配置Aironet 600系列OfficeExtend接入点

目录

简介

本文档提供有关配置用于Cisco Aironet® 600系列OfficeExtend无线接入点(OEAP)的思科无线局域网(WLAN)控制器的要求的信息。Cisco Aironet 600系列OEAP支持拆分模式操作，而且具有需要通过WLAN控制器进行配置的设施，以及可由最终用户在本地配置的功能。本文档还提供了有关正确连接和支持功能集所需的配置的信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Aironet 600系列OfficeExtend接入点(OEAP)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

设置准则

- 以下控制器支持Cisco Aironet 600系列OEAP：Cisco 5508、WiSM-2和Cisco 2504。
- 支持Cisco Aironet 600系列OEAP的第一个控制器版本是7.0.116.0
- 控制器的管理接口必须位于可路由的IP网络上。
- 需要更改公司防火墙配置，以允许具有UDP端口号5246和5247的流量。

Office Extend解决方案概述

- 向用户提供一个预先设定了公司控制器IP地址的接入点(AP)，或者用户可以从配置屏幕（设置HTML页面）输入控制器的IP地址。
- 用户将AP插入其家用路由器。
- AP从其主路由器获取IP地址，加入预置控制器并创建安全隧道。
- 然后，Cisco Aironet 600系列OEAP会通告公司SSID，它将相同的安全方法和服务通过WAN扩展到用户家中。
- 如果配置了远程LAN，则AP上的一个有线端口将通过隧道返回控制器。
- 然后，用户可另外启用本地SSID供个人使用。

防火墙配置指南

防火墙上的常规配置是允许CAPWAP控制和CAPWAP管理端口号通过防火墙。Cisco Aironet 600系列OEAP控制器可放置在DMZ区域中。

注意：需要在WLAN控制器和Cisco Aironet 600系列OEAP之间的防火墙上打开UDP 5246和5247端口。

下图显示了DMZ上的Cisco Aironet 600系列OEAP控制器：

以下是防火墙配置示例：

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

为了将内部AP-Manager IP地址作为CAPWAPP发现响应数据包的一部分传输到OfficeExtend AP，控制器管理员需要确保在AP-Manager接口中启用了NAT，并且向AP发送了正确的NATed IP地址。

注意：默认情况下，启用NAT时，WLC在AP发现期间仅使用NAT IP地址进行响应。如果AP存在于NAT网关的内部和外部，请发出以下命令，以便将WLC设置为同时使用NAT IP地址和非NAT（内部）管理IP地址进行响应：

<#root>

```
config network ap-discovery nat-ip-only disable
```

注意：只有在WLC具有NAT IP地址时，才需要执行此操作。

下图显示了NAT是否已启用，假设WLC具有NAT IP地址：

注意：如果控制器配置了互联网可路由IP地址并且不在防火墙后面，则不需要在控制器中进行此配置。

Office Extend AP-600配置步骤

Cisco Aironet 600系列OEAP将作为本地模式接入点连接到WLC。

注意：600系列不支持监控器、H-REAP、嗅探器、恶意程序检测、网桥和SE-Connect模式，这些模式不可配置。

注意：1040、1130、1140和3502i系列接入点中的Cisco Aironet 600系列OEAP功能要求为混合REAP (H-REAP)配置AP，并将AP的子模式设置为Cisco Aironet 600系列OEAP。这对于600系列来说是不可能的，因为它使用本地模式，并且不能更改。

MAC过滤可在初始加入过程中用于AP身份验证，以防止未经授权的Cisco Aironet 600系列OEAP设备加入控制器。下图显示启用MAC过滤和配置AP安全策略的位置：

此处输入以太网MAC（不是无线电MAC地址）。此外，如果将MAC地址输入到Radius服务器，则必须使用小写。您可以在AP事件日志中查看有关如何发现以太网MAC地址的信息（稍后将详细介绍）。

无线局域网和远程局域网配置设置

Cisco Aironet 600系列OEAP上有一个物理远程LAN端口(黄色端口#4)。其配置方式与WLAN非常相似。但是，因为它不是无线端口，并且是AP背面的有线LAN端口，因此它被调出并作为远程LAN端口进行管理。

虽然设备上只有一个物理端口，但如果使用集线器或交换机，最多可以连接四个有线客户端。

注意：远程局域网客户端限制支持将交换机或集线器连接到多个设备的远程局域网端口，或者直接连接到连接到该端口的Cisco IP电话。

注意：只有前四个设备可以连接，直到其中一个设备空闲超过一分钟。如果使用802.1x身份验证，则尝试在有线端口上使用多个客户端时可能会出现问题。

注意：此数字不会影响为控制器WLAN设置的十五个限制。

远程LAN的配置与控制器上配置的WLAN和访客LAN的配置类似。

WLAN是无线安全配置文件。这些是您的公司网络使用的配置文件。Cisco Aironet 600系列OEAP最多支持两个WLAN和一个远程LAN。

远程LAN与WLAN类似，不同之处在于它映射到接入点背面的有线端口(黄色端口#4)，如下图所示：

注意：如果您有两个以上的WLAN或多个远程LAN，则需要将所有这些LAN放入一个AP组中。

下图显示了WLAN和远程LAN的配置位置：

下图显示了一个示例OEAP组名称：

下图显示了WLAN SSID和RLAN配置：

如果将Cisco Aironet 600系列OEAP输入到AP组中，则配置该AP组时适用两个WLAN和一个远程LAN的相同限制。此外，如果Cisco Aironet 600系列OEAP在默认组中（这意味着它不在定义的AP组中），则需要将WLAN/远程LAN ID设置为小于ID 8，因为此产品不支持更高的ID集。

保留ID设置为小于8的设置，如下图所示：

注意：如果创建其他WLAN或远程LAN的目的是更改Cisco Aironet 600系列OEAP所使用的WLAN或远程LAN，请在启用600系列上的新WLAN或远程LAN之前禁用您正在删除的当前WLAN或远程LAN。如果为AP组启用多个远程LAN，请禁用所有远程LAN，然后仅启用一个。

如果为一个AP组启用了两个以上的WLAN，请禁用所有WLAN，然后仅启用两个。

WLAN安全设置

在WLAN中设置安全设置时，600系列不支持某些特定元素。

对于第2层安全性，Cisco Aironet 600系列OEAP仅支持以下选项：

- 无
- WPA+WPA2
- 静态WEP也可用于。11n数据速率，但不可用于。

注意：仅应选择802.1x或PSK。

TKIP和AES的WPA和WPA2的安全加密设置必须相同，如下图所示：

以下图像提供了TKIP和AES不兼容设置的示例：

注意：注意安全设置允许不支持的功能。

这些图像提供了兼容设置的示例：

MAC 过滤

安全设置可以保持打开状态、设置为MAC过滤或设置为Web身份验证。默认使用MAC过滤。

下图显示了第2层和第3层MAC过滤：

管理QoS设置：

还应管理高级设置：

注意：

- 不应启用覆盖盲区检测。
- 不应启用Aironet IE（信息元素），因为它们未被使用。
- 管理帧保护(MFP)也不受支持，应禁用或配置为可选，如下图所示：

- 不支持客户端负载均衡和客户端频段选择，不应启用这些功能：

支持的用户计数

任何时候仅允许15个用户连接600系列上提供的WLAN控制器WLAN。在第一个客户端之一取消身份验证或控制器上出现超时之前，第16个用户无法进行身份验证。

注意：此数字是600系列上所有控制器WLAN的累计数字。

例如，如果配置了两个控制器WLAN，并且其中一个WLAN上有15个用户，则届时任何用户都不能加入600系列上的其他WLAN。此限制不适用于最终用户在专供个人使用的600系列上配置的本地专用WLAN，并且这些专用WLAN或有线端口上连接的客户端不会影响这些限制。

信道管理和设置

600系列的无线电通过600系列的本地GUI控制，而不是通过无线局域网控制器控制。

尝试通过控制器控制频谱信道、功率或禁用无线电将对600系列没有任何影响。

只要本地GUI上的默认设置在两个频谱中均为默认值，600系列就会在启动期间扫描和选择2.4 GHz和5.0 GHz信道。

注意：如果用户在本机禁用一个或两个无线电（该无线电也被禁止用于公司访问）（如上所述），则RRM和高级功能（如监控、H-REAP、嗅探器）的功能超出了面向家庭和远程工作人员使用的Cisco Aironet 600系列OEAP的功能。

此处在Cisco Aironet 600系列OEAP的本地GUI上配置了5.0 GHz的信道选择和带宽。

注意：

- 5 GHz提供20和40 MHz宽设置。
- 不支持2.4 GHz 40 MHz宽频段，固定在20 MHz频段。
- 2.4 GHz中不支持40 MHz宽（信道绑定）。

其他警告

Cisco Aironet 600系列OEAP专为单AP部署而设计。因此，不支持在600系列之间进行客户端漫游。

注意：在控制器上禁用802.11a/n或802.11b/g/n可能不会在Cisco Aironet 600系列OEAP上禁用这些频谱，因为本地SSID可能仍在工作。

最终用户可以对Cisco Aironet 600系列OEAP内部的无线电启用/禁用控制。

有线端口支持802.1x

在此初始版本中，仅命令行界面(CLI)支持802.1x。

注意：尚未添加GUI支持。

这是Cisco Aironet 600系列OEAP背面的有线端口(黄色端口#4)，绑定到远程LAN（请参阅前面关于配置远程LAN的部分）。

您可以随时使用show命令显示当前的远程LAN配置：

<#root>

show remote-lan <*remote-lan-id*>

要更改远程LAN配置，必须先将其禁用：

<#root>

remote-lan disable <*remote-lan-id*>

为远程LAN启用802.1X身份验证：

<#root>

config remote-lan security 802.1X enable <*remote-lan-id*>

可以使用以下命令撤消该命令：

<#root>

config remote-lan security 802.1X disable <*remote-lan-id*>

对于远程LAN，“加密”始终为“无”(如show remote-lan所示)且不可配置。

如果要使用本地EAP（在控制器中）作为身份验证服务器：

<#root>

config remote-lan local-auth enable <*profile-name*> <*remote-lan-id*>

其中，profile是通过控制器GUI(Security > Local EAP)或CLI(config local-auth)定义的。有关此命令的详细信息，请参阅控制器指南。

您可以使用以下命令撤消它：

<#root>

config remote-lan local-auth disable <*remote-lan-id*>

或者，如果使用外部AAA身份验证服务器：

- config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>
- config remote-lan radius_server auth enable/disable <remote-lan-id>

其中server是通过控制器GUI(Security > RADIUS > Authentication)或CLI(config radius auth)配置的。有关此命令的详细信息，请参阅控制器指南。

完成配置后，启用远程LAN：

<#root>

config remote-lan enable <*remote-lan-id*>

请使用show remote-lan <remote-lan-id>命令以验证您的设置。

对于远程LAN客户端，您需要启用802.1X身份验证并相应地配置。请参阅您的设备用户指南。

OEAP-600接入点配置

下图显示Cisco Aironet 600系列OEAP的布线图：

Cisco Aironet 600系列OEAP的默认DHCP作用域是10.0.0.x，因此您可以使用地址10.0.0.1浏览端口1-3上的AP。默认用户名和密码为admin。

注意：这不同于使用Cisco作为用户名和口令的AP1040、1130、1140和3502i。

如果无线电已启动，并且已配置个人SSID，则您可以无线访问配置屏幕。否则，需要使用本地以太网端口1-3。

要登录，默认用户名和密码为admin。

注意：黄色端口#4对于本地使用来说处于非活动状态。如果在控制器上配置了远程LAN，则此端口会在AP成功加入控制器后通过隧道返回。为了浏览设备，在本地使用端口1-3：

成功浏览到设备后，您将看到主状态屏幕。此屏幕提供无线电和MAC统计信息。如果尚未配置无线电，配置屏幕将允许用户启用无线电、设置信道和模式、配置本地SSID和启用WLAN设置。

在SSID屏幕上，用户可以配置个人WLAN网络。设置公司无线电SSID和安全参数，并从控制器向下

推送这些参数（在您使用控制器的IP配置WAN之后），并且成功加入网络。

下图显示了SSID本地MAC过滤配置：

用户配置个人SSID后，下方的屏幕允许用户在专用家庭SSID上设置安全性，启用无线电，并根据需要配置MAC过滤。如果个人网络使用802.11n速率，建议用户选择身份验证类型、加密类型和启用WPA2-PSK和AES的口令。

注意：如果用户选择禁用其中一个或两个无线电（同时禁用两个无线电供企业使用），则这些SSID设置与企业设置不同。

在本地有权访问管理控制设置的用户可以控制核心功能，如无线电启用/禁用，除非设备受密码保护且由管理员配置。因此，必须注意不要禁用这两个无线电，因为即使设备成功加入控制器，这也会导致连接丢失。

下图显示系统安全设置：

预计家庭远程工作人员会在家庭路由器后面安装Cisco Aironet 600系列OEAP，因为此产品并非旨在替代家庭路由器的功能。这是因为此产品的当前版本不支持防火墙、PPPoE支持或端口转发。这些是客户期望在家庭路由器中能找到的功能。

虽然此产品可以在没有家用路由器的情况下使用，但出于上述原因，建议不要将其定位为家庭路由器。此外，直接连接到某些调制解调器可能存在兼容性问题。

鉴于大多数家庭路由器的DHCP作用域在192.168.x.x范围内，此设备的默认DHCP作用域为10.0.0.x，并且是可配置的。

如果家用路由器恰好使用10.0.0.x，则必须将Cisco Aironet 600系列OEAP配置为使用192.168.1.x或兼容的IP地址，以避免网络冲突。

下图显示了DHCP作用域配置：

注意：如果Cisco Aironet 600系列OEAP未由IT管理员转移或配置，则用户需要输入公司控制器的IP地址（请参阅下文），以便AP可以成功加入控制器。在成功加入后，AP应从控制器下载最新的映像和配置参数（例如公司WLAN设置）。此外，如果配置了远程局域网设置，有线端口#4在Cisco Aironet 600系列OEAP的背面。

如果它没有加入，请验证控制器的IP地址是否可通过互联网访问。如果启用了MAC过滤，请验证是否已成功将MAC地址输入控制器。

下图显示Cisco Aironet 600系列OEAP控制器的IP地址：

OEAP-600接入点硬件安装

下图显示了Cisco Aironet 600系列OEAP的物理特性：

此AP设计为安装在桌子上，并且有橡胶支脚。它还可以安装在墙上，或者使用提供的托架直立放置。尝试将AP尽可能靠近目标用户。避免使用金属表面较大的区域，例如将设备放在金属桌面上或靠近大镜子。AP与用户之间的墙壁和物体越多，信号强度越低，而且会降低性能。

注意：此AP使用+12伏电源，不使用以太网供电(PoE)。此外，设备不提供PoE。确保将正确的电源适配器用于AP。此外，请确保不使用来自其他设备（例如笔记本电脑和IP电话）的其他适配器，因为这些适配器可能会损坏AP。

该单元可通过塑料锚或木螺钉安装在墙壁上。

该单元可以使用所提供的托架直立安装。

Cisco Aironet 600系列OEAP的边缘设有天线。用户应该注意不要将AP放置在金属物体或障碍物附近可能导致信号定向或减弱的区域。天线增益在两个频段中均约为2 dBi，设计为以360度模式辐射。类似于灯泡（没有灯罩），其目标是向所有方向辐射。将AP视为一个灯泡，并尝试将其放在用户附近。

金属物体（如镜子）会像灯罩一样阻挡信号。如果信号必须穿透或穿过实心物体，您可能会遇到吞吐量或范围降低的问题。如果您希望连接（例如在三层住宅中），请避免将AP放置在地下室，并尝试将AP安装在家庭内的中心位置。

接入点有六根天线（每个频段三根）。

此图显示2.4 GHz天线辐射图（取自左下角天线）。

此图显示5 GHz天线辐射图（取自中右天线）：

排除OEAP-600故障

检验初始配线是否正确。这确认Cisco Aironet 600系列OEAP上的WAN端口已连接到路由器，可以成功接收IP地址。如果AP似乎没有加入控制器，请将PC连接到端口1-3（家庭客户端端口），并查看是否可以使用默认IP地址10.0.0.1浏览到AP。默认用户名和密码为admin。

验证是否已设置公司控制器的IP地址。如果没有，请输入IP地址并重新启动Cisco Aironet 600系列OEAP，以便尝试建立到控制器的链路。

注意：公司端口#4（黄色）不能用于浏览设备以进行配置。除非配置了远程LAN，否则这实际上是“死端口”。然后，它将通过隧道返回公司（用于有线企业连接）

检查事件日志以查看关联如何进行（稍后将详细介绍）。

下图显示了Cisco Aironet 600系列OEAP布线图：

下图显示Cisco Aironet 600系列OEAP连接端口：

如果Cisco Aironet 600系列OEAP无法加入控制器，建议您检查以下项目：

1. 验证路由器是否正常运行且已连接到Cisco Aironet 600系列OEAP的WAN端口。
2. 将PC连接到Cisco Aironet 600系列OEAP的一个端口1-3。它应该能看到Internet。
3. 验证企业控制器的IP地址是否在AP中。
4. 确认控制器处于DMZ中且可通过互联网访问。

5. 确认加入并确认思科徽标LED为蓝色或紫色。

6. 如果AP需要加载新映像并重新启动，请留出足够时间。

7. 如果使用防火墙，请验证UDP 5246和5247端口是否未被阻止。

下图显示Cisco Aironet 600系列OEAP徽标LED状态：

如果连接过程失败，则LED会循环显示颜色或闪烁橙色。如果出现这种情况，请检查事件日志以了解详细信息。为了访问事件日志，请浏览到AP（使用个人SSID或有线端口1-3）并捕获此数据供IT管理员查看。

下图显示Cisco Aironet 600系列OEAP事件日志：

如果加入过程失败，并且这是Cisco Aironet 600系列OEAP首次尝试连接到控制器，请检查Cisco Aironet 600系列OEAP的AP加入统计信息。为此，您需要AP的基本无线电MAC。事件日志中可以找到此信息。以下是包含注释的事件日志示例，以帮助您解释以下内容：

一旦知道这一点，您就可以查看控制器监控器统计信息，以确定Cisco Aironet 600系列OEAP是否已加入控制器或者是否曾经加入控制器。此外，这还应说明发生故障的原因或是否发生故障。

如果需要AP身份验证，请验证是否已在小写情况下将Cisco Aironet 600系列OEAP以太网MAC地址（不是无线电MAC地址）输入到Radius服务器。您还可以从事件日志中确定以太网MAC地址。

在控制器上搜索Cisco Aironet 600系列OEAP

如果您确定可以从连接到本地以太网端口的PC访问Internet，但AP仍无法加入控制器，并且您已确认在本地AP GUI中配置了控制器IP地址并且可访问，则请确认该AP是否已成功加入。也许AP不在AAA服务器中。或者，如果DTLS握手失败，则AP可能在控制器上出现错误证书或日期/时间错误。

如果Cisco Aironet 600系列OEAP设备无法加入控制器，请验证控制器是否在DMZ上可访问，并且是否打开UDP端口5246和5247。

如何调试客户端关联问题

AP正确加入控制器，但无线客户端无法与公司SSID关联。检查事件日志以查看关联消息是否到达AP。

下图显示客户端与企业SSID与WPA或WPA2关联的正常事件。对于采用开放式身份验证或静态WEP的SSID，只有一个`ADD MOBILE`事件。

事件日志-客户端关联

如果(Re)Assoc-Req事件不在日志中，请验证客户端是否具有正确的安全设置。

如果日志中显示(Re)Assoc-Req事件，但客户端无法正确关联，请对客户端的控制器启用debug client <MAC地址>命令，并调查问题，方法与使用其他Cisco非OEAP接入点的客户端相同。

如何解释事件日志

以下事件日志和注释可帮助您对其他Cisco Aironet 600系列OEAP连接问题进行故障排除。

以下是从Cisco Aironet 600系列OEAP事件日志文件中收集的一些示例，其中包含有助于解释事件日志的注释：

Internet连接不可靠时

此部分中的事件日志示例可能发生在Internet连接失败或最终非常缓慢或断断续续时。这可能是由您的ISP网络、ISP调制解调器或您的家庭路由器导致的。有时，来自ISP的连接会断开或变得不可靠。发生这种情况时，CAPWAP链路（回公司隧道）可能会发生故障或遇到困难。

以下是事件日志中此类故障的示例：

其他调试命令

在酒店或其他付费使用场所使用Cisco Aironet 600系列OEAP时，在Cisco Aironet 600系列OEAP通过隧道返回控制器之前，您需要穿过封闭花园。为此，请将笔记本电脑插入一个有线本地端口（端口1-3）或使用个人SSID登录酒店并满足初始屏幕要求。

从AP的主端连接到Internet后，设备会建立DTLS隧道和您的公司SSID。然后，有线端口#4（假设配置了远程LAN）将变为活动状态。

注意：这可能需要几分钟的时间，请观察思科徽标LED的蓝色或紫色，以表示成功加入。此时，个人和企业连接都处于活动状态。

注意：当酒店或其他ISP断开连接时（通常为24小时），隧道会中断。然后，您必须重新开始相同的流程。这是有意为之，也是正常的。

下图显示了Office Extend的付费配置：

下图显示了其他调试命令（无线电接口信息）：

已知问题/警告

当您将配置文件从控制器上载到TFTP/FTP服务器时，远程LAN配置将作为WLAN配置上载。有关详细信息，请参阅Cisco无线LAN控制器和版本7.0.116.0的轻量接入点发行版本注释。

在OEAP-600上，如果CAPWAP连接由于控制器上的身份验证失败而失败，在OEAP-600尝试重新启动CAPWAP尝试之前，OEAP-600上的Cisco徽标LED可能会关闭一段时间。这是正常现象，因此您应该注意，如果徽标LED暂时关闭，AP不会熄灭。

此OEAP-600产品的登录名与之前的OEAP接入点不同，为了与诸如Linksys等家庭产品一致，默认用户名为admin，密码为admin；其他Cisco OEAP接入点（例如AP-1130和AP-1140）的默认用户名为Cisco，密码为Cisco。

此第一版OEAP-600支持802.1x，但仅在CLI上受支持。尝试更改GUI的用户可能会丢失其配置。

当您在酒店或其他付费场所使用OEAP-600时，在OEAP-600能够通过隧道返回控制器之前，您需要穿过封闭花园。只需将笔记本电脑插入一个本地有线端口（端口1-3）或使用个人SSID登录酒店并

满足初始屏幕即可。从AP的主端连接到Internet后，设备会建立DTLS隧道，并且您的公司SSID和有线端口#4（假设已配置远程LAN）会变为活动状态。请注意，这可能需要几分钟的时间，请观察思科徽标LED是否呈蓝色或紫色，以表示成功加入。此时，个人和企业连接都处于活动状态。

注意：当酒店或其他ISP断开连接时（通常为24小时），隧道可能会中断，您必须重新启动同一进程。这是有意为之，也是正常的。

Office Extend in pay for use场所

以下是Cisco 7.2版本中引入的一些其他增强功能：

- GUI中添加了802.1x安全功能
- 能够禁用从控制器对AP进行本地WLAN访问-禁用个人SSID，仅允许公司配置
- 信道分配可选选项
- 支持从2个企业SSID更改为3个SSID
- 支持双RLAN端口功能

GUI中添加了802.1x安全功能

802.1x现已添加到GUI

有关远程LAN端口的身份验证的说明。

能够禁用从控制器对AP进行本地WLAN访问-禁用个人SSID，仅允许公司配置

禁用本地无线局域网访问

信道分配可选选项包括：

- AP在本地控制
- WLC控制

RF信道和功率分配现在由本地或WLC控制

支持双RLAN端口功能（仅限CLI）

此注意事项适用于使用双RLAN端口功能的OEAP-600系列AP，此功能允许OEAP-600以太网端口3作为远程LAN运行。仅允许通过CLI进行配置，以下是一个示例：

```
Config network oeap-600 dual-rlan-ports enable|disable
```

如果未配置此功能，则单端口4 remote-lan将继续运行。每个端口对每个端口使用唯一的远程LAN。

远程LAN映射不同，这取决于使用的是默认组还是AP组。

默认组

如果使用默认组，则具有偶数远程LAN ID的单个远程LAN将映射到端口4。例如，remote-lan-id 2的remote-lan映射到端口4（在OEAP-600上）。具有奇数编号的remote-lan ID的remote-lan将映射到OEAP-600上的端口3。

例如，请看以下两个remote-lan：

```
(Cisco Controller) >show remote-lan summary

Number of Remote LANS.......................... 2

RLAN ID  RLAN Profile Name    Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

rlan2具有偶数的远程lan ID 2，因此映射到端口4。rlan3具有奇数的远程lan ID 3，因此映射到端口3。

AP组

如果使用AP组，则到OEAP-600端口的映射取决于AP组的顺序。要使用AP组，您必须首先从AP组中删除所有远程LAN和WLAN，并将其留空。然后将两个远程LAN添加到AP组。首先添加端口3 AP remote-LAN，然后添加端口4远程组，最后添加所有WLAN。

如本例所示，远程局域网在列表中的第一个位置映射到端口3，在列表中的第二个位置映射到端口4：

```
RLAN ID  RLAN Profile Name      Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

相关信息

- Cisco 无线 LAN 控制器配置指南 7.0 版
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。