



无线局域网控制器 (WLC) 设计和功能常见问题

问题

- 前言
- 设计常见问题解答
- 功能常见问题解答
- 相关信息

前言

本文提供无线局域网控制器 (WLC) 的设计与功能的常见问题解答。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

设计常见问题解答

Q. 如何配置交换机以连接 WLC?

A. 将连接 WLC 的交换机端口配置为 IEEE 802.1Q 中继端口。确保交换机只允许使用必要的 VLAN。通常，WLC 的管理接口和 AP-Manager 接口都处于未标记状态。这意味着它们假定使用所连接交换机的本地 VLAN。并非必需。您可以为这些接口分配单独的 VLAN。有关详细信息，请参阅无线 LAN 控制器和轻量接入点基本配置示例中的为 WLC 配置交换机部分。

Q. 当接入点 (AP) 在控制器中注册后，与 WLAN 客户端之间的所有网络往来流量是否都要通过无线 LAN 控制器 (WLC) 进行隧道传输?

A. 当 AP 加入 WLC 后，两个设备之间将形成一个无线接入点控制和设置协议 (CAPWAP) 隧道。所有流量（包括所有客户端流量）都将通过该 CAPWAP 隧道发送。

唯一的例外是当 AP 处于混合 REAP 模式时。当与控制器的连接丢失时，混合 REAP 接入点可以在本地交换客户端数据流量，并在本地进行客户端认证。当连接到控制器后，它们也能将流量发送回控制器。

Q. 我能否在远程办公室安装轻量接入点 (LAP) 并在总部安装 Cisco 无线局域网控制器 (WLC)? LWAPP/CAPWAP 能否通过广域网工作?

A. 可以，您可以通过 WAN 连接 AP 与 WLC。当 LAP 配置为远程边缘接入点 (REAP) 或混合远程边缘接入点 (H-REAP) 模式时，LWAPP/CAPWAP 可以通过广域网工作。这两种模式都允许由通过 WAN 链路连接的远程控制器来控制 AP。流量将桥接到本地 LAN 链路上，从而避免了不必要地通过 WAN 链路发送本地流量。这实际上是在无线网络中使用 WLC 的几大优点之一。

注意：并非所有轻量 AP 都支持这些模式。例如，只有 1131、1140、1242、1250 和 AP801 LAP 支持 H-REAP。只有 1030 AP 支持 REAP，1010 和 1020 AP 不支持 REAP。在计划实现这些模式之前，请检查以确定 LAP 是否支持它。已转换为 LWAPP 的 Cisco IOS® 软件 AP (自治 AP) 不支持 REAP。

Q. REAP 和 H-REAP 模式如何工作?

A. 在 REAP 模式下，所有控制和管理流量（包括认证流量）都通过隧道返回 WLC，而所有数据流量则在远程办公室 LAN 内进行本地交换。当失去与 WLC 的连接时，除了第一个 WLAN (WLAN1) 以外的所有 WLAN 都将终止。当前与此 WLAN 相关联的所有客户端将予以保留。要在失去连接期间允许新客户端在此 WLAN 上成功进行认证并得到服务，请将此 WLAN 的认证方法配置为 WEP 或 WPA-PSK，以便能够在 REAP 中进行本地认证。有关 REAP 部署的详细信息，请参阅分支机构的 REAP 部署指南。

在 H-REAP 模式中，接入点通过隧道将控制和管理流量（包括认证流量）返回 WLC。如果 WLAN 配置了 H-REAP 本地交换，则来自 WLAN 的数据流量将在远程办公室进行本地桥接，否则数据流量将发送回 WLC。当失去与 WLC 的连接时，除了配置了 H-REAP 本地交换的前八个 WLAN 以外的所有 WLAN 都将终止。当前与这些 WLAN 相关联的所有客户端将予以保留。要在失去连接期间允许新客户端在这些 WLAN 上成功进行认证并得到服务，请将此 WLAN 的认证方法配置为 WEP、WPA PSK 或 WPA2 PSK，以便能够在 H-REAP 中进行本地认证。

有关 H-REAP 的详细信息，请参阅 H-REAP 设计与部署指南。

Q. 远端边界接入点 (REAP) 与混合 REAP (H-REAP) 有何区别？

A. REAP 不支持 IEEE 802.1Q VLAN 标记。因此，它不支持多个 VLAN。来自所有 Service Set Identifier (SSID) 的流量将在相同的子网上终止，但 H-REAP 支持 IEEE 802.1Q VLAN 标记。来自每个 SSID 的流量可以划分给一个唯一 VLAN。

当失去与 WLC 的连接时，即在独立模式下，REAP 只为一个 WLAN 提供服务，也就是第一个 WLAN。所有其他 WLAN 将处于非激活状态。在 H-REAP 中，在失去连接期间最多可支持 8 个 WLAN。

另一个主要区别是，在 REAP 模式中，数据流量只能进行本地桥接，而不能交换回中心办公室，但在 H-REAP 模式中，您可以选择将流量交换回中心办公室。来自配置了 H-REAP 本地交换的 WLAN 的流量将进行本地交换。来自其他 WLAN 的数据流量将交换回中心办公室。

有关 REAP 的详细信息，请参阅《带轻量 AP 和无线局域网控制器 (WLC) 的远端边界接入点 (REAP) 配置示例》。

有关 H-REAP 的详细信息，请参阅“配置混合 REAP”。

Q. WLC 上支持多少 WLAN？

A. 现在从软件版本 5.2.157.0 开始，WLC 可以为轻量接入点控制多达 512 个 WLAN。每个 WLAN 都有一个单独的 WLAN ID (1 到 512)、一个单独的配置文件名和一个 WLAN SSID，并且可以为其分配唯一的安全策略。控制器可向每个连接的接入点发布最多 16 个 WLAN，但您可以在控制器上创建多达 512 个 WLAN，然后有选择地将这些 WLAN (使用接入点组) 发布到不同的接入点以更好地管理您的无线网络。

注意：Cisco 2106、2112 和 2125 控制器最多只能支持 16 个 WLAN。

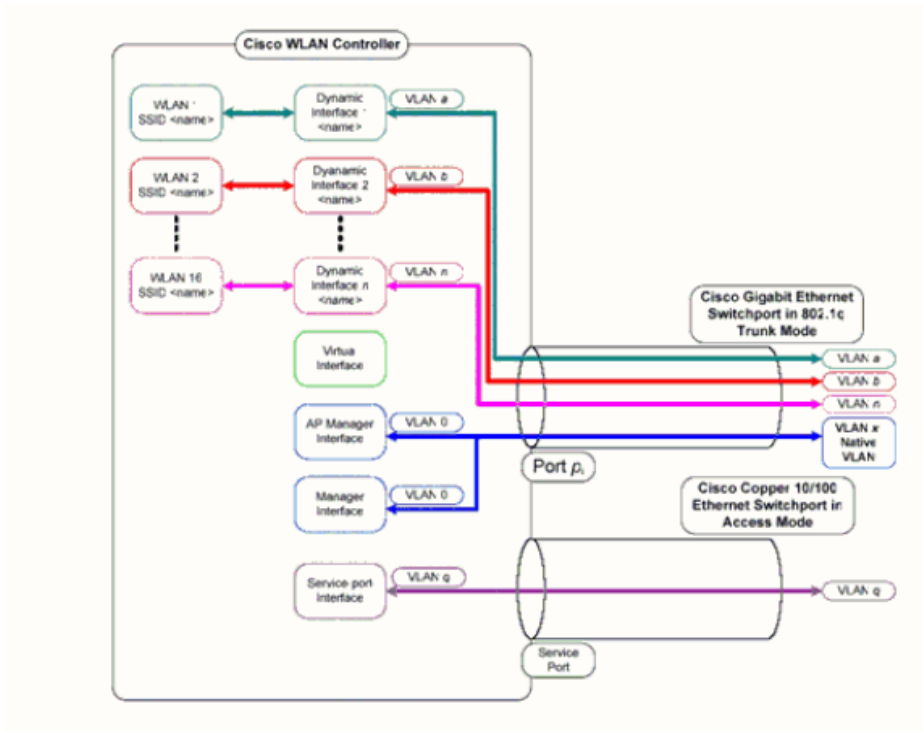
注意：关于配置的 WLAN 指南的详细信息在 WLCs，请阅读 Cisco 无线 LAN 控制器配置指南的创建的王LAN 部分，版本 7.0.116.0。

Q. 我如何在我的无线局域网控制器 (WLC) 上配置 VLAN？

A. 在 WLC 中，VLAN 绑定到在一个唯一 IP 子网中配置的接口。该接口映射到 WLAN。然后，与此 WLAN 相关联的客户端将属于该接口的 VLAN，并从该接口所属的子网中为其分配一个 IP 地址。要在 WLC 上配置 VLAN，请完成无线局域网控制器上的 VLAN 配置示例中的过程。

Q. 我们提供了两个具有两种不同动态接口的 WLAN。每个接口都有其自己的 VLAN，且不同于管理接口 VLAN。这似乎可行，但我们尚未提供中继端口以允许使用我们的 WLAN 使用的 VLAN。接入点 (AP) 是否会为数据包添加管理接口 VLAN 标记？

A. AP 不会为数据包添加管理接口 VLAN 标记。AP 将来自客户端的数据包封装在轻量接入点协议 (LWAPP)/CAPWAP 中，然后将其传递给 WLC。WLC 随后剥离 LWAPP/CAPWAP 报头并使用适当的 VLAN 标记将数据包转发给网关。VLAN 标记取决于客户端所属的 WLAN。WLC 依靠网关将数据包路由到其目的地。要能够为多个 VLAN 传递流量，您必须将上行链路交换机配置为中继端口。下图解释了 VLAN 是如何与控制器工作的：



Q. WLC 的哪个 IP 地址用于 AAA 服务器的认证？

A. WLC 为涉及 AAA 服务器的任何认证机制（第 2 层或第 3 层）使用管理接口的 IP 地址。关于端口和接口的更多信息在 WLC，参考配置的端口并且建立接口 Cisco 无线 LAN 控制器配置指南的部分，发布 7.0.116.0。

Q. 我在同一 VLAN 中有 10 个 Cisco 1000 系列轻量接入点 (LAP) 和 2 个无线局域网控制器 (WLC)。如何能够注册 6 个 LAP 以关联到 WLC1，而其余 4 个关联到 WLC2？

A. LWAPP/CAPWAP 允许动态冗余和负载均衡。例如，如果您为选项 43 指定多个 IP 地址，LAP 会向 AP 接收的每个 IP 地址发送 LWAPP/CAPWAP 发现请求。在 WLC 的 LWAPP/CAPWAP 发现响应中，WLC 会嵌入以下信息：

- 有关当前 LAP 负载（定义为当时加入 WLC 的 LAP 的数量）的信息
- LAP 容量
- 连接到 WLC 的无线客户端的数量

LAP 随后尝试加入负载最小的 WLC，即可用 LAP 容量最大的 WLC。此外，在 LAP 加入 WLC 后，LAP 从其加入的 WLC 学习移动组中另一个 WLC 的 IP 地址。

一旦 LAP 加入 WLC，您便可以在其下次重新启动期间让该 LAP 加入某个特定 WLC。为此，需要为 LAP 分配主要、次要和第三 WLC。当 LAP 重新启动时，它将寻找主要 WLC 并加入该 WLC，而不管该 WLC 上的负载如何。如果主要 WLC 未响应，它将寻找次要 WLC，如果仍无响应，则寻找第三 WLC。有关如何为 LAP 配置主 WLC 的详细信息，请参阅轻量接入点的 WLAN 控制器故障转移配置示例中的为轻量 AP 分配主要、次要和第三控制器部分。

Q. 2100 系列无线局域网控制器 (WLC) 不支持哪些功能？

A. 2100 系列控制器不支持以下硬件功能：

- 服务端口（单独的带外管理 10/100 Mb/s 以太网接口）

2100 系列控制器不支持以下软件功能：

- VPN 终端（如 IPSec 和 L2TP）
- 访客控制器隧道的终止（支持访客控制器隧道的起源）
- 外部 Web 身份验证 Web 服务器列表
- 第 2 层 LWAPP
- 生成树
- 端口镜像
- Cranite
- 堡垒
- AppleTalk
- QoS 每用户带宽合同
- IPv6 穿透
- 链路聚合 (LAG)
- 组播单播模式

- 有线访客接入

Q. 5500 系列控制器不支持哪些功能？

A. 5500 系列控制器不支持以下软件功能：

- 静态 AP 管理器接口

注意：5500 系列控制器不要求您配置 AP 管理器接口。默认情况下，管理接口将充当 AP 管理器接口，接入点可通过此接口加入。

- 非对称移动隧道
- 生成树协议 (STP)
- 端口镜像
- 第 2 层访问控制列表 (ACL) 支持
- VPN 终端 (如 IPSec 和 L2TP)
- VPN 穿透选项
- 802.3 桥接、AppleTalk 和 Point-to-Point Protocol over 以太网 (PPPoE) 的配置

Q. 网状网络不支持哪些功能？

A. 网状网络中不支持以下这些控制器功能：

- 多国家/地区支持
- 基于负载的 CAC (网状网络仅支持基于带宽的 CAC, 即静态 CAC。)
- 高可用性 (快速检测信号和主发现加入计时器)
- EAPFASTv1 和 802.1X 身份验证
- 接入点加入优先级 (Mesh 接入点有一个固定的优先级。)
- 本地签名证书
- 基于位置的服务

Q. 无线局域网控制器上的制造商安装证书的有效期是多长时间？

A. WLC 上的制造商安装证书的有效性为 10 年。

Q. 我在相同的移动组中为故障切换配置了两个无线局域网控制器 (WLC)，分别名为 WLC1 和 WLC2。我的轻量接入点 (LAP) 当前注册在 WLC1 中。如果 WLC1 发生故障，注册到 WLC1 的 AP 在切换到备用 WLC (WLC2) 期间是否要重新启动？此外，在此故障切换期间，WLAN 客户端是否会丢失与 LAP 的 WLAN 连接？

A. 是，如果 WLC1 发生故障，LAP 将取消在 WLC1 中的注册，然后重新启动，并重新注册到 WLC2。由于 LAP 要重新启动，因此关联的 WLAN 客户端将丢失与重新启动的 LAP 的连接。有关信息，请参阅统一无线网络中的 AP 负载均衡与 AP 后退。

Q. 漫游是否取决于无线局域网控制器 (WLC) 所配置使用的轻量接入点协议 (LWAPP)？在第 2 层 LWAPP 模式下运行的 WLC 能否执行第 3 层漫游？

A. 只要控制器上的移动分组配置正确，客户端漫游就应该能够正常工作。漫游不受 LWAPP 模式 (第 2 层或第 3 层) 影响。但是，建议尽可能使用第 3 层 LWAPP。

注意：Cisco 仅支持 Layer2 模式 410x 和 440x 系列 WLCs 和 Cisco 1000 系列接入点。其他无线局域网控制器和轻量接入点平台不支持 Layer2 LWAPP。

Q. 当客户端决定漫游到一个新接入点 (AP) 或控制器时，漫游过程是怎样的？

A. 以下是当客户端漫游到新 AP 时所发生的事件序列：

1. 客户端通过 LAP 向 WLC 发送重新关联请求。
2. WLC 将移动消息发送给移动组中的其他 WLC 以找出客户端之前所关联的 WLC。
3. 原始 WLC 将做出响应并通过移动消息提供有关客户端的信息，如 MAC 地址、IP 地址、QoS、安全上下文等。
4. WLC 用所提供的客户端详细信息更新其数据库；然后，必要时客户端将重新进行认证过程。客户端当前关联的新 LAP 也要连同其他详细信息一起在 WLC 的数据库中进行更新。这样，客户端 IP 地址将在 WLC 之间的漫游过程中予以保留，从而有助于提供无缝漫游。

关于漫游在一个统一的环境的更多信息，参考 Cisco 无线 LAN 控制器配置指南的配置的移动组部分，版本 7.0.116.0。

注意：在重新关联过程中，无线客户端不会发出 (802.11) 认证请求。无线客户端只会直接发出重新关联请求。然后，它将完成 802.1x 认证。

Q. 当网络中有防火墙时，需要为 LWAPP/CAPWAP 通信启用哪些端口？

A. 您必须启用以下端口：

- 为 LWAPP 流量启用如下 UDP 端口：
 - 数据 - 12222
 - 控制 - 12223
- 为 CAPWAP 流量启用以下 UDP 端口：
 - 数据 - 5247
 - 控制 - 5246
- 为移动性流量启用如下 UDP 端口：
 - 16666 - 安全模式
 - 16667 - 非安全模式

移动消息和数据消息通常通过 EtherIP 数据包进行交换。防火墙必须启用 IP 协议 97 以允许 EtherIP 数据包通过。如果使用 ESP 封装移动数据包，您在打开 UDP 端口 500 时必须允许 ISAKMP 通过防火墙。您还必须启用 IP 协议 50 以允许加密数据通过防火墙。

以下端口为可选端口（可根据自己的需要决定是否启用）：

- 用于 SNMP 的 TCP 161 和 162（适用于 Wireless Control System [WCS]）
- UDP 69，用于 TFTP
- TCP 80 和/或 443，用于通过 HTTP 或 HTTPS 的 GUI 访问
- TCP 23 和/或 22，用于通过 Telnet 或安全壳 (SSH) 的 CLI 访问

Q. 无线局域网控制器是否同时支持 SSHv1 和 SSHv2？

A. 无线 LAN 控制器仅支持 SSHv2。

Q. 无线局域网控制器 (WLC) 是否支持反向 ARP (RARP)？

A. Reverse Address Resolution Protocol (RARP) 是用于获取给定链路层地址（如以太网地址）的 IP 地址的链路层协议。具有固件版本 4.0.217.0 或更高固件版本的 WLC 支持 RARP。任何更早的版本都不支持 RARP。

Q. 我能否在无线局域网控制器 (WLC) 上使用内部 DHCP 服务器以便为轻量接入点 (LAP) 分配 IP 地址？

A. 控制器包含一个内部 DHCP 服务器。该服务器通常用在尚没有 DHCP 服务器的分支机构中。要访问 DHCP 服务，请在 WLC GUI 中单击 Controller 菜单；然后单击页面左侧的选项 Internal DHCP Server。关于如何配置在 WLC 的 DHCP 范围的更多信息，参考 Cisco 无线 LAN 控制器配置指南的配置的 DHCP 部分，版本 7.0.116.0。

内部服务器为管理接口上的无线客户端、LAP、设备模式 AP 提供 DHCP 地址，并提供从 LAP 中继来的 DHCP 请求。WLC 不会为有线网络中的上游设备提供地址。内部服务器不支持 DHCP 选项 43，因此 AP 必须使用另一种方法定位控制器的管理接口 IP 地址，如本地子网广播、DNS、Priming 或无线电发现。

注意：4.0 以前的 WLC 固件版本不支持 LAP 的 DHCP 服务，除非 LAP 直接连接到 WLC。那时内部 DHCP 服务器功能只用于为连接到无线 LAN 网络的客户端提供 IP 地址。

Q. WLAN 下的 DHCP Required 字段有何用处？

A. DHCP Required 是一个可为 WLAN 启用的选项。它要求与该特定 WLAN 相关联的所有客户端都通过 DHCP 获取 IP 地址。具有静态 IP 地址的客户端不允许关联到该 WLAN。此选项位于 WLAN 的 Advanced 选项卡下。仅当客户端的 IP 地址存在于 WLC 的 MSCB 表中时，WLC 才允许与客户端之间进行流量往来。WLC 会在其 DHCP Request 或 DHCP Renew 期间记录客户端的 IP 地址。这要求客户端每次重新关联到 WLC 时都要更新其 IP 地址，因为客户端每次因漫游或会话超时取消关联时，其条目都会从 MSCB 表中清除。客户端必须重新进行认证并重新关联到 WLC，从而将客户端条目重新添加到表中。

Q. Cisco 集中密钥管理 (CCKM) 在 LWAPP/CAPWAP 环境中如何工作？

A. 在初始客户端关联过程中，AP 或 WLC 在无线客户端通过 802.1x 认证后将协商确定一个成对主密钥 (PMK)。WLC 或 WDS AP 将为每个客户端缓存 PMK。当无线客户端重新关联或漫游时，它会跳过 802.1x 认证并立即验证 PMK。

WLC 在 CCKM 中的唯一特殊实现方式是 WLC 通过移动数据包（如 UDP 16666）交换客户端 PMK。

Q. 我如何对无线局域网控制器 (WLC) 和轻量接入点 (LAP) 设定双工设置？

A. Cisco 无线产品在速度和双工都进行自动协商时工作效果最佳，但您确实可以通过选项设定 WLC 和 LAP 的双工设

置。要设定 AP 速度/双工设置，您可以在控制器上为 LAP 配置双工设置，然后再将其应用于 LAP。

您可以使用 `configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name>` 命令通过 CLI 设定双工设置。只有 4.1 及更高版本支持此命令。

要为 WLC 物理接口设定双工设置，请使用 `config port physicalmode {all|port} {100h|100f|10h|10f}` 命令。

此命令将指定的或所有前面板 10/100BASE-T 以太网端口设置为 10 Mbps 或 100 Mbps 的专用半双工或全双工运行模式。注意，在为端口手动配置任何物理模式之前，您必须使用 `config port autoneg disable` 命令禁用自动协商。此外，还要注意 `config port autoneg` 命令会覆盖使用 `config port physicalmode` 命令所做的设置。默认情况下，所有端口均设置为自动协商。

注意： 光纤端口无法更改速度设置。

Q. 如果轻量接入点 (LAP) 没有注册到控制器，能否跟踪其名称？

A. 如果您的 AP 完全关闭且没有注册到控制器，则无法通过控制器跟踪 LAP。唯一的办法是您可以访问这些 AP 所连接的交换机，并使用以下命令找出它们连接的交换机端口：

```
show mac-address-table address <mac address>
```

这将为您提供此 AP 连接的交换机的端口号。然后，发出以下命令：

```
show cdp nei <type/num> detail
```

此命令的输出还会提供 LAP 名称。但是，这种方法仅在您的 AP 已通电且连接到交换机时才是可行的。

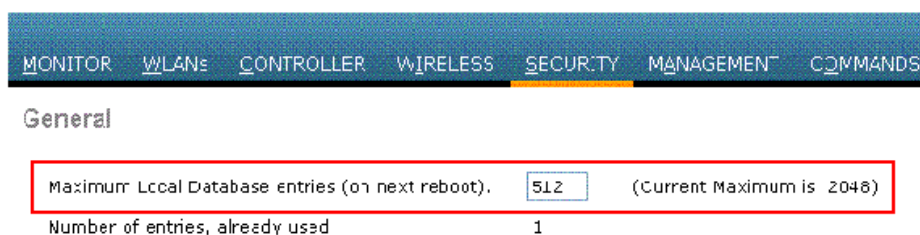
Q. 我在我的控制器上配置了 512 个用户。有没有任何方式增加用户数量无线局域网控制器的 (WLC) ？

A. 本地用户数据库对最多在安全>General 页的 2048 个条目被限制。此数据库由 (包括大厅大使) 的本地管理用户， (包括来宾用户) 的净用户， MAC 过滤器共享条目， 接入点 authorization list 条目和排除列表项。所有这些类型的用户总共不能超过已配置的数据库大小。

为了增加本地数据库，请使用从 CLI 的此命令：

```
<Cisco Controller>config database size ?  
<count> Enter the maximum number of entries (512-2048)
```

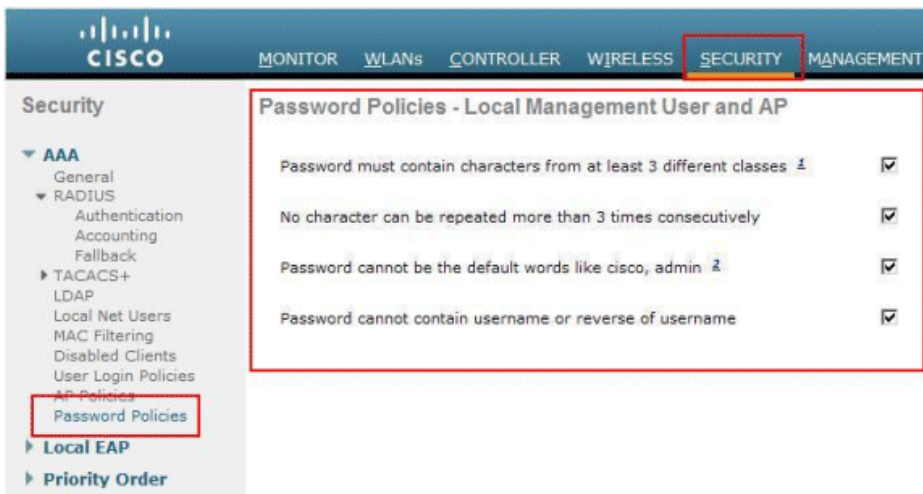
注意： 您必须保存配置和重置系统 (使用 `reset system` 命令) 为了更改能生效。



Q. 如何强制执行在 WLCs 的强口令策略？

A. WLCs 允许您定义强口令策略。使用 CLI 或 GUI，这可以执行。

在 GUI 中，请去安全>AAA >密码策略。此页有可以选择为了强制执行强口令的一系列的选项。示例如下：



为了从WLC CLI执行此，请使用设置switchconfig强pwd {案例检查|连续检查|默认检查|用户名检查|全检查} {enable (event)|禁用} 命令：

- 案例检查-检查同样的出现 字符连续三次。
- 连续检查-检查是否默认值或 使用其变形。
- 默认检查-检查是否或者用户名或其 使用反向。
- 全检查-启用/禁用所有强 密码检查。

问。 被动客户端特性如何使用在无线局域网控制器？

A. 被动客户端是无线设备，例如缩放比例和打印机那 配置与静态IP地址。这些客户端不传送任何IP 信息例如IP地址、子网掩码和网关信息，当他们 关联用接入点。结果，当使用被动客户端， 除非他们使用DHCP，控制器从未认识IP地址。

WLCs当前作为ARP请求的一个代理。当接收ARP后 请求，控制器回应ARP响应而不是通过 请求直接地对客户端。此方案有两个优点：

- 派出ARP请求给客户端的上行设备 不知道客户端哪里查找。
- 电池操作的设备的电源例如移动电话和打印机 因为他们不必须响应到每个ARP，保留 请求。

因为无线控制器没有任何IP相关信息 关于被动客户端，它不能回答任何ARP请求。当前 行为不允许ARP请求转移到被动客户端。其中任一 设法访问一个被动客户端的应用程序将发生故障。

被动客户端特性启用ARP请求和答复是 交换在有线的和无线客户端之间。此功能，当启用， 允许控制器通过从有线的ARP请求对无线客户端直到 希望的无线客户端达到运转状态。

关于如何配置被动客户端特性的信息，请读 部分 使用 配置被动客户端的GUI 思科 无线局域网控制器配置指南，版本 7.0.116.0。

问。 如何请能I设置客户端用RADIUS服务器重新鉴别 每三分钟或在任何指定的时间段？

A. 在WLC的会话超时参数可以用于完成 这。默认情况下，会话超时参数配置在1800秒 在重新验证前发生。

更改此值为180秒为了做客户端 在三分钟之后重新鉴别。

为了访问会话超时参数，请点击 在GUI的WLAN菜单。它显示WLAN列表 配置在WLC。单击客户端所属的 WLAN。转到 高级选项卡。和您寻找Enable (event)会话 超时参数。更改默认值到180，并且单击 运用使更改生效。

当发送在Access-Accept，与终止行动值一起 RADIUS请求， Session-timeout属性指定最大 在再验证前服务提供的秒钟。在这种情况下， Session-timeout属性用于装载在内的ReAuthPeriod常数 重新验证802.1X计时器状态机。

问。 我有一访客隧道，在IP (EoIP)通道的以太网，配置 在我的4400无线局域网控制器(WLC)之间，作为锚点WLC， 并且几远程WLCs。通过能此锚点WLC转发子网广播 从有线网络的EoIP通道到无线客户端关联与 远程控制器？

A. 不， WLC4400不转送从有线的IP子网广播 对无线客户端的侧在EoIP通道间。这不支持的 功能。思科不支持子网广播隧道也不组播 访客访问拓扑。因为访客WLAN强制客户端入网点 到网络的一个非常详细的位置，主要防火墙的外部， 子网广播隧道可以是安全问题。

问。 在无线局域网控制器(WLC)和轻量级接入点协议 (LWAPP)设置，什么差分服务代码点重视通过 语音流量？如何在 WLC 上实现 QoS？

A. Cisco Unified无线网络(UWN)解决方案WLAN支持四 级别QoS :

- 白金服务/语音
- 金牌服务/视频
- 银牌服务/尽力 (默认值)
- 铜牌服务或背景

您能配置语音流量WLAN使用白金服务QoS, 分配 使用古铜色QoS和分配其他流量的低带宽WLAN之间 其他QoS级别。请参阅分配 对一WLAN的QoS配置文件欲知更多信息。

问。 是支持Linksys以太网网桥Cisco无线统一 解决方案?

A. 不支持, WLC 仅支持 Cisco WGB 产品。Linksys WGBs不是 支持的。虽然Cisco无线统一的解决方案不支持 Linksys WET54G和WET11B以太网网桥, 您在a能使用这些设备 无线统一的解决方案配置, 如果使用这些指南:

- 只将一个设备连接到 WET54G 或 WET11B。
- 启用克隆在WET54G或WET11B的MAC功能克隆 连接的设备。
- 安装最新的驱动程序和固件在设备连接对 WET54G或WET11B。此指南对JetDirect打印机是特别重要 因为初期的固件版本引起问题由于DHCP。

注意: 不支持其他第三方网桥。被提及的步骤能 也为其他第三方网桥请尝试。

问。 如何我请存储在无线局域网控制器的配置文件 (WLC) ?

A. WLC 包含两种内存:

- 可变的RAM —拿着当前, 激活控制器 配置
- 非易失性RAM (NVRAM) —保持重新启动 配置

当您配置在WLC时的操作系统, 您正在修改 可变的RAM。您必须保存从可变的RAM的配置到 NVRAM为了确保, WLC在当前配置里重新启动。

知道是重要的哪个内存您正在修改, 当您实行时 这些任务:

- 使用配置向导。
- 清除控制器配置。
- 保存配置。
- 重置控制器。
- 注销 CLI。

功能常见问题解答

问。 我如何设置在的可扩展的认证协议(EAP)类型 无线局域网控制器(WLC) ? 我要验证访问控制 服务器(ACS)设备和我获得“不支持的EAP”输入 日志。

A. WLC 上没有单独的 EAP 类型设置。轻的EAP (LEAP), EAP灵活验证通过获取建立隧道(EAP-FAST), 或者Microsoft 已保护EAP (MS-PEAP), 配置IEEE 802.1x或wi-fi受保护的访问 (WPA) (如果以WPA使用802.1x)。支持的任何EAP类型 RADIUS后端和在客户端通过802.1x标记支持。EAP 设置在客户端和RADIUS服务器必须配比。

完成这些步骤为了通过的GUI启用EAP WLC :

1. 从WLC GUI, 请单击 WLAN。
2. 这将显示 WLC 中配置的 WLAN 的列表。单击某个 WLAN。
3. 在WLAN > Edit, 请点击 安全选项卡。
4. 点击Layer2, 并且选择第2层安全 802.1x或WPA+WPA2。 您能也配置是可行的802.1x参数 同一个窗口。然后, WLC 转发在之间的EAP验证数据包 无线客户端和认证服务器。
5. 点击AAA服务器, 并且选择 从下拉菜单的认证服务器此WLAN的。我们假设, 认证服务器已经配置全局。关于如何的信息 通过命令行界面(CLI)启用在WLCs的EAP选项, 参考 到 使用 配置RADIUS的CLI 部分 思科 无线局域网控制器 配置指南, 版本 7.0.116.0。

问。 什么是快速 SSID 更改?

A. 快速 SSID 更改允许客户端在 SSID 之间移动。当 客户端发送一不同的SSID的一个新的关联, 在的客户端条目 控制器连接表, 在客户端被添加到新前, 清除 SSID。当快速SSID更改禁用时, 控制器强制执行延迟 在客户端允许移动向一新的SSID前。关于如何的信息 更改enable (event)快速的SSID, 参考 配置 快速SSID更改 部分 思科 无线局域网控制器 配置指南, 版本7.0.116.0。

问。 能定在能连接到无线客户端的数量的一限制 LAN ?

A. 您能限制为能连接到a客户端的数量 WLAN，是有用的在方案您有客户端有限数量 那能连接到控制器。您能配置客户端的数量 每WLAN取决于平台您使用。

阅读部分 配置 客户端最大每WLAN 思科 无线局域网控制器配置指南，版本7.0.116.0为 关于客户端的信息每另外平台的WLAN限制 无线局域网控制器。

问。 什么是PKC，并且如何执行它与无线局域网控制器一起使用（WLC）？

A. PKC 是指积极密钥缓存。它设计作为分机 到802.11i IEEE标准。

PKC是在Cisco 2006/410x/440x系列控制器启用的功能 哪些许可证适当地装备无线客户端漫游，不用全双工 与AAA服务器的再验证。为了首先了解PKC，您 需要了解关键高速缓冲存储。

密钥缓存是 WPA2 中添加的功能。这允许移动 通过a获取缓存主密钥的站点(成对地主密钥[PMK])与接入点(AP)的成功认证，和在a重新使用它 有同样AP的将来关联。这意味着给的移动 设备需要一次验证与特定AP，并且缓存密钥为 未来使用。关键高速缓冲存储通过叫作PMK标识符的机制被处理 (PMKID)，是PMK、字符串、站点和MAC的哈希 AP的地址。PMKID可唯一标识 PMK。

与关键高速缓冲存储，一个无线站点必须验证与其中每一 希望获得服务从的AP。这引入明显的延迟和 开销，请延迟 hand-off进程，并且能禁止能力 支持实时应用。为了解决此问题， PKC是 介绍与WPA2。

PKC允许通过a以前获取了的站点重新使用PMK 成功认证进程。这排除对站点的需要 当漫游时，请验证新的AP。

所以，在漫游的内部控制器，当移动设备移动 从一个AP到另一个在同一个控制器，客户端重新计算PMKID 使用以前使用的PMK和在关联过程中提交它。 WLC 将搜索其 PMK 缓存以确定是否有这样一个条目。如果它 它绕过802.1x认证过程和立即启动 WPA2密钥交换。如果它不，通过标准的802.1X 认证过程。

在 WPA2 中，默认启用了 PKC。所以，当您启用WPA2 在WLC的WLAN配置的下第2层安全， PKC在启用 WLC。并且，请配置AAA服务器和无线客户端适当的EAP的 验证。

请求方使用在客户端应该也支持WPA2 PKC的指令能工作。PKC在控制器之间可能也实现 漫游环境。

注意： PKC不与Aironet Desktop软件(ADU)一起使用作为客户端 请求方。

问。 控制器上的以下超时设置是什么意思： 地址解析服务(ARP)超时、用户空闲超时和会话 超时？

A. ARP超时用于删除在的ARP条目 从网络了解的设备的WLC。

User Idle Timeout: 当用户是空闲没有其中任一 与LAP的通信作为用户空闲超时设置的时间的， 客户端由WLC deauthenticated。客户端必须重新鉴别和 重新关联对WLC。用于客户端能脱离的情况 从其没有通知LAP的相关的LAP。这能发生，如果 电池在客户端去死或客户端关联移动离开。

注意： 为了访问ARP和用户空闲超时在WLC GUI，请去 控制器菜单。从选择常规 查找ARP和用户空闲超时字段的左手边。

会话超时是客户端的最大时间 有WLC的会话。在此时间之后， WLC DE验证客户端，和 客户端通过再整个验证(再验证)进程。这是安全防范措施的一部分，以便轮换加密密钥。如果您 以密钥管理使用一个可扩展的认证协议(EAP)方法，重新生成密钥发生在每固定间隔为了派生新的加密 密钥。没有密钥管理，此超时值是无线的 客户端需要执行一全双工重新验证。会话超时是特定 WLAN。此参数可以从WLAN访问> Edit菜单。

问。 什么是 RFID 系统? Cisco 当前支持哪些 RFID 标记?

A. 射频识别(RFID)是使用无线电的技术 一相当短程通信的频率通信。一基本RFID 系统撰写RFID标记、RFID读者和处理的软件。

当前 Cisco 支持来自 AeroScout 和 Pango 的 RFID 标记。更多 关于如何的信息配置AeroScout标记，参考 WLC AeroScout RFID标记的配置。

问。 我能否在 WLC 上执行本地 EAP 认证? 有其中任一 描述解释此本地EAP功能?

A. 可以，EAP 认证可以在 WLC 上本地执行。本地EAP 是允许用户和无线客户端是的认证方法 验证本地在WLC。它设计用于远程办公室那 要维护连接对无线客户端，当后端系统 变得打乱，或者外部验证服务器断开。当您 启用本地EAP，WLC 作为认证服务器。更多 关于如何的信息请配置本地EAP法塞特验证的一WLC，参考 到 本地 在无线局域网控制器的EAP验证用EAP-FAST和LDAP服务器 配置示例。

问。 什么是 WLAN 覆盖功能? 如何配置此功能? 能够 当他们故障切换对备份时，膝部维护WLAN覆盖值 WLC ?

A. WLAN覆盖功能使我们从在中选择WLAN 在能积极地使用根据个人LAP基本类型的WLC的配置。要配置 WLAN 覆盖，请完成以下步骤：

1. 在WLC GUI中, 请点击无线 菜单。
2. 点击在左手边的选项无线电, 和 选择802.11 a/n或802.11 b/g/n.
3. 点击从下拉菜单的配置链路 找到在对应于AP名称您的右侧 要配置WLAN覆盖。
4. 从下拉式WLAN的覆盖选择Enable (event) 菜单。WLAN覆盖菜单是最后项目在的左边 窗口。
5. 在WLC配置所有WLAN的列表 出现。
6. 从此列表, 请检查您希望的WLAN 出现在LAP, 并且单击申请更改采取 效果。
7. 在您做这些后, 请保存您的配置 更改。

当他们得到登记时, AP保留WLAN覆盖值 其他WLCs, 在您要改写条件下的WLAN配置文件和Ssid是 配置在所有WLCs间。

注意: 在控制器软件版本5.2.157.0中, WLAN覆盖功能 从控制器GUI和CLI删除。如果您的控制器是 配置为WLAN覆盖和 您请升级到控制器软件版本 5.2.157.0, 控制器删除WLAN配置并且广播所有 WLAN。如果配置, 您能指定仅该某WLAN传送 接入点组。每接入点通告仅已启用WLAN那 属于其接入点组。

注意: 接入点组不启用WLAN将传送每 AP无线接口。

问。 是支持IPv6 Cisco无线LAN控制器(WLCs)和 轻量级接入点(膝部) ?

A. 目前, 4400和4100系列控制器只支持IPv6 客户端转接。尚未提供本地 IPv6 支持。

为了启用在WLC的IPv6, 请检查IPv6 在WLAN SSID配置的Enable复选框在WLAN下> Edit页。

此外, 还需要以太网组播模式 (EMM) 以支持 IPv6。如果您 禁用EMM, 使用IPv6丢失连接的客户端设备。为了启用 EMM, 去Controller>一般页, 并且从以太网请组播 模式下拉菜单, 选择单播或 组播。这启用组播或者在单播模式或 组播模式。当组播启用作为组播单播时, 数据包是 复制为每个AP。这可以是密集的处理, 因此请使用它以 小心。组播已启用, 组播组播使用使用者指定 要执行一更加传统的组播的组播地址对接入点 (AP)。

注意: 2006 控制器不支持 IPv6。

并且, 有Cisco Bug ID CSCsg78176, 防止使用IPv6 转接, 当使用AAA Override功能。

问。 执行Cisco 2000系列无线局域网控制器(WLC)支持Web 来宾用户的验证?

A. 所有 Cisco WLC 都支持 Web 认证。Web验证 是用于的第3层认证方法验证有简单的用户 认证证书。这里不涉及加密。完成这些步骤 命令启用此功能:

1. 从GUI, 请点击WLAN 菜单。
2. 单击某个 WLAN。
3. 去安全选项卡并且选择层 3。
4. 检查Web策略方框并且选择 验证。
5. 单击 Apply 以保存更改。
6. 为了创建在WLC的一个数据库 验证用户, 去在GUI的Security菜单, 选择 本地使用户获得, 并且完成这些操作:
 - a. 定义访客的访客用户名和密码能使用 命令登录。这些值区分大小写。
 - b. 选择您使用的 WLAN ID。

注意: 对于更多详细配置, 参考 无线 LAN控制器Web身份验证配置示例。

问。 能否以无线模式管理 WLC?

A. 如果启用, 则可以通过无线模式管理 WLC。更多 关于如何的信息启动无线模式参考 启用 对GUI和CLI的无线连接 部分 思科 无线局域网控制器配置指南, 版本7.0.116.0。

问。 什么是链路聚合 (LAG)? 如何我请启用在无线局域网的滞后 控制器(WLCs) ?

A. 滞后捆绑WLC的所有端口到单个EtherChannel 接口。系统动态地管理数据流负载平衡和端口 与滞后的冗余。

通常, 在WLC的接口有多个参数关联与 它, 包括IP地址, 默认网关(IP子网), 主要的 物理端口、附属物理端口、VLAN标记和DHCP服务器。当滞后是 没使用, 每个接口通常被映射对物理端口, 但是多个 接口可能也被映射到单个WLC端口。当使用滞后, 系统动态地映射接口到聚集的端口通道。这 在输出冗余和负载均衡的帮助。当端口发生故障, 接口 动态地被映射到下一个可用的物理端口, 并且膝部是 平衡在端口间。

当滞后在WLC时启用, WLC传送在同样的数据帧 他们接收的端口。WLC依靠邻居交换机 在EtherChannel间的负载均衡流量。WLC不执行其中任一 EtherChannel负载平衡独自地。

问。 什么模拟无线局域网控制器(WLCs)支持链接聚合 (滞后) ?

A. 在软件版本6.0的Cisco 5500系列控制器支持滞后或 在软件版本3.2的最新, Cisco 4400系列控制器支持滞后或 以后和滞后在控制器在思科内自动地启用 WiSM和Catalyst 3750G集成无线局域网控制器交换机。没有 滞后, 一个Cisco 4400系列控制器支持的每个分布式系统端口 48接入点。使用无滞后, 逻辑思科4402的控制器 的 端口支持50接入点, 思科4404

控制器的逻辑端口 支持100接入点和逻辑端口Catalyst的3750G 集成无线局域网控制器交换机和在每个思科WiSM控制器支持150接入点。

Cisco 2106 和 2006 WLC 不支持 LAG。更早模式，这样 作为Cisco 4000系列WLC，请勿支持滞后。

问。 什么是在Unified无线的自动锚点移动性功能 网络？

A. 自动锚点移动性(或访客WLAN移动性)用于改善负载 漫游的客户端平衡和安全您的无线LAN的(WLAN)。下面 漫游情况的正常，客户端设备加入WLAN和停住对 与联系他们的第一个控制器。如果客户端漫游对一不同的子网，客户端漫游的控制器设置的一外国会话 客户端用锚点控制器。使用使用自动锚点移动性 功能，您能指定控制器或套控制器作为锚点 客户端的点WLAN的。

注意： 不能为第 3 层移动性配置移动锚点。 移动性锚点仅使用访客隧道。

问。 能思科2006无线局域网控制器(WLC)配置作为锚点 WLAN ？

A. 不能将 Cisco 2000 系列 WLC 指定为 WLAN 的锚点。然而，在一Cisco 2000系列WLC创建的WLAN能有Cisco 4100系列WLC和Cisco 4400系列WLC作为其锚点。

问。 无线 LAN 控制器使用哪种移动隧道？

A. 控制器软件版本4.1通过5.1支持不对称的两个 并且对称移动性建立隧道。控制器软件版本5.2或以上 支持建立隧道仅对称的移动性，总是当前启用 默认。

在不对称隧道，对有线网络的客户端的流量路由 直接地通过外国控制器。不对称隧道中断，当 上游路由器安排反向路径过滤(RPF)启用。在这种情况下， 因为RPF检查保证的那客户端的流量丢弃在路由器 回到源地址的路径匹配数据包来的路径。

当对称移动性建立隧道启用时，所有客户端的流量是 发送对锚点控制器，并且能顺利地然后通过RPF检查。 对称移动隧道在以下情况下也很有用：

- 如果防火墙安装在客户端信息包路径丢弃数据包 因为源IP地址不匹配的子网数据包 接收，这是有用的。
- 如果锚点控制器的访问点组VLAN不同的 比在外国控制器的WLAN接口VLAN：在这种情况下，客户端 在移动性期间，流量在不正确VLAN可以发送 事件。

问。 如何我们访问WLC，当网络是时 下来？

A. 当网络发生故障时，可以通过服务端口访问 WLC。此端口分配在一完全不同的子网的一个IP地址从其他 WLC的端口和如此呼叫带外管理。欲知更多信息， 参考 配置 端口和接口 部分 思科 无线局域网控制器配置指南，版本7.0.116.0。

问。 执行Cisco无线LAN控制器(WLCs)支持故障切换(或 冗余)功能？

A. 是，如果有两个或多个WLCs在您的WLAN网络，您能 为冗余配置他们。通常，LAP加入对已配置的主要的 WLC。一旦主要的WLC发生故障，LAP重新启动并且加入在的另一WLC 移动组。故障切换是功能，LAP为主要的WLC轮询 一旦是工作，并且加入主要的WLC。请参阅 WLAN 轻量级接入点配置示例的控制器故障切换。

问。 什么是使用预验证访问控制列表(ACL)无线局域网控制器(WLCs) ？

A. 使用预验证ACL，作为名称暗示，您能允许客户端 到/从一个特定IP地址的流量在客户端以前验证。当曾经外部Web服务器Web验证，某些WLC时 平台需要外部Web服务器的(思科预验证ACL 5500系列控制器，一个Cisco 2100系列控制器，Cisco 2000系列和 控制器网络模块)。其他WLC平台， 预验证ACL不是必须。然而，它是良好的做法 当曾经时，请配置外部Web服务器的预验证ACL 外部Web验证。

问。 我的网络中有一个 MAC 过滤 WLAN 和一个完全开放的 WLAN。客户端是否会默认选择开放的 WLAN？或者 执行客户端 与在MAC过滤器设置的WLAN ID自动地产生关联？并且， 为什么有在MAC过滤器的一个“接口”选项？

A. 客户端能联合到客户端配置的所有WLAN to connect。在MAC过滤器的接口选择给能力应用 对WLAN或接口的过滤器。如果多个WLAN附加对 同样接口，您能应用MAC过滤器到接口，不用需要 创建每个WLAN的一个过滤器。

问。 如何能配置管理用户的TACACS认证的 无线局域网控制器(WLC) ？

A. 从 WLC 版本 4.1 开始，WLC 支持 TACACS。参考 配置 TACACS+为了知道如何配置TACACS+验证 WLC的管理用户。

问。 什么是使用在a的额外的认证失败设置 无线局域网控制器(WLC) ？

A. 该设置是客户端排除策略之一。客户端 排除是在控制器的一个安全功能。策略用于 列入黑名单客户端为了防止对网络或攻击的非法访问 对无线网络。

当此额外的Web认证失败策略启用，当a 失败的Web认证尝试客户编号超过5，控制器 考虑客户端超出了Web最大尝试 验证和列入黑名单客户端。

完成这些步骤为了启用或禁用此 设置：

1. 从WLC GUI，去安全>无线保护 策略>客户端排除策略。
2. 检查或不选定额外的Web验证 失败。

问。 我将我的自治接入点 (AP) 转换为轻量模式。在 轻量AP协议 (LWAPP) 模式用客户端的AAA RADIUS服务器 认为，客户端通常跟踪与根据的RADIUS认为 WLC的IP地址。是它可能设置根据的RADIUS认为 关联的AP的MAC地址对该WLC而不是IP地址的 WLC ？

A. 可以，可以通过 WLC 方面的配置完成此设置。完成这些 步骤：

1. 从控制器GUI，在安全> Radius下 认为，有呼叫站ID类型的一个下拉框。选择 AP MAC地址。
2. 通过 LWAPP AP 日志对此进行验证。 在那里，显示的您能看到被叫站ID字段 特定的客户端关联AP的MAC地址。

问。 您如何更改Wi-Fi保护访问 (WPA) 握手超时 重视在无线局域网控制器 (WLC) 通过CLI ？我知道我能执行此 Cisco IOS接入点 (AP) 有dot11 WPA握手的 超时值 命令，但是如何请执行您 执行此在WLC ？

A. 能力通过WLCs配置WPA握手超时是 集成在软件版本4.2和以上。您不需要此选项 初期的WLC软件版本。

可使用以下命令更改 WPA 握手超时值：

```
config advanced eap eapol-key-timeout <value>
config advanced eap eapol-key-retries <value>
```

默认值继续反射WLCs当前 行为。

- the default value for eapol-key-timeout is 1 second.
- the default value for eapol-key-retries is 2 retries

注意： 在IOS AP，此设置是可配置与dot11 WPA握手命令。

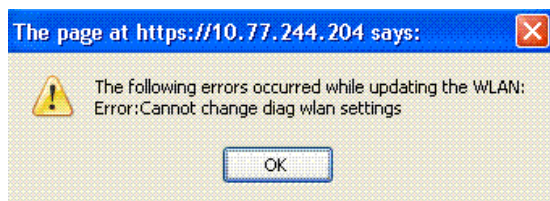
您能也配置与下选项的其他EAP参数 设置提前的eap命令。

```
(Cisco Controller) >config advanced eap ?
eapol-key-timeout
  Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
  Configures EAPOL-Key Max Retries.
identity-request-timeout
  Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
  Configures EAP-Identity-Request Max Retries.
key-index
  Configure the key index used for
  dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
  Configure to ignore the same username count
  reaching max in the EAP identity response
request-timeout
  Configures EAP-Request Timeout in seconds.
request-retries
  Configures EAP-Request Max Retries.
```

问。 什么是诊断信道功能的目的是在WLAN的 > 编辑>Advanced页？

A. 诊断信道功能使您排除故障问题 对客户端通信的方面与WLAN。客户端和接入点可以是 接通识别通信的原因的定义的 测验 困难客户端体验然后准许纠正措施 请被采取使客户端可操作在网络。您能使用 启用诊断信道和您的控制器GUI或 CLI能使用 运行诊断测试的控制器CLI或WCS。

诊断信道只能用于测试。如果尝试 配置验证或加密WLAN的用诊断信道 已启用，您看到此错误：



问。在 WLC 上可以配置的最大 AP 组数是多少？

A. 此列表显示 AP 组最大您能配置在 WLC ：

- 50 接入点组最大数量 Cisco 2100 系列的 控制器和控制器网络模块
- 300 接入点组最大数量 Cisco 4400 系列的 控制器、思科 WiSM 和思科 3750G 无线局域网控制器 交换机
- 500 接入点组最大数量 Cisco 5500 系列的 控制器

相关信息

- 无线 LAN 控制器 (WLC) FAQ
- 无线 LAN 控制器 (WLC) 错误和系统消息 FAQ
- 轻量 接入点 FAQ
- 思科 无线局域网控制器配置指南，版本 7.0.116.0
- 在无线局域网控制器的 IPv6 支持
- 问答

版权所有 ©1992–2014 思科系统

文件创建日期：2013 年 8 月 5 日

http://www.cisco.com/cisco/web/support/CN/110/1105/1105735_wlc-design-ftrs-faq.html
