

无线局域网控制器(WLC)设计和功能常见问题

文档ID118833

已更新：2015年3月02日

 [下载 pdf文档](#)

 [打印](#)

[Feedback](#)

相关产品

- [Cisco 4400 系列无线局域网控制器](#)
- [思科5500系列无线控制器](#)
- [思科无线服务模块2 \(WiSM2\)](#)
- [思科2500系列无线控制器](#)
- [思科2100系列无线局域网控制器](#)
- [Cisco Catalyst 3750 系列集成无线局域网控制器](#)
- [Cisco Catalyst 6500 系列/7600 系列无线服务模块 \(WiSM\)](#)
- [Cisco 2000 系列无线局域网控制器](#)
- [Cisco 无线局域网控制器模块](#)
- [Cisco 4100 系列无线局域网控制器](#)
- [+请显示更多](#)

Contents

[Introduction](#)

[设计常见问题解答](#)

[功能FAQ](#)

[Related Information](#)

[相关的思科支持社区讨论](#)

Introduction

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。

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

[设计常见问题解答](#)

[Q. 如何配置交换机连接WLC ?](#)

A. 配置交换端口，WLC被连接，作为IEEE 802.1Q中继端口。切记仅必要的VLAN在交换机允许。通常，管理和WLC的AP管理器接口留给无示踪。这意味着他们假设连接的交换机的本地VLAN。这

不是必要的。您能分配独立的VLAN到这些接口。欲知更多信息，请参见[配置无线局域网控制器和轻量接入点基本配置示例的WLC部分](#)的[交换机](#)。

Q. 所有网络流量是否从和对WLAN客户端通过无线局域网控制器(WLC)建立隧道，一旦接入点(AP)用控制器得到登记？

A. 当AP加入WLC时，无线访问接入点协议(CAPWAP)隧道控制和设置形成在两个设备之间。所有数据流，包括所有客户端的流量，通过CAPWAP隧道被发送。

此的唯一的例外是，当AP是混合收割模式时。当他们的与控制器的连接丢失时，混合收割接入点可本地交换客户端数据数据量和进行客户端验证本地。当他们被联系到控制器时，他们能也送回数据流到控制器。

Q. 在远程办公室安装轻量级接入点(膝部)和能否在总部安装Cisco无线LAN控制器(WLC)？LWAPP/CAPWAP是否在广域网工作？

A. 是，您能有在广域网间的WLCs从APs。LWAPP/CAPWAP在广域网工作，当膝部在远程边缘AP (请收割)时或混合的远程边缘AP (H-REAP)模式被配置。这些模式之一由通过广域网链路被连接的远程控制器允许AP的控制。数据流桥接在LAN链路上本地，避免需要不必要地发送在广域网链路的本市通话业务。这是精密地一个最巨大的优点的有WLCs在您的无线网络。

Note: 不是所有的轻量APs技术支持这些模式。例如，支持H-REAP仅模式1131年，1140,1242，1250和AP801膝部。收割模式1030个AP仅支持，但是APs不支持的1010和1020收割。在您计划实现这些模式前，请检查确定膝部是否支持它。软件APs的Cisco IOS (自动APs)被转换成了LWAPP不支持收割。

Q. 如何收割，并且H-REAP模式工作？

A. 在**收割**模式下，所有控制和管理数据流，包括认证数据流，被以隧道传输回到WLC。但是所有数据流量在远程办公室LAN内本地交换。当与WLC的连接丢失时，所有WLANs被终止除了第一WLAN (WLAN1)。当前被关联对此WLAN的所有客户端保留。为了允许新的客户端成功验证和得到在此WLAN的服务在停工期内，请配置此WLAN的认证方法作为WEP或WPA-PSK，以便认证完成本地。关于的更多信息请收割配置，是指[在分支机构收割部署指南](#)。

在**H-REAP**模式下，接入点以隧道传输控制和管理数据流，包括认证数据流，回到WLC。从WLAN的数据流量在远程办公室桥接本地，如果WLAN配置有H-REAP本地交换，或者数据流量被退还到WLC。当与WLC的连接丢失时，所有WLANs被终止除了与H-REAP本地交换的前八配置。当前被关联对这些WLANs的所有客户端保留。为了允许新的客户端成功验证和得到在这些的服务在停工期的WLANs，配置此WLAN的认证方法作为WEP、WPA PSK或者WPA2 PSK，以便认证完成本地在H-REAP。

关于H-REAP的更多信息，请参见[H-REAP设计和部署指南](#)。

Q. 远程边缘AP (收割)和Hybrid-REAP (H-REAP)有何区别？

A. **REAP**不支持IEEE 802.1Q VLAN标记。同样地，它不支持多个VLAN。从所有服务集标识(SSID)的数据流在相同子网，但是H-REAP支持IEEE 802.1Q VLAN标记终止。从每SSID的数据流可以被分段到唯一的VLAN。

当对WLC的连接在独立模式下时丢失，即，请收割服务仅一WLAN，即，第一WLAN。撤销其他WLANs。在H-REAP，8 WLANs在停工期内支持。

另一个主要区别是，请收割模式，数据流量可能只桥接本地。它不可以是交换式回到中心局，但是，在H-REAP模式下，您有选项交换数据流回到中心局。从配置的数据流与H-REAP本地交换本地交换。从其他WLANs的数据流量是交换式回到中心局。

参考远程[边缘AP \(请收割\)与轻量APs和无线局域网控制器\(WLCs\)配置示例](#)关于的更多信息收割。

参考[配置混合收割](#)关于H-REAP的更多信息。

Q. WLC支持WLANs多少？

A. 从软件版本5.2.157.0，WLC能当前控制512 WLANs轻量级接入点的。每WLAN有分开的WLAN ID (1至512)，分开的配置文件名字和—WLAN SSID，并且可以分配唯一安全策略。控制器发布16 WLANs到每连接的接入点，但是您能创建512 WLANs在控制器选择性地然后发布这些WLANs (使用接入点组)对更好管理您的无线网络的不同的接入点。

Note: Cisco 2106，2112和2125个控制器只支持16 WLANs。

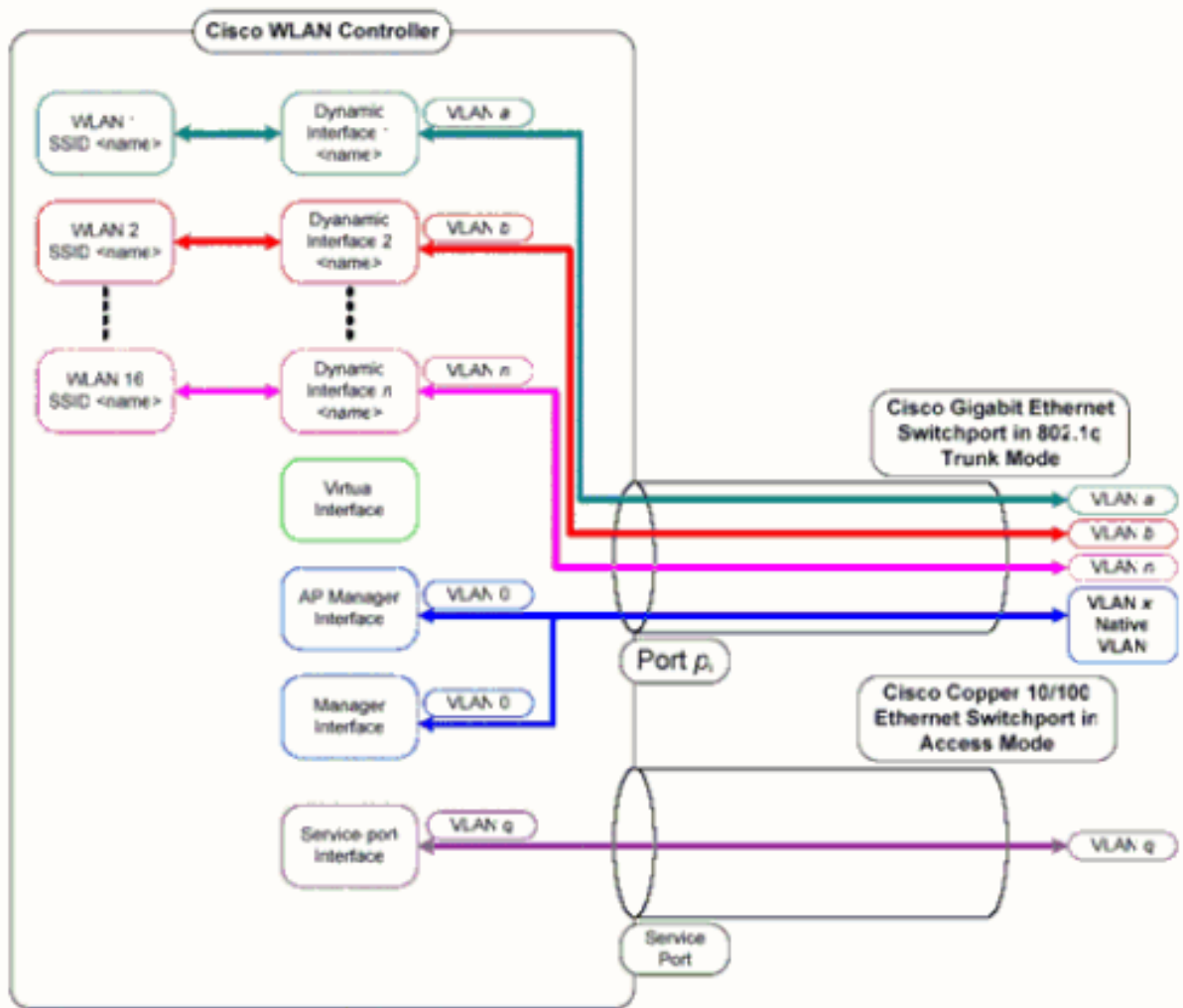
Note: 关于配置WLANs指南的详细信息在WLCs，请阅读[Cisco无线LAN控制器配置指南的创建的WLANs部分，版本7.0.116.0](#)。

Q. 如何能配置在无线局域网控制器(WLC)的VLAN？

A. 在WLC，VLAN附加对在唯一IP子网配置的接口。此接口被映射在WLAN上。然后，联合对此WLAN的客户端属于接口的VLAN和分配从接口属于的子网的一个IP地址。为了配置在您的WLC的VLAN，请完成在[VLAN的程序在无线局域网控制器配置示例](#)。

Q. 我们设置了两WLANs与两个不同的动态接口。每个接口有其自己的VLAN，跟管理接口VLAN不同。这似乎工作，但是我们未设置中继端口允许我们的WLAN使用的VLAN。接入点(AP)是否用管理接口VLAN标记信息包？

A. AP用管理接口VLAN不标记信息包。AP封装自客户端的信息包轻量级AP协议的(LWAPP)/CAPWAP，然后传递信息包对WLC。WLC然后剥离LWAPP/CAPWAP报头并且转发信息包到有适当的VLAN标记的网关。VLAN标记依靠客户端属于的WLAN。WLC依靠网关路由信息包到他们的目的地。为了能通过多个VLAN的数据流，您必须配置上行链路交换机作为中继端口。此图表解释VLAN如何与控制器一起使用：



Q. WLC的哪个IP地址使用认证与AAA服务器？

A. WLC使用管理接口的IP地址所有认证机制(介入一个AAA服务器的第2层或第3)层。关于端口和接口的更多信息在WLC，请参见[Cisco无线LAN控制器配置指南的配置的端口和接口部分，版本7.0.116.0](#)。

Q. 我有十Cisco 1000系列轻量级接入点(膝部)和两个无线局域网控制器(WLCs)在同样VLAN。如何能注册六膝部联合到WLC1和联合的其他四膝部对WLC2？

A. LWAPP/CAPWAP允许动态冗余和负载均衡。例如，如果为选项43指定超过一个IP地址，LAP发送LWAPP/CAPWAP发现请求到AP收到的其中每一个IP地址。在WLC LWAPP/CAPWAP发现回应，WLC嵌入此信息：

- 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
- 被联络到WLC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，您能做LAP加入在其下辆重新启动内的一特定WLC。为了执行此，为LAP请分配一主要的，附属和第三WLC。当LAP重新启动，它寻找主要的WLC并且加入该WLC对立于在该WLC的负荷。如果主要的WLC不回应，寻找第二，如果无响应，第三。关于如何配置LAP的主要的

WLC的更多信息，请参见[WLAN控制器故障切换的轻量AP部分的分配主要的，附属和第三控制器轻量级接入点配置示例](#)。

Q. 什么是2100系列无线局域网控制器的功能(WLCs)不支持？

A. 2100系列控制器不支持这些硬件特点：

- 服务端口(分开的带外管理10/100 Mb/s以太网接口)

2100系列控制器不支持这些软件功能：

- VPN终端(例如IPsec和L2TP)
- 客户控制器隧道的终端(支持客户控制器隧道的起源)
- 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单个用户的带宽合同
- IPv6 穿透
- 链路聚合(滞后)
- 组播单播模式
- 有线访客访问

Q. 5500系列控制器不支持什么功能？

A. 5500系列控制器不支持这些软件功能：

- 静态AP管理器接口 **Note:** 对于5500系列控制器，没有要求您配置AP管理器接口。默认情况下管理接口作为AP管理器接口，并且接入点在此接口能加入。
- 不对称移动性建立隧道
- 生成树协议(STP)
- 端口镜像
- 第2层访问控制表(ACL)技术支持
- VPN终端(例如IPSec和L2TP)
- VPN转接选项
- 802.3桥接，AppleTalk和以太网点对点协议(PPPoE)的配置

Q. 网状网络不支持什么功能？

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
- 基于负荷的CAC (只基于带宽的网状网络技术支持或者静态，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(网接入点有固定的优先级。)

- 局部重要的认证
- 基于位置的服务

Q. 什么是有效性周期制造商安装的证书(MICs)在无线局域网控制器和轻量AP的证书？

A. MIC的有效性周期在WLC的是10年。同一个有效性周期10年应用于轻量AP的证书从创建(它是否是MIC或自签证书(SSC))。

Q. 我有两个无线局域网控制器(WLCs)名为在故障切换的同样移动组内被配置的WLC1和WLC2。我的轻量级接入点(LAP)当前向WLC1登记。如果WLC1发生故障，AP注册对WLC1重新启动在其往生存WLC (WLC2)的转换时？并且，在此故障切换期间，WLAN客户端是否丢失与LAP的WLAN连接？

A. 是，如果WLC1发生故障，LAP从WLC1注销登记，重新启动，然后重新登记与WLC2。由于LAP重新启动，相关的WLAN客户端丢失连接对重新启动的LAP。相关信息，请参见[AP负载均衡和AP退路在统一的无线网络](#)。

Q. 漫游是否是从属于轻量接入点无线局域网控制器的协议(LWAPP)模式(WLC)配置使用？WLC在的第2层LWAPP模式下运行可执行漫游的第3层？

A. 只要正确地配置组队在控制器的移动性，漫游的客户端应该良好工作。漫游由LWAPP模式是未受影响的(第2层或第3)层。然而，推荐在任何可能的情况下使用第3层LWAPP。

Note: Cisco仅支持第2层模式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第2层LWAPP。

Q. 什么是发生的漫游的进程，当客户端决定漫游到新的接入点(AP)或控制器时？

A. 这是发生的事件顺序，当客户端漫游对新的AP：

1. 客户端发送一个再聚集请求到WLC通过LAP。
2. WLC传送移动性信息到移动组的其他WLCs为了发现与哪WLC客户端以前是关联的。
3. 原始WLC回应信息，例如MAC地址、IP地址、QoS，安全上下文等等关于客户端通过移动性消息。
4. WLC更新其与提供的客户端细节的数据库;客户端然后通过再验证进程，如果需要。客户端当前产生关联的新的LAP与在WLC的数据库的其他详细资料一起也更新。这样，客户端IP地址保留漫游在WLCs之间，帮助提供无缝的漫游。

关于漫游在一个统一的环境里的更多信息，请参见[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](#)。

Note: 无线客户端不在再聚集时派出(802.11)认证请求。无线客户端立即派出再聚集。然后，它将通过802.1x认证。

Q. 当有在网络时的防火墙需要为LWAPP/CAPWAP通信允许什么端口？

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
- Enable (event) CAPWAP数据流的这些UDP端口：数据- 5247控制- 5246
- 为移动性流量启用如下 UDP 端口：16666 -获取的模式16667 -无担保的模式

移动性和数据信息通过EtherIP信息包通常被交换。在防火墙必须允许IP协议97允许EtherIP信息包。如果使用ESP封装移动性信息包，您必须通过防火墙允许ISAKMP，当您打开UDP端口500时。您必须也打开IP协议50允许加密的数据穿过防火墙。

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
- Telnet的TCP 23并且/或者22或安全壳SSH CLI访问的

Q. 无线局域网控制器是否支持SSHv1和SSHv2？

A. 无线局域网控制器支持仅SSHv2。

Q. 反向ARP (RARP)通过无线局域网控制器(WLCs)支持？

A. 反向地址转换协议(RARP)是用于的链路层协议获得一个提供的链路层地址的一个IP地址例如以太网地址。RARP用与固件版本4.0.217.0或以上的WLCs支持。任何更早版本不支持RARP。

Q. 能否使用在无线局域网控制器(WLC)的内部DHCP服务器为了分配IP地址到轻量级接入点(膝部)？

A. 控制器包含一个内部DHCP服务器。此服务器用于已经没有一个DHCP服务器的分支机构典型地。为了访问DHCP服务，请点击从WLC GUI的**控制器**菜单;然后请点击在页的左手边的选项**内部DHCP服务器**。关于如何配置在WLC的DHCP范围的更多信息，请参见[Cisco无线LAN控制器配置指南的配置的DHCP部分，版本7.0.116.0](#)。

内部服务器提供DHCP地址给无线客户端，膝部、工具模式APs在管理接口和从膝部被传递的DHCP请求。WLCs为设备从未提供地址上行在有线网络。内部服务器不支持DHCP选项43，因此AP必须使用一个备选方法找出控制器的管理接口IP地址，例如本地子网广播、DNS、飞沫或者通过空气发现。

Note: WLC固件版本，在4.0不支持膝部的前DHCP服务，除非膝部直接地被连接到WLC。内部DHCP服务功能用于只提供IP地址给连接到无线LAN网络的客户端。

Q. 在WLAN下的DHCP要求的字段表示什么？

A. 需要的DHCP是可以是启用的为WLAN的选项。它需要联合对该特定的WLAN的所有客户端通过DHCP获得IP地址。客户端用静态IP地址不允许联合到WLAN。此选项被找到在WLAN的高级选项卡下。只有当其IP地址是存在WLC的MSCB表里，WLC允许到/从客户端的数据流。WLC记录客户端的IP地址在其DHCP请求期间或DHCP更新。这要求客户端更新每次重新关联对WLC的其IP地址，因为客户端每次分离，当部分的其漫游进程或会话超时，其条目从MSCB表被清除。客户端必须再重新鉴别和重新关联到WLC，在表里再做客户端条目。

Q. Cisco Centralized Key Management (CCKM)如何工作在LWAPP/CAPWAP环境

里？

A. 在最初的客户端关联时，AP或WLC协商一把成对地万能密钥(PMK)，在无线客户端通过802.1x认证后。WLC或WDS AP缓存每个客户端的PMK。当无线客户端重新关联或漫游时，它跳过802.1x认证并且立即验证PMK。

WLC的唯一的特殊实施在CCKM的是WLCs交换客户端PMK通过移动性信息包，例如UDP 16666。

Q. 如何设在无线局域网控制器(WLC)和轻量级接入点(膝部)的双工设置？

A. Cisco无线产品工作良好，当速度和双工自动交涉时，但是您有设的选项在WLC和膝部的双工设置。为了设AP速度/双工设置，您能配置膝部的双工设置在控制器，反之，然后推进他们对膝部。

配置ap以太网双工<auto/half/full>速度<auto/10/100/1000> <all/Cisco AP Name>是命令通过CLI设双工设置。此命令用仅版本4.1和以上支持。

为了设WLC物理接口的双工设置，请使用**设置端口physicalmode {全部|端口} {100h|100f|10h|10f}**命令。

此命令设置指定或专用的10 Mbps或100 Mbps，半双工或者全双工操作的所有前面板10/100BASE-T以太网端口。注意您必须禁用与**disable命令设置端口的autoneg**的自动协商，在您手工配置在端口前的所有物理模式。并且，请注意**autoneg命令设置的端口**改写设置做用**设置端口physicalmode**命令。默认情况下，所有端口设置为自动协商。

Note: 没有办法更改在光纤端口的速度设置。

Q. 有没有方式跟踪轻量级接入点(LAP)的名字，当没有注册到控制器时？

A. 如果您的AP完全地下来和没有注册到控制器，没有办法您能通过控制器跟踪LAP。唯一方法是您能访问这些保持的APs被连接的交换机和您能找到他们被联系的连接孔使用此命令，：

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

这产生您在此AP被连接的交换机的端口号。然后，请发出此命令：

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

此命令的输出也给予LAP名字。然而，当您的AP被加电并且被连接到交换机时，此方法只是可能的。

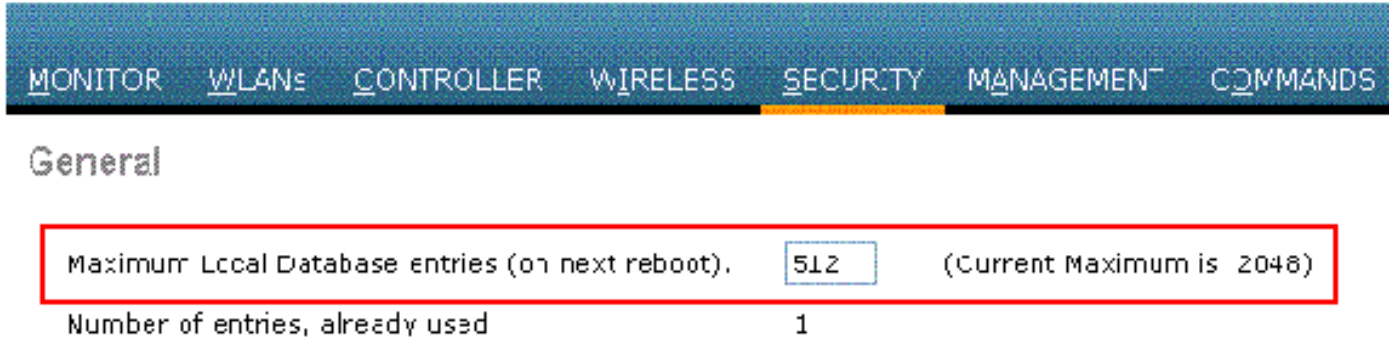
Q. 我配置了我的控制器的512个用户。有没有任何方式增加用户的数量无线局域网控制器的(WLC)？

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，(包括客人身份的用户)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：

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

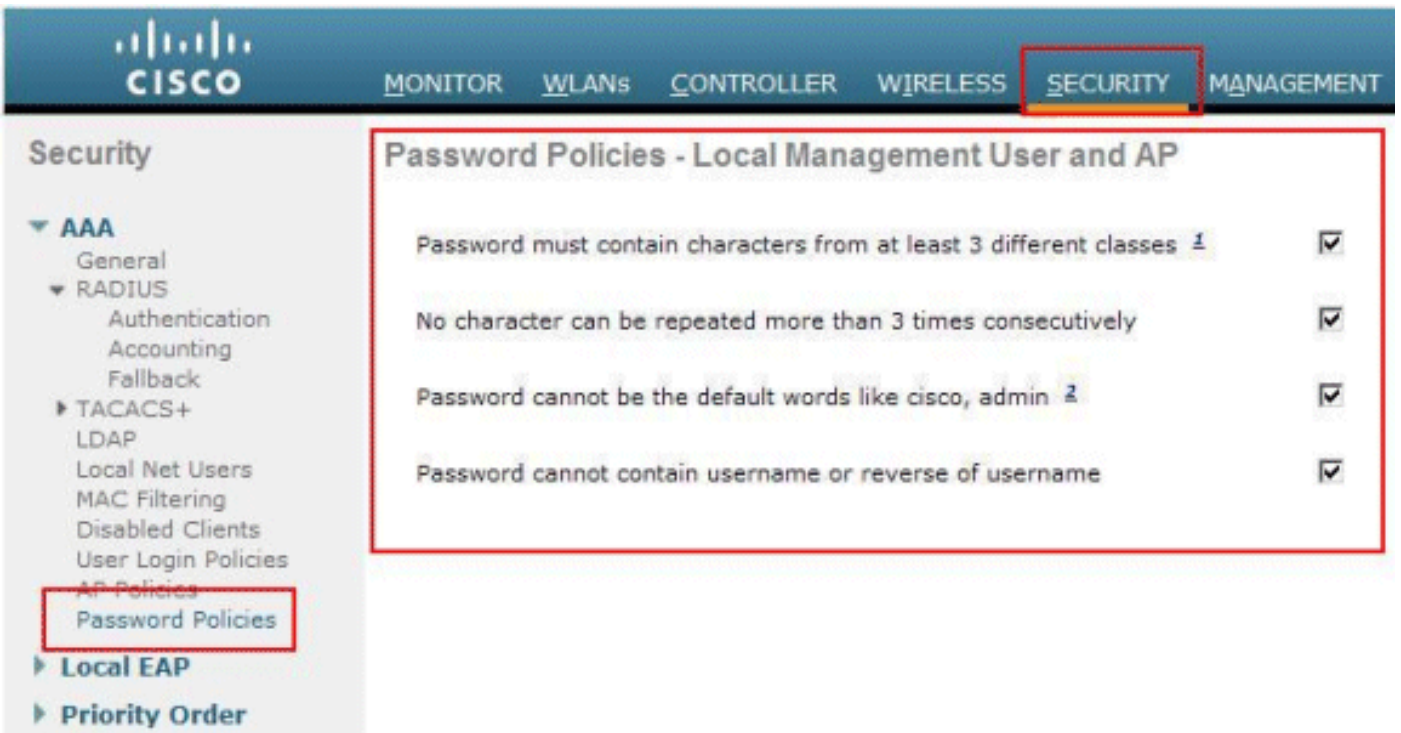
Note: 您必须保存配置和重置系统(使用reset system命令)为了更改能生效。



Q. 如何强制执行由于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严格pwd {案例检查/连续检查/默认值检查/用户名检查/全检查} {enable (event)}功能失效命令：

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

- **案例检查**-检查同样的出现时间 字符连续三次。
- **连续检查**-是否检查默认值或 使用其变形。
- **默认值检查**-是否检查或者用户名或其 使用反向。
- **全检查**-启用/禁用所有严格 密码检查。

Q. 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 配置有静态IP地址。这些客户端不传输任何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。当接受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 不知道哪里找出客户端。
- 电池操作的设备的功率例如移动电话和打印机 因为他们不必须回应每个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 工作情况不允许ARP请求转移到被动客户端。Any 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enable (event) ARP请求和回应是 交换在配线之间和无线客户端。此功能，当启用，允许控制器通过从配线的ARP请求对无线客户端直到 期望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 Cisco 无线局域网控制器配置指南，版本7.0.116.0。](#)

Q. 如何请能|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，会话超时参数被配置在1800秒 在再验证前发生。

更改此值到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WLANs菜单。它显示WLANs列表 在WLC配置。点击客户端属于的WLAN。去 **高级选项卡**。和您查找*Enable (event)*会话 超时参数。更改DEFAULT值到180，并且点击 要使更改发挥作用适用。

当发送在Access-Accept，与终止行动值一起 RADIUS请求，Session-timeout属性指定最大数量 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ReAuthPeriod恒定在内再验证802.1X计时器状态机。

Q. 我有一客户隧道，在IP (EoIP)隧道的以太网，被配置 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。能此锚点WLC今后子网广播通过 从有线网络的EoIP隧道到与产生关联的无线客户端 远程控制器？

A. 不，WLC4400不转送从有线的IP子网广播 支持给在EoIP隧道间的无线客户端。这不是支持的功能。Cisco不支持子网广播隧道也不组播 访客访问拓扑。因为客户WLAN强制客户端Point of Presence 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。

Q. 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？QoS如何实现在WLC？

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

- 白金/voice
- 金子/视频
- 银/尽力(默认值)
- 铜牌服务/背景

您能配置语音流量WLAN使用白金QoS，分配 使用古铜色QoS和分配其他数据流的低带宽WLAN之间 其他QoS级别。请参阅 [分配对-WLAN的QoS配置文件](#)欲知更多信息。

Q. 是Linksys支持以太网网桥Cisco无线统一 解决方案？

A. 不，WLC支持Cisco仅WGB产品。Linksys WGBs不是 支持。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：

- 只连接一个设备到WET54G或WET11B。
- Enable (event)克隆在WET54G或WET11B的MAC功能克隆 连接的设备。
- 在设备上安装最新的驱动程序和固件被连接到 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。

Note: 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被尝试。

Q. 如何我请存储配置文件在无线局域网控制器 (WLC)？

A. WLC包含两内存：

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

当您配置操作系统在WLC时，您修改 可变的RAM。您必须从中可变的RAM拯救配置到 NVRAM为了确信，在当前配置的WLC重新启动。

知道是重要的哪内存您修改，当您实行时 这些任务：

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

功能FAQ

Q. 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)工具和我获得“不支持的EAP”输入 日志。

A. 没有在WLC的单独的EAP键入设置。轻的EAP (LEAP)，EAP灵活的认证通过获取建立隧道 (EAP-FAST)，或者Microsoft 保护的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。

通过在的GUI完成这些步骤为了enable (event) EAP WLC :

1. 从WLC GUI, 请点击 **WLANs**。
2. 在WLC的配置列表发表。点击WLAN。
3. 在**WLANs > Edit**, 请点击 **安全**选项。
4. 点击第**2层**, 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EAP认证信息包在之间 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, 已经配置得认证服务器全局。关于如何的信息 enable (event)在WLCs的EAP选项通过命令行界面(CLI), 参考对 [使用 配置RADIUS的CLI](#) 部分 [Cisco 无线局域网控制器配置指南, 版本 7.0.116.0](#)。

Q. 快速的SSID更改什么 ?

A. 快速SSID更改允许客户端移动在Ssid之间。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 连接表, 在客户端被添加到新前, 控制器清除 SSID。当快速SSID更改是失效的时, 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, 是指 [配置 快速SSID更改](#) 部分 [Cisco 无线局域网控制器配置指南, 版本7.0.116.0](#)。

Q. 能定在能连接到无线客户端的数量的一限制 LAN ?

A. 您能定限制为能连接到a客户端的数量 WLAN, 是有用的在方案您有客户端的有限数量 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 客户端的最大数量每WLAN](#) [Cisco 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。

Q. 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代表积极的关键缓存。它设计了作为扩展名 对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无充分漫游 与AAA服务器的再验证。为了首先了解PKC, 您需要了解关键缓存。

关键缓存是被添加到WPA2的功能。这允许移动 驻防缓存万能密钥(成对地万能密钥[PMK])它通过 a获取 与接入点(AP)的成功的验证, 和在a**重新使用它 与同样AP的将来关联**。这意味着特定移动 设备需要一次验证与特定AP, 并且缓存键为 未来使用。关键缓存通过叫作PMK标识的机制被处理 (PMKID), 是PMK、字符串、位置和MAC的哈希 AP的地址。PMKID独特识别PMK。

与关键缓存, 一个无线位置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, 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以前获取了的位置重新使用PMK 成功的验证进程。这排除对位置的需要 当漫游时, 请验证新的APs。

所以, 在漫游的内部控制器, 当一个移动设备移动 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搜索其PMK高速缓冲存储器确定 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。

默认情况下PKC启用WPA2。所以，当您enable (event) WPA2 在WLC的WLAN配置的下第2层安全， PKC在被启用 WLC。并且，请配置AAA服务器和无线客户端适当的EAP的 认证。

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 漫游的环境。

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

Q. 什么是这些超时设置的解释在控制器：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。

用户空闲超时：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搬走。

Note: 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 与WLC的会话。在此时间之后，WLC DE验证客户端，和 客户端通过再整个认证(再验证)进程。这是转动加密密钥的安全预防措施的部分。如果您 以密钥管理使用一个可扩展的认证协议(EAP)方法， 键变更发生在每个固定的间隔为了派生新的加密 键。没有密钥管理，此超时值是无线的的时间 客户端需要执行一个充分的再验证。会话超时是特定的 WLAN。此参数可以从WLANs被获取> **Edit**菜单。

Q. 什么是RFID系统？标记Cisco当前支持什么RFID ？

A. 射频识别(RFID)是使用无线电的技术 相当短程通信的频率通信。一基本的RFID 系统由RFID标记、RFID读者和处理软件组成。

目前Cisco支持从AeroScout和Pango的RFID标记。更多 关于如何的信息配置AeroScout标记，是指 [WLC AeroScout RFID标记的配置](#)。

Q. 可进行EAP验证本地在WLC ？有其中任一 描述解释此本地EAP功能？

A. 是， EAP验证在WLC可以进行本地。本地EAP 是允许用户和无线客户端是的认证方法 本地验证在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，或者外部认证服务器断开。当您 enable (event)本地EAP， WLC担当认证服务器。更多 关于如何的信息请配置本地EAP快速的认证的一WLC，参考 对 [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](#)。

Q. 有何WLAN覆盖功能？如何配置此功能？当他们失效对备份时，膝部维护 WLAN覆盖值 WLC ？

A. WLAN覆盖功能enable (event)选择WLANs的我们从在中 在能积极地使用根据一个单个LAP基本类型的WLC的配置。完成这些步骤为了配置WLAN覆盖：

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的名字您的右侧 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被配置所有WLANs的列表 出现。
6. 从此列表，请检查您希望的**WLANs** 出现在LAP，并且点击**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，APs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。

Note: 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被去除了。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配置并且播放所有 WLANs。您能指定仅某一WLANs传输，如果配置 接入点组。每接入点通告仅启用WLANs那属于其接入点组。

Note: 接入点组没有enable (event) WLANs传输每 AP无线接口。

Q. 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。不支持本地IPv6技术支持。

为了在WLC的enable (event) IPv6，检查**IPv6** 在WLAN SSID配置的**Enable**复选框在WLAN下> Edit页。

并且，以太网要求组播模式(EMM)支持IPv6。如果您 禁用EMM，使用IPv6丢失连接的客户端设备。为了enable (event) 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**。此enable (event)在单播模式下组播或者或 组播模式。当组播被启用作为组播单播时，信息包是 复制为每个AP。这可以是密集的处理，因此请使用它以 注意。组播启用，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 (APs)。

Note: 2006个控制器不支持IPv6。

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

Q. 执行Cisco 2000系列无线局域网控制器(WLC)支持Web 客人身份的用户的认证 ?

A. 所有Cisco WLCs支持Web认证。Web认证 是用于的第3层认证方法验证有简单的用户 认证证书。加密不是包含的。完成这些步骤 订购对enable (event)此功能：

1. 从GUI，请点击**WLAN** 菜单。
2. 点击**WLAN**。
3. 去**安全**选项并且选择层 **3**。
4. 检查**Web策略**机箱并且选择 **认证**。
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**净用户，和完成这些动作：定义客户的客户用户名和密码能使用 登录的命令。这些值区分大小写。选择您使用的WLAN ID。**Note:** 关于详细配置，请参见 [无线 LAN控制器Web身份验证配置示例](#)。

Q. WLC能管理在无线模式下 ?

A. 一旦是启用的，WLC可以通过无线模式管理。更多 关于对enable (event)无线模式如何的信息是指 [启用 对GUI和CLI的无线连接](#) 部分 [Cisco 无线局域网控制器配置指南，版本7.0.116.0](#)。

Q. 什么是链路聚合(滞后) ? 如何在无线局域网的enable (event)滞后 控制器(WLCs) ?

A. 滞后捆绑在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的接口有多个参数产生关联与它，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一个物理端口，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，接口动态地被映射对下个可用的物理端口，并且膝部是平衡在端口间。

当滞后在WLC时被启用，WLC传送在同样的数据帧 他们被接受的端口。WLC依靠邻居交换机在EtherChannel间的负载均衡数据流。WLC不执行其中任一 EtherChannel负载平衡独自地。

Q. 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Cisco内自动地被启用 WiSM和Catalyst 3750G集成无线局域网控制器交换机。没有 滞后，在一个Cisco 4400系列控制器技术支持的每个分布式系统端口 48接入点。使用无滞后，逻辑Cisco 4402的控制器的 端口支持50接入点，Cisco 4404控制器的逻辑端口 支持100接入点和逻辑端口在Catalyst 3750G 集成无线局域网控制器交换机和在每个Cisco WiSM控制器 支持150接入点。

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

Q. 什么是在统一的无线的自动锚点移动性功能 网络 ?

A. 自动锚点移动性(或客户WLAN移动性)用于改进负荷 漫游的客户端的平衡和安全您的无线LAN的(WLANs)。下面 正常漫游的情况，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个不同的子网，客户端漫游的控制器设置的一次外国会话 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。

Note: 不能为第3层移动性配置移动性锚点。移动性锚点仅使用客户隧道。

Q. 能Cisco 2006无线局域网控制器(WLC)被配置作为锚点 WLAN ?

A. 一Cisco 2000系列WLC不可能被选定作为WLAN的一个锚点。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。

Q. 无线局域网控制器使用什么类型移动性建立隧道 ?

A. 控制器软件版本4.1通过5.1技术支持不对称的两个 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 默认值。

在不对称的隧道，对有线网络的客户端的流量路由 直接地通过外国控制器。不对称的隧道中断，当上游路由器安排反向路径过滤(RPF)被启用。在这种情况下，因为RPF检查保证的那客户端的流量下降在路由器 回到源地址的路径匹配信息包来的路径。

当对称移动性建立隧道是启用的时，所有客户端的流量是发送到锚点控制器，并且能顺利地然后通过RPF检查。在这些情况下对称移动性建立隧道也是有用的：

- 如果客户端信息包路径的防火墙安装丢弃信息包 因为IP原地址不匹配的子网信息包 被接受，这是有用的。
- 如果在锚点控制器的访问点的组VLAN是不同的 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，数据流在不正确VLAN可以被发送 事件。

Q. 如何我们访问WLC，当网络是时 下来？

A. 当网络发生故障时，WLC可以由服务端口获取。此端口分配在一个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 [Cisco 无线局域网控制器配置指南，版本7.0.116.0](#)。

Q. 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加入对被配置的主要的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。参考 [WLAN 控制器故障切换轻量级接入点配置示例](#)。

Q. 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，作为名字暗示，您能允许客户端 到/从一个特定IP地址的数据流在客户端以前验证。当曾经外部Web服务器Web认证，某些WLC时 平台需要外部Web服务器的(Cisco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不是必须的。然而，它是一种好习惯 当曾经时，请配置外部Web服务器的预验证ACL 外部Web认证。

Q. 我有一MAC被过滤的WLAN和一完全地开放WLAN在我的网络。默认情况下客户端是否选择开放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被配置的所有WLAN to connect。在MAC过滤器的界面选择产生能力适用对WLAN或接口的过滤器。如果多个WLANs附加对 同样接口，您能应用MAC过滤器于接口，不需要 创建每单个WLAN的一台过滤器。

Q. 如何能配置管理用户的TACACS认证的 无线局域网控制器(WLC)？

A. 起源于WLC版本4.1，WLCs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。

Q. 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. 此设置是其中一个客户端排除策略。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。

有此额外的Web认证失败策略功能，当a 失败的Web认证尝试的客户编号超过5，控制器 考虑客户端超出了Web最大尝试 认证和列入黑名单客户端。

完成这些步骤为了enable (event)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认证 故障。

Q. 我转换了我的自治接入点(AP)成轻量级模式。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RADIUS认为根据 被关联的AP的MAC地址对该WLC而不是IP地址的 WLC？

A. 是，这可以执行与WLC边配置。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日志验证此。在那里，显示的您能看到被叫站ID字段 特定的客户端是关联的AP的MAC地址。

Q. 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(APs)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。

这些命令可以用于更改WPA握手超时：

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

默认值继续反射WLCs当前 工作情况。

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

Note: 在IOS APs，此设置与dot11是可配置的 WPA握手命令。

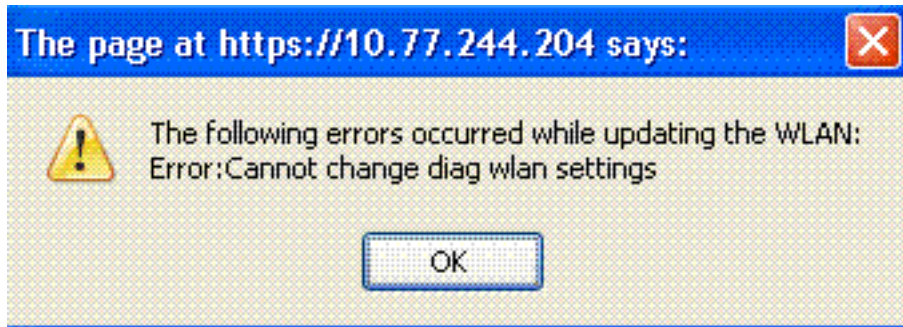
您能用下选项也配置其他EAP参数 设置先进的eap命令。

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

Q. 什么是诊断的信道功能的目的是在WLAN的 > 编辑>Advanced页？

A. 诊断的信道功能enable (event)排除问题故障的您 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试 困难客户端经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 控制器GUI或CLI对enable (event)诊断的信道和您能使用 运行诊断测试的控制器CLI或WCS。

诊断的信道可以用于只测试。如果尝试 用诊断的信道配置认证或加密WLAN的 启用，您看到此错误：



Q. 什么是的AP组的最大数量在WLC可以被配置？

A. 此列表显示AP组的最大数量您能配置 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、Cisco WiSM和Cisco 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

Related Information

- [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](#)
- [Cisco 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技术支持](#)
- [无线 产品技术支持](#)
- [技术支持和 文档 - Cisco Systems](#)

本文档是否是有用？[有](#) [没有](#)

感谢您的反馈。

[打开支持案例](#)（需要[思科服务合同](#)。）

相关的思科支持社区讨论

[Cisco支持公共](#)是为您一个论坛询问和应答问题，共用建议，和 与您的对等体合作。

有关本文档中所用的规则信息，请参阅 [Cisco Technical Tips Conventions](#)。

已更新：2015年3月02日

文档ID118833