查看无线局域网控制器 (WLC) 设计和功能常见问题解答

目录

WLC功能常见问题

相关信息

简介

SSHv1

本文档介绍有关无线局域网控制器设计和功能的最新信息。

先决条件

要求

本文档没有任何特定的要求。

组件使用

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您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。

WLC设计常见问题解答

问：如何配置交换机以连接WLC？

A.将WLC连接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，请参阅为WLC配置交换机。

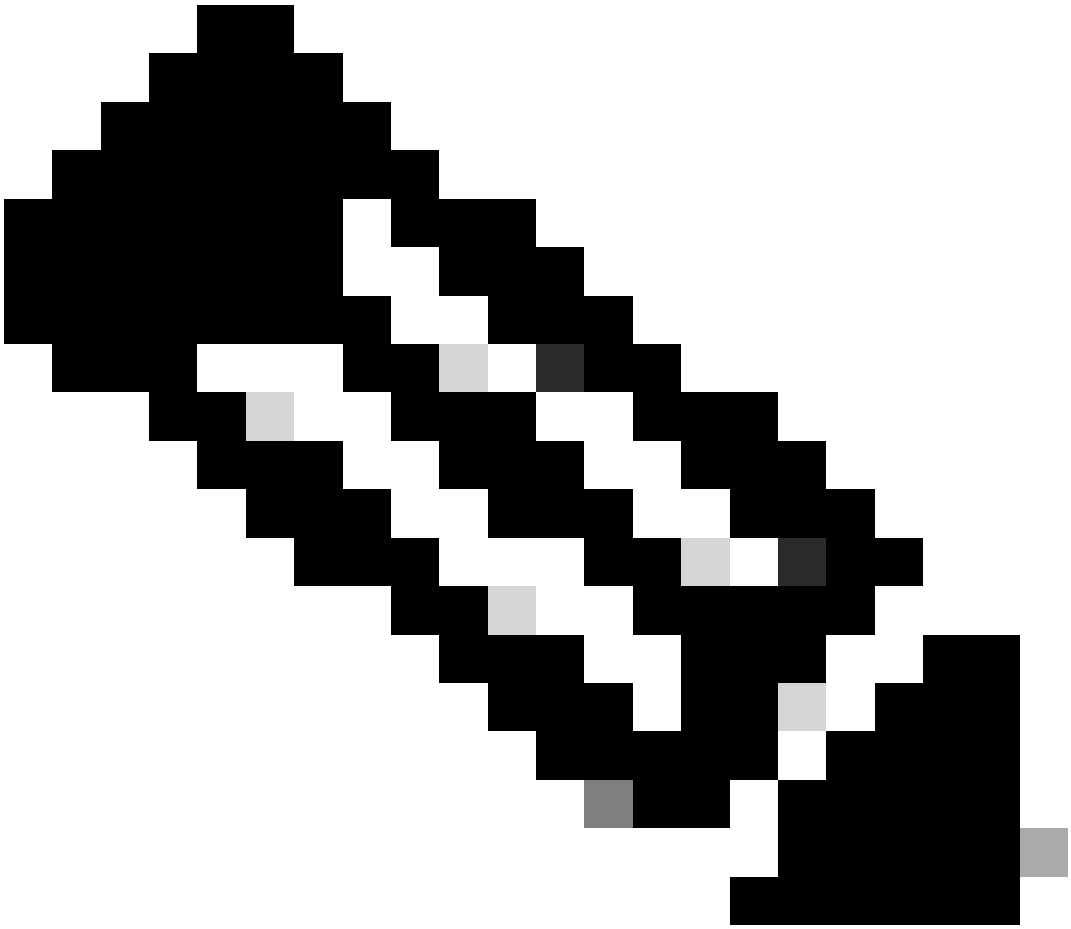
问： 当接入点 (AP) 在控制器中注册后，与 WLAN 客户端之间的所有网络往来流量是否都要通过无线 LAN 控制器 (WLC) 进行隧道传输？

答：当AP加入WLC时，会在两台设备之间形成无线接入点控制和配置协议(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。

问： 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？

答：可以，WLC可以通过WAN与AP连接。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。

问： 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模式下，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《FlexConnect无线分支机构控制器部署指南》。

问： 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。

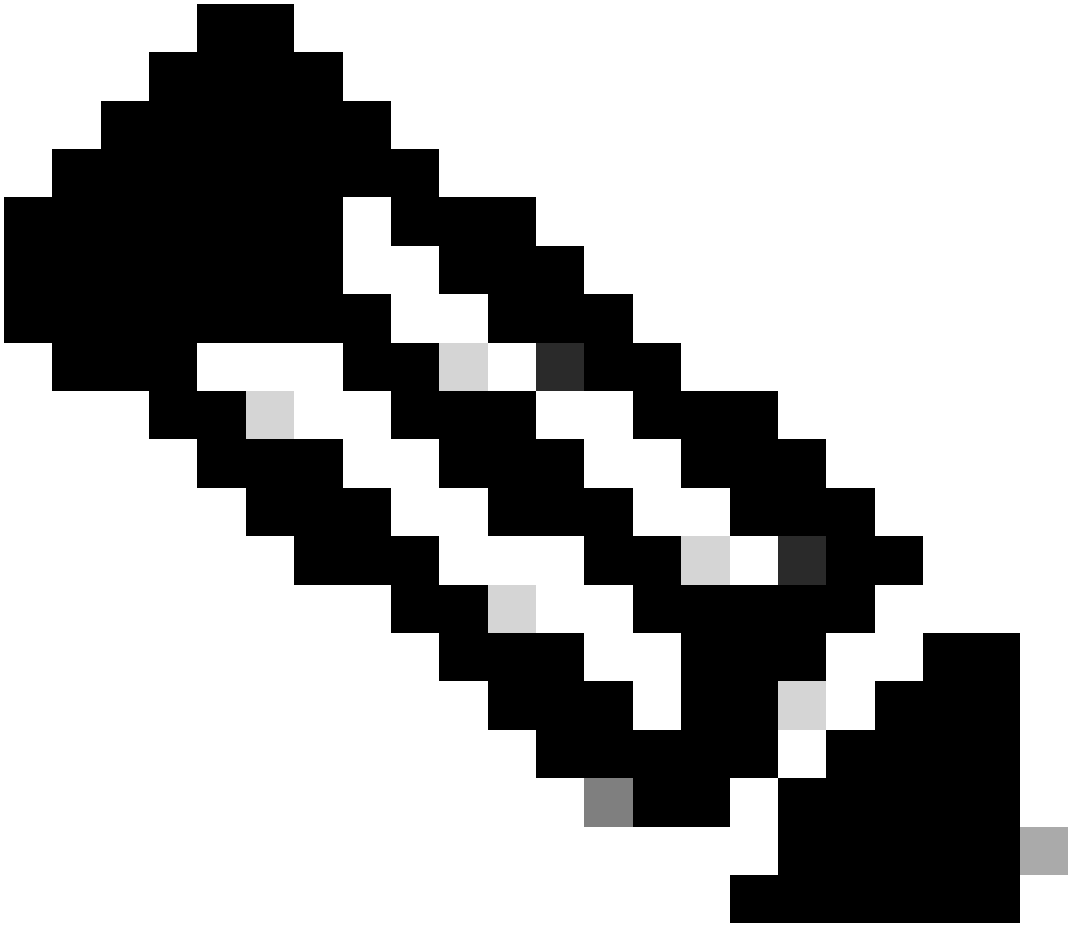
另一个主要区别是，在 REAP 模式中，数据流量只能进行本地桥接，而不能交换回中心办公室，但在 H-REAP 模式中，您可以选择将流量交换回中心办公室。来自配置了 H-REAP 本地交换的 WLAN 的流量将进行本地交换。来自其他 WLAN 的数据流量将交换回中心办公室。

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》。

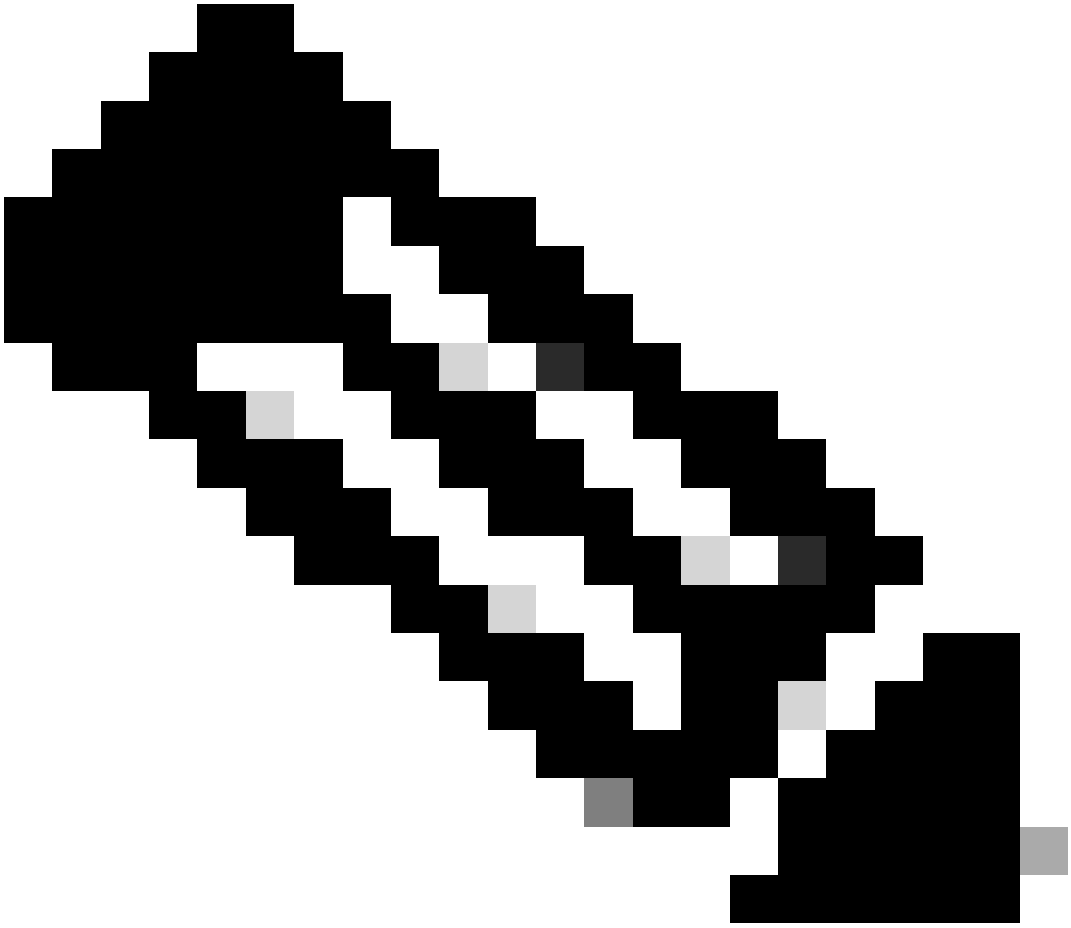
有关H-REAP的详细信息，请参阅配置混合REAP。

问： WLC 上支持多少 WLAN？

答：从软件版本5.2.157.0开始，WLC现在可以控制最多512个轻量接入点的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控制器仅支持最多16个WLAN。



注意：有关在WLC上配置WLAN的指南的详细信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版中的创建WLAN部分。

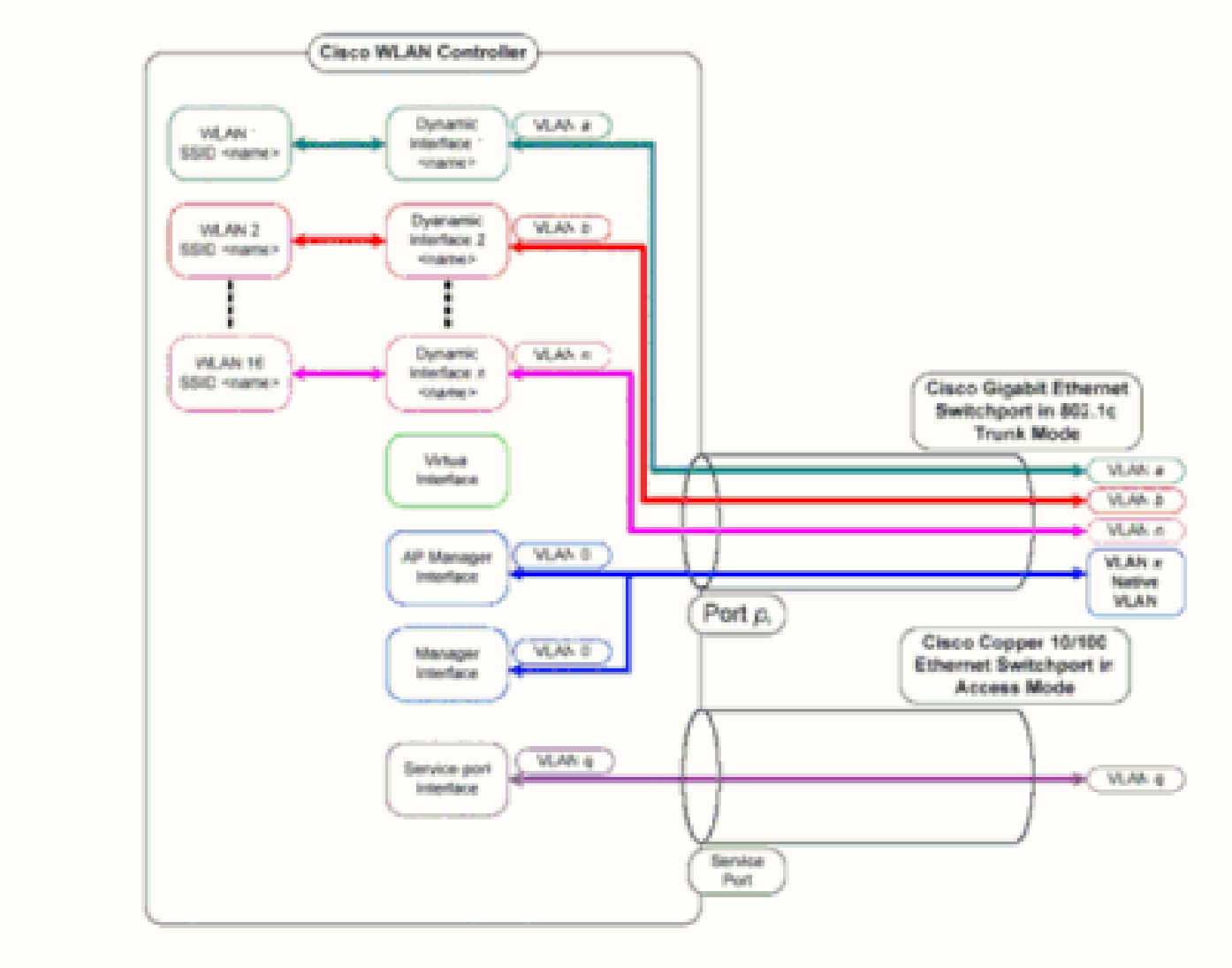
问： 我如何在我的无线局域网控制器 (WLC) 上配置 VLAN？

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。

问： 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，但我们尚未调配中继端口以允许使用我们的 WLAN 所使用的 VLAN。 无线接入点 (AP) 是否会使用管理接口 VLAN 为数据包添加标签？

A.AP不使用管理接口VLAN标记数据包。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：



问： WLC 的哪个 IP 地址用于 AAA 服务器的认证？

A.WLC将管理接口的IP地址用于任何涉及AAA服务器的身份验证机制（第2层或第3层）。有关WLC上的端口和接口的详细信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版的配置端口和接口部分。

问： 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

部分

问： 2100 系列无线局域网控制器 (WLC) 不支持哪些功能？

答： 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
- 尖晶石
- 要塞
- 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

问： 5500 系列控制器不支持哪些功能？

答： 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：对于5500系列控制器，不需要配置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（例如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

问： 网状网络不支持哪些功能？

A.网状网络不支持以下控制器功能：

- 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

问： 无线局域网控制器上的制造商安装证书(MIC)和轻量AP证书的有效期是多少？

A.WLC上MIC的有效期为10年。从创建开始，轻量AP证书(无论是MIC证书还是自签名证书(SSC))的有效期相同，均为10年。

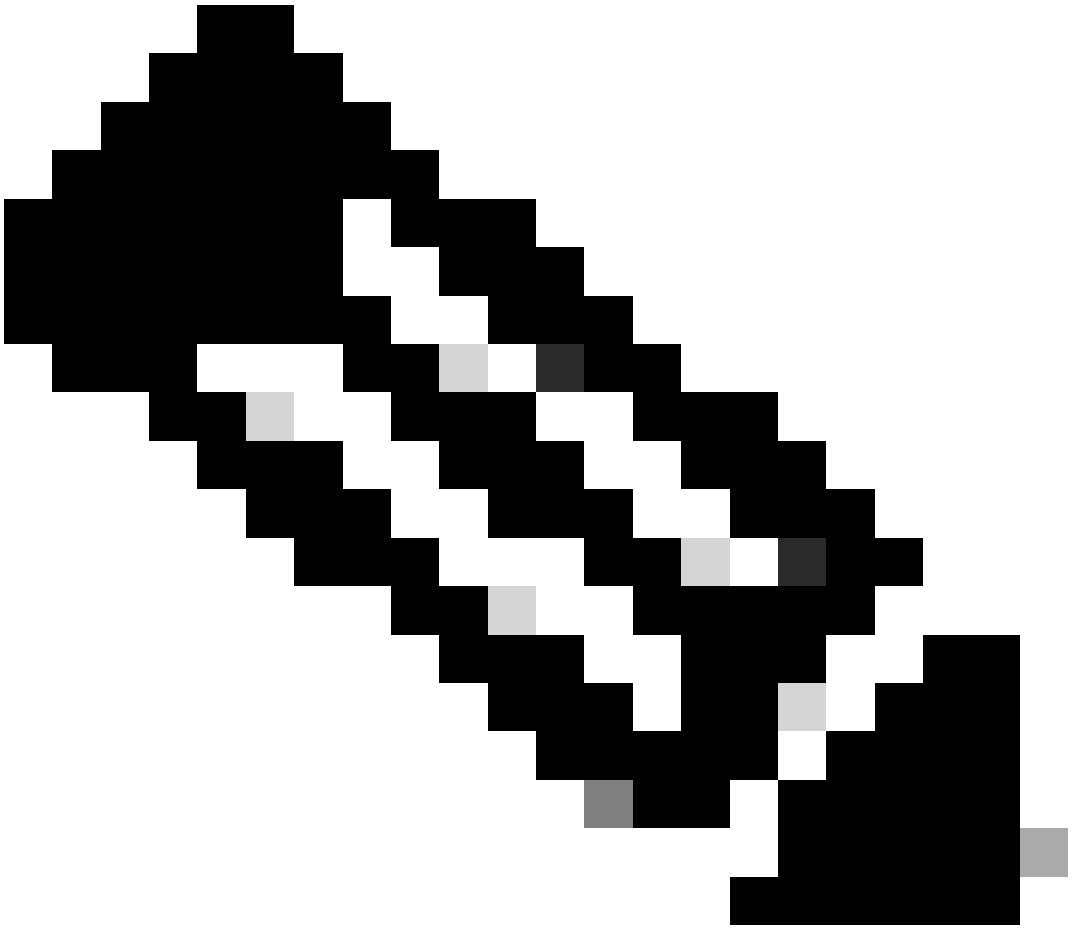
问： 我在相同的移动组中为故障切换配置了两个无线局域网控制器 (WLC)，分别名为 WLC1 和 WLC2。我的轻量接入点 (LAP) 当前注册在 WLC1 中。如果 WLC1 发生故障，注册到 WLC1 的 AP 在切换到备用 WLC (WLC2) 期间是否要重新启动？此外，在此故障切换期间，WLAN 客户端是否会丢失与 LAP 的 WLAN 连接？

A.是。如果WLC1发生故障，LAP将从WLC1取消注册并重新启动，然后向WLC2重新注册。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。

问： 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，客户端漫游必须能够正常工作。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：只有Cisco 410x和440x系列WLC以及Cisco 1000系列接入点支持第2层模式。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。

问： 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？

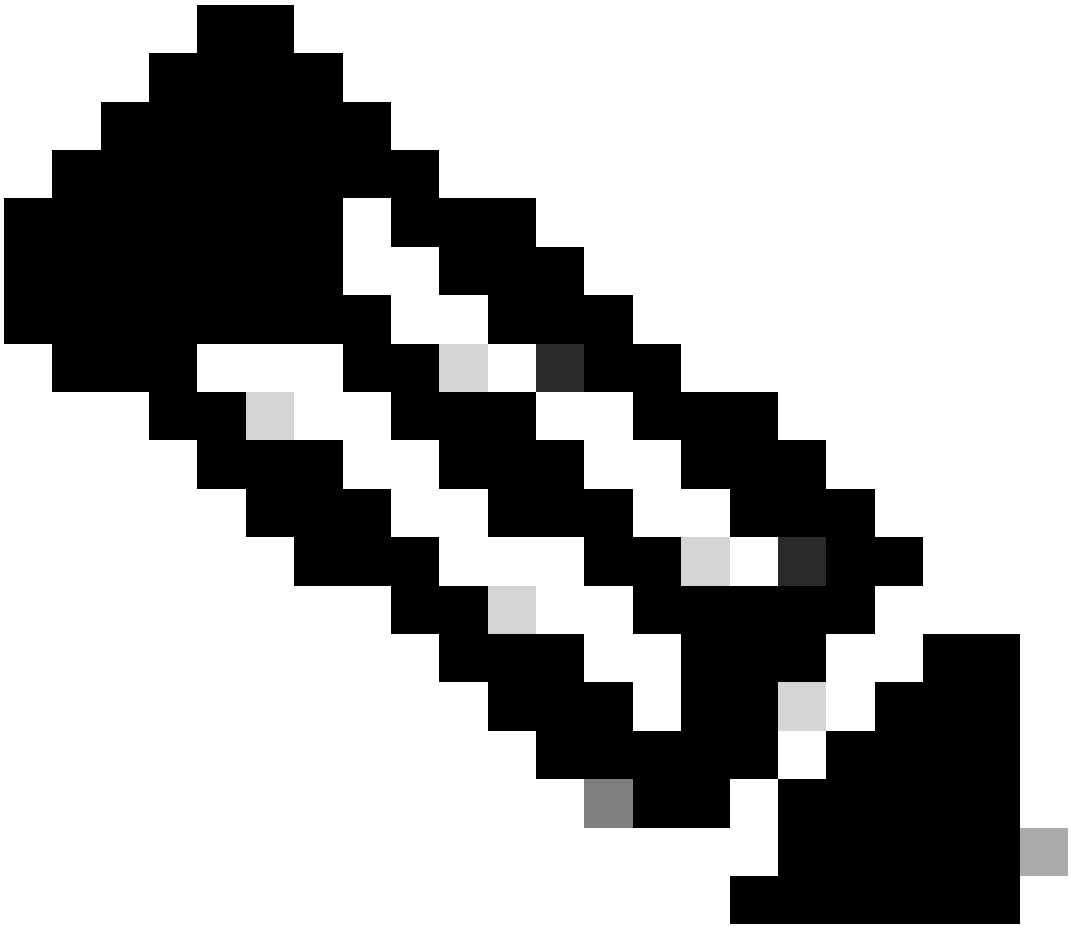
A.这是客户端漫游到新AP时所发生的一系列事件：

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通过移动消息以有关客户端的信息做出响应，例如MAC地址、IP地址、QoS、安全情景等。

4. WLC使用提供的客户端详细信息更新其数据库；然后，如有必要，客户端完成重新身份验证过程。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。



注意：无线客户端在重新关联期间不发出(802.11)身份验证请求。无线客户端只会直接发出重新关联请求。然后，它可以通过802.1x身份验证。

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

A.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

问： 无线局域网控制器是否同时支持 SSHv1 和 SSHv2？

答：无线局域网控制器仅支持SSHv2。

问： 无线局域网控制器 (WLC) 是否支持反向 ARP (RARP)？

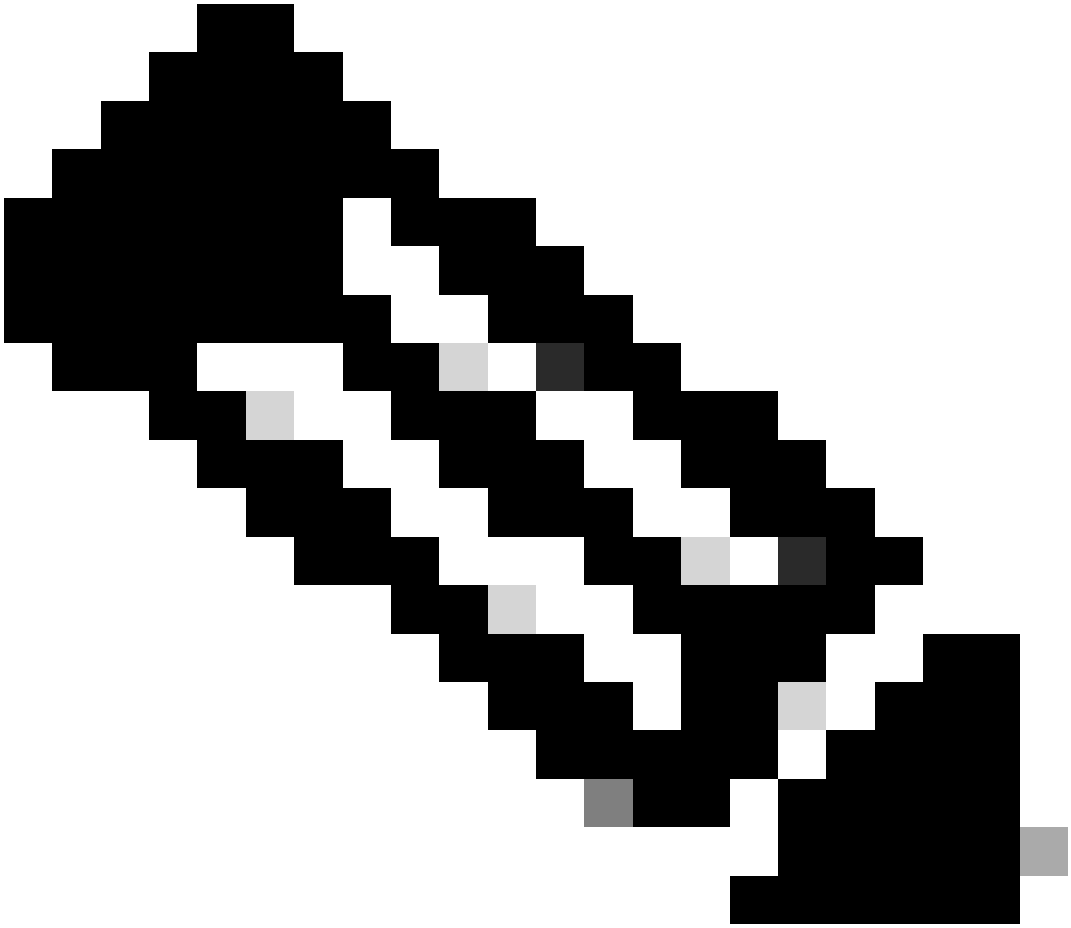
A.反向地址解析协议(RARP)是一种链路层协议，用于获取给定链路层地址（如以太网地址）的IP地址。具有固件版本 4.0.217.0 或更高固件版本的 WLC 支持 RARP。任何更早的版本都不支持 RARP。

问： 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。有关如何在WLC上配置DHCP范围的详细信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版的配置DHCP部分。

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：除非LAP直接连接到WLC，否则4.0之前的WLC固件版本不支持LAP的DHCP服务。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。

问： WLAN 下的 DHCP Required 字段有何用处？

A.DHCP Required是可为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。

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

答：在初始客户端关联期间，无线客户端通过802.1x身份验证后，AP或WLC将协商成对主密钥(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。

问： 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？

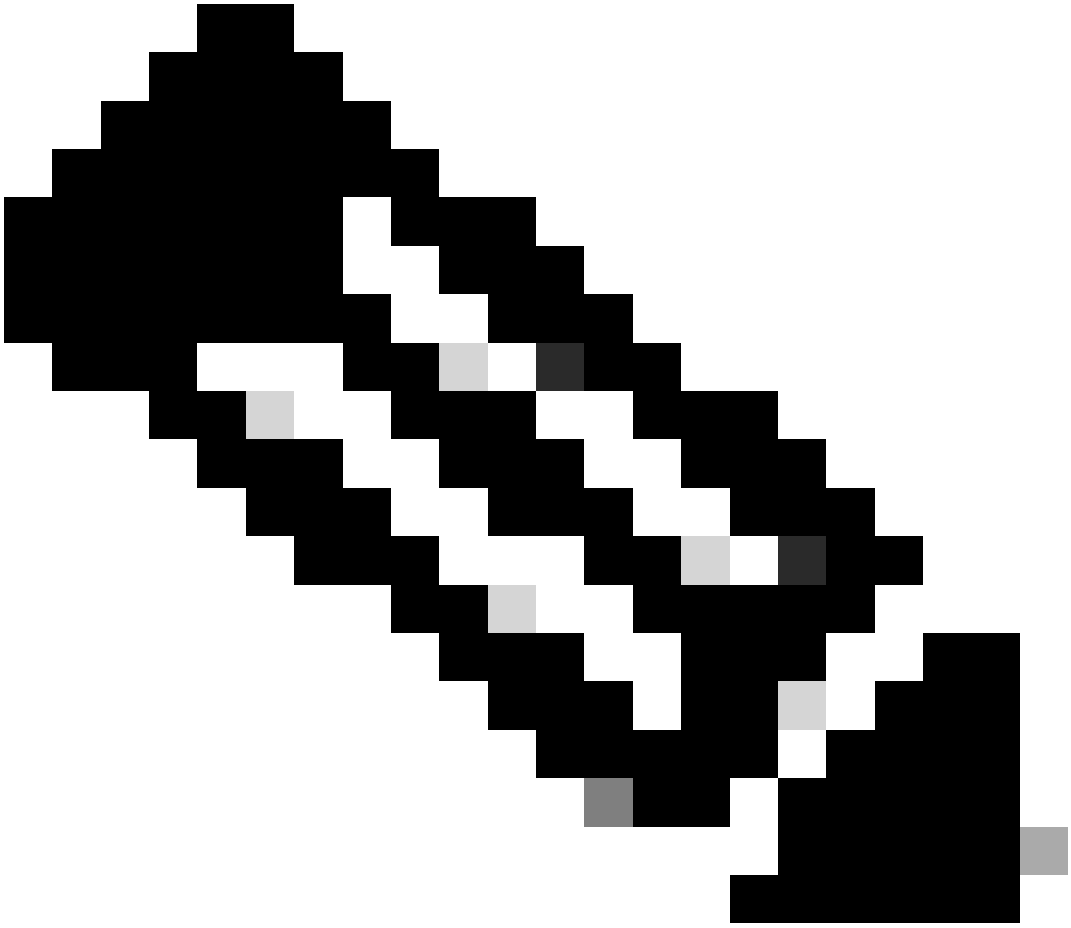
答：当速度和双工都自动协商时，Cisco无线产品效果最佳，但您可以选择在WLC和LAP上设置双工设置。要设定 AP 速度/双工设置，您可以在控制器上为 LAP 配置双工设置，然后再将其应用于 LAP。

配置ap以太网双工<auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name>

是通过CLI设置双工设置的命令。此命令仅在4.1版及更高版本中受支持。

要为WLC物理接口设置双工设置，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：无法更改光纤端口的速度设置。

问： 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AP已完全关闭并且未注册到控制器，您将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：

```
<#root>
```

```
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：

```
<#root>
```

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

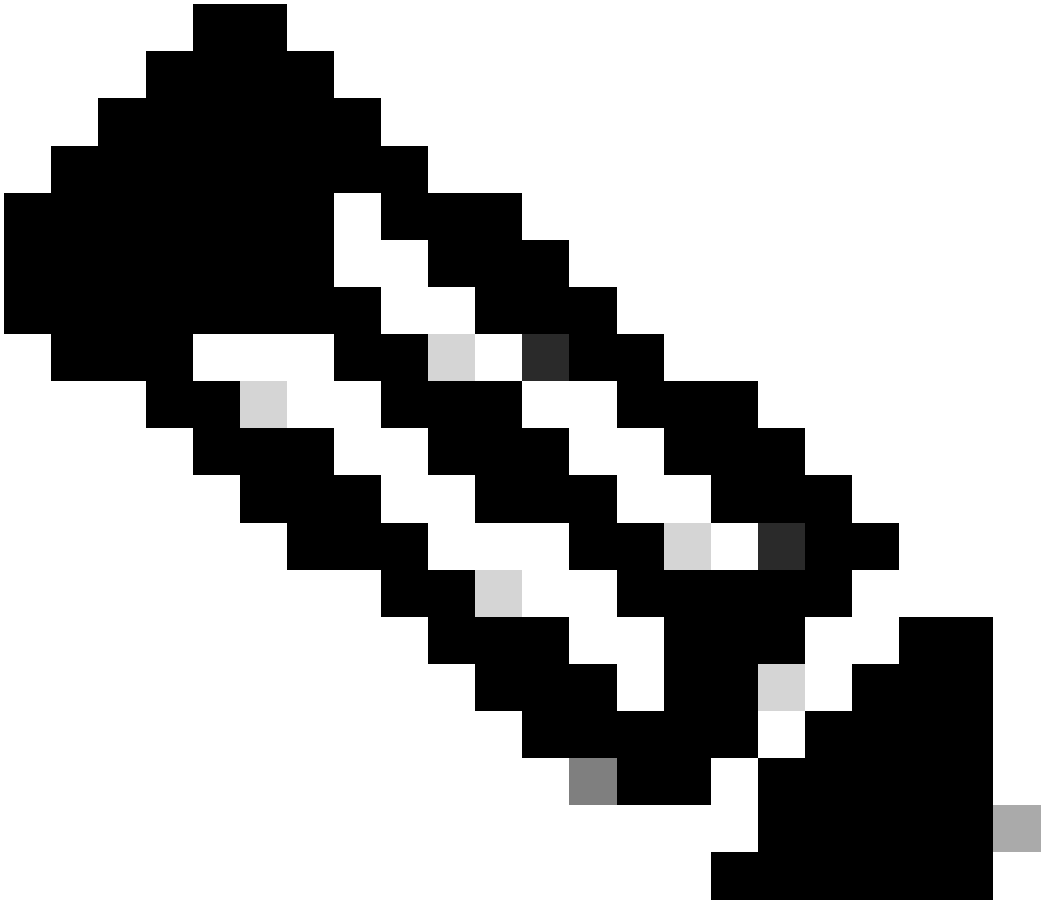
此命令的输出还会提供 LAP 名称。但是，这种方法仅在您的 AP 已通电且连接到交换机时才是可行的。

问： 我在我的控制器上配置了 512 个用户。是否有方法增加无线局域网控制器 (WLC) 上的用户数？

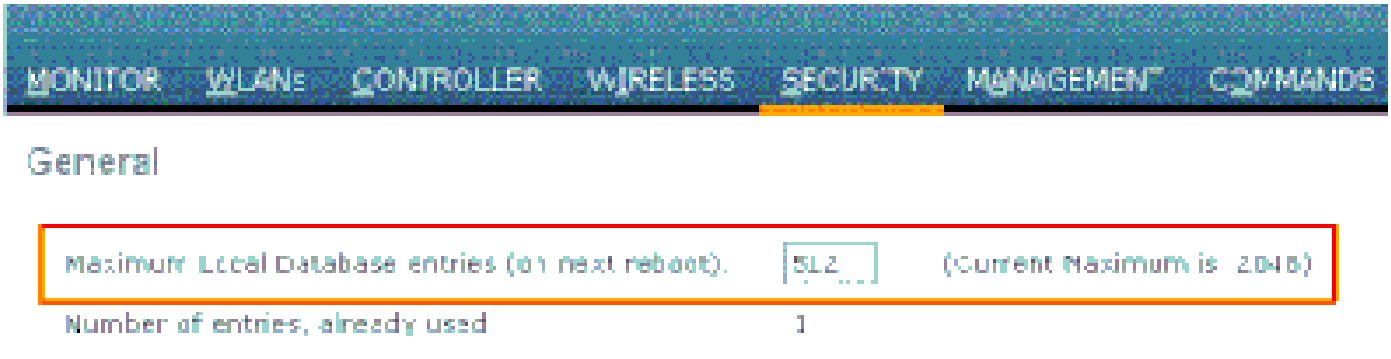
A.本地用户数据库在**Security** > **General**页面上的条目数量最多为2048个。此数据库由本地管理用户（包括接待大使）、网络用户（包括访客用户）、MAC过滤器条目、接入点授权列表条目和排除列表条目共享。所有这些类型的用户总共不能超过已配置的数据库大小。

要增加本地数据库，请从CLI使用以下命令：

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



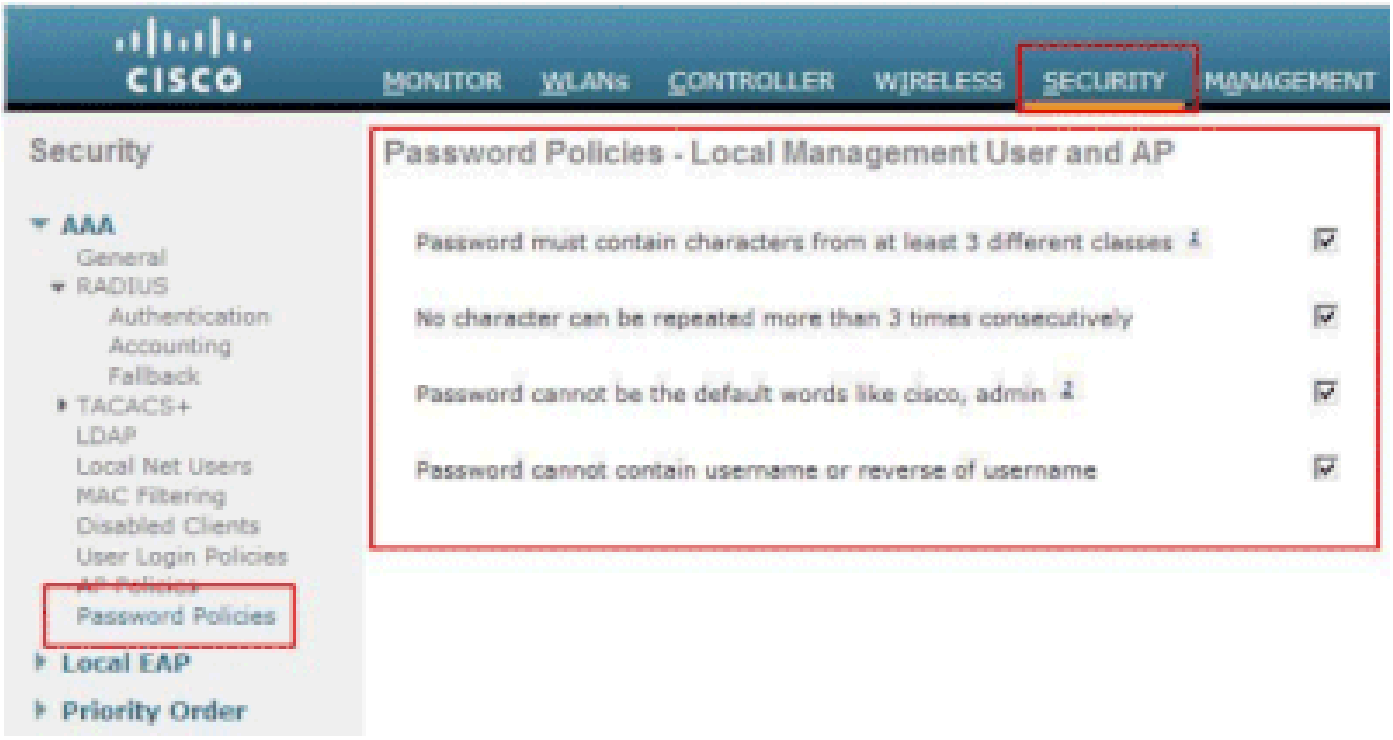
注意：您必须保存配置并重置系统（使用reset system命令），以使更改生效。



问： 如何在WLC上实施强密码策略？

A.WLC允许您定义强密码策略。这可以使用CLI或GUI完成。

在GUI中，转至**Security** > **AAA** > **Password Policies**。此页面包含一系列选项，可以选择这些选项来实施强密码。例如：



问： 如何在无线局域网控制器上使用被动客户端功能？

答：被动客户端是配置了静态IP地址的无线设备，如刻度尺和打印机。当这些客户端与接入点关联时，它们不会传输任何IP信息，例如IP地址、子网掩码和网关信息。因此，当使用被动客户端时，除非使用DHCP，否则控制器永远不会知道IP地址。

WLC当前充当ARP请求的代理。收到ARP请求后，控制器将以ARP响应做出响应，而不是直接将请求传递给客户端。此方案有两个优势：

- 向客户端发出ARP请求的上游设备无法知道客户端的位置。
-

电池供电设备（例如移动电话和打印机）的电源得到保留，因为它们不必响应每个ARP请求。

由于无线控制器没有任何有关被动客户端的IP相关信息，因此它无法响应任何ARP请求。当前行为不允许将ARP请求传输到被动客户端。任何尝试访问被动客户端的应用都可能失败。

通过被动客户端功能，可以在有线和无线客户端之间交换ARP请求和响应。启用此功能后，控制器可以将ARP请求从有线客户端传递到无线客户端，直到所需的无线客户端进入RUN状态。

有关如何配置被动客户端功能的信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版中使用GUI配置被动客户端部分。

问： 如何能将客户端设置为每隔三分钟或按任意指定时间间隔向 RADIUS 服务器重新进行认证？

A.可以使用WLC上的会话超时参数完成此操作。默认情况下，会话超时参数配置为 1800 秒，之后将重新进行认证。

将此值更改为 180 秒即可在三分钟后要求客户端重新进行认证。

要访问会话超时参数，请单击 GUI 中的 WLANs 菜单。这将显示 WLC 中配置的 WLAN 的列表。单击客户端所属的 WLAN。转到 **Advanced< span>** 选项卡并找到*Enable Session* Timeoutparameter。将默认值更改为 180，并单击 Apply 以使更改生效。

当在 Access-Accept 中发送并伴随一个 RADIUS-Request 的 Termination-Action 值时，Session-Timeout 属性将指定在重新进行认证之前提供服务的最大秒数。在这种情况下，Session-Timeout 属性用于在 802.1X Reauthentication Timer 状态机内载入 ReAuthPeriod 常量。

问： 我在充当锚点 WLC 的 4400 无线局域网控制器 (WLC) 和若干远程 WLC 之间配置了一个访客隧道 Ethernet over IP (EoIP) 隧道。此锚点 WLC 能否通过 EoIP 隧道将子网广播从有线网络转发到与远程控制器关联的无线客户端？

答：不，WLC 4400不会通过EoIP隧道将IP子网广播从有线端转发到无线客户端。不支持该功能。Cisco 不支持访客接入拓扑中的子网广播或组播的隧道传输。因为访客 WLAN 会将客户端入网点强制确定为网络中一个非常特定的位置，并且多数情况下位于防火墙之外，因此子网广播的隧道传输可能会导致安全问题。

问： 在无线 LAN 控制器 (WLC) 和轻量接入点协议 (LWAPP) 的设置过程中，要为语音流量传递哪些差分服务代码点 (DSCP) 值？如何在 WLC 上实现 QoS？

答：思科统一无线网络(UWN)解决方案WLAN支持四个级别的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

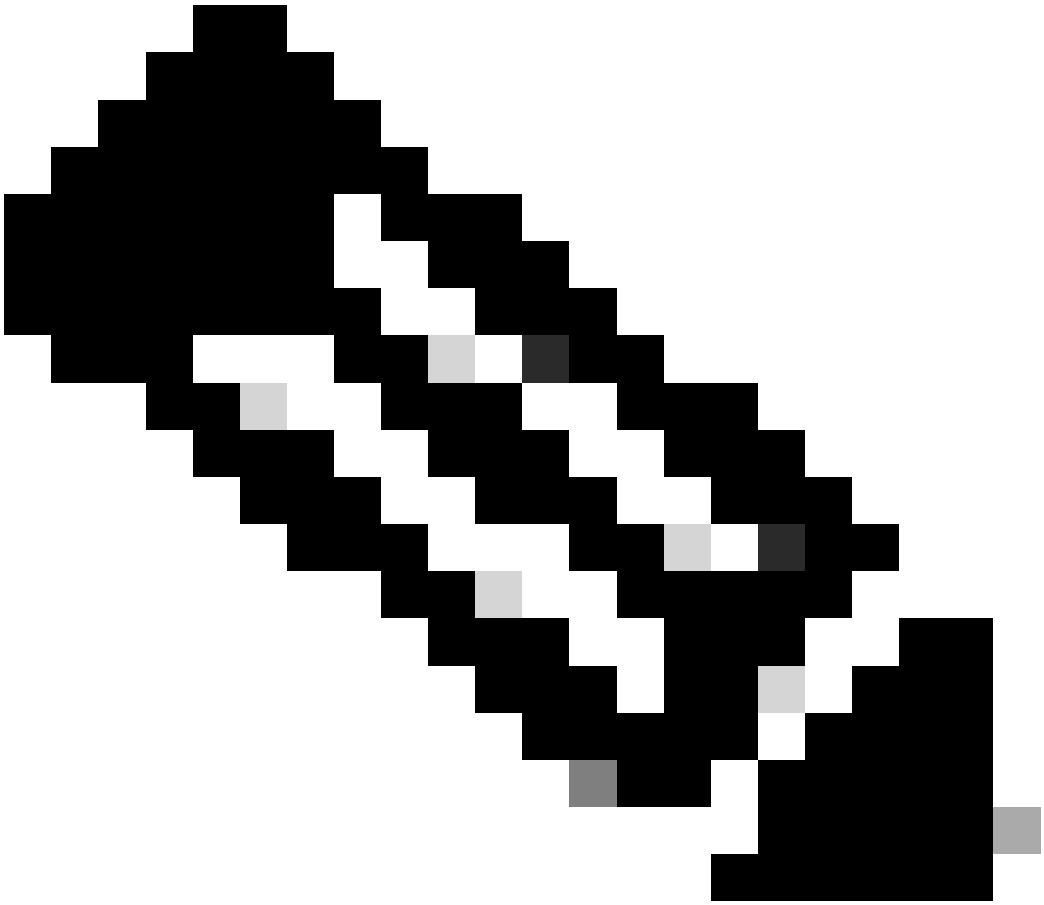
您可以将语音流量 WLAN 配置为使用白金服务 QoS，指定低带宽 WLAN 使用铜牌服务 QoS，并为所有其他流量指定其他 QoS 级别。有关详细信息，请参阅将QoS配置文件分配到WLAN。

问：Cisco无线统一解决方案是否支持Linksys以太网网桥？

答：不，WLC仅支持Cisco WGB产品。不支持 Linksys WGB。虽然 Cisco 无线统一解决方案不支持 Linksys WET54G 和 WET11B 以太网桥，但如果遵循以下原则，则可以在无线统一解决方案配置中使用这些设备：

- 只将一个设备连接到 WET54G 或 WET11B。

- 在 WET54G 或 WET11B 上启用 MAC 克隆功能以克隆连接的设备。
- 在连接到 WET54G 或 WET11B 的设备上安装最新的驱动程序和固件。该原则对于 JetDirect 打印机尤为重要，因为早期的固件版本会导致 DHCP 问题。



注意：不支持其他第三方网桥。您也可以针对其他第三方网桥尝试这里所述的步骤。

问： 如何在无线 LAN 控制器 (WLC) 上存储配置文件？

A. WLC包含两种内存：

- 易失性 RAM — 保存当前活动的控制器配置
- 非易失性 RAM (NVRAM) — 保存重新启动配置

当您在 WLC 中配置操作系统时，就是在修改易失性 RAM。您必须将易失性 RAM 中的配置保存到 NVRAM 中，以确保 WLC 使用当前的配置重新启动。

在执行以下任务时，了解您正在修改哪种内存非常重要：

- 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。

WLC功能常见问题

问：如何在无线局域网控制器(WLC)上设置可扩展身份验证协议(EAP)类型？我想要认证访问控制服务器 (ACS) 设备，但在日志中得到“unsupported EAP”类型。

A. WLC上没有单独的EAP类型设置。对于轻量 EAP (LEAP)、EAP Flexible Authentication via Secure Tunneling (EAP-FAST) 或 Microsoft Protected EAP (MS-PEAP)，只需配置 IEEE 802.1x 或 Wi-Fi Protected Access (WPA)（如果您使用 WPA 与 802.1x）。RADIUS 后端和客户端上支持的任何 EAP 类型都是通过 802.1x 标记支持的。客户端和 RADIUS 服务器上的 EAP 设置必须匹配。

要在 WLC 上通过 GUI 启用 EAP，请完成以下步骤：

1. 在 WLC GUI 中，单击 WLANs。
2. 这将显示 WLC 中配置的 WLAN 的列表。单击某个 WLAN。
3. 在 WLANs > Edit 中，单击 **Security** 选项卡。
4. 单击**Layer 2**并选择Layer 2 Security作为802.1x或WPA+WPA2。您还可以在同一窗口中配置所提供的 802.1x 参数。然后，WLC 将在无线客户端和认证服务器之间转发 EAP 认证数据包。
5. 单击 AAA 服务器并从此 WLAN 的下拉菜单中选择认证服务器。我们假定已经以全局方式配置了认证服务器。

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。当客户端针对某个不同的 SSID 发送一个新关联时，系统将清除控制器连接表中的相应客户端条目，然后再将客户端添加到新 SSID 中。禁用快速 SSID 更改时，控制器将强制执行一个延迟，然后才允许客户端移动到新 SSID 中。有关如何启用快速SSID更改的信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版的配置快速SSID更改部分。

问： 我能否对可以连接到无线LAN的客户端数量设置一个限制？

答：您可以设置可连接到WLAN的客户端数量的限制，这在可连接到控制器的客户端数量有限的情况下非常有用。每个WLAN可以配置的客户端数量取决于您使用的平台。

有关无线局域网控制器不同平台的每个WLAN的客户端限制的信息，请参阅Cisco无线局域网控制器配置指南7.0.116.0版中的配置每个WLAN的最大客户端数量部分。

问： 什么是 PKC？它如何与无线局域网控制器 (WLC) 一起工作？

A. PKC代表主动密钥缓存。它是作为对 802.11i IEEE 标准的扩展设计的。

PKC是Cisco 2006/410x/440x系列控制器中启用的一种功能，它允许正确配置的WireleTalk与Tech Writer联系。ss客户端漫游时无需使用AAA服务器进行完全重新身份验证。要了解 PKC，首先需要了解密钥缓存。

密钥缓存是 WPA2 中添加的功能。这允许移动站缓存它通过接入点(AP)的成功身份验证获得的主密钥（成对主密钥[PMK]），并**在将来与同一AP的关**联中重复使用它。这意味着给定移动设备需要与特定 AP 进行一次认证，然后缓存密钥以供将来使用。密钥缓存是通过一种称为 PMK 标识符 (PMKID) 的机制处理的，它是 PMK、一个字符串、站点和 AP 的 MAC 地址的哈希。PMKID 可唯一标识 PMK。

即使使用密钥缓存，无线站也必须与希望从中获取服务的每个 AP 进行认证。这会产生明显的延迟和系统开销，从而延迟传递过程，并会限制支持实时应用的能力。为解决此问题，WPA2 中引入了 PKC。

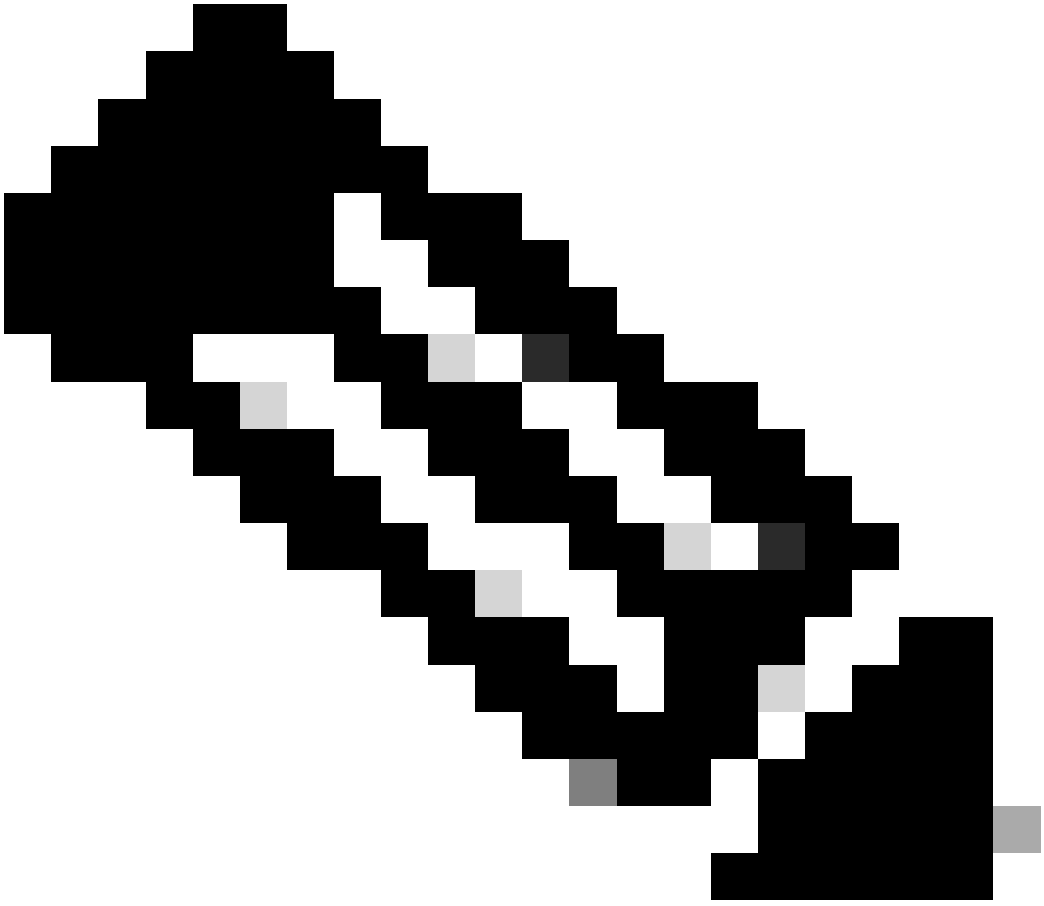
PKC 允许站点重复使用它以前通过成功的认证过程获取的 PMK。这样在漫游时，站点就无需再针对新 AP 进行认证。

因此，在控制器内的漫游中，当移动设备从一个 AP 移动到同一控制器上的另一个 AP 时，客户端会在关联过程中使用以前使用的

PMK 重新计算 PMKID 并出示它。WLC 将搜索其 PMK 缓存以确定是否有这样一个条目。如果有，则会绕过 802.1x 认证过程并立即启动 WPA2 密钥交换。如果没有，则进行标准 802.1X 认证过程。

在 WPA2 中，默认启用了 PKC。因此，当您在 WLC 的 WLAN 配置下启用 WPA2 作为 第 2 层安全时，就会在 WLC 上启用 PKC。此外，还要为 AAA 服务器和无线客户端配置适当 EAP 认证。

客户端使用的请求方还必须支持WPA2才能使PKC正常工作。在控制器间的漫游环境中也可以实现 PKC。

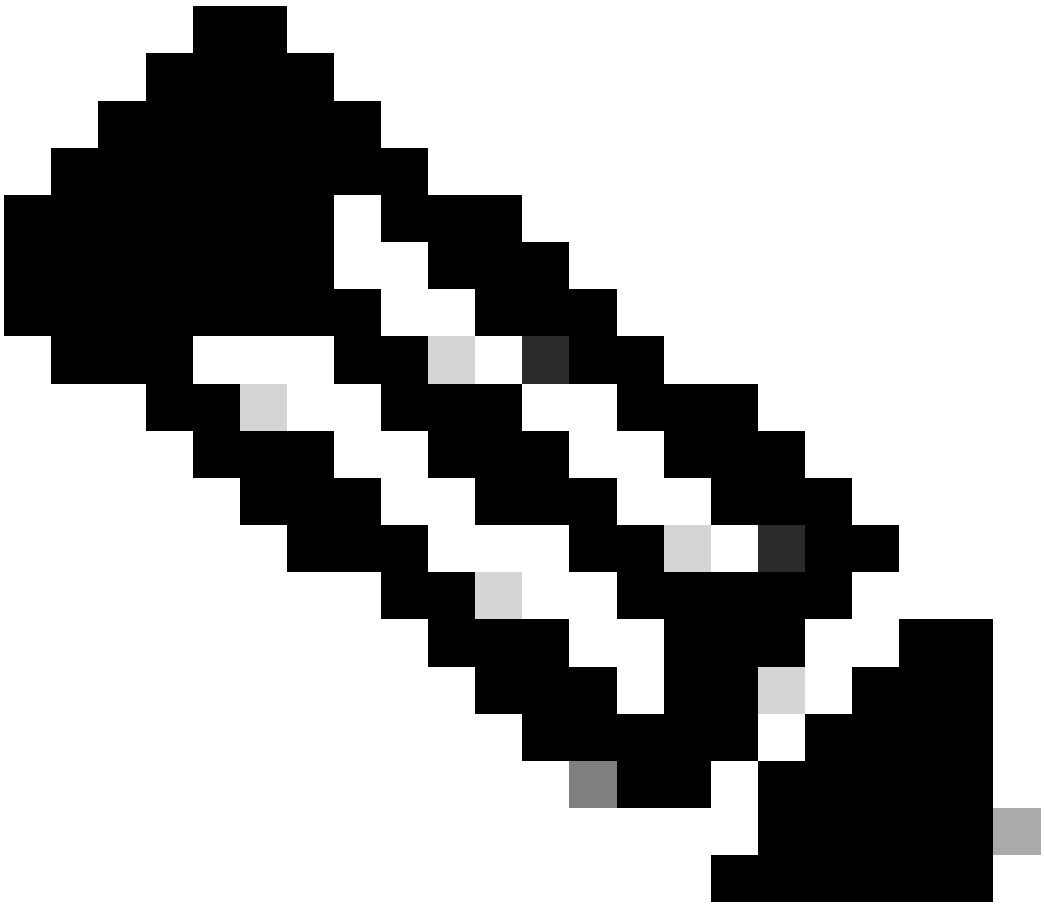


注意：PKC不能与Aironet桌面实用程序(ADU)一起作为客户端请求方。

问： 控制器上这些超时设置的解释是什么：地址解析协议(ARP)超时、用户空闲超时和会话超时？

A.ARP超时用于在WLC上删除从网络中获知的设备的ARP条目。

User Idle Timeout：当用户在设置为User Idle Timeout的时间段内未与LAP进行任何通信时，WLC将解除对客户端的身份验证。客户端必须重新进行认证并重新关联到 WLC。该设置适用于客户端可能会离开关联的 LAP 而不通知 LAP 的情况。如果客户端的电池电量耗尽或客户端关联离开，就会发生这种情况。



注意：要在WLC GUI上访问ARP Timeout和User Idle Timeout，请转到Controller菜单。选择左侧的 General 并找到 ARP Timeout 和 User Idle Timeout 字段。

Session Timeout是客户端与WLC之间的会话的最长时间。在此时间过后，WLC 将取消客户端的认证，客户端必须重新进行完整的认证（重新认证）过程。这是安全防范措施的一部分，以便轮换加密密钥。如果为密钥管理使用可扩展的认证协议 (EAP) 方法，则会定期重新计算密钥以生成新的加密密钥。如果没有密钥管理，此超时值将是无线客户端执行完全的重新认证所需的时间。会话超时是特定于 WLAN 的。可以通过**WLANs**>编辑菜单**来**访问此参数。

问： 什么是 RFID 系统？Cisco 当前支持哪些 RFID 标记？

A.射频识别(RFID)是一种使用射频通信进行较短距离通信的技术。一个基本 RFID 系统由 RFID 标记、RFID 阅读器和处理软件组成。

当前 Cisco 支持来自 AeroScout 和 Pango 的 RFID 标记。有关如何配置AeroScout标记的详细信息，请参阅《AeroScout RFID标记的WLC配置》。

问： 我能否在 WLC 上执行本地 EAP 认证？有没有解释这种本地 EAP 功能的任何文档？

A.是，可以在WLC上本地执行EAP身份验证。本地 EAP 认证方法允许用户和无线客户端在 WLC 上进行本地认证。它设计用于远程办公室，当后端系统中断或外部认证服务器停机时使其能够保持与无线客户端的连接。当您启用本地 EAP 时，WLC 将充当认证服务器。有关如何为本地 EAP-Fast 认证配置 WLC 的详细信息，请参阅《使用 EAP-FAST 和 LDAP 服务器在无线局域网控制器上配置本地 EAP 认证的示例》。

问： 什么是 WLAN 覆盖功能？如何配置此功能？当LAP故障切换到备用WLC时，LAP能否保持WLAN覆盖值？

A.WLAN覆盖功能使我们能够从在WLC上配置的WLAN中选择WLAN，这些WLAN可基于单个LAP主动使用。要配置 WLAN 覆盖，请完成以下步骤：

1. 在 WLC GUI 中，单击 Wireless 菜单。

2. 单击左侧的**Radios**选项并选择**802.11 a/n**或**802.11 b/g/n**。

3. 在右侧的下拉菜单中单击与要在其上配置 WLAN 覆盖的 AP 名称相对应的 Configure 链接。

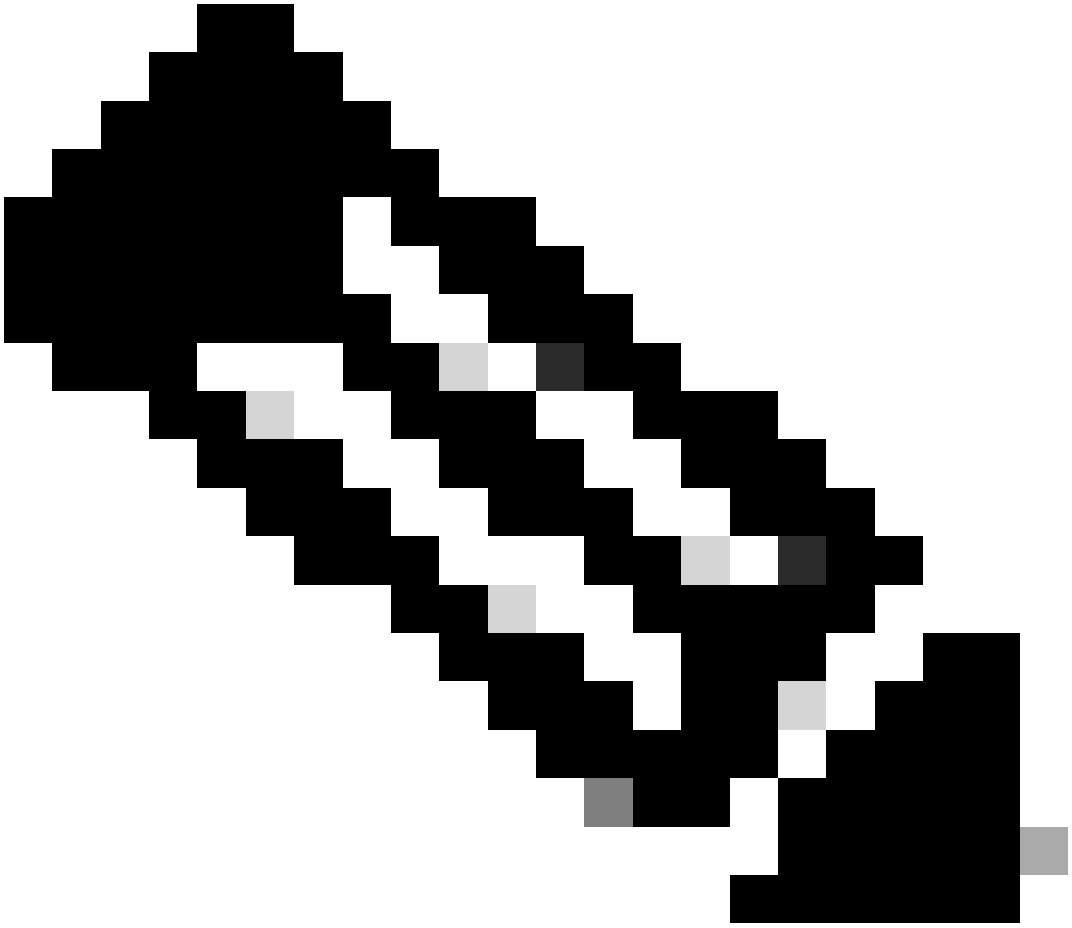
4. 从 WLAN Override 下拉菜单中选择 Enable。WLAN Override 菜单是窗口左侧的最后一项。

5. 这时将显示 WLC 上配置的所有 WLAN 的列表。

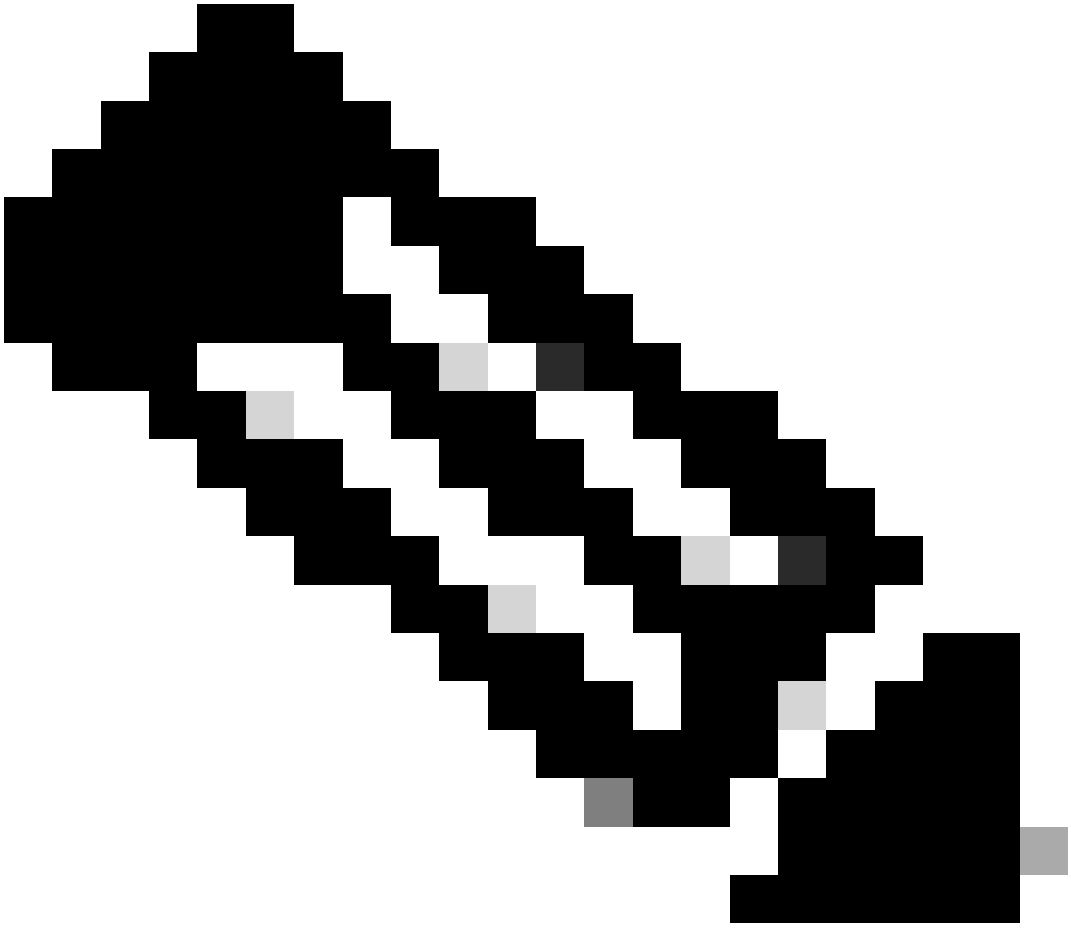
6. 在此列表中，选中希望其出现在 LAP 上的 WLAN，并单击 Apply 以使更改生效。

7. 完成更改后保存您的配置。

如果在所有 WLC 上都配置了要覆盖的 WLAN 配置文件和 SSID，则当注册到其他 WLC 时，AP 将保留 WLAN 覆盖值。



注意：在控制器软件版本5.2.157.0中，已从控制器GUI和CLI中删除WLAN覆盖功能。如果您的控制器配置了 WLAN 覆盖，并且您升级到控制器软件版本 5.2.157.0，控制器将删除 WLAN 配置并广播所有 WLAN。如果您配置接入点组，则可以指定仅传输特定 WLAN。每个接入点将仅通告属于其接入点组的启用的 WLAN。



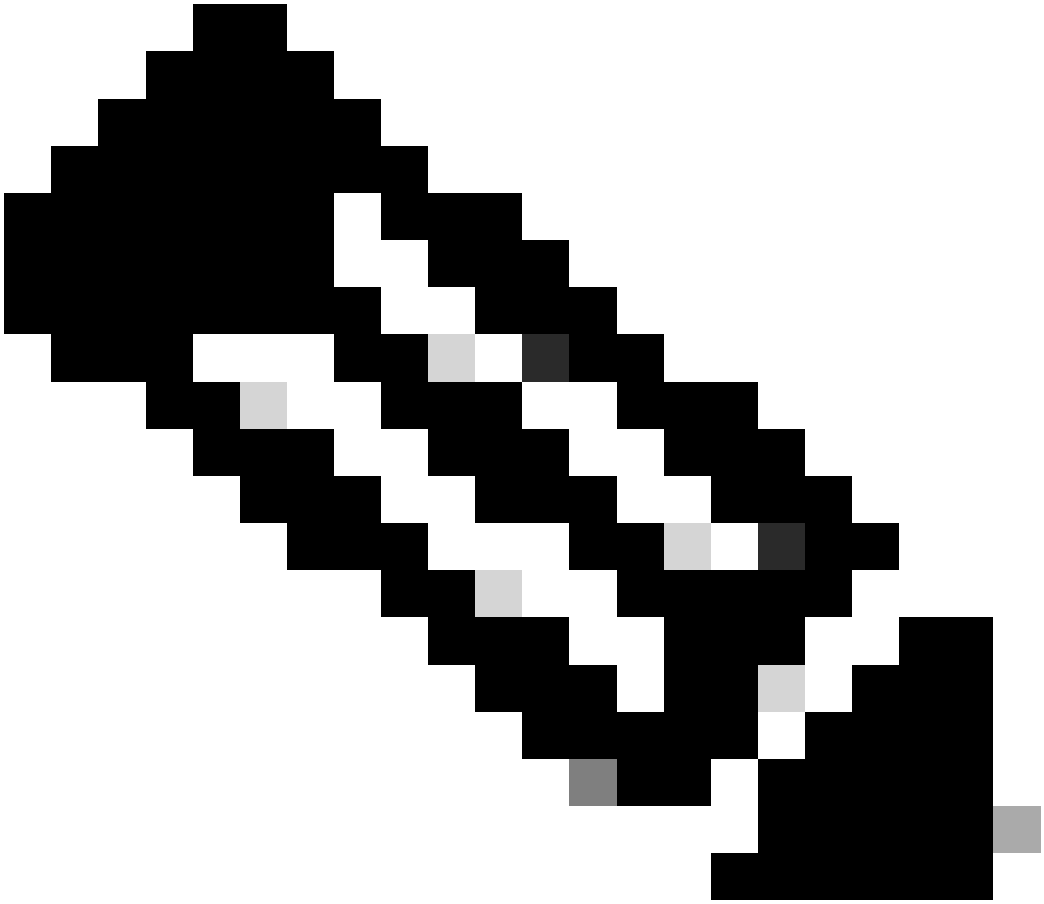
注意：接入点组不会允许在AP的每个无线电接口上传输WLAN。

问： Cisco 无线局域网控制器 (WLC) 和轻量接入点 (LAP) 是否支持 IPv6？

答：目前，4400和4100系列控制器仅支持IPv6客户端直通。尚未提供本地 IPv6 支持。

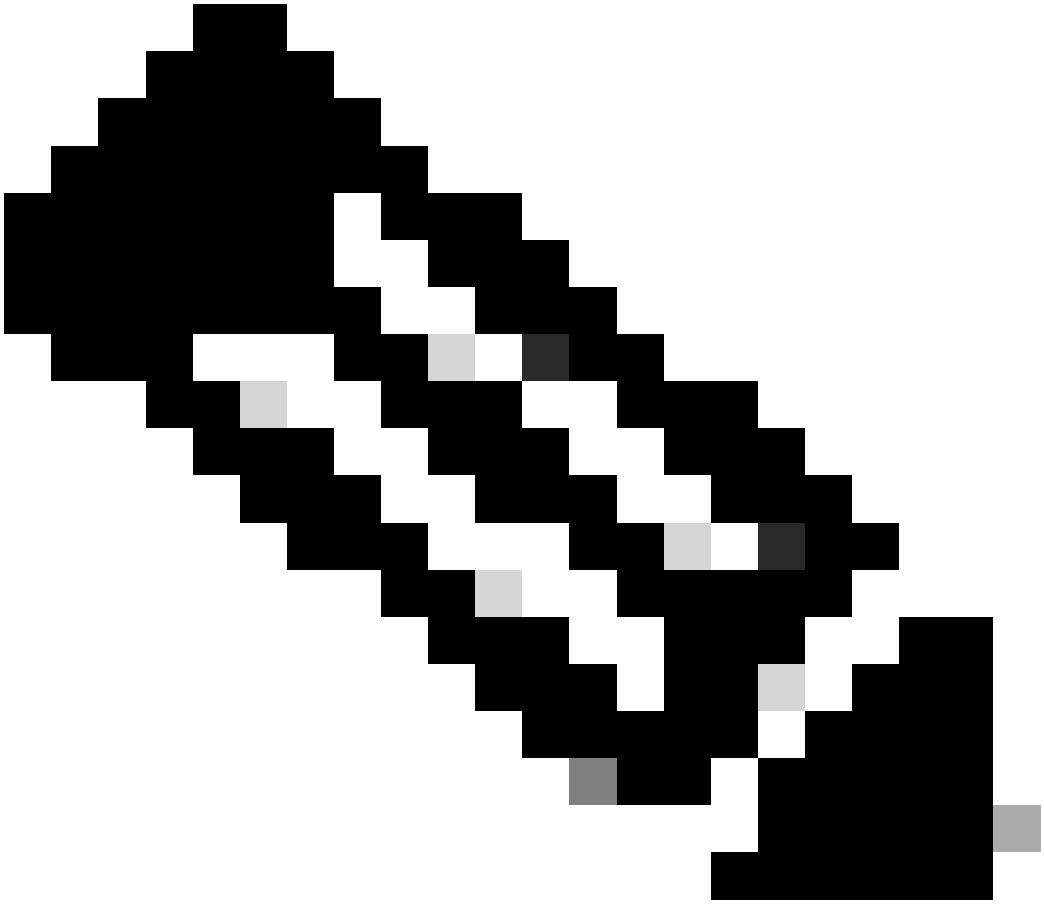
要在 WLC 上启用 IPv6，请在 WLAN > Edit 页面的 WLAN SSID 配置下选中 IPv6 Enable 复选框。

此外，还需要以太网组播模式 (EMM) 以支持 IPv6。如果禁用 EMM，使用 IPv6 的客户端设备将会失去连接。要启用 EMM，请转到 Controller > General 页面并从 Ethernet Multicast Mode 下拉菜单中选择 Unicast 或 Multicast。这将以单播模式或组播模式启用组播。当组播作为组播单播启用时，将为每个 AP 复制数据包。这会占用大量处理器，因此需谨慎使用。作为组播启用的组播将使用用户指定的组播地址向接入点 (AP) 进行更传统的组播。



注意：2006控制器不支持IPv6。

此外，当使用 AAA 覆盖功能时，一个 Bug（Cisco Bug ID CSCsg78176）会禁止使用 IPv6 穿透。



注意：只有思科注册用户才能访问内部思科工具和信息。

问： Cisco 2000 系列无线 LAN 控制器 (WLC) 是否支持访客用户的 Web 认证？

A.所有Cisco WLC都支持Web身份验证。Web 认证是第 3 层认证方法，用于使用简单认证凭据认证用户。这里不涉及加密。要启用此功能，请完成以下步骤：

1. 在 GUI 中，单击 WLAN 菜单。

2. 单击某个 **WLAN**。

3. 转到 **Security** 选项卡并选择 **Layer 3**。

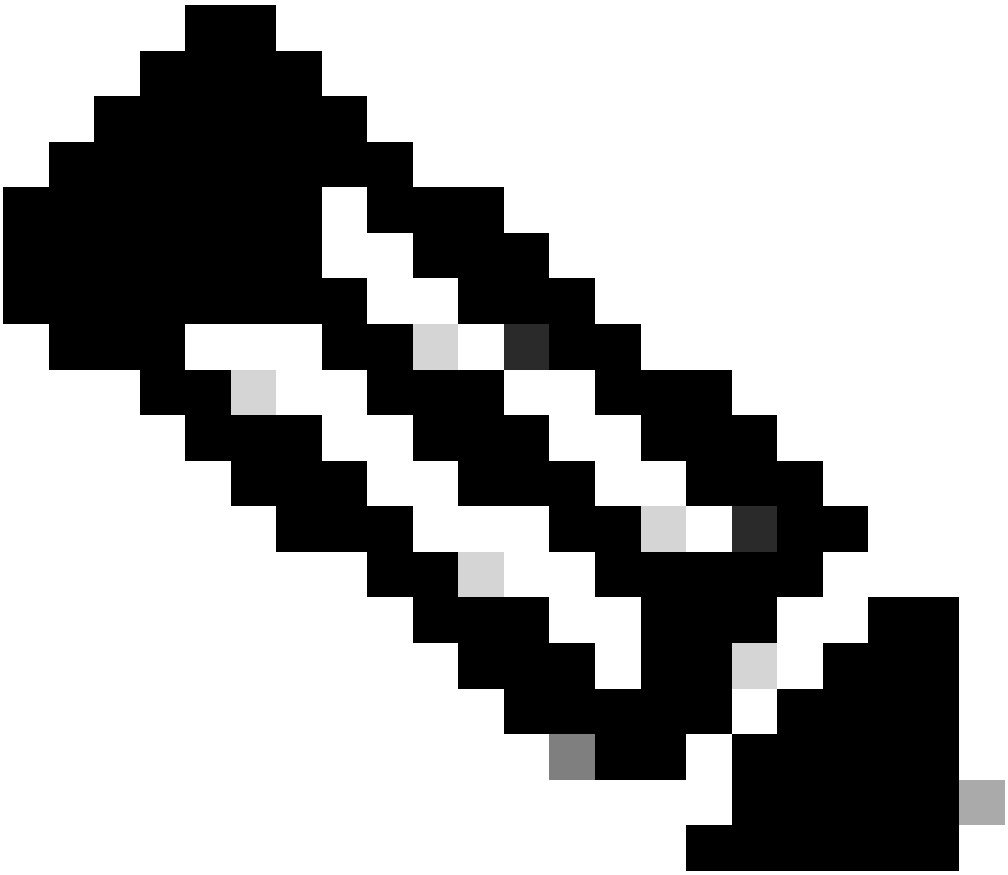
4. 选中 Web Policy 框并选择 **Authentication**。

5. 单击 Apply 以保存更改。

6. 要在WLC上创建用于认证用户的数据库，请转到GUI中的**Security**菜单并选择**Local Net User< /strong>，然后完成以下操作：**

    a. 定义访客用来登录的访客用户名和口令。这些值区分大小写。

    b. 选择您使用的 WLAN ID。



注意：有关详细配置，请参阅无线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. WLC一旦启用，便可以通过无线模式进行管理。有关如何启用无线模式的详细信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版的“启用与GUI和CLI的无线连接”部分。

问： 什么是链路聚合 (LAG)？如何在无线局域网控制器 (WLC) 上启用 LAG？

A.LAG将WLC上的所有端口捆绑到单个EtherChannel接口中。系统使用 LAG 动态管理流量负载均衡和端口冗余。

通常，WLC 上的接口有多个参数与之关联，其中包括 IP 地址、默认网关（对于 IP 子网）、主物理端口、辅助物理端口、VLAN 标记和 DHCP 服务器。如果未使用 LAG，每个接口通常会映射到一个物理端口，但也可以将多个接口映射到一个 WLC 端口。使用 LAG 时，系统会动态地将接口映射到聚合的端口信道。这有助于实现端口冗余和负载均衡。当某个端口发生故障时，接口将动态地映射到下一个可用物理端口，并且 LAP 将在各个端口间实现均衡。

当 WLC 上启用了 LAP 时，WLC 会在接收数据帧的相同端口上转发数据帧。WLC 依靠相邻交换机在 EtherChannel 间均衡流量负载。WLC 自己不执行任何 EtherChannel 负载均衡。

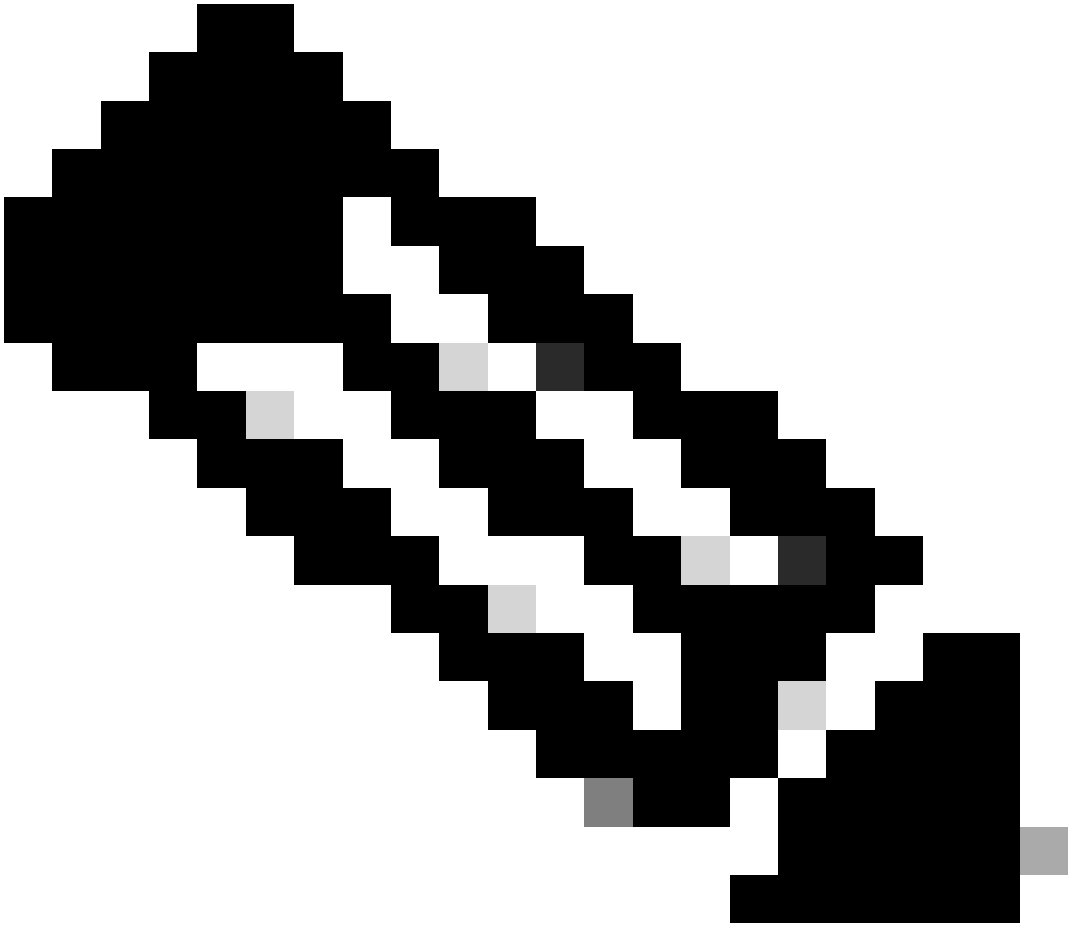
问： 哪些型号的无线局域网控制器 (WLC) 支持链路聚合 (LAG)？

答：Cisco 5500系列控制器在软件版本6.0或更高版本中支持LAG，Cisco 4400系列控制器在软件版本3.2或更高版本中支持LAG，并且Cisco WiSM和Catalyst 3750G集成无线LAN控制器交换机内的控制器上自动启用LAG。在不启用 LAG 的情况下，Cisco 4400 系列控制器上的每个分布系统端口最多支持 48 个接入点。启用LAG后，Cisco 4402控制器逻辑端口支持最多50个接入点，Cisco 4404控制器逻辑端口支持最多100个接入点，Catalyst 3750G集成无线LAN控制器交换机上的逻辑端口和每个Cisco WiSM控制器上的逻辑端口支持最多150个接入点。

Cisco 2106 和 2006 WLC 不支持 LAG。早期型号（如 Cisco 4000 系列 WLC）不支持 LAG。

问： Unified 无线网络中的自动锚点移动功能是什么？

答：自动锚点移动性（或访客WLAN移动性）用于改善无线LAN (WLAN)上漫游客户端的负载均衡和安全性。在正常漫游情况下，客户端设备将加入某个 WLAN 并锚定到它们联系到的第一个控制器。如果客户端漫游到其他子网，客户端漫游到的控制器将为具有锚定控制器的客户端建立一个外来会话。使用自动锚点移动功能，您可以指定一个或一组控制器作为 WLAN 上的客户端的锚点。



注意：不能为第3层移动性配置移动锚点。移动锚点仅用于访客隧道。

问： 能否将 Cisco 2006 无线局域网控制器 (WLC) 配置为 WLAN 的一个锚点？

答：不能将Cisco 2000系列WLC指定为WLAN的锚点。但是，在 Cisco 2000 系列 WLC 上创建的 WLAN 可以使用 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至5.1同时支持非对称和对称移动隧道。控制器软件版本 5.2 及更高版本只支持对称移动隧道，现在该功能默认始终是启用的。

在不对称隧道中，流向有线网络的客户端流量将直接通过外来控制器进行路由。当上游路由器启用了反向路径过滤 (RPF) 时，不对称隧道将断开。在这种情况下，路由器将丢弃客户端流量，因为 RPF 检查将确保返回源地址的路径与数据包传输来的路径相匹配。

如果启用对称移动隧道，所有客户端流量将发送到锚点控制器，并能顺利通过 RPF 检查。对称移动隧道在以下情况下也很有用：

- 安装在客户端数据包路径中的防火墙因源 IP 地址与接收数据包的子网不匹配而丢弃数据包。
- 如果锚点控制器上的接入点组VLAN与外部控制器上的WLAN接口VLAN不同：在这种情况下，在移动性事件期间客户端流量可能会在不正确的VLAN上发送。

问： 当网络发生故障时，我们如何访问 WLC？

A.当网络发生故障时，可通过服务端口访问WLC。系统为该端口分配了一个与 WLC 的其他端口完全不同的子网中的 IP 地址，因此称为带外管理。有关详细信息，请参阅Cisco无线LAN控制器配置指南7.0.116.0版的配置端口和接口部分。

问： Cisco 无线局域网控制器 (WLC) 是否支持故障切换（或冗余）功能？

A.是，如果您的WLAN网络中有两个或多个WLC，则可以配置它们以提供冗余。通常，一个 LAP 会加入到所配置的主 WLC。一旦主 WLC 发生故障，LAP 将重新启动并加入到移动组中的另一个 WLC。在故障切换功能中，LAP 将轮询主 WLC 并会在其可以工作时立即加入主 WLC。有关详细信息，请参阅轻量接入点的WLAN控制器故障切换配置示例。

问： 无线局域网控制器 (WLC) 中的预认证访问控制列表 (ACL) 有何用途？

A.使用预身份验证ACL（顾名思义），即使在客户端进行身份验证之前，您也可以允许客户端数据流出入特定IP地址。使用外部Web服务器进行Web身份验证时，某些WLC平台需要为外部Web服务器（Cisco 5500系列控制器、Cisco 2100系列控制器、Cisco 2000系列和控制器网络模块）预身份验证ACL。对于其他WLC平台，预身份验证ACL不是必需的。但是，在使用外部Web身份验证时，一种好的做法是为外部Web服务器配置预身份验证ACL。

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，客户端是否会自动与 MAC 过滤器上设置的 WLAN ID 相关联？ 此外，为什么 MAC 过滤器上会有一个“接口”选项？

A.客户端可以关联到客户端配置为连接到的任何WLAN。MAC 过滤器中的接口选项可用于将过滤器应用到 WLAN 或某个接口。如果多个 WLAN 绑定到相同的接口，您可以为该接口应用 MAC 过滤器而无需为每个 WLAN 分别创建过滤器。

问： 如何为无线局域网控制器 (WLC) 上的管理用户配置 TACACS 认证？

A.从WLC版本4.1开始，WLC支持TACACS。请参阅配置TACACS+以了解如何配置TACACS+以认证WLC的管理用户。

问： 无线局域网控制器 (WLC) 中的过度认证失败设置有何用途？

A.此设置是客户端排除策略之一。客户端排除是控制器上的一项安全功能。该策略用于排除客户端，以防止非法访问网络或攻击无线网络。

启用此过度Web身份验证失败策略后，当客户端尝试失败次数超过5次时，控制器会认为客户端已超过Web身份验证的最大尝试次数，并排除客户端。

要启用或禁用此设置，请完成以下步骤：

1. 在 WLC GUI 中，转到 Security > Wireless Protection Policies > Client Exclusion Policies。

2. 选中或取消选中 Excessive Web Authentication Failures。

问： 我将我的自治接入点 (AP) 转换为轻量模式。在使用 AAA RADIUS 服务器进行客户端审计的轻量级无线接入点协议 (LWAPP) 模式下，通常是基于 WLC 的 IP 地址跟踪客户端的 RADIUS 审计。 能否基于与该 WLC 关联的 AP 的 MAC 地址而不是该 WLC 的 IP 地址设置 RADIUS 记帐？

A.是，可以使用WLC端配置完成此操作。请完成以下步骤：

1. 在控制器 GUI 中的 Security > Radius Accounting 下，有一个“Call Station ID Type”下拉框。选择 AP MAC Address。
2. 通过 LWAPP AP 日志对此进行验证。在该日志中，您会看到 called-station ID 字段显示了特定客户端所关联的 AP 的 MAC 地址。

问： 如何通过 CLI 在无线局域网控制器 (WLC) 上更改 Wi-Fi Protected Access (WPA) 握手超时值？我知道我可以在Cisco IOS接入点(AP)上使用**dot11 wpa handshake timeoutvalue**命令进行此项更改，但如何在WLC上执行此操作？

A.软件版本4.2及更高版本中集成了通过WLC配置WPA握手超时的功能。早期的 WLC 软件版本中不需要此选项。

可使用以下命令更改 WPA 握手超时值：

<#root>

config advanced eap eapol-key-timeout

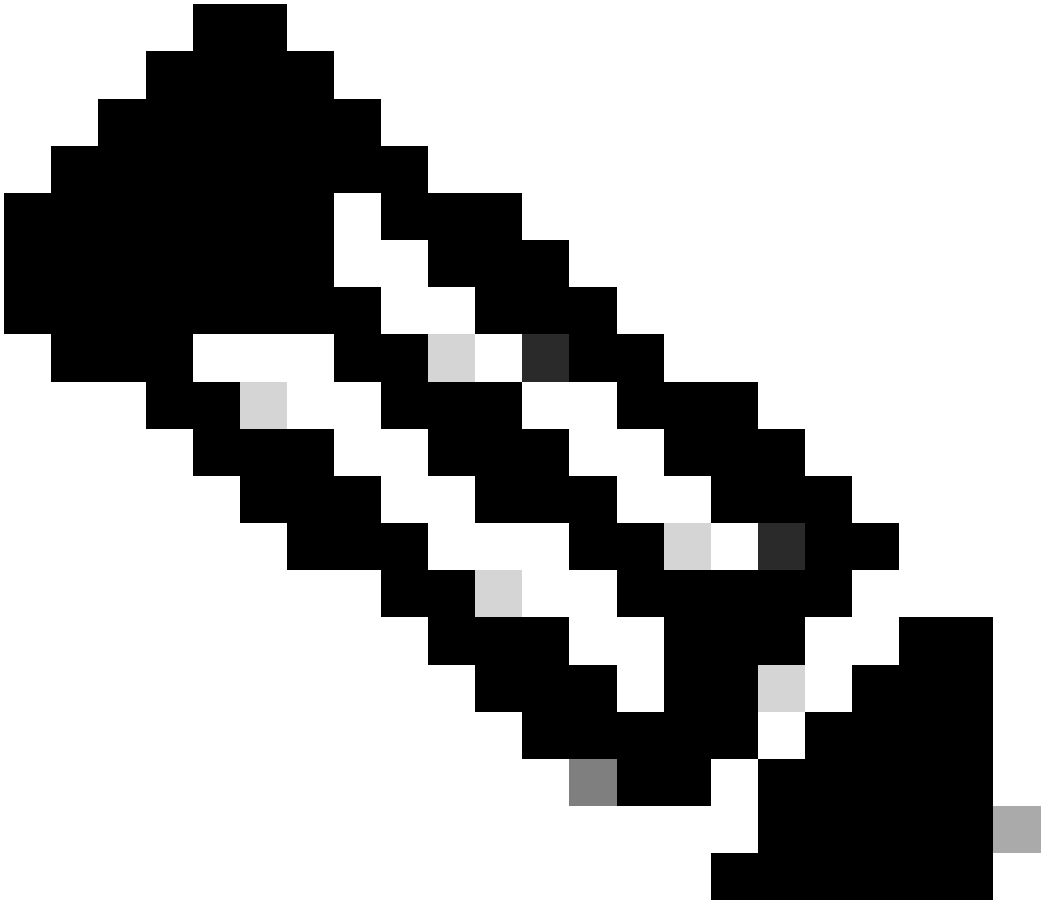
<value>

config advanced eap eapol-key-retries

<value>

默认值继续反映 WLC 的当前行为。

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



注意：在Cisco IOS AP上，可使用dot11 wpa handshake命令配置此设置。

您还可以使用 config advanced eap 命令下的选项配置其他 EAP 参数。

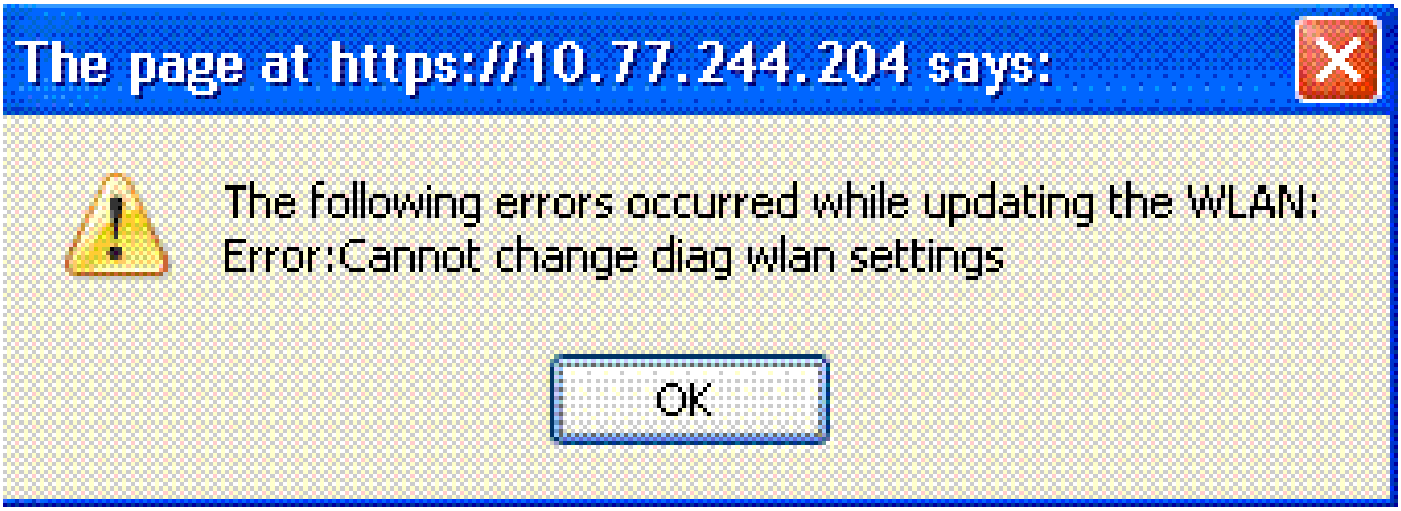
```
(Cisco Controller) >config advanced eap ?

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： WLAN > Edit > Advanced 页面上的诊断信道功能有何用途？

A.诊断信道功能使您能够排查与WLAN的客户端通信相关的问题。您可以对客户端和接入点进行一组定义的测试以确定客户端通信困难的原因，然后采取纠正措施以使客户端能够在网络上正常工作。您可以使用控制器 GUI 或 CLI 启用诊断信道，并且可以使用控制器 CLI 或 WCS 运行诊断测试。

诊断信道只能用于测试。如果在启用诊断信道的情况下尝试为 WLAN 配置认证或加密，您会看到以下错误：



问： 在 WLC 上可以配置的最大 AP 组数是多少？

A.此列表显示可在WLC上配置的AP组的最大数量：

- 对于 Cisco 2100 系列控制器和控制器网络模块，最多可以配置 50 个接入点组
- 对于 Cisco 4400 系列控制器、Cisco WiSM 和 Cisco 3750G 无线 LAN 控制器交换机，最多可以配置 300 个接入点组
- 对于 Cisco 5500 系列控制器，最多可以配置 500 个接入点组

相关信息

- 无线局域网控制器(WLC)错误和系统消息常见消息
- 轻量接入点常见问题
-

无线局域网控制器上的IPv6支持

- **无线产品支持**
- **思科技术支持和下载**

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）。