思科 Aironet 1130 AG 系列 AP H-Reap 模式设计和部署指南

文档编号: **71250**

介绍

前提

要求

使用的设备

惯例

LWAPP 背景知识

在思科统一无线网络架构中部署 **LWAPP**

混合式远端边界无线接入点

H-REAP 原理

H-REAP 重要概念

H-REAP 控制器发现

H-REAP 无线安全支持

TRUNK 与非 TRUNK

H-REAP 设计及功能限制

H-REAP WAN 需求

H-REAP 配置

有线网络准备

H-REAP 使用命令行进行控制器发现

H-REAP 控制器配置

H-REAP 排障

H-REAP 无法加入控制器

H-REAP Console 口无法配置并返回错误信息

客户端无法连接到 H-REAP

H-REAP 是否可以工作在 NAT 下?在配置静态 NAT 的环境中，WLC 和 H-REAP 时候可以放置在静态 NAT 后？

H-REAP Q&A

相关信息

介绍

混合式远端边界无线接入点（AP）（H-REAP）是一种适用于分支机构和远程办公室的无线部署解决方案。它使客户可以通过广域网（WAN）链路对分支机构或远程办公室的AP进行配置和控制，而不需要在每个办公室部署一个控制器（Controller）。当与Controller之间的链路中断时，工作在H-REAP模式的AP可以在本地进行客户端的数据交换以及身份验证。当AP重新可以连接到Controller时，H-REAP模式下的AP也可以重新与Controller之间建立数据隧道。

前提

要求

H-REAP模式仅在以下设备上支持：1130AG，1240AG，1250和AP801系列AP；2100和4400系列控制器，Catalyst 3750G系列集成无线局域网控制器交换机，Cisco WiSM服务模块，以及集成多业务路由器（ISR）上的控制器网络模块。

使用的设备

本文的内容是基于以下的硬件平台与软件版本的：

- 思科WLC（ 2100和4400系列） 5.1版
- 基于1130， 1240和1250一系列LAP的轻量级接入点协议（ LWAPP ）

惯例

更多文档惯例的信息，请参见思科技术提示惯例。

LWAPP 背景知识

LWAPP作为思科统一无线网络架构的基础，指定了两个不同的主要模式用于AP的操作：

- Split-MAC（分离MAC）— 在Split-MAC模式下，系统承担了在802.11中规定的接入点和控制器之间互操作的主要功能。在这种配置中，控制器不仅负责802.11认证和关联过程的处理，它还作为所有用户流量单一的入口和出口。分离MAC的接入点将所有客户端流量通过与控制器之间LWAPP数据隧道传回控制器（ LWAPP控制数据流也遵循同样的数据隧道）。
- Local MAC（本地MAC）— 本地MAC模式，在AP上实现充分的802.11功能，通过将客户端数据流终结在AP的有线端口上来允许数据层与控制路径的分离。这不仅使得本地的无线资源直接连入AP，同时允许LWAPP控制路径（AP和控制器之间的链路， AP和控制器）中断时，无线服务能够得以保持，提供链路的容错性。这样的功能，对于只有少数几个接入点，通过WAN链路与总部进行连接的小型远程办公室和分支机构之间来说特别有用，与部署一台控制器的成本比起来更加合理。

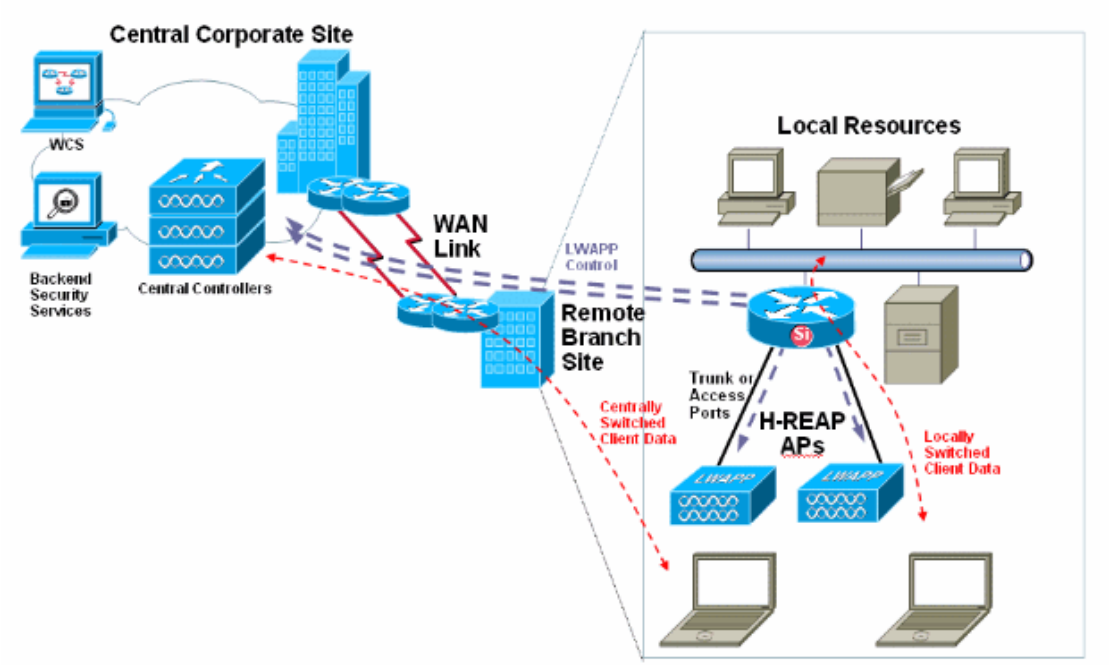
在思科统一无线网络架构中部署 LWAPP

所有基于LWAPP的接入点都支持分裂MAC模式，在系统配置接口通常被称为本地模式

（勿将之与LWAPP中的“Local MAC”混淆），但只有Aironet 1030 REAP属于Local MAC类别，在系统配置中明确称为REAP。
1030 REAP，在提供广域网故障容错和本地数据交换的同时，可能无法满足所有远程和分支办公室安装的需要。虽然1030 REAP在无线侧支持数据分离（通过对多种基本服务集标识符[BSSIDs]的支持），但在有线侧，由于缺乏对802.1Q的支持，无法实现数据分离。不同的无线数据最终将会落到相同的有线子网上去。此外，在广域网链路发生故障时，1030 REAP将仅提供在控制器上明确指定的WLAN的服务。
正是由于这两个限制，H-REAP应运而生。

混合式远端边界无线接入点

H-REAP，是在1131，1242，1250和AP801系列AP上支持的特性，同时只在CUWN4.0及以后支持改特性。该软件可选的特性使得对Split MAC和Local MAC两种LWAPP部署模式的支持更加灵活。基于每个WLAN的配置，该WLAN内的客户端数据既可以通过H-REAP进行本地交换，也可以通过H-REAP与控制器间的隧道传回控制器。此外，在H-REAP进行本地交换的客户端的数据流量可以通过802.1Q的TAG实现有线侧不同WLAN数据的分离。在广域网链路中断发生时，本地WLAN的数据交换以及本地认证仍然能够照常运行。
以下是一张H-REAP部署的示意图



如图所示，H-REAP设计用于为远程和分支办公室的部署。
本文档概述了H-REAP的原理，控制器和接入点的配置，以及网络设计方面的考虑。

H-REAP 原理

H-REAP 重要概念

有几个不同的模式，H-REAP有多种不同的模式，通过不同的模式，H-REAP可以实现本地和中心的切换以及广域网链路的自存活性。两套模式的结合使用，在不同的配对情况下提供一系列的功能，也存在不同的局限性。

以下是这两套模式：

- **集中交换与本地交换**
  H-REAP上的WLAN（将安全，服务质量和其他参数整合于SSID的协议组）可设置为需要将所有的数据流量通过隧道传回到控制器（称为集中交换）或WLAN可能配置为将客户端数据终结在本地的H-REAP的有线端口上（称为本地交换）。进行本地交换的WALN可以选择对数据进行802.1Q标记，允许这些WLAN可以在AP的以太网接口上进行独立的传输。
- **连接与独立**
  当LWAPP控制层数据与控制器的连接有效，则称H-REAP处于连接模式，也就是说WAN链路没有中断。独立模式是指H-REAP与控制器之间不再存在控制连接时的工作状态。

注：当H-REAP处于连接模式，所有H-REAP安全认证处理进程（如后端RADIUS身份验证和成对主密钥[PMK]推送）都发生在控制器端。无论AP处于哪种模式，所有802.11认证和关联进程的处理都发生在H-REAP端。在连接模式下，H-REAP的关联/验证都由控制器代理。在独立模式下，AP不能告知控制器此类进程的发生。

H-REAP的功能性取决于其不同的运作模式（一个H-REAP处于连接还是独立模式），以及每个WLAN的数据交换（集中交换还是本地交换）和无线安全是怎样配置的。

当一个客户端连接到的H-REAP后，AP将所有的认证信息转发至控制器，成功验证后，客户端的数据包将会按照与其关联WLAN的配置，要么进行本地交换，要么通过数据隧道传回给控制器进行集中交换。由客户端的认证机制以及数据交换方式的不同，根据WLAN的配置以及AP/控制器间的连接性的不同，建立在H-REAP上的WLAN可处于下列任何一种状态：

- **中心认证，集中交换** — 在此状态下，对于给定的WLAN，AP将所有客户端身份验证请求以及客户端数据都转发到控制器。这种状态只有当AP的LWAPP控制路径是通的时候才是有效的。这意味着在H-REAP处于连接模式。不管身份验证方法是怎样的，当WAN中断的情况下，任何通过隧道连接至控制器的WLAN都将丢失。
- **中央认证，本地交换** — 在此状态下，对于给定的WLAN，控制器处理所有的客户端身份验证，并在H-REAP进行本地数据交换。在客户端身份验证成功后，控制器发出LWAPP控制命令，控制H-REAP在本地对特定的客户端数据进行交换。.在客户端认证成功后，LWAPP信息将针对每个客户端进行发送。这种状态只适用于连接模式。
- **本地认证，本地交换** — 在此状态下，H-REAP在本地处理客户端的接入认证以及

交换客户端的数据包。这种状态这只有在独立模式时是后效的，同时支持的认证类型只能是AP本地可以处理的类型。

注：所有的二层的无线数据加密始终是由AP进行处理的。当AP处于连接状态时，所有客户端身份验证进程都将发生在控制器侧（或从控制器进行上传，根据WLAN和控制器的配置而定）。

- **认证失效，本地交换** — 在此状态下，对于给定的WLAN，H-REAP拒绝接受任何新的客户端尝试进行的身份验证，但它继续发出beacon和probe回复，以保持现有客户的正确连接。只有在独立模式下该状态是有效的。

  如果本地交换WLAN配置为接受任何身份验证类型，这些认证类型需要由控制器进行处理（如的EAP认证[动态WEP/WPA/WPA2/802.11i] ，WebAuth ，或者NAC认证）时，当广域网中断，AP进入认证失效，当地交换状态。在这之前，它处于中心认证，本地交换状态。现有的无线客户端连接能够得以保持，同时能够继续使用本地的有线资源，但新的客户端关联将不被允许。如果使用Web认证的用户的Web认证超时，或者，如果使用802.1X认证的用户的EAP Key有效期满需要进行重认证时，现存的客户端将失去连接，同时重新进行连接的请求将被拒绝（这个时间间隔具体是由RADIUS服务器制定的，并不是标准的）。此外，802.11漫游（在H-REAP之间进行）将会触发802.1X重认证，因此，客户端所在的AP将不运行新发起的连接请求。

  当这样一个WLAN的客户端数量为0时，H-REAP停止所有相关802.11职能，不再发送特定SSID的Beacon，此时WLAN进入下一个H-REAP状态：验证失效，交换失效。

  注：在控制器软件版本4.2或更高版本中，WLAN配置的802.1X，WPA-802.1X，WPA2-802.1X，或是CCKM，都可以工作在独立模式。但是，这些认证类型需要一个外部RADIUS服务器进行配置。更多细节，将在下文述及。

- **认证失效，交换失效** — 在此状态下，WLAN断开现有客户的关联，停止发送Beacon响应客户端发送的Probe。 该状态只在独立模式时有效。

  客户端数据配置为转发回控制器的WLAN转入验证失效，交换失效状态。此外，验证类型独立于控制器的WLAN，当没有客户端连接的时候会进入该状态。

  当H-REAP进入独立模式，WLAN的认证方式配置为开放，共享，WPA-PSK ，或是WPA2-PSK时，将进入“本地认证，本地交换”状态，并继续进行新的客户端认证。

  控制器软件版本4.2或更高版本，这也适用于WLAN的认证方式配置为802.1X，WPA-802.1X，WPA2-802.1X，或CCKM时，但这些认证类型需要一个外部RADIUS服务器进行配置。其他WLAN进入“认证失效，交换时效”状态（如WLAN配置为中央交换）或“认证失效，本地交换”状态（如WLAN为本地交换） 。

  当H-REAP进入独立模式，它中断所有进行集中交换的客户端的关联。对于进行Web认证的WLAN，当前连接的客户端不会被中断关联，但当与之关联的客户端数量达

到0时，H-REAP不再发送Beacon。它还发送向发起Web认证请求的客户端发出断开关联的信息。基于控制器的网络行为，如网络访问控制（ NAC ）和Web认证（Guest用户访问权限）将失效，同时接入点不再向控制器发送任何入侵检测系统（ IDS ）报告。此外，大多数无线资源管理（RRM）功能，如邻居发现，噪音，干扰，负载，和覆盖范围测量，使用的邻居列表，和流氓AP控制和检测，都将失效。然而，H-REAP在独立模式下支持动态频率选择。

注：如果您的控制器配置了NAC属性 ，那么只有当AP处于连接模式时，客户端才能正常关联。当NAC被启用，您需要建立一种不健康（或隔离）的VLAN ，使属于该VLAN任何客户端的数据能够通过该控制器，即使WLAN配置为本地交换，同样有效。在客户端被分配到一个隔离的VLAN，其所有数据包将进行集中交换。

H-REAP即使进入独立模式后仍然能够保持客户端的连接。但是，一旦AP重新建立与控制器之间的连接，它会首先断开所有的客户的关联，应用控制器下发的新的配置信息，重新允许客户端的连接。

H-REAP 控制器发现

在思科统一无线网络架构内，H-REAP支持每个控制器发现机制的特点。一旦AP得到一个IP地址（通过DHCP动态获得，或通过静态配置），AP就试图通过IP广播，DHCP选项43，DNS和空中配置（ OTAP ）在系统中发现控制器。最后，H-REAP记录下它们原先进行连接的控制器的IP地址。不同LAP注册到WLC的方式可以参阅Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)相关文档。

关于控制器发现有几点需要注意的。这些考虑适用于所有Aironet AP，而不仅仅是H-REAP。

- 如果AP通过DHCP获得IP地址，DHCP选项43仅仅是一个可行的H-REAP用户发现控制器的方法。
- OTAP只对已经连接到一个控制器和下载代码的AP有效。OTAP还要求其他附近的接入点发现并连接到一个控制器上，同时，其上OTAP已被启用。
- 支持H-REAP功能的AP不支持LWAPP2层模式。控制器必须设置成工作在3层LWAPP模式下。
- 更多接入点/控制器发现方式相关的信息，可在Deploying Cisco 440X Series Wireless LAN Controllers文档中找到。

除了这些传统的控制器发现机制，软件版本4.0和更高版本允许带有Console端口的Aironet AP支持通过控制台命令行进行手动配置。现在可以手动为AP设定静态IP地址，主机名，以及该AP应该连接的控制器的IP地址。这意味着，在其他发现机制无法实现的情况下，可以通过Console端口，手动对AP发现控制器所有的必要信息进行配置。

虽然这一功能在所有具有Console口的AP上都支持（而不只是用于H-REAP的配置），这个功能对于H-REAP特别有用，因为他们更可能被安装在没有配备DHCP服务器和控制器发现机制的地方，如在一个分支办公室。.因此，这一新的Console访问省却了H-REAP的两次运输：一次到一个中心节点进行配置，第二次到远程站点进行安装。

H-REAP 无线安全支持

基于之前提到的不同的模式和状态，H-REAP所支持的安全特性各不相同。任何需要在数据路径上进行控制的安全类型，如VPN，无法在进行本地交换的WLAN上实现，因为如果数据没有转发回控制器的话，WLC无法对数据进行控制。当H-REAP与控制器之间的路径是通的，任何其他的安全类型都能在集中交换或当地交换的WLAN中得到支持。当这个路径中断时，只有这些安全类型中的一部分，允许新客户端连接到本地交换的WLAN上。

如前所述，为了能够支持的802.1X EAP认证，在独立模式下的H-REAP需要有本地的RADIUS服务器来对客户端进行认证。此备份RADIUS服务器可以被控制器使用。你可以通过控制器的命令行为每个H-REAP AP配置一个备份RADIUS服务器，也可以通过控制器的图形控制界面或命令行为一个H-REAP组配置一个备份RADIUS服务器。为单个H-REAP AP配置的备份服务器可以覆盖为H-REAP组配置的备份服务器。

参阅Cisco Wireless LAN Controller Configuration Guide, Release 5.1的Configuring Hybrid-REAP Groups部分详细信息如何配置H-REAP组。

当H-REAP处于连接模式下，控制器可以设置和用户排除名单/黑名单，以防止一些客户与它的接入点进行关联。这个功能无论是在自动或手动方式下都可能发生。根据全局和每个WLAN的配置，客户可以由于主机的原因，多次失败验证的原因，以及任何特定的时间而被排除。客户端还可以被手动地加入到这一排除名单中。只有当接入点处于连接模式时，这一功能才能实现。但是，被列入这一排除名单的客户端即使是在独立模式，仍然无法连接到AP。

像VPN，Cranite，AirFortress需要控制器强制所有的流量都必须通过特定的节点（如VPN控制器或Cranite / AirFortress设备）。因此，WLAN的这些安全配置无法在本地交换中应用。如果需要部署这些安全方法，H-REAP WLAN，WPN，Cranite或AirFortress资源对H-REAP来说都必须是本地的，这样，客户端可以直接访问这些资源。即使有这样的安全资源在H-REAP本地可达，由于WLAN部署的本地交换，无论是控制器还是接入点都无法执行这样的安全政策。

注：如果WLAN使用的是Mac认证（本地的或上游的），当AP是在独立模式，将不再允许额外的客户端进行身份认证，相同模式下，配置802.1X或Web认证的WLAN同样会遇到这样的问题。

TRUNK 与非 TRUNK

H-REAP可以连接到802.1Q Trunk连接或未打标的接入连接。当连接到Trunk连接，H-REAP通过native VLAN发送LWAPP控制和数据流量回到控制器。本地交换的WLAN可将其流量转发到任何可用的VLAN （native VLAN，或其他VLAN）。当设置为运行在接入连接（没有802.1Q tag信息），H-REAP将所有LWAPP信息和本地交换的客户端

数据转发到与之相连的唯一的网段中去。

为H-REAP选择交换端口模式的一般准则如下：

- 如果有一个以上的WLAN配置为本地交换，同时对这些SSID对应的流量对应到不同的子网，那么使用Trunk连接。AP和上联交换机端口都需要配置802.1Q trunk。配置H-REAP为802.1Q中继是最常见的配置，并能提供最大的灵活性。
- 当H-REAP有不超过一个本地交换WLAN或多个本地交换WLAN不需要在有线端进行分离时，使用接入连接。需要知道的是，Trunk连接仍然是可取的，如果在这种情况下需要将LWAPP信息和用户数据分开的话。但是，这既不是一个配置的要求，也不是一个安全风险。

注：H-REAP有线接口默认运行在接入连接。

H-REAP 设计及功能限制

由于H-REAP的目的是控制器跨过WAN链路对AP进行控制，不仅有设计考虑，必须牢记当设计一个具有H-REAP的无线网络时，也有一些功能是完全或在部分的不支持。

每个地方H-REAP的部署数量是没有限制的。

由于事实上，在许多偏远的地方部署时，都只有少数的H-REAP，完全的无线资源管理（RRM）的功能可能并不在每个H-REAP站点得到支持。完全的无线资源管理代码可以在H-REAP中得到支持，但发射功率控制（TPC）算法只能在四个或多余是个AP在彼此可见范围内是才能被触发。因此，一些H-REAP可能永远不会关闭其无线模块。因此，在没有自动关闭电源的前提下，H-REAP不会上调发射功率，以补偿检测到的覆盖空洞。

动态频率选择（ DFS）在连接和独立模式下都能支持。

注：请参阅Radio Resource Manager under Unified Wireless Networks得到更多的无线资源管理的具体实现细节。

能够提供准确的设备位置的能力在不同地点之间有很大的不同，在较大程度上取决于部署的H-REAP的数量和密度。定位的精度在很大程度上取决于，信息收集得到的丰富程度，而这与AP的数量直接相关。由于H-REAP的部署在范围上有很大不同，这个位置信息的收集会大大减少，因此定位精度会大大折扣。对于H-REAP部署方式试图达到的最大可能的精度，思科声明的定位精度在这种环境中无法得到支持。

注：H-REAP并不是旨在提供定位服务。因此，思科不能保证在H-REAP模式下的定位精度。

本地交换WLAN通常支持2层漫游。为了提供这种漫游，确保分配给本地交换WLAN相同的VLAN在所有需要进行漫游服务的H-REAP之间是必须的。这意味着，客户在漫游后并不需要重新通过DHCP获取客户端地址。这有助于在漫游过程中减少延时。

发生在H-REAP上的本地交换WLAN之间的漫游可能需要50毫秒和1500毫秒，这取决于广域网时延， RF设计和环境特点，以及安全类型和客户的具体漫游实现。

WLC版本4.2.61.0及更高版本支持使用思科集中密钥管理（ CCKM ）的快速安全的无线漫游。 H-REAP支持使用CCKM的2层快速安全无线漫游。这一特性可以保护需要完全的RADIUS EAP身份验证的客户端从一个AP漫游到另一个。为了在H-REAP上使用支持CCKM的快速漫游，你需要配置H-REAP组。

H-REAP组 — 为了更好地组织和管理您的H-REAP，您可以创建H-REAP组，并为之指定具体的AP。所有组内的H-REAP共享相同的CCKM，WLAN，以及备份RADIUS服务器的配置信息。如果您有多个H-REAP部署在偏远的办公室或在不通的楼层上，当您要一次性配置所有这些H-REAP时，这一特性非常有帮助。例如，您可以为一个H-REAP组配置一个备份RADIUS服务器，而不是为每一个AP配置同一台服务器。每台控制器，可以配置多达20个H-REAP组，每个组内可以包含最多25个AP。

控制器软件版本5.0.148.0包含两个新的H-REAP组特性：

- 备份RADIUS服务器 — 您可以对控制器进行配置，允许工作在独立模式下的H-REAP进行充分的802.1X认证。你可以设置一个主RADIUS服务器或一主一备RADIUS服务器。
- 本地认证 — 您可以对控制器进行配置，允许工作在独立模式下的H-REAP为最多20静态配置用户提供LEAP或EAP - FAST认证。当每个H-REAP计入控制器时，控制器向其发送用户名和密码的静态列。每个组内的AP只对与它自己的相关客户进行认证。此功能对于从一个胖AP网络迁移到LWAPP H-REAP网络，并不需要维持一个庞大的用户数据库，也没有添加其他硬件设备，以取代在原胖AP网络中可用的RADIUS服务器功能，这样的功能是非常理想的。

参阅Cisco Wireless LAN Controller Configuration Guide, Release 5.1的Configuring Hybrid-REAP Groups部分详细信息如何配置H-REAP组。

如同所有基于LWAPP的AP，H-REAP可能被部署在NAT设备或边界后面，而控制器可能不会。除了组播，每个功能和特点在这样的环境下都是支持的。单播配置的组播运行良好，只有组播设置控制器的组播功能无法正常工作。

H-REAP WAN 需求

因为H-REAP专为跨越WAN链路部署而设计，它已经针对这样的部署进行了优化。虽然H-REAP可以在在这些偏远的网络设计方案中灵活部署，但是仍然有一些指导方针，需要在设计具有H-REAP功能的网络架构时遵守。

- 一个H-REAP AP可以配置一个静态IP地址或通过DHCP获得地址。在DHCP获取地址的情况下，DHCP服务器必须是本地的，必须能够在AP启动时提供IP地址。
- H-REAP最多支持四个分割包或至少500字节（MTU）WAN链接。
- 在AP和控制器之间的往返时延不得超过100毫秒（ms），LWAPP控制数据包优先级

必须高于所有其他流量。

- 控制器可以通过单播或组播包的形式向AP发送组播包。在H-REAP部署模式下，AP仅可以接收单播形式的组播包。
- 为了在H-REAP上使用支持CCKM的快速漫游，您需要配置H-REAP组。
- H-REAP AP支持1-1的网络地址转换（NAT）配置。除了组播功能，对于其他所有的特性，H-REAP还支持端口地址翻译（PAT）。当跨越边界的NAT配置了单播选项时，组播仍然能够得到支持。H-REAP还支持多对一的NAT /PAT边界，除非你想在所有的集中交换的WLAN中实现真正组播操作。
- H-REAP AP支持多个SSID 。
- NAC OOB部署，仅在配置成集中交换的H-REAP的WLAN上支持。这是在配置层本地交换的H-REAP的WLAN上不支持。
- H-REAP的主备控制器必须具有相同的配置。否则的话，接入点会丢失其配置和某些功能，如无线覆盖，AP组VLAN，静态信道数量等，有可能无法正常运行。此外，一定要在两个控制器上重复H-REAP的SSID和指数。

注：在升级过程中，每个AP需要通过WAN链接更新4MB的代码。

为了确保这一延迟限制，强烈建议在接入点和控制器之间，对网络流量进行优先配置，以使LWAPP控制（UDP端口12223）流量的有线及最高。如果LWAPP控制流量没有处于优先地位，其他网络流量的峰值，导致WAN链路拥塞而不能传递AP和控制器之间的控制信息，将很可能导致H-REAP经常在连接模式和独立模式之间频繁转换。

频繁的H-REAP翻动会造成严重的连接问题。如果没有适当的流量优先级设置，在远端部署控制器可能是一种更加审慎的做法，以确保一致和稳定的无线接入。

注：无论H-REAP是否将客户端流量转发回到控制器， LWAPP数据路径会将所有802.11客户端探针和认证/关联请求，无线资源管理的邻居信息，和EAP和网络身份认证请求转发回控制器。因此，确保LWAPP数据（UDP端口12222）在任何位置的AP和控制器之间没有阻挡。

H-REAP 配置

有线网络准备

部署H-REAP网络的第一步是配置H-REAP所连接的交换机。这个交换机配置的例子包括一个本地VLAN配置（H-REAP用来和控制器进行LWAPP通信的网段）和两个子网，两个本地交换的WLAN数据将终结在这两个网段上。如果IP地址没有提供给AP和本地交换的WLAN的客户端，那么，DHCP服务，需要通过其他方式提供，或需要提供静态的地址。虽然DHCP是一种推荐的方式，一些人可能会选择为AP配置静态地址，而为无线用户提供DHCP服务。为简单起见，多余的交换机配置在这个例子已被删除。

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
```

```
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H-REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

注：在这个例子中IP地址和其后所有的配置完全是用于说明目的。因此，IP地址必须根据每个网络的需求进行规划。

在此配置中，H-REAP连接到第一FastEthernet接口，通过交换机上的native VLAN（VLAN10）经DHCP获得地址。不必要的VLAN是从与H-REAP互联的trunk中去除了，以此限制处理无关的数据包。VLAN 11和VLAN 12可向与之关联的两个WLAN的客户段提供DHCP服务。

注：H-REAP所连接的交换机需要上连至路由基础设施。H-REAP最佳部署经验标明，远端/WAN路由基础设施应该优先考虑转发LWAPP控制（UDP端口12223）数据。

H-REAP 使用命令行进行控制器发现

H-REAP通常使用DHCP选项43或DNS解析来进行控制器发现。如果这两种方式不可用，需要向远程站点管理员提供详细的信息，使每个H-REAP配置相应的控制器IP地址。另外，H-REAP本身的IP地址同样可以手动进行设置（如果不想使用DHCP或者条件不具备

的情况下）。

这个例子详细说明如何通过AP的Console口配置H-REAP的IP地址，主机名，控制器的IP地址。

AP_CLI#**lwapp ap hostname ap1130**
ap1130#**lwapp ap ip address 10.10.10.51 255.255.255.0**
ap1130#**lwapp ap ip default-gateway 10.10.10.1**
ap1130#**lwapp ap controller ip address 172.17.2.172**

注：AP必须运行启用LWAPP的Cisco IOS软件版本12.3(11)JX1或更高版本，以支持这些命令。以SKU前缀开头的LAP（例如，AIR-LAP-1131AG-A-K9），运行的是Cisco IOS软件版本12.3(11)JX1或更高版本。

这些配置命令只在独立模式下被AP所接受。

如果一个AP从来没有连接到过一个控制器，AP预设的命令行密码是Cisco。一旦AP连接到一个控制器，密码被更改后，才能通过Console进行命令行的配置。仅命令行有效的控制器命令语法如下：

(WLC_CLI)>**config ap username <user-id> password <passwd> {all | <AP name>}**

对于上面的AP，这个命令可能被这样用：

(WLC_CLI)>**config ap username admin password pass ap1130**

注：虽然此命令需要建立一个用户名，但供以后使用。

注：所有的显示和调试命令可以在默认密码更改前使用。

H-REAP 控制器配置

一旦在H-REAP已经发现并加入了控制器，所有H-REAP配置都是通过控制器的网页或命令行界面完成的（或者，配置可集中通过无线控制系统[ＷＣＳ]完成）。本节中H-REAP的配置，通过控制器的图形界面完成。

在此示例中WLAN配置如下（定制配置视需要而定）

WLAN SSID	Security	Switching
Corporate	WPA2 (802.1X)	Local
RemoteSite	WPA2 - PSK	Local

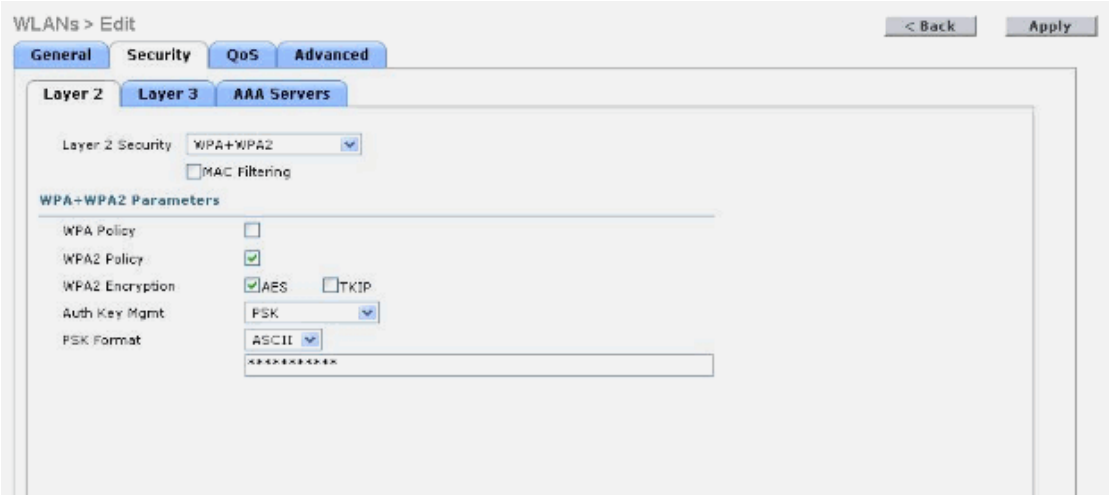
Guest	WebAuth	Central (Tunneled to DMZ Controller)

为了使一个H-REAP AP作为一个H-REAP工作，与之相连的控制必须至少有一个本地交换WLAN（如果不这样做，H-REAP的高可用性功能将无法实现） 。

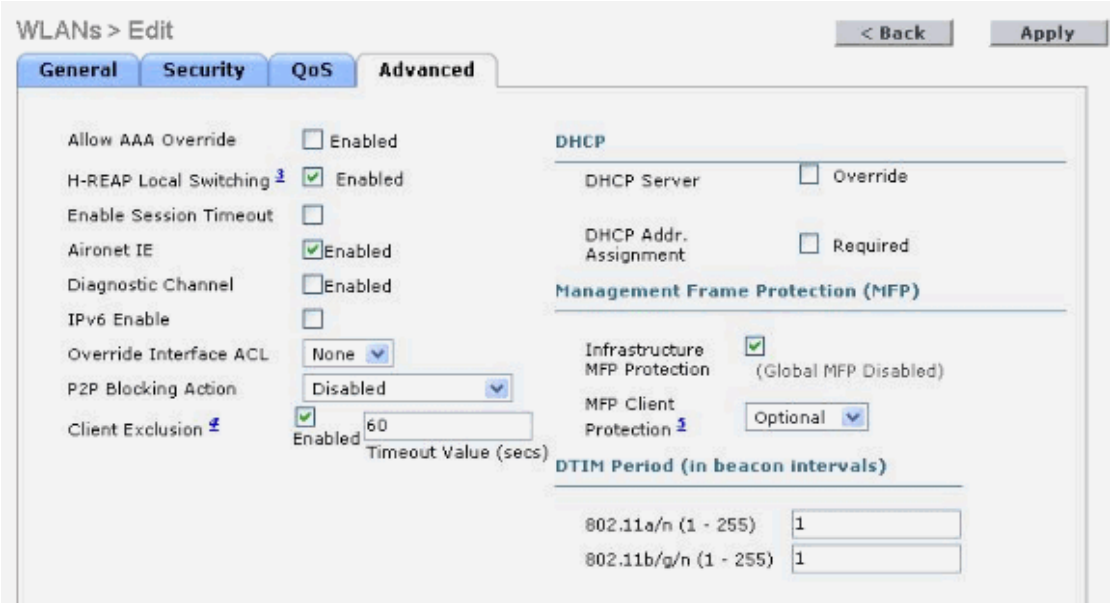
完成这些步骤，以便配置本地交换WLAN：

1.返回主网页的控制器，选择**WLAN**，然后单击**NEW**。
2.指定的WLAN的名称（这也将被用来作为SSID ） ，并单击**Apply**。

3.在WLAN>Edit页中，点击Security标签。在2层安全中选择安全类型。
在此示例中， WPA2-PSK是理想的。选择的**WPA + WPA2**。



4.勾选**WPA2 Policy**，以指定的WLAN的WPA功能。
5.勾选**AES**以确定加密方法。
6.在Auth Key Mgmt下，从下拉菜单中选择的**PSK**。
根据所需的key格式，选择取决于易用性和客户端的支持情况，可以选择ASCII或十六进制数。ASCII字符通常是比较容易，因为字母数字字符都可接受。选择ASCII码 ，并输入想要的预共享密钥。
7.单击高级选项卡。勾选**H-REAP Local Switching**确保WLAN启用。



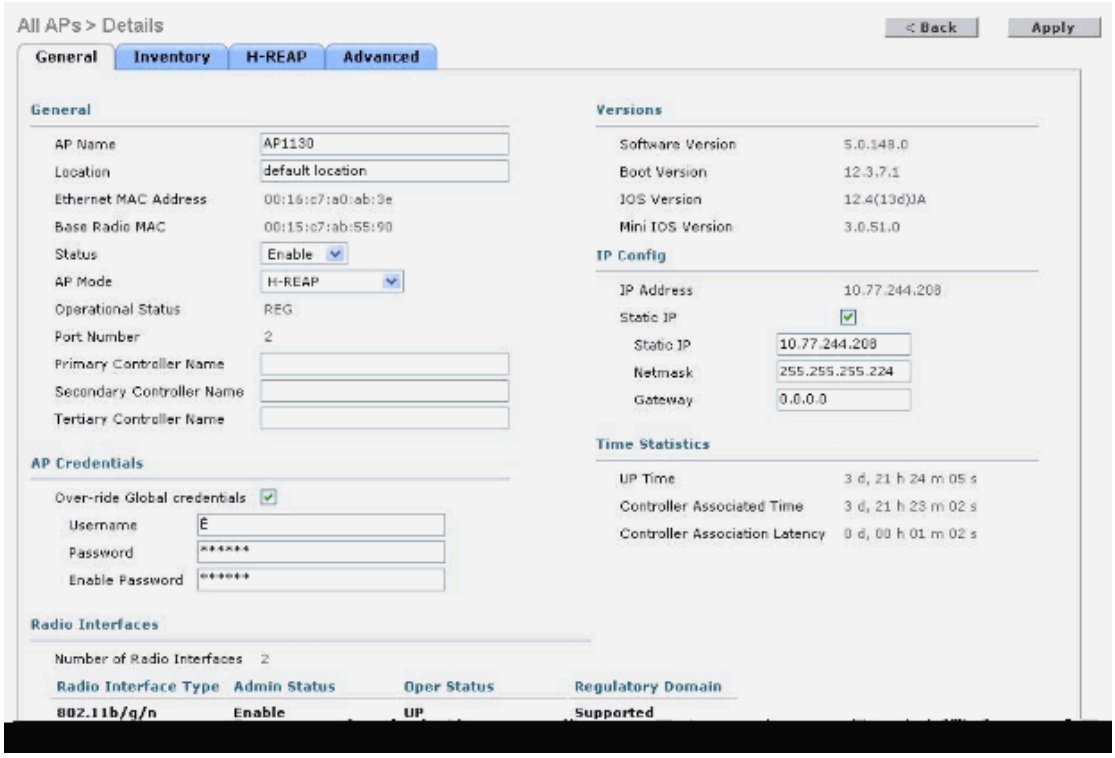
如果没有这一步，WLAN不允许数据终结在H-REAP。

注：AP如果没有配置为运行在H-REAP模式的话，将会忽略H-REAP本地交换设置，所有客户端数据将会转发回到控制器。

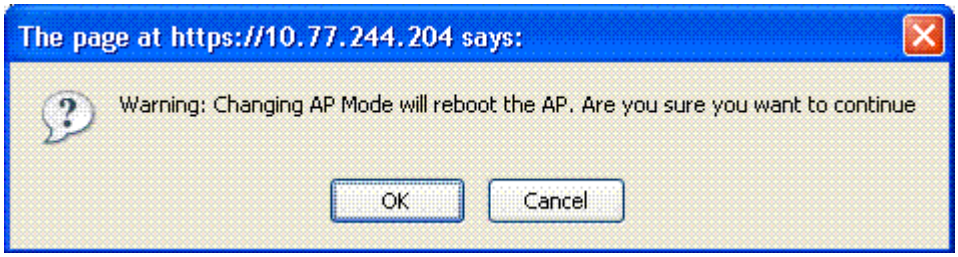
当H-REAP WLAN设置完成后，接入点就可以配置为工作在H-REAP模式下。

8. AP发现加入控制器后，到控制器的网络界面下的Wireless标题下，然后按一下旁边的**Detail**，进入AP的选择。

9.在AP Mode标题下，从下拉菜单中选择**H-REAP**，改变接入点的默认本地模式操作功能为H-REAP模式。



10.单击**Apply**。AP需要重新启动才能使模式配置生效。



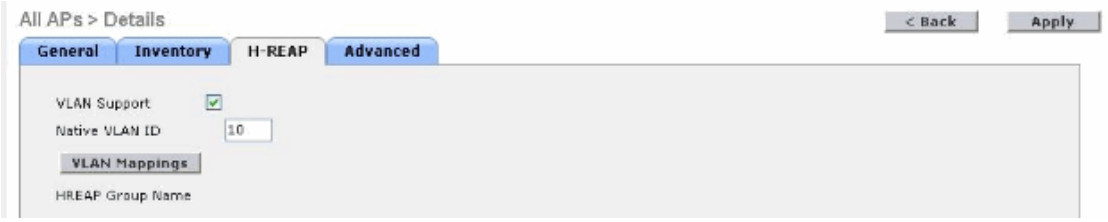
AP重新启动，重新发现控制器，并再次加入控制器。

11.返回**Wireless**标题，并选择相同的AP **Detail**链接。

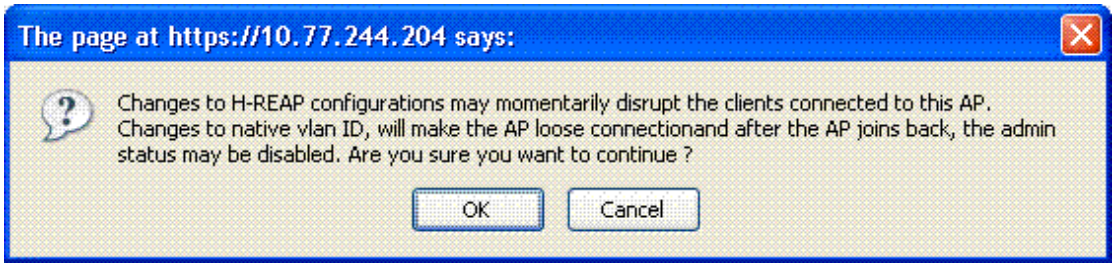
默认情况下，在H-REAP没有运行在Trunk上。虽然交换机端口可以设置为trunk模式，AP仍与控制器通过native VLAN进行通信。如果交换机端口处于trunk模式，需要H-REAP同样运行在该模式下，那么VLAN的支持必须启用。

12.单击的H-REAP标签。勾选**VLAN Support**。

13.基于H-REAP所连接的交换机端口的配置，输入AP的native VLAN ID号码（在这个例子中，VLAN 10）。



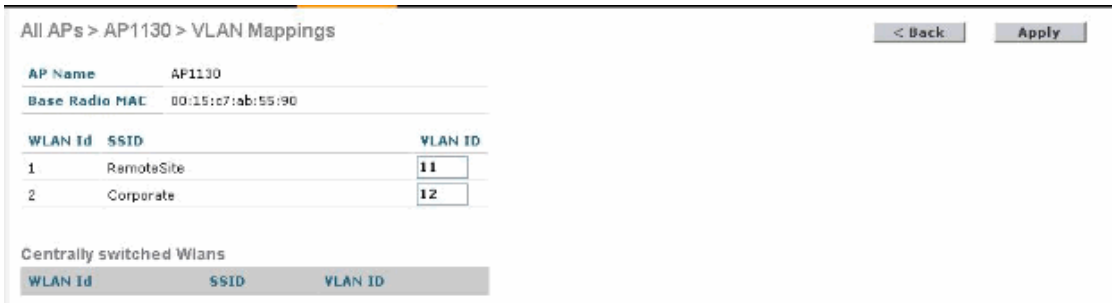
14.单击**Apply**，以便制定的变化。



因为在H-REAP重置以太网端口的配置，AP可能短时间内失去与控制器之间的连接。弹出窗口警告说明了这种可能性。单击**OK**。

注：如弹出警告说明的，AP有可能将重新加入控制器在停用状态。重新进入Wireless标题下的**Detail**链接。然后选择**Enable**旁边的管理状态。应用设置，并继续配置。

15.进入所需配置AP的详细配置页，选择H-REAP标签，然后按一下**VLAN Mapping** ，以配置802.1Q标记为本地交换WLAN。

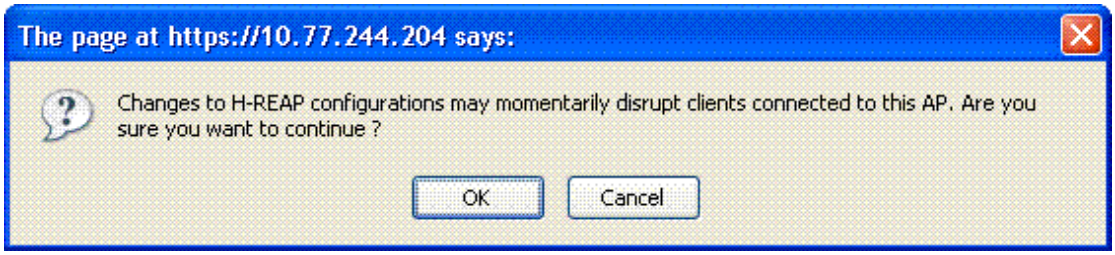


16.按照每个WLAN设置本地的VLAN用户客户端数据的终结。

注：WLAN未配置为支持H-REAP本地交换前，不允许在这里对802.1Q标记进行配置。

注：本地交换WLAN都可以共享相同的VLAN ID或者也可以各不相同。只要相应的VLAN出现在H-REAP所连接的交换机端口上，其他并无限制。

17.单击**Apply**，应用以保存更改。



当VLAN/WLAN的映射发生变化时，WLAN服务会暂时中断。单击**OK**以确认这一点。

必要的WLAN已经创建并配置，AP设置为操作在H-REAP模式，启用了VLAN的支持，并为本地的VLAN配置对应的WLAN。.如果对于每个VLAN，DHCP可用，客户能够连接到每一个无线局域网，得到各自所属VLAN的地址，并能通过流量。H-REAP的配置现已完成。

H-REAP 排障

有几个常见的场景和情况导致无法进行H-REAP配置和客户端连接。本节提供了一些这种情况及其建议的补救措施。

H-REAP 无法加入控制器

这可能有几个原因。首先检查以下内容：

- **每个H-REAP，必须有恰当的IP地址。**
  如果使用的是DHCP，通过控制台的接入点，确认接入点获得IP地址。
  AP_CLI# **show dhcp lease**
  如果使用的是静态地址，通过控制台的接入点，检查以确保正确的IP地址配置。
  AP_CLI# **show lwapp ip config**
  纠正错误配置。

- **确保AP的IP连接，可以ping通控制器管理地址。**
  一旦IP地址确认了，检查，以确保AP能够与控制器管理IP地址进行通信。使用ping命令，使用如下语法：
  AP_CLI# **ping <WLC management IP address>**
  如果没有成功，确保上游网络配置正确，并且能够通过广域网访问回到公司网络。验证控制器正常工作，而不是在任何NAT /PAT比设备后。确保UDP端口12222和12223在路径上的防火墙都被开放。从控制器ping至AP。

- **确认AP和控制器之间的LWAPP连接。**
  一旦H-REAP和控制器之间IP连接已经确认，在控制器上执行LWAPP调试，以确认LWAPP信息通过广域网进行了通信，并确定相关的问题。在控制器上，首先建立一个MAC过滤器来限制调试的输出。使用此命令，以限制输出的命令限定到一个接

入点。

AP_CLI# **debug mac addr <AP's wired MAC address>**

一旦设置限制调试输出，打开LWAPP调试。

AP_CLI# **debug lwapp events enable**

如果没有LWAPP调试信息输出，确保了H-REAP至少有一个方法可以发现控制器。如果这种方法已经使用（如DHCP选项43或DNS），确认它们的配置正确。如果没有其他发现方法在使用，确保控制器的IP地址已经通过Console命令行输入到AP中。

AP_CLI# **lwapp ap controller ip address <WLC management IP address>**

- **在控制器和H-REAP上检查LWAPP操作。**

  如果至少有一个控制器发现方法可以使用，核实LWAPP信息由AP发往控制器。此命令已默认启用。

  AP_CLI# **debug lwapp client errors**

  进一步了解哪个控制器和AP之间的通信，可以从UDP数据信息发送的IP地址看出。查看每个数据包的源地址和目的地址可以查看AP的IP栈。

  AP_CLI# **debug ip udp AP_CLI**

  如果从Conaol看出，AP正与控制器通信，有可能是它已加入集群中的另一个控制器。为了验证H-REAP是否连接到控制器上，使用此命令。

  AP_CLI# **show lwapp reap**

- **确认AP已经加入了正确的控制器。**

  如果在发现阶段，其他控制器的IP地址交给AP，那么H-REAP可能加入另一个控制器。验证发现机制提供的控制器的IP地址是正确的。查明该AP所加入的控制器的IP地址。

  AP_CLI# **show lwapp reap status**

  登录控制器的Web图形用户界面。.确保所有控制器的IP和MAC地址已经输入到移动控制器名单，他们都有着同样的移动组名称。然后，设置AP的主要，次要以及第三控制器，支配该控制器AP的连接。这项配置可以通过AP的Detail链接配置完成。如果问题在于H-REAP加入了另一个控制器，使用的WCS的管理能力可以大大减少该问题。

- **解决证书问题，如果接入点正试图加入控制器，但却失败了。**

  如果可以在控制器上看到LWAPP信息，但是AP却未能加入，这可能是一个证书的问题。欲了解更多LWAPP解决疑难问题的窍门，包括故障排除证书问题，请参阅LWAPP Upgrade Tool Troubleshoot Tips。

H-REAP Console 口无法配置并返回错误信息

任何配置命令（或者配置或清除配置）通过-REAP的CLI执行是返回ERROR！命令被禁用的信息。这种情况可能有两种原因：

- 在连接模式下的H-REAP不允许通过Console进行配置或清除任何配置。当AP处于这

个工作状态，配置必须通过控制器接口进行。如果需要通过命令行对AP进行配置时，确保接入点工作在独立模式，然后尝试重新输入任何配置命令。

- 一旦接入点已连接到一个控制器（即使H-REAP已经恢复独立模式），在设置一个新的密码之前，AP的Console将不允许配置命令。每个H-REAP的密码都需要更改。这只能通过该AP所连接的控制器的命令行进行配置。此命令的语法可以用在控制器上对单个AP的Console密码或所有AP的Console密码进行配置：

  (WLC_CLI)> **config ap username <user-id> password <passwd> {all | <AP name>}**

  注：对于一个AP还没有确定其控制台的密码，注意，此配置将只发送给AP，虽然是在控制器上输入的命令。任何后来加入的AP，将需要再次输入命令。

  已经被赋予了一个非默认密码，同时AP处于独立模式，将AP仍然不允许访问这些命令。为了能够更改H-REAP的配置，取消原已存在的静态IP地址和控制器的IP地址配置是必要的。这种配置被称为LWAPP私有配置，任何新的AP的CLI命令可以输入前需要将之删除。为了做到这一点，输入下面的命令：

  AP_CLI# **clear lwapp private-config**

  注：当加入到控制器的时候，AP也可以恢复出厂默认配置。点击Wireless标题下的AP的Derail链接，选择清楚配置按钮。AP的配置将被抹去，并重新启动。

  注：所有的显示和调试命令，都将可以正常使用，AP无需设置非默认密码，AP也无需处于连接模式。

  只有这样，任何LWAPP配置才有可能完成。

客户端无法连接到 H-REAP

完成这些步骤：

1.确认接入点加入了适当的控制器，该控制器至少有一个正确配置（和启用）的WLAN，并确保了H-REAP模式是在启用状态。

2.在客户端侧，确认WLAN的SSID可用（在控制器上，配置无线广播SSID，可以帮助排障过程）。检查在客户端上的WLAN的安全配置。客户端的安全配置是大多数连接故障的问题所在。

3.确保客户在本地交换的WLAN拿到了合适的地址。如果使用的是DHCP，请确保DHCP服务器设定是否正确。如果使用静态地址配置，确保客户端配置正确的IP地址。

4.为了进一步解决客户端连接问题，在H-REAP的Console口，输入此命令。

AP_CLI# **show lwapp reap association**

5.为了进一步解决客户端连接问题，和限制在控制器上进一步调试的输出，使用此命令。

AP_CLI# **debug mac addr <client’s MAC address>**

6.为了调试客户的802.11连接问题，使用此命令。

AP_CLI# **debug dot11 state enable**

7.用此命令调试客户的802.1X认证过程和失败。

AP_CLI# debug dot1x events enable

8.后端控制器/Radius信息可使用此命令进行调试。

AP_CLI# **debug aaa events enable**

9.另外，使用一套完整的客户端调试命令，使用此命令。

AP_CLI# **debug client <client’s MAC address>**

H-REAP 是否可以工作在 NAT 下?在配置静态 NAT 的环境中，WLC 和 H-REAP 时候可以放置在静态 NAT 后？

是的，对于AP可以。确保AP的源端口没有被NAT设备改变。通常对于静态NAT，这不是一个问题。但是，将这些情况考虑在内：

- 在控制器和AP之间，有两个主要的被NAT了的UDP连接： LWAPP数据连接和LWAPP控制连接。
- 源端口在AP侧是一个临时的动态端口（>1024）。在控制器侧，它是一个固定的目的端口（12222，12223）。
- UDP连接的翻译是基于超时。这意味着，目前的连接创造一定时间后如果不适用就会被删除，它是基于超时（可能是较短或较长，这取决是您的NAT设备）。
- LWAPP控制是积极的。一般情况下，您可以知道每30秒它会发送一个数据包（回声保持）。因此，LWAPP控制连接的Nat翻译，你可以假设，它会不断刷新的NAT超时。
- LWAPP数据只会当存在活动时才会有流量。对于没有任何客户端的接入点，LWAPP数据的NAT翻译会超时（例如，超过90秒没有活动），如果AP出现了新的流量，会重新建立NAT连接。如果新的NAT条目使用的是相同的源端口号，那么你将不会碰到任何问题。但是，如果UDP源端口改变了，那么WLC将丢弃该数据包，因为现在的LWAPP隧道信息数据不再和AP加入控制器时创建的一致。
- 因此，只要您的NAT设备保持UDP连接的源端口，那么它将能够工作。否则的话，数据流会被丢弃，虽然AP能够加入控制器，但无线客户端的数据流无法正常通过。

参阅Hybrid Remote Edge Access Point (H-REAP) Basic Troubleshooting获取更多H-REAP的排障信息。

H-REAP Q&A

问：如果我配置LAPs在地理位置偏远的地方如H-REAP，我可以给那些LAP配置主备控制器吗？

例如：有一个主要控制器在A点和一个次要控制器B点

如果在A点的控制器失效，LAP切换加入到B点的控制器上。如果两个控制器都失效，LAP是否会进入H-REAP本地模式？

.答：是的。首先，LAP切换至其备份控制器。无线局域网的所有本地交换的数据没有变化，集中交换的数据将被转发至新的控制器。如果备份控制器失效，WLAN将切换至本地交换（开放/预共享密钥认证/你正在做的AP认证）仍然保持连接。

问：配置为本地模式的AP如何处理配置为H-REAP本地交换模式的WLAN？

答：本地模式AP如常对待这些接入点的WLAN。身份验证和数据流量都将转发回到WLC 。在WAN链接失效的情况下，这些WLAN将完全失效。

相关信息

- **Cisco Wireless LAN Controller Configuration Guide, Release 4.0**
- **Wireless LAN Controller (WLC) Software Upgrade**
- **Wireless LAN Controller (WLC) Troubleshoot FAQ**
- **WLAN Technology Support**
- **H-REAP Modes of Operation Configuration Example**
- **Hybrid Remote Edge Access Point (H-REAP) Basic Troubleshooting**
- **Wireless LAN Controller Configuration Examples and TechNotes**
- **Wireless LAN Controller (WLC) Error and System Messages FAQ**
- **Wireless Control System (WCS) Error and System Messages**
- **Technical Support & Documentation - Cisco Systems**

更新时间: 2008-8-21 文档编号: 71250
