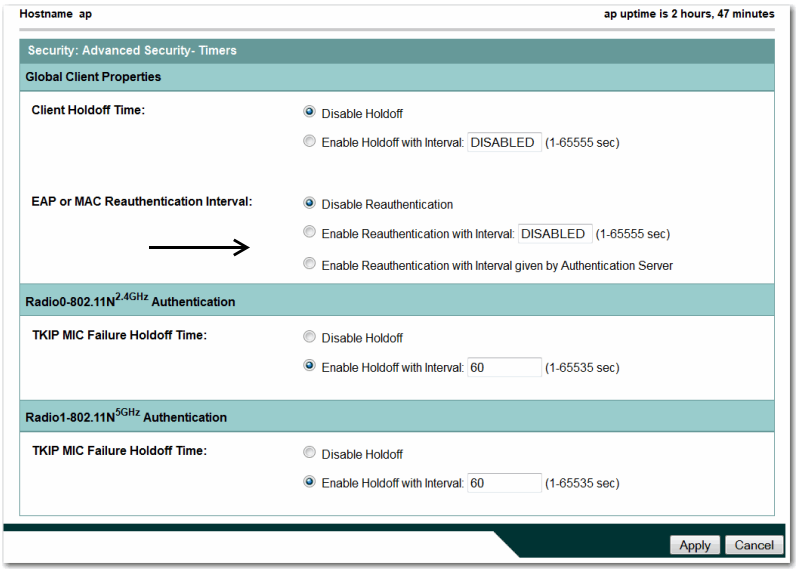
14. 在 TACACS+ Server Timeout (TACACS+ 服务器超时) 域中，指定接入点在重新发送请求之前等待 TACACS+ 请求应答的时间 (单位：秒)。
15. 在 RADIUS Server Timeout (RADIUS 服务器超时) 域中，指定接入点在重新发送请求之前等待 RADIUS 请求应答的时间 (单位：秒)。
16. 在 RADIUS Server Retransmit Retries (RADIUS 服务器重传重试次数) 域中，指定接入点停止尝试之前将每个 RADIUS 请求发送到服务器的次数。

    如果将多个 RADIUS 服务器配置用于 EAP 验证，则启用 Dead Server List (停机服务器列表) 选项。指定当接入点尝试执行 RADIUS 服务器验证时，跳过未应答的 RADIUS 服务器的时长。在 Server remains on list for (服务器保留在列表的时间) 文本域中输入该时长。
17. 单击 Global Server Properties (全局服务器属性) 区域中的 Apply (应用)。

配置高级 EAP 参数

RADIUS 服务器现已添加完成，随后可配置高级 EAP 参数。以下步骤可选，可跳过这些步骤以加快设置。

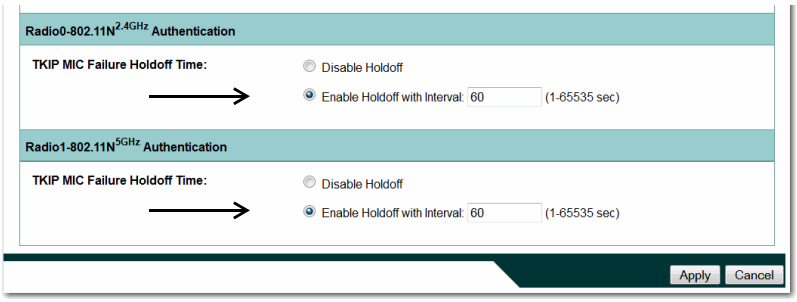
1. 单击 Security (安全)。
2. 从 Security (安全) 菜单中，单击 Advanced Security (高级安全)。
3. 单击 Timers (计时器) 选项卡转到指定 EAP 验证的页面。



4. 选择启用重新验证的某个选项。

   这些间隔选项设置重试 EAP 验证的频率。您可自己输入时间，或使用由 RADIUS 服务器提供的时间。

5. 在 TKIP MIC Failure Holdoff Time (TKIP MIC 故障锁定时间) 文本域中，输入接入点等待无线客户端响应 EAP 验证请求的时长。



6. 单击 Apply (应用)。

使用 CLI 配置本地验证器接入点

在特权 EXEC 模式下，根据以下步骤将接入点配置为本地验证器。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 启用作为本地验证器的接入点，然后进入验证器的配置模式。

   ```
   radius-server local
   ```

4. 将接入点添加到使用本地验证器的单元列表中。

   输入接入点的 IP 地址和用于验证本地验证器和其他接入点之间的通信的共享密钥。您必须在使用本地验证器的接入点上输入此共享密钥。如果本地验证器也为客户端设备提供服务，则必须输入本地验证器接入点，将其作为 NAS。

   提示 密钥字符串中的前导空格会被忽略，但密钥中间和末尾的空格有效。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

   重复以下步骤添加使用本地验证器的每个接入点。

   ```
   nas ip-address key shared-key
   ```

5. (可选) 进入用户组配置模式，然后配置一个可分配共享设置的用户组。

   ```
   group group-name
   ```

6. (可选) 指定一个将由用户组成员使用的 VLAN。

   接入点将组成员移动到该 VLAN，并覆盖其他 VLAN 分配。只能将一个 VLAN 分配给组。

   ```
   vlan vlan
   ```

7. (可选) 最多可输入 20 个 SSID，以限制这些 SSID 的用户组的成员。

   接入点检查客户端用于关联的 SSID 是否与列表中的某个 SSID 相匹配。如果 SSID 不匹配，则客户端解除关联。

   ```
   ssid ssid
   ```

8. (可选) 输入接入点再次对组成员执行验证之前要等待的秒数。

   重验证功能将为用户提供一个新的加密密钥。默认设置为 0，这表示从不要求组成员执行重验证。

   ```
   reauthentication time seconds
   ```

9. (可选) 为了防止密码猜测攻击，可在设定的错误密码次数后将用户组成员锁定一段时间。
   - count - 触发用户名锁定的失败密码次数。
   - time - 锁定持续的秒数。如果输入 `infinite`，则管理员必须手动解锁被锁定的用户名。

     有关解锁客户端设备的说明，请参见第 327 页的 “ 解锁锁定的用户名 ”。

   ```
   block count count
   time { seconds | infinite }
   ```

10. 退出组配置模式并返回验证器配置模式。

    ```
    exit
    ```

11. 输入允许使用本地验证器执行验证的 LEAP 和 EAP-FAST 用户。

    您必须为每个用户输入用户名和密码。如果您只知道密码的 NT 值 (该值可在验证服务器数据库中找到)，可输入 NT 哈希值 (一串十六进制数字)。

    要添加用于基于 MAC 验证的客户端设备，输入客户端的 MAC 地址作为用户名和密码。输入 12 个十六进制数字作为用户名和密码，数字之间不得有句点或短划线。例如，对于 MAC 地址 0009.5125.d02b，输入 *00095125d02b* 作为用户名和密码。

    为限制只有用户才能执行 MAC 验证，输入 `mac-auth-only`。

    要将用户添加到某个用户组，输入组名。如果未指定组，则不将该用户分配到特定的 VLAN，且始终不会强制执行重验证。

    ```
    user username
    { password | nthash } password
    [ group group-name ]
    [mac-auth-only]
    ```

12. 返回到特权 EXEC 模式。

    ```
    end
    ```

13. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

本例说明了如何创建一个由三个接入点使用的本地验证器，其中接入点包含三个用户组和多个用户：

```
AP# configure terminal
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74
group clerks
AP(config-radsrv)# user stpatrick password snake100
group clerks
AP(config-radsrv)# user nick password uptown group
clerks
AP(config-radsrv)# user 00095125d02b password
00095125d02b group clerks mac-auth-only
AP(config-radsrv)# user 00095125d02b password
00095125d02b group cashiers
```

```
AP(config-radsrv)# user 00079431f04a password
00079431f04a group cashiers

AP(config-radsrv)# user carl password 272165 group
managers

AP(config-radsrv)# user vic password lid178 group
managers

AP(config-radsrv)# end
```

配置其他接入点使用本地验证器

将本地验证器添加到接入点的服务器列表的方式与添加其他服务器的方式相同。有关在接入点上设置 RADIUS 服务器的详细说明，请参见第 377 页的 “ 配置 RADIUS 和 TACACS+ 服务器 ”

重要事项	如果本地验证器接入点也为客户端设备提供服务，则必须将本地验证器配置为自行对客户端设备进行验证。

在使用本地验证器的接入点上，使用 `radius-server host` 命令输入作为 RADIUS 服务器的本地验证器。

接入点尝试使用服务器的顺序与您在接入点配置中输入的服务器顺序相匹配。

如果第一次配置接入点使用 RADIUS，首先输入主 RADIUS 服务器，最后输入本地验证器。

重要事项	您必须输入 1812 作为验证端口，输入 1813 作为结算端口。本地验证器在 UDP 端口 1813 上侦听 RADIUS 结算数据包。它会弃用结算数据包，而将应答数据包发送回 RADIUS 客户端，以防止客户端认为服务器已关闭。

使用 `radius-server deadtime` 命令设置时间间隔。在此间隔内，接入点不尝试使用不应答的服务器。这就无需在尝试下一个已配置的服务器之前等待请求超时。在您指定的时长 (单位：分钟) 内 (高达 1440 (24 小时))，附加请求跳过标记为停机的服务器。

本例说明了如何设置两个主服务器以及一个本地验证器，其中服务器停机时间为 10 分钟：

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001 key 77654

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646 key 77654

AP(config)# radius-server host 10.91.6.151 auth-port
1812 acct-port 1813 key 110337

AP(config)# radius-server deadtime 10
```

在本例中，如果到主服务器的 WAN 链路发生故障，则在启用 LEAP 的客户端设备关联时，接入点完成以下步骤。

1. 它尝试第一个服务器，超时多次，然后将第一个服务器标记为停机。
2. 它尝试第二个服务器，超时多次，然后将第二个服务器标记为停机。
3. 它使用本地验证器进行尝试并获得成功。

如果在 10 分钟的停机间隔内另一个客户端设备需要执行验证，则接入点跳过前两个服务器，首先尝试本地验证器。在停机间隔后，接入点尝试使用主服务器进行验证。设置停机时间时，必须在跳过停机服务器和尽量通过主服务器检查 WAN 链路并开始运行之间取得良好的折衷。

每次接入点尝试使用停机的主服务器时，尝试验证的客户端设备会报告验证超时。当主服务器超时且接入点尝试本地验证器时，客户端设备执行重试。可以延长思科客户端设备的超时值，以适应预期的服务器超时。

要从接入点配置删除本地验证器，使用 `no radius-server host hostname | ip-address` 全局配置命令。

配置 EAP-FAST 设置

EAP-FAST 验证的默认设置适用于大多数无线局域网。但是，您可根据网络要求自定义凭证超时值、权限 ID 和服务器密钥。

配置 PAC 设置

本节介绍了如何配置保护访问凭证 (PAC) 设置。 EAP-FAST 客户端设备第一次尝试使用本地验证器执行验证时，本地验证器为客户端生成一个 PAC。也可以手动生成 PAC，然后使用 Aironet Client 实用工具导入 PAC 文件。

PAC 有效期

您可限制 PAC 有效的天数以及在有效期结束后 PAC 仍有效的宽限期。默认情况下， PAC 的有效期为 2 天 (一天默认情况下间 + 一天宽限期)。您还可将有效期和宽限期设置应用到一组用户。

使用以下命令配置 PAC 的有效期和宽限期：

```
AP(config-radsrv-group)# [no] eapfast pac expiry
days [grace days]
```

输入一个 2...4095 之间的天数。输入 no 格式的命令将有效期或宽限期设为无穷大。

在本例中，用户组的 PAC 有效期为 100 天，宽限期为 2 天：

```
AP(config-radsrv-group)# eapfast pac expiry 100
grace 2
```

手动生成 PAC

本地验证器自动为请求 PAC 的 EAP-FAST 客户端生成 PAC。但是，对于某些客户端设备，您可手动生成 PAC。输入命令时，本地验证器生成一个 PAC 文件并将其写入到指定的网络位置。用户将 PAC 文件导入到客户端配置文件。

使用以下命令手动生成 PAC：

```
AP# radius local-server pac-generate filename
username [password password] [expiry days]
```

输入 PAC 文件名时，输入本地验证器写入 PAC 文件的完整路径 (如 tftp://172.1.1.1/test/user.pac)。密码可选，若没有指定，使用 CCX 客户端理解的默认密码。有效期也是可选的，若没有指定，默认情况下间为一天。

在本例中，本地验证器为用户名 *joe* 生成 PAC，通过密码 `bingo` 对文件提供密码保护，将 PAC 有效期设为 10 天，并将 PAC 文件写入到 TFTP 服务器 (10.0.0.5):

```
AP# radius local-server pac-generate tftp://
10.0.0.5 joe password bingo expiry 10
```

配置权限 ID

所有 EAP-FAST 验证器均通过一个权限身份 (AID) 进行识别。本地验证器将其 AID 发送至验证客户端，客户端检查其数据库中是否有匹配的 AID。如果客户端不能识别该 AID，它将请求一个新的 PAC。

使用以下命令将 AID 分配给本地验证器：

```
AP(config-radserv)# [no] eapfast authority id
identifier
```

```
AP(config-radserv)# [no] eapfast authority info
identifier
```

eapfast authority id 命令分配客户端设备在验证期间使用的 AID。

配置服务器密钥

本地验证器使用服务器密钥所生成的 PAC 加密，并在对客户端执行验证时解密 PAC。服务器保持两个密钥 —— 一个主密钥和一个辅助密钥，并使用主密钥来加密 PAC。默认情况下，服务器使用默认值作为主密钥，但不使用辅助密钥，除非您配置了辅助密钥。

当本地验证器接收到客户端 PAC 时，它尝试用主密钥解密 PAC。如果主密钥解密失败且配置过辅助密钥，验证器将尝试使用辅助密钥解密 PAC。如果解密失败，验证器将拒绝 PAC，将其视为无效。

使用以下命令配置服务器密钥：

```
AP(config-radsrv)# [no] eapfast server-key primary
{[auto-generate] | [ [0 | 7] key]}

AP(config-radsrv)# [no] eapfast server-key
secondary [0 | 7] key
```

密钥可包含多达 32 个十六进制数字。

- 在密钥前加 0，输入一个未加密的密钥。
- 在密钥前加 7，输入一个加密密钥。

使用 no 格式的命令将本地验证器复位到默认设置，即将默认值作为主密钥。

由接入点时钟引起的潜在 PAC 故障

本地验证器使用接入点时钟来产生 PAC 以及确定 PAC 是否有效。但是，依靠接入点时钟会导致 PAC 故障。

如果本地验证器接入点从 NTP 服务器接收其时间设置，在启动与同步 NTP 服务器之间有一个时间间隔。在此间隔内，接入点使用其默认情况下间设置。

如果本地验证器在此间隔内生成 PAC，则在接入点接收到来自 NTP 服务器的新时间设置时， PAC 失效。如果 EAP-FAST 客户端尝试在启动和 NTP 同步之间的时间间隔内执行验证，本地验证器拒绝客户端 PAC，将其视为无效。

如果本地验证器没有从 NTP 服务器接收其时间设置，则它频繁地重新启动，由本地验证器生成的 PAC 会在适当的时间失效。当接入点重新启动时复位接入点时钟，因此时钟上的经过时间尚未达到 PAC 有效期。

将本地验证器限制为一种验证类型

默认情况下，本地验证器接入点执行客户端设备的 LEAP 验证、EAP-FAST 验证和基于 MAC 的验证。但是，您可将本地验证器限制为仅执行一种或两种验证类型。使用 no 格式的验证命令将验证器限制为一种验证类型：

```
AP(config-radsrv)# [no] authentication [eapfast]
[leap] [mac]
```

由于默认情况下启用所有验证类型，因此输入 **no** 格式的命令来禁用验证类型。例如，如果希望验证器仅执行 LEAP 验证，请输入以下命令：

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

解锁锁定的用户名

在锁定时间到期之前，或将锁定时间设为无穷大时，可以解锁用户名。在本地验证器的特权 EXEC 模式下，输入以下命令解锁锁定的用户名：

```
AP# clear radius local-server user username
```

查看本地验证器统计数据

在特权 EXEC 模式下，输入以下命令查看本地验证器收集的统计数据：

```
AP# show radius local-server statistics
```

本例显示了本地验证器的统计数据：

```
Successes            : 0          Unknown usernames    : 0
Client blocks        : 0          Invalid passwords    : 0
Unknown NAS          : 0          Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes            : 0          Unknown usernames    : 0
Client blocks        : 0          Invalid passwords    : 0
Corrupted packet     : 0          Unknown RADIUS message : 0
No username attribute : 0         Missing auth attribute : 0
Shared key mismatch  : 0          Invalid state attribute: 0
Unknown EAP message  : 0          Unknown EAP auth type  : 0
Auto provision success : 0        Auto provision failure : 0
PAC refresh          : 0          Invalid PAC received   : 0
```

```
Username                    Successes  Failures  Blocks
nicky                               0         0       0
jones                               0         0       0
jsmith                              0         0       0
Router#sh radius local-server statistics
Successes             : 1           Unknown usernames      : 0
Client blocks         : 0           Invalid passwords      : 0
Unknown NAS           : 0           Invalid packet from NAS: 0
```

统计数据的第 1 部分列出了来自本地验证器的累计统计数据。

第二部分列出了授权使用本地验证器的每个接入点 (NAS) 的统计数据。本节中的 EAP-FAST 统计数据包括以下信息：

- 自动配置成功 —— 自动生成的 PAC 数目
- 自动配置失败 —— 由于无效握手数据包或无效用户名或密码而未生成 PAC 的数目
- PAC 刷新 —— 客户端刷新 PAC 的次数
- 接收的无效 PAC —— 接收的已过期、验证器不能解密或分配给不位于验证器数据库中的客户端用户名的 PAC 数目

第 3 部分列出了单个用户的统计数据。如果某个用户被阻止，且锁定时间设为无穷大，则在该用户的统计数据行末尾显示 *blocked*。如果锁定时间不是无穷大，则在该用户的统计数据行末尾显示 *Unblocked in x seconds*。

使用以下特权 EXEC 模式命令将本地验证器的统计数据复位到零：

```
AP# clear radius local-server statistics
```

调试消息

在特权 EXEC 模式下，输入以下命令控制本地验证器的调试信息显示：

```
AP# debug radius local-server { client | eapfast |
error | packets}
```

使用命令选项显示以下调试信息：

- 使用 `client` 选项来显示与客户端验证失败有关的错误消息。
- 使用 `eapfast` 选项显示与 EAP-FAST 验证有关的错误消息。使用子选项选择特定的调试信息：
  - `encryption` —— 关于所接收和发送的数据包的加密和解密信息。
  - `events` —— 关于所有 EAP-FAST 事件的信息。
  - `pac` —— 与 PAC 有关的事件信息，例如， PAC 生成和验证。
  - `pkts` —— 从 EAP-FAST 客户端收发的数据包。
- 使用 `error` 选项显示与本地验证器有关的错误消息。
- 使用 `packets` 选项打开已发送和已接收的 RADIUS 数据包内容的显示。

备注：

配置密文组

本章介绍了如何配置使用 Wi-Fi 保护访问 (WPA) 和思科集中密钥管理 (CCKM) 验证密钥管理所需的密文组，包括 AES、消息完整性检查 (MIC)、临时密钥完整性协议 (TKIP) 和 广播密钥旋转。

密文组

电台覆盖范围内的任何人都可以调到电台频率并收听广播信号。类似地，在接入点覆盖范围内，任何无线网络设备都可收到接入点的无线电传输信号。我们建议您在无线网络中使用完整的加密方式。

密文组是一组加密和完整性算法，用于保护无线局域网上的无线电通讯。您必须使用密文组来启用 WPA 或 CCKM。

密文组可使用 CLI 中的 “encryption mode cipher” 命令或 Web 浏览器界面中的密码下拉菜单来启用。包含 AES CCMP 的密文组为无线局域网提供最高的安全性，只包含 WEP 的密文组最不安全，不建议使用。

AES-CCMP —— AES-CCMP 基于美国国家标准与技术研究院 FIPS 出版物 197 中定义的高级加密标准 (AES)，是一种对称分组密文算法，可使用 128、 192 和 256 位密钥加密和解密数据。 AES-CCMP 优于 WEP 加密，在 IEEE 802.11i 标准中定义。

- WEP (有线等效保密)

  WEP 是一种 802.11 标准加密算法，最初设计用于为无线局域网提供有线局域网相同等级的隐私性。但由于基本 WEP 结构存在缺陷，攻击者不需要费太大的功夫便能破坏隐私性。

  提示 要正确运行，需要将思科 802.11n 无线电装置配置为不加密或 AES-CCMP 加密。

- TKIP (临时密钥完整性协议)

  TKIP 是一种围绕着 WEP 的算法组，设计用于在运行 WEP 的旧式硬件上实现最高的安全性。广播密钥旋转 (也被称为 “ 组密钥更新 ”)

  广播密钥旋转允许接入点生成完全随机的组密钥，并定期更新所有具有密钥管理功能的客户端。 Wi-Fi 保护访问 (WPA) 还提供附加的组密钥更新选项。

关于 WPA 的详细信息，请参见第 340 页的 “WPA 密钥管理 ”。

重要事项	当启用广播密钥旋转时，使用静态 WEP 的客户端设备无法使用接入点。当仅使用密钥管理 (例如，动态 WEP (802.1x)、 EAP 与 WPA 或预共享密钥) 时支持广播密钥旋转。

配置密文组

以下小节介绍了如何配置密文组和附加功能，例如， MIC、 TKIP 和广播密钥旋转。

启用密文组

在特权 EXEC 模式下，根据以下步骤启用密文组。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。 2.4 GHz 无线电方式为 radio 0， 5 GHz 无线电方式为 radio 1。

   ```
   interface dot11radio { 0 | 1 }
   ```

3. 启用您所需保护的密文组。

   第 333 页的表 101 中列出了匹配您所配置的验证密钥管理的密文组选择指南。

4. (可选) 选择您想要启用安全功能的 VLAN。

5. 设置密文选项。

要配置密文模式 `TKIP + WEP 128` 或 `TKIP + WEP 40`，必须将 WPA 密钥管理配置为可选。

```
encryption
[vlan vlan-id]
mode ciphers
{[aes | aes-ccm | ckip | tkip]} {[wep128 | wep40]}
```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用加密命令的 `no` 格式禁用密文组。

将 WPA 或 CCKM 与密文组相匹配

如果您将接入点配置为使用 WPA 或 CCKM 验证密钥管理，则必须选择兼容验证密钥管理类型的密文组。下表列出了兼容 WPA 和 CCKM 的密文组。

表 101 - 兼容 WPA 和 CCKM 的密文组

验证密钥管理类型	兼容密文组
CCKM	wep128 加密模式密文 wep40 加密模式密文 ckip 加密模式密文 cmic 加密模式密文 ckip-cmic 加密模式密文 tkip 加密模式密文 aes 加密模式
WPA	tkip 加密模式密文 tkip wep128 加密模密文 tkip wep40 加密模式密文 eas 加密模式密文 tkip wep128 和 tkip wep-40 加密模式密文仅在将 WPA 配置为可选时使用。

重要事项

如果使用 WPA 和 CCKM 进行密钥管理，则仅支持 tkip 和 aes 密文。如果仅使用 CCKM 进行密钥管理，则支持 ckip、cmic、 ckip-cmic、 tkip、 wep 和 aes 密文。

当为 SSID 配置 TKIP 密文 (不是 TKIP + WEP 128 或 TKIP + WEP 40) 时，该 SSID 必须使用 WPA 或 CCKM 密钥管理。对于使用 TKIP 密文、但未启用 WPA 或 CCKM 密钥管理的 SSID，客户端验证将失败。

关于 WPA 的完整描述和配置验证密钥管理的说明，请参见第 340 页的 “WPA 密钥管理 ”。

启用和禁用广播密钥旋转

广播密钥旋转默认为禁用。当启用广播密钥旋转时，使用静态 WEP 的客户端设备无法使用接入点。当仅使用密钥管理 (例如，动态 WEP (802.1x)、 EAP 与 WPA 或预共享密钥) 时支持广播密钥旋转。

在特权 EXEC 模式下，根据以下步骤启用广播密钥旋转。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio { 0 | 1 }
   ```

3. 启用广播密钥旋转。
4. 输入每次广播密钥旋转之间相隔的秒数。
5. (可选) 输入想要启用广播密钥旋转的 VLAN。

关于启用验证密钥管理的详细说明，请参见第 335 页的 “ 配置验证类型 ”。

```
broadcast-key
change seconds
[ vlan vlan-id ]
[ membership-termination ]
[ capability-change ]
```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用加密命令的 no 格式禁用广播密钥旋转。

本例启用 VLAN 22 上的广播密钥旋转，并将旋转间隔设为 300 秒：

```
ap5100# configure terminal
ap5100(config)# interface dot11radio 0
ap5100(config-if)# broadcast-key vlan 22 change 300
ap5100(config-if)# end
```

配置验证类型

本章介绍了如何在接入点上配置验证类型。

验证类型

验证类型与为接入点配置的 SSID 绑定在一起。如果要将同一接入点与不同类型的客户端设备使用，您可配置多个 SSID。

关于配置多个 SSID 的完整说明，请参见第 289 页的 “ 配置 多个 SSID”。

在无线客户端设备可通过接入点与网络通信之前，接入点必须对其进行验证。为确保最高安全性，网络也必须使用 MAC 地址或 EAP 验证 (网络中验证服务器所用的验证类型) 对客户端设备进行验证。

重要事项	默认情况下，接入点的服务类型属性设置为 “ 仅验证 ”，它向验证服务器发送重新验证请求。但一些 Microsoft IAS 服务器不支持 “ 仅验证 ” 服务类型属性。根据用户要求，将服务类型属性设为 :dot11 aaa authentication attributes service-type login-user 或 dot11 aaa authentication attributes service-type framed-user。默认情况下，服务类型登录将在访问请求中发送。

接入点使用多种验证机制或类型，且可同时使用多种。

接入点开放式验证

开放式验证允许任何设备进行验证并尝试与接入点通信。使用开放式验证，任何无线设备都可进行接入点验证。

接入点共享密钥验证

思科提供符合 IEEE 802.11b 标准的共享密钥验证。但由于共享密钥存在安全性缺陷，应避免使用它。

在共享密钥验证期间，接入点向任何尝试与接入点通信的设备发送未加密的质询文本串。请求验证的设备加密质询文本，并将其发回接入点。如果质询文本加密正确，接入点允许请求设备进行验证。

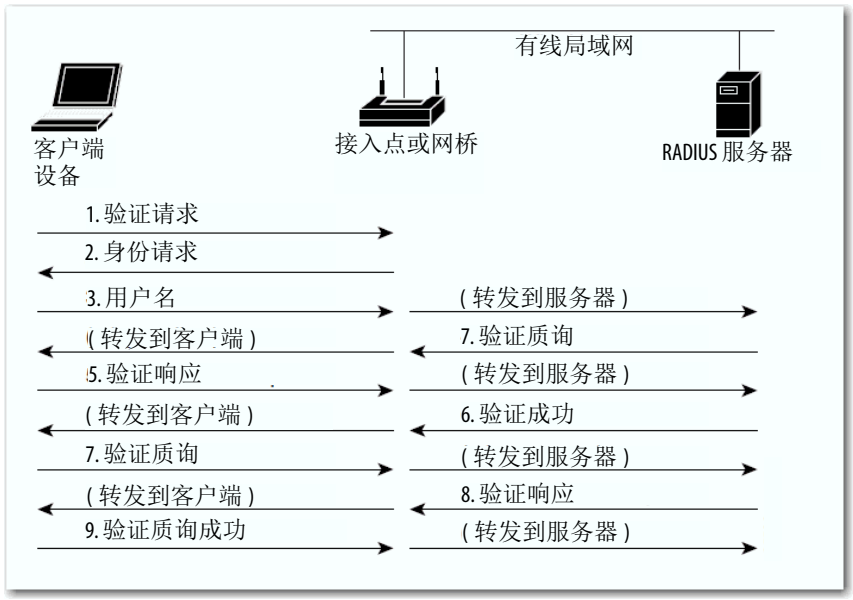
但是，未加密的质询和加密的质询均可被监控，因此，入侵者可通过比较未加密和加密文本串来计算 WEP 密钥，致使接入点易受攻击。由于存在这一缺陷，共享密钥验证的安全性不如开放式验证。与开放式验证一样，共享密钥验证不依靠网络中的 RADIUS 服务器。

网络 EAP 验证

这种验证类型可为无线网络提供最高的安全级别。通过使用可扩展的验证协议 (EAP) 与 EAP 的 RADIUS 服务器交互，接入点可帮助无线客户端设备和 RADIUS 服务器执行相互验证。

当接入点和客户端设备启用 EAP 时，将按照下图所示的顺序执行网络验证。

图 101 - EAP 验证顺序



在步骤 1...9 中，无线客户端设备和有线局域网中的 RADIUS 服务器使用 802.1x 和 EAP 通过接入点执行相互验证。 RADIUS 服务器向客户端发送验证质询。

客户端使用用户提供的密码执行单向加密，以生成质询响应，并将其发送给 RADIUS 服务器。通过使用来自用户数据库的信息， RADIUS 服务器创建自己的响应，并将其与客户端的响应相比较。当 RADIUS 服务器验证客户端后，将以相反的顺序重复该过程，由客户端验证 RADIUS 服务器。

EAP 验证类型有多种，但无论采用哪种类型，接入点的工作方式都相同：它将来自无线客户端设备的验证消息转发到 RADIUS 服务器，并将来自 RADIUS 服务器的验证消息转发到无线客户端设备。

关于在接入点上设置 EAP 的说明，请参见第 341 页的 “ 将验证类型分配到 SSID”。

网络 MAC 地址验证

接入点将无线客户端设备的 MAC 地址转发到网络中的 RADIUS 服务器，服务器对照允许 MAC 地址列表检查该地址。由于入侵者可伪造 MAC 地址，基于 MAC 的验证的安全性不如 EAP 验证。

但对于没有 EAP 功能的客户端设备，基于 MAC 的验证可作为备用验证方法。

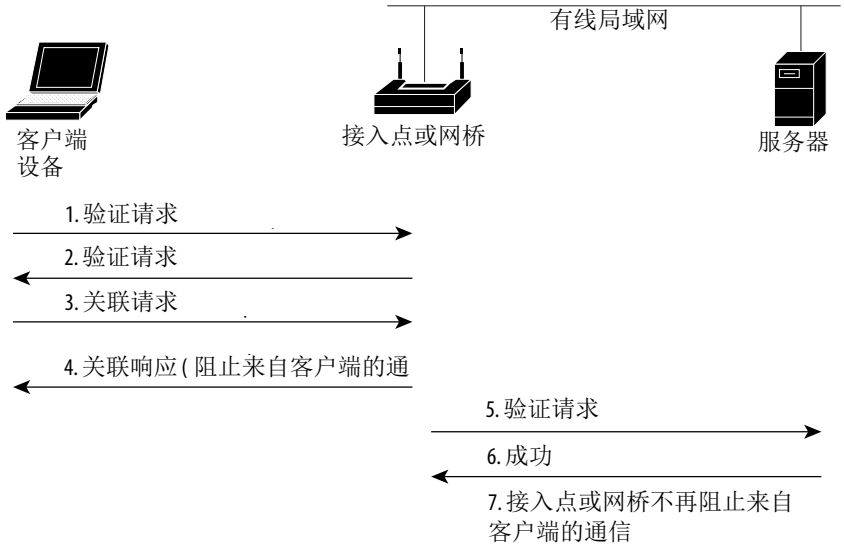
关于启用基于 MAC 的验证的说明，请参见第 341 页的 “ 将验证类型分配到 SSID”。

提示　如果您的网络中没有 RADIUS 服务器，您可在接入点的 Advanced Security: MAC Address Authentication (高级安全性：MAC 地址验证) 页面中创建允许 MAC 地址列表。 MAC 地址未在列表中的设备将不允许进行验证。

提示　如果您的无线局域网中的 MAC 验证的客户端经常漫游，您可在接入点上启用 MAC 验证缓存。由于接入点仅验证 MAC 地址缓存中的设备，而不向验证服务器发送请求，因此， MAC 验证缓存可降低系统开销。关于如何启用该功能的说明，请参见第 347 页的 “ 配置 MAC 验证缓存 ”。

下图显示了基于 MAC 的验证的执行顺序。

图 102 - 基于 MAC 的验证的执行顺序



结合使用基于 MAC 的验证、 EAP 验证和开放式验证

您可设置接入点结合使用基于 MAC 的验证和 EAP 验证，对客户端设备进行验证。当启用该功能时，使用 802.11 开放式验证关联到接入点的客户端设备将先尝试 MAC 验证；如果 MAC 验证成功，客户端设备加入网络。如果 MAC 验证失败，将进行 EAP 验证。

关于设置此类验证组合的说明，请参见第 341 页的 “ 将验证类型分配到 SSID”。

在已验证客户端上使用 CCKM

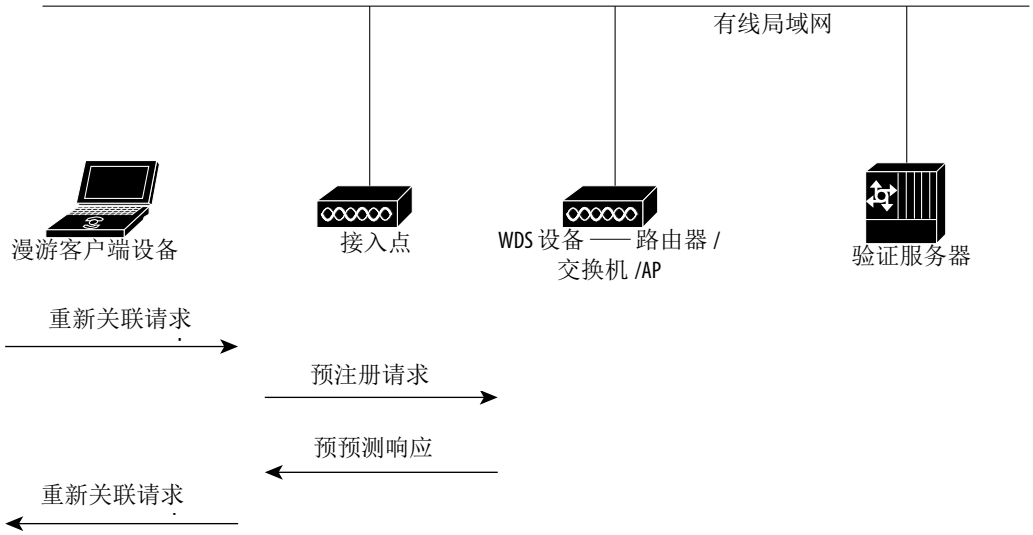
使用思科集中密钥管理 (CCKM)，已验证客户端设备可从一个接入点漫游到另一个接入点，重新关联期间不会有任何可以察觉到的延迟。网络中的接入点提供无线域服务 (WDS)，并为子网上启用 CCKM 的客户端设备创建安全凭证缓存。当启用 CCKM 的客户端设备漫游到新的接入点时，凭证的 WDS 接入点缓存可显著缩短重新关联所需的时间。当客户端设备漫游时， WDS 接入点将客户端的安全凭证转发到新的接入点，重新关联过程将缩短至漫游客户端和新接入点之间交换两个数据包所需的时间。

- 关于在接入点上启用 CCKM 的说明，请参见第 341 页的 “ 将验证类型分配到 SSID”。
- 关于在无线局域网上设置 WDS 接入点的详细说明，请参见第 365 页的 “ 配置接入点使用 WDS 设备 ”。

重要事项 对于使用 SSID 关联的客户端设备 (已启用 CCKM)，不支持已分配 RADIUS 的 VLAN 功能。

下图显示了使用 CCKM 的重新关联过程。

图 103 - 使用 CCKM 重新关联客户端



WPA 密钥管理

Wi-Fi 保护访问 (WPA) 协议是一种基于标准的可互操作安全增强协议，可显著提升现有和未来无线局域网系统的数据保护和访问控制级别。其基于即将生效的 IEEE 802.11i 标准，并向前兼容。 WPA 利用 TKIP (临时密钥完整性协议) 进行数据保护， 802.1X 进行验证密钥管理。

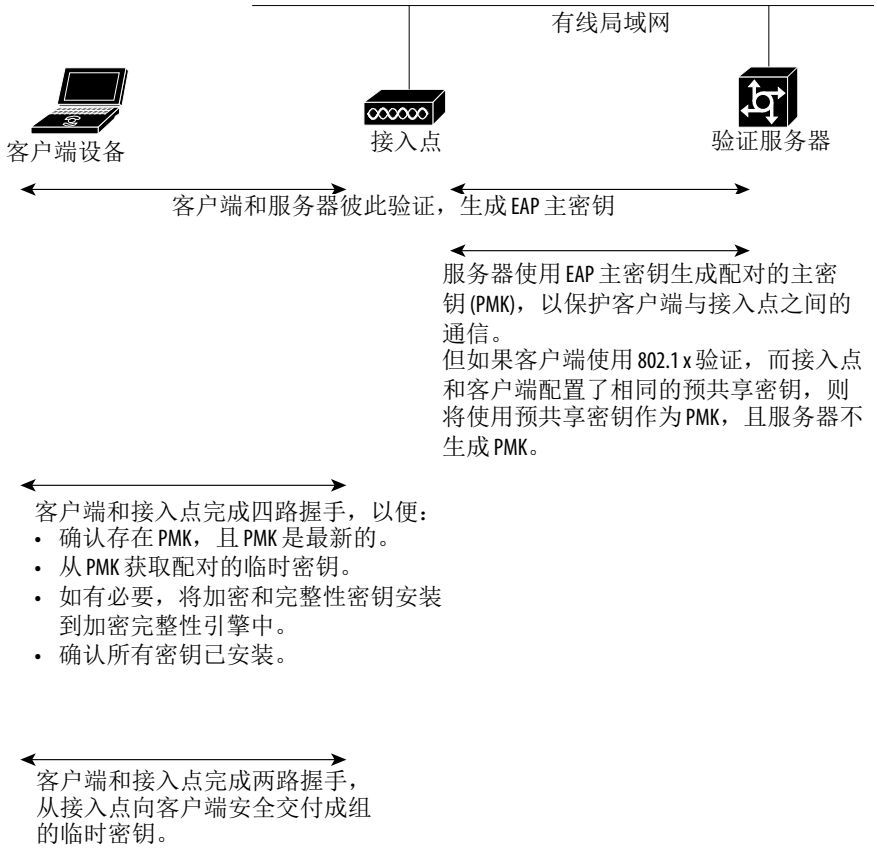
WPA 密钥管理支持两种互斥的管理类型：WPA 和 WPA 预共享密钥 (WPA-PSK)。通过 WPA 密钥管理，客户端和验证服务器使用 EAP 验证方法相互验证，客户端和服务器生成成对主密钥 (PMK)。使用 WPA 时，服务器动态生成 PMK，并将其传送到接入点。而当使用 WPA-PSK 时，可在客户端和接入点上配置预共享密钥，并将该预共享密钥用作 PMK。

重要事项　单播和多播密文组在 WPA 信息元素中公告 (并在 802.11 关联时协商)，它们可能与明确分配的 VLAN 中支持的密文组不匹配。如果 RADIUS 服务器分配新的 VLAN ID，而它使用的密文组不同于之前协商的密文组，则接入点和客户端将无法切换回新的密文组。当前，WPA 和 CCKM 协议不允许在初次 802.11 密文协商阶段后更改密文组。否则，客户端设备将从无线局域网中断开。

关于在接入点上配置 WPA 密钥管理的说明，请参见第 341 页的 “ 将验证类型分配到 SSID”。

下图显示了 WPA 密钥管理过程。

图 104 - WPA 密钥管理过程



配置验证类型

本节介绍了如何配置验证类型。您可将配置类型附加到接入点的 SSID 中。关于设置多重 SSID 的详细信息，请参见第 289 页的 “ 配置 多个 SSID”。

提示 无线接入点没有默认的 SSID。

将验证类型分配到 SSID

在特权 EXEC 模式下，根据以下步骤配置 SSID 的验证类型。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 创建一个 SSID，然后进入新 SSID 的 SSID 配置模式。

   SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。

   ```
   dot11 ssid ssid-string
   ```

3. (可选) 将该 SSID 的验证类型设置为开放式。

   开放式验证允许任何设备进行验证并尝试与接入点通信。

   ```
   authentication open
   [mac-address list-name [alternate]]
   [[optional] eap list-name]
   ```

   a. (可选) 将 SSID 的验证类型设置为开放式验证结合 MAC 地址验证。

      接入点强制所有客户端设备执行 MAC 地址验证后才能加入网络。使用 list-name 指定验证方法列表。

      alternate 关键字允许客户端设备使用 MAC 或 EAP 验证加入网络；成功完成任一验证的客户端均可加入网络。

   b. (可选) 将 SSID 的验证类型设置为开放式验证结合 EAP 验证。

      接入点强制所有客户端设备执行 EAP 验证后才能加入网络。使用 list-name 指定验证方法列表。

optional 关键字允许客户端设备使用开放式或 EAP 验证进行关联和验证。该设置主要供需要特殊客户端访问能力的服务提供商使用。

提示 配置为 EAP 验证的接入点将强制所有关联客户端设备执行 EAP 验证。不使用 EAP 的客户端设备将无法使用接入点。

由于共享密钥的安全性缺陷，我们建议您避免使用它。您可只将共享密钥验证分配给一个 SSID。

4. (可选) 将 SSID 的验证类型设置为网络 EAP。

```
authentication network-eap list-name
[mac-address list-name]
```

当可扩展的验证协议 (EAP) 与兼容 EAP 的 RADIUS 服务器交互时，接入点可帮助无线客户端设备和 RADIUS 服务器执行相互验证，并生成动态单播 WEP 密钥。但接入点不强制所有客户端设备执行 EAP 验证。

a. (可选) 将 SSID 的验证类型设置为网络 EAP 结合 MAC 地址验证。

b. 使用 list-name 指定验证方法列表。

关联到接入点的所有客户端设备都必须执行 MAC 地址验证。

5. (可选) 将 SSID 的验证类型设置为 WPA、 CCKM 或两者皆有。

```
authentication key-management { [wpa] [cckm] }
[ optional ]
```

如果使用 optional 关键字， WPA 和 CCKM 客户端之外的其他客户端设备也可使用该 SSID。如果未使用 optional 关键字，则仅允许 WPA 或 CCKM 客户端设备使用该 SSID。

- 要为 SSID 启用 CCKM，还必须启用网络 EAP 验证。当为 SSID 启用 CCKM 和网络 EAP 后，使用 LEAP、 EAP-FAST、 PEAP/GTC、 MSPEAP、 EAP-TLS 和 EAP-FAST 的客户端设备可使用 SSID 进行验证。
- 要为 SSID 启用 WPA，还必须启用开放式验证、网络 EAP 验证或两者。

当为 SSID 同时启用 WPA 及 CCKM 时，必须先输入 WPA，然后输入 CCKM。任何 WPA 客户端可尝试进行验证，但仅 CCKM 语音客户端可进行验证。

启用 CCKM 或 WPA 前，必须先使用密文组选项中的一种设置 SSID 的 VLAN 的加密方式。要同时启用 CCKM 及 WPA，必须将加密方式设置为包含 TKIP 的密文组。

关于配置 VLAN 加密方式的说明，请参见第 331 页的 “ 配置密文组 ”。

如果为 SSID 启用了无预共享密钥的 WPA，则密钥管理类型为 WPA。如果启用了有预共享密钥的 WPA，则密钥管理类型为 WPA-PSK。

- 关于配置预共享密钥的说明，请参见第 345 页的 “ 配置附加 WPA 设置 ”。
- 关于设置无线局域网使用 CCKM 和子网上下文管理器的详细说明，请参见第 353 页的 “ 配置 WDS 和快速 安全漫游 ”。

6. 返回到特权 EXEC 模式。

```
end
```

7. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

使用 SSID 命令的 no 格式禁用 SSID 或禁用 SSID 功能。

本例将 SSID batman 的验证类型设置为网络 EAP 结合 CCKM 验证密钥管理。使用 batman SSID 的客户端设备使用 adam 服务器列表进行验证。经过验证后，启用 CCKM 的客户端可使用 CCKM 执行快速重新关联。

```
ap1200# configure terminal
ap1200(config)# dot11 ssid batman
ap1200(config-ssid)# authentication network-eap
adam
ap1200(config-ssid)# authentication key-management
cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

配置附加 WPA 设置

使用两种可选设置配置接入点的预共享密钥，并调节组密钥的更新频率。

设置预共享密钥

当无线局域网上不提供基于 802.1X 的验证时，如果要支持 WPA，必须在接入点上配置预共享密钥。您可以 ASCII 或十六进制字符格式输入预共享密钥。如果以 ASCII 字符格式输入密钥，可输入 8...63 个字符，且接入点将扩展密钥。如果以十六进制字符格式输入密钥，则必须输入 64 个十六进制字符。

配置组密钥更新

在 WPA 过程的最后一个步骤，接入点将组密钥分配给验证客户端设备。您可使用这些可选设置配置接入点，以根据客户端关联和取消关联来更改和分配组密钥：

- 中止成员身份

  当任何已验证设备取消与接入点的关联时，接入点生成并分配新的组密钥。该功能可以让关联设备保持组密钥的私密性，但如果网络上的客户端频繁地在多个接入点之间漫游，会产生一些开销通信。

- 功能切换

  当最后一个非密钥管理型 (静态 WEP) 客户端取消关联时，接入点生成并分配动态组密钥；当第一个非密钥管理型 (静态 WEP) 客户端验证时，它分配静态配置的 WEP 密钥。在 WPA 迁移模式下，当没有静态 WEP 客户端与接入点关联时，该功能可显著提升密钥管理功能的安全性。

在特权 EXEC 模式下，根据以下步骤配置 WPA 预共享密钥和组密钥更新选项。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入 SSID 的 SSID 配置模式。

   ```
   dot11 ssid ssid-string
   ```

3. 使用 WPA，为客户端设备 (也使用静态 WEP 密钥) 输入预共享密钥。

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

   使用十六进制或 ASCII 字符输入密钥。如果使用十六进制，则必须输入 64 个十六进制字符，以完成 256 位密钥。如果使用 ASCII，则必须至少输入 8 个字母、数字或符号，接入点将为您扩展密钥。您最多可输入 63 个 ASCII 字符。

1. 进入无线电接口的接口配置模式。

   ```
   interface dot11radio { 0 | 1 }
   ```

   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

2. 输入步骤 2 中定义的 ssid，将 ssid 分配给所选的无线电接口。

   ```
   ssid ssid-string
   ```

3. 返回到特权 EXEC 模式。

   ```
   exit
   ```

4. 使用广播密钥旋转命令配置附加的 WPA 组密钥更新。

   ```
   broadcast-key [ vlan vlan-id ]
   { change seconds }
   [ membership-termination ]
   [ capability-change ]
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

本例显示使用 WPA 和组密钥更新选项为客户端配置预共享密钥：

```
ap# configure terminal
ap(config)# dot11 ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-
termination capability-change
```

配置 MAC 验证缓存

如果您的无线局域网中的 MAC 验证的客户端经常漫游，您可在接入点上启用 MAC 验证缓存。由于接入点仅验证 MAC 地址缓存中的设备，而不向验证服务器发送请求，因此， MAC 验证缓存可降低系统开销。当客户端设备完成到验证服务器的 MAC 验证后，接入点将客户端的 MAC 地址添加到缓存。

在特权 EXEC 模式下，根据以下步骤启用 MAC 验证缓存。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用接入点上的 MAC 验证缓存。

   ```
   dot11 aaa mac-authen filter-cache [timeout seconds]
   ```

   使用 **timeout** 选项配置缓存中 MAC 地址的超时值。输入 30...65555 之间的秒数。默认值为 1800 (30 分钟)。当输入超时值时，将自动启用 MAC 验证缓存。

3. 返回到特权 EXEC 模式。

   ```
   exit
   ```

4. 显示 MAC 验证缓存中的条目。包括客户端 MAC 地址，以显示特定客户端的条目。

   ```
   show dot11 aaa mac-authen filter-cache [address]
   ```

5. 清除缓存中的所有条目。包括客户端 MAC 地址，以清除缓存中的特定客户端。

   ```
   clear dot11 aaa mac-authen filter-cache [address]
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

本例显示了如何启用 MAC 验证缓存并设置一小时的超时值：

```
ap# configure terminal
ap(config)# dot11 aaa mac-authen filter-cache
timeout 3600
ap(config)# end
```

使用 `dot11 aaa mac-authen filter-cache` 命令的 no 格式禁用 MAC 验证缓存。例如：

```
no dot11 aaa authentication mac-authen filter-cache
```

配置验证延迟、超时和间隔

对于通过接入点验证的客户端设备，在特权 EXEC 模式下，根据以下步骤配置延迟时间、重新验证周期和验证超时。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入客户端设备在验证失败后进行重新验证前必须等待的秒数。

   ```
   dot11 holdoff-time seconds
   ```

   当客户端登录失败三次或未能响应接入点的三次验证请求后，便激活延迟时间。输入 1...65555 之间的秒数。

3. 输入接入点在验证失败前必须等待客户端回应 EAP/dot1x 消息的秒数。输入 1...120 之间的秒数。

   ```
   dot1x timeout supp-response seconds [local]
   ```

   可将 RADIUS 服务器配置为发送不同超时值，以覆盖原来配置的值。输入 `local` 关键字配置接入点，忽略 RADIUS 服务器值并使用配置的值。

   可选的 `no` 关键字将超时值重置为默认值 30 秒。

4. 进入无线电接口的接口配置模式。

   ```
   interface dot11radio { 0 | 1 }
   ```

   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

5. 输入接入点强制已验证客户端重新验证前等待的间隔值 (秒)。

   ```
   dot1x reauth-period { seconds | server }
   ```

   输入服务器关键字，以配置接入点使用验证服务器指定的重新验证周期。如果使用该选项，则配置您的验证服务器使用 RADIUS 属性 27，会话超时。

   该属性设置将服务提供给客户端的最大秒数，此后将终止会话或提示符。在客户端设备执行 EAP 验证时，服务器将该属性发送给接入点。

提示　如果配置了 SSID 的 MAC 地址验证和 EAP 验证，则服务器将为客户端设备发送 MAC 和 EAP 验证的会话超时属性。接入点将使用客户端最后执行的验证的会话超时属性。例如，如果客户端执行 MAC 地址验证，然后执行 EAP 验证，接入点将使用服务器的 EAP 验证会话超时值。

为避免使用会话超时属性时造成混淆，可在验证服务器上为 MAC 和 EAP 验证配置相同的会话超时值。

6. 配置 TKIP MIC 失败保持时间。

   ```
   countermeasure tkip hold-time seconds
   ```

   如果接入点在 60 秒内检测到 MIC 失败两次，则其在保持时间内将阻止该接口上的所有 TKIP 客户端。

7. 返回到特权 EXEC 模式。

   ```
   end
   ```

8. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用这些命令的 `no` 格式将值恢复为默认值。

为 802.1X 请求者创建并应用 EAP 方法配置文件

本节介绍了 802.1X 请求者 EAP 方法列表的可选配置。配置 EAP 方法配置文件，使得请求者不应答一些 EAP 方法，即使它们在客户端上可用。例如，如果 RADIUS 服务器支持 EAP-FAST 和 LEAP，在某些配置下，服务器一开始可配置 LEAP，而不是更安全的方法。如果未定义首选 EAP 方法列表，则请求者支持 LEAP，但这有助于强制请求者使用更安全的方法 (如 EAP-FAST)。

- 使用 no 命令否认命令，或将其恢复到默认值。
- 使用 show eap registrations method 命令查看当前可用的 (已注册的) EAP 方法。
- 使用 show eap sessions 命令查看现有 EAP 会话。

关于 802.1X 请求者的更多信息，请参见第 212 页的 “ 创建凭证配置文件 ”。

创建 EAP 方法配置文件

在特权 EXEC 模式下，根据以下步骤定义新的 EAP 配置文件。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入配置文件的名称。

   ```
   eap profile profile name
   ```

3. (可选) —— 输入 EAP 配置文件的描述。

   描述

4. 输入一种或多种允许的 EAP 方法。

   ```
   method fast
   ```

   提示 虽然 EAP-GTC、 EAP-MD5 和 EAP-MSCHAPV2 显示为子参数，但它们仅用作隧道式 EAP 验证的内部方式，不得作为主验证方式。

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running config startup-config
   ```

将 EAP 配置文件应用到上行链路 SSID

该操作通常用于工作组网桥或接入点。在特权 EXEC 模式下，根据以下步骤将 EAP 配置文件应用到上行链路 SSID。

1. 进入全局配置模式。
   ```
   configure terminal
   ```
2. 进入无线电接口的接口配置模式。
   ```
   interface dot11radio {0 | 1}
   ```
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。
3. 将上行链路 SSID 分配给无线电接口。
   ```
   ssid ssid
   ```
4. 返回到配置终端模式。
   ```
   exit
   ```
5. 输入配置文件预配置的配置文件名称。
   ```
   eap profile profile
   ```
6. 返回到特权 EXEC 模式。
   ```
   end
   ```
7. (可选) 将您的输入保存到配置文件中。
   ```
   copy running config startup-config
   ```

配置 WDS 和快速 安全漫游

本章描述了如何配置无线域服务 (WDS) 的接入点和客户端服务的快速安全漫游。

WDS

当在网络上配置无线域服务时，无线局域网上的接入点使用 WDS 设备 (可以是接入点、集成服务路由器或配置为 WDS 设备的交换机)，为客户端设备提供快速、安全的漫游以及参与无线管理。

配置为 WDS 设备的接入点最多支持 60 个参与接入点，配置为 WDS 设备的集成服务路由器 (ISR) 最多支持 100 个参与接入点。

提示 单个接入点最多可支持 16 个移动组。

当客户端设备从一个接入点漫游到另一个接入点时，快速而安全的漫游可提供快速的重新验证，以防止语音及其他时间敏感型应用中的延迟。

WDS 设备的作用

WDS 设备可在无线局域网上执行若干任务：

- 公布其 WDS 功能，并参与为无线局域网选择最佳的 WDS 设备。当为 WDS 配置无线局域网时，您可将一台设备设为主要候选 WDS，将一台或更多其他设备设为后备候选 WDS。如果主要 WDS 设备掉线，其中一个后备 WDS 设备将取代其位置。
- 重新验证子网中的所有接入点，与每个接入点建立安全通信信道。
- 作为与参与接入点关联的所有 802.1x 验证客户端设备的穿透设备。
- 注册子网中使用动态密钥的所有客户端设备，为它们建立会话密钥，并缓存其安全凭证。当客户端漫游到另一个接入点时，WDS 设备会将客户端的安全凭证转发到新的接入点。

该表列出了由可配置为 WDS 设备的平台所支持的参与接入点的数量。

表 102 - WDS 设备支持的参与接入点

配置为 WDS 设备的单元	支持的参与接入点
同时为客户端设备服务的接入点	30
禁用无线电接口的接入点	60

使用 WDS 设备的接入点的作用

无线局域网上的接入点与 WDS 设备在此类活动中进行交互：

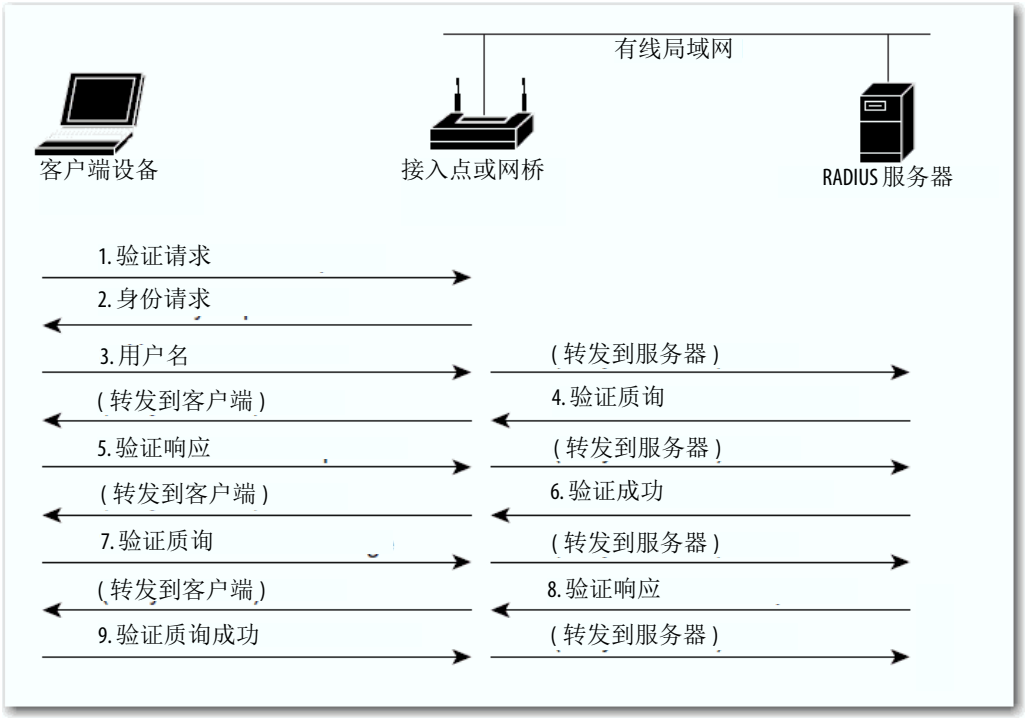
- 发现并跟踪当前 WDS 设备，并将 WDS 广告转至无线局域网。
- 验证 WDS 设备，建立到 WDS 设备的安全通信信道。
- 使用 WDS 设备注册相关的客户端设备。
- 向 WDS 设备报告无线电数据。

快速安全漫游

许多无线局域网中的接入点为移动客户端设备 (在整个设施的不同接入点间漫游) 提供服务。当漫游到不同的接入点时，运行在客户端设备上的某些应用需要快速重新关联。例如，语音应用需要无缝漫游，以防止谈话中的延迟和间隔。

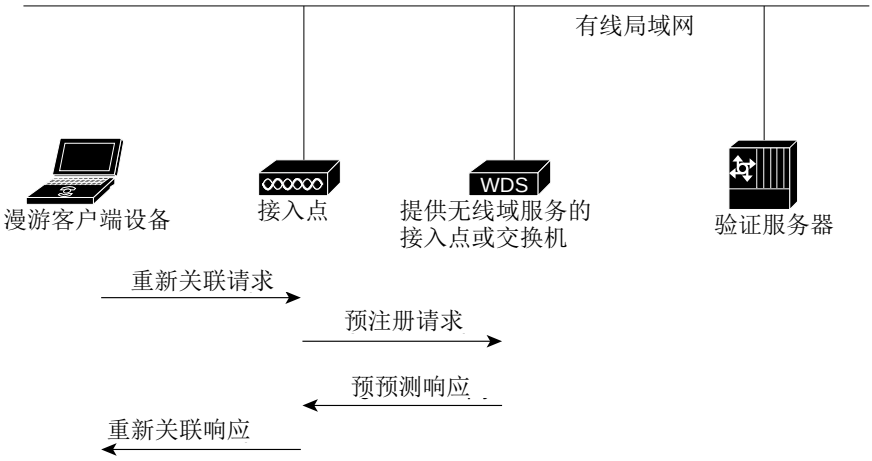
在正常工作期间，启用 EAP 功能的客户端设备通过执行完整的 EAP 验证与新接入点相互验证，其中包括与主要 RADIUS 服务器进行通信。

图 105 - 使用 RADIUS 服务器进行客户端验证



但是，当您将无线局域网配置用于快速安全漫游时，启用 EAP 功能的客户端设备从一个接入点漫游到另一个接入点，并不会涉及主要 RADIUS 服务器。使用 Cisco 集中密钥管理 (CCKM)，配置用于提供无线域服务 (WDS) 的设备可取代 RADIUS 服务器的位置，并快速验证客户端，以便语音或其他时间敏感型应用不会有任何可以察觉的延迟。该图显示使用 CCKM 进行客户端验证。

图 106 - 使用 CCKM 和 WDS 接入点进行客户端重新关联



WDS 设备保持无线局域网中支持 CCKM 的客户端设备的凭证缓存。当支持 CCKM 的客户端从一个接入点漫游到另一个接入点时，客户端向新接入点发送重新关联请求，新接入点把请求转至 WDS 设备。

WDS 设备将客户端的凭证转发到新接入点，新接入点向客户端发送重新关联响应。在客户端和新的接入点之间仅传送两个数据包，大大缩短了重关联时间。此外，客户端也使用重新关联响应来生成单播密钥。

有关配置接入点来支持快速安全漫游的说明，请参见第 368 页的 “ 配置快速安全漫游 ”。

配置 WDS

本节描述了如何在网络上配置 WDS。

WDS 指南

在配置 WDS 时应遵循以下指南：

- 同时为客户端设备服务的 WDS 接入点最多支持 30 个参与接入点，但禁用无线电的 WDS 接入点最多支持 60 个参与接入点。
- WDS 模式最多仅支持 60 个基础架构接入点和 1200 个客户端。
- 中继接入点不支持 WDS。当以太网发生故障时，不得将中继接入点配置为候选 WDS，也不得将 WDS 接入点配置为返回 (后退) 到中继模式。

关于 WDS 的要求

要配置 WDS，您必须使无线局域网上具有这些项目：

- 至少一个可配置为 WDS 设备的接入点
- 验证服务器 (或配置为本地验证器的接入点)

配置概览

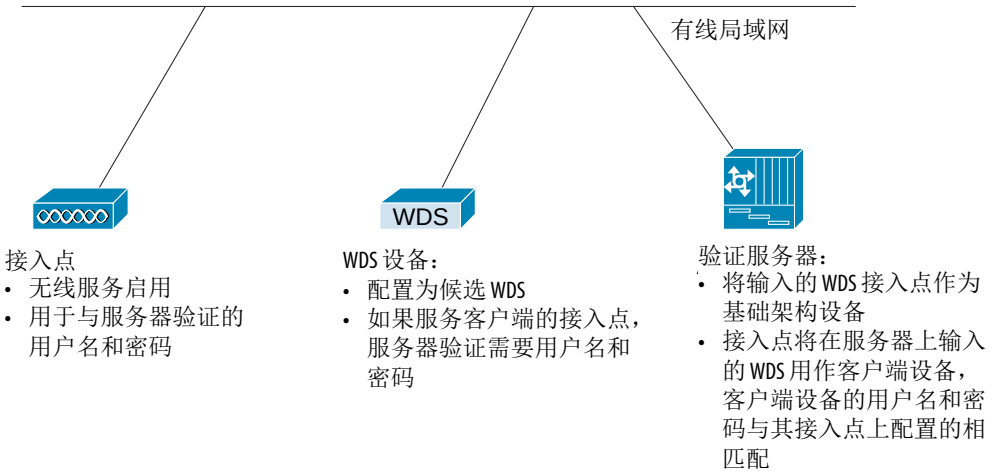
您必须完成三个主要步骤来设置 WDS 和快速安全漫游。

1. 将接入点配置为潜在 WDS 设备。本章给出了将接入点配置为 WDS 设备的说明。

2. 配置其他接入点，以使用 WDS 设备。
3. 在网络上配置验证服务器，以验证 WDS 设备和使用 WDS 设备的接入点。

该图显示了参与 WDS 的每个设备所需的配置。

图 107 - 参与 WDS 的设备上的配置



将接入点配置为潜在 WDS 设备

对于主要候选 WDS，配置一个无需服务大量客户端设备的接入点。如果客户端设备在 WDS 接入点启动时与之关联，则客户端可以等待几分钟后进行验证。

当 WDS 启用后， WDS 接入点执行和跟踪所有验证。因此，您必须在 WDS 接入点上配置 EAP 安全设置。

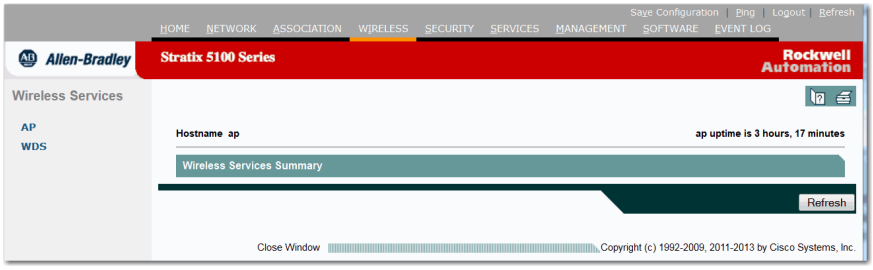
关于在接入点上配置 EAP 的说明，请参见第 341 页的 “ 配置验证类型 ”。

在您希望配置为主要 WDS 接入点的接入点上，根据以下步骤操作将接入点配置为主要候选 WDS。

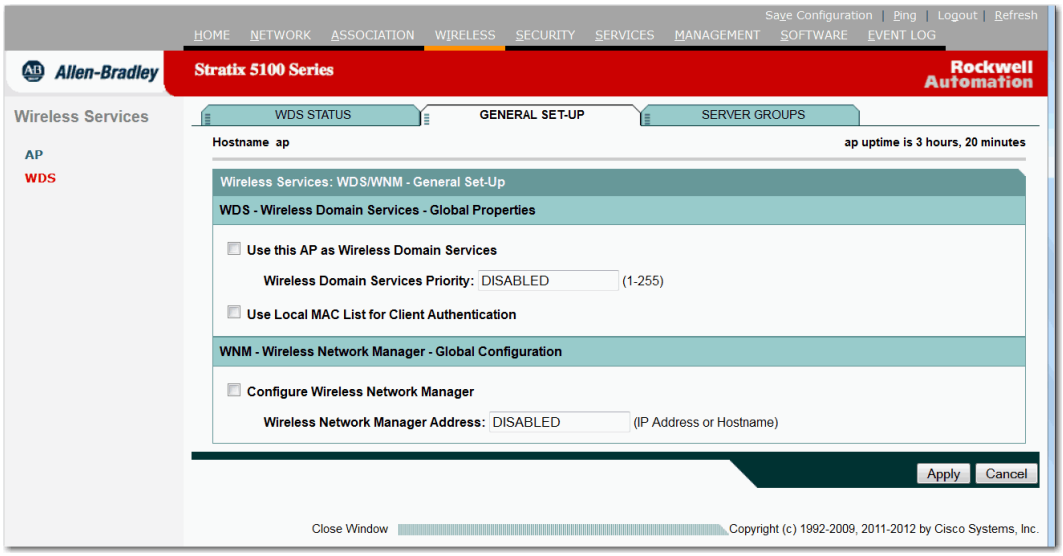
1. 跳转到 Wireless Services Summary (无线服务概要) 页面。

下图显示了 Wireless Services Summary (无线服务概要) 页面。

图 108 - Wireless Services Summary (无线服务概要) 页面



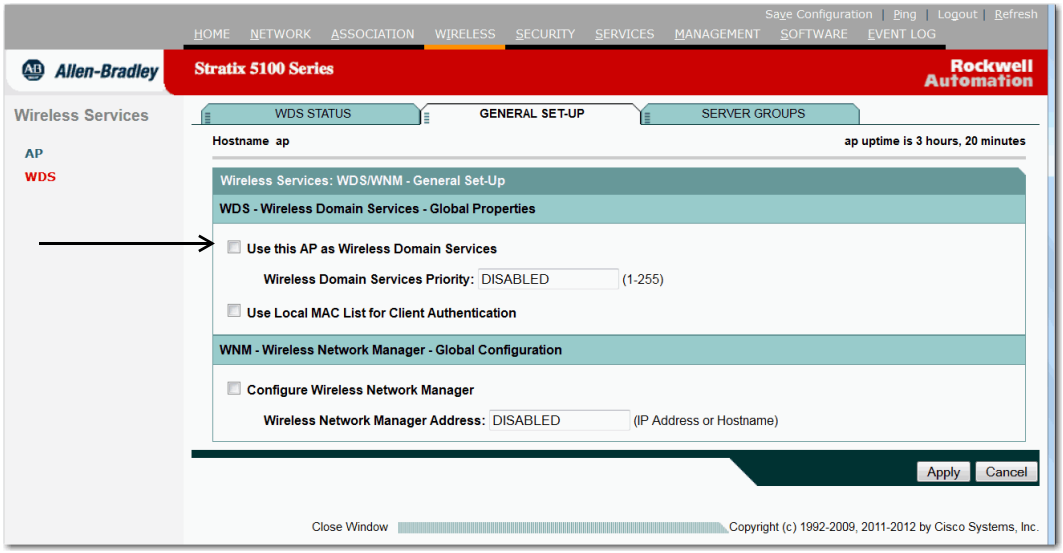
2. 单击 WDS 跳转到 WDS/WNM Summary (WDS/WNM 概要) 页面。



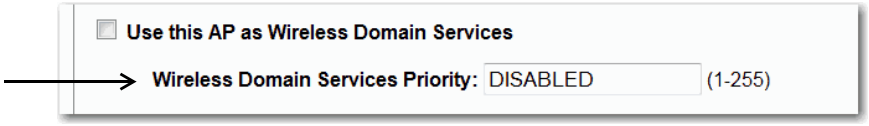
3. 在 WDS/WNM Summary (WDS/WNM 概要) 页面上，单击 General Setup (常规设置) 跳转到 WDS/WNM General Setup (WDS/WNM 常规设置) 页面。

   显示 WDS/WNM General Setup (WDS/WNM 常规设置)。

图 109 - WDS/WNM General Setup (WDS/WNM 常规设置) 页面



4. 选中 Use this AP as Wireless Domain Services (使用该 AP 提供无线域服务) 复选框。
5. 在 Wireless Domain Services Priority (无线域服务优先级) 域，输入介于 1...255 的优先级编号，以设置该候选 WDS 的优先级。



优先级域中编号最高的候选 WDS 接入点将成为代理 WDS 接入点。例如，如果一个候选 WDS 被分配了优先级 255，另一个候选 WDS 被分配了优先级 100，则优先级 255 的候选 WDS 将作为代理 WDS 接入点。

6. (可选) 选中 Use Local MAC List for Client Authentication (使用本地 MAC 列表进行客户端验证)。

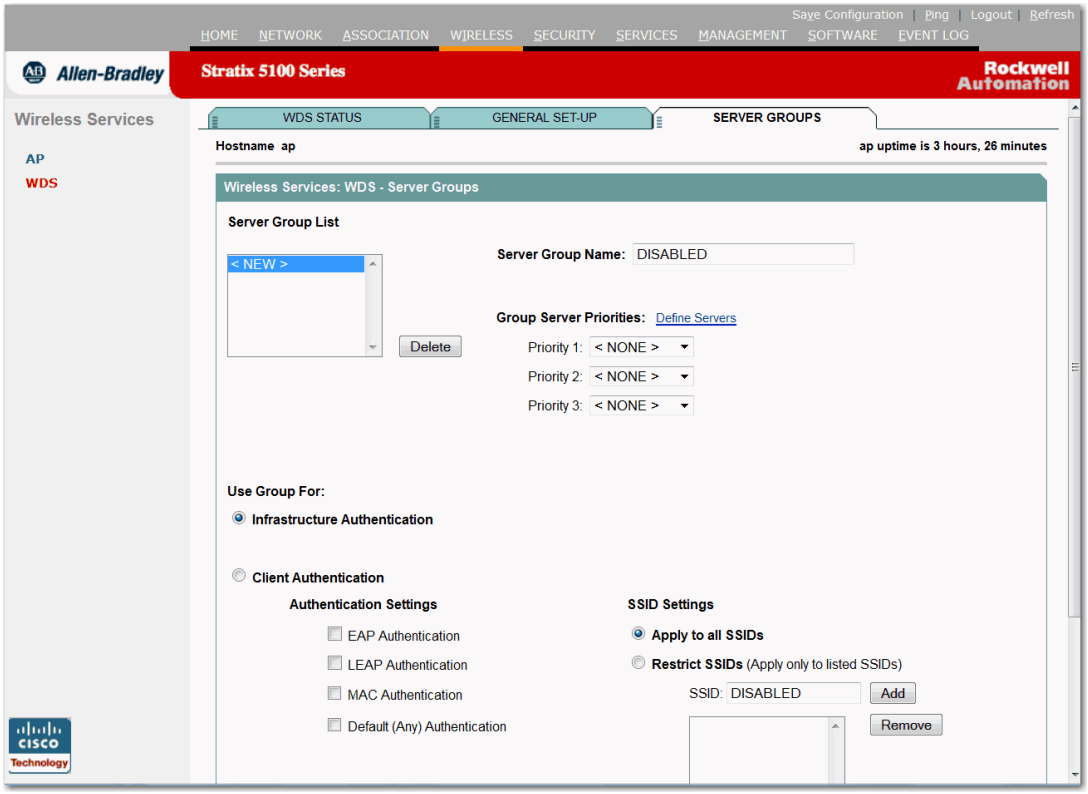
   这可通过使用 WDS 设备上配置的本地地址列表中的 MAC 地址验证客户端设备。如果未选中该复选框，则 WDS 设备将使用 Server Groups (服务器组) 页面中指定的 MAC 地址验证服务器，根据 MAC 地址来验证客户端。

   提示 选择 Use Local MAC List for Client Authentication (使用本地 MAC 列表进行客户端验证) 复选框不会强制客户端设备执行基于 MAC 的验证。它为基于服务器的 MAC 地址验证提供了一个本地备选方案。

7. 单击 Apply (应用)。
8. 跳转到 WDS Server Groups (WDS 服务器组) 页面，单击 Server Groups (服务器组)。

显示 WDS Server Groups (WDS 服务器组) 页面。

图 110 - WDS Server Groups (WDS 服务器组) 页面



配置服务器组

根据以下说明为使用 WDS 接入点的基础架构设备 (接入点) 创建服务器组 (用于 802.1x 验证)。

1. 在 Server Group Name (服务器组名称) 域输入组名称。
2. 从优先级 1 下拉菜单中，选择主要服务器。

   如果需要添加到组的服务器未显示在 Priority (优先级) 下拉菜单中，请单击 Define Servers (定义服务器) 浏览至 Server Manager (服务器管理器) 页面。配置服务器，然后返回到 WDS Server Groups (WDS 服务器组) 页面。

   提示　如果您的网络上没有验证服务器，则可将接入点或 ISR 配置为本地验证服务器。有关配置说明，请参见第 307 页的 " 将接入点配置为本地验证器 "。

3. (可选) 从优先级 2 和 3 下拉菜单中选择后备服务器。
4. 单击 Apply (应用)。

5. 配置服务器列表，用于对客户端设备进行 802.1x 验证。

   您可使用特定验证类型指定单独的客户端列表，如 EAP、LEAP、 PEAP 或基于 MAC，或使用任何验证类型来指定客户端设备列表。

6. 在 Server Group Name (服务器组名称) 域中输入服务器的组名称。
7. 从优先级 1 下拉菜单中，选择主要服务器。

   如果需要添加到组的服务器未显示在 Priority (优先级) 下拉菜单中，请单击 Define Servers (定义服务器) 浏览至 Server Manager (服务器管理器) 页面。配置服务器，然后返回到 WDS Server Groups (WDS 服务器组) 页面。

8. (可选) 从优先级 2 和 3 下拉菜单中选择后备服务器。
9. (可选) 选择 Restrict SSID (限制 SSID)，使用特定 SSID 来限制客户端设备对服务器组的使用。
10. 在 SSID 域中输入 SSID，并单击 Add (添加)。

    要删除一个 SSID，请在 SSID 中高亮显示，并单击 Remove (删除)。

11. 单击 Apply (应用)。
12. 将 WDS 接入点配置用于 LEAP 验证。

    关于配置 LEAP 的说明，请参见第 335 页的 " 配置验证类型 "。

提示 如果您的 WDS 接入点为客户端设备服务，请根据第 365 页的 " 配置接入点使用 WDS 设备 " 中的说明配置 WDS 接入点，以使用 WDS。

CLI 配置示例

本例显示了与第 359 页的 “ 将接入点配置为潜在 WDS 设备 ” 中所列步骤等效的 CLI 命令：

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server
infrastructure infra_devices
AP(config)# wlccp authentication-server client any
client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

在本例中，基础架构设备通过服务器组 infra_devices 进行验证；使用 SSID fred 或 ginger 的客户端设备通过服务器组 client_devices 进行验证。

有关本例中使用的命令的完整说明，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide (思科 Aironet 接入点和网桥的思科 IOS 命令参考指南)。

配置接入点使用 WDS 设备

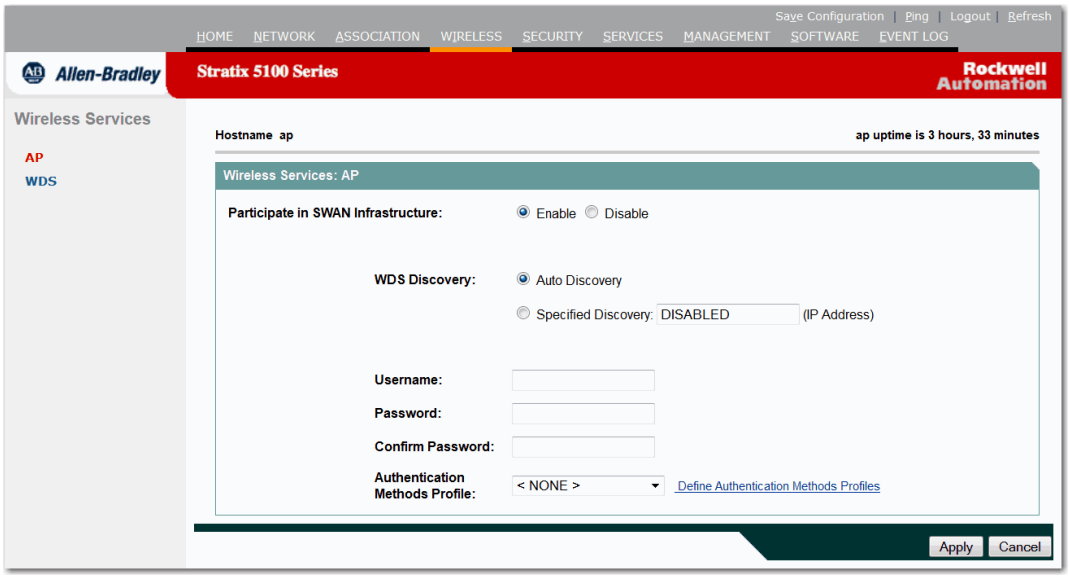
要参与 WDS，基础架构接入点应运行与 WDS 相同的 IOS 版本。

根据以下步骤配置接入点，以通过 WDS 设备进行验证并参与 WDS。

1. 浏览到 Wireless Services Summary (无线服务概要) 页面。
2. 单击 AP，浏览到 Wireless Services AP (无线服务 AP) 页面。

这将显示 Wireless Services (无线服务) 页面。

图 111 - Wireless Services AP (无线服务 AP) 页面



3. 单击 Participate in SWAN Infrastructure (参与 SWAN 基础架构) 设置中的 Enable (启用)。
4. 在 Username (用户名) 域，输入接入点的用户名。

   该用户名必须与在验证服务器上为接入点创建的用户名匹配。
5. 在 Password (密码) 域，输入接入点的密码，并在 Confirm Password (确认密码) 域中再次输入密码。

   该密码必须与在验证服务器上为接入点创建的密码匹配。
6. 单击 Apply (应用)。

配置与 WDS 进行交互的接入点自动执行下列步骤：

- 发现并跟踪当前 WDS 设备，并将 WDS 广告转至无线局域网。
- 验证 WDS 设备，建立到 WDS 设备的安全通信信道。
- 使用 WDS 设备注册相关的客户端设备。

CLI 配置示例

本例显示了与第 365 页的 “ 配置接入点使用 WDS 设备 ” 中所列步骤等效的 CLI 命令：

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7
wes7win8
AP(config)# end
```

在本例中，启用接入点与 WDS 设备进行交互，并使用 APWestWing 作为用户名， wes7win8 作为密码，以在验证服务器上进行验证。当在验证服务器上将接入点设置为客户端时，必须配置相同的用户名和密码对。

有关本例中使用的命令的完整说明，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide (思科 Aironet 接入点和网桥的思科 IOS 命令参考指南)。

配置仅 WDS 模式

使用 `wlccp wds mode wds-only` 命令， WDS 接入点可在仅 WDS 模式下工作。在发布该命令并重新加载后，接入点开始在仅 WDS 模式下工作。

- 在仅 WDS 模式下， dot11 子系统未被初始化，因此无法配置 dot11 接口相关命令。
- 在仅 WDS 模式下， WDS 最多支持 60 个基础架构接入点和 1200 个客户端。使用以下命令的 `no` 格式可关闭仅 WDS 模式。使用 `show wlccp wds` 命令可显示 WDS 接入点的工作模式。
- 要将 WDS 接入点设为在 AP 和 WDS 模式下工作，请使用 `no wlccp wds mode wds-only` 命令和使用 `write erase` 命令来立即重新加载接入点。

在接入点重新加载之后， dot11 无线电子系统执行初始化。接入点和 WDS 直接关联到无线客户端。在该模式下， WDS 支持 30 个架构接入点和 600 个客户端以及 20 个直接客户端关联。

查看 WDS 信息

在 Web 浏览器界面上，浏览到 Wireless Services Summary (无线服务概要) 页面来查看 WDS 状态概要。

在特权 EXEC 模式下的 CLI 上，可使用这些命令来查看有关当前 WDS 设备及其他参与 CCKM 的接入点的信息：

命令	描述
`show wlccp ap`	对参与 CCKM 的接入点使用该命令，以显示 WDS 设备的 MAC 地址、 WDS 设备的 IP 地址、接入点状态 (正在验证、已验证或已注册)、架构验证器的 IP 地址和客户端设备 (MN) 验证器的 IP 地址。
`show wlccp wds { ap | mn } [ detail ] [ mac-addr` *`mac-address`* `]`	在 WDS 设备上，只使用该命令来显示有关接入点和客户端设备的缓存信息。 • ap —— 参与 CCKM 的接入点。 – 该命令提供每个接入点的 MAC 地址、 IP 地址、状态 (正在验证、已验证或已注册) 和生命周期 (接入点必须进行重新验证前的剩余秒数)。 – 使用 `mac-addr` 选项获取有关特定接入点的信息。 • mn —— 有关客户端设备的缓存信息，也被称为移动节点。 – 命令可提供每个客户端的 MAC 地址、与客户端有关的接入点 (cur-AP) 和状态 (正在验证、已验证或已注册)。 – 详情选项可提供客户端的生命周期 (客户端必须进行重新验证前的剩余秒数)、SSID 和 VLAN ID。 – 使用 `mac-addr` 选项显示有关特定客户端设备的信息。 • 如果您只输入 `show wlccp wds`，将显示接入点的 IP 地址、 MAC 地址、优先级和接口状态 (管理上独立、活动、后备、候选或仅 WDS)。 • 如果状态为后备，则 `show wlccp wds` 命令可提供当前 WDS 设备 的 IP 地址、MAC 地址和优先级。 • 如果状态为仅 WDS，则 `show wlccp wds` 命令可提供设备的 MAC 地址、 IP 地址、接口状态、接入点计数和移动节点计数。

调试消息

在特权 EXEC 模式下，可使用这些调试命令来控制与 WDS 设备交互的设备的调试消息显示：

表 103 - 调试命令

命令	描述
`debug wlccp ap {mn | wds-discovery | state}`	使用该命令，可打开与客户端设备 (mn) 有关的调试消息显示、WDS 发现过程以及接入点与 WDS 设备的验证 (状态)。
`debug wlccp dump`	使用该命令，可执行 WLCCP 数据包的转储 (以二进制格式收发)。
`debug wlccp packet`	使用该命令，可打开进出 WDS 设备的数据包显示。
`debug wlccp wds [aggregator | authenticator | nm | state | statistics]`	使用该命令及其选项，可打开 WDS 调试消息显示。使用统计选项，可打开失败统计显示。
`debug wlccp wds authenticator {all | dispatcher | mac-authen | process | rxdata | state-machine | txdata}`	使用该命令及其选项，可打开与验证有关的 WDS 调试信息显示。

配置快速安全漫游

在配置 WDS 之后，配置用于 CCKM 的接入点可为关联的客户端设备提供快速安全漫游。本节描述了如何在无线局域网上配置快速安全漫游。

关于快速安全漫游的要求

要配置快速安全漫游，您必须使无线局域网上具有这些项目：

- 至少一个接入点、 ISR 或可配置为 WDS 设备的交换机 (配有 WLSM)
- 配置为参与 WDS 的接入点
- 配置为快速安全漫游的接入点
- 验证服务器 (或接入点、 ISR，或配置为本地验证器的交换机)
- 思科 Aironet 客户端设备或符合思科兼容扩展 (CCX) 版本 2 或更高版本的思科兼容客户端设备

有关配置 WDS 的说明，请参见第 357 页的 “ 配置 WDS”。

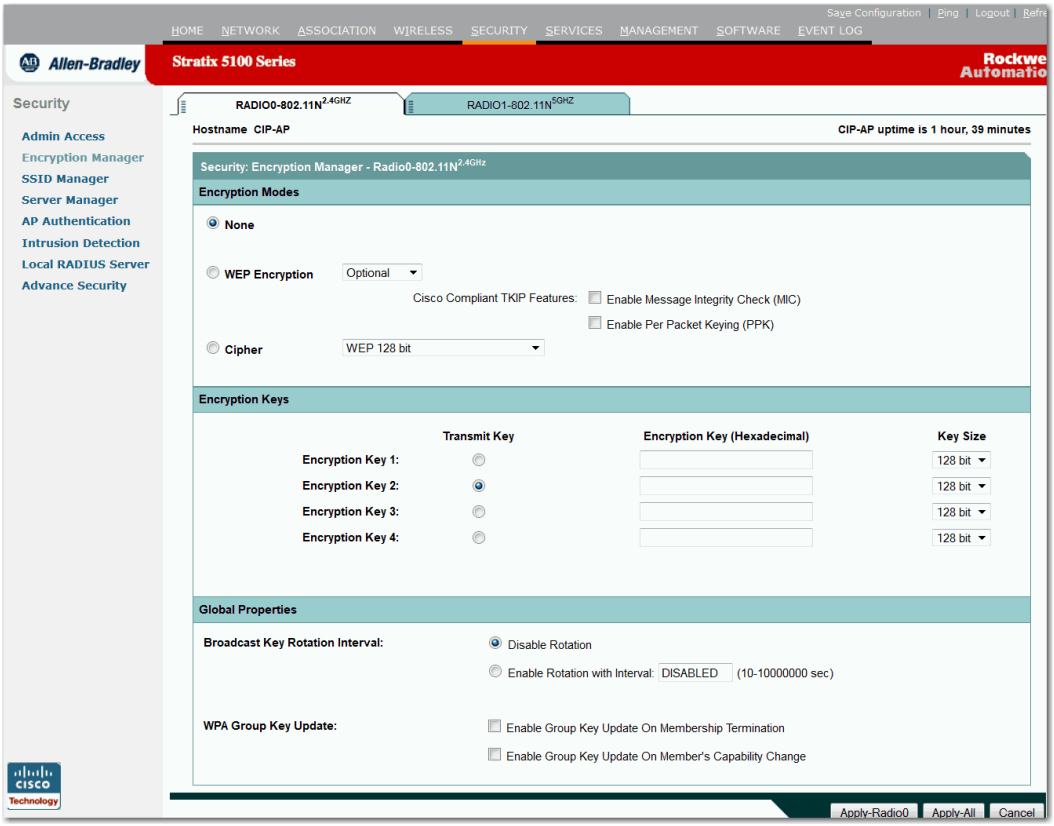
配置接入点来支持快速安全漫游

要支持快速安全漫游，必须将无线局域网上的接入点配置为参与 WDS，并且它们必须为至少一个 SSID 启用 CCKM 验证密钥管理。根据以下步骤为 SSID 配置 CCKM。

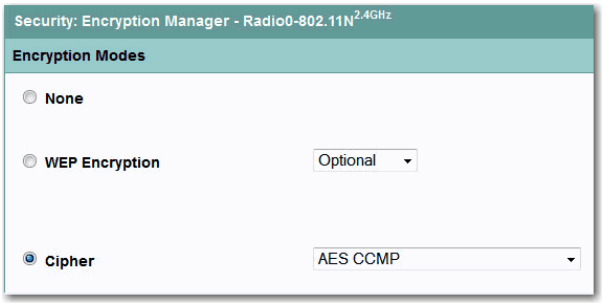
1. 浏览到接入点 GUI 上的 Encryption Manager (加密管理器) 页面。

   该图显示了 Encryption Manager (加密管理器) 页面的顶部。

图 112 - Encryption Manager (加密管理器) 页面

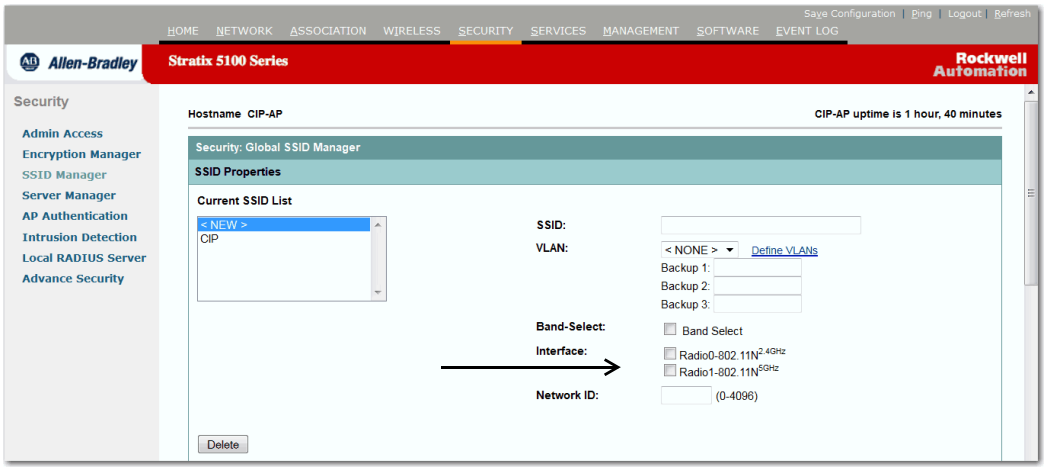


2. 单击 Cipher (密文)。
3. 从 Cipher (密文) 下拉菜单中选择 AES-CCMP。

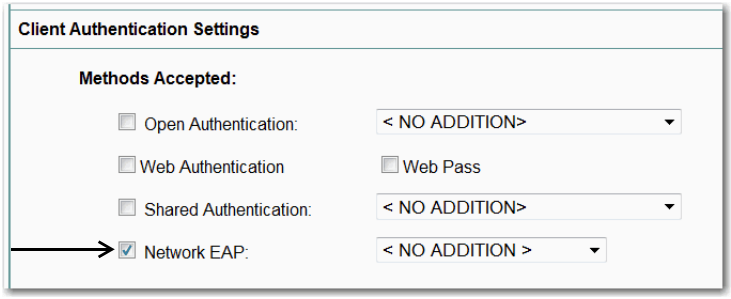


4. 单击 Apply (应用)。
5. 跳转到 SSID Manager (SSID 管理器) 页面。

图 113 - SSID Manager (SSID 管理器) 页面

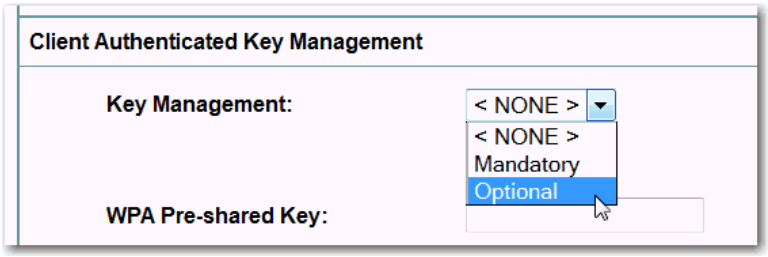


6. 在支持 CCKM 的 SSID 上选择这些设置：
   a. 如果接入点包含多个无线电接口，请选择 SSID 适用的接口。
   b. 在 Authentication Settings (验证设置) 下，选择 Network EAP (网络 EAP)。

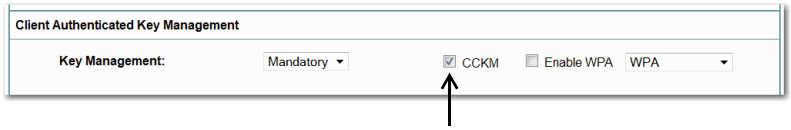


当启用 CCKM 后，您必须启用 Network EAP (网络 EAP) 作为验证类型。

   c. 在 Authenticated Key Management (验证密钥管理) 下选择 Mandatory (强制) 或 Optional (可选)。



   – 如果选择 Mandatory (强制)，仅支持 CCKM 的客户端可使用 SSID 进行关联。
   – 如果选择 Optional (可选)，不支持 CCKM 的 CCKM 客户端可使用 SSID 进行关联。
   d. 选中 CCKM 复选框。



7. 单击 Apply (应用)。

CLI 配置示例

本例显示了与第 369 页的 “ 配置接入点来支持快速安全漫游 ” 中所列步骤等效的 CLI 命令：

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap
eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

在本例中，通过配置 SSID 快速漫游来支持网络 EAP 和 CCKM，AES-CCM 密文组在 2.4 GHz 无线电接口上启用，而 SSID 快速漫游也在 2.4 GHz 无线电接口上启用。

管理帧保护

管理帧保护可针对在接入点和客户端工作站之间传递管理消息提供一系列安全功能。 MFP 由两个功能组件构成：基础架构 MFP 和客户端 MFP。

基础架构 MFP 提供基础架构支持。基础架构 MFP 在广播和直接管理帧中采用消息完整性检查 (MIC)，这些框架可协助检测伪设备和拒绝服务攻击。客户端 MFP 提供客户端支持。通过使众多常见的 WLAN 攻击无效化，客户端 MFP 可保护经过验证的客户端免受伪造帧的影响。管理帧保护操作需要一个 WDS。

概览

客户端 MFP 可对在接入点和支持 CCXv5 的客户端工作站之间发送的 3 级管理帧进行加密，以便 AP 和客户端可以丢弃伪造的 3 级管理帧，采取预防性措施，例如，在 AP 和经过验证和关联的客户端工作站之间传输的管理帧。

客户端 MFP 利用由 IEEE 802.11i 定义的安全机制来保护 3 级单播管理帧。 STA 在重新关联请求的 RSNIE 中协商的单播密文组可用于保护单播数据和 3 级管理帧。在工作组网桥、中继器或非根网桥模式下，接入点必须协商 TKIP 或 AES-CCMP 来使用客户端 MFP。

保护单播管理帧

单播 3 级管理帧通过应用 AES-CCMP 或 TKIP 进行保护，这与用于数据帧的保护方式类似。如果加密方式为 AES-CCMP 或 TKIP 加上密钥管理 WPA 版本 2，则客户端 MFP 仅针对自主接入点启用。

保护广播管理帧

为防止使用广播帧进行攻击，支持 CCXv5 的接入点将不发射任何 3 级广播管理帧。如果启用客户端 MFP，工作组网桥、中继器或非根网桥模式下的接入点会丢弃 3 级广播管理帧。如果加密方式为 AES-CCMP 或 TKIP 加上密钥管理 WPA 版本 2，则客户端 MFP 仅针对自主接入点启用。

在根模式下用于接入点的客户端 MFP

根模式下的自主接入点支持混合模式客户端。如果支持 CCXv5 的客户端采用协商密文组 AES 或 TKIP 以及 WPAv2，则表示其启用了客户端 MFP。对于不支持 CCXv5 的客户端，则不会启用客户端 MFP。默认情况下，客户端 MFP 对于接入点上的特定 SSID 是可选的，因此可在 SSID 配置模式下使用 CLI 启用或禁用。

对于特定 SSID，客户端 MFP 可被配置为必需或可选。要将客户端 MFP 配置为必需，必须将 SSID 配置为强制采用密钥管理 WPA 版本 2。如果密钥管理不是强制性 WPAv2，则会显示错误消息，且 CLI 命令被拒绝。如果在客户端 MFP 配置为必需且采用密钥管理 WPAv2 的情况下试图更改密钥管理，则会显示错误消息并拒绝 CLI 命令。当配置为可选时，如果 SSID 支持 WPAv2，则会启用客户端 MFP ； 否则将禁用客户端 MFP。

配置客户端 MFP

以下 CLI 命令用于为根模式下的接入点配置客户端 MFP。

```
ids mfp client required
```

该 SSID 配置命令在特定的 SSID 上将客户端 MFP 启用为必需。当执行该命令时，如果 SSID 绑定至 Dot11Radio 接口，则会复位 Dot11Radio 接口。此外，该命令也要求为 SSID 配置强制性 WPA 版本 2。如果没有为 SSID 配置强制性 WPAv2，则会显示错误消息，且命令将被拒绝。

```
no ids mfp client
```

该 SSID 配置命令在特定的 SSID 上禁用客户端 MFP。当执行该命令时，如果 SSID 绑定至 Dot11Radio 接口，则会复位 Dot11Radio 接口。

```
ids mfp client optional
```

该 SSID 配置命令在特定的 SSID 上将客户端 MFP 启用为可选。当执行该命令时，如果 SSID 绑定至 Dot11Radio 接口，则会复位 Dot11Radio 接口。如果 SSID 支持 WPAv2，将针对该特定 SSID 启用客户端 MFP，否则将禁用客户端 MFP。

```
show dot11 ids mfp client statistics
```

使用该命令，可在 Dot11Radio 接口的接入点控制台上显示客户端 MFP 统计数据。

```
clear dot11 ids mfp client statistics
```

使用该命令，可清除客户端 MFP 统计数据。

```
authentication key management wpa version {1|2}
```

使用该命令，可明确指定用于特定 SSID 的 WPA 密钥管理的 WPA 版本。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 将接入点配置为 MFP 生成器。

   启用时，接入点为每个帧通过添加消息完整性检查信息元素 (MIC IE)，实现对管理帧的保护。任何复制、修改或重发帧的尝试都将导致 MIC 失效，致使任何被配置为检测 (验证) MFP 帧的接收接入点报告该不一致。接入点必须是 WDS 的成员。

   ```
   dot11 ids mfp generator
   ```

3. 将接入点配置为 MFP 检测器。

当启用时，接入点将验证其从其他接入点收到的管理帧。如果其收到的任何帧不包括有效、预期的 MIC IE，则会向 WDS 报告这种不一致。接入点必须是 WDS 的成员。

```
dot11 ids mfp detector
```

4. 输入 SNTP 服务器的名称或 IP 地址。

```
sntp server server IP address
```

5. 返回到特权 EXEC 模式。

```
end
```

6. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

在特权 EXEC 模式下，根据以下步骤配置 WDS：

1. 进入全局配置模式。

```
configure terminal
```

2. 将 WDS 配置为 MFP 分配器。

当启用时， WDS 可管理签名密钥，以用于创建 MIC IE，并将其在生成器和检测器之间安全传输。

```
dot11 ids mfp distributor
```

3. 返回到特权 EXEC 模式。

```
end
```

4. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

配置验证失败限制

设置验证失败限制可保护网络免受称为 EAPOL 洪泛的拒绝服务攻击。如果客户端和接入点之间发生 802.1X 验证，这会在接入点、验证器和验证服务器之间触发一系列报文 (通过使用 EAPOL 报文格式)。如果验证尝试次数过多，则验证服务器 (通常为 RADIUS 服务器) 很快会不堪重负。如果不进行调整，单个客户端触发的验证请求就足以影响您的网络。

在监控模式下，接入点跟踪 802.1X 客户端尝试通过接入点进行验证的速率。如果网络被过多的验证尝试攻击，当超过验证阈值时，接入点会生成一个警告。

您可在接入点上配置这些限制：

- 通过接入点的 802.1X 尝试次数
- 接入点上的 EAPOL 洪泛持续时间 (以秒为单位)

当接入点检测到过多的验证尝试时，其会将 MIB 变量设置为指示以下信息：

- 检测到 EAPOL 洪泛。
- 验证尝试次数
- 具有最多验证尝试次数的客户端的 MAC 地址

在特权 EXEC 模式下，根据以下步骤设置接入点上触发故障的验证限制。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置验证尝试的次数和 EAPOL 洪泛在接入点上触发故障的秒数。

   ```
   dot11 ids eap attempts number period seconds
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

备注：

配置 RADIUS 和 TACACS+ 服务器

本章介绍了如何启用和配置远程验证拨入用户服务 (RADIUS) 和增强型终端访问控制器访问控制系统 (TACACS+)，在验证和授权过程中提供详细的结算信息和灵活的管理控制。 RADIUS 和 TACACS+ 通过 AAA 实现，且只能通过 AAA 命令启用。

提示 您可将接入点配置为本地验证器，提供主服务器的备用设备或在无 RADIUS 服务器的网络上提供验证服务。有关将接入点配置为本地验证器的详细说明，请参见第 335 页的 " 配置验证类型 "。

配置和启用 RADIUS

RADIUS 是一个分布式客户端 / 服务器系统，可保护网络免受非法访问。 RADIUS 客户端在支持的思科设备上运行，将验证请求发送到中央 RADIUS 服务器，其中包含了所有用户验证和网络服务访问信息。 RADIUS 主机通常是一个多用户系统，其运行思科安全访问控制服务器版本 3.0、 Livingston、 Merit、 Microsoft 或其他软件供应商的 RADIUS 服务器软件。如需了解更多信息，请参见 RADIUS 服务器文档。

在需要访问安全的以下网络环境中使用 RADIUS。

- 包含多供应商接入服务器的网络，每个服务器均支持 RADIUS。

  例如，来自多个供应商的接入服务器使用一个基于 RADIUS 服务器的安全数据库。在拥有多供应商接入服务器的基于 IP 的网络中，拨入用户通过一个 RADIUS 服务器进行验证，该服务器经自定义与 Kerberos 安全系统一起工作。

- 实际应用支持 RADIUS 协议的一站式网络安全环境，例如使用智能卡访问控制系统的接入环境。

- 已使用 RADIUS 的网络。

  您可将包含 RADIUS 客户端的接入点添加到网络。

- 需要资源结算的网络。

  您可使用独立于 RADIUS 验证或授权的 RADIUS 结算功能。RADIUS 结算功能允许在服务开始和结束时发送数据，显示在会话期间所用的资源量 (如时间、数据包、字节等)。因特网服务提供商可使用免费版本的 RADIUS 接入控制和结算软件来满足特定的安全和结算需求。

RADIUS 不适合在以下网络安全环境中使用。

- 交换机到交换机或路由器到路由器环境。

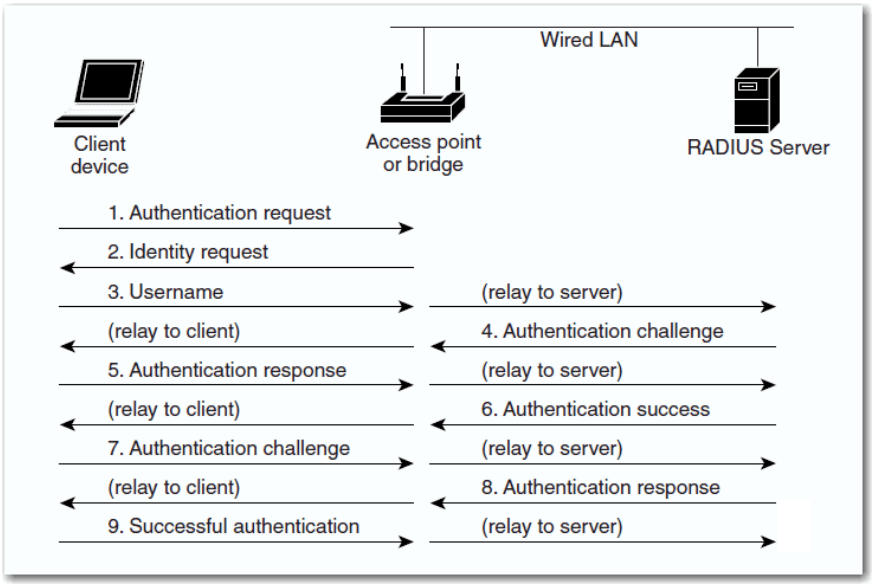
  RADIUS 不提供双向验证。如果非思科设备要求进行验证，RADIUS 可用于在一台设备和一台非 Cisco 设备之间完成验证。

- 使用各种服务的网络。 RADIUS 通常将一个用户绑定到一种服务模式。

RADIUS 操作

当无线用户尝试登录和验证访问权限由 RADIUS 服务器控制的接入点时，将在下图所示的步骤中执行网络验证。

图 114 - EAP 验证顺序



在步骤 1...9 中，无线客户端设备和有线局域网中的 RADIUS 服务器使用 802.1x 和 EAP 通过接入点执行相互验证。 RADIUS 服务器向客户端发送验证质询。客户端使用用户提供的密码执行单向加密，以生成质询响应，并将其发送给 RADIUS 服务器。

通过使用来自用户数据库的信息， RADIUS 服务器创建自己的响应，并将其与客户端的响应相比较。当 RADIUS 服务器验证客户端后，将以相反的顺序重复该过程，由客户端验证 RADIUS 服务器。

EAP 验证类型有多种，但无论采用哪种类型，接入点的工作方式都相同：它将来自无线客户端设备的验证消息转发到 RADIUS 服务器，并将来自 RADIUS 服务器的验证消息转发到无线客户端设备。有关使用 RADIUS 服务器设置客户端验证的说明，请参见第 341 页的“ 将验证类型分配到 SSID”。

配置 RADIUS

本节介绍了如何配置接入点来支持 RADIUS。至少，您必须确定运行 RADIUS 服务器软件的主机，并定义 RADIUS 验证的方法列表。您也可选择定义 RADIUS 授权和结算的方法列表。

方法列表定义了用于验证、授权或跟踪用户帐户的序列和方法。可使用方法列表指定要使用的一个或多个安全协议，确保在初始方法失败时提供一个备用系统。软件使用所列的第一个方法验证、授权或跟踪用户帐户；如果该方法没有响应，软件将选择列表中的下一个方法。该过程将持续到通过列出的一种方法成功通信，或列表中的方法用完为止。

您可在配置接入点的 RADIUS 功能之前访问和配置 RADIUS 服务器。

提示 在您输入 `aaa new-model` 命令之前， RADIUS 服务器的 CLI 命令被禁止。

默认配置

默认情况下， RADIUS 和 AAA 被禁用。为防止安全功能失效，不能使用 SNMP 通过网络管理应用程序配置 RADIUS。当启用时， RADIUS 可对通过 CLI 或 HTTP (设备管理器) 访问接入点的用户进行验证。

识别 RADIUS 服务器主机

接入点与 RADIUS 服务器的通信涉及多个组件：

- 主机名称或 IP 地址
- 验证目标端口
- 结算目标端口
- 密钥字符串
- 超时时间
- 重传值

可通过它们的主机名称或 IP 地址、主机名称和特定的 UDP 端口号或它们的 IP 地址和特定的 UDP 端口号来识别 RADIUS 安全服务器。

组合 IP 地址和 UDP 端口号创建一个唯一的标识符，允许将不同的端口单独定义为提供一种特定 AAA 服务的 RADIUS 主机。该唯一标识符允许将 RADIUS 请求发送至相同 IP 地址的服务器上的多个 UDP 端口。

提示 对于思科 IOS 版本 12.2(8)JA 及更新版本，接入点使用一个随机选择的 UDP 源端口号 (范围为 21645 - 21844) 与 RADIUS 服务器进行通信。

如果同一 RADIUS 服务器上的两个不同主机条目配置用于同一服务 —— 例如，结算 —— 所配置的第二个主机条目将充当第一个条目的故障切换备用条目。在本例中，如果第一个主机条目无法提供结算服务，接入点尝试使用同一设备上配置的第二个主机条目来执行结算服务。(RADIUS 主机条目的尝试次序与其配置次序相同。)

RADIUS 服务器和接入点使用一个共享密文字符串来加密密码和交换响应。要配置 RADIUS 使用 AAA 安全命令，必须指定运行 RADIUS 服务器守护进程的主机以及与接入点共享的密文 (密钥) 字符串。

可对所有 RADIUS 服务器中的每个服务器以全局方式配置超时、重传和加密密钥值，或在全局和每服务器设置中对它们进行配置。

将这些设置全局应用于与接入点通信的所有 RADIUS 服务器，使用三个独特的全局配置命令：

```
radius-server timeout
radius-server retransmit
radius-server key
```

要将这些值应用到一个特定的 RADIUS 服务器，使用 `radius-server host` 全局配置命令。

提示 如果在接入点上配置了全局和每个服务器功能 (超时、重传和密钥命令)，每个服务器的定时器、重传和密钥值命令将覆盖全局定时器、重传和密钥值命令。

有关在所有 RADIUS 服务器上配置这些设置的信息，请参见第 392 页的 “ 配置所有 RADIUS 服务器 ”。

您可配置接入点使用 AAA 服务器组将用于验证的现有服务器主机进行分组。更多信息，请参见第 385 页的 “ 定义 AAA 服务器组 ”。

在特权 EXEC 模式下，根据以下步骤配置每服务器 RADIUS 服务器通信。该过程必须执行。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 指定远程 RADIUS 服务器主机的 IP 地址或主机名称。
   - (可选) 对于 `auth-port` *`port-number`*，指定用于验证请求的 UDP 目标端口。
   - (可选) 对于 `acct-port` *`port-number`*，指定用于结算请求的 UDP 目标端口。

- (可选) 对于 `timeout seconds`，指定接入点在重发送之前等待 RADIUS 服务器应答的时间间隔。其范围为 1...1000。

  该设置将忽略 `radius-server timeout` 全局配置命令设置。如果未使用 `radius-server host` 命令设置超时，将使用 `radius-server timeout` 命令的设置。
- (可选) 对于 `retransmit retries`，指定在服务器没有响应或响应缓慢时，将 RADIUS 请求重新发送至服务器的次数。其范围为 1...1000。

  如果未使用 `radius-server host` 命令设置重新发送值，则将使用 `radius-server retransmit` 全局配置命令的设置。
- (可选) 对于 `key string`，指定在接入点和 RADIUS 服务器上运行的 RADIUS 守护进程之间使用的验证和加密密钥。

提示　密钥属于文本字符串，它必须与 RADIUS 服务器上使用的加密密钥相匹配。始终将密钥配置为 radius-server host 命令的最后一项。前导空格将被忽略，但密钥中间和末尾可使用空格。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

要配置接入点识别与一个 IP 地址关联的多个主机条目，根据需要输入以下命令多次，确保每个 UDP 端口号均不相同。接入点软件按您指定的顺序搜索主机。设置特定 RADIUS 主机使用的超时、重新发送和加密密钥值。

```
radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
```

4. 当需要启用结算时，进入 SSID 的 SSID 配置模式。

   SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。

   ```
   dot11 ssid ssid-string
   ```

5. 启用该 SSID 的 RADIUS 结算。对于 list-name，指定结算方法列表。

   ```
   accounting list-name
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. 确认您的输入。

   ```
   show running-config
   ```

8. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要删除指定的 RADIUS 服务器，使用 `no radius-server host` *`hostname | ip-address`* 全局配置命令。

本例显示了如何将一个 RADIUS 服务器配置为用于验证，另一个服务器用于结算：

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

本例显示了如何配置用于 `RADIUS` 结算的 `SSID`：

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

本例显示了如何将 *`host1`* 配置为 `RADIUS` 服务器，以及使用默认端口执行验证和结算：

```
AP(config)# radius-server host host1
```

您还需要在 RADIUS 服务器上配置一些设置。这些设置包括接入点的 IP 地址以及服务器和接入点要共享的密钥字符串。

配置 RADIUS 登录验证

要配置 AAA 验证，您可定义一个命名验证方法列表，然后将该列表应用到不同接口。方法列表定义了验证类型以及要执行的顺序。必须在执行任何所定义的验证类型之前将方法列表应用于特定的接口。唯一的例外情况是默认方法列表 (巧合的是也被命名为 default)。除了已经过明确定义的命名方法列表，默认的方法列表将自动应用到所有其他接口。

方法列表描述了验证用户时的顺序以及调用的验证方法。您可指定一个或多个安全性协议用于验证，从而确保当初始方法失败时可使用备用验证系统。软件使用列出的第一种方法来验证用户；如果该方法未能响应，软件将选择列表中的第二种验证方法。该过程将持续，直至通过所列验证方法顺利通信，或者定义的所有方法都被排除。如果验证在该循环的任一点失败 —— 即安全服务器或本地用户名数据库拒绝用户访问 —— 验证过程将停止，且不再尝试其他验证方法。

在特权 EXEC 模式下，根据以下步骤配置登录验证。该过程必须执行。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 创建登录验证方法列表。
   - 当 `login authentication` 命令中没有指定命名列表时，如果要创建默认列表，可使用 default 关键字，并在后面输入默认情况下使用的方法。默认方法列表将自动应用到所有接口。
   - 对于 *method1...*，指定验证算法尝试的实际方法。附加验证方法仅在前一种方法返回错误时才会使用 (而不是失败)。

   选择以下其中一种方法：
   - 命令行

     使用命令行密码进行验证。必须在使用该验证方法之前定义一个命令行密码。使用 `password` *password* 命令行配置命令。
   - `Local` （**本地**）

     使用本地用户名数据库进行验证。您必须将用户名信息输入到数据库中。使用 `username` *password* 全局配置命令。
   - `Radius`

     使用 RADIUS 验证。在使用该验证方法之前，您必须先配置 RADIUS 服务器。更多信息，请参见第 380 页的 “ 识别 RADIUS 服务器主机 ”。

   ```
   aaa authentication login {default | list-name}
   method1 [method2...]
   ```

4. 进入命令行配置模式，配置希望应用于验证列表的命令行。

   ```
   line [console | tty | vty] line-number [ending-line-
   number]
   ```

5. 将验证列表应用到命令行或命令行组。
   - 如果指定了 `default`，则将使用通过 `aaa authentication login` 命令创建的默认列表。
   - list-name 指定通过 `aaa authentication login` 命令创建的列表。

   ```
   login authentication {default | list-name}
   ```

6. 将接入点配置为在 NAS_ID 属性中发送其系统名称，以便进行验证。

   ```
   radius-server attribute 32 include-in-access-req
   format %h
   ```

7. 返回到特权 EXEC 模式。

   ```
   end
   ```

8. 确认您的输入。

   ```
   show running-config
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要禁用 AAA，使用 `no aaa new-model` 全局配置命令。
- 要禁用 AAA 验证，使用 `no aaa authentication login {default | list-name} method1 [method2...]` 全局配置命令。

要禁止对登录或返回默认值执行 RADIUS 验证，使用 `no login authentication {default | list-name}` 命令行配置命令。

定义 AAA 服务器组

您可配置接入点使用 AAA 服务器组将用于验证的现有服务器主机进行分组。选择所配置服务器主机的一个子集，并将其用于特定的服务。服务器组与全局服务器主机列表一起使用。列表包含了所选服务器主机的 IP 地址。

若每个条目具有一个唯一的标识符 (组合 IP 地址和 UDP 端口号)，服务器组还包含用于同一服务器的多个主机条目，从而允许将不同的端口单独定义为提供一种特定 AAA 服务的 RADIUS 主机。如果在同一 RADIUS 服务器上为相同服务 (例如，结算) 配置了两个不同的主机条目，则配置的第二个主机条目将作为第一个条目的故障切换备用条目。

您可使用 `server` 组服务器配置命令将特定服务器关联到已定义的服务器组。您可通过 IP 地址识别服务器，或通过可选的 `authport` 和 `acct-port` 关键字识别多个主机实例或条目。

在特权 EXEC 模式下，根据以下步骤定义 AAA 服务器组，并将特定的 RADIUS 服务器与之关联。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 指定远程 RADIUS 服务器主机的 IP 地址或主机名称。
   - (可选) 对于 `auth-port` *port-number*，指定用于验证请求的 UDP 目标端口。
   - (可选) 对于 `acct-port` *port-number*，指定用于结算请求的 UDP 目标端口。
   - (可选) 对于 `timeout` *seconds*，指定接入点在重发送之前等待 RADIUS 服务器应答的时间间隔。

     其范围为 1...1000。该设置将忽略 `radius-server timeout` 全局配置命令设置。如果未使用 `radius-server host` 命令设置超时，将使用 `radius-server timeout` 命令的设置。
   - (可选) 对于 `retransmit` *retries*，指定在服务器没有响应或响应缓慢时，将 RADIUS 请求重新发送至服务器的次数。

     其范围为 1...1000。如果未通过 `radius-server hostp` 命令设置任何重传值，使用 `radius-server retransmit` 全局配置命令的设置。
   - (可选) 对于 `key` *string*，指定在接入点和 RADIUS 服务器上运行的 RADIUS 守护进程之间使用的验证和加密密钥。

   提示　密钥属于文本字符串，它必须与 RADIUS 服务器上使用的加密密钥相匹配。始终将密钥配置为 radius-server host 命令的最后一项。前导空格将被忽略，但密钥中间和末尾可使用空格。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

   要配置接入点识别与一个 IP 地址关联的多个主机条目，根据需要输入以下命令多次，确保每个 UDP 端口号均不相同。接入点软件按您指定的顺序搜索主机。设置特定 RADIUS 主机使用的超时、重新发送和加密密钥值。

   ```
   radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
   ```

4. 使用一个组名定义 AAA 服务器组。

   该命令将接入点置于服务器组配置模式。

   ```
   aaa group server radius group-name
   ```

5. 将特定 RADIUS 服务器关联到定义的服务器组。

   对 AAA 服务器组中的每个 RADIUS 服务器重复该步骤。组中的每个服务器都必须在步骤 2 中预先定义。

   ```
   server ip-address
   ```

6. 返回到特权 EXEC 模式。

   ```
   end
   ```

7. 确认您的输入。

   ```
   show running-config
   ```

8. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

9. 启用 RADIUS 登录验证。

   参见第 383 页的 " 配置 RADIUS 登录验证 "。

   - 要删除指定的 RADIUS 服务器，使用 `no radius-server host` *hostname*|*ip-address* 全局配置命令。
   - 要从配置列表中删除一个服务器组，使用 `no aaa group server radius` *group-name* 全局配置命令。
   - 要删除 RADIUS 服务器的 IP 地址，使用 `no server` *ip-address* 服务器组配置命令。

在本例中，将接入点配置为识别两个不同的 RADIUS 组服务器 (*group1* 和 *group2*)。 Group1 在同一 RADIUS 服务器上有两个配置了相同服务的不同主机条目。第二个主机条目作为第一个条目的故障切换备用条目。

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646

AP(config)# aaa group server radius group1

AP(config-sg-radius)# server 172.20.0.1 auth-port
1000 acct-port 1001

AP(config-sg-radius)# exit

AP(config)# aaa group server radius group2

AP(config-sg-radius)# server 172.20.0.1 auth-port
2000 acct-port 2001

AP(config-sg-radius)# exit
```

配置用户特权访问和网络服务的 RADIUS 授权

使用 AAA 授权限制提供给用户的服务。当启用 AAA 授权时，接入点使用从用户配置文件提取的信息 (即在本地用户数据库或安全服务器中) 来配置用户会话。当用户配置文件中的信息允许时，用户被授予访问所请求服务的权限。

提示 本节介绍了如何设置接入点管理员而不是无线电客户端设备的授权。

您可使用 `aaa authorization` 全局配置命令和 `radius` 关键字来设置将用户网络访问限制为特权 EXEC 模式的参数。

`aaa authorization exec radius local` 命令设置以下授权参数：

- 如果已使用 RADIUS 执行验证，则使用 RADIUS 进行特权 EXEC 访问验证。
- 如果未使用 RADIUS 执行验证，则使用本地数据库。

提示 对于已通过 CLI 登录的验证用户，即使配置过授权，也会绕过授权。

在特权 EXEC 模式下，根据以下步骤指定特权 EXEC 访问和网络服务的 RADIUS 授权。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置接入点，对所有网络相关服务请求执行用户 RADIUS 授权。

   ```
   aaa authorization network radius
   ```

3. 配置接入点执行用户 RADIUS 授权，确定用户是否具有特权 EXEC 访问权限。

   `exec` 关键字可返回用户配置文件信息 (例如， `autocommand` 信息)。

   ```
   aaa authorization exec radius
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

   要禁用授权，使用 `no aaa authorization {network | exec}` ***method1*** 全局配置命令。

配置拆接数据包

拆接数据包 (PoD) 也称为拆接报文。可在因特网工程任务组 (IETF) 因特网标准 RFC 3576 中找到关于 PoD 的附加信息。

拆接数据包包含一种终止已连接会话的方法。 PoD 是一种 RADIUS Disconnect_Request 数据包，设计为在验证代理服务器希望在 RADIUS access_accept 数据包接受会话后断开用户的连接时使用。至少在两种情况下需要使用该数据包：

- 检测到欺诈使用，在接受呼叫之前不能执行。
- 当预付费接入时间用完时，断开热点用户的连接。

当会话终止时， RADIUS 服务器将一个拆接报文发送到网络接入服务器 (NAS)、接入点或 WDS。对于 802.11 会话，必须在 Pod 请求中提供 Calling-Station-ID [31] RADIUS 属性 (客户端的 MAC 地址)。接入点或 WDS 尝试解除关联相关会话，然后将一个拆接响应报文发送给 RADIUS 服务器。报文类型如下：

- 40 —— 断开连接请求
- 41 —— 断开连接 —— ACK
- 42 —— 断开连接 —— NAK

提示

- 有关如何配置 PoD 请求的说明，请参见 RADIUS 服务器应用文档。
- 接入点不阻止客户端后续的重关联尝试。由安全管理员负责在发出 PoD 请求之前禁用客户端帐户。
- 当配置了 WDS 时，将 PoD 请求转发至 WDS。 WDS 将解除关联请求转发到父接入点，然后从其自有的内部表中清除会话。
- 思科 CNS Access Registrar (CAR) RADIUS 服务器支持 PoD，但 v4.0 及更早版本的思科 Secure ACS 服务器不支持 PoD。

在特权 EXEC 模式下，根据以下步骤配置 PoD。

1. 进入全局配置模式。

   `configure terminal`

2. 当提供特定的会话属性时，允许由来自 RADIUS 服务器的请求断开用户会话。

   `port` *`port number`* —— (可选) 接入点监听 PoD 请求的 UDP 端口。默认值为 1700。

   - `auth-type`

     802.11 会话不支持该参数。
   - `clients`

     (可选) —— 最多可将 4 个 RADIUS 服务器指定为客户端。如果存在该配置，且 PoD 请求来自一个不位于列表上的设备，则拒绝该请求。
   - `Ignore`

     (可选) —— 当设为 *`server_key`* 时，则在收到 PoD 请求时不对共享密文进行验证。
   - `session-key`

     802.11 会话不支持此参数。
   - `server-key`

     配置共享密文字符串。

string —— 在网络接入服务器和客户端工作站之间共享的共享密文字符串。两个系统的共享密文必须相同。

提示 该参数后输入的任何数据都被视为共享秘密字符串。

```
aaa pod server [port port number]
[auth-type {any | all | session-key}] [clients
client 1...] [ignore {server-key string...|
session-key }] | server-key string...]}
```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

启动 RADIUS 结算

AAA 结算功能跟踪用户正在访问的服务以及他们所消耗的网络资源量。当启用 AAA 结算时，接入点以结算记录的形式向 RADIUS 安全服务器报告用户活动。

每个结算记录包括结算属性值 (AV) 对，并存储在安全服务器上。该数据随后可用于网络管理、客户端计费或审计。

有关由接入点发送且拥有的属性的完整列表，请参见第 397 页的 “ 由接入点发送的 RADIUS 属性 ”。

在特权 EXEC 模式下，根据以下步骤为每个思科 IOS 特权级别及网络服务启用 RADIUS 结算功能：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 为所有网络相关服务请求启用 RADIUS 结算。

   ```
   aaa accounting network start-stop radius
   ```

3. 将接入点配置为在 NAS_IP_ADDRESS 属性中发送 BVI IP 地址，以便对记录进行结算。

   ```
   ip radius source-interface bvi1
   ```

4. 输入结算更新间隔，单位为分钟。

   ```
   aaa accounting update periodic minutes
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. 确认您的输入。

   ```
   show running-config
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

   要禁用结算，使用 `no aaa accounting {network | exec} {start-stop}` *method1...* 全局配置命令。

选择 CSID 格式

可以在 RADIUS 数据包的 Called-Station-ID (CSID) 和 Calling-Station-ID 属性中选择 MAC 地址格式。使用 `dot11 aaa csid` 全局配置命令选择 CSID 格式。

下表列出了格式选项，并给出了相应的 MAC 地址实例。

选项	MAC 地址示例
默认	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
未格式化	000785b35f4a

要返回默认的 CSID 格式，使用 **no** 格式的 `dot11 aaa csid` 命令或输入

```
dot11 aaa csid default
```

提示　您还可以使用 `wlccp wds aaa csid` 命令来选择 CSID 格式。

配置所有 RADIUS 服务器

在特权 EXEC 模式下，根据以下步骤配置接入点和所有 RADIUS 服务器之间的全局通信设置。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 指定在接入点和所有 RADIUS 服务器之间使用的共享密文字符串。

   提示　密钥属于文本字符串，它必须与 RADIUS 服务器上使用的加密密钥相匹配。前导空格将被忽略，但密钥中间和末尾可使用空格。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

   ```
   radius-server key string
   ```

3. 指定接入点放弃之前将每个 RADIUS 请求发送到服务器的次数。默认值为 3 ； 范围为 1...1000。

   ```
   radius-server retransmit retries
   ```

4. 指定接入点在重新发送请求之前等待 RADIUS 请求应答的时间 (单位：秒)。

   默认值为 5 ；范围为 1...1000。

   ```
   radius-server timeout seconds
   ```

5. 使用该命令导致思科 IOS 软件将未能响应验证请求的 RADIUS 服务器标记为 " 停机 "，从而避免在尝试下一个配置的服务器之前等待请求超时。

   在您指定的时长 (单位：分钟) 内 (最高达 1440 (24 小时))，附加请求跳过标记为停机的 RADIUS 服务器。

   提示 当定义了多个 RADIUS 服务器时，需要对该命令进行配置。如果未配置，则不执行客户端验证。当定义了一个 RADIUS 服务器时，该命令为可选。

   ```
   radius-server deadtime minutes
   ```

6. 将接入点配置为在 NAS_ID 属性中发送其系统名称，以便进行验证。

   ```
   radius-server attribute 32 include-in-access-req
   format %h
   ```

7. 返回到特权 EXEC 模式。

   ```
   end
   ```

8. 确认您的设置。

   ```
   show running-config
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

本例说明了如何设置两个主服务器以及一个本地验证器，其中服务器停机时间为 10 分钟：

```
AP(config)# aaa new-model


AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001 key 77654


AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646 key 77654


AP(config)# radius-server host 10.91.6.151 auth-
port 1812 acct-port 1813 key 110337


AP(config)# radius-server deadtime 10
```

要返回重传、超时和停机时间的默认设置，使用以下命令的 `no` 格式。

配置接入点使用供应商相关 RADIUS 属性

因特网工程任务组 (IETF) 草案标准规定了一种使用供应商特定属性 (属性 26) 在接入点和 RADIUS 服务器之间传送供应商特定信息的方法。供应商相关属性 (VSA) 允许供应商支持并不通用的个人扩展属性。

思科 RADIUS 工具使用规范中建议的格式支持一个供应商相关选项。思科的供应商 ID 是 9，所支持的选项具有供应商类型 1，即 cisco-avpair。该值是具有以下格式的字符串：

```
protocol : attribute sep value *
```

协议是特定授权类型的思科协议属性值。属性和值是在思科 TACACS+ 规范中定义的一个相应 AV 对， sep = 用于必选属性，星号 (*) 用于可选属性。这可将 TACACS+ 授权可用的一整套功能供 RADIUS 使用。

例如，以下 AV 对在 IP 授权期间激活名为 ip address pools 的多个思科功能 (在 PPP 的 IPCP 地址分配期间)：

```
cisco-avpair= ”ip:addr-pool=first“
```

下例显示了如何给从接入点登录的用户提供到特权 EXEC 命令的快速访问：

```
cisco-avpair= ”shell:priv-lvl=15“
```

其他供应商拥有各自唯一的供应商 ID、选项和关联 VSA。如需了解关于供应商 ID 和 VSA 的更多信息，请参见 RFC 2138，“ 远程验证拨入用户服务 (RADIUS)。 ”

在特权 EXEC 模式下，根据以下步骤配置接入点识别和使用 VSA。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 允许接入点按 RADIUS IETF 属性 26 的定义识别和使用 VSA。
   - (可选) 使用 `accounting` 关键字将已识别的供应商相关属性组限制为仅结算属性。
   - (可选) 使用 `authentication` 关键字将已识别的供应商相关属性组限制为仅验证属性。

如果输入该命令时不带关键字，将使用结算和验证供应商相关属性。

```
radius-server vsa send [accounting | authentication]
```

3. 返回到特权 EXEC 模式。

```
end
```

4. 确认您的设置。

```
show running-config
```

5. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

有关 RADIUS 属性的完整列表或关于 VSA 26 的更多信息，请参见出版物 Cisco IOS Security Configuration Guide for Release 12.2 (思科 IOS 安全配置指南 (版本 12.2))。

配置接入点进行供应商专有 RADIUS 服务器通信

虽然 RADIUS 的 IETF 标准草案规定了在接入点和 RADIUS 服务器之间交换供应商专有信息的方法，一些供应商已通过独特的方式扩展了 RADIUS 属性集。思科 IOS 软件支持一部分供应商专有 RADIUS 属性。

正如前文所述，配置 RADIUS (无论是供应商专有或与 IETF 草案兼容) 时，必须指定运行 RADIUS 服务器守护进程的主机以及与接入点共享的密文字符串。通过 `radius-server` 全局配置命令指定 RADIUS 主机和密文字符串。

在特权 EXEC 模式下，根据以下步骤指定供应商专有 RADIUS 服务器主机和共享密文字符串。

1. 进入全局配置模式。

```
configure terminal
```

2. 指定远程 RADIUS 服务器主机的 IP 地址或主机名称，并确认其正在使用一种供应商专有 RADIUS 工具。

```
radius-server host {hostname | ip-address} non-standard
```

3. 指定在接入点和供应商专有 RADIUS 服务器之间使用的共享密文字符串。

接入点和 RADIUS 服务器使用该文本字符串加密密码以及交换响应。

提示　密钥属于文本字符串，它必须与 RADIUS 服务器上使用的加密密钥相匹配。前导空格将被忽略，但密钥中间和末尾可使用空格。如果密钥中使用了空格，则除非将引号作为密钥的一部分，否则不要使用引号将密钥括起来。

```
radius-server key string
```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的设置。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

   - 要删除供应商专有 RADIUS 主机，使用 `no radius-server host {hostname | ip-address} non-standard` 全局配置命令。
   - 要禁用密钥，使用 `no radius-server key` 全局配置命令。

本例显示了如何指定供应商专有 RADIUS 主机以及如何在接入点和服务器之间使用密钥 `rad124`：

```
AP(config)# radius-server host 172.20.30.15
nonstandard
AP(config)# radius-server key rad124
```

显示 RADIUS 配置

要显示 RADIUS 配置，使用 `show running-config` 特权 EXEC 命令。

提示　当在接入点上配置了 DNS 时，`show running-config` 显示服务器的 IP 地址而不是服务器名称。

由接入点发送的 RADIUS 属性

第 397 页的表 104 到第 397 页的表 106 标出了由接入点在 access-request、access-accept、和 accounting-request 数据包中发送至客户端的属性。

表 104 - 在 Access-Request 数据包中发送的属性

属性 ID	描述
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC 地址)
31	Calling-Station-ID (MAC 地址)
32	NAS-Identifier(1)
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

(1) 如果配置了属性 32 (include-in-access-req)，接入点将发送 NAS 标识符。

表 105 - Access-Accept 数据包中的属性

属性 ID	描述
25	Class
27	Session-Timeout
64	Tunnel-Type(1)
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA (属性 26)	LEAP session-key
VSA (属性 26)	Auth-Algo-Type
VSA (属性 26)	SSID

(1) RFC2868 ； 定义了一个 VLAN 覆盖号。

表 106 - 在 Accounting-Request (启动) 数据包中发送的属性

属性 ID	描述
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type

表 106 - 在 Accounting-Request (启动) 数据包中发送的属性

属性 ID	描述
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface

表 107 - Accounting-Request (更新) 数据包中发送的属性

属性 ID	描述
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	VLAN-ID
VSA (属性 26)	Connect-Progress
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface

表 108 - Accounting-Request (停止) 数据包中发送的属性

属性 ID	描述
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets

表 108 - Accounting-Request (停止) 数据包中发送的属性 (续)

属性 ID	描述
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	Disc-Cause-Ext
VSA (属性 26)	VLAN-ID
VSA (属性 26)	Connect-Progress
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface
VSA (属性 26)	Auth-Algo-Type

默认情况下，接入点的服务类型属性设置为 “ 仅验证 ”，它向验证服务器发送重新验证请求。但一些 Microsoft IAS 服务器不支持 “ 仅验证 ” 服务类型属性。根据用户要求，将 service-type 属性设为：

```
dot11 aaa authentication attributes service-type
login-user
```

或

```
dot11 aaa authentication attributes service-type
framed-user。
```

默认情况下，在接入请求中发送服务类型 “login”。

配置和启用 TACACS+

TACACS+ 是一个安全应用程序，它为尝试获取接入点访问曲线的用户提供集中验证。和 RADIUS 不同， TACACS+ 不对关联至接入点的客户端设备进行验证。

TACACS+ 服务保持在 TACACS 守护进程 (通常在 UNIX 或网页 NT 工作站中运行) 的数据库中。配置接入点上的 TACACS+ 功能之前请访问并配置 TACACS+ 服务器。

TACACS+ 提供了独立且模块化的验证、授权和结算设施。TACACS+ 允许单个接入控制服务器 (TACACS+ 守护进程) 来单独提供每项服务：验证、授权和结算。每种服务可连接到其自身的数据库，以便使用该服务器或网络上可用的其他服务，具体取决于守护进程的功能。

TACACS+ 通过 AAA 安全服务进行管理，可提供以下服务：

验证

通过登录和密码对话框、质询和响应及报文支持，提供对管理员验证的完全控制。

验证设施可与管理员进行对话 (例如，在提供用户名和密码后，通过几个问题 (如家庭住址、母亲的娘家姓、服务类型和社保号) 质询用户)。TACACS+ 验证服务还可将消息发送至管理员屏幕。例如，消息会通知管理员，由于公司的密码时效政策，必须更改他们的密码。

授权

在管理员会话期间对管理员功能提供精细的控制，包括但不限于：设置自动命令、访问控制、会话持续时间或协议支持。您也可对管理员通过 TACACS+ 授权功能执行的命令添加限制条件。

Accounting (结算)

收集计费、审计和报告信息，并将它们发送至 TACACS+ 守护进程。网络管理员可使用结算设施来跟踪管理员活动以便进行安全审计，或提供用户结算信息。结算记录包括管理员身份、开始和停止时间、所执行的命令 (如 PPP)，数据包数量和字节数。

TACACS + 协议提供了接入点和 TACACS+ 守护进程之间的验证，并保持机密，因为接入点和 TACACS+ 守护进程之间的所有协议交换均被加密。

您需要一个运行 TACACS+ 守护进程软件的系统在接入点上使用 TACACS+。

TACACS+ 操作

当管理员尝试通过 TACACS+ 对接入点进行验证，从而实现简单的 ASCII 登录时，将发生以下过程：

1. 当建立连接时，接入点联系 TACACS+ 守护进程来获取用户名提示，然后显示给管理员。
2. 管理员输入用户名，然后接入点联系 TACACS+ 守护进程来获取密码提示。
3. 向管理员显示密码提示，管理员输入密码，然后密码被发送到 TACACS+ 守护进程。

   TACACS+ 允许在守护进程和管理员之间保持会话，直到守护进程接收足够的信息来验证管理员身份。守护进程提示输入用户名和密码组合，但可能包括其他条目，如用户母亲的娘家姓。
4. 接入点最终收到来自 TACACS+ 守护进程的以下一种响应。

响应	描述
ACCEPT	管理员通过验证，可重新开始服务。如果接入点配置为需要授权，则在此时开始授权。
REJECT	管理员未经过验证。管理员可能被拒绝访问，或提示重新尝试登录序列，具体取决于 TACACS+ 守护进程。
ERROR	在通过守护进程进行验证期间或守护进程和接入点之间的网络连接期间发生错误。如果收到错误响应，接入点通常会尝试使用另一种方法对管理员进行验证。
续	给管理员提示其他验证信息。

   通过验证后，如果已经在接入点上启用了授权，管理员进入额外的授权阶段。管理员必须首先成功完成 TACACS+ 验证，然后才能继续进行 TACACS+ 授权。
5. 如果需要使用 TACACS+ 授权，则再次联系 TACACS+ 守护进程，随后守护进程返回一个 ACCEPT 或 REJECT 授权响应。如果返回 ACCEPT 响应，响应将包含属性格式的数据，用于将 EXEC 或 NETWORK 会话转给管理员，以确定管理员可以访问的服务：
   - Telnet、 rlogin 或特权 EXEC 服务
   - 连接参数，包括主机或客户端 IP 地址、访问列表和管理员超时

配置 TACACS+

要配置接入点以支持 TACACS+，您必须标识保持 TACACS+ 守护进程的主机，并定义 TACACS+ 验证的方法列表。您可定义 TACACS+ 授权和结算的方法列表 (可选)。

方法列表定义了验证使用的方法及顺序，以便对管理员进行验证、授权或记账。可使用方法列表指定要使用的一个或多个安全协议，确保在初始方法失败时提供一个备用系统。

软件使用列出的第一种方法来对管理员验证、授权或记账；如果该方法未能响应，软件将选择列表中的下一种方法。该过程将持续到通过列出的一种方法成功通信，或列表中的方法用完为止。

默认 TACACS+ 配置

默认情况下， TACACS+ 和 AAA 被禁用。

为防止安全性失效，您不能通过网络管理程序来配置 TACACS+。启用后， TACACS+ 可对通过 CLI 访问接入点的管理员进行验证。

标识 TACACS+ 服务器主机和设置验证密钥

您可配置接入点使用单台服务器或 AAA 服务器组，将现有服务器主机组合在一起进行验证。您可将服务器分组，选择所配置服务器主机的一个子集，并将其用于特定的服务。服务器组使用全局服务器主机列表，其中包含所选服务器主机的 IP 地址。

在特权 EXEC 模式下，根据以下步骤标识 IP 主机或维护 TACACS+ 服务器的主机，并设置加密密钥 (可选)。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 标识 IP 主机或维护 TACACS+ 服务器的主机。

   输入该命令多次，以创建首选主机列表。软件将根据您指定的顺序搜索主机。

   - *hostname* 用于指定主机的名称或 IP 地址。
   - (可选) `port` *integer* 用于指定服务器端口号。

     默认端口为 49。范围为 1...65535。
   - (可选) `timeout` *integer* 用于指定接入点等待守护进程响应的时间 (秒)，该时间过后无响应将超时，并报告一个错误。

     默认值为 5 秒。范围为 1...1000 秒。

- (可选) key *string* 用于指定加密和解密接入点和 TACACS+ 守护进程之间所有通信的加密密钥。TACACS+ 守护进程上必须配置相同的密钥，加密才能成功。

```
tacacs-server host hostname [port integer] [timeout integer] [key string]
```

3. 启用 AAA。

```
aaa new-model
```

4. (可选) 定义 AAA 服务器组及组名。

   该命令将接入点置于服务器组子配置模式。

```
aaa group server tacacs+ group-name
```

5. (可选) 将特定 TACACS+ 服务器关联到定义的服务器组。对 AAA 服务器组中的每台 TACACS+ 服务器重复该步骤。

   组中的每个服务器都必须在步骤 2 中预先定义。

```
server ip-address
```

6. 返回到特权 EXEC 模式。

```
end
```

7. 确认您的输入。

```
show tacacs
```

8. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

- 要删除指定的 TACACS+ 服务器名称或地址，可使用 `no tacacs-server host hostname` 全局配置命令。
- 要从配置列表中删除服务器组，可使用 `no aaa group server tacacs+ group-name` 全局配置命令。
- 要删除 TACACS+ 服务器的 IP 地址，可使用 `no server ip-address` 服务器组子配置命令。

配置 TACACS+ 登录验证

要配置 AAA 验证，您可定义一个命名验证方法列表，然后将该列表应用到不同接口。方法列表定义验证类型以及执行的顺序；要让定义的验证方法得以执行，必须先将其应用到特定的接口。唯一的例外情况是默认方法列表 (巧合的是也被命名为 default)。除了已经过明确定义的命名方法列表，默认的方法列表将自动应用到所有其他接口。定义的方法列表将优先于默认方法列表。

方法列表描述了验证用户时的顺序以及调用的验证方法。您可指定一个或多个安全性协议用于验证，从而确保当初始方法失败时可使用备用验证系统。软件使用列出的第一种方法来验证用户；如果该方法未能响应，软件将选择列表中的第二种验证方法。

该过程将持续，直至通过所列验证方法顺利通信，或者定义的所有方法都被排除。如果验证在该循环的任一点失败 —— 即安全服务器或本地用户名数据库拒绝管理员访问 —— 验证过程将停止，且不再尝试其他验证方法。

在特权 EXEC 模式下，根据以下步骤配置登录验证。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用 AAA。

   ```
   aaa new-model
   ```

3. 创建登录验证方法列表。
   - 当 `login authentication` 命令中没有指定命名列表时，如果要创建默认列表，可使用 default 关键字，**并在后面输入默认情况下使用的方法**。默认方法列表将自动应用到所有接口。
   - *`list-name`* 用于指定一个字符串，以命名刚创建的列表。
   - *`method1`*... 用于指定验证算法尝试使用的方法。附加验证方法仅在前一种方法返回错误时才会使用 (而不是失败)。

选择以下其中一种方法：

- 命令行

  使用命令行密码进行验证。必须在使用该验证方法之前定义一个命令行密码。使用 `password` *`password`* 命令行配置命令。

- 本地

  使用本地用户名数据库进行验证。您必须将用户名信息输入到数据库中。使用 `username` *`password`* 全局配置命令。

- `tacacs+`

  使用 TACACS+ 验证。在使用该验证方法之前，您必须先配置 TACACS+ 服务器。

  ```
  aaa authentication login {default | list-name}
  method1 [method2...]
  ```

4. 进入命令行配置模式，配置想要应用验证列表的命令行。
5. 进入命令行配置模式。
6. 配置命令行。
7. 应用验证列表。

   ```
   line [console | tty | vty] line-number [ending-line-
   number]
   ```

8. 将验证列表应用到命令行或命令行组。
   - 如果指定了 `default`，则将使用通过 `aaa authentication login` 命令创建的默认列表。
   - *list-name* 指定通过 `aaa authentication login` 命令创建的列表。

   ```
   login authentication {default | list-name}
   ```

9. 返回到特权 EXEC 模式。

   ```
   end
   ```

10. 确认您的输入。

    ```
    show running-config
    ```

11. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

- 要禁用 AAA，使用 `no aaa new-model` 全局配置命令。
- 要禁用 AAA 验证，使用 `no aaa authentication login {default | list-name} method1 [method2...]` 全局配置命令。
- 要禁用登录时的 TACACS+ 验证或返回到默认值，使用 `no login authentication {default | list-name}` 命令行配置命令。

配置特权 EXEC 访问和网络服务的 TACACS+ 授权

使用 AAA 授权限制提供给管理员的服务。当启用 AAA 授权时，接入点使用从管理员配置文件中提取的信息 (保存在本地用户数据库或安全服务器中) 来配置管理员会话。当管理员配置文件中的信息允许时，管理员被授予访问所请求的服务的权限。

您可使用 `aaa authorization` 全局配置命令，通过 `tacacs+` 关键字设置参数，限制管理员网络访问特权 EXEC 模式。

`aaa authorization exec tacacs+ local` 命令用于设置这些授权参数。

- 如果已使用 TACACS+ 执行验证，则使用 TACACS+ 进行特权 EXEC 访问验证。
- 如果未使用 TACACS+ 执行验证，则使用本地数据库。

提示 即使配置了授权，通过 CLI 登录的已验证管理员将绕过授权。

在特权 `EXEC` 模式下，根据以下步骤为特权 `EXEC` 访问和网络服务指定 `TACACS+` 授权：

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置接入点，为所有网络相关服务请求执行管理员 TACACS+ 授权。

   ```
   aaa authorization network tacacs+
   ```

3. 配置接入点执行管理员 TACACS+ 授权，以确定管理员是否有特权 EXEC 访问权限。

   `exec` 关键字可返回用户配置文件信息 (例如， `autocommand` 信息)。

   ```
   aaa authorization exec tacacs+
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要禁用授权，使用 `no aaa authorization {network | exec} method1` 全局配置命令。

启动 TACACS+ 结算

AAA 结算功能可追踪管理员访问的服务以及他们所消耗的网络资源量。启用 AAA 结算后，接入点以结算记录的方式向 TACACS+ 安全服务器报告管理员活动。每个结算记录包括结算属性值 (AV) 对，并存储在安全服务器上。该数据随后可用于网络管理、客户端计费或审计。

在特权 EXEC 模式下，根据以下步骤为各个思科 IOS 特权级别和网络服务启用 TACACS+ 结算。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 为所有网络相关服务请求启用 TACACS+ 结算。

   ```
   aaa accounting network start-stop tacacs+
   ```

3. 启用 TACACS+ 结算时，将在特权 EXEC 过程开始时发送开始记录结算通知，在结束时发出停止记录通知。

   ```
   aaa accounting exec start-stop tacacs+
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要禁用结算，使用 `no aaa accounting {network | exec} {start-stop}` *method1...* 全局配置命令。

显示 TACACS+ 配置

要显示 TACACS+ 服务器统计数据，可使用 `show tacacs` 特权 EXEC 命令。

备注：

配置 VLAN

本章通过以下几节介绍了如何配置接入点，使其根据有线局域网上的 VLAN 设置运行：

VLAN

VLAN 是一种按功能、项目团队或应用进行逻辑分段的交换网络，而不是根据物理或地理位置来分段。例如，特定工作组团队使用的所有工作站和服务器都可连接到相同的 VLAN，不管它们以何种物理连接方式连接到网络，或者它们是否可与其他团队组合。您可使用 VLAN 通过软件来重新配置网络，而不需要实际插拔及移动设备或接线。

可将 VLAN 视为存在于定义的交换机组内的广播域。 VLAN 由通过一个桥接域连接的多个终端系统 (主机或网络设备 (如网桥和路由器) 组成。各类网络设备均支持桥接域，例如，在自身与每个 VLAN 的独立组之间运行桥接协议的局域网交换机。

VLAN 提供局域网配置中通常由路由器提供的分段服务。 VLAN 负责处理可扩展性、安全和网络管理。在设计和构建交换式局域网网络时，需要考虑几个关键问题：

- LAN 分段
- 安全性
- 广播控制
- 性能
- 网络管理
- VLAN 之间的通信

您可通过向接入点添加 IEEE 802.11Q 标签识别，将 VLAN 扩展到无线 LAN。发向不同 VLAN 的帧将通过具有不同加密密钥的不同 SSID 上的无线接入点 / 工作组网桥进行传输。只有与该 VLAN 关联的客户端会接收那些数据包。反之，在被转发到有线网络之前，来自与某个 VLAN 关联的客户端的数据包将进行 802.11Q 标记。

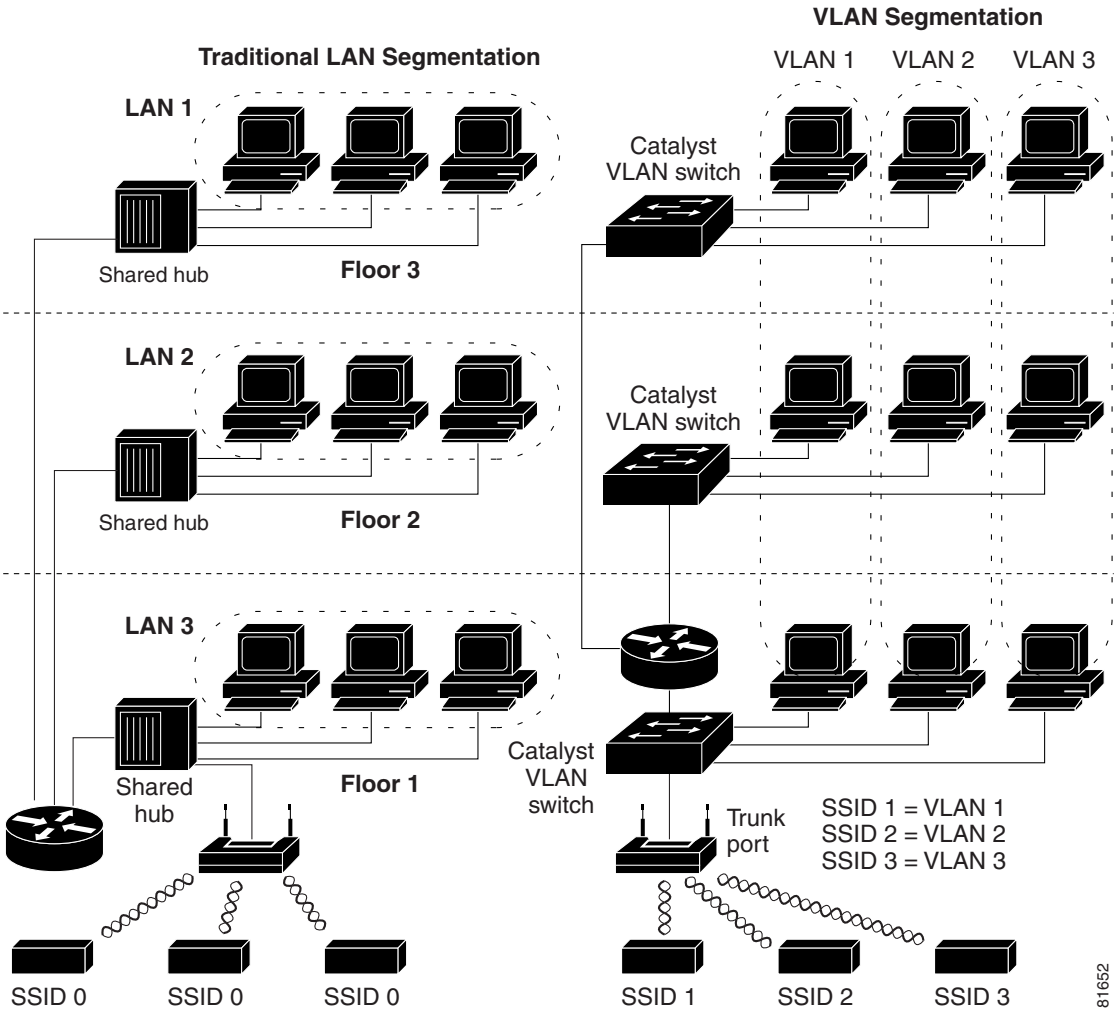
如果在接入点的千兆以太网接口上配置了 802.1q，即使未在接入点上定义 VLAN1，接入点仍将始终在 VLAN1 上发送保持激活信号。因此，以太网交换机连接到接入点并生成警告消息。接入点和交换机上不丢失功能。但交换机日志将包含无意义的消息，它们可能淹没更重要的消息，使其被忽视。

当接入点上的所有 SSID 都关联到移动网络时，该行为会造成一些问题。如果所有 SSID 都关联到移动网络，接入点所连接的以太网交换机端口会被配置为接入端口。接入端口通常被分配到接入点的本征 VLAN，但它不一定是 VLAN1，这会导致以太网交换机生成警告消息，声称是从接入点发送了带 802.1q 标签的流量。

您可禁用保持激活功能，避免交换机产生过量的消息。

下图显示了传统物理局域网分段与连接无线设备的逻辑 VLAN 分段之间的差异。

图 115 - LAN 分段与包含无线设备的 VLAN 分段



将无线设备并入 VLAN

VLAN 的基本无线组件由接入点以及使用无线技术关联到接入点的客户端组成。接入点通过干线端口以物理方式连接到网络 VLAN 交换机 (VLAN 在此配置)。到 VLAN 交换机的物理连接经由接入点的以太网端口实现。

从根本上说，配置接入点连接到特定 VLAN 的关键在于 —— 配置其 SSID 识别该 VLAN。由于 VLAN 是通过 VLAN ID 或名称进行标识，因此，如果接入点上的 SSID 被配置为识别特定的 VLAN ID 或名称，则将建立到 VLAN 的连接。当该连接建立后，具有相同 SSID 的已关联无线客户端设备便可通过接入点访问 VLAN。 VLAN 处理与客户端之间往来数据的方式与其处理有线连接往来数据的方式相同。您可在接入点上最多配置 16 个 SSID，因此最多可支持 16 个 VLAN。但您只能将一个 SSID 分配给 VLAN。

您可使用 VLAN 功能更加灵活高效地部署无线设备。例如，一个接入点可处理网络访问方式和权限各异的多名用户的特定要求。如果没有 VLAN 功能，则必须根据分配给用户的访问方式和权限部署多个接入点，从而服务不用类别的用户。

以下是两种常见的无线 VLAN 部署策略：

- 按用户组分段：将无线局域网用户社区分段，强制每个用户组使用不同的安全策略。

  例如，您可在企业环境中创建三个有线和无线 VLAN，可供全职员工、兼职员工和访客访问。

- 按设备类型分段：将无线局域网分段，允许安全机制各异的不同设备加入网络。

  例如，一些无线用户拥有仅支持 WPA2-PSK (预共享密钥) 的手持设备，还有一些无线用户拥有使用 802.1x 和 EAP 方法的高级设备。您可将这些设备分组，将它们隔离在独立的 VLAN 中。

  提示 您无法在中继器接入点上配置多个 VLAN。中继器接入点仅支持本征 VLAN。

配置 VLAN

当在接入点上配置 VLAN 时，本征 VLAN 必须是 VLAN1。

配置接入点支持 VLAN 只需三步。

1. 在无线和以太网端口启用 VLAN。
2. 将 SSID 分配给 VLAN。
3. 为 SSID 分配验证设置。

将 SSID 分配给 VLAN。

本节介绍了如何将 SSID 分配给 VLAN 以及如何在接入点的无线电和以太网端口上启用 VLAN。

- 关于为 SSID 分配验证类型的详细说明，请参见第 335 页的 “ 配置验证类型 ”
- 关于为 SSID 分配其他设置的说明，请参见第 289 页的 “ 配置多个 SSID”。

由于最多可在接入点上配置 16 个 SSID， LAN 上最多支持配置 16 个 VLAN。但对于大多数部署而言，建议创建的 SSID / VLAN 数不要超过三个，以降低系统开销。

在特权 EXEC 模式下，根据以下步骤将 SSID 分配给 VLAN，并在接入点的无线电和以太网端口上启用 VLAN。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 创建一个 SSID，然后进入新 SSID 的 SSID 配置模式。

   SSID 最多可包含 32 个字母数字字符。 SSID 区分大小写。

   SSID 最多可包含 32 个区分大小写的字母数字字符。第一个字符不得包含下列字符：
   - 感叹号 (!)
   - 井号 (#)
   - 分号 (;)

   下列字符无效，不得用于 SSID 中：
   - 加号 (+)
   - 右方括号 (])
   - 斜杠 (/)
   - 引号 (")

- TAB
- 末尾空格

提示　您可使用 ssid 命令的验证选项为每个 SSID 配置验证类型。

关于配置验证类型的说明，请参见第 335 页的“配置验证类型”。

```
dot11 ssid ssid-string
```

3. (可选) 将 SSID 分配给用户网络上的 VLAN。

   使用 SSID 关联的客户端设备将被分组到该 VLAN 中。输入 1...4095 之间的 VLAN ID。但您只能将一个 SSID 分配给 VLAN。

   提示　如果您的网络使用 VLAN 名称，您还可将名称分配给接入点上的 VLAN。

   有关说明，请参见第 415 页的“将名称分配给 VLAN”。

   ```
   vlan vlan-id
   ```

4. 返回到无线接口的接口配置模式。

   ```
   exit
   ```

5. 进入无线 VLAN 子接口的接口配置模式。

   ```
   interface dot11radio 0.x | 1.x
   ```

   其中， x 是 VLAN 编号

6. 启用无线电接口的 VLAN。

   (可选) 将 VLAN 指定为本征 VLAN。在许多网络中，本征 VLAN 为 VLAN 1。

   ```
   encapsulation dot1q vlan-id [native]
   ```

7. 返回到全局配置模式。

   ```
   exit
   ```

8. 进入以太网 VLAN 子接口的接口配置模式。

   ```
   interface gigabitEthernet0.x
   ```

9. 启用以太网接口的 VLAN。

   (可选) 将 VLAN 指定为本征 VLAN。在许多网络中，本征 VLAN 为 VLAN 1。

   ```
   encapsulation dot1q vlan-id [native]
   ```

10. 返回到特权 EXEC 模式。

    ```
    end
    ```

11. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

本例显示了如何：

a. 命名 SSID。

b. 将 SSID 分配给一个 VLAN。

c. 在无线电和以太网端口上启用 VLAN 作为本征 VLAN。

```
ap1200Router# configure terminal
ap1200Router(config)# interface dot11radio0
ap1200Router(config-if)# ssid batman
ap1200Router(config-if)# exit
ap1200Router(config)# dot11 ssid batman
ap1200Router(config-ssid)# vlan 1
ap1200Router(config-ssid)# exit
ap1200Router(config)# interface dot11radio0.1
ap1200Router(config-subif)# encapsulation dot1q 1
native
ap1200Router(config-subif)# exit
ap1200Router(config)# interface gigabitEthernet0.1
ap1200Router(config-subif)# encapsulation dot1q 1
native
ap1200Router(config-subif)# exit
ap1200Router(config)# end
```

将名称分配给 VLAN

除了数字 ID，您还可向 VLAN 分配一个名称。VLAN 名称最多可包含 32 个 ASCII 字符。接入点将使用表格保存各 VLAN 名称和 ID 对。

VLAN 名称使用准则

使用 VLAN 名称时，请遵循以下准则：

- 由于从 VLAN 名称到 VLAN ID 的映射操作对每个接入点而言都在本地，因此在整个网络中，您可将相同的 VLAN 名称分配给不同的 VLAN ID。

  提示 如果无线局域网上的客户端要求无缝漫游，我们建议为所有接入点的 VLAN ID 分配相同的 VLAN 名称，或者只使用无名称的 VLAN ID。

- 在您的接入点上配置的每个 VLAN 都必须拥有一个 ID，但 VLAN 名称却是可选的。

- VLAN 名称最多可包含 32 个 ASCII 字符。但是， VLAN 名称不能是 1...4095 之间的数字。例如， *vlan4095* 是一个有效的 VLAN 名称，但 *4095* 不是。接入点将数字 1...4095 预留用于 VLAN ID。

创建VLAN 名称

在特权 EXEC 模式下，根据以下步骤向 VLAN 分配名称。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 向 VLAN ID 分配 VLAN 名称。名称最多可包含 32 个 ASCII 字符。

   ```
   dot11 vlan-name name vlan vlan-id
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

使用命令的 `no` 格式删除 VLAN 的名称。使用 `show dot11 vlan-name` 特权 EXEC 命令列出接入点上配置的所有 VLAN 名称和 ID 对。

使用 RADIUS 服务器向 VLAN 分配用户

当进行网络验证时，您可通过配置 RADIUS 验证服务器将用户或用户组分配给特定 VLAN。

在 WPA 信息元素中分发 (并在 802.11 关联期间协商) 的单播和多播密文组可能与明确分配的 VLAN 中支持的密文组不匹配。如果 RADIUS 服务器分配新的 VLAN ID，而 VLAN ID 使用的密文组不同于之前协商的密文组，则接入点和客户端将无法切换回新的密文组。当前，WPA 和 CCKM 协议不允许在初次 802.11 密文协商阶段后更改密文组。否则，客户端设备将从无线局域网中断开。

VLAN 映射过程由以下步骤组成。

1. 客户端设备使用在接入点上配置的任何 SSID 关联至接入点。
2. 客户端开始 RADIUS 验证。
3. 当客户端成功验证后， RADIUS 服务器将客户端映射到特定的 VLAN，与为客户正在接入点上使用的 SSID 定义的 VLAN 映射无关。如果服务器没有返回客户端的任何 VLAN 属性，客户端将被分配到由在接入点上本地映射的 SSID 指定的 VLAN 上。

这些都是用于 vlan-id 分配的 RADIUS 用户属性。每个属性都必须具有介于 1...31 之间的公共标签值，以确定分组关系。

- IETF 64 (隧道类型)：将该属性设置为 VLAN。
- IETF 65 (隧道介质类型)：将该属性设置为 802。
- IETF 81 (隧道私人组 ID)：将该属性设置为 vlan-id。

查看在接入点上配置的 VLAN

在特权 EXEC 模式下，可使用 `show vlan` 命令查看接入点支持的 VLAN。这是运行 `show vlan` 命令所得的示例输出：

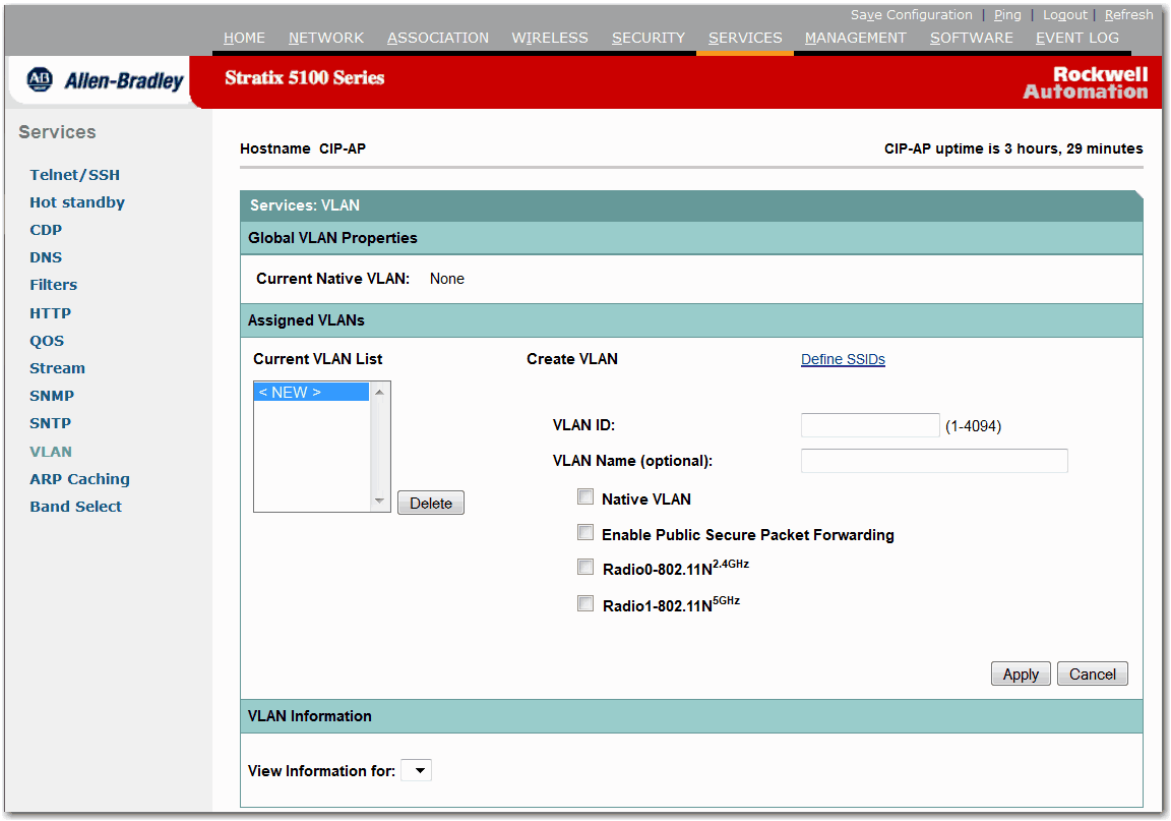
```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)


   vLAN Trunk Interfaces:  Dot11Radio0
GigabitEthernet0
Virtual-Dot11Radio0


 This is configured as native Vlan for the
following interface(s) :
Dot11Radio0
GigabitEthernet0
Virtual-Dot11Radio0
Protocols Configured:   Address:            Received:       Transmitted:
       Bridging       Bridge Group 1           201688                 0
       Bridging       Bridge Group 1           201688                 0
       Bridging       Bridge Group 1           201688                 0


Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)


   vLAN Trunk Interfaces:  Dot11Radio0.2
GigabitEthernet0.2
Virtual-Dot11Radio0.2
Protocols Configured:   Address:            Received:       Transmitted:
```

使用 Stratix 5100 设备管理器配置和启用带 SSID 的 VLAN

默认 VLAN 是管理 VLAN，所有未标记的帧均与该默认 VLAN ID 隐式关联。将您的其中一个 VLAN 配置为本征。

完成以下步骤配置 VLAN。

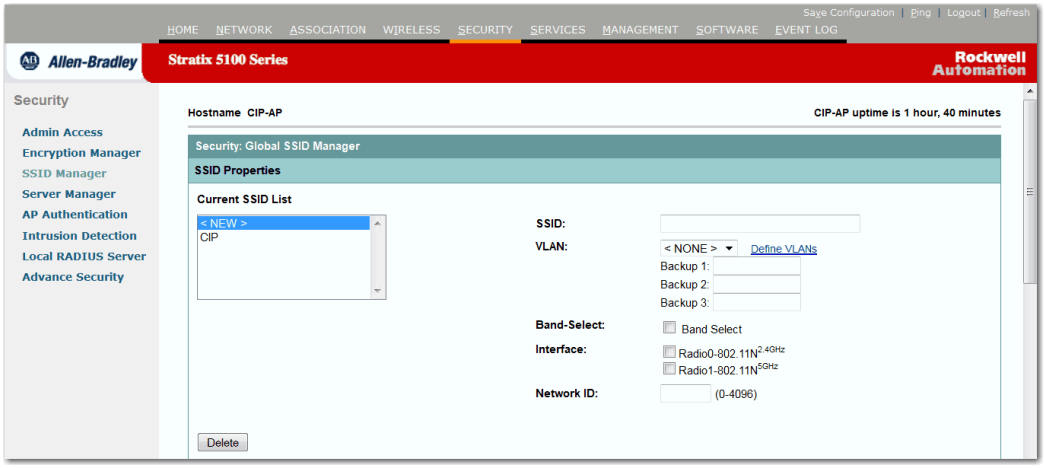
1. 从 Services (服务) 菜单中选择 Services (服务)。
2. 单击 VLAN。



3. 输入介于 1...4095 之间的唯一 VLAN ID 编号。
4. 确定您是否希望该 VLAN ID 成为本征 VLAN。
5. 单击与该 VLAN ID 关联的无线电装置。
6. 单击 Apply (应用)。

   如果不单击 Apply (应用)，新的 VLAN 便将不会保存，在 SSID 页面上也不会看到它。

7. 单击 Define SSID (定义 SSID) 链接跳转到 SSID Manager (SSID 管理器) 页面。



8. 选择要与该 VLAN 映射的唯一 SSID。

   如果没有可用的唯一 SSID，请选择新的设置并创建新的 SSID。

9. 从列表中选择 VLAN 编号，以与唯一 SSID 进行关联。

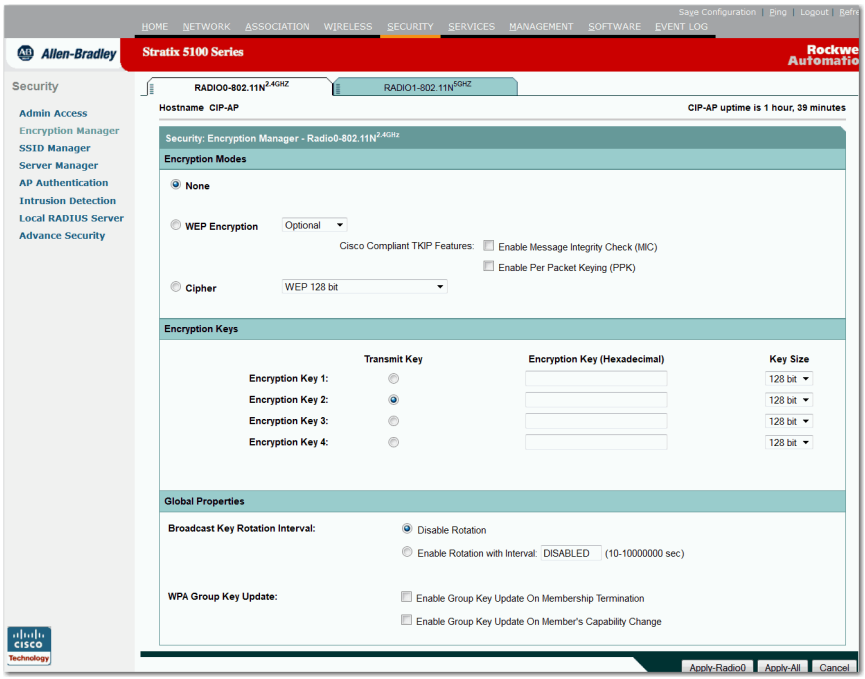
10. 单击 Apply (应用) 以保存配置。

设置 VLAN 的加密方式

现在，您已完成 VLAN 的配置，您必须设置 VLAN 的加密方式。完成以下步骤设置 VLAN 的加密方式。

1. 单击 Security (安全) 跳转到 Security Summary (安全概要) 页面。
2. 从 Security (安全) 菜单中选择 Encryption Manager (加密管理器)。

   显示 Encryption Manager (加密管理器) 页面。



3. 从 Set Encryption Mode and Keys for VLAN (设置 VLAN 的加密模式和密钥) 下拉列表中选择您正在配置的 VLAN。

   提示　该 VLAN 下拉列表仅在启用 VLAN 后才会显示。如果不存在 VLAN，则加密设置应用于所有 SSID。

4. 在 Encryption Mode (加密模式) 区域，确定当无线客户端与接入点通信时需要采取何种加密模式 (如有的话)。

重要事项　为确保最高安全级别，建议使用 AES CCMP。

5. 单击 Apply (应用)。

配置 QoS

本章描述了如何配置接入点上的服务质量 (QoS)。通过此功能，可在牺牲其他流量的条件下优先处理某些流量。在不使用 QoS 时，接入点为每个数据包 (无论数据包的内容和大小) 提供尽力服务。它发送数据包时不提供关于可靠性、延迟界限或吞吐量的任何保证。

重要事项 有关在本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide (思科 Aironet 接入点和网桥的思科 IOS 命令参考指南)。

无线局域网的 QoS

通常，网络以最大流量方式工作，即所有流量的优先级均相同，被及时发送的机会均等。当发生拥塞时，所有流量被丢弃的机会相同。

在配置接入点的 QoS 时，可以选择特定的网络流量，确定其优先级，并使用拥塞管理和拥塞避免技术，提供优先处理。在无线局域网中部署 QoS 使网络性能更具可预测性，带宽利用率更高。

当配置 QoS 时，创建 QoS 策略，并将策略应用到接入点上配置的 VLAN。如果不在网络上使用 VLAN，则可将 QoS 策略应用到接入点的以太网和无线电端口。

重要事项 启用 QoS 时，接入点默认情况下使用 Wi-Fi 多媒体 (WMM) 模式。有关 WMM 的信息，请参见第 429 页的 “Wi-Fi 多媒体模式 ”。

无线局域网的 QoS 与有线局域网的 QoS 的比较

无线局域网的 QoS 部署与其他思科设备的 QoS 部署不一样。在启用 QoS 时，接入点执行以下操作：

- 不对数据包进行分类；它们根据 DSCP 值、客户端类型 (例如无线电话) 或 802.1q 或 802.1p 标签中的优先级值确定数据包的优先级。
- 不构建内部 DSCP 值；它们仅支持通过将 IP DSCP、优先级或协议值分配给 2 层 CoS 值完成映射。
- 仅在无线电出站端口上执行类似排队的 EDCF。
- 仅在以太网出站端口上执行 FIFO 排队。
- 仅支持 MQC 策略映射设置 COS 操作。
- 当启用无线电话的 QoS 元素功能时，来自语音客户端的流量优先级高于来自其他客户端的流量优先级。
- 通过使用协议值设为 119 的级别映射 IP 协议语句支持 Spectralink 电话。

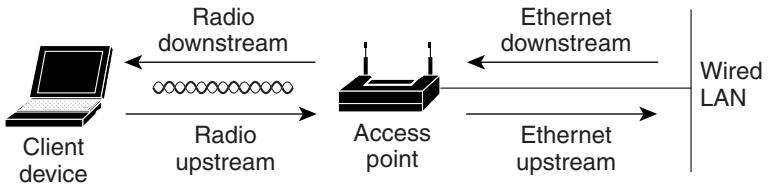
QoS 对无线局域网的影响

无线局域网的 QoS 功能是 802.11e 标准的一个子集。根据流量分类，无线局域网的 QoS 对通过 WLAN 发出的来自接入点的流量进行优先处理。

和其他介质一样，您无法觉察到 QoS 对轻载无线局域网的影响。随着无线局域网上的负载增多， QoS 的优势越来越明显，它能将选定流量类型的延迟、抖动和丢包控制在可接受的范围内。

无线局域网的 QoS 侧重于确定接入点下游设备的优先级。下图显示了上游和下游通信流量。

图 116 - 上游和下游通信流量



- 无线电下游流量是从接入点发送至无线客户端设备的流量。此流量是无线局域网上 QoS 的关注目标。
- 无线电上游流量是从无线电客户端设备发送至接入点的流量。无线局域网的 QoS 不影响此流量。
- 以太网下游流量是从交换机或路由器发送至接入点的以太网端口的流量。如果在交换机或路由器上启用了 QoS，交换机或路由器会优先处理发送至接入点的流量，并限制其速率。
- 以太网上游流量是从接入点以太网端口发送至有线局域网上的交换机或路由器的流量。根据流量分类，接入点不对发送至有线局域网的流量优先处理。

QoS 设置的优先级

启用 QoS 时，接入点根据每个数据包的 2 层服务级别值对数据包进行排队。接入点在此顺序中应用 QoS 策略。

数据包已分类

当接入点收到来自启用了 QoS 的交换机或路由器的已分类数据包时，它们将数据包分为非零 802.1Q/P user_priority 值，接入点使用此分类，且不对数据包应用其他 QoS 策略规则。现有的分类优先级高于接入点上的所有其他策略。

重要事项	即使尚未配置 QoS 策略，接入点总是接受通过无线电接口接收的已标记 802.1P 的数据包。

无线电话的QoS 元素设置

如果启用了无线电话的 QoS 元素设置，则为一些无线电话供应商的客户端创建动态语音分类器，可以让无线电话流量的优先级高于其他客户端的流量。此外，还将启用 QoS 基本服务集 (QBSS)，以推广信标和探测响应帧中的通道负载信息。某些 IP 电话根据流量负载使用 QBSS 元素确定要关联的接入点。

通过 Stratix 5100 设备管理器配置 QoS

以下步骤描述了如何配置接入点的服务质量 (QoS)。通过此功能，可在牺牲其他流量的条件下对某些流量进行优先处理。在不使用 QoS 时，接入点为每个数据包 (无论数据包的内容和大小) 提供尽力服务。

通常，网络以最大流量方式工作，即所有流量的优先级均等，被及时发送的机会相等。当发生拥塞时，所有流量被丢弃的机会相同。

在配置接入点的 QoS 时，可以选择特定的网络流量，根据其相对重要性确定其优先级，并使用拥塞管理和拥塞避免技术，提供优先处理。在无线局域网中部署 QoS 使网络性能更具可预测性，带宽利用率更高。

当配置 QoS 时，创建 QoS 策略，并将策略应用到接入点上配置的 VLAN。如果不在网络上使用 VLAN，则可将 QoS 策略应用到接入点的以太网和无线电端口。

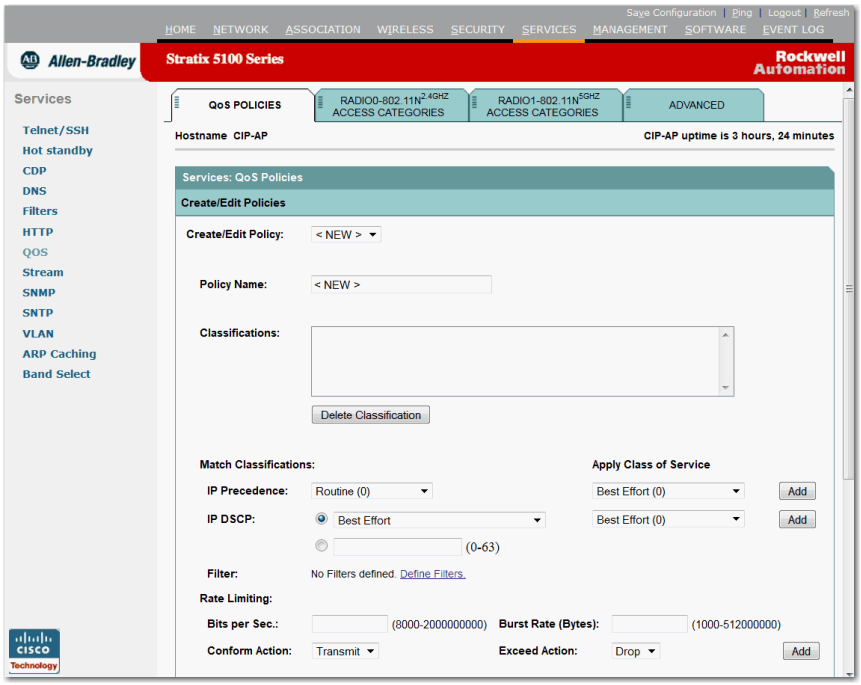
默认情况下禁用 QoS。配置接入点的 QoS 之前，请牢记以下信息：

- 部署 QoS 的最重要准则就是熟悉无线局域网上的流量。如果您知道无线客户端设备使用的各个应用，这些应用对延迟的敏感度以及与这些应用有关的流量，您可配置 QoS 来提高性能。
- QoS 不会为无线局域网创建附加的带宽；它帮助控制带宽的分配。如果您的无线局域网的带宽十分充裕，则可能无需配置 QoS。

重要事项	如果在无线局域网上使用 VLAN，确保在配置 QoS 之前在接入点上配置了所需的 VLAN。

按以下步骤配置接入点的 QoS。

1. 从顶部菜单中单击 Services (服务)。
2. 从 Services (服务) 菜单中单击 QoS。



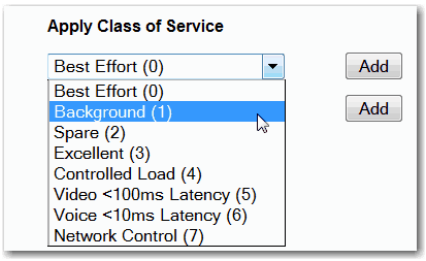
3. 选择 <NEW> Create/Edit Policy (< 新建 > 创建 / 编辑策略) 域，或选择一个现有的策略。
4. 在 Policy Name (策略名称) 输入域中输入 QoS 策略的名称。

   名称最多包含 25 个字母数字字符。不得在策略名称中包括空格。

   如果要优先处理的数据包在 IP header TOS (IP 报头 TOS) 域中包含 IP 优先级信息，从 IP Precedence (IP 优先级) 下拉菜单中选择一个 IP 优先级分类。菜单选项包括以下条目：

   - Routine (例程)(0)
   - Priority (优先级)(1)
   - Immediate (立即)(2)
   - Flash (快速)(3)
   - Flash Override (快速覆盖)(4)
   - Critic/CCP (5)
   - Internet Control (因特网控制)(6)
   - Network Control (网络控制)(7)

5. 从 Apply Class of Service (应用服务级别) 下拉菜单中，选择希望接入点为从 IP Precedence (IP 优先级) 菜单中所选类型的数据包应用的服务级别。



6. 接入点将 IP Precedence (IP 优先级) 选项与服务级别选项进行匹配。

Apply Class of Service (应用服务级别) 菜单中有以下设置：

- Best Effort (尽力服务)(0)
- Background (后台)(1)
- Spare (备用)(2)
- Excellent (出色)(3)
- Control Lead (控制超前)(4)
- Video <100 ms Latency (视频 <100 ms 延迟)(5)
- Voice <100 ms Latency (语音 <100 ms 延迟)(6)
- Network Control (网络控制)(7)

7. 单击 IP Precedence (IP 优先级) 的 Class of Service (服务级别) 菜单旁的 Add (添加)。

在 Classifications (分类) 域中显示分类。要删除一种分类，选择该分类，然后单击 Classifications (分类) 域旁的 Delete (删除)。

如果要优先处理的数据包在 IP header TOS (IP 报头 TOS) 域中包含 IP DSCP 优先级信息，从 IP DSCP 下拉菜单中选择一个 IP DSCP 分类。以下是菜单选项：

- Best Effort (尽力服务)
- Assured Forwarding - Class 1 Low (保证转发 —— 级别 1 低)
- Assured Forwarding - Class 1 Medium (保证转发 —— 级别 1 中)
- Assured Forwarding - Class 1 High (保证转发 —— 级别 1 高)
- Assured Forwarding - Class 2 Low (保证转发 —— 级别 2 低)
- Assured Forwarding - Class 2 Medium (保证转发 —— 级别 2 中)
- Assured Forwarding - Class 2 High (保证转发 —— 级别 2 高)
- Assured Forwarding - Class 3 Low (保证转发 —— 级别 3 低)
- Assured Forwarding - Class 3 Medium (保证转发 —— 级别 3 中)
- Assured Forwarding - Class 3 High (保证转发 —— 级别 3 高)
- Assured Forwarding - Class 4 Low (保证转发 —— 级别 4 低)

- Assured Forwarding - Class 4 Medium (保证转发 —— 级别 4 中)
- Assured Forwarding - Class 4 High (保证转发 —— 级别 4 高)
- Class Selector 1 (级别选择器 1)
- Class Selector 2 (级别选择器 2)
- Class Selector 3 (级别选择器 3)
- Class Selector 4 (级别选择器 4)
- Class Selector 5 (级别选择器 5)
- Class Selector 6 (级别选择器 6)
- Class Selector 7 (级别选择器 7)
- Expedited Forwarding (加速转发)

8. 从 Apply Class of Service (应用服务级别) 下拉菜单中，选择希望接入点为从 IP DSCP 菜单中所选类型的数据包应用的服务级别。

   接入点将 IP DSCP 选项与服务级别选项进行匹配。

9. 单击 IP DSCP 的 Class of Service (服务级别) 菜单旁的 Add (添加)。

   在 Classifications (分类) 域中显示分类。

   如果需要在无线局域网上优先处理来自 Spectralink 电话 (IP 协议 119) 的数据包，使用 Apply Class of Service (应用服务级别)。选择希望接入点应用到 Spectralink 电话数据包的服务级别。接入点将 Spectralink 电话数据包与服务级别选项进行匹配。

10. 单击 IP Protocol 119 (IP 协议 119) 的 Class of Service (服务级别) 菜单旁的 Add (添加)。

    在 Classifications (分类) 域中显示分类。

    如果要对 VLAN 上的所有数据包设置默认分类，使用 Apply Class of Service (应用服务级别) 选择希望接入点应用到 VLAN 上的所有数据包的服务级别。接入点将所有数据包与服务级别选项进行匹配。

11. 对 VLAN 上的数据包单击 Default classification (默认分类) 的 Class of Service (服务级别) 菜单旁的 Add (添加)。

    在 Classifications (分类) 域中显示分类。

12. 将分类添加到策略完成后，单击 Apply Class of Service (应用服务级别) 下拉菜单中的 Apply (应用)。
    - 要取消策略，将所有域复位到默认值，单击 Apply Class of Service (应用服务级别) 下拉菜单下的 Cancel (取消)。
    - 要删除整个策略，单击 Apply Class of Service (应用服务级别) 下拉菜单下的 Delete (删除)。

13. 使用 Apply Policies to Interface/VLANs (将策略应用于接口 / VLAN) 下拉菜单将策略应用于接入点以太网和无线电接口。
    - 如果在接入点上配置了 VLAN，在此区域显示每个 VLAN 虚拟端口的下拉菜单。
    - 如果未在接入点上配置 VLAN，显示每个接口的下拉菜单。
14. 单击页面底部的 Apply (应用)，将策略应用于接入点端口。

    如果希望接入点优先处理所有语音数据包，而与 VLAN 无关，则单击 Advanced (高级) 选项卡。

可使用思科 IOS 命令 `dot11 phone dot11e` 允许支持标准 QBSS 负载 IE。

本例显示了如何允许 IEEE 802.11 电话支持传统 QBSS 负载元件：

```
AP(config)# dot11 phone
```

本例显示了如何允许 IEEE 802.11 电话支持标准 (IEEE 802.11e) QBSS 负载元件：

```
AP(config)# dot11 phone dot11e
```

本例显示了如何停止或禁止 IEEE 802.11 电话支持：

```
AP(config)# no dot11 phone
```

15. 在接入点上创建的策略 —— 创建并应用于 VLAN 或接入点接口的 QoS 策略优先级为第三，排在已分类数据包和 QoS Element for Wireless Phones (无线电话的 QoS 元素) 设置之后。
16. VLAN 上所有数据包的默认分类 —— 如果为 VLAN 上的所有数据包设置了默认分类，则该策略位于优先级列表中的第四位。

Wi-Fi 多媒体模式

启用 QoS 时，接入点默认情况下使用 Wi-Fi 多媒体 (WMM) 模式。WMM 相对于基本 QoS 模式提供以下增强功能：

- 接入点将每个数据包的服务级别添加到要传送到接收站的数据包的 802.11 报头中。
- 每个访问级别都有各自的 802.11 序号。序号允许高优先级数据包中断低优先级数据包的重试，而不会导致接收侧的重复校验缓冲区溢出。
- 根据接收器上的访问级别完成 WPA 重播检测。和 802.11 顺序编号一样， WPA 重播检测允许高优先级数据包中断低优先级重试，而不会在接收侧发送重播信号。
- 对于配置为允许的访问级别，允许有资格通过正常退避程序执行发送的发射器在所配置的发送机会 (指定的微秒数) 期间发送一组待处理的数据包。发送一组待处理的数据包可提高吞吐量，因为每个数据包无需等待退避来获得访问；相反，可立即依次发送数据包。
- 启用 U-APSD Power Save (U-APSD 节能)。

接入点使用发送至支持 WMM 的客户端设备的数据包中的 WMM 增强功能。接入点对发送至不支持 WMM 的客户端的数据包应用基本 QoS 策略。

通过 CLI 使用 no dot11 qos mode wmm 配置接口命令禁用 WMM。要通过 web 浏览器界面禁用 WMM，取消选中 QoS Advanced (QoS 高级) 页上无线电接口的复选框。

IGMP 监听

当在交换机上启用了因特网组成员协议 (IGMP) 监听，且客户端从一个接入点漫游到另一个接入点时，将丢弃客户端的多播会话。当启用了接入点的 IGMP 监听助手时，接入点将一个通用查询发送至无线局域网，提示客户端发送 IGMP 成员报告。当网络基础设施接收到主机的 IGMP 成员报告时，它确保发送主机的多播数据流。

默认情况下启用 IGMP 监听助手。要禁止该助手，浏览到 QoS Policies - Advanced (QoS 策略 —— 高级) 页面，选中 Disable (禁止)，然后单击 Apply (应用)。

重要事项　如果没有多播路由器用于处理来自主机的 IGMP 查询和应答，则禁止在接入点上配置 IGMP 监听。当启用 IGMP 监听时，所有多播组通信必须发送 IGMP 查询和应答数据包。如果没有检测到 IGMP 查询或应答数据包，则丢弃该组的所有多播通信。

AVVID 优先级映射

AVVID 优先级映射功能映射标记为服务级别 5 到服务级别 6 的以太网数据包。此功能允许接入点将正确的优先级应用于语音数据包，从而与思科 AVVID 网络兼容。

默认情况下启用 AVVID 优先级映射。要禁止映射，浏览到 QoS Policies - Advanced (QoS 策略 —— 高级) 页面，选择 No for Map Ethernet Packets with CoS 5 to CoS 6 (对 CoS 5 到 CoS 6 的数据包不执行映射)，然后单击 Apply (应用)。

WiFi 多媒体 (WMM)

通过使用 Admission Control (准入控制) 复选框，可启用接入点无线电接口上的 WMM。当启用准入控制时，与接入点关联的客户端必须完成 WMM 准入控制步骤，然后才能使用该接入类别。

速率限制

速率限制便于控制接口上发送或接收的数据流量。基于级别的策略功能执行以下功能：

- 根据用户自定义的标准，限制某类流量的输入或输出传输速率。
- 通过设置 IP 优先级值、 IP 差分服务代码点 (DSCP) 值和服务质量 (QoS) 组标记数据包。

当使用 P2MP 设置时，此功能用于限制从每个非根网桥发送至根网桥的上游流量的速率。要限制下游流量的速率，在根侧路由器 / 交换机上应用级别映射。

重要事项　仅对以太网入口应用速率限制。

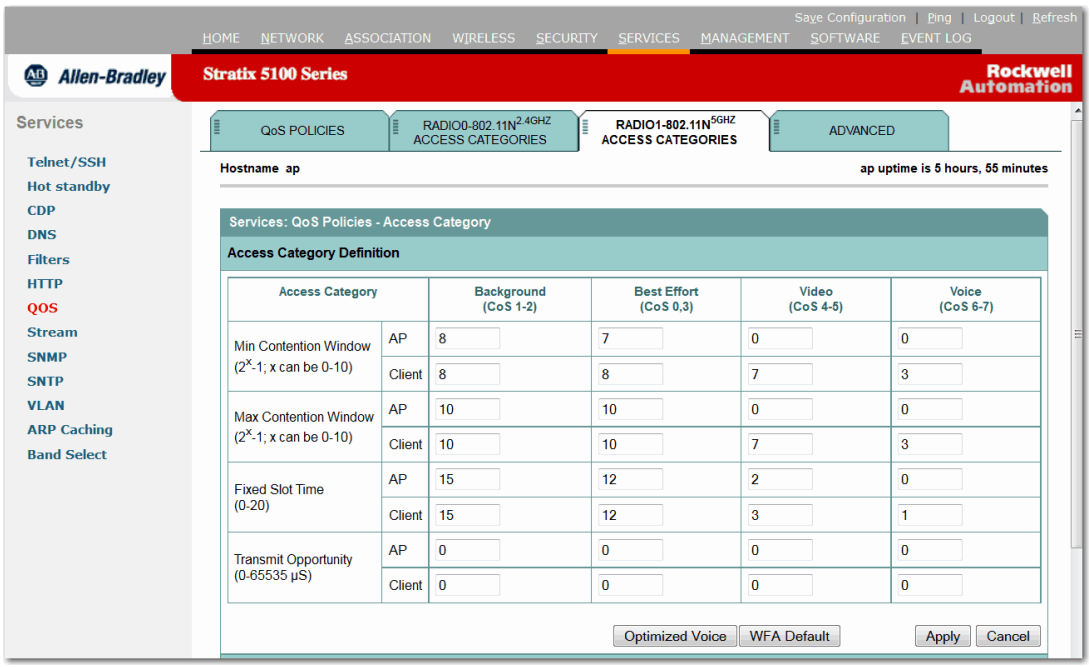
调节无线电接入类别

接入点使用无线电接入类别来计算每个数据包的退避时间。通常，高优先级数据包的退避时间较短。

Min and Max Contention (最小和最大争用值) 页面上各域及 Slot Time (时隙) 域中的默认值基于 IEEE 标准 802.11e 推荐的设置。有关这些值的详细信息，请参见标准。 Stratix 5100 接入点预配置了适用于工业控制流量的最优值。

下图显示了 Radio Access Categories (无线电接入类别) 页面。双无线电接入点的每个无线电装置均有一个 Radio Access Categories (无线电接入类别) 页面。

图 117 - Radio Access Categories (无线电接入类别) 页面



配置标称速率

当接入点收到来自 WMM 客户端的 ADDTS (添加通信流量) 请求时，它根据 CLI 命令 traffic-stream 定义的标称速率检查 ADDTS 请求中的标称速率或最小 PHY 速率。如果它们不一致，则接入点拒绝 ADDTS 请求。

如果选择最优语音设置 (参见第 431 页的图 117)，则配置以下标称速率：

- 5.5 Mbps、 6.0 Mbps、 11.0 Mbps、 12.0 Mbps 和 24.0 Mbps

重要事项	上述速率很适合思科电话。第三方无线电话可使用不同的标称速率或最小 PHY 速率。您需要为这些电话启用附加标称速率。

最优语音设置

通过使用 Admission Control (准入控制) 复选框，可控制客户端对接入类别的使用。当启用了某种接入类别的准入控制时，与接入点关联的客户端必须完成 WMM 准入控制步骤，然后才能使用该接入类别。

配置呼叫准入控制

配置接入点上的呼叫准入控制 (CAC) 包含以下步骤。

1. 配置无线电。
2. 启用 SSID 上的准入控制。

根据以下步骤配置接入点无线电的准入控制。

有关使用 CLI 配置准入控制的思科 IOS 命令列表，请参见 Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide (思科 Aironet 接入点和网桥的思科 ISO 命令参考指南)。

1. 单击您想要配置的无线电装置的 Access Categories (接入类别) 页面。

第 431 页的图 117 显示了 Access Categories (接入类别) 页面的一个实例。

2. 选中 `Voice (CoS 6-7)`（**语音**）下的 `Admission Control` (准入控制)。
3. 在 `Max Channel Capacity (%)` (最大通道容量) 域中输入语音要使用的最大通道百分比。
4. 在 `Roam Channel Capacity (%)` (漫游通道容量) 域中输入漫游要使用的最大通道百分比。

从 `Max Channel Capacity (%)` (最大通道容量) 域中减去漫游呼叫所使用的通道百分比 (最高为域中的指定值)。

例如，假设在 `Max Channel Capacity (%)` (最大通道容量) 域中输入了 75%，在 `Roam Channel Capacity (%)` (漫游通道容量) 域中输入了 6%。如果漫游呼叫使用通道的 5%，则语音可使用的最大通道量为 70%。

5. 要使用视频接入类别 (AC = 2) 进行信号发布，选中 `Video (CoS 4-5)` (视频) 下的 Admission Control （准入控制）?

重要事项	在 SSID 上启用准入控制之前，所配置的准入控制设置不会生效。

启用准入控制

根据以下步骤启用 SSID 上的准入控制。

1. 打开 SSID Manager (SSID 管理器) 页面。
2. 选择一个 SSID。
3. 在 `General Settings` (常规设置) 下，在 `Call Admission Control` (呼叫准入控制) 域中选择 `Enable` (启用)。

准入控制故障排除

您可使用两个 CLI 命令来显示信息，帮助您排除准入控制问题：

- 要显示无线电装置 0 上的当前准入控制设置，输入以下命令：

  ```
  # show dot11 cac int dot11Radio 0
  ```

- 要显示无线电装置 1 上的当前准入控制设置，输入以下命令：

  ```
  # show dot11 cac int dot11Radio 1
  ```

- 要显示许可流以及准入控制和 MT 的信息，输入以下命令：

  ```
  # show dot11 traffic-streams
  ```

备注：

配置过滤器

本章描述了如何通过 Web 浏览器界面配置和管理 MAC 地址、 IP 和接入点上的以太网类型过滤器。

过滤器

协议过滤器 (IP 协议、 IP 端口和以太网类型) 阻止或允许通过接入点的以太网和无线电端口使用特定的协议。您可设置单个协议过滤器或过滤器组。您可过滤有线局域网上的无线客户端设备和 / 或用户协议。例如，无线接入点无线电端口上的 SNMP 过滤器阻止无线客户端设备使用带有该接入点的 SNMP，但不阻拦来自有线局域网的 SNMP 访问。

IP 地址和 MAC 地址过滤器允许或禁止向特定的 IP 或 MAC 地址来回转发单播和多播数据包。您可以创建一个过滤器，允许通过除指定地址外的所有地址的流量，也可阻止除指定地址外的所有地址的流量。

您可使用 Web 浏览器界面或在 CLI 中输入命令来配置过滤器。

提示

您可在接入点的 QoS 策略中包含过滤器。有关设置 QoS 策略的详细说明，请参见第 421 页的 " 配置 QoS"。

通过使用 CLI，您可配置多达 2,048 个要过滤的 MAC 地址。但是，通过使用 Web 浏览器界面，只能配置最多 43 个要过滤的 MAC 地址。

使用 CLI 命令配置过滤器

要使用 CLI 命令配置过滤器，可使用访问控制列表 (ACL) 和网桥组。

重要事项	避免同时使用 CLI 和 Web 浏览器界面来配置无线设备。如果通过 CLI 配置无线设备， Web 浏览器界面会显示配置的不准确解析。但是，不准确并不一定意味着该无线设备配置错误。例如，若使用 CLI 配置 ACL， Web 浏览器界面显示如下消息： 使用 CLI 命令在接口 Dot11Radio0 上配置了过滤器 700。必须通过 CLI 清除才能使 Web 界面正常运行。 如果您看到该消息，请使用 CLI 删除 ACL，然后使用 Web 浏览器界面重新配置它们。

创建基于时间的 ACL

基于时间的 ACL 是可在特定时间段内启用或禁用的 ACL。此功能提供了定义允许或拒绝某些流量类型的访问控制策略的稳定性和灵活性。

下例说明了如何通过 CLI 配置基于时间的 CLI，其中，在工作日的营业时间内，允许在网络内外进行 Telnet 连接：

重要事项	根据您的要求，可在 Stratix 5100 接入点的千兆以太网端口或无线电端口上定义基于时间的 ACL。该功能禁止在网桥组虚拟接口 (BVI) 上应用。

根据以下步骤创建基于时间的 ACL。

1. 通过 CLI 登录到 AP。
2. 使用控制台端口或 Telnet 通过以太网接口或无线接口访问 ACL。
3. 进入全局配置模式。
4. 创建一个时间范围。对于本例，测试：

   ```
   AP<config>#time-range Test
   ```

5. 创建一个时间范围：

   ```
   AP<config>#time-range periodic weekdays 7:00 to
   19:00
   ```

   这允许用户在工作日的 7:00...19:00 期间进行访问。

6. 创建一个 ACL。对于本例， 101：

   ```
   AP<config># ip access-list extended 101
   ```

```
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255 eq telnet time-range Test
```

重要事项 该 ACL 允许 Telnet 流量流经网络，以便进行指定的时间范围测试。它还允许在工作日将 Telnet 会话发送至 AP。

7. 将基于时间的 ACL 应用到以太网接口：

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
```

ACL 记录

AP 平台的桥接接口不支持 ACL 记录。当在桥接接口上应用时，其工作方式如同未配置记录选项，且记录功能不生效。但是，只要将一个单独的 ACL 用于 BVI 接口， ACL 记录即可完美地用于 BVI 接口。

CLI 配置示例

本例显示了与第 442 页的 “ 使用 MAC 地址 ACL 阻止或允许客户端关联到接入点 ” 中所列步骤等效的 CLI 命令。

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

在本例中，只有 MAC 地址位于访问列表 777 中的客户端设备才允许关联至接入点。接入点阻止来自所有其他 MAC 地址的关联。

有关本例中使用的命令的完整说明，请参见思科 Aironet 接入点和网桥的思科 IOS 命令参考。

通过 Stratix 5100 设备管理器配置过滤器

本章节描述了如何通过 Stratix 5100 设备管理器的 Web 浏览器界面配置和管理接入点上的 MAC 地址、 IP 和以太网类型过滤器。

完成以下两个步骤来配置和启用过滤器。

1. 使用过滤器设置页面命名和配置过滤器。
2. 启用过滤器。

有关详细的说明，请参见以下章节：

- 第 439 页的 “ 配置和启用 MAC 地址过滤器 ”
- 第 444 页的 “ 配置和启用 IP 过滤器 ”
- 第 450 页的 “ 配置和启用以太网类型过滤器 ”

配置和启用 MAC 地址过滤器

MAC 地址过滤器允许或禁止将单播和多播数据包转发给特定的 MAC 地址。您可创建一个过滤器，允许通过除指定地址外的所有 MAC 地址的流量，或者阻止除指定地址外的所有 MAC 地址的流量。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

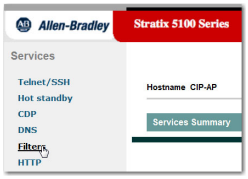
重要事项 通过使用 CLI 命令，可以配置要过滤的 MAC 地址，但由于 NVRAM 限制，当 MAC 过滤器数量超过 600 个时，您需要使用 FTP 或 TFTP。但是，通过使用 Web 浏览器界面，只能配置最多 43 个要过滤的 MAC 地址。

重要事项 MAC 地址过滤器功能强大，若设置过滤器错误，您会锁定自己，无法访问接入点。如果不小心将自己锁定导致无法访问接入点，请使用 CLI 禁用过滤器。

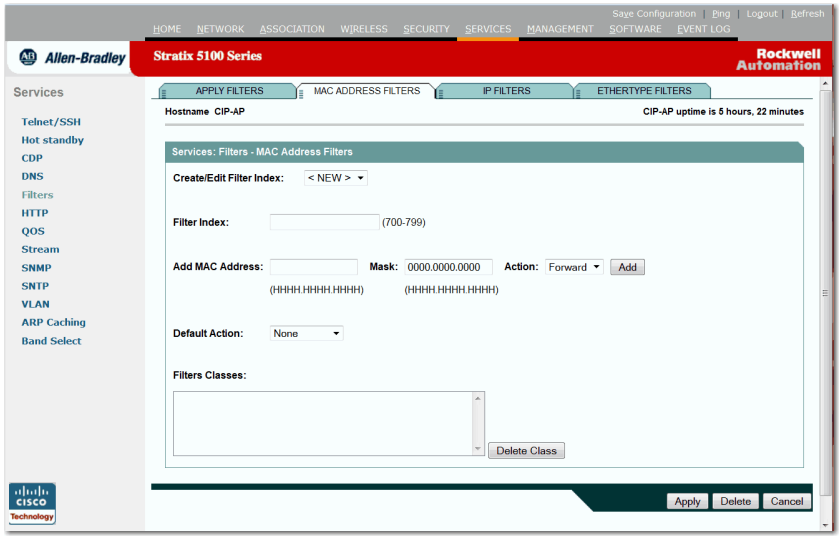
使用 MAC Address Filters (MAC 地址过滤器) 页面创建接入点的 MAC 地址过滤器。根据以下步骤创建 MAC 地址过滤器。

1. 从顶部导航菜单中单击 Services (服务)。

2. 从 Services (服务) 菜单中单击 Filters (过滤器) 转入 Services: Filters - Apply Filters (服务：过滤器 —— 应用过滤器) 页面。



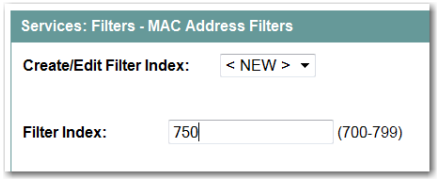
3. 在 Apply Filters (应用过滤器) 页面，单击页面顶部的 MAC Address Filters (MAC 地址过滤器) 选项卡。



如果正在创建一个新的 MAC 地址过滤器，确保在 Create/Edit Filter Index (创建 / 编辑过滤器索引) 菜单中选择了 <NEW> (默认值)。

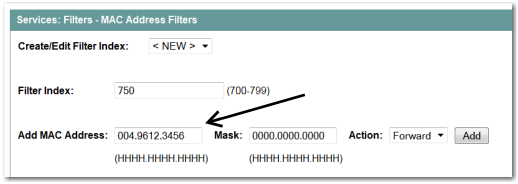
要编辑过滤器，从 Create/Edit Filter Index (创建 / 编辑过滤器索引) 菜单中选择过滤器编号。

4. 在 Filter Index (过滤器索引) 域中，用一个范围为 700...799 的数字命名过滤器。



您所分配的数字将用于创建过滤器的访问控制列表 (ACL)。

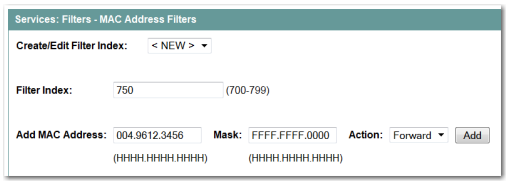
5. 在 Add MAC Address (添加 MAC 地址) 域中输入一个 MAC 地址。



输入地址，并用句点分隔三个四字符组，例如，0040.9612.3456。

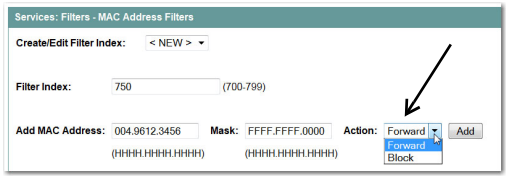
提示　如果您打算阻止除指定允许的地址外的所有 MAC 地址的通信，则将 MAC 地址置于允许的 MAC 地址列表中。

6. 使用 Mask (掩码) 输入域指示从左到右的位数，过滤器根据 MAC 地址进行检查。



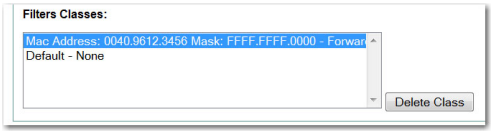
例如，要与 MAC 地址完全匹配 (用于检查所有位)，输入 FFFF.FFFF.FFFF。若仅检查前 4 个字节，输入 FFFF.FFFF.0000。

7. 从 Action (操作) 下拉菜单中选择 Forward (转发) 或 Block (阻止)。



8. 单击 Add (添加)。

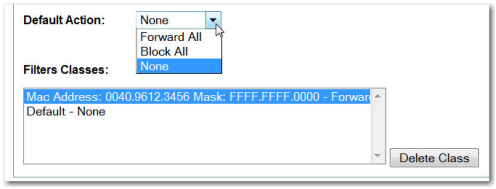
MAC 地址将显示在 Filters Classes (过滤器类别) 域中。



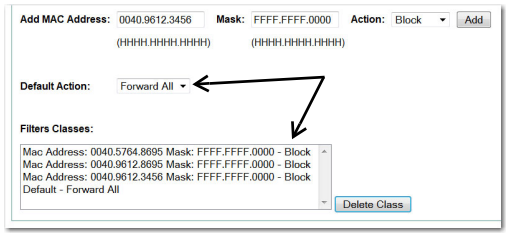
要从 Filters Classes (过滤器类别) 列表中删除 MAC 地址，选择该类别，然后单击 Delete (删除)。

9. 重复步骤 5 至步骤 8，将地址添加到过滤器中。

10. 从 Default Action (默认操作) 菜单中选择 Forward All (全部转发) 或 Block All (全部阻止)。



过滤器的默认操作必须是过滤器中至少一个地址的相反操作。



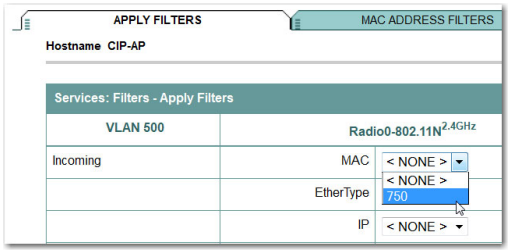
例如，如果输入多个地址并选择了 Block (阻止) 作为这些地址的操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。

11. 单击 Apply (应用)。

    过滤器在接入点上保存，但在 Apply Filters (应用过滤器) 页面上应用它们之前，过滤器不会启用。

12. 返回 Apply Filters (应用过滤器) 页面。

13. 从其中一个 MAC 下拉菜单中选择过滤器编号。



    您可将过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

14. 单击 Apply (应用)。

    在所选端口上启用过滤器。

如果没有立即过滤客户端，则单击 System Configuration (系统配置) 页面上的 Reload (重新加载) 重启接入点。要转入 System Configuration (系统配置) 页面，单击任务菜单中的 System Software (系统软件)，然后单击 System Configuration (系统配置)。

重要事项	MAC 地址被阻止的客户端设备不能通过接入点发送和接收数据，但它们作为未认证的客户端设备仍位于关联表中。当接入点停止监控它们、接入点重启动或客户端关联至另一个接入点时， MAC 地址被阻止的客户端设备从关联表中消失。

使用 MAC 地址 ACL 阻止或允许客户端关联到接入点

您可使用 MAC 地址 ACL 阻止或允许关联到接入点。您可使用 ACL 过滤与接入点无线电装置的关联，而不是过滤通过某个接口的流量。

根据以下步骤使用 ACL 过滤与接入点无线电装置的关联。

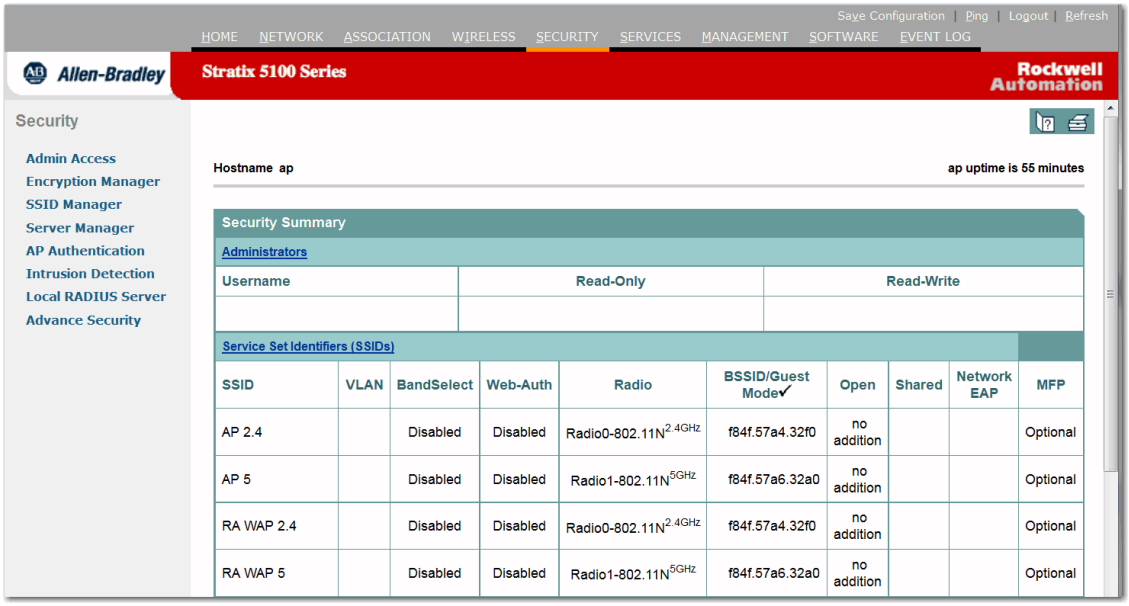
1. 执行第 439 页的 " 配置和启用 MAC 地址过滤器 " 中的步骤 1 - 10 创建 ACL。

    对于您希望允许关联的 MAC 地址，从 Action (操作) 菜单中选择 Forward (转发)。对于您希望阻止关联的地址，选择 Block (阻止)。从 Default Action (默认操作) 菜单中选择 Block All (全部阻止)。

2. 从主菜单中单击 Security (安全)。

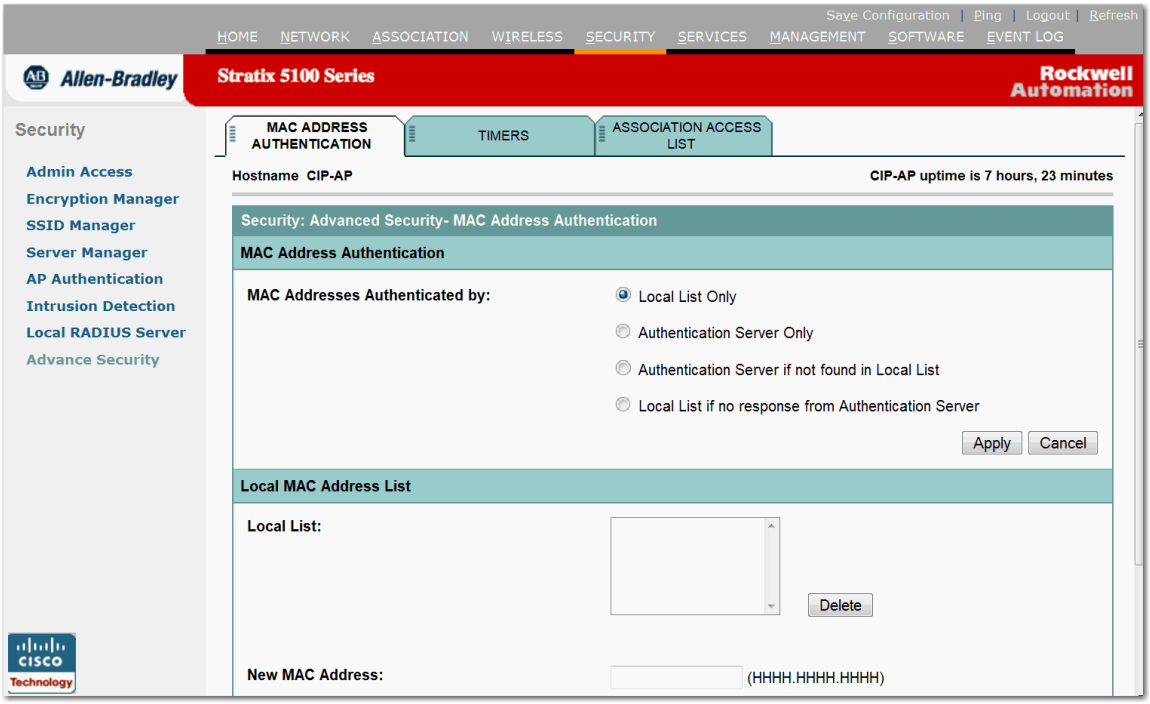
    下图显示了 Security Summary (安全概要) 页面。

图 118 - Security Summary (安全概要) 页面



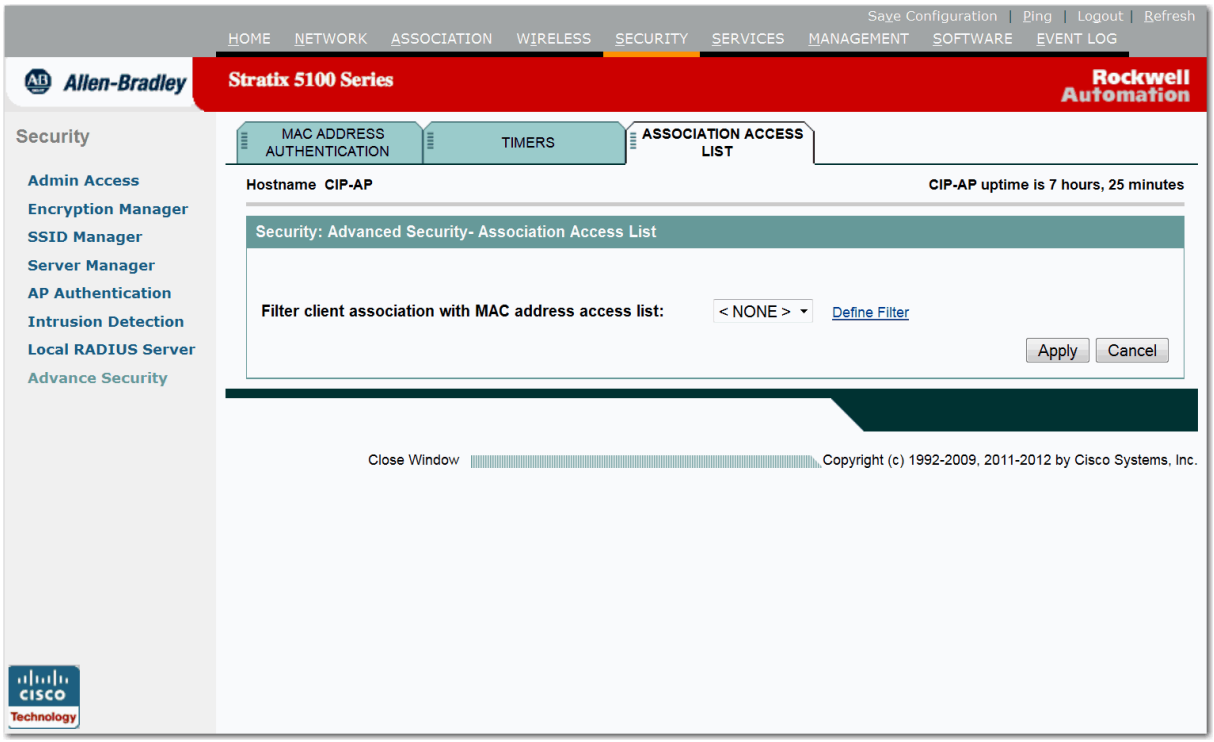
3. 单击 Advanced Security (高级安全)。

图 119 - Advanced Security: MAC Address Authentication (高级安全：MAC 地址验证) 页面



4. 单击 Association Access List (关联访问列表) 选项卡。

图 120 - Association Access List (关联访问列表) 页面



5. 从下拉菜单中选择 MAC 地址 ACL。
6. 单击 Apply (应用)。

配置和启用 IP 过滤器

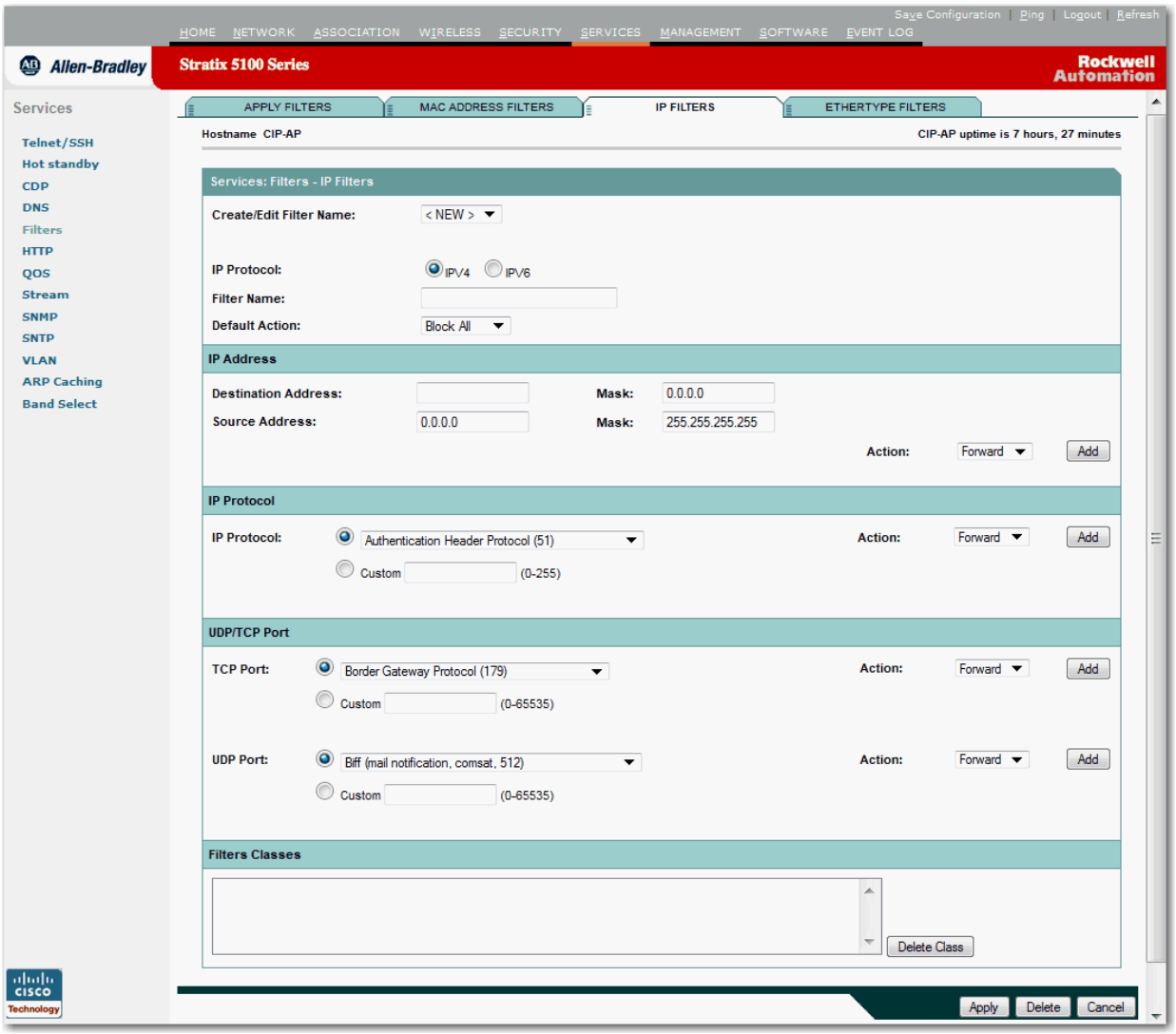
IP 过滤器 (IP 地址、 IP 协议和 IP 端口) 阻止或允许通过接入点的以太网和无线电端口使用特定的协议，而 IP 地址过滤器允许或阻止转发特定 IP 地址的往来单播和多播数据包。

您可以创建一个过滤器，允许通过除指定地址外的所有地址的流量，也可阻止除指定地址外的所有地址的流量。您可以创建包含一种、两种或所有三种 IP 过滤方法的元素的过滤器。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

使用 IP Filters (IP 过滤器) 页面创建接入点的 IP 过滤器。

1. 从主菜单中单击 Services (服务)。
2. 在 Services (服务) 页面列表中，单击 Filters (过滤器)。
3. 在 Apply Filters (应用过滤器) 页面中，单击 IP Filters (IP 过滤器) 选项卡。

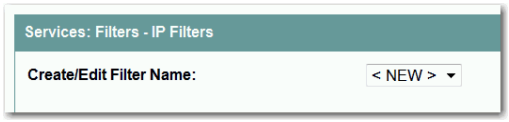
图 121 - IP Filters (IP 过滤器) 页面



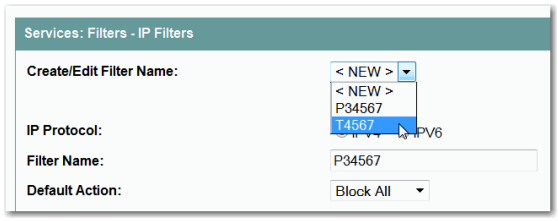
创建IP 过滤器

根据以下步骤创建 IP 过滤器。

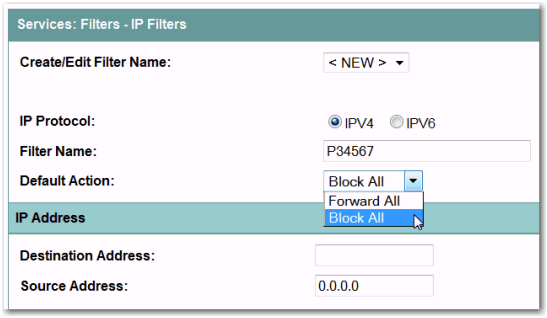
1. 如果正在创建一个新的过滤器，确保在 Create/Edit Filter Name (创建 / 编辑过滤器名称) 菜单中选择了 <NEW> (默认值)。



要编辑一个现有的过滤器，选择此过滤器名称。



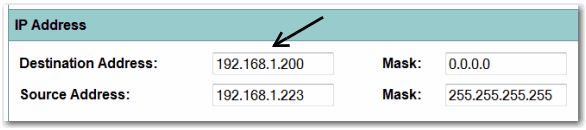
2. 在 Filter Name (过滤器名称) 域中输入新过滤器的描述性名称。
3. 从 Default Action (默认操作) 下拉菜单中，选择 Forward all (全部转发) 或 Block all (全部阻止)。



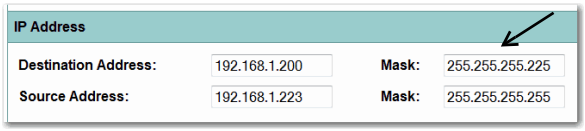
过滤器的默认操作必须是过滤器中至少一个地址的相反操作。例如，如果创建一个包含某个 IP 地址、IP 协议和 IP 端口的过滤器，并对它们选择了 Block (阻止) 操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。

4. 要过滤某个 IP 地址，在 IP Address (IP 地址) 域中输入该地址。

重要事项　如果您打算阻止除指定允许的地址外的所有 IP 地址的通信，则将计算机地址置于允许的地址列表中，避免失去与接入点的连接。



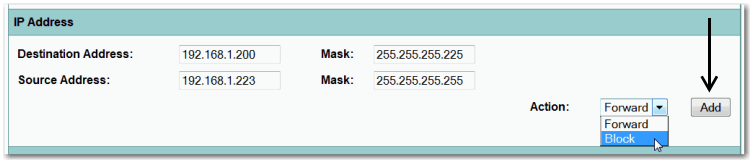
5. 在 Mask (掩码) 域中输入 IP 地址的掩码。



输入掩码，并用句点分隔字符组，例如， 112.334.556.778。

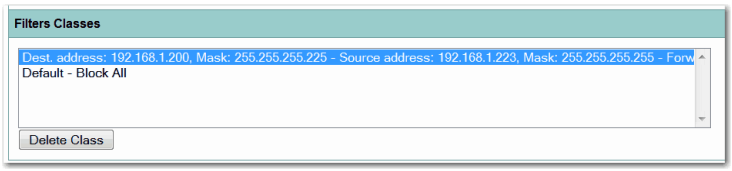
如果输入 255.255.255.255 作为掩码，接入点将接受任何 IP 地址。如果输入 0.0.0.0，则接入点将查找与您在 IP Address (IP 地址) 域中的输入完全匹配的 IP 地址。在该域中输入掩码的效果与在 CLI 中输入掩码的效果相同。

6. 从 Action (操作) 菜单中选择 Forward (转发) 或 Block (阻止)。



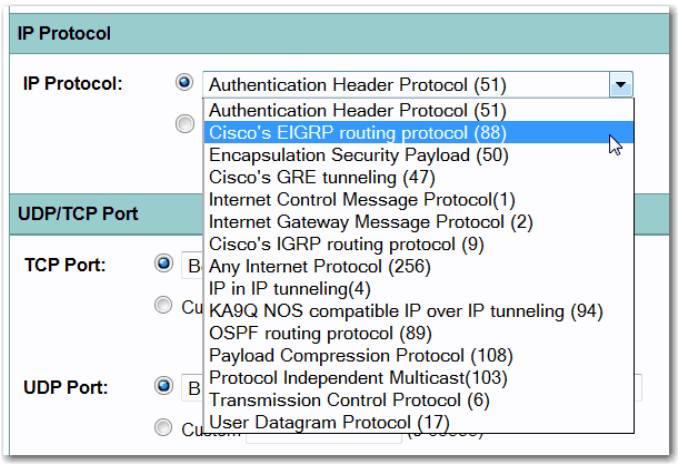
7. 单击 Add (添加)。

地址出现在 Filters Classes (过滤器类别) 域中。要从 Filters Classes (过滤器类别) 列表中删除地址，则选择相关地址，然后单击 Delete Class (删除类别)。

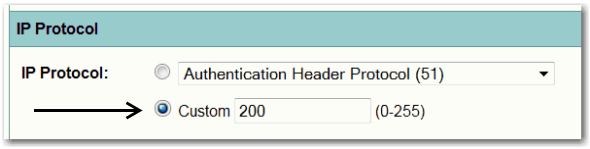


如果不需要将 IP 协议或 IP 端口元素添加到过滤器，则跳至 步骤 15 在接入点上保存过滤器。

8. 要过滤某个 IP 协议，从 IP Protocol (IP 协议) 下拉菜单中选择其中一种公共协议，或选择 Custom (自定义) 单选按钮，然后在 Custom (自定义) 域中输入现有 ACL 的编号。



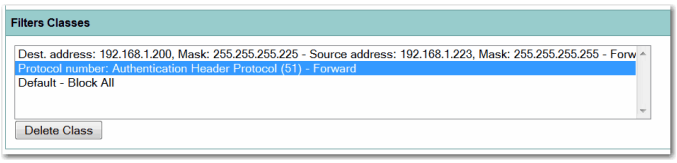
输入一个范围为 0...255 的 ACL 编号。有关 IP 协议列表及其数字代号的信息，请参见第 523 页的 “ 协议过滤器 ”。



9. 从 Action (操作) 菜单中选择 Forward (转发) 或 Block (阻止)。

10. 单击 Add (添加)。

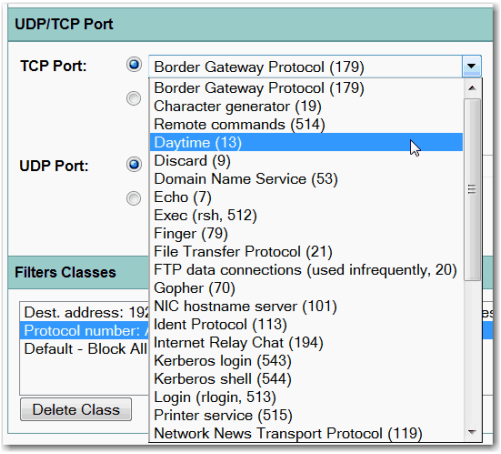
    协议出现在 Filters Classes (过滤器类别) 域中。



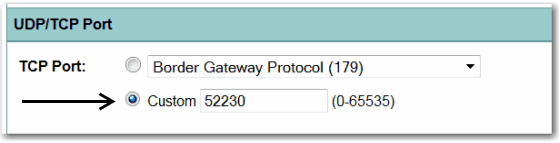
    要从 Filters Classes (过滤器类别) 列表中删除协议，选择该协议，然后单击 Delete (删除)。

    如果不需要将 IP 端口元素添加到过滤器，则跳至步骤 15 在接入点上保存过滤器。

11. 要过滤某个 TCP 或 UDP 端口协议，从 TCP Port (TCP 端口) 或 UDP Port (UDP 端口) 下拉菜单中选择其中一种公共端口协议，或选择 Custom (自定义) 单选按钮，然后在其中一个 Custom (自定义) 域中输入现有协议的编号。



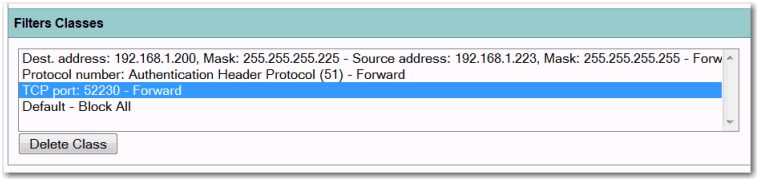
12. 输入一个 0...65535 之间的协议编号。



13. 从 Action (操作) 菜单中选择 Forward (转发) 或 Block (阻止)。

14. 单击 Add (添加)。

    协议出现在 Filters Classes (过滤器类别) 域中。



    要从 Filters Classes (过滤器类别) 列表中删除协议，选择该协议，然后单击 Delete (删除)。

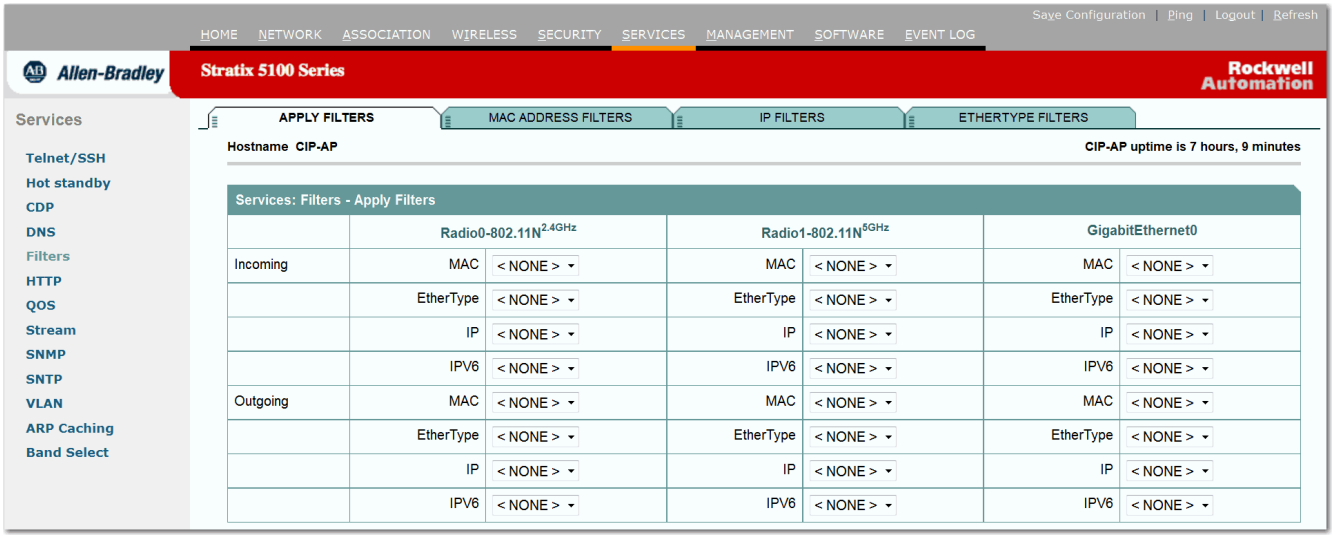
15. 当过滤器完成后，单击 Apply (应用)。

    过滤器在接入点上保存，但在 Apply Filters (应用过滤器) 页面上应用它们之前，过滤器不会启用。

16. 单击 Apply Filters (应用过滤器) 选项卡返回 Apply Filters (应用过滤器) 页面。

    第 449 页的图 122 显示了 Apply Filters (应用过滤器) 页面。

图 122 - Apply Filters (应用过滤器) 页面



17. 从其中一个 IP 下拉菜单中，选择过滤器名称。

    您可将过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

18. 单击 Apply (应用)。

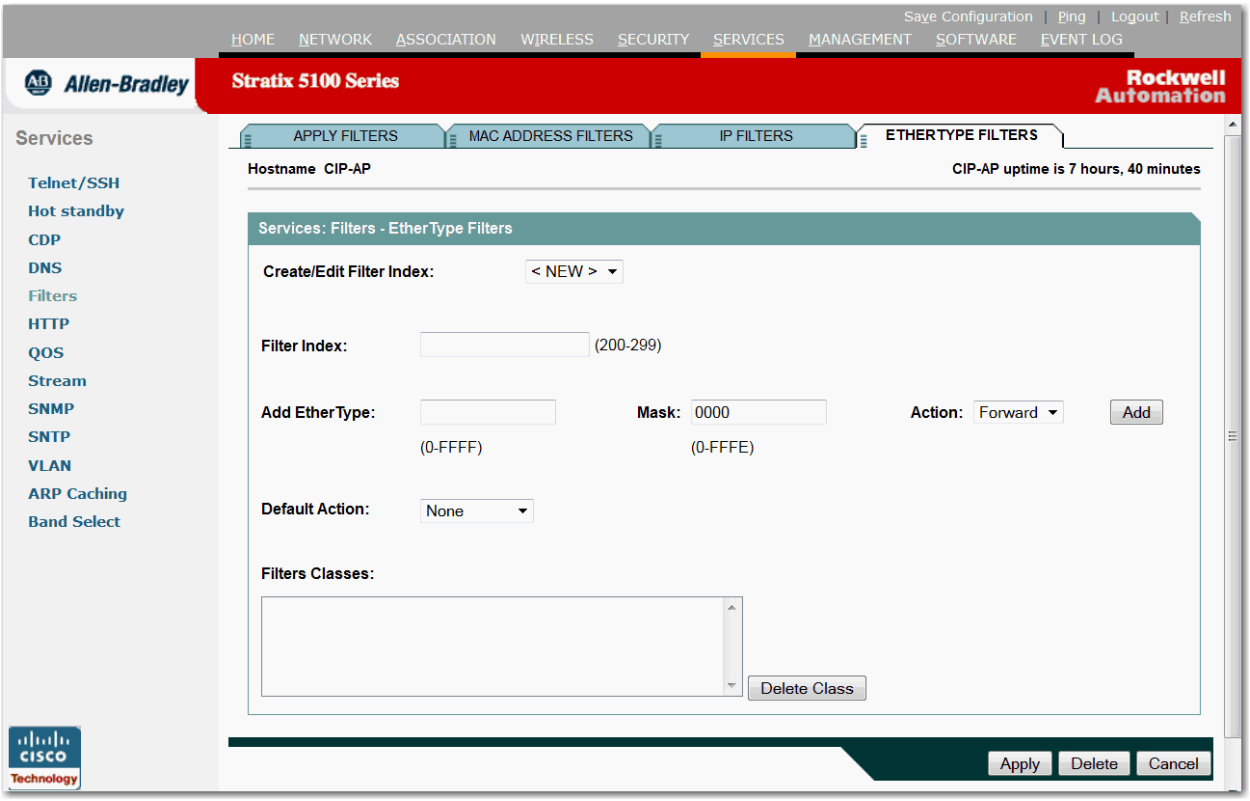
    在所选端口上启用过滤器。

配置和启用以太网类型过滤器

以太网类型过滤器用于阻止或允许通过接入点的以太网和无线电端口使用特定的协议。您可将所创建的过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

使用 Ethertype Filters (以太网类型过滤器) 页面创建接入点的以太网类型过滤器。下图显示了 Ethertype Filters (以太网类型过滤器) 页面。

图 123 - Ethertype Filters (以太网类型过滤器) 页面



根据以下步骤转到 Ethertype Filters (以太网类型过滤器) 页面。

1. 从主菜单中单击 Services (服务)。
2. 在 Services (服务) 页面列表中，单击 Filters (过滤器)。
3. 在 Apply Filters (应用过滤器) 页面中，单击 Ethertype Filters (以太网类型过滤器) 选项卡。

创建以太网类型过滤器

根据以下步骤创建以太网类型过滤器：

1. 根据链接路径转到 Ethertype Filters (以太网类型过滤器) 页面。
2. 如果创建新过滤器，确保在 Create/Edit Index (创建 / 编辑索引) 菜单中选择 <NEW> (新) (默认值)。

   要编辑现有过滤器，选择 Create/Edit Index (创建 / 编辑索引) 菜单中选择过滤器编号。

3. 在 Filter Index (过滤器索引) 域中，用一个范围为 200...299 的数字命名过滤器。

   您所分配的数字将用于创建过滤器的访问控制列表 (ACL)。

4. 在 Add Ethertype (添加以太网类型) 域中输入一个以太网类型编号。

   有关协议列表及其数字代号的信息，请参见第 523 页的 “ 协议过滤器 ”。

5. 在 Mask (掩码) 域中输入以太网类型的掩码。

   如果输入 0，掩码需要与以太网类型精确匹配。

6. 从 Action (操作) 菜单中选择 Forward (转发) 或 Block (阻止)。

7. 单击 Add (添加)。

   以太网类型出现在 Filters Classes (过滤器类别) 域中。要从 Filters Classes (过滤器类别) 列表中删除以太网类型，则选择相关以太网类型，然后单击 Delete Class (删除类别)。重复步骤 4 至步骤 7，将以太网类型添加到过滤器中。

8. 从 Default Action (默认操作) 菜单中选择 Forward All (全部转发) 或 Block All (全部阻止)。

   过滤器的默认操作必须是过滤器中至少一个以太网类型的相反操作。例如，如果输入多个以太网类型，并选择了 Block (阻止) 作为它们的操作，则必须选择 Forward All (全部转发) 作为过滤器的默认操作。

9. 单击 Apply (应用)。

   过滤器在接入点上保存，但在 Apply Filters (应用过滤器) 页面上应用它们之前，过滤器不会启用。

10. 单击 Apply Filters (应用过滤器) 选项卡返回 Apply Filters (应用过滤器) 页面。

11. 从其中一个 Ethertype (以太网类型) 下拉菜单中选择过滤器编号。

    您可将过滤器应用到以太网和 / 或无线电端口，或传入和 / 或传出数据包。

12. 单击 Apply (应用)。

    在所选端口上启用过滤器。

备注：

配置 CDP

本章介绍了如何在接入点上配置 思科发现协议 (CDP)。如果您不准备使用 CDP，我们建议您关闭该功能。

重要事项 关于本章中使用的命令的完整语法和用法信息，请参见以下出版物：

- Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges (思科 Aironet 接入点和网桥的思科 IOS 命令参考)
- Cisco IOS Configuration Fundamentals Command Reference for Release 12.2 (思科 IOS 配置基本命令参考，第 12.2 版)

关于在设备管理器中配置 CDP 的信息，请参见第 137 页的 “CDP 页面 ”。

CDP

思科发现协议 (CDP) 是一种运行在所有思科网络设备上的设备发现协议。每台设备向多播地址发送标识消息，每台设备监视其他设备发送的消息。 CDP 数据包中的信息用于网络管理软件。

接入点以太网端口上默认启用了 CDP。但是，当无线电端口关联到另一个无线架构设备 (例如，接入点或网桥) 时， CDP 仅在接入点无线电端口上启用。CDP 在接入点上配置的最小 VLAN 编号上发送。当无线网络中使用了多个 VLAN 时，我们建议将配置的最小 VLAN 编号用作原生 VLAN。

重要事项 要让无线局域网实现最佳性能，如果接入点上启用了 VLAN，则禁用所有无线电接口和子接口的 CDP。

配置 CDP

本节介绍了 CDP 配置信息和过程：

默认 CDP 配置

下表列出了默认的 CDP 设置。

表 109 - 默认 CDP 配置

功能	默认设置
CDP 全局状态	启用
CDP 接口状态	启用
CDP 保持时间 (数据包保持时间 (秒))	180
CDP 计时器 (每隔 x 秒发送数据包)	60

配置 CDP 特性

您可配置 CDP 保持时间 (接入点丢弃 CDP 数据包前等待的秒数) 和 CDP 计时器 (接入点发送 CDP 数据包的间隔秒数)。

在特权 EXEC 模式下，根据以下步骤配置 CDP 保持时间和 CDP 计时器。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. (可选) 指定接收设备保留设备所发送的信息的时间长度，在此之后，信息将被丢弃。

   范围为 10...255 s ； 默认值为 180 s。

   ```
   cdp holdtime seconds
   ```

3. (可选) 设置 CDP 更新的传输频率 (s)。

   范围为 5...254 s ； 默认值为 60 s。

   ```
   cdp timer seconds
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

使用 CDP 命令的 no 格式恢复到默认设置。

本例显示了如何配置和验证 CDP 特性：

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end
```

```
AP# show cdp

全局 CDP 信息：
        发送保持时间值 120 秒
        每隔 50 秒发送一次 CDP 数据包
```

关于 CDP show 命令的更多信息，请参见第 457 页的 “ 监视和维护 CDP”。

禁用和启用 CDP

CDP 默认已启用。在特权 EXEC 模式下，根据以下步骤禁用 CDP 设备发现功能。

1. 进入全局配置模式。
   ```
   configure terminal
   ```
2. 禁用 CDP。
   ```
   no cdp run
   ```
3. 返回到特权 EXEC 模式。
   ```
   end
   ```

在特权 EXEC 模式下，根据以下步骤启用 CDP：

1. 进入全局配置模式。
   ```
   configure terminal
   ```
2. 在禁用 CDP 后进入 CDP。
   ```
   cdp run
   ```
3. 返回到特权 EXEC 模式。
   ```
   end
   ```

本例显示了如何启用 CDP。

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

禁用和启用接口上的 CDP

在所有支持的接口上，默认已启用 CDP 发送和接收 CDP 信息。

在特权 EXEC 模式下，根据以下步骤禁用接口上的 CDP。

1. 进入全局配置模式。
   `configure terminal`
2. 进入接口配置模式，输入要禁用 CDP 的接口。
   `interface` *`interface-id`*
3. 禁用接口上的 CDP。
   `no cdp enable`
4. 返回到特权 EXEC 模式。
   `end`
5. (可选) 将您的输入保存到配置文件中。
   `copy running-config startup-config`

在特权 EXEC 模式下，根据以下步骤启用接口上的 CDP：

1. 进入全局配置模式。
   `configure terminal`
2. 进入接口配置模式，输入要启用 CDP 的接口。
   `interface` *`interface-id`*
3. 在禁用后，启用接口上的 CDP。
   `cdp enable`
4. 返回到特权 EXEC 模式。
   `end`
5. (可选) 将您的输入保存到配置文件中。
   `copy running-config startup-config`

本例显示了如何启用接口上的 CDP。

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```

监视和维护 CDP

要监视和维护设备上的 CDP，在特权 EXEC 模式下执行一个或多个此类任务。

命令	描述
`clear cdp counters`	将通信计数器重置为零。
`clear cdp table`	删除邻居信息的 CDP 表。
`show cdp`	显示全局信息，例如，发送数据包的传输频率和保持时间。
`show cdp entry` *`entry-name`* `[protocol | version]`	显示特定邻居的信息。 您可输入星号 (*) 显示所有 CDP 邻居，或输入邻居名称获取信息。 您还可限制显示的信息，仅显示特定邻居上启用的协议信息，或设备上运行的软件版本的信息。
`show cdp interface [`*`type number`*`]`	显示已启用 CDP 的接口的信息。 您可限制显示的信息，仅显示接口类型或接口数量，例如，输入 `gigabitethernet 0/1`，将只显示千兆以太网端口 1 上的信息。
`show cdp neighbors [`*`type number`*`] [detail]`	显示邻居的信息，包括设备类型、接口类型和编号、保持时间设置、功能、平台和端口 ID。 您可限制显示的信息，只显示特定类型的邻居或接口编号，或扩展信息显示以提供更多详细信息。
`show cdp traffic`	显示 CDP 计数器，包括已发送和接收的数据包数量以及校验和错误。

备注：

配置 SNMP

本章介绍了如何在接入点上配置 简单网络管理协议 (SNMP)。

关于本章中使用的命令的完整语法和用法信息，请参见以下出版物：

- Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges (思科 Aironet 接入点和网桥的思科 IOS 命令参考)
- Cisco IOS Configuration Fundamentals Command Reference for Release 12.3 (思科 IOS 配置基本命令参考，第 12.3 版)

SNMP

SNMP 是一种应用层协议，为 SNMP 管理器和代理之间的通信提供一种消息格式。 SNMP 管理器可以是网络管理系统 (NMS) 的一部分。代理和管理信息库 (MIB) 驻留在接入点中。要在接入点上配置 SNMP，应定义管理器和代理之间的关系。

SNMP 代理包含 MIB 变量， SNMP 管理器可请求或更改这些值。管理器可从代理获取值，或将其保存到代理中。代理收集来自 MIB (设备参数和网络数据的信息库) 的数据。代理还可响应管理器获取和设置数据的请求。

代理可给管理器发送非请求陷阱。陷阱是向 SNMP 管理器提醒网络状况的消息。陷阱表示不正确的用户验证、重启动、链接状态 (上行或下行)、MAC 地址追踪、TCP 连接关闭、到邻居的连接丢失或其他重要事件。

SNMP 版本

该软件版本支持以下 SNMP 版本：

- SNMPv1 —— 简单网络管理协议， RFC 1157 中定义的完整互联网标准。
- SNMPv2C 具备以下特性：
  - SNMPv2 —— SNMP 第 2 版， RFC 1902...1907 中定义的互联网协议草案。
  - SNMPv2C —— SNMPv2 基于社区的管理框架， RFC 1901 中定义的实验性互联网协议。
- SNMPv3 具备以下特性：
  - 支持 SHA 和 MD5 验证协议以及 DES56 加密。
  - 三种安全级别：无验证和无隐私 (NoAuthNoPriv)、验证和无隐私 (AuthNoPriv) 以及验证和隐私 (AuthPriv)。

SNMPv3 支持最高的 SNMP 通信安全级别。 SNMPv1 和 SNMPv2 的社区字符串以明文保存和传输，不进行加密。在 SNMPv3 安全模型中，SNMP 用户经过验证并加入用户组中。将根据用户组限制对系统数据的访问。

必须配置 SNMP 代理，以使用管理工作站支持的 SNMP 版本。代理可与多个管理器通信；因此，您可配置软件，以支持使用 SNMPv3 协议与一个管理工作站通信，并使用 SNMPv2 或 SNMPv1 协议与另一个管理工作站通信。

下表列出了接入点支持的 SNMP 版本和安全级别：

表 110 - SNMP 版本和安全级别

SNMP 版本	安全级别	验证	加密
v1	NoAuthNoPriv	社区字符串匹配	无
v2C	NoAuthNoPriv	社区字符串匹配	无
v3	NoAuthNoPriv	用户名匹配	无
v3	AuthNoPriv	HMAC-MD5 或 HMAC-SHA 算法	无
v3	AuthPriv	HMAC-MD5 或 HMAC-SHA 算法	DES 56 位加密

关于 SNMPv3 的详细信息，请参见出版物：Configuring Simple Network Management Protocol (配置简单网络管理协议)。

SNMP 管理器功能

SNMP 管理器使用 MIB 中的信息来执行下表中所述的操作。

表 111 - SNMP 操作

操作	描述
get-request	从指定变量提取值。
get-next-request	从表格中的变量提取值。(2)
get-bulk-request(1)	提取大块数据，否则需要传输许多小块数据，例如，表格中的多行。
get-response	回复 NMS 发送的 get-request、 get-next-request 和 set-request 请求。
set-request	将值保存到特定的变量中。
陷阱	当事件发生时， SNMP 代理将向 SNMP 管理器发送非请求消息。

(1) get-bulk 命令仅适用于 SNMPv2。

(2) 使用该操作， SNMP 管理器无需知晓确切的变量名称。随后执行搜索，从表格中查找所需的变量。

SNMP 代理功能

SNMP 代理按照以下方式响应 SNMP 管理器请求：

- 获取 MIB 变量 - SNMP 代理将响应 NMS 的请求而开始该功能。代理提取所请求 MIB 变量的值，并以该值响应 NMS。
- 设置 MIB 变量 - SNMP 代理将响应 NMS 的消息而开始该功能。SNMP 代理将 MIB 变量的值更改为 NMS 所请求的值。

SNMP 代理还将发送非请求陷阱消息，通知 NMS 在代理上发生重要事件。陷阱条件的实例包括但不仅限于：当端口或模块启用或停用时、当生成树拓扑发生更改时以及当验证失败时。

SNMP 社区字符串

SNMP 社区字符串作为嵌入式密码，用于对访问 MIB 对象进行认证。要使 NMS 访问接入点， NMS 上的社区字符串定义必须至少匹配接入点上的三种社区字符串定义之一。

社区字符串有以下几种属性：

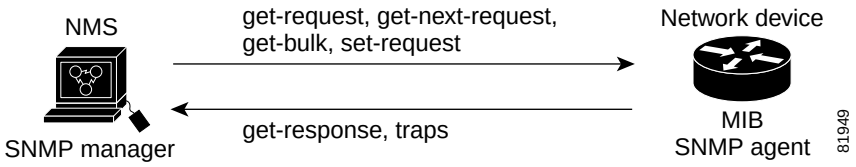
- 只读 —— 赋予授权管理工作站对 MIB 中除社区字符串之外的所有对象的读权限，但没有写权限。
- 读写 —— 赋予授权管理工作站对 MIB 中所有对象的读写权限，但不允许访问社区字符串。

使用 SNMP 访问 MIB 变量

网络管理软件 (NMS) 使用接入点 MIB 变量设置设备变量，并轮询网络上设备的特定信息。轮询结果可使用图形方式显示，经分析后可对互联网故障进行故障处理，从而提升网络性能、验证设备配置、监控通信负载等。

如下所示， SNMP 代理收集 MIB 的数据。代理可将陷阱 (特定事件的通知) 发送到 SNMP 管理器，由它来接收和处理陷阱。陷阱是向 SNMP 管理器提醒网络状况的消息，例如，不正确的用户验证、重启动、链接状态 (下行或下行)、 MAC 地址追踪等。 SNMP 代理还能以 `get-request?get-next-request` 和 `set-request` 格式响应 SNMP 管理器发送的与 MIB 相关的查询。

图 124 - SNMP 网络



关于支持的 MIB 以及如何访问它们的信息，请参见第 529 页的 “ 支持的 MIB”。

配置 SNMP

本节介绍了如何在接入点上配置 SNMP。

默认 SNMP 配置

下表显示了默认的 SNMP 配置。

功能	默认设置
SNMP 代理	禁用
SNMP 社区字符串	默认状态，未配置字符串。但当使用 Web 浏览器界面启用 SNMP 后，接入点自动创建公共社区，并可对 IEEE802dot11 MIB 进行只读访问。
SNMP 陷阱接收器	未配置
SNMP 陷阱	未启用

启用 SNMP 代理

不存在专门用于启用 SNMP 的 CLI 命令。所输入的第一个 `snmp-server` 全局配置命令可启用支持的 SNMP 版本。

您还可在 Web 浏览器界面的 SNMP Properties (SNMP 属性) 页面启用 SNMP。当在 Web 浏览器界面启用 SNMP 后，接入点将自动创建名为 public 的社区字符串，并可只读访问 IEEE802dot11 MIB。

配置社区字符串

您可使用 SNMP 社区字符串定义 SNMP 管理器和代理之间的关系。社区字符串的作用类似于密码，旨在控制对接入点上代理的访问。

您可指定以下一个或多个与字符串关联的特性 (可选)：

- SNMP 管理器的 IP 地址访问列表，列表中的管理器可使用社区字符串获得代理的访问权限
- MIB 视图，定义了特定社区可访问的所有 MIB 对象的子集

- 社区可访问的 MIB 对象的读写或只读权限

提示 在当前的思科 IOS MIB 代理工具中，默认社区字符串对应 Internet MIB 对象子树。由于 IEEE802dot11 位于 MIB 对象树的另一个分支下，必须在 IEEE802dot11 MIB 上启用独立的社区字符串或视图，或者在 MIB 对象树中的 ISO 对象上启用公共视图和社区字符串。

ISO 是 IEEE (IEEE802dot11) 和 Internet 的公共父级节点。该 MIB 代理的特性与未运行思科 IOS 软件的接入点上其他 MIB 代理的不同。

在特权 EXEC 模式下，根据以下步骤在接入点上配置社区字符串。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 配置社区字符串。
   - string 指定用作密码的字符串，用于控制对 SNMP 协议的访问。您可配置一个或多个任意长度的社区字符串。
   - (可选) access-list-number 用于输入 IP 标准访问列表，编号为 1...99 和 1300...1999。
   - (可选) view mib-view 用于指定社区可访问的社区 MIB 视图，例如， ieee802dot11。

     关于使用 snmp-server view 命令通过 IEEE 视图访问标准 IEEE 802.11 MIB 对象的说明，请参见第 468 页的 “snmp-server view 命令 ”。
   - (可选) 如果要让授权管理工作站提取 MIB 对象，则指定只读 (ro)；或者，如果要让授权管理工作站提取和修改 MIB 对象，则指定读 / 写 (rw)。默认情况下，社区字符串允许所有对象的只读权限。

   提示 要访问 IEEE802dot11 MIB，必须在 IEEE802dot11 MIB 上启用独立的社区字符串或视图，或者在 MIB 对象树中的 ISO 对象上启用公共视图和社区字符串。

   ```
   snmp-server community string
   [ access-list-number ]
   [ view mib-view ]
   [ro | rw]
   ```

3. (可选) 如果在第 2 步中指定了 IP 标准访问列表编号，则创建列表，并根据需要多次重复命令。
   - 对于 access-list-number，输入第 2 步中指定的访问列表编号。
   - 如果条件匹配， deny 关键字将拒绝访问。如果条件匹配，permit 关键字将允许访问。
   - 对于 source，输入允许使用社区字符串获得代理访问权限的 SNMP 管理器的 IP 地址。
   - (可选) 对于 source-wildcard，在要应用的来源的通配符位输入小数点符号。在想要忽略的位上放置一个。

4. 请记住，访问列表始终以隐式拒绝声明结尾。

   ```
   access-list access-list-number {deny | permit}
   source [source-wildcard]
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. 确认您的输入。

   ```
   show running-config
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

要禁用 SNMP 社区的访问，可将该社区的社区字符串设为空字符串 (不输入社区字符串值)。要删除特定的社区字符串，使用 `no snmp-server community` string 全局配置命令。

本例显示了如何为 SNMP 分配字符串 `open` 和 `ieee`，以允许两者的读写权限，并指定 open 为非 IEEE802dot11-MIB 对象的查询社区字符串，`ieee` 为 IEEE802dot11-mib 对象的查询社区字符串：

```
ap(config)# snmp-server view dot11view ieee802dot11
included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view
ieee802dot11 rw
```

指定 SNMP 服务器组名称

要配置新的 SNMP 组合或 SNMP 用户到 SNMP 视图的映射表，可在全局配置模式下使用下列命令：

配置新的 SNMP 组合或 SNMP 用户到 SNMP 视图的映射表。

```
snmp-server group [groupname  {v1 | v2c | v3 [auth |
noauth | priv]}][read readview] [write writeview]
[notify notifyview] [access  access-list]
```

配置 SNMP 服务器主机

要配置 SNMP 陷阱操作的接收方，可在全局配置模式下使用下列命令：

```
snmp-server host host [traps | informs][version {1
| 2c | 3 [auth | noauth | priv]} ] community-string
[udp-port port] [notification-type]
```

配置 SNMP 服务器用户

要配置 SNMP 组的新用户，可在全局配置模式下使用下列命令：

```
snmp-server user username [groupname remote ip-
address
[udp-port port] {v1 | v2c | v3 [encrypted] [auth
{md5 | sha}  auth-password [priv des56 priv
password]] [access access-list]
```

配置陷阱管理器和启用陷阱

陷阱管理器是接收和处理陷阱的管理工作站。陷阱是发生特定事件时接入点生成的系统警报。默认情况下，未定义陷阱管理器，也不发送陷阱。

运行该思科 IOS 版本的接入点拥有无限量的陷阱管理器。社区字符串的长度为任意。

下表介绍了支持的接入点陷阱 (通知类型)。您可启用任意几个或所有陷阱，并配置陷阱管理器来接收它们。

表 112 - 支持的接入点陷阱

通知类型	描述
authenticate-fail	启用验证失败陷阱。
config	启用 SNMP 配置更改陷阱。
deauthenticate	启用客户端设备取消验证陷阱。
disassociate	启用客户端设备解除关联陷阱。
dot11-qos	启用 QoS 更改陷阱。
entity	启用 SNMP 实体更改陷阱。
rogue-ap	启用伪接入点检测陷阱。
snmp	启用 SNMP 事件陷阱。
switch-over	启用切换陷阱。
Syslog	启用 syslog 陷阱。
wlan-wep	启用 WEP 陷阱。

一些通知类型无法通过 snmp-server enable 全局配置命令来控制，例如， udp-port。这些通知类型始终为启用。您可对特定主机使用 snmp-server host 全局配置命令，接收第 466 页的表 112 中所列的通知类型。

在特权 EXEC 模式下，根据以下步骤配置接入点向主机发送陷阱。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 指定陷阱消息的接收方。

- host-addr 用于指定主机的名称或地址 (目标接收方)。
- 指定**陷阱** (默认值)，以将 SNMP 陷阱发送给主机。指定**通知**，以将 SNMP 通知发送给主机。
- 指定支持的 SNMP 版本。默认值为版本 1，不提供通知功能。版本 3 有三种安全级别：
  - auth —— 指定数据包验证，但不加密
  - noauth —— 指定数据包不验证，不加密
  - priv —— 指定数据包验证并加密
- community-string 用于指定要通过通知操作发送的字符串。虽然您可以使用 snmp-server host 命令设置该字符串，但我们建议您在使用 snmp-server host 命令之前先使用 snmp-server community 命令定义该字符串。
- 对于 notification-type，使用第 466 页的表 112 中列出的关键字。

```
snmp-server host host-addr {traps | informs}
{version {1 | 2c | 3 {auth | noauth | priv}}}
community-string [udp-port port]
notification-type
```

3. 启用发送特定陷阱的接入点。

   关于陷阱列表，请参见第 466 页的表 112。

   要启动多种陷阱类型，必须为每种陷阱类型发出独立的 snmp-server enable traps 命令。

   ```
   snmp-server enable traps notification-types
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

   要从接收陷阱中删除指定的主机，使用 `no snmp-server host` host 全局配置命令。要禁用特定的陷阱类型，使用 `no snmp-server enable traps` notification-types 全局配置命令。

设置代理联系人和位置信息

在特权 EXEC 模式下，根据以下步骤设置 SNMP 代理的系统联系人和位置，以便可通过配置文件访问这些配置。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 设置系统联系人字符串。

   例如：

   ```
   snmp-server contact Dial System Operator at beeper
   21555.
   ```

3. 设置系统位置字符串。

   例如：

   ```
   snmp-server location Building 3/Room 222
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

`snmp-server view` 命令

在全局配置模式下，使用 `snmp-server view` 命令通过 IEEE 视图和 dot11 读写社区字符串访问标准 IEEE 802.11 MIB 对象。

本例显示了如何启用 IEEE 视图和 dot11 读写社区字符串：

```
AP(config)# snmp-server view ieee ieee802dot11
included

AP(config)# snmp-server community dot11 view ieee RW
```

SNMP 示例

本例显示了如何启用 SNMPv1、SNMPv2C 和 SNMPv3。配置允许任何 SNMP 管理器使用社区字符串 public 以只读权限访问所有对象。该配置不会导致接入点发送任何陷阱。

```
AP(config)# snmp-server community public
```

本例显示了如何为 SNMP 分配字符串 open 和 ieee，以允许两者的读写权限，并指定 open 为非 IEEE802dot11-MIB 对象的查询社区字符串，ieee 为 IEEE802dot11-mib 对象的查询社区字符串：

```
bridge(config)# snmp-server view dot11view
ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view
ieee802dot11 rw
```

本例显示如何允许任何 SNMP 管理器使用社区字符串 public 以只读权限访问所有对象。接入点还使用 SNMPv1 向主机 192.180.1.111 和 192.180.1.33 发送配置陷阱，使用 SNMPv2C 向主机 192.180.1.27 发送配置陷阱。社区字符串 public 将通过陷阱发送。

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c
public
AP(config)# snmp-server host 192.180.1.111 version 1
public
AP(config)# snmp-server host 192.180.1.33 public
```

本例显示了如何允许使用 comaccess 社区字符串对访问列表 4 的成员的所有对象进行只读访问。其他 SNMP 管理器都无权访问各模块。SNMP 验证失败陷阱由 SNMPv2C 使用社区字符串 public 发送给主机 cisco.com。

```
AP(config)# snmp-server community comaccess ro 4
AP(config)# snmp-server enable traps snmp
authentication
AP(config)# snmp-server host cisco.com version 2c
public
```

本例显示了如何给主机 cisco.com 发送实体 MIB 陷阱。社区字符串受限。除任何之前已启用的陷阱之外，第一行还启用接入点发送实体 MIB 陷阱。第二行指定这些陷阱的目标，并覆盖主机 cisco.com 之前的 `snmp-server host` 命令。

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted
entity
```

本例显示了如何启用接入点使用社区字符串 public 串向主机 myhost.cisco.com 发送所有陷阱：

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com public
```

本例显示了如何配置以下 SNMPv3 设置：

- 视图名称 (iso)
- SNMP 引擎 ID (1234567890)，该代理使用其向 IP 地址为 1.4.74.10 的远程主机标识自身身份
- SNMPv3 组 (admin)，支持隐私加密，组中所有用户都对 iso 视图中定义的所有对象有读写权限
- SNMP 用户 (joe)，它属于 admin 组，使用 MD5 验证进行查询，使用 xyz123 作为 MD5 密码，使用 DES56 数据查询加密，使用 key007 作为加密密钥
- SNMP 用户 (fred)，它属于 admin 组，使用 MD5 验证进行查询，使用 abc789 作为 MD5 加密密码，使用 DES56 数据查询加密，使用 key99 作为加密密钥

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10
1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read
iso write iso
AP(config)# snmp-server user joe admin v3 auth md5
xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3
encrypted auth md5 abc789 priv des56 key99
```

提示 在输入本例中最后一个命令后， show running-config 和 show startup-config 命令将只显示一部分 SNMP 配置。

显示 SNMP 状态

要显示 SNMP 输入和输出统计信息，包括非法社区字符串条目、错误和请求变量的数量，可使用 `show snmp` 特权 EXEC 命令。

关于该显示画面中各域的信息，请参见 Cisco IOS Configuration Fundamentals Command Reference (思科 IOS 配置基础命令参考)。

备注：

配置工作组网桥模式、中继器模式和备用接入点

本章描述了如何将接入点配置为工作组网桥、中继器或热备用单元。

工作组网桥模式

可以将 Stratix 5100 接入点配置为工作组网桥。在工作组网桥模式下，单元作为客户端关联到另一个接入点，并为连接到其以太网端口的设备提供一个网络连接。

例如，如果您需要为一组网络打印机提供无线连接，您可将打印机连接到集线器或交换机，再将集线器或交换机连接到接入点以太网端口，并将接入点配置为工作组网桥。工作组网桥关联到网络上的一个接入点。

如果接入点有两个无线电装置，则 2.4 GHz 无线电或 5 GHz 无线电均可在工作组网桥模式下工作。当将一个无线电接口配置为工作组网桥时，另一个无线电接口仍然处于启用状态。

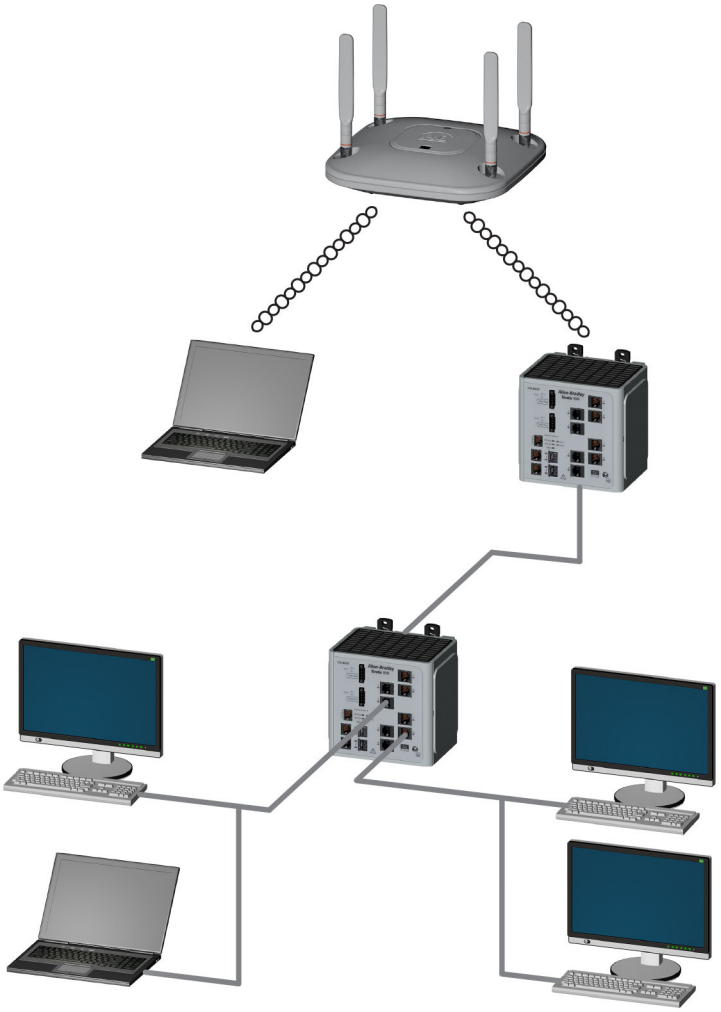
重要事项 如果将其以太网端口连接到有线局域网，则工作组网桥模式下的接入点会形成网桥回路。为避免在网络上形成网桥回路，请在将其配置为工作组网桥之前或之后立即将工作组网桥从有线局域网断开。

如果在指定为工作组网桥父设备的根接入点上配置多个 BSSID，则当添加或删除父设备上的 BSSID 时，父设备的 MAC 地址可能会更改。如果在无线局域网上使用多个 BSSID 且无线局域网上的工作组网桥被配置为关联到特定父设备，则当添加或删除父接入点上的 BSSID 时，请检查工作组网桥的关联状态。如有必要，重新配置工作组网桥，以使用 BSSID 的新 MAC 地址。

虽然作为网桥工作，工作组网桥模式下的接入点的无线电范围却是有限的。工作组网桥不支持距离设置，这项设置允许您配置无线网桥在数千米范围内通信。

下图显示了工作组网桥模式下的接入点。

图 125 - 工作组网桥模式下的接入点



将工作组网桥作为基础架构设备或客户端设备

工作组网桥所关联的接入点可将工作组网桥作为基础架构设备或简单的客户端设备。默认情况下，接入点和网桥将工作组网桥作为客户端设备。

为提高可靠性，可对接入点和网桥进行配置，以不将工作组网桥作为客户端设备，而是和接入点或网桥一样作为基础架构设备。将工作组网桥作为架构设备表示接入点能可靠地将多播数据包 (包括地址解析协议 (ARP) 数据包) 发送至工作组网桥。可使用基础架构 —— 客户端配置接口命令来配置接入点和网桥，将工作组网桥作为基础架构设备。

对接入点和网桥进行配置，将工作组网桥作为客户端设备，便于将更多工作组网桥关联到同一接入点，或使用非基础架构 SSID 进行关联。可靠多播传输的性能成本 —— 复制发送至每个工作组网桥的每个多播数据包 —— 会限制可关联到接入点或网桥的基础架构设备数量，包括工作组网桥。

为将可以关联到接入点的工作组网桥数量增至 20 个以上，接入点必须降低将多播数据包发送至工作组网桥的可靠性。随着可靠性的下降，接入点不能确认多播数据包是否到达目标工作组网桥，因此处于接入点覆盖范围边缘的工作组网桥会丢失 IP 连接。

当将工作组网桥视为客户端设备时，性能提高，但可靠性会降低。可使用非基础架构客户端配置接口命令来配置接入点和网桥，将工作组网桥作为简单的客户端设备。这是默认设置。

如果连接到工作组网桥的设备需要与接入点或网桥具有同等的网络可靠性，则将工作组网桥用作基础架构设备。如果这些条件为真，请将工作组网桥作为客户端设备：

- 有超过 20 个工作组网桥关联到同一接入点或网桥
- 工作组网桥采用非基础架构 SSID 进行 关联
- 工作组网桥为移动式 (例如不在固定位置)，且可能会在接入点之间漫游

将工作组网桥配置用于漫游

如果工作组网桥为移动式，则可将其配置为扫描与父接入点或网桥是否能建立更好的无线电连接。使用该命令，可将工作组网桥配置为移动工作站：

```
ap(config)# mobile station
```

当启用该设置时，如果工作组网桥遇到不理想的接收信号强度指标 (RSSI)、过多的无线电干扰或较高的失帧率时，其将扫描是否存在新的父级关联。使用这些标准，配置为移动工作站的工作组网桥将搜索新的父级关联，并在其丢失当前关联前漫游到新的父设备。当禁用移动工作站设置 (默认设置) 时，工作组网桥在丢失当前关联前不搜索新的关联。

将工作组网桥配置用于有限通道扫描

在铁路等移动环境中，当工作组网桥从一个接入点漫游到另一个接入点时，工作组网桥会被限制为仅扫描一组有限通道，而不是扫描所有通道，以降低手动关闭延迟。通过限制工作组网桥仅扫描一些必要通道，移动工作组网桥可实现并保持不间断的无线局域网连接，同时提供快速、顺畅的漫游。

配置有限通道组

该有限通道组使用移动工作站扫描 `<set of channels>` 命令进行配置，以触发扫描所有或指定通道。对于可配置的最大通道数量没有任何限制。可配置的最大通道数量仅受无线电装置支持的通道数量的限制。当执行后，工作组网桥仅扫描该有限通道组。此外，该有限通道特性也会影响工作组网桥从已关联接入点接收的已知通道列表。如果它们也是有限通道组的一部分，则只将通道添加到已知通道列表。

下例显示了如何使用命令。在本例中，通道 1、 6 和 11 被指定用于扫描：

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with
CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

使用 `no mobile station scan` 命令来恢复扫描所有通道。

忽略 CCX 邻居列表

此外，工作组网桥还使用 CCX 报告 (如相邻 AP 报告或增强邻居列表报告) 来更新其已知通道列表。但是，当将工作组网桥配置用于有限通道扫描时，它无需通过处理 CCX 报告来更新其已知通道列表。

使用移动工作站忽略邻居列表命令，以禁用对 CCX 邻居列表报告的处理。如果将工作组网桥配置为只用于有限通道扫描，该命令有效。本例显示了如何使用该命令

```
ap#

ap#confure terminal

Enter configuration commands, one per line.  End
with CNTL/Z.

ap(config)#int d0

ap(config-if)#mobile station ignore neighbor-list

ap(config-if)#end
```

工作组网桥 VLAN 标签

工作组网桥 (WGB) VLAN 标签功能便于根据统一 WGB 解决方案的 VLAN 数量来隔离 VLAN 流量。

当启用该功能时， WGB 会在从 VLAN 客户端向无线局域网控制器 (WLC) 发送数据包时删除 802.1q 报头。 WGB 会将不带 802.1q 报头的数据包发送到 VLAN 客户端，但当将帧转发到交换机后方的 WGB 时，必须向 WGB 代码添加 802.1q 报头。

WGB 使用互联网接入点协议 (IAPP) 协会消息中的有线客户端 VLAN 信息对 WLC 进行更新。 WLC 将 WGB 客户端作为 VLAN 客户端，并根据源 MAC 地址将数据包转发到正确的 VLAN 接口。

在上行方向， WGB 在发送到 WLC 时从数据包中删除 802.1q 报头。在下行方向，当将数据包转发到连接有线客户端的交换机时， WLC 将不带 802.1q 标签的数据包发送到 WGB，且 WGB 根据目标 MAC 地址添加 4 字节的 802.1q 报头。

有关 VLAN 的详细信息，请参见第 409 页的 “ 配置 VLAN”。

```
WGB(config)#workgroup-bridge unified-vlan-client
```

配置工作组网桥模式

在特权 EXEC 模式下，根据以下步骤将接入点配置为工作组网桥。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。

   ```
   interface dot11radio {0 | 1}
   ```

3. 设置到工作组网桥的无线电作用。如果接入点包含两个无线电装置，将自动禁用没有设为工作组网桥模式的无线电装置。

   ```
   station-role workgroup-bridge
   ```

4. 创建工作组网桥用于关联到父接入点或网桥的 SSID。

   ```
   ssid ssid-string
   ```

5. (可选) 如果父接入点被配置为需要 EAP 验证，则配置当工作组网桥执行 EAP 验证时使用的凭证配置文件。

   凭证配置文件中的用户名和密码必须与在验证服务器上为工作组网桥设置的用户名和密码一致。

   ```
   dot1x credentials profile-name
   ```

6. 退出 SSID 配置模式并返回无线电接口配置模式。

   ```
   exit
   ```

7. (可选) 输入需要关联到工作组网桥的接入点的 MAC 地址。
   - (可选) 最多可输入四个父接入点的 MAC 地址。工作组网桥首先尝试关联到 MAC 地址 1 ；如果该接入点未响应，则工作组网桥尝试其父级列表中的下一个接入点。当在父接入点上配置了多个 BSSID 时，如果添加或删除父设备上的 BSSID，则父设备的 MAC 地址可能变化。
   - (可选) 此外，也可输入以秒为单位的超时值，以确定工作组网桥在尝试列表中的下一个父设备之前尝试关联到父接入点的时间。输入 0... 65535 秒之间的超时值。

   ```
   parent {1-4} mac-address [timeout]
   ```

8. 退出无线电配置模式并返回全局配置模式。

   ```
   exit
   ```

9. (可选) 将工作组网桥配置为移动工作站。当启用该设置时，如果工作组网桥遇到不理想的接收信号强度指标 (RSSI)、过多的无线电干扰或较高的失帧率时，其将扫描是否存在新的父级关联。当禁用该设置 (默认设置) 时，工作组网桥在丢失其当前关联前不搜索新的关联。

   ```
   mobile station
   ```

10. 返回到特权 EXEC 模式。

    ```
    end
    ```

11. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

本例显示了如何将接入点配置为工作组网桥。在本例中，工作组网桥采用配置的凭证配置文件 EAP 配置文件来执行 EAP 验证。

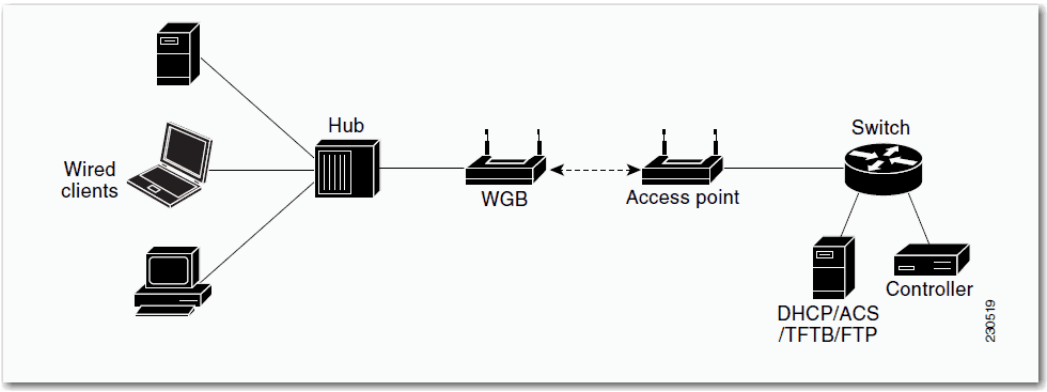
```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-if)# exit
AP(config)# dot11 ssid infra
AP(config-ssid)# dot1x credentials EAP-profile
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# end
```

在轻量环境中使用工作组网桥

可将接入点配置为工作组网桥，以便它能代表通过以太网连接到工作组网桥接入点的客户端提供到轻量接入点的无线连接。通过获知其有线客户端在以太网接口上的 MAC 地址，并通过使用互联网接入点协议 (IAPP) 消息将其报告给轻量接入点，工作组网桥可通过单独的无线网段连接到有线网络。

工作组网桥可通过建立到轻量接入点的单独连接来提供到有线客户端的无线接入连接。轻量接入点将工作组网桥作为无线客户端。

图 126 - 轻量环境中的工作组网桥



如果轻量接入点出现故障，工作组网桥将尝试关联到其他接入点。

轻量环境中的工作组网桥使用指南

在轻量网络中使用工作组网桥时请遵循这些指南。

- 工作组网桥可以是支持工作组网桥模式、并运行思科 IOS Release JA 或更高版本 (在 32-MB 接入点上) 的任何自主接入点。

  提示 如果接入点有两个无线电装置，则可只配置其中一个用于工作组网桥模式。该无线电装置用于连接到轻量接入点。我们建议您禁用第二个无线电装置。

执行下列操作之一，在工作组网桥上启用工作组网桥模式：

- 在工作组网桥接入点 GUI 的 Settings (设置) > Network Interfaces (网络接口) 页面上选择工作组网桥在无线电网络中的作用。
- 在工作组网桥接入点 CLI 上，输入该命令：`station-role workgroup-bridge`
- 仅支持客户端模式 (默认值) 下的工作组网桥。不支持基础架构模式下的工作组网桥。执行下列操作之一，在工作组网桥上启用客户端模式：
- 在工作组网桥接入点 GUI 上，将 Reliable Multicast to workgroup bridge (可靠多播到工作组网桥) 参数选为 Disabled (禁用)。
- 在工作组网桥接入点 CLI 上，输入该命令：`no infrastructure client`.

  提示 多 VLAN 和中继线不支持与工作组网桥一同使用。

- 与工作组网桥一同使用时，支持以下轻量功能：
  - 访客 N+1 冗余
  - 本地 EAP
- 与工作组网桥一同使用时，不支持以下轻量功能：
  - Idle Timeout (闲置超时)
  - Web 验证

  提示 如果工作组网桥关联到 Web 验证 WLAN，则将工作组网桥添加到排除列表，并删除所有工作组网桥有线客户端。

- 在网状网络中，工作组网桥可关联到任何轻量网状接入点，无论其作为根接入点还是网状接入点。
- 连接到工作组网桥的有线客户端不进行安全验证。相反，工作组网桥所连接的接入点将对其进行验证。因此，我们建议以物理方式固定工作组网桥的有线侧。
- 对于 3 层漫游，如果在工作组网桥已经漫游到另一个控制器 (例如外部控制器) 后将有线客户端插入到工作组网桥网络，则有线客户端的 IP 地址仅显示在锚控制器上，而不是外部控制器上。

- 当从控制器中删除工作组网桥记录时，也将删除工作组网桥有线客户端的所有记录。
- 连接到工作组网桥的有线客户端会继承工作组网桥的 QoS 和 AAA 覆盖属性。
- 连接到工作组网桥的有线客户端不支持以下功能：
  - MAC 过滤
  - 链路测试
  - Idle Timeout (闲置超时)
- 无需在控制器上配置任何内容，即可启用工作组网桥与轻量接入点通信。但是，为了确保正确通信，请在控制器上创建 WLAN，其要与在工作组网桥上配置的 SSID 和安全方法一致。

工作组网桥配置示例

下面是使用 WPA2-PSK 与预共享密钥的工作组网桥接入点的配置示例。

```
ap#confure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
ap(config) #dot11 ssid WGB-PSK
ap(config-ssid) #authentication open
ap(config-ssid) #authentication key-management wpa
version 2
ap(config-ssid) #wpa-psk ascii presharedkey
ap(config-ssid) #exit
ap(config) #interface dot11Radio 1
ap(config-if) #encryption mode ciphers aes-ccm
ap(config-if) #ssid WGB-PSK
ap(config-if) #station-role workgroup-bridge
ap(config-if) #end
```

要确认工作组网桥是否关联到接入点，请在工作组网桥上输入该命令：

```
show dot11 association
```

如果有线客户端在较长一段时间内未发送流量，工作组网桥将从其网桥表中删除客户端，即使流量连续发送到有线客户端。因此，向有线客户端输送流量的操作将会失败。为了避免流量损失，可通过将工作组网桥上的超时定时器配置为较大值，来防止将有线客户端从网桥表中删除。可在工作组网桥上使用以下 IOS 命令来实现这一目的：

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

其中， bridge-group-number 是介于 1...255 之间的值， seconds 是介于 10...1,000,000 秒之间的值。我们建议将 seconds 参数配置为大于有线客户端的空闲时间的值。

中继器接入点

中继器接入点未连接到有线局域网；其位于连接到有线局域网的接入点的无线电范围内，以扩展基础架构的范围或克服阻碍无线电通信的障碍。可将 2.4 GHz 无线电装置或 5 GHz 无线电装置配置为中继器。在带两个无线电装置的接入点中，只有一个接入点可配置为中继器；另一个接入点必须配置为根无线电。

中继器通过将数据包发送至另一个中继器或连接到有线局域网接入点，在无线用户和有线局域网之间转发流量。数据通过能为客户端提供最佳性能的路由进行发送。当将接入点配置为中继器时，接入点的以太网端口不转发流量。

您可设置中继器接入点链，但位于中继器链末端的客户端设备的吞吐量较低。由于每个中继器都必须接收然后在相同通道上重新发送每个数据包，您添加到链上的每个中继器的吞吐量减半。

中继器接入点关联到具有最佳连接的接入点。但是，您可指定与中继器关联的接入点。在中继器和根接入点之间设置静态的特定关联会提高中继器性能。

要设置中继器，必须在父 (根) 接入点和中继接入点上启用 Aironet 扩展。默认情况下启用 Aironet 扩展。这会提高接入点理解与接入点相关联的思科 Aironet 客户端设备的能力。禁用 Aironet 扩展有时会提高接入点和非思科客户端设备之间的互操作性。非思科客户端设备与中继器接入点及中继器所关联根接入点之间通信时有可能存在困难。

必须将基础架构 SSID 分配到本征 VLAN。如果在接入点或无线网桥上创建了多个 VLAN，则无法将基础架构 SSID 分配到非本征 VLAN。当在非本征 VLAN 上配置基础架构 SSID 时，会显示以下消息：

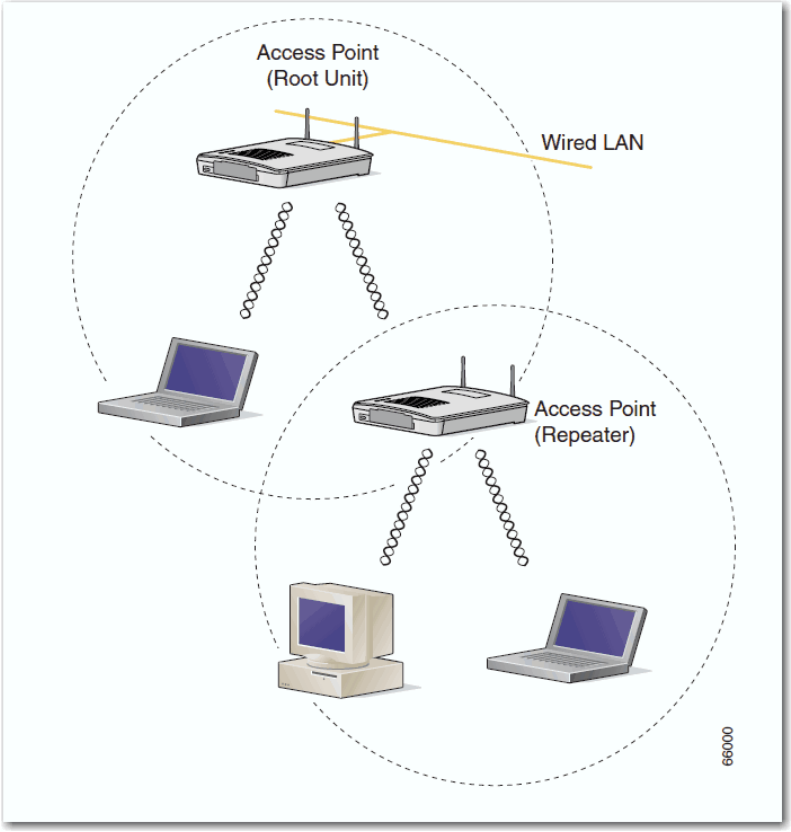
```
SSID [xxx] must be configured as native-vlan before
enabling infrastructure-ssid
```

提示 由于接入点为每个无线电接口都创建了虚拟接口，中继器接入点与根接入点关联两次：一次用于实际接口，一次用于虚拟接口。

您无法在中继器接入点上配置多个 VLAN。中继器接入点仅支持本征 VLAN。

下图显示了作为中继器的接入点。

图 127 - 作为中继器的接入点



配置中继器接入点

本节提供了将接入点设置为中继器的说明。

默认配置

默认情况下，接入点被配置为根单元。下表显示了用于控制接入点在无线局域网中的作用的默认设定值。

功能	默认设置
工作站作用	根
父	无
扩展	Aironet

中继器指南

在配置中继器接入点时应遵循这些指南：

- 使用中继器服务无需较高吞吐量的客户端设备。中继器可扩展无线局域网的覆盖区域，但会大大降低吞吐量。
- 当与中继器关联的客户端设备并非都是思科 Aironet 客户端时，使用中继器。非思科客户端设备与中继器接入点通信时有时会出现问题。
- 请确保在中继器接入点上配置的数据传输速率与父接入点上的数据传输速率匹配。关于配置数据传输速率的说明，请参见第 261 页的 “ 配置无线电数据传输 速率 ”。
- 中继器接入点仅支持本征 VLAN。无法在中继器接入点上配置多个 VLAN。

提示

运行思科 IOS 软件的中继器接入点无法关联到不运行思科 IOS 软件的父接入点。

中继器接入点不支持无线域服务 (WDS)。当以太网发生故障时，不得将中继接入点配置为候选 WDS，也不得将 WDS 接入点配置为返回到中继模式。

如果在指定为中继器父设备的根接入点上配置多个 BSSID，则当添加或删除父设备上的 BSSID 时，父设备的 MAC 地址可能会更改。如果在无线局域网上使用多个 BSSID 且无线局域网上的中继器被配置为关联到特定父设备，则当添加或删除父接入点上的 BSSID 时，请检查中继器的关联状态。如有必要，重新配置已解除关联的设备，以使用新的 BSSID MAC 地址。

设置中继器

在特权 EXEC 模式下，根据以下步骤将接入点配置为中继器。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 进入无线电接口的接口配置模式。

   – 2.4 GHz 802.11n 无线电类型为 0。

   – 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio { 0 | 1 }
   ```

3. 创建中继器用于关联到根接入点的 SSID ；在下一步中，将该 SSID 指定为基础架构 SSID。如果在根接入点上创建基础架构 SSID，则也在中继器上创建相同的 SSID。

   ```
   ssid ssid-string
   ```

4. 将 SSID 指定为基础架构 SSID。中继器使用该 SSID 关联到根接入点。基础架构设备必须使用该 SSID 关联到中继器接入点，除非也输入可选的关键字。

   必须将基础架构 SSID 分配到本征 VLAN。如果在接入点或无线网桥上创建了多个 VLAN，则无法将基础架构 SSID 分配到非本征 VLAN。当在非本征 VLAN 上配置基础架构 SSID 时，会显示以下消息：

   SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid

   ```
   infrastructure-ssid [optional]
   ```

5. 退出 SSID 配置模式并返回无线电接口配置模式。

   ```
   exit
   ```

6. 将无线局域网中的接入点的作用设置为中继器。

   ```
   station-role repeater
   ```

7. 如果 Aironet 扩展被禁用，请启用 Aironet 扩展。

   ```
   dot11 extensions aironet
   ```

8. (可选) 输入中继器应关联的接入点的 MAC 地址。

   最多可输入四个父接入点的 MAC 地址。中继器首先尝试关联到 MAC 地址 1 ；如果该接入点未响应，则中继器尝试位于其父级列表中的下一个接入点。

   当在父接入点上配置了多个 BSSID 时，如果添加或删除父设备上的 BSSID，则父设备的 MAC 地址可能变化。

(可选) 此外，也可输入以秒为单位的超时值，以确定中继器在尝试列表中的下一个父设备之前尝试关联到父接入点的时间。输入 0 至 65535 秒之间的超时值。

```
parent {1-4} mac-address [timeout]
```

9. 返回到特权 EXEC 模式。

```
end
```

10. (可选) 将您的输入保存到配置文件中。

```
copy running-config startup-config
```

本例显示了如何为中继器接入点设置三个潜在父设备。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

对齐天线

当将接入点配置为中继器时，您可使用 `dot11 antenna-alignment` 命令将其天线与另一个远程天线对齐。

该命令用于调用对齐测试。无线电装置与其父设备取消关联，检测邻近的无线设备，并记录 MAC 地址和收到的响应的信号强度。超时后，无线电装置与其父设备重新关联。

根据以下步骤运行天线对齐测试。

1. 进入特权 EXEC 模式。

```
Enable
```

2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   dot11 dot11radio { 0 | 1 }
   ```
3. 确立在超时之前运行天线对齐测试的时间 (以秒为单位)。默认值为 5 秒。

   ```
   antenna-alignment timeout
   ```

   使用 `show dot11 antenna-alignment` 命令列出响应探头的最近 10 台设备的 MAC 地址和信号级别。

确认中继器工作情况

在设置中继器之后，检查中继器接入点顶部上的状态指示灯。如果中继器正常工作，中继器和根接入点上的状态指示灯应该呈蓝色常亮。

中继器接入点显示为与根接入点关联表中的根接入点相关联。

将中继器设置 为 WPA 客户端

WPA 密钥管理使用加密方法组合来保护客户端设备和接入点之间的通信。您可将中继器接入点设置为像其他启用 WPA 的客户端设备一样进行网络验证。

在特权 EXEC 模式下，根据以下步骤将中继器设置为 WPA 客户端。

1. 进入全局配置模式。

   ```
   configure terminal
   ```
2. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio { 0 | 1 }
   ```
3. 创建一个 SSID，然后进入新 SSID 的 SSID 配置模式。

   SSID 最多由 32 个字母数字字符组成，但不包含空格。SSID 区分大小写。

   ```
   ssid ssid-string
   ```
4. 为 SSID 启用开放式验证。

   ```
   authentication open
   ```
5. 为 SSID 启用经 WPA 验证密钥管理。

   ```
   authentication key-management wpa
   ```
6. 将 SSID 指定为中继器用于关联到其他接入点的 SSID。

   ```
   infrastructure ssid
   ```

7. 输入中继器的预共享密钥。

   使用十六进制或 ASCII 字符输入密钥。如果使用十六进制，则必须输入 64 个十六进制字符，以完成 256 位密钥。如果使用 ASCII，必须输入 8...63 个 ASCII 字符，且接入点将为您扩展密钥。

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

8. 返回到特权 EXEC 模式。

   ```
   end
   ```

9. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

热备用

热备用模式可将接入点指定为另一个接入点的后备。备用接入点将被置于其所监控的接入点附近，其配置与被监控接入点完全相同。备用接入点与作为客户端的被监控接入点关联，并通过以太网和无线电端口向被监控接入点发送 IAPP 查询。如果被监控接入点未能响应，备用接入点将进入联机状态，在网络中取代被监控接入点的位置。

除 IP 地址外，备用接入点的设置可能与被监控接入点上的设置完全相同。如果被监控接入点离线，且备用接入点取代其在网络中的位置，设置一致可确保客户端设备能够轻松切换到备用接入点。

备用接入点以设备到设备的关系监控另一个接入点，而不是接口到接口的关系。例如，您无法将备用接入点的 5 GHz 无线电装置配置为监控接入点 α 中的 5 GHz 无线电装置，也无法将备用的 2.4 GHz 无线电装置配置为监控接入点 β 中的 2.4 GHz 无线电装置。此外，您无法将双无线电接入点中的某个无线电装置配置为备用无线电装置，将另一个无线电装置配置作为客户端设备。

提示　在默认情况下，热备用模式为禁用。

如果被监控接入点发生故障且备用接入点取代其位置，则当维修或更换被监控接入点时，请在备用接入点上重复热备用设置。备用接入点不会自动恢复到备用模式。

如果添加或删除被监控单元上的 BSSID，被监控接入点的 MAC 地址可能改变。如果在无线局域网上使用多个 BSSID，当添加或删除被监控接入点上的 BSSID 时，请检查备用单元的状态。如有必要，重新配置备用单元，以使用 BSSID 的新 MAC 地址。

配置热备用

当设置备用接入点时，必须输入备用单元所监控接入点的 MAC 地址。在配置备用接入点前，记录被监控接入点的 MAC 地址。

备用接入点必须在被监控接入点上复制数个密钥设置。这些设置是：

- 主 SSID (以及在被监控接入点上配置的其他 SSID)
- 默认 IP 子网掩码
- 默认网关
- 数据传输速率
- 加密设置
- 验证类型和验证服务器

如果被监控接入点离线，且备用接入点取代其在网络中的位置，设置一致可确保客户端设备能够轻松切换到备用接入点。检查被监控接入点，并在设置备用接入点前记录这些设置。

提示 与备用接入点关联的无线客户端设备在热备用设置过程中丢失连接。

使用 CLI 配置热备用接入点

当设置备用接入点时，必须输入备用单元所监控接入点的 MAC 地址。在配置备用接入点前，记录被监控接入点的 MAC 地址。

此外，备用接入点还必须在被监控接入点上复制几个密钥设置。这些设置是：

- 主 SSID (以及在被监控接入点上配置的其他 SSID)
- 默认 IP 子网掩码
- 默认网关
- 数据传输速率
- WEP 设置
- 验证类型和验证服务器

检查被监控接入点，并在设置备用接入点前记录这些设置。

重要事项　与备用接入点关联的无线客户端设备在热备用设置过程中丢失连接。

提示　要快速复制备用接入点上被监控接入点的设置，请将被监控接入点配置保存并将其加载至备用接入点上。

在特权 Exec 模式下，根据以下步骤在接入点上启用热备用模式。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 将接入点置于备用模式，并指定被监控接入点上无线电装置的 MAC 地址。

   当双无线电接入点配置为监控另一个双无线电接入点时，必须输入被监控 2.4 GHz 和 5 GHz 无线电装置的 MAC 地址。首先输入 2.4 GHz 无线电装置的 MAC 地址，然后是 5 GHz 无线电装置的 MAC 地址。

   如果添加或删除被监控单元上的 BSSID，被监控接入点的 MAC 地址可能改变。如果在无线局域网上使用多个 BSSID，当添加或删除被监控接入点上的 BSSID 时，请检查备用单元的状态。如有必要，重新配置备用单元，以使用 BSSID 的新 MAC 地址。

   ```
   iapp standby mac-address
   ```

3. 进入无线电接口的接口配置模式。
   - 2.4 GHz 802.11n 无线电类型为 0。
   - 5 GHz 802.11n 无线电类型为 1。

   ```
   interface dot11radio { 0 | 1 }
   ```

4. 创建备用接入点用于关联到被监控接入点的 SSID ；在下一步中，将该 SSID 指定为基础架构 SSID。如果在被监控接入点上创建基础架构 SSID，则也在备用接入点上创建相同的 SSID。

   ```
   ssid ssid-string
   ```

5. 将 SSID 指定为基础架构 SSID。备用接入点使用该 SSID 关联到被监控接入点。如果备用接入点取代被监控接入点的位置，基础架构设备必须使用该 SSID 关联到备用接入点，除非您也输入可选关键字。

   ```
   infrastructure-ssid [optional]
   ```

6. 如果被监控接入点配置为需要 LEAP 验证，则在其执行 LEAP 验证时配置备用接入点使用的用户名和密码。该用户名和密码必须与在验证服务器上为备用接入点设置的用户名和密码匹配。

   ```
   authentication client username username
   password password
   ```

7. 退出 SSID 配置模式并返回无线电接口配置模式。

   ```
   exit
   ```

8. 设置备用接入点向被监控接入点的无线电装置和以太网端口发送查询的间隔秒数。默认轮询频率是 2 秒。

   ```
   iapp standby poll-frequency seconds
   ```

9. 设置备用接入点等待的秒数，在此之后，如果被监控接入点仍未能响应，将认定被监控接入点发生故障。默认超时为 20 秒。

   如果备用和被监控接入点之间的桥接路径缺失的时间会超过 20 秒，请增大备用超时设置 (例如在生成树重新计算期间)。

   如果被监控接入点被配置为选择最不拥挤的无线电通道，便可增加备用超时设置。被监控单元最多有 40 秒的时间来选择最不拥挤的通道。

   ```
   iapp standby timeout seconds
   ```

10. (可选) 配置备用接入点，使其在备用单元激活时向被监控接入点发送 Dumb Device Protocol (DDP) 消息，以禁用被监控接入点的无线电装置。该功能将阻止关联到被监控接入点的客户端设备保持与故障设备的关联。

    ```
    iapp standby primary-shutdown
    ```

11. 确认您的输入。
    - 如果接入点处于备用模式，则显示备用参数，包括被监控接入点的 MAC 地址、轮询频率和超时值。
    - 如果接入点不处于备用模式，将显示 `no iapp standby mac-address` 消息。

    ```
    show iapp standby-parms
    ```

12. 返回到特权 EXEC 模式。

    ```
    end
    ```

13. (可选) 将您的输入保存到配置文件中。

    ```
    copy running-config startup-config
    ```

在启用备用模式之后，配置从被监控接入点记录的设置，以与备用接入点上的设置相匹配。

确认备用设备工作情况

使用该命令，检查备用接入点的状态：

```
show iapp standby-status
```

该命令可提供备用接入点的状态。该表列出了可能显示的备用状态消息。

表 113 - 备用状态消息

消息	描述
备用 IAPP 被禁用	接入点未被配置用于备用模式。
IAPP —— AP 处于备用模式	接入点处于备用模式。
IAPP —— AP 工作在活动模式下	备用接入点已接管受监控接入点，并作为根接入点工作。
IAPP —— AP 工作在中继器模式下	备用接入点已接管受监控接入点，并作为中继器接入点工作。
备用状态：正在初始化	备用接入点正在初始化受监控接入点的链路测试。
备用状态：接管	备用接入点已切换为活动模式。
备用状态：已停止	备用模式已由配置命令停止。
备用状态：以太网链路测试失败	从备用接入点到受监控接入点的以太网链路测试失败。
备用状态：无线电链路测试失败	从备用接入点到受监控接入点的无线电链路测试失败。
备用状态：备用错误	发生未定义错误。
备用状态：初始化	备用接入点正在初始化受监控接入点的链路测试。
备用状态：正在运行	备用接入点正工作在备用模式下，并正在运行至受监控接入点的链路测试。
备用状态：已停止	备用模式已由配置命令停止。
备用状态：未运行	接入点未处于备用模式。

使用该命令，可检查备用配置：

```
show iapp standby-parms
```

该命令可提供备用接入点的 MAC 地址、备用超时和轮询频率值。如果未配置任何备用接入点，将显示该消息：

```
no iapp standby mac-address
```

如果备用接入点接管被监控接入点，则可使用 show iapp statistics 命令来帮助确定备用接入点接管的原因。

备注：

配置系统消息记录

本章描述了如何配置接入点上的系统消息记录。

如需了解本章中使用的命令的完整语法和用法信息，请参见 Cisco IOS Security Command Reference for Release 12.3 (思科 IOS 安全命令参考，第 12.3 版)。

系统消息记录

默认情况下，接入点将系统消息和 `debug privileged EXEC` 命令的输出结果发送到记录进程。根据您的配置，记录进程就将记录消息分配给各目标地址进行控制，例如，日志缓冲区、终端线路或 UNIX syslog 服务器。该进程还将消息发送给控制台。

提示 syslog 格式与 4.3 BSD UNIX 兼容。

当禁用记录进程后，只能将消息发送给控制台。消息生成后随即被发出，因此，消息和调试输出中穿插了提示或其他命令的输出。在生成消息的进程完成后，在控制台上显示消息。

可设置消息的严重性等级，据此控制在控制台上显示的消息类型以及各目标地址。可对日志消息添加时间戳，或设置 syslog 源地址以增强实时调试和管理性能。

可使用接入点命令行界面 (CLI) 或将消息保存到一个正确配置的 syslog 服务器，访问已记录的系统消息。接入点软件在一个内部缓冲区中保存 syslog 消息。您可通过 Telnet 访问接入点或查看 syslog 服务器上的日志，从而远程监控系统消息。

配置系统消息记录

本节描述如何配置系统消息记录。系统日志消息可包含多达 80 个字符和一个百分比符号 (%)，之后跟随可选的序号或时间戳信息 (若已配置)。采用以下格式显示消息：

```
seq no:timestamp: %facility-severity-
MNEMONIC:description
```

百分号之前的消息部分取决于全局配置命令的设置：

```
service sequence-numbers, service timestamps log
datetime, service timestamps log datetime
[localtime] [msec] [show-timezone], or service
timestamps log uptime
```

下表给出了 syslog 消息的元素。

表 114 - 系统日志消息元素

元素	描述
序号	只有在配置了 service sequence-numbers **全局配置命令**时，才能给日志消息标记一个序号。 更多信息，请参见第 503 页的 " 启用和禁用日志消息中的序号 "。
时间戳格式： *mm/dd hh:mm:ss* 或 *hh:mm:ss* (short uptime) 或 *d h* (long uptime)	消息或事件的日期和时间。只有在配置了 service timestamps log [datetime | log] 全局配置命令时才显示此信息。 更多信息，请参见第 502 页的 " 启用和禁用日志消息上的时间戳 "。
设施	即消息所指的设施，例如， SNMP、 SYS。 设施可以是硬件设备、协议或系统软件的一个模块。其表示了系统消息的来源或原因。
严重性	0...7 范围内的单位代码表示消息的严重性。有关严重性等级的描述，请参见第 505 页的表 116。
助记符	唯一描述消息的文本字符串。
描述	包含所报告事件详细信息的文本字符串。

本例显示了一条接入点系统消息的一部分：

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1,
changed state to up

00:00:47: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up

00:00:47: %LINK-3-UPDOWN: Interface
GigabitEthernet0/2, changed state to up

00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, changed state to down

00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to down
2

*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from
console by vty2 (10.34.195.36)

18:47:02: %SYS-5-CONFIG_I: Configured from console
by vty2 (10.34.195.36)

*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I:
Configured from console by vty2 (10.34.195.36)
```

默认系统消息记录配置

下表显示了默认系统消息记录配置。

表 115 - 默认系统消息记录配置

功能	默认设置
记录到控制台的系统消息	启用
控制台严重性	调试 (及更低等级；请参见第 505 页的表 116)
记录缓冲区大小	4096 字节
记录历史大小	1 条消息
时间戳	禁用
同步记录	禁用
记录服务器	禁用
Syslog 服务器 IP 地址	未配置
服务器设施	Local7 (参见第 510 页的表 117)
服务器严重性	信息 (及更低的数字等级；参见第 505 页的表 116)

禁用和启用消息记录

默认情况下启用消息记录。必须启用消息记录，方可将消息发送到除控制台外的任何目标地址。启用后，日志消息发送到记录进程，随后进程将消息记录到指定的位置，这与生成消息的进程异步执行。

在特权 EXEC 模式下，根据以下步骤禁用消息记录。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 禁用消息记录。

   ```
   no logging on
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

   或

   ```
   show logging
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

禁用记录进程会减慢接入点执行速度，因为在将消息写入到控制台之前，进程必须等待将消息写入后才能继续执行。当禁用记录进程时，一旦生成消息，立即在控制台上显示消息，通常出现在命令输出的中间。

`logging synchronous` 全局配置命令也会影响控制台上消息的显示。当启用此命令时，只有在按下 Return (返回) 后才会显示消息。更多信息，请参见第 502 页的 “ 启用和禁用日志消息上的时间戳 ”。

要在禁用后重新启用消息记录，使用 `logging on` 全局配置命令。

设置消息显示目标设备

如果启用了消息记录，则除了将消息发送到控制台外，还可将消息发送至特定的位置。在特权 EXEC 模式下，您可使用以下一个或多个命令指定接收消息的位置。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

   将消息记录到一个内部缓冲区。默认缓冲区大小是 4096。范围为 4096...2147483647 字节。等级包括紧急 0、报警 1、临界 2、错误 3、警告 4、通知 5、信息 6 及调试 7。

   提示 缓冲区大小不能太大，因为接入点可能因其他任务出现内存不足。使用 show memory 特权 EXEC 命令查看接入点上的空闲处理器内存；但是，该值是最大可用值，不得将缓冲区大小设为这一数值。

   ```
   logging buffered [size] [level]
   ```

2. 将消息记录到 UNIX syslog 服务器主机。

   对于 `host`，指定要用作 syslog 服务器的主机的名称或 IP 地址。

   要创建接收记录消息的 syslog 服务器列表，输入以下命令一次以上。

   有关完整的 syslog 服务器配置步骤，请参见第 508 页的 “ 配置 UNIX Syslog 服务器 ”。

   ```
   logging host
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 在当前会话期间将消息记录到一个非控制台终端。

   终端参数设置命令在本地设置，在会话结束后不再有效。必须为每个会话执行以下步骤，查看调试消息。

   ```
   terminal monitor
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

logging buffered 全局配置命令将记录消息复制到一个内部缓冲区。缓冲区为环形，因此在缓冲区已满时，较新的消息覆盖较早的消息。

- 要显示在缓冲区中记录的消息，使用 show logging 特权 EXEC 命令。所显示的第一条消息是缓冲区中最早的消息。
- 要清除缓冲区的内容，使用 clear logging 特权 EXEC 命令。
- 要禁止记录到控制台，使用 no logging console 全局配置命令。
- 要禁止记录到文件，使用 no logging file [severity-level-number | type] 全局配置命令。

启用和禁用日志消息上的时间戳

默认情况下，不对日志消息加时间戳。

在特权 EXEC 模式下，根据以下步骤允许对日志消息加时间戳。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用日志时间戳。

   第一条命令允许对日志消息加时间戳，显示自系统重启后的时间。

   第二条命令允许对日志消息加时间戳。根据所选的选项，时间戳可包括相对于当地时区的日期和时间 (毫秒) 以及时区名称。

   ```
   service timestamps log uptime
   ```

   或

   ```
   service timestamps log datetime [msec] [localtime]
   [show-timezone]
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 为了禁用调试和日志消息的时间戳，使用 `no service timestamps` 全局配置命令。
- 本例显示了启用 `service timestamps log datetime` 全局配置命令时的部分记录显示：

  ```
  *Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from
  console by vty2 (10.34.195.36)
  ```

- 本例显示了启用 `service timestamps log uptime` 全局配置命令时的部分记录显示：

  ```
  00:00:46: %LINK-3-UPDOWN: Interface Port-channel1,
  changed state to up
  ```

启用和禁用日志消息中的序号

由于可能存在多个日志消息具有相同时间戳的情况，可通过序号显示消息，从而可以明确指向某条消息。默认情况下，不显示日志消息中的序号。

在特权 EXEC 模式下，根据以下步骤在日志消息中启用序号。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用序号。

   ```
   service sequence-numbers
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. 确认您的输入。

   ```
   show running-config
   ```

5. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要禁用序号，使用 `no service sequence-numbers` 全局配置命令。
- 本例显示了启用序号时的部分记录显示：

  ```
  000019: %SYS-5-CONFIG_I: Configured from console by
  vty2 (10.34.195.36)
  ```

定义消息严重性等级

通过指定消息的严重性等级，可显示选定设备显示的消息，该部分内容在第 505 页的表 116 中描述。指定等级使得在目标地址显示该等级及更低等级的消息。

在特权 EXEC 模式下，根据以下步骤定义消息严重性等级。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 限制记录到控制台的消息。

   默认情况下，控制台接收调试消息及更低等级的消息 (参见第 505 页的表 116)。

   ```
   logging console level
   ```

3. 限制记录到终端线路的消息。

   默认情况下，终端接收调试消息及更低等级的消息 (参见第 505 页的表 116)。

   ```
   logging monitor level
   ```

4. 限制记录到 syslog 服务器的消息。

   默认情况下， syslog 服务器接收信息消息及更低等级的消息 (参见第 505 页的表 116)。

   有关完整的 syslog 服务器配置步骤，请参见第 508 页的 “ 配置 UNIX Syslog 服务器 ”。

   ```
   logging trap level
   ```

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. 确认您的输入。

   ```
   show running-config
   ```

   或

   ```
   show logging
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要禁止记录到控制台，使用 `no logging console` 全局配置命令。
- 要禁止记录到非控制台的终端，使用 `no logging monitor` 全局配置命令。
- 要禁止记录到 syslog 服务器，使用 `no logging trap` 全局配置命令。

下表描述了 *level* 关键字。它还列出了从最严重等级到最轻等级对应的 UNIX syslog 定义。

表 116 - 消息记录等级关键字

等级关键字	等级	描述	Syslog 定义
紧急	0	系统不稳定	LOG_EMERG
警报	1	需立即采取措施	LOG_ALERT
临界	2	临界状况	LOG_CRIT
错误	3	错误情况	LOG_ERR
警告	4	警告状况	LOG_WARNING
通知	5	正常但重要的状况	LOG_NOTICE
信息	6	仅信息消息	LOG_INFO
调试	7	调试消息	LOG_DEBUG

软件生成四种消息类别：

- 关于软件或硬件故障的错误消息，在从**警告**到**紧急**的各不同等级上显示。以下消息类型表示受影响的接入点功能。
- `debug` 命令的输出结果，在**调试**等级显示。调试命令通常只能由技术支持中心 (TAC) 使用。
- 接口开启或关闭跳转及系统重启动消息，在**通知**等级显示。以下消息仅用于提供信息；不影响接入点功能。
- 重新加载请求和低进程堆栈消息，在**信息**等级显示。以下消息仅用于提供信息；不影响接入点功能。

提示 验证请求日志消息不会记录到 syslog 服务器上。思科 Aironet 接入点不支持该功能。

限制发送至历史表和 SNMP 的 Syslog 消息

如果使用 `snmp-server enable trap` 全局配置命令允许将 syslog 消息陷阱发送至 SNMP 网络管理站，则可更改已发送且存储在接入点历史表中的消息等级。此外，还可更改存储在历史表中的消息数目。

消息存储在历史表中，因为不能确保 SNMP 陷阱到达目标地址。默认情况下，即使 syslog 陷阱未启用，也将等级为 `warning` 及更低等级的消息 (参见第 505 页的表 116) 存储在历史表中。

在特权 EXEC 模式下，根据以下步骤更改等级和历史表大小的默认值。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 更改存储在历史文件中且发送至 SNMP 服务器的 `syslog` 消息的默认等级。

   请参见第 505 页的表 116，了解关于等级关键字列表的信息。

   默认情况下，发送**警告**、**错误**、**临界**、**报警**和**紧急**消息。

   ```
   logging history level
   ```

   指定可存储在历史表中的 `syslog` 消息的数目。默认值是存储一条消息。范围是 1...500 条消息。

   ```
   logging history size number
   ```

3. 指定可存储在历史表中的 syslog 消息的数目。

   默认值是存储一条消息。范围是 1...500 条消息。

   ```
   logging history size number
   ```

4. 返回到特权 EXEC 模式。

   ```
   end
   ```

5. 确认您的输入。

   ```
   show running-config
   ```

6. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

当历史表已满 (它包含通过 `logging history size` 全局配置命令指定的最大消息条目数)，从表中删除最早的消息条目，以便存储新的消息条目。

要将 syslog 消息记录返回默认等级，使用 `no logging history` 全局配置命令。要将历史表中的消息数目返回默认值，使用 `no logging history size` 全局配置命令。

设置记录速率限制

可对接入点每秒记录的消息数目设置限定值。可对所有消息或对发送至控制台的消息设置限定值，且可指定不限制具有特定严重性的消息。要禁止速率限制，使用 `no logging rate-limit` 全局配置命令。

在特权 EXEC 模式下，根据以下步骤启用记录速率限制。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 启用以秒为单位的记录速率限制。
   - (可选) 将限制应用于所有记录或仅记录到控制台的消息。
   - (可选) 不限制具有特定严重性的消息。

   ```
   logging rate-limit seconds
   [all | console]
   [except severity]
   ```

3. 返回到特权 EXEC 模式。

   ```
   end
   ```

4. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

配置 UNIX Syslog 服务器

后续章节描述了如何配置 4.3 BSD UNIX 守护进程以及定义 UNIX 系统记录设施。

将消息记录到UNIX Syslog 守护进程

将系统日志消息发送至 UNIX syslog 服务器之前，必须在 UNIX 服务器上配置 syslog 守护进程。作为根节点登陆，然后执行以下步骤。

提示 某些最新版本的 UNIX syslog 守护程序默认情况下不再接受来自网络的 syslog 数据包。如果您的系统属于此类情况，则使用 UNIX man syslogd 命令确定必须从 syslog 命令行中添加或删除哪些选项，以允许记录远程 syslog 消息。

1. 向文件 /etc/syslog.conf 添加如下所示的命令行：

   ```
   local7.debug /usr/adm/logs/cisco.log
   ```

   `local7` 关键字指定要使用的记录设施；有关设施的信息，请参见第 510 页的表 117。`debug` 关键字指定 syslog 等级，有关严重性等级的信息，请参见第 505 页的表 116。 syslog 守护程序将处于此等级或更严重等级的消息发送至下一个域中指定的文件。文件必须已存在， syslog 守护程序必须具有此文件的写权限。

2. 在 UNIX shell 提示符中输入以下命令，创建日志文件：

   ```
   $ touch /usr/adm/log/cisco.log
   $ chmod 666 /usr/adm/log/cisco.log
   ```

3. 输入以下命令，确保 syslog 守护进程读取最新更改：

   ```
   $ kill -HUP `cat /etc/syslog.pid`
   ```

如需了解更多信息，请参见 UNIX 系统上的 `man syslog.conf` 和 `man syslogd` 命令。

配置UNIX 系统记录设施

将系统日志消息发送至外部设备时，会使接入点将消息识别为来自任何一个 UNIX syslog 设施。

在特权 EXEC 模式下，根据以下步骤配置 UNIX 系统设施消息记录。

1. 进入全局配置模式。

   ```
   configure terminal
   ```

2. 输入 IP 地址，将消息记录到 UNIX syslog 服务器主机。

   要创建接收记录消息的 syslog 服务器列表，输入以下命令一次以上。

   ```
   logging host
   ```

3. 限制记录到 syslog 服务器的消息。

   默认情况下， syslog 服务器接收信息消息及更低等级的消息。

   ```
   logging trap level
   ```

   请参见第 505 页的表 116，了解关于 level 关键字的信息。

4. 配置 syslog 设施。

   默认值为 `local7`。

   ```
   logging facility facility-type
   ```

   请参见第 510 页的表 117，了解 facility-type 关键字的信息。

5. 返回到特权 EXEC 模式。

   ```
   end
   ```

6. 确认您的输入。

   ```
   show running-config
   ```

7. (可选) 将您的输入保存到配置文件中。

   ```
   copy running-config startup-config
   ```

- 要删除 syslog 服务器，使用 `no logging host global` 配置命令，并指定 syslog 服务器 IP 地址。
- 要禁止记录到 syslog 服务器，输入 `no logging trap` 全局配置命令。

下表列出了思科 IOS 软件支持的 4.3 BSD UNIX 系统设施。如需了解关于这些设施的更多信息，请参见 UNIX 操作系统的操作手册。

表 117 - 记录设施类型关键字

设施类型关键字	描述
auth	授权系统
cron	Cron 设施
daemon	系统守护程序
kern	内核
local0-7	本地定义的消息
lpr	行式打印机系统
mail	邮件系统
news	USENET 新闻
sys9	系统使用
sys10	系统使用
sys11	系统使用
sys12	系统使用
sys13	系统使用
sys14	系统使用
Syslog	系统日志
User	用户进程
uucp	UNIX 到 UNIX 复制系统

显示记录配置

要显示当前记录配置和日志缓冲区的内容，使用 `show logging` 特权 EXEC 命令。

有关该画面中各域的信息，请参见出版物 Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference (思科 IOS 配置基础命令参考及思科 IOS IP 和 IP 路由命令参考)。

要显示记录历史文件，使用 `show logging history` 特权 EXEC 命令。

故障处理

本章介绍了无线接入点 / 工作组网桥出现基本故障时的故障处理步骤。

如需了解最新最全面的故障处理信息，请参见思科 TAC 网站， URL 地址为 (选择 Top Issues (重要问题)，然后选择 Wireless Technologies (无线技术))：http://www.cisco.com/tac

检查状态指示灯。

如果您的无线设备无法进行通信，请检查无线接入点 / 工作组网桥顶部的状态指示灯。

详细说明请参见第 46 页的 “ 接入点状态指示灯 ”。

检查基本设置

基本设置不匹配是无线客户端连接丢失的最常见原因。如果无线设备无法与客户端设备通信，检查本节所描述的区域。

SSID

尝试与无线设备关联的无线客户端必须与无线设备使用相同的 SSID。如果客户端设备的 SSID 与无线范围内无线设备的 SSID 不匹配，客户端设备将无法关联。

预共享密钥

如果使用预共享密钥配置 WPA2 密钥管理，则根 AP 和客户端 (或工作组网桥) 需要将密钥配置为相同的值。

更多信息，请参见第 331 页的 “ 配置密文组 ”。

安全设置

尝试与无线设备的验证的无线客户端必须支持无线设备中配置的相同安全选项，例如， EAP 或 LEAP、 MAC 地址验证、消息完整性检查 (MIC) 和 802.1X 协议版本等。

如果您的无线客户端使用的是 EAP-FAST 验证，则必须配置开放式验证 + EAP 验证。如果未配置开放式验证 + EAP 验证，将会显示警告消息。如果使用的是 CLI，则将显示下列警告消息：

> SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP can also be configured (SSID 配置警告：[SSID]：如果无线客户端使用的是 EAP-FAST，则也必须配置开放式验证 + EAP)。

如果使用的是 GUI，则将显示该警告消息：

> 警告：
> 网络 EAP 仅用于 LEAP 验证。如果将无线电客户端配置为使用 EAP-FAST 验证，则也可配置开放式验证 + EAP。

如果无线客户端无法与无线设备进行验证，请联系系统管理员，获取客户端适配器的正确安全设置，以及与无线设备设置兼容的客户端适配器驱动程序和固件版本。

提示 在 Aironet 客户端实用工具 (ACU) 中， Status (状态) 页面中显示的无线设备 MAC 地址是无线设备无线接口的 MAC 地址。接入点以太网端口的 MAC 地址打印在接入点背部的标签上。

复位到默认配置

如果忘记了配置无线设备所需的密码，则需要完全复位配置。

重要事项 下列步骤将所有配置设置复位到出厂默认值，包括密码、安全设置、IP 地址和 SSID。默认用户名为 “ 空白域 ”，密码为 wirelessap。密码区分大小写。

模式按钮

根据以下步骤使用模式按钮删除当前的配置，将接入点的所有设置恢复到出厂默认值。

1. 断开接入点的电源 (外部电源的电源插座或内部电源的以太网电缆)。
2. 按下并按住模式按钮，同时重新连接接入点的电源。
3. 按住模式按钮，直到状态指示灯变为红色 (约 20...30 秒)，然后松开按钮。
4. 在接入点重启后，必须使用 Web 浏览器界面或 CLI 重新配置接入点。

提示 接入点将使用出厂默认值进行配置，包括设为使用 DHCP 接收 IP 地址的 IP 地址。默认用户名为空白，密码为 wirelessap (区分大小写)。

Web 浏览器界面

根据以下步骤使用 Web 浏览器界面删除当前的配置，将无线设备的所有设置恢复到出厂默认值。

1. 打开 Internet 浏览器。必须使用 Microsoft Internet Explorer (版本 6.x 或更高版本) 或 Netscape Navigator (版本 7.x 或更高版本)。
2. 在浏览器地址行中输入无线设备 IP 地址并按下回车键。

   将显示 Enter Network Password (输入网络密码) 画面。
3. 在 User Name (用户名) 域中输入用户名。
4. 在 Password (密码) 域中输入无线设备密码并按下回车键。

   将显示 Summary Status (概要状态) 页面。
5. 单击 System Software (系统软件)。

   将显示 System Software (系统软件) 画面。
6. 单击 System Configuration (系统配置)。

   将显示 System Configuration (系统配置) 画面。
7. 单击 Reset to Defaults (复位到默认值) 或 Reset to Defaults (Except IP) (复位到默认值 (IP 地址除外))。
8. 如果要保留静态 IP 地址，选择 Reset to Defaults (Except IP) (复位到默认值 (IP 地址除外))。
9. 单击 Restart (重新启动)。

   系统将重新启动。
10. 在无线设备重新启动后，必须使用 Web 浏览器界面或 CLI 命令重新配置无线设备。

    默认用户名为空，密码为 wirelessap (区分大小写)。

使用 CLI 复位出厂默认值

根据以下步骤使用 CLI 命令删除当前的配置，将无线设备的所有设置恢复到出厂默认值。

1. 使用 Telnet 会话打开 CLI，或使用控制台端口连接到无线设备。
2. 断开再重新接通电源，重新启动无线设备。

   等待无线设备启动，直到显示命令提示符，且无线设备开始解压映像。该过程可能需要一分钟。

   当在 CLI 上看到以下命令行时，按下 Esc 键。

   ```
   Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/
   c350-k9w7-mx.v122_13_ja.20031010"
   ...##################################################
   ############################
   ##################################################
   ############################
   ##################################################
   ############################
   ####################
   ```

3. 在 ap: 提示符位置，输入 `flash_init` 命令来初始化闪存。

   ```
   ap: flash_init
   Initializing Flash...
   flashfs[0]: 142 files, 6 directories
   flashfs[0]: 0 orphaned files, 0 orphaned
   directories
   flashfs[0]: Total bytes: 7612416
   flashfs[0]: Bytes used: 3407360
   flashfs[0]: Bytes available: 4205056
   flashfs[0]: flashfs fsck took 0 seconds.
   ...done initializing Flash.
   ```

4. 使用 `dir flash:` 命令显示闪存中的内容，查找 config.txt 配置文件。

   ```
   ap: dir flash:
   Directory of flash:/
   3 .rwx 223 <date> env_vars
   4 .rwx 2190 <date> config.txt
   5 .rwx 27 <date> private.config
   150 drwx 320 <date> c350.k9w7.mx.122.13.JA
   4207616 bytes available (3404800 bytes used)
   ```

5. 使用 `rename` 命令将 config.txt 文件名称更改为 config.old。

   ```
   ap: rename flash:config.txt flash:config.old
   ```

6. 使用 reset 命令重新启动无线设备。

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
   using eeprom values
WRDTR,CLKTR: 0x80000800 0x80000000
RQDC ,RFDC : 0x80000033 0x000001cb
   ddr init done
IOS Bootloader - Starting system.
Xmodem file system is available.
DDR values used from system serial eeprom.
WRDTR,CLKTR: 0x80000800, 0x80000000
RQDC, RFDC : 0x80000033, 0x000001cb
```

7. 当接入点完成软件重启后，建立到接入点的新的 Telnet 会话。

   无线设备将使用出厂默认值进行配置，包括 IP 地址 (设置为使用 DHCP 接收 IP 地址)、默认用户名 (空白) 和密码 (wirelessap)。

8. 当加载 IOS 软件后，您可使用 del **特权** EXEC 命令从闪存中删除 config.old 文件。

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

重新加载接入点映像

如果无线设备发生固件故障，则必须使用 Web 浏览器界面或按下并按住模式按钮约 30 秒，重新加载映像文件。如果无线设备固件仍完全正常且您想要升级固件映像，您可使用浏览器界面。但如果接入点的固件映像已损坏，则必须使用模式按钮。在这种情况下，您必须通过 Telnet 或控制台端口连接使用 CLI 重新加载映像文件。

HTTP 接口

您还可使用 Web 浏览器界面重新加载无线设备映像文件。 Web 浏览器界面支持使用 HTTP 或 TFTP 界面加载映像文件。

提示 当使用浏览器重新加载映像文件时，并不更改无线设备的配置。

通过 HTTP 界面，您可浏览到计算机上的无线设备映像文件，将映像文件下载到无线设备。根据以下说明使用 HTTP 界面。

1. 打开 Internet 浏览器。

   必须使用 Microsoft Internet Explorer (版本 6.x 或更高版本) 或 Netscape Navigator (版本 7.x)。

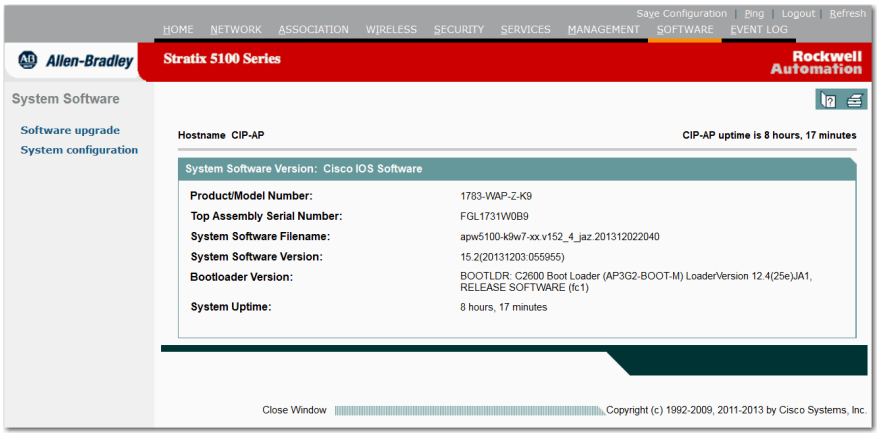
2. 在浏览器地址行中输入无线设备 IP 地址并按下回车键。

   将显示 Enter Network Password (输入网络密码) 画面。

3. 输入用户和密码，并单击回车键。

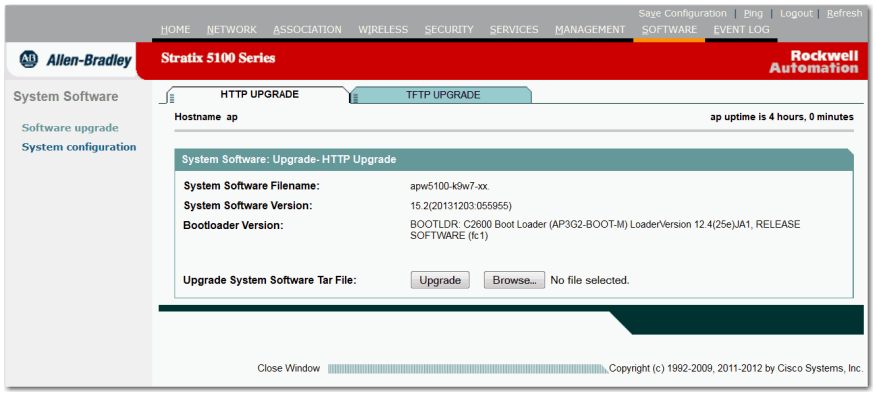
4. 单击 System Software (系统软件) 选项卡。

   将显示 Summary Status (概要状态) 页面。



5. 单击 Software Upgrade (软件升级)。

   将显示 HTTP Upgrade (HTTP 升级) 画面。



6. 浏览到计算机上的映像文件。
7. 单击 Upload (上传)。

TFTP 接口

通过 TFTP 界面，您可使用网络设备上的 TFTP 服务器来加载无线设备映像文件。根据以下说明来使用 TFTP 服务器 .

1. 打开 Internet 浏览器。

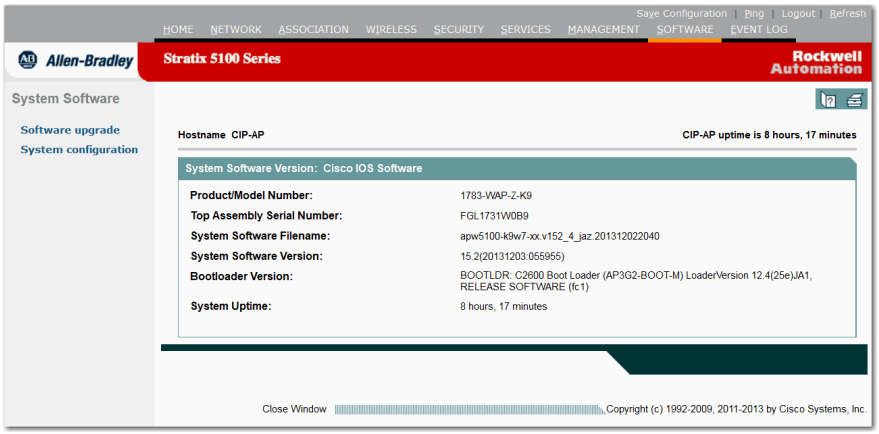
   必须使用 Microsoft Internet Explorer (版本 6.x 或更高版本) 或 Netscape Navigator (版本 7.x)。

2. 在浏览器地址行中输入无线设备 IP 地址并按下回车键。

   将显示 Enter Network Password (输入网络密码) 画面。

3. 输入用户和密码，并单击回车键。

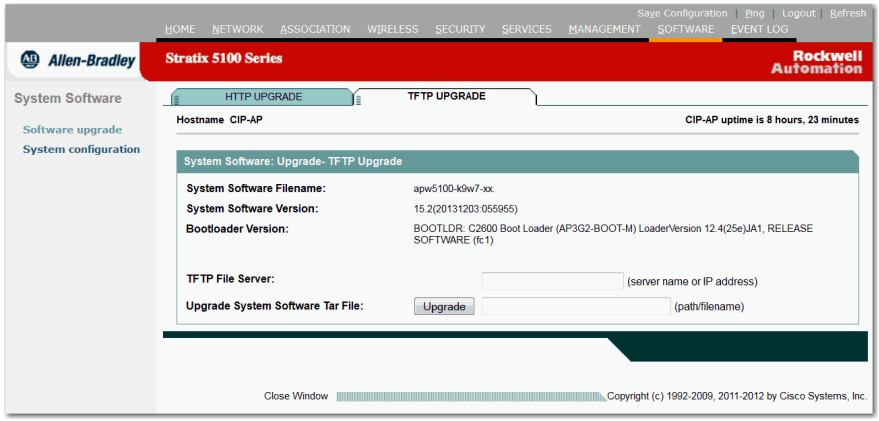
4. 单击 System Software (系统软件) 选项卡。



5. 单击 Software Upgrade (软件升级)。

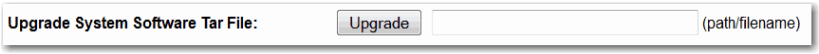
   将显示 HTTP Upgrade (HTTP 升级) 画面。

6. 单击 TFTP Upgrade (TFTP 升级) 选项卡。



7. 在 TFTP Server (TFTP 服务器) 域中，输入 TFTP 服务器的 IP 地址。

8. 在 Upload New System Image Tar File (上传新系统映像 Tar 文件) 域中，输入映像文件的文件名。



   - 如果文件位于 TFTP 服务器根目录的子目录中，将在文件名中包括 TFTP 服务器根目录的相对路径。
   - 如果文件位于 TFTP 根目录中，则只需输入文件名。

9. 单击 Upload (上传)。

CLI

根据以下说明使用 CLI 命令重新加载无线设备映像。当无线设备开始启动时，您可中断启动过程，使用引导加载程序命令从 TFTP 服务器加载映像，替换接入点中的映像。

提示 当使用 CLI 重新加载映像文件时，并不更改无线设备的配置。

1. 使用到无线设备控制台端口的连接启动 CLI。
2. 断开再重新接通电源，重新启动无线设备。
3. 等待无线设备启动，直到其开始解压映像。当在 CLI 上看到以下命令行时，按下 Esc 键。

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/
c350-k9w7-mx.v122_13_ja.20031010"
...##################################################
############################
##################################################
############################
##################################################
############################
####################
```

4. 当显示 ap: 命令提示符时，输入 **set** 命令，为无线设备分配 IP 地址、子网掩码和默认网关。

提示 当使用 set 命令输入 IP-ADDR (IP 地址)、NETMASK (网络掩码) 和 DEFAULT_ROUTER (默认路由器) 选项时，必须使用大写字符。

输入内容类似于下例：

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

5. 输入 `tftp_init` 命令，准备无线设备进行 TFTP 连接。

```
ap: tftp_init
```

6. 输入 `tar` 命令从 TFTP 服务器加载并解压新映像。

   命令必须包括以下信息：

- -xtract 选项，加载后解压映像
- TFTP 服务器的 IP 地址
- TFTP 服务器上包含映像的目录
- 映像名称
- 映像目标 (无线设备闪存)

输入内容类似于下例：

```
ap: tar -xtract tftp://192.168.130.222/images/c350-
k9w7-tar.122-13.JA1.tar flash:
```

当显示画面填满时， CLI 将暂停并显示 --MORE-- 。

7. 单击空格键继续。

```
extracting info (229 bytes)

c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)

c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)

c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0
(bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
appsui.js (558 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
back.htm (205 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
cookies.js (5027 bytes).

extracting c350-k9w7-mx.122-13.JA1/html/level1/
forms.js (15704 bytes)...

extracting c350-k9w7-mx.122-13.JA1/html/level1/
sitewide.js (14621 bytes)...

extracting c350-k9w7-mx.122-13.JA1/html/level1/
config.js (2554 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
stylesheet.css (3215 bytes)

c350-k9w7-mx.122-13.JA1/html/level1/images/
(directory) 0 (bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/ap_title_appname.gif (1422 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_1st.gif (1171 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_cbottom.gif (318 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_current.gif (348 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last.gif (386 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last_filler.gif (327 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last_flat.gif (318 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_nth.gif (1177 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_leftnav_dkgreen.gif (869 bytes)

 -- MORE --
```

提示 如果没有按下空格继续，过程将会超时，无线设备将停止解压映像。

8. 输入 `set BOOT` 命令，指定新映像为无线设备重启时使用的映像。

   无线设备将创建与映像名称相同的映像目录，必须在命令中包含该目录。输入内容类似于下例：

   ```
   ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
   ```

9. 输入 `set` 命令，检查引导加载程序的条目。

   ```
   ap: set
   BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
   DEFAULT_ROUTER=192.168.133.1
   IP_ADDR=192.168.133.160
   NETMASK=255.255.255.0
   ```

10. 输入 `boot` 命令，重新启动无线设备。

    当无线设备重启时，它将加载新映像。

    ```
    ap: boot
    ```

获取 TFTP 服务器软件

您可从多个网站下载 TFTP 服务器软件。我们建议从此处下载共享软件 TFTP 实用工具：http://tftpd32.jounin.net

根据网站上的说明安装和使用实用工具。

备注：

协议过滤器

本附录中的表格列出了一些您可在接入点过滤的协议。

Ethertype 协议

在各表格中，“ 协议 ” 列列出了协议名称，“ 附加标识 ” 列列出了该协议的别名，“ISO 代号 ” 列列出了各协议的数字代号。

表 118 - Ethertype 协议

协议	附加标识符	ISO 代号
ARP	–	0x0806
RARP	–	0x8035
Ip	–	0x0800
Berkeley Trailer Negotiation	–	0x1000
局域网测试	–	0x0708
X.25 三级	X.25	0x0805
Banyan	–	0x0BAD
CDP	–	0x2000
DEC XNS	XNS	0x6000
DEC MOP 转储 / 加载	–	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	–	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	–	0x00E0
IPX 802.3	–	0x00FF
Novell IPX (旧)	–	0x8137
Novell IPX (新)	IPX	0x8138
EAPOL (旧)	–	0x8180
EAPOL (新)	–	0x888E

表 118 - Ethertype 协议 (续)

协议	附加标识符	ISO 代号
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet 配置测试	–	0x9000
NetBUI	–	0xF0F0

IP 协议

表 119 - IP 协议

协议	附加标识符	ISO 代号
虚拟	–	0
Internet 控制消息协议	ICMP	1
Internet 组管理协议	IGMP	2
传输控制协议	TCP	6
外部网关协议	EGP	8
PUP	–	12
CHAOS	–	16
用户数据报协议	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
封装表头	encap_hdr	98
Spectralink 语音协议	SVP Spectralink	119
raw	–	255

IP 端口协议

表 120 - IP 端口协议

TCP 端口服务多路复用	tcpmux	1
应答	–	7
取消 (9)	–	9
系统状态 (11)	–	11
日期查询 (13)	–	13
网络状态 (15)	–	15
气象报告协议	qotd quote	17
消息发送协议	msp	18
ttytst 源	chargen	19
FTP 数据	ftp-data	20
FTP 控制 (21)	FTP	21

表 120 - IP 端口协议 (续)

安全外壳 (22)	ssh	22
Telnet	–	23
简单邮件传输协议	SMTP mail	25
时间	timserver	37
资源位置协议	RLP	39
IEN 116 域名服务器	Name	42
whois	nicname 43	43
域名服务器	DNS domain	53
MTP	–	57
BOOTP 服务器	–	67
BOOTP 客户端	–	68
TFTP	–	69
gopher	–	70
rje	netrjs	77
finger	–	79
超文本传输协议	HTTP www	80
ttylink	LINK	87
Kerberos v5	Kerberos krb5	88
supdup	–	95
主机名	hostnames	101
TSAP	iso-tsap	102
CSO 域名服务器	cso-ns csnet-ns	105
远程 Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap 身份验证	auth	113
sftp	–	115
uucp 路径	–	117
网络新闻传输协议	Network News readnews nntp	119
USENET 新闻传输协议	Network News readnews nntp	119
网络时间协议	ntp	123
NETBIOS 名称服务	netbios-ns	137

表 120 - IP 端口协议（续）

NETBIOS 数据报服务	netbios-dgm	138
NETBIOS 会话服务	netbios-ssn	139
临时邮件访问协议 v2	Interim Mail Access Protocol IMAP2	143
简单网络管理协议	SNMP	161
SNMP 陷阱	SNMP Trap	162
基于 IP 的 ISO CMIP 管理	CMIP Management Over IP cmip-man CMOT	163
基于 IP 的 ISO CMIP 代理	cmip-agent	164
X 显示管理控制协议	xdmcp	177
NeXTStep 页面服务器	NeXTStep	178
边界网关协议	BGP	179
Prospero	–	191
互联网中继聊天	IRC	194
SNMP Unix 多路复用	smux	199
AppleTalk 路由	at-rtmp	201
AppleTalk 名称绑定	at-nbp	202
AppleTalk 应答	at-echo	204
AppleTalk 区域信息	at-zis	206
NISO Z39.50 数据库	z3950	210
IPX	–	213
交互邮件访问协议 v3	imap3	220
Unix 清单服务器	ulistserv	372
Syslog	–	514
Unix 后台处理程序	spooler	515
talk	–	517
ntalk	–	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	–	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
网络字典	webster	765

表 120 - IP 端口协议 (续)

SUP 服务器	supfilesrv	871
swat for SAMBA	swat	901
SUP 调试	supfiledbg	1127
ingreslock	–	1524
Prospero 非特权型	prospero-np	1525
RADIUS	–	1812
并发版本系统	CVS	2401
Cisco IAPP	–	2887
非无线电以太网	RFE	5002

备注：

支持的 MIB

本附录列出了在该软件版本下，接入点支持的简单网络管理协议 (SNMP) 管理信息库 (MIBs)。思科 IOS SNMP 代理支持 SNMPv1、SNMPv2 和 SNMPv3。

MIB 列表

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-LBS-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB

- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- CISCO-WDS-INFO-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

使用 FTP 访问 MIB 文件

根据以下步骤使用 FTP 获取各 MIB 文件。

1. 使用 FTP 访问服务器 ftp.cisco.com。
2. 使用该用户名登录：anonymous。
3. 当提示输入密码时，输入电子邮件用户名。
4. 在 `ftp>` 提示符中，将目录更改为 /pub/mibs/v1 或 /pub/mibs/v2。
5. 使用 `get MIB_filename` 命令获取 MIB 文件的副本。

提示 您还可从思科网站获取关于 MIB 的信息：
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

错误和事件消息

本附录列出了 CLI 错误和 事件消息。

惯例

系统错误消息将以下表中的格式显示。

表 1 - 系统错误消息惯例

消息组件	描述	示例
错误标识符	对错误归类的字符串。	STATION-ROLE
软件组件	用于标识错误的软件组件的字符串。	AUTO_INSTALL
严重性等级	用于指示错误严重程度的数字字符串。	0-LOG-EMERG —— 紧急情况，完全不能工作 1-LOG-ALERT —— 警告用户发生严重问题 2-LOG-CRIT —— 警告可能发生严重的关键错误 3-LOG-ERR —— 警告错误状况，大多数功能能够正常工作；但需要小心 4-LOG-WARNING —— 用户可根据意愿忽略的警告 5-LOG-NOTICE —— 可能需要用户关注的注意事项 6-LOG-INFO —— 参考信息 (不严重) 7-LOG-DEBUG —— 调试信息 (不严重)

表 1 - 系统错误消息惯例 (续)

消息组件	描述	示例
操作标志	供代码使用用于显示附加操作的内部标记。	0 —— 无操作标志 MSG-TRACEBACK —— 包括追溯及消息 MSG-PROCESS —— 包括过程信息及消息 MSG-CLEAR —— 指示条件已被清除 MSG-SECURITY —— 指示安全消息 MSG-NOSCAN —— 禁止 EEM 模式屏蔽
%d	整数。	2450
%e	MAC 地址。	000b.fcff.b04e
S	提供更多错误详细信息的消息字符串。	“Attempt to protect port 1640 failed.”
x	十六进制数字。	0x001

软件自动升级消息

下表介绍了升级软件时显示的消息。

表 2 - 软件自动升级消息

消息	说明	建议的操作
SW-AUTO-UPGRADE-2-FATAL_FAILURE: “Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.	自动升级软件失败。检查软件是否已被删除。将软件复制到闪存中。	重启设备之前，先复制软件。
SW-AUTO-UPGRADE-7-DHCP_CLIENT_FAILURE: “%s”: Auto upgrade of the software failed.”	自动升级软件失败。	确保 DHCP 客户端正在运行。
SW-AUTO-UPGRADE-7-DHCP_SERVER_FAILURE: “%s”: Auto upgrade of the software failed.”	自动升级软件失败。	确保 DHCP 服务器已正确配置。
SW-AUTO-UPGRADE-7_BOOT_FAILURE: “%s”: Auto upgrade of the software failed.”	自动升级软件失败。	重启设备。如果再次出现该消息，则完整复制显示的错误消息，将其报告给您的技术支持代表。
AUTO-INSTALL-4-STATION_ROLE: “%s”: The radio is operating in automatic install mode.”	无线电装置运行在自动安装模式下。	使用 **station-role** 配置接口命令，将无线电配置为除安装模式之外的其他模式。
AUTO-INSTALL-4-IP_ADDRESS_DHCP: “The radio is operating in automatic install mode and has set ip address dhcp.”	无线电装置运行在自动安装模式下，并被配置为通过 DHCP 接收 IP 地址。	使用 **station-role** 配置接口命令，将无线电配置为除安装模式之外的其他模式。
Error Message: AUTO-INSTALL-6_STATUS: “%s” %s. RSSI=-%d dBm.: “The radio is operating in install mode.”	无线电装置运行在自动安装模式下。	使用 **station-role** 配置接口命令，将无线电配置为除安装模式之外的其他模式。
AVR_IMAGE_UPDATE-7-UPDATE_COMPLETE: “The AVR "$d" firmware was successfully updated.”	接入点 AVR 固件已成功更新。	无需操作。
AVR_IMAGE_UPDATE-2-UPDATE_FAILURE: “The AVR "$d" firmware is not current. Update error: "$s".”	AVR 固件不是最新版本，更新失败。	复制错误消息，将其报告给您的技术支持代表。
AVR_IMAGE_UPDATE-4-UPDATE_SKIPPED: “AVR "$d" update processing was skipped:"$s".”	发生错误，已跳过 AVR 更新过程。	无需操作。
AVR_IMAGE_UPDATE-4-UPDATE_START: “The system is updating the AVR "$d" firmware.Please wait...“	系统正在更新 AVR 固件。	无需操作。

关联管理消息

下表介绍了与关联管理相关的错误消息。

表 3 - 关联管理消息

消息	说明	建议的操作
DOT11-3-BADSTATE: “%s %s ->%s.”	802.11 关联和管理使用表格驱动的状态机通过各种状态跟踪和转换关联。当关联接收到多种可能事件之一时，将发生状态转换。当发生该错误时，则表示关联接收到一个在该状态下未预期的事件。	系统将继续运行，但会丢失生成该错误的关联。完整复制显示的错误消息，并将其报告给您的技术支持代表。
DOT11-6-ASSOC: “Interface %s, Station %s e% %s KEY_MGMT (%s), MSGDEF_LIMIT_MEDIUM.”	指示的工作站关联到所示接口的接入点。	无。
DOT11-6-ADD: “Interface %s, Station %e associated to parent %e.”	指示的工作站关联到所示接口的父接入点。	无。
DOT11-6-DISASSOC: Interface %s, Deauthenticating Station %e #s	工作站与接入点取消关联。	无需操作。
DOT11-6-ROAMED: “Station %e roamed to %e.”	指示的工作站漫游到指示的新接入点。	无。
DOT11-4-ENCRYPT_MISMATCH: “Possible encryption key mismatch between interface %s and station %e.”	指示的接口与指示的工作站的加密设置不匹配。	检查该接口和故障工作站的加密配置，确认配置相匹配。
DOT11-4-DIVER_USED: Interface $s, Mcs rates 8-15 disabled due to only one transmit or recieve antenna enabled	要达到这些速率，至少需要启用 2 条接收和发送天线。	完整复制控制台或系统日志中显示的错误消息。使用 Output Interpreter 研究并尝试解决错误：https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl 还可对缺陷工具包执行搜索：http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.
DOT11-4-NO_HT: Interface %s, Mcs rates disabled on vlan %d due to %s	配置不正确，无法使用 HT 速率。	完整复制控制台或系统日志中显示的错误消息。使用 Output Interpreter 研究并尝试解决错误：https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl 还可对缺陷工具包执行搜索：http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.
DOT11-4-NO_MBSSID_BACKUP_VLAN: Backup VLANs cannot be configured if MBSSID is not enabled:"$s" not started	要启用备用 VLAN，配置 MBSSID 模式。	在设备上配置 MBSSID。

解压消息

下表介绍了解压错误消息。

表 4 - 解压消息

消息	说明	建议的操作
SOAP-4-UNZIP_OVERFLOW: “Failed to unzip %s, exceeds maximum uncompressed html size.”	由于文件太大，解压缩过程使用的缓冲区不足， HTTP 服务器无法响应 HTTP GET 请求来提取压缩文件。	确保文件是有效的 HTML 页面。如果是的话，需要将未解压的文件复制到闪存中，以通过 HTTP 提取该文件。

系统日志消息

下表介绍了系统日志消息。

表 5 - 系统日志消息

消息	说明	建议的操作
%DOT11-4-LOADING_RADIO: Interface [chars], loading the radio firmware ([chars])	无线电装置已停止加载新的固件。	无需操作。
%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]	数据链路层线路协议的状态已改变。	无需操作。
%SYS-5-RESTART: System restarted --[chars]	请求重新加载或重新启动。	该消息仅作通知之用。无需操作。
%SYS-5-CONFIG_I: Configured from [chars] by [chars]	路由器配置已更改。	该消息仅作通知之用。无需操作。
%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]	所示接口上的数据链路层线路协议的状态已改变。	无需操作。
%SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start	SNMP 服务器已完成冷启动。	该消息仅作通知之用。无需操作。
%SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].	系统时钟已修改。	该消息仅作通知之用。无需操作。

802.11 子系统消息

下表介绍了子系统消息。

表 6 - 子系统消息

消息	说明	建议的操作
DOT11-6-FREQ_USED: “Interface %s, frequency %d selected.”	在扫描未使用的频率时，指示的接口选择了所示的频率。	无。
DOT11-4-NO-VALID_INFRA_SSID: “No infrastructure SSID configured. %s not started.”	未配置基础架构 SSID，无法启动指示的接口。	需要在无线电配置中添加至少一个基础架构 SSID。
DOT11-4-VERSION_UPGRADE: “Interface %d, upgrading radio firmware.”	当启动指示的接口时，接入点找到错误的固件版本。无线电接口加载所需的版本。	无。
DOT11-2-VERSION_INVALID: “Interface %d, unable to find required radio version %x.%x/ %d/	当尝试升级所示接口上的无线电固件时，接入点发现思科 IOS 软件随附的所示无线电固件版本不正确。	无。
DOT11-3-RADIO_OVER_TEMPERATURE: “Interface %s Radio over temperature detected.”	无线电接口的内部温度超过所示无线电接口的最大值。	采取必要措施，降低内部温度。这些步骤因安装情况而异。
DOT11-6-RADIO_TEMPERATURE_NORMAL: “Interface %s radio temperature returned to normal.”	无线电接口的内部温度已返回到所示无线电接口的正常值。	无。
DOT11-3-TX_PWR_OUT_OF_RANGE: “Interface %s Radio transmit power out of range.”	发射器功率等级超出所示无线电接口的正常范围。	从网络和服务上拆除该设备。
DOT11-3-RADIO_RF_LO: “Interface %s Radio cannot lock RF freq.”	无线电锁相环 (PLL) 电路无法在所示的接口上锁定正确的频率。	从网络和服务上拆除该设备。
DOT11-3-RADIO_IF_LO: “Interface %s Radio cannot lock IF freq.”	无线电中频 (IF) PLL 无法在所示接口上锁定正确的频率。	从网络和服务上拆除该设备。
DOT11-6-FREQ_SCAN: “Interface %s Scanning frequencies for %d seconds.”	对接口上最不拥挤的频率启动扫描，持续时间达到所示时长。	无。
DOT11-2-NO_CHAN_AVAIL: “Interface %s, no channel available.”	无可用频率，很可能是因为在之前的 30 分钟内检测到雷达。	无。
DOT11-6-CHAN_NOT_AVAIL: “DFS configured frequency %d Mhz unavailable for %d minute(s).	在当前通道上检测到雷达。动态频率选择 (DFS) 规范要求在通道上 30 秒内无传输。	无。
DOT11-6-DFS_SCAN_COMPLETE: “DFS scan complete on frequency %d MHz.”	设备已在所示的频率上完成动态频率扫描 (DFS) 过程。	无。

表 6 - 子系统消息 (续)

消息	说明	建议的操作
DOT11-6-DFS_SCAN_START: "DFS: Scanning frequency %d MHz for %d seconds."	设备已开始 DFS 扫描过程。	无。
DOT11-6-DFS_TRIGGERED: "DFS: triggered on frequency %d MHz."	DFS 在所示频率上检测到雷达信号。	无。通道将被置于未占用列表达 30 分钟，并选择新的通道。
DOT11-4-DFS_STORE_FAIL: "DFS: could not store the frequency statistics."	将 DFS 统计数据写入闪存时失败。	无。
DOT11-4-NO_SSID: "No SSIDs configured, %d not started."	所有 SSID 均已从配置中删除。必须至少为无线电接口配置一个 SSID。	在接入点上至少配置一个 SSID。
DOT11-4-NO_SSID_VLAN: "No SSID with VLAN configured. %s not started."	没有为 VLAN 配置 SSID。未启动所示的接口。	必须至少为每个 VLAN 配置一个 SSID。在所示的接口上至少为 VLAN 添加一个 SSID。
DOT11-4-NO_MBSSID_VLAN: "No VLANs configured in MBSSID mode. %s not started."	在 MBSSID 模式下没有配置 VLAN。未启动所示的接口。	必须在所示接口的配置中至少为 VLAN 添加一个 SSID。
DOT11-4-NO_MBSSID_SHR_AUTH: "More than 1 SSID with shared authentication method in non-MBSSID mode % is down".	未启用 MBSSID 时，仅限 1 个 SSID 拥有共享验证方法。	删除 Dot11Radio 无线电接口或将 SSID 的验证模式更改为开放式配置。
DOT114-NO_MBSSID_BACKUP_VLAN: "Backup VLANs cannot be configured if MBSSID is not enabled. %s not started.	要启用备用 VLAN，配置 MBSSID 模式。	在设备上配置 MBSSID。
IF-4-MISPLACED_VLAN_TAG: "Detected a misplaced VLAN tag on source Interface %. Dropping packet.	在所示的接口上检测到收到 802.1Q VLAN 标签，但该标签无法正确解析。收到的数据包封装或解封装不正确。	无
DOT11-2-FW_LOAD_NET: "Interface %s cannot load on boot. Place image in flash root directory and reload."	在接入点启动时，无法从网络加载无线电映像。	将映像放置在闪存文件系统的根目录中。
DOT11-4-FW_LOAD_DELAYED: "Interface %s, network filesys not ready. Delaying firmware (%s) load."	当在所示接口升级新固件时，网络文件系统未运行或未就绪。标识固件文件的加载过程被延迟。	确保网络已运行并就绪，然后再尝试升级新固件。
DOT11-3-FLASH_UNKNOWN_RADIO: "Interface %s has an unknown radio."	当在所示接口尝试升级新固件时，无法确定无线电类型。	重新启动系统，看看是否可以完成固件升级。
DOT11-4-UPLINK_ESTABLISHED: "Interface %s associated to AP %s %e %s.	所示的中继器已关联到所示的根接入点。客户端现在可关联到所示的中继器，并可传送通信数据。	无。
DOT11-2-UPLINK_FAILED: "Uplink to parent failed: %s."	由于所示的原因，到父接入点的连接失败。上行链路接口停止了连接尝试。	尝试重置上行链路接口。如果问题仍然存在，请联系技术支持。
DOT11-4-CANT_ASSOC: "Interface %, cannot associate %s."	所示的接口设备无法关联到所示的父接入点。	检查父接入点与该设备的配置，确保它们相匹配。
DOT11-4-CANT_ASSOC: "Interface Dot11Radio 0, cannot associate."	父接入点不支持客户端 MFP。该错误消息仅出现在工作组网桥、中继器或非根网桥模式下的接入点上，当 WGB、中继器或非根网桥配置为需要 (或必需) 客户端 MFP SD，但根客户端 MFP 被禁用时，将会看到该消息。	检查父接入点与该设备的配置，确保它们相匹配。
DOT11-2-PROCESS_INITIALIZATION_FAILED: "The background process for the radio could not be started: %s)	由于一些原因，所示接口的初始化过程失败，可能是临时性错误。	重新加载接入点。如果该操作无法修复问题，则执行断电重启。如果仍然失败，尝试将接入点固件版本降至之前的版本。
DOT11-2-RADIO_HW_RESET: "Radio subsystem is undergoing hardware reset to recover from problem."	发生不可恢复的错误，无法通过软件重置解决。	无。
DOT11-2-RESET_RADIO: "Interface %s, Radio %s, Trying hardware reset on radio."	通过软件重置启动失败的无线电接口。尝试硬件重置，重置设备上的所有无线电接口。	无。

表 6 - 子系统消息 (续)

消息	说明	建议的操作
DOT11-4-MAXRETRIES: "Packet to client %e reached max retries, removing the client."	已达到数据包最大发送重试限值，正在删除客户端。该错误消息指示接入点尝试轮询客户端一定次数，但未收到响应。因此，客户端已从关联表中删除。当客户端和接入点尝试在噪声较大的 RF 环境中进行通信时，经常会发生该问题。	要解决该问题，在接入点运行载波忙碌测试，并通过快照查看无线电频谱中是否存在噪声。尝试消除任何有害噪声。 更多信息，请参见第 287 页的 " 执行载波载波忙碌测试 "。 如果该区域中有多个接入点，它们的通道信号可能会发生重叠，或与周围区域的其他无线设备的通信信号重叠。在 Network Interfaces (网络接口) 中更改通道，选择 Radio-802.11。有三个不重叠的通道：1、 6 和 11。
DOT11-4-RM_INCAPABLE: "Interface %s	所示的接口不支持无线电管理功能。	无。
DOT11-4-RM_INCORRECT_INTERFACE: "Invalid interface, either not existing or non-radio."	无线电管理请求发现，接口不存在或不是无线电接口。	无。
DOT11-3-POWERS_INVALID: "Interface %s, no valid power levels available."	无线电驱动程序未发现有效的功率等级设置。	查看并纠正功率源和设置。
DOT11-4-RADIO_INVALID_FREQ: "Operating frequency (%d) invalid - performing a channel scan."	所示的工作频率无效。正在执行通道扫描，以选择有效的频率。	无。
DOT11-4-RADIO_NO_FREQ: "Interface &s, all frequencies have been blocked, interface not started."	所设置的工作频率无效，正在强制执行通道扫描，以选择有效的工作频率。	无。
DOT11-4-BCN_BURST_NO_MBSSID: "Beacon burst mode is enabled but MBSSID is not enabled, %s is down."	只有在所示的接口上启用 MBSSID 之后才能启用信标突发模式。	在所示的接口上启用 MBSSID 或禁用信标突发。
DOT11-4-BCN_BURST_TOO_MANY_DTIMS: "Beacon burst mode is enabled and there are too many different DTIM periods defined. %s is down.	信标突发模式最多只支持四个唯一 DTIM 值，每个最多四个 BSS。	将为接口设置的 SSID 上唯一 DTIM 的数量更改为合理的值。
DOT11-2-RADIO_INITIALIZATION_ERROR: "The radio subsystem could not be initialized (%s)."	在尝试初始化无线电子系统时检测到严重错误。	重新加载系统。
DOT11-4-UPLINK_NO_ID_PWD: "Interface %s, no username/password supplied for uplink authentication."	用户未输入用户名和 / 或密码。	输入用户名和 / 或密码后重试。
DOT11-5-NO_IE_CFG: "No IEs configured for %s (ssid index %u)."	在尝试将信标或探头响应应用到无线电接口时，所示的 SSID 索引上未定义信标或探头。	检查 IE 配置。
DOT11-4-FLASHING_RADIO: "Interface %s, flashing radio firmware (%s)."	所示的无线电接口已停止加载新的固件。	无。
DOT11-4-LOADING_RADIO: "Interface %s, loading the radio firmware (%s)."	所示的无线电接口已停止加载新的固件。	无。
DOT11-2-NO_FIRMWARE: "Interface %s, no radio firmware file (%s) was found."	在尝试升级固件时，未在闪存文件系统中找到无线电接口的文件。或者，接入点上的 IOS 已损坏。	设备中加载的映像错误。根据所使用的无线电类型找到正确的映像。要解决该问题，您可将新的思科 IOS 映像重新加载接入点。 关于重新加载映像的说明，请参见第 516 页的 " 重新加载接入点映像 "。 如果接入点上的 IOS 已损坏，使用模式按钮重新加载接入点映像。 参见第 513 页的 " 模式按钮 "。
DOT11-2-BAD_FIRMWARE: "Interface %s, radio firmware file (%s) is invalid."	在尝试升级所示接口的固件时，发现所示的无线电固件文件无效。	确保将正确的固件映像文件放入设备所预期的正确位置。
DOT11-2-RADIO_FAILED: "Interface %s, failed - %s."	所示接口上的无线电驱动程序发现严重错误，因此，该接口已关闭。	无。

表 6 - 子系统消息 (续)

消息	说明	建议的操作
DOT11-4-FLASH_RADIO_DONE: "Interface %s, flashing radio firmware completed."	所示接口的无线电固件升级已完成，无线电接口使用新固件重新启动。	无。
DOT11-4-UPLINK_LINK_DOWN: "Interface %s, parent lost: %s."	由于所示的原因，到所示接口上父接入点的连接已丢失。设备尝试寻找新的父接入点。	无。
DOT11-4-CANT_ASSOC: Cannot associate: $s	由于所示的原因，设备无法建立到父接入点的连接。	确认该父接入点的基本配置设置 (SSID、 WEP 及其他设置) 与该设备是否相匹配。
DOT11-4-CLIENT_NOT_FOUND: "Client was not found."	在检查 MIC 时未找到客户端。	无。
DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client	发送到客户端的某个数据包多次未能成功送达，已达到最大重试次数。客户端已从关联表中删除。	无。
DOT11-4-BRIDGE_LOOP: "Bridge loop detected between WGB %e and device %e."	所示的工作组网桥报告所示的以太网客户端之一的地址，且接入点已将该地址标记为在网络中的其他位置。	单击接入点 GUI 的 Associations (关联) 页面上的 Refresh (刷新), 或者在 CLI 上输入 `clear dot11 statistics` 命令。
DOT11-4-ANTENNA_INVALID: "Interface %s, current antenna position not supported, radio disabled."	所示的 AIR-RM21A 无线电模块不支持外部天线的高增益位置 (高增益位置平折在接入点上)。当天线处于高增益位置时，接入点自动禁用无线电接口。	折叠 AIR-RM21A 无线电模块上的天线，使其与接入点本体呈 90° 角。
DOT11-6-ANTENNA_GAIN: "Interface %s, antenna position/gain changed, adjusting transmitter power."	天线增益已更改，因此，必须调整允许的功率等级列表。	无。
DOT11-4-DIVER_USED: "Interface %s Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled."	要达到所列的速率，至少需要启用 2 条接收和发送天线。	在接入点安装并启用至少 2 条接收或发送天线。
DOT11-3-RF-LOOPBACK_FAILURE: "Interface %s Radio failed to pass RF loopback test."	所示接口的无线电回路测试失败。	无。
DOT11-3-RF-LOOPBACK_FREQ_FAILURE: "Interface %s failed to pass RF loopback test."	所示接口给定频率下的无线电回路测试失败。	无。
DOT11-7-AUTH_FAILED: "Station %e Authentication failed"	所示工作站验证失败。	请确认用户输入了正确的用户名和密码，并确认验证服务器已联机。
DOT11-7-CCKM_AUTH_FAILED: "Station %e CCKM authentication failed."	所示工作站 CCKM 验证失败。	确认配置为使用 WDS 接入点的接入点拓扑工作正常。
DOT11-4-CCMP_REPLAY: "AES-CCMP TSC replay was detected on packet (TSC 0x%11x received from &e)."	帧上指示存在 AES-CCMP TSC 回放。接收到的数据包中存在 AES-CCMP TSC 回放基本就表示存在主动攻击。	无。
DOT11-4-CKIP_MIC_FAILURE: "CKIP MIC failure was detected on a packet (Digest 0x%x) received from %e)."	帧上检测到 CKIP MIC 故障。接收到的数据包中存在 CKIP MIC 故障基本就表示存在主动攻击。	无。
DOT11-4-CKIP_REPLAY: "CKIP SEQ replay was detected on a packet (SEQ 0x&x) received from %e."	帧上检测到 CKIP SEQ 回放。接收到的数据包中存在 CKIP SEQ 回放基本就表示存在主动攻击。	无。
DOT11-4-TKIP_MIC_FAILURE: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key."	所示工作站的单播帧 (使用所示的成对密钥在本地解密) 上检测到 TKIP Michael MIC 故障。	接收到的数据包中存在 Michael MIC 故障可能指示网络存在主动攻击。在无线局域网中搜索并删除潜在的伪设备。该故障还可能指示客户端配置错误或故障。
DOT11-4-TKIP_MIC_FAILURE_REPORT: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key	接入点从所示的工作站接收到 EAPOL 密钥，通知接入点 TKIP Michael MIC 在由该接入点发送的数据包上失败。	无。

表 6 - 子系统消息 (续)

消息	说明	建议的操作
DOT11-3-TKIP_MIC_FAILURE_REPEATED: "Two TKIP Michael MIC failures were detected within %s seconds on %s interface. The interface will be put on MIC failure hold state for next %d seconds"	在所示时间内在所示的接口上检测到两个 TKIP Michael MIC 故障。由于这通常指示网络上存在主动攻击，接口将在指示的时间内置于暂停状态。在此暂停时间内，使用该 TKIP 密文的工作站取消关联，且在保持时间结束之前无法重新关联。在暂停时间结束后，接口可正常工作。	MIC 故障通常指示网络中存在主动攻击。从您的无线局域网中搜索并删除潜在的伪设备。如果这是误报警，则不得将接口暂停这么长时间，必须使用 countermeasure tkip hold-time 命令调节暂停时间。
DOT11-4-TKIP_REPLAY: "TKIP TSC replay was detected on a packet (TSC 0x%ssx received from %e)."	帧上检测到 TKIP TSC 回放。接收到的数据包中存在 TKIP TSC 回放基本就表示存在主动攻击。	无。
DOT11-4-WLAN_RESOURCE_LIMIT: "WLAN limit exceeded on interface %s and network-id %d."	该接入点已达到 16 个 VLAN 或 WLAN 的限值。	如果接入点尝试关联 RADIUS 分配的网络 ID，则取消配置或减少静态 VLAN。
SOAP-3-WGB_CLIENT_VLAN_SOAP: "Workgroup Bridge Ethernet client VLAN not configured."	没有为连接到工作组网桥的客户端设备配置 VLAN。	配置 VLAN，以接受连接到工作组网桥的客户端设备。
DOT11-4-NO_VLAN_NAME: "VLAN name %s from RADIUS server is not configured for station %e."	必须在接入点中配置 RADIUS 服务器返回的 VLAN 名称。	在接入点中配置 VLAN 名称。
DOT11-4-NO_VLAN_ID: "VLAN id %d from Radius server is not configured for station %e."	必须在接入点中配置 RADIUS 服务器返回的 VLAN ID。	在接入点中配置 VLAN ID。
SOAP-3-ERROR: "Reported on line %d in file %s.%s."	在控制器 ASIC 所示文件名中的所示行号上发生内部错误。	无。
SOAP_FIPS-2-INIT_FAILURE: "SOAP FIPS initialization failure: %s."	SOAP FIPS 初始化失败。	无。
SOAP_FIPS-4-PROC_FAILURE: "SOAP FIPS test failure: %s."	SOAP FIPS 测试严重错误。	无。
SOAP_FIPS-4-PROC_WARNING: "SOAP FIPS test warning: %s."	SOAP FIPS 测试非严重错误。	
SOAP_FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."	SOAP FIPS 的 IOS 加密例程自检失败。	复制 IOS 映像。
SOAP_FIPS-2-SELF_TEST_RAD_FAILURE: "RADIO crypto FIPS self test failed at %s on interface %s %d."	SOAP FIPS 的无线电加密例程自检失败。	检查无线电映像。
SOAP_FIPS-2-SELF_TEST_IOS_SUCCESS: "IOS crypto FIPS self test passed."	SOAP FIPS 自检通过。	无
SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS: "RADIO crypto FIPS self test passed on interface %s %d."	无线电接口上 SOAP FIPS 自检通过。	
DOT11-6-MCAST_DISCARD: "%s mode multicast packets are discarded in %s multicast mode."	接入点被配置为工作组网桥，在客户端模式下丢弃基础架构模式多播数据包，并在基础架构模式下丢弃客户端模式多播数据包。	无

接入点间协议消息

消息	说明	建议的操作
DOT11-6-STANDBY_ACTIVE: "Standby to Active, Reason = %s (%d)."	由于所示的原因，接入点从待机模式转换为活动模式。	无。
DOT11-6-STANDBY_REQUEST: "Hot Standby request to shutdown radios from %e."	因为在该接入点的无线电接口上检测到故障，所示的待机接入点请求该接入点关闭其无线电接口。	无。
DOT11-6-ROGUE_AP: "Rogue AP %e reported. Reason: %s."	由于所示的原因，工作站报告潜在的伪接入点。	无。

本地验证器消息

消息	说明	建议的操作
RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]	本地 RADIUS 服务器接收到一个验证请求，但未能识别转发该请求的网络接入服务器 (NAS) 的 IP 地址。	确保无线局域网中的每个接入点都已配置为本地 RADIUS 服务器上的 NAS。
RADSRV-4-NAS_KEYMIS: NAS shared key mismatch.	本地 RADIUS 服务器接收到一个验证请求，但消息签名指示共享密钥文本不匹配。	更正 NAS 或本地 RADIUS 服务器上的共享密钥配置。
RADSRV-4_BLOCKED: Client blocked due to repeated failed authentications	用户未通过验证次数超过所配置的触发锁定次数，该帐户已被禁用。	使用 `clear radius local-server user` *username* 特权 EXEC 命令解除用户锁定，或在配置的锁定时间到期后停止锁定用户。
DOT1X-SHIM-6-AUTH_OK: “Interface %s authenticated [%s].”	802.1x 验证成功。	无
DOT1X-SHIM-3-AUTH_FAIL: “Interface %s authentication failed.”	连接设备的 802.1x 验证失败。	检查客户端以及 RADIUS 服务器上的 802.1x 凭证配置。
DOT1X-SHIM-3-INIT_FAIL: “Unable to init - %s.”	在中介层初始化期间发生错误。	
DOT1X-SHIM-3-UNSUPPORTED_KM: “Unsupported key management: %X.”	在中介层初始化期间发生错误。发现不支持的密钥管理类型。	无。
DPT1X-SHIM-4-PLUMB_KEY_ERR: “Unable to plumb keys - %s.”	在中介层尝试探测密钥时发生意外错误。	无。
DOT1X-SHIM-3-PKT_TX_ERR: “Unable to tx packet -%s.”	在中介层尝试发送 dot1x 数据包时发生意外错误。	无
DOT1X-SHIM-3-ENCAP_ERR: “Packet encap failed for %e.”	在中介层尝试发送 dot1x 数据包时发生意外错误。数据包封装失败。	无。
DOT1X-SHIM-3-SUPP_START_FAIL: “Unable to start supplicant on %s.”	在中介层尝试在所示接口启动 dot1x 客户端时发生意外错误。	无。
DOT1X-SHIM=3-NO_UPLINK: “No uplink found for %s.”	在处理 dot11 接口上的 dot1x 事件或消息时，在应该有上行链路接口的位置未找到接口。	无。
Information Group rad_acct: Radius server <ip address> is responding again (previously dead). Error Group acct: No active radius servers found. Id 106	当在接入点上配置了 `radius-server deadtime 10` 命令时将会出现该消息。该命令用于设置时间间隔，在此时间后，接入点不再尝试使用不响应的服务器。这样可避免请求超时所需的等待时间，可尽快尝试下一个配置的服务器。在数分钟内，标记为停机的 RADIUS 服务器将被后续请求跳过，除非所有服务器都标记为停机。配置 10 分钟停机时间表示在 10 分钟内无法使用该服务器。	如果不希望出现该日志，可禁用该命令。实际上，该消息不是大问题，它只是信息日志。

WDS 消息

消息	说明	建议的操作
WLCCP-WDS-6-REPEATER_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.	中继器接入点不支持 WDS。	无。
WLCCP-WDS-6-PREV_VER_AP: A previous version of AP is detected.	WDS 设备检测到早期的接入点版本。	无。
WLCCP-AP-6-INFRA: WLCCP Infrastructure Authenticated	接入点成功验证到 WDS 设备。	无。
WLCCP-AP-6-STAND_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode	接入点丢失到 WDS 设备的连接，进入待机模式。	无。
WLCCP-AP-6-PREV_VER_WDS: A previous version of WDS is detected	接入点检测到早期的 WDS 版本。	检查网络上是否存在不支持的 WDS 版本。
WLCCP-AP-6-UNSUP_VER_WDS: An unsupported version of WDS is detected	接入点检测到不支持的 WDS 版本。	检查网络上是否存在不支持的 WDS 版本。

消息	说明	建议的操作
WLCCP-NM-3-WNM_LINK_DOWN: Link to WNM is down	网络管理器未响应保持活动消息。	检查网络管理器或到网络管理器的网络路径是否有问题。
WLCCP-NM-6-WNM_LINK_UP: Link to WNM is up	网络管理器现正响应保持活动消息。	无。
WLCCP-NM-6-RESET: Resetting WLCCP-NM	网络管理器 IP 地址变化或临时性资源不足状态都可能导致 WDS 网络管理器子系统重置，但很快将恢复正常操作。	无。
WLCCP-WDS-3-RECOVER: "%s	WDS 降级恢复错误。	无。

Mini IOS 消息

消息	说明	建议的操作
MTS-2-PROTECT_PORT_FAILURE: An attempt to protect port [number] failed	尝试保护端口时初始化失败。	无。
MTS-2-SET_PW_FAILURE: Error %d enabling secret password.	用户尝试启用密文密码时，初始化失败。	无
Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]:	当通过 CLI 保存配置更改时，将会在接入点 CLI 接口上出现该警告消息。这是由于闪存中空间不足。当无线电接口崩溃时，将创建 .rcore 文件。这些文件指示无线电接口中的固件或硬件问题，虽然硬件问题发生的几率很小。	可删除在闪存中生成的 rcore 文件来禁用该警告消息。rcore 文件的扩展名为 .rcore。这些文件可删除，因为它们仅显示无线电接口在某个时刻崩溃的信息。.rcore 文件可在 CLI 会话中列出，类似于：r15_5705_AB50_A8341F30.rcore

接入点 / 网桥消息

消息	说明	建议的操作
APBR-4-SEND_PCKT_FAILED: Failed to Send Packet on port ifDescr (error= errornum)errornum: status error number	HASH(0x2096974)	接入点或网桥发送数据包失败。当存在外部噪声或干扰时会出现该情况。
检查噪声源或干扰源。	APBR-6-DDP_CLNT_RESET: Detected probable reset of hosthost: host MAC address HASH(0x2080f04)	接入点或网桥检测到另一个基础架构设备已重新启动。
如果该消息持续显示，则重启接入点。		

思科发现协议消息

消息	说明	建议的操作
CDP_PD-2-POWER_LOW: %s - %s %s (%e)	未能给系统提供足够的电源。	重新配置或更换内部电源。

外部 RADIUS 服务器错误消息

消息	说明	建议的操作
RADUYS:response-authenticator decrypt fail, paklen 32	该错误消息表示 RADIUS 服务器和接入点之间的 RADIUS 共享密钥不匹配。	确保 RADIUS 服务器和接入点上使用的共享密钥相同。

传感器消息

消息	说明	建议的操作
SENSOR-3-TEMP_CRITICAL: System sensor "d" has exceeded CRITCAL temperature thresholds	其中一个环境测试点测量值超过极端阈值。	纠正指定的条件，否则作为预防性措施，系统将自动关机。输入 show environment all 命令，帮助确定其是否是由温度或电压条件引起的。如果这是一条紧急温度警告，请确认路由器风扇工作正常，且房间的冷却装置和空调工作正常。该状况可能导致系统不能正常工作。
SENSOR-3-TEMP_NORMAL: "s" temperature sensor is now normal	其中一个环境测试点的测量值低于正常的工作温度。	无需操作。
SENSOR-3-TEMP_SHUTDOWN: Shuting down the system because of dangerously HIGH temperature at sensor "d".	其中一个环境测试点的测量值超出路由器的工作温度。	检查高温的原因。
SENSOR-3-TEMP_WARNING: "s" temparature sensor "d" has exceeded WARNING temperature thresholds	其中一个环境测试点的测量值超过警告阈值。	密切监视状况，如有可能，通过冷却周边环境来予以纠正。
SENSOR-3-VOLT_CRITICAL: System sensor "d" has exceeded CRITCAL voltage thresholds	其中一个环境测试点的测量值超过极端电压阈值。	纠正指定的条件，否则作为预防性措施，系统将自动关机。输入 show environment all 命令，帮助确定其是否是由电压条件引起的。该状况可能导致系统不能正常工作。
SENSOR-3-VOLT_NORMAL: System sensor "d"("d") is now operating under NORMAL voltage	其中一个环境测试点的测量值低于正常工作电压。	无需操作。
SENSOR-3-VOLT_WARNING: Voltage monitor "d"("d") has exceeded voltage thresholds	其中一个电压测试点的测量值指示电压超出正常范围。	检查电源或联系 TAC。

SNMP 错误消息

消息	说明	建议的操作
SNMP-3-AUTHFAILIPV6: Authentication failure for SNMP request from host Unrecognized format ' %P'	该未正确验证的主机发送了一个 SNMP 请求。	确保 SNMP 请求中使用的社区 / 用户名已在路由器中配置。
SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full	由于输入队列中已占满错误， SNMP 数据包已被丢弃	使用 show snmp 命令查看丢弃的数据包数量。停止任何 SNMP 访问设备，直到消除错误条件。
SNMP-3-INTERRUPT_CALL_ERR: "s" function, cannot be called from interrupt handler	该消息指示曾调用中断处理程序的功能。这是不允许的，因为调用会失败，而设备将重新启动到 malloc 调用堆栈的底部。	如果该消息再次出现，则完整复制显示的消息，将其报告给您的技术支持代表。
SNMP-4-NOENGINEIDV6: Remote snmpEngineID for Unrecognized format ' %P' not found when creating user: "s"	尝试创建用户失败。这可能是因为未配置远程代理 (或 SNMP 管理器) 的引擎 ID。	配置远程 snmpEngineID 并重新配置用户。如果问题依然存在，完整复制显示的错误消息，将其报告给您的技术支持代表。
SNMP_MGR-3-MISSINGHOSTIPV6: Cannot locate information on SNMP informs host: Unrecognized format ' %P'	提及的 SNMP 的表格条目通知无法找到目标。因此，信息通知未被发送给该目标。	运行 show snmp host 和 show snmp 命令。完整复制所显示的错误消息和显示命令的输出，将其报告给您的技术支持代表。通过 snmp-server host 配置命令删除并再次添加通知目标，即可清除该条件。否则，必须重新加载系统。

SSH 错误消息

消息	说明	建议的操作
SSH-5-SSH2_CLOSE: SSH2 Session from "%s" (tty = "%d") for user '"%s"' using crypto cipher '"%s"', hmac '"%s"' closed	SSH 会话关闭信息	无需操作 — 通知消息
SSH-5-SSH2_SESSION: SSH2 Session request from "%s" (tty = "%d") using crypto cipher '"%s"', hmac '"%s"' "%s"	SSH 会话请求信息	无需操作 — 通知消息
SSH-5-SSH2_USERAUTH: User '"%s"' authentication for SSH2 Session from "%s" (tty = "%d") using crypto cipher '"%s"', hmac '"%s"' "%s"	SSH 用户验证状态信息	无需操作 — 通知消息
SSH-5-SSH_CLOSE: SSH Session from "%s"(tty = "%d") for user '"%s"' using crypto cipher '"%s"' closed	SSH 会话关闭信息	无需操作 — 通知消息
SSH-5-SSH_SESSION: SSH Session request from "%s" (tty = "%d") using crypto cipher '"%s"' "%s"	SSH 会话请求信息	无需操作 — 通知消息
SSH-5-SSH_USERAUTH: User '"%s"' authentication for SSH Session from "%s" (tty = "%d") using crypto cipher '"%s"' "%s"	SSH 用户验证状态信息	无需操作 — 通知消息

在本手册中使用以下术语和缩写词。对于此处未列出的术语定义，请参见 Allen-Bradley Industrial Automation Glossary (Allen-Bradley 工业自动化术语表，出版号：AG-7.1)。

802.11 该 IEEE 标准指定在 2.4 GHz 频段中工作的 1 和 2 兆比特 / 秒 (Mbps) 无线局域网的载波侦听介质访问控制和物理层规范。

802.11A 该 IEEE 标准指定在 5 GHz 频段中工作的无线局域网的载波侦听介质访问控制和物理层规范。

802.11B 该 IEEE 标准指定在 2.4 GHz 频段中工作的 5.5 Mbps 和 11 Mbps 无线局域网的载波侦听介质访问控制和物理层规范。

802.11g 该 IEEE 标准指定在 2.4 GHz 频段中工作的 6、 9、 12、 18、 24、 36、 48 和 54 Mbps 局域网的载波侦听介质访问控制和物理层规范。

802.3af 该 IEEE 标准指定以太网供电 (PoE) 的机制。该标准提供了通过标准以太网电缆供电和提供数据的能力。

BOOTP 引导协议。一种将 IP 地址静态分配给网络上的设备的协议。

BPSK 由符合 IEEE 802.11b 标准的无线局域网使用的一种调制技术，可实现 1 Mbps 速率传输。

CCK 补码键控。由符合 IEEE 802.11b 标准的无线局域网使用的一种调制技术，可实现 5.5 Mbps 和 11 Mbps 速率传输。

CCKM 思科集中式密钥管理。通过使用 CCKM，通过验证的客户端设备可从一个接入点漫游到另一个接入点，而不会在重关联期间出现任何可觉察的延迟。网络中的接入点提供无线域服务 (WDS)，并为子网上启用 CCKM 的客户端设备创建安全凭证缓存。当启用 CCKM 的客户端设备漫游到新的接入点时，凭证的 WDS 接入点缓存可显著缩短重新关联所需的时间。

CSMA 载波侦听多路访问。由 IEEE 802.11 规范指定的一种无线局域网介质访问方法。

dBi 一种全向天线比率，通常用于测量天线增益。 dBi 值越大，增益越高，覆盖角越尖锐。

DHCP 动态主机配置协议。许多操作系统可使用的一种协议，将指定范围内的 IP 地址自动发给网络上的设备。设备在管理员定义的指定时间内保持所分配的地址。

DNS 域名系统服务器。一种将文本翻译成 IP 地址的服务器。服务器保持主机字母和数字混合命名的名称及相应的 IP 地址的数据库。

DSSS 直接序列扩频。一种扩频无线电传输类型，可在很宽的频段范围内连续传播信号。

EAP 可扩展验证协议。一种可选的 IEEE 802.1x 安全功能，该功能非常适合拥有庞大用户群、且需要访问启用 EAP 远程验证拨入用户服务 (RADIUS) 服务器的机构。

ETSI 欧洲电信标准化协会 (ETSI) 开发了被许多欧洲国家及其他国家采用的标准。根据 ETSI 规范，功率输出和 EIRP 规范与美国区别很大。

GHz 千兆赫兹。每秒 10 亿个周期。一种频率度量单位。

IEEE 电气与电子工程师协会。一个通过其出版物、会议和标准制定活动为电气工程师服务的专业协会。该机构负责以太网 802.3 和无线局域网 802.11 规范。

IP 地址 工作站的网际协议 (IP) 地址。

IP 子网掩码 用于标识 IP 子网的编号，表明该 IP 地址是否可在局域网上识别，或是否必须通过网关才能到达。该编号的表示方式与 IP 地址类似；例如：255.255.255.0。

MAC 介质访问控制地址。在以太网数据包中用于识别以太网设备而使用的唯一 48 位编号，例如，接入点或客户端适配器。

PoE 以太网供电，描述通过以太网电缆供电的标准化或自组织系统。将数据和电力传送到无线接入点等设备的单根电缆。使用 PoE 的优点是可通过长电缆传送数据和电力。

RF 无线电频率。无线电技术通用术语。

RP-TNC 思科 Aironet 无线电设备和天线独有的一种连接器。涵盖扩频设备的 FCC 规则的第 15.203 部分限制了可用于传输设备的天线类型。根据本规则，思科 Aironet 和所有其他无线局域网供应商一样，为其无线电设备和天线配备了一种独特的连接器，以防止将未经认证的天线连接至无线电设备。

SSID 服务集标识符 (也被称为无线电网络名称)。用于识别无线电网络的唯一标识符，只有使用该标识符，工作站才能相互通信或与接入点通信。 SSID 可以是任意字母数字输入，最大长度为 32 个字符。

UNII 未经许可的国家信息基础设施 - 关于 UNII 设备在 5.15...5.35 GHz 和 5.725...5.825 GHz 的频段内工作的法规。

UNII-1 关于 UNII 设备在 5.15...5.25 GHz 频段内工作的法规。

UNII-2 关于 UNII 设备在 5.25...5.35 GHz 频段内工作的法规。

UNII-3 关于 UNII 设备在 5.725...5.825 GHz 频段内工作的法规。

WDS 无线域服务 (WDS)。在无线局域网中提供 WDS 的接入点保持无线局域网中支持 CCKM 的客户端设备的凭证缓存。当支持 CCKM 的客户端从一个接入点漫游到另一个接入点时， WDS 接入点将客户端凭证转发到具有多播密钥的新接入点。在客户端和新的接入点之间仅传送两个数据包，大大缩短了重关联时间。

WEP 有线等效保密。在 802.11 标准内定义的一种可选安全机制，可使无线设备的链路完整性等于电缆。

WPA Wi-Fi 保护访问 (WPA) 是一种基于标准的可互操作安全增强机制，可显著提高现有和未来无线局域网系统的数据保护和访问控制级别。其基于即将生效的 IEEE 802.11i 标准，并向前兼容。 WPA 利用 TKIP (临时密钥完整性协议) 进行数据保护， 802.1X 进行验证密钥管理。

单播数据包 发送至特定 IP 地址的单个数据消息 (数据包)。

多播数据包 发送至多个地址的单个数据消息 (数据包)。

多播数据包 发送到同一子网内所有地址的单个数据消息 (数据包)。

多路径 作为物理对象无线电信号回弹而产生的回波。

范围 发射器信号发送距离的一种线性度量。

发送功率 无线电传输的功率等级。

蜂窝 无线设备可与基站通信的无线电范围或覆盖范围。蜂窝大小取决于传输速度、所使用的天线类型、物理环境以及其他因素。

工作站 安装了客户端适配器的计算设备。

固件 烧写在存储器芯片中的软件。

基础设施 有线以太网。

接入点 一种无线局域网数据收发器，其使用无线电波将有线网络与无线工作站相连。

接收器灵敏度 接收器能够接收并正确转换成数据的最弱信号的度量单位。

客户端 一种使用无线接入点 / 工作组网桥的服务与局域网上的其他设备进行通信的无线电设备。

扩频 一种无线电传输技术，其相对于其他技术采用更宽的带宽传送用户信息，以实现改善干扰公差和无许可证操作等优势。

漫游 某些接入点具备这一功能，其允许您穿行于某个场所，同时保持与局域网的连接。

偶极子天线 一种包含两个 (通常为内部) 元件的低增益 (2.2-dBi) 天线。

全向 一种以球形图案发射其信号的天线。

全向 这通常指一种主要为圆形的天线辐射图案。

时隙 在发生冲突后，重新发送数据包之前设备等待的时长。短时隙可减少退避时间，即增加吞吐量。

数据包 在网络上通信的一个基本信息单元。数据包通常包括路由信息和数据，有时还会附带错误检测信息。

数据传输速率 设备支持的数据传输速率范围。数据传输速率的单位为兆比特 / 秒 (Mbps)。

四相相移键控 由符合 IEEE 802.11b 标准的无线局域网使用的一种调制技术，可实现 2 Mbps 速率传输。

天线增益 天线增益是衡量天线在某个空间区域内引导或聚集无线电能量的指标。高增益天线在特定方向具有更集中的辐射方向图。

调制 将用户信息与发射器的载波信号组合的多种技术中的任意一种。

退避时间 在局域网上发送数据包之前，工作站等待的随机时间长度。退避时间是时隙的倍数，因此时隙时间减少最终会降低退避时间，即增大吞吐量。

网关 一种将互不兼容的两个网络相连的设备。

文件服务器 一种文件存储库，以便局域网中可以共享文件、邮件和程序。

信标 通知无线设备可用性和是否存在的一种无线局域网数据包。信标数据包通过接入点和基站发送；但是，当在计算机至计算机 (自组织) 模式下工作时，客户端无线电卡发送信标。

已关联 工作站被配置为与接入点进行无线通信。

以太网 使用最广泛的有线局域网。以太网使用载波侦听多路访问 (CSMA) 允许计算机共享一个网络，并根据所使用的物理层以 10、 100 或 1000 Mbps 的速率工作。

域名 指根据组织类型或地理位置划分网络或网络资源的文本名称；例如：name.com —— 商业； name.edu —— 教育； name.gov —— 政府；ISPname.net —— 网络提供商 (例如， ISP) ； name.ar —— 阿根廷；name.au —— 澳大利亚，等等。

正交频分复用技术 (OFDM) 由符合 IEEE 802.11a 标准的无线局域网使用的一种调制技术，用于以 6、 9、 12、 18、 24、 36、 48 和 54 Mbps 的速率进行传输。

自组织网络 由不包含接入点的工作站构成的一种无线网络。

数字

字母

A

B

C

D

F

G

H

J

K

L

M

P

Q

R

S

T

W

X

Y

Z

罗克韦尔自动化支持

罗克韦尔自动化公司在网站上提供可帮助您使用其产品的技术信息。
您可访问 http://www.rockwellautomation.com/support，获取技术和应用说明、示例代码和软件补丁包的链接。也可访问支持中心 https://rockwellautomation.custhelp.com/ 获取软件更新，查找支持对话与支持论坛、技术信息、 FAQ，并登记参与产品通知更新。

另外，我们还提供多种安装、配置和故障处理支持计划。有关详细信息，请与本地分销商或罗克韦尔自动化销售代表联系，或者访问 http://www.rockwellautomation.com/services/online-phone。

安装帮助

如果您在安装后的最初 24 小时内遇到问题，请查阅本手册中包含的信息。您可以联系客户支持来获取首次帮助，以协助您安装好产品并完成试运行。

美国或加拿大	1.440.646.3434
美国或加拿大以外地区	使用 http://www.rockwellautomation.com/rockwellautomation/support/overview.page 上的 Worldwide Locator，或联系当地的罗克韦尔自动化代表。

新产品退货

在所有产品出厂前，罗克韦尔自动化公司都会进行测试，以确保产品完全可用。但是，如果您的产品不能正常工作需要退货，请遵循下列步骤。

美国	联系您的经销商。必须向分销商提供客户支持案例号码 (可拨打以上电话号码获取) 才能完成退货流程。
美国以外地区	请联系您当地的罗克韦尔自动化代表，以了解退货程序。

文档反馈

您的意见将帮助我们更好地满足您的文档需求。如果有任何关于如何改进本文档的建议，请填写 http://www.rockwellautomation.com/literature/ 上提供的表格 (出版号：RA-DU002)。

中文网址 www.rockwellautomation.com.cn
新浪微博 www.weibo.com/rockwellchina

动力、控制与信息解决方案总部
美洲地区：罗克韦尔自动化，南二大街1201号，密尔沃基市，WI 53204-2496 美国，电话：(1) 414.382.2000，传真：(1) 414.382.4444
欧洲/中东/非洲：罗克韦尔自动化，NV, Pegasus Park, De Kleetlaan 12a, 1831布鲁塞尔，比利时，电话：(32) 2 663 0600, 传真：(32) 2 663 0640
亚太地区：罗克韦尔自动化，香港数码港道100号数码港3座F区14楼1401-1403 电话：(852)2887 4788 传真：(852)2508 1486
中国总部：上海市徐汇区虹梅路1801号宏业大厦 邮编：200233 电话：(86 21)6128 8888 传真：(86 21)6128 8899
客户服务电话：400 620 6620 (中国地区)　　+852 2887 4666 (香港地区)

出版物 1783-UM006B-ZH-P - 2015 年 1 月
代替 1783-UM006A-ZH-P2014 年 5 月