目录

简介

本文档通过一个配置示例说明如何使用无线 LAN 控制器 (WLC) 配置 MAC 过滤器。本文档还讨论如何根据 AAA 服务器授权轻量接入点 (LAP)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 有关 LAP 和 Cisco WLC 配置的基本知识
- 有关 Cisco 统一无线安全解决方案的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 5.2.178.0 的 Cisco 4400 WLC
- Cisco 1230AG 系列 LAP
- 具有固件 4.4 的 802.11 a/b/g 无线客户端适配器
- Aironet Desktop Utility (ADU) 版本 4.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

WLC 上的 MAC 地址过滤器（MAC 身份验证）

在 WLC 上创建 MAC 地址过滤器时，将根据用户所使用的客户端的 MAC 地址允许或拒绝他们访问 WLAN 网络。

WLC 上支持两种类型的 MAC 身份验证：

- 本地 MAC 身份验证
- 使用 RADIUS 服务器的 MAC 身份验证

使用本地 MAC 身份验证，用户 MAC 地址存储在 WLC 上的数据库中。当用户尝试访问为 MAC 过滤配置的 WLAN 时，将根据 WLC 上的本地数据库对客户端 MAC 地址进行验证，如果身份验证成功，则授权该客户端访问 WLAN。

默认情况下，WLC 本地数据最多支持 512 个用户条目。

本地用户数据库对最多2048个条目被限制。本地数据库存储下列项的条目：

- 本地管理用户，包括大厅大使
- 本地网络用户，包括来宾用户
- MAC过滤器条目
- 排除列表项
- 接入点authorization list条目

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)
```

或者，也可使用 RADIUS 服务器执行 MAC 地址身份验证。唯一的不同之处是，用户 MAC 地址数据库存储在 RADIUS 服务器而不是 WLC 中。当用户数据库存储在 RADIUS 服务器中时，WLC 将客户端 MAC 地址转发到 RADIUS 服务器进行客户端验证。然后，RADIUS 服务器根据它所拥有的数据库验证 MAC 地址。如果客户端身份验证成功，则授予该客户端访问 WLAN 的权限。可以使用支持 MAC 地址身份验证的任何 RADIUS 服务器。

在 WLC 上配置本地 MAC 身份验证

要在 WLC 上配置本地 MAC 身份验证，请完成以下步骤：

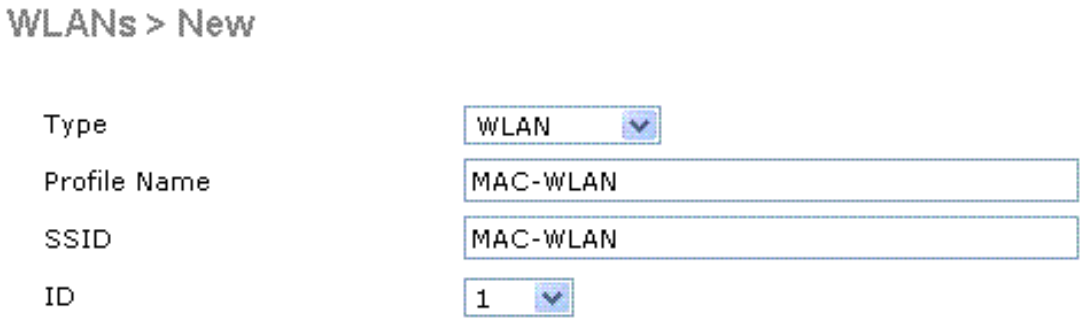
1. 配置 WLAN 并启用 MAC 过滤
2. 使用客户端 MAC 地址在 WLC 上配置本地数据库**注意：** 在配置 MAC 身份验证之前，必须针对基本操作配置 WLC 并将 LAP 注册到 WLC 中。本文档假设已针对基本操作配置了 WLC 且 LAP 已注册到 WLC 中。如果您是尝试设置 WLC 以对 LAP 执行基本操作的新用户，请参阅在无线 LAN 控制器 (WLC) 中注册轻量 AP (LAP)。**注意：** 无线客户端上不需要特殊配置来支持

MAC 身份验证。

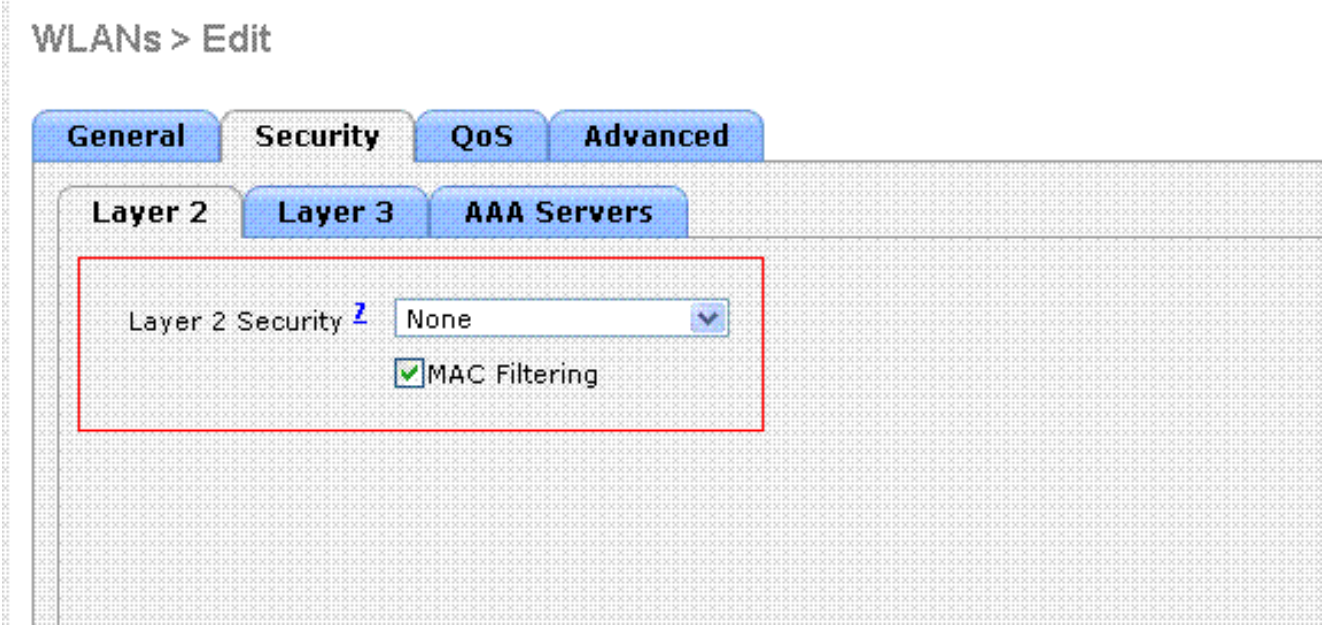
配置 WLAN 并启用 MAC 过滤

要配置使用 MAC 过滤的 WLAN，请完成以下步骤：

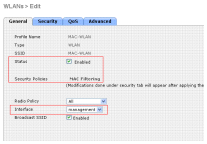
1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本示例中，WLAN 命名为 *MAC-WLAN* 且 WLAN ID 为 1。



3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。



在 Security Policies > Layer 2 Security 下，选中 **MAC Filtering** 复选框。这将为 WLAN 启用 MAC 身份验证。在 General Policies > Interface Name 下，选择 WLAN 被映射到的接口。在本例中，WLAN 被映射到管理接口。根据 WLAN 的设计要求选择其他参数。单击 **Apply**。



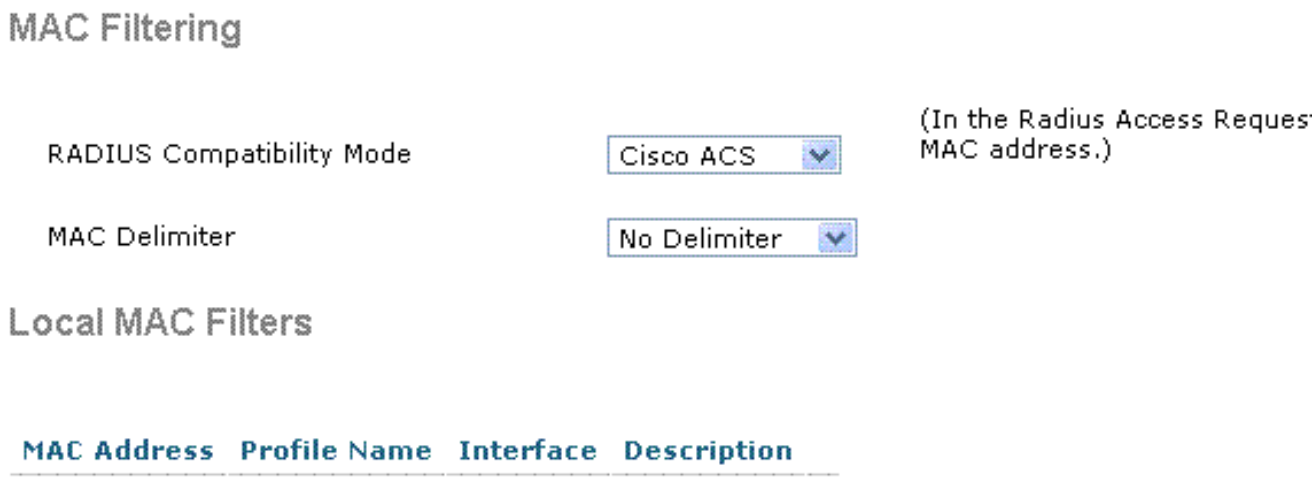
下一步是使用客户端 MAC 地址在 WLC 上配置本地数据库。

有关如何在 WLC 上配置动态接口 (VLAN) 的详细信息，请参阅无线 LAN 控制器上的 VLAN 配置示例。

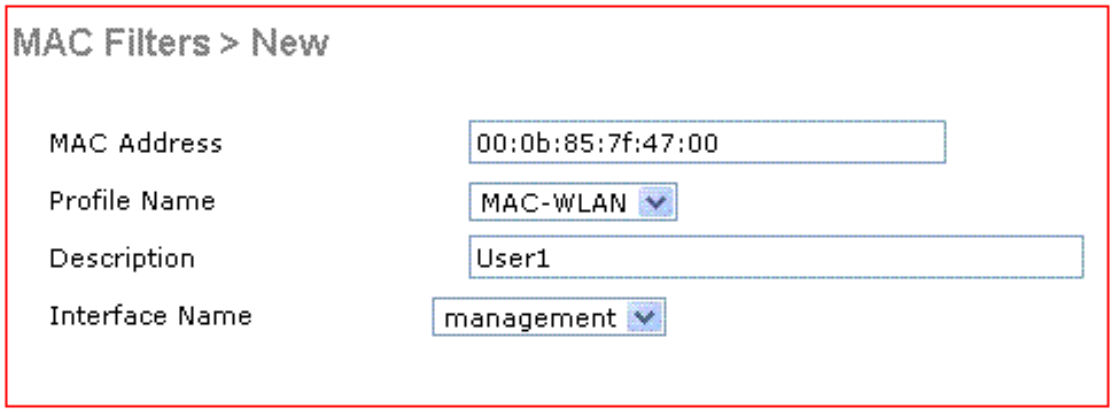
使用客户端 MAC 地址在 WLC 上配置本地数据库

要在 WLC 上使用客户端 MAC 地址配置本地数据库，请完成以下步骤：

1. 在控制器 GUI 中单击 **Security**，然后单击左侧菜单中的 MAC Filtering。此时将显示 MAC Filtering 窗口。



2. 单击 **New** 以在 WLC 上创建一个本地数据库 MAC 地址条目。
3. 在 MAC Filters > New 窗口中，输入客户端的 MAC 地址、配置文件名称、说明和接口名称。示例如下：



4. 单击 **Apply**。
5. 要向本地数据库中添加更多客户端，请重复步骤 2 到 4。现在，当客户端连接到此 WLAN 时，WLC 将根据本地数据库验证客户端 MAC 地址。如果验证成功，则授权该客户端访问网络。**注意：** 在本示例中，只使用了 MAC 地址过滤器，而未使用任何其他第 2 层安全机制。Cisco 建议应将 MAC 地址身份验证与其他第 2 层或第 3 层安全方法一起使用。不建议只使用

MAC 地址身份验证来保护您的 WLAN 网络，因为它不提供强有力的安全机制。

配置使用 RADIUS 服务器的 MAC 身份验证

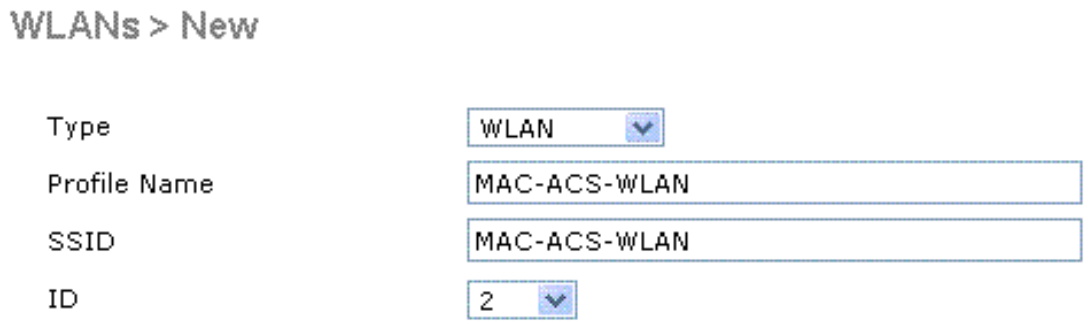
要配置使用 RADIUS 服务器的 MAC 身份验证，请完成以下步骤。在本示例中，使用 Cisco Secure ACS 服务器作为 RADIUS 服务器。

1. 配置 WLAN 并启用 MAC 过滤
2. 使用客户端 MAC 地址配置 RADIUS 服务器

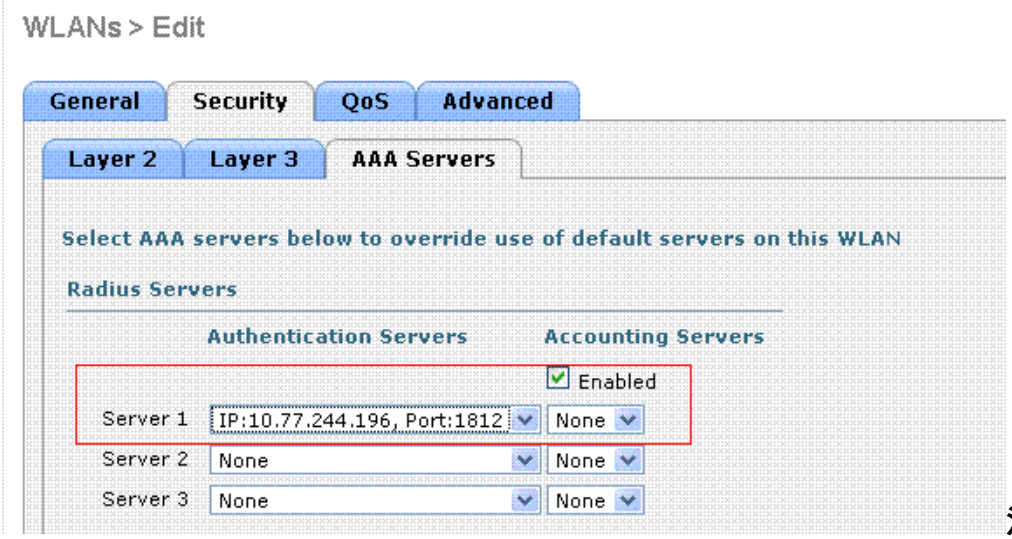
配置 WLAN 并启用 MAC 过滤

要配置使用 MAC 过滤的 WLAN，请完成以下步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本示例中，WLAN 命名为 *MAC-ACS-WLAN* 且 WLAN ID 为 2。



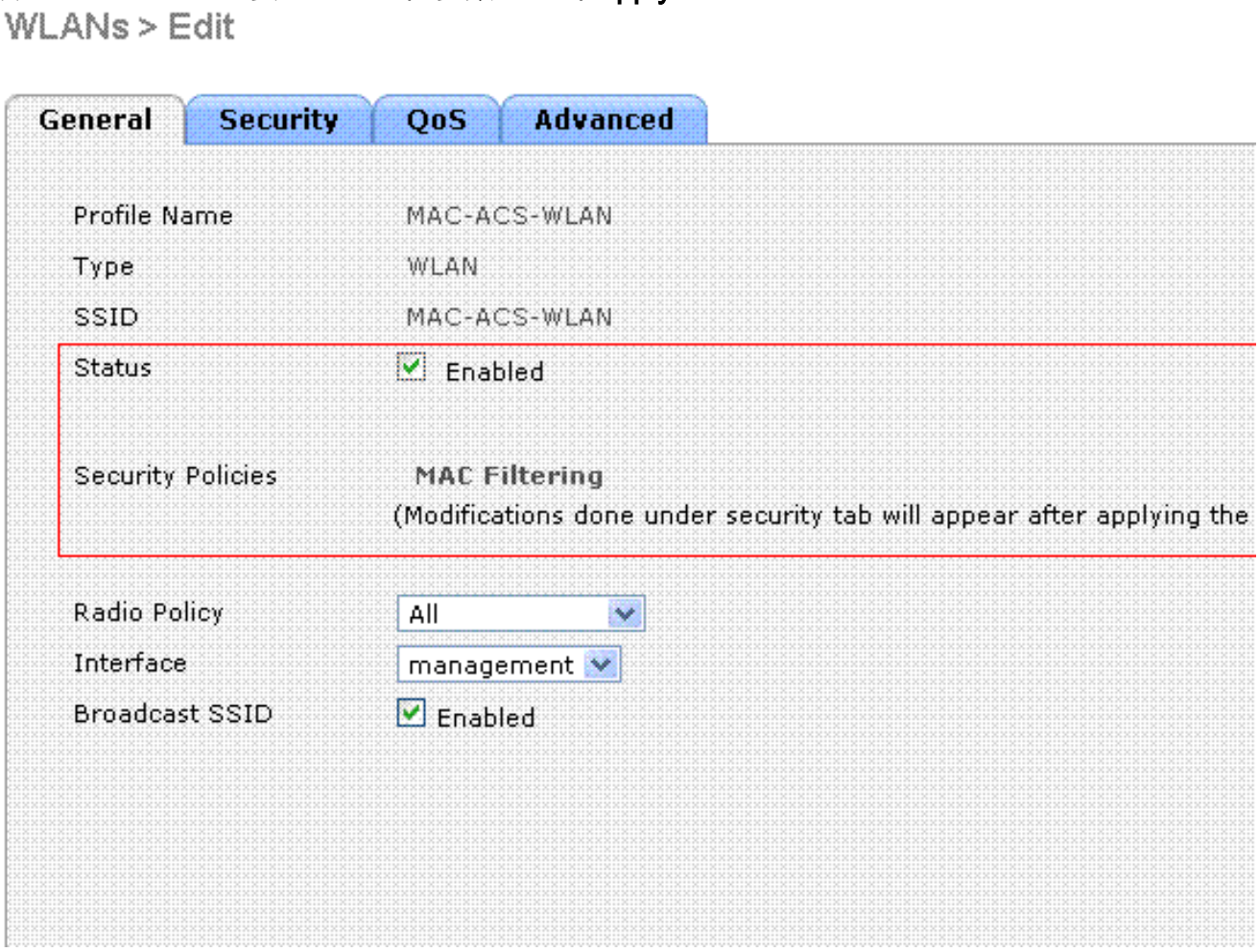
3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。在 Security Policies > Layer 2 Security 下，选中 **MAC Filtering** 复选框。这将为 WLAN 启用 MAC 身份验证。在 General Policies > Interface Name 下，选择 WLAN 被映射到的接口。在 RADIUS servers 下，选择将用于 MAC 身份验证的 RADIUS 服务器。



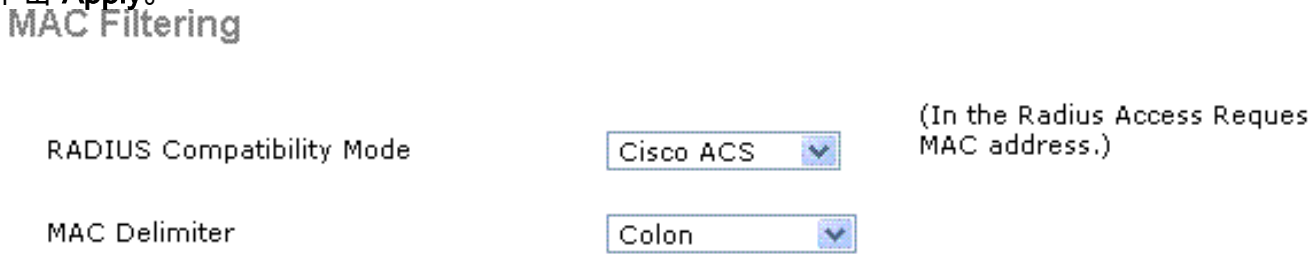
注意： 您应在

Security > Radius Authentication 窗口中定义 RADIUS 服务器并启用 RADIUS 服务器，然后才能从 WLAN > Edit 窗口中选择 RADIUS 服务器。

根据 WLAN 的设计要求选择其他参数。单击 **Apply**。



5. 单击 **Security > MAC Filtering**。
6. 在 MAC Filtering 窗口中，在 RADIUS Compatibility Mode 下选择 RADIUS 服务器的类型。本示例使用 Cisco ACS。
7. 从 MAC Delimiter 下拉菜单中，选择 MAC delimiter。本示例使用 Colon。
8. 单击 **Apply**。

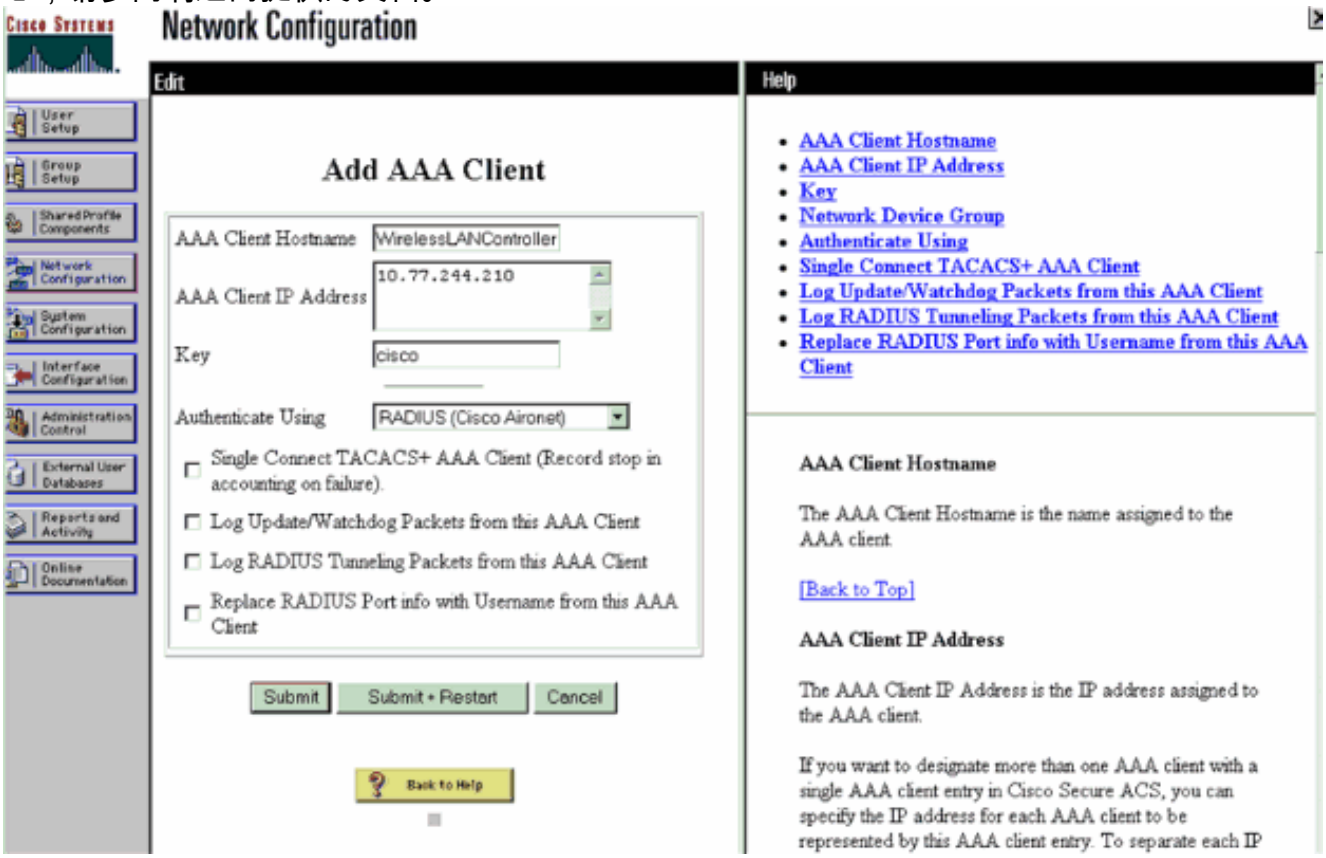


下一步是使用客户端 MAC 地址配置 ACS 服务器。

使用客户端 MAC 地址配置 RADIUS 服务器

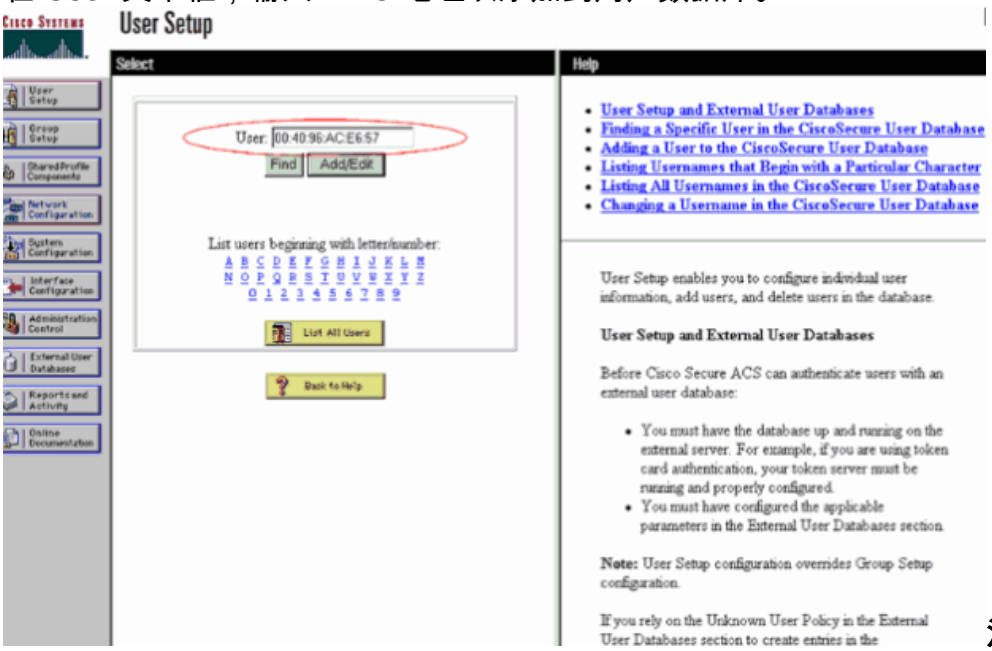
要向 ACS 中添加 MAC 地址，请完成以下步骤：

1. 在 ACS 服务器上将 WLC 定义为 AAA 客户端。从 ACS GUI 中单击 **Network Configuration**。
2. 当出现 Network Configuration 窗口时，定义 WLC 的名称、IP 地址、共享密钥和身份验证方法（RADIUS Cisco Aironet 或 RADIUS Airespace）。有关其他非 ACS 身份验证服务器的信息，请参阅制造商提供的文档。



注意： 在 WLC 和 ACS 服务器上配置的共享密钥必须匹配。共享密钥区分大小写。

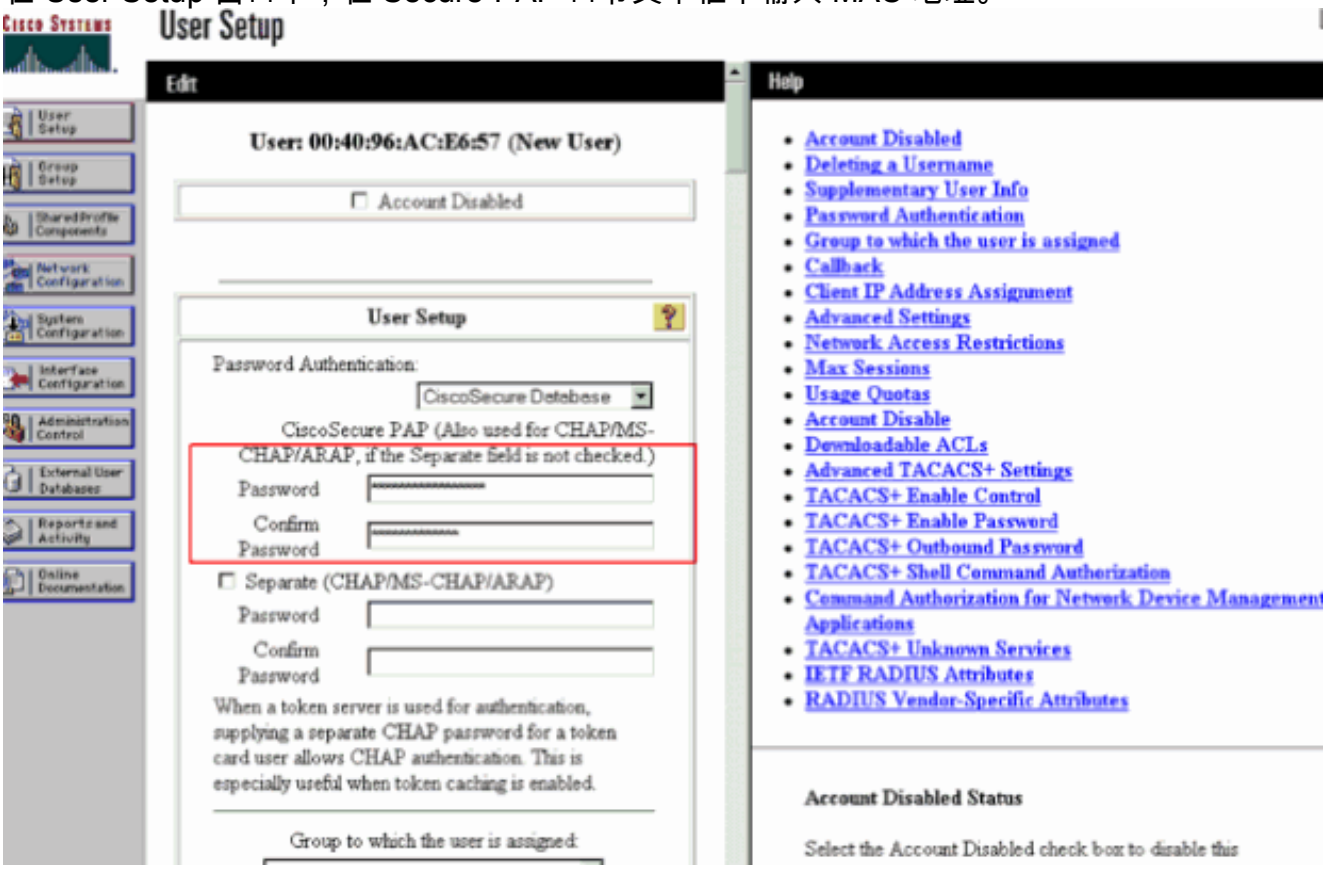
3. 从 ACS 主菜单中，单击 **User Setup**。
4. 在 User 文本框，输入 MAC 地址以添加到用户数据库。



注意： MAC 地址必须

与作为用户名和口令由 WLC 发送的 MAC 地址完全一致。如果身份验证失败，请检查失败的尝试日志以查看 WLC 如何报告 MAC。请不要剪切并粘贴 MAC 地址，因为这可能引入虚拟字符。

5. 在 User Setup 窗口中，在 Secure-PAP 口令文本框中输入 MAC 地址。



注意： MAC 地址必须与作为用户名和口令由 WLC 发送的 MAC 地址完全一致。如果身份验证失败，请检查失败的尝试日志以查看 AP 如何报告 MAC。请不要剪切并粘贴 MAC 地址，因为这可能引入虚拟字符。

6. 单击 **submit**。
7. 要向 ACS 数据库中添加更多用户，请重复步骤 2 到 5。现在，当客户端连接到此 WLAN 时，WLC 会将凭据传送给 ACS 服务器。ACS 服务器根据 ACS 数据库验证这些凭据。如果客户端 MAC 地址存在于数据库中，ACS RADIUS 服务器将向 WLC 返回身份验证成功消息，客户端将被授予访问 WLAN 的权限。

使用 CLI 在 WLC 上配置 MAC 过滤器

本文档前面已讨论如何使用 WLC GUI 配置 MAC 过滤器。您也可以使用 CLI 在 WLC 上配置 MAC 过滤器。您可以使用以下命令在 WLC 上配置 MAC 过滤器：

- 发出**设置WLAN MAC过滤enable (event) wlan_id**命令为了启用MAC过滤。bEnter**显示WLAN**命令为了验证您有MAC过滤为WLAN启用。
- **config macfilter add** 命令：通过 **config macfilter add** 命令，可以添加 MAC 过滤器、接口、说明等等。使用 **config macfilter add** 命令可在 Cisco 无线 LAN 控制器上创建 MAC 过滤器条目。使用此命令可在 Cisco 无线 LAN 控制器上添加无线 LAN 的本地客户端。此过滤器将绕过 RADIUS 身份验证过程。**config macfilter add** MAC_address wlan_id [interface_name] [description] [IP address] **示例：**输入一个静态 MAC 到 IP 的地址映射。执行该操作可支持*被动客户端*，即，不使用 DHCP 也不传输未经请求的 IP 数据包的客户端。**>config macfilter add** 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
- **config macfilter ip-address** 命令通过 **config macfilter ip-address** 命令，可以将一个现有 MAC

过滤器映射到一个 IP 地址。使用以下命令可将 IP 地址配置到本地 MAC 过滤器数据库中：**config macfilter ip-address** MAC_address IP address **示例：**>**config macfilter add** 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51

配置已禁用客户端的超时

您能配置已禁用客户端的一超时。不能验证三次在尝试联合期间的客户端从更加进一步的关联尝试自动地禁用。在超时周期之后超时，客户端允许重试验证，直到关联或发生故障验证和再被排除。

输入**timeout命令config wlan exclusionlist的wlan_id**为了配置已禁用客户端的超时。超时值可以是从1到65535秒，或者您能输入0为了永久禁用客户端。

验证

使用以下命令可验证 MAC 过滤器配置是否正确：

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show macfilter摘要**？显示所有MAC过滤器条目摘要。
- **show macfilter详细信息<client** *MAC地址***>** ？MAC过滤器条目的详细的显示。

以下是 **show macfilter summary** 命令的一个示例：

```
(Cisco Controller) >show macfilter summaryMAC Filter RADIUS Compatibility mode.............
Cisco ACSMAC Filter Delimiter.......................... NoneLocal Mac Filter TableMAC Address
WLAN Id          Description-----------------------   --------------   -------------------------
-------00:40:96:ac:e6:57          1             Guest(Cisco Controller) >show macfilter detail
00:40:96:ac:e6:57
```

以下是 **show macfilter detail** 命令的一个示例：

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57MAC
Address..................................... 00:40:96:ac:e6:57WLAN
Identifier.............................. 1Interface Name.............................
mac-clientDescription..................................... Guest
```

故障排除

您可以使用以下命令来排除配置问题：

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug aaa全部启用**？提供所有AAA消息调试。
- **debug mac addr <client-MAC-address xx:** *xx : xx : xx : xx : xx* **>** ？为了配置调试的MAC，请使用**mac命令的调试。**

以下是 **debug aaa all enable** 命令的一个示例：

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657Wed May 23 11:13:55 2007:
Looking up local blacklist 004096ace657Wed May 23 11:13:55 2007: User 004096ace657
authenticatedWed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0)
for mobile 00:40:96:ac:e6:57Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97cWed May
23 11:13:55 2007: structureSize.............................76Wed May 23 11:13:55 2007:
resultCode.................................0Wed May 23 11:13:55 2007:
protocolUsed.............................0x00000008Wed May 23 11:13:55 2007:
proxyState.................................                                    00:40:96:AC:E6:57-
```

```
00:00Wed May 23 11:13:55 2007: Packet contains 2 AVPs:Wed May 23 11:13:55 2007:     AVP[01]
Service-Type.............................                                    0x0000000a (10) (4
bytes)Wed May 23 11:13:55 2007:     AVP[02] Airespace / Interface-Name.............
staff-vlan (10 bytes)Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute
6Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5Wed May 23 11:13:55
2007: 00:40:96:ac:e6:57 Applying new AAA override for                              station
00:40:96:ac:e6:57Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station
00:40:96:ac:e6:57source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag:
0xffffffff, sessionTimeout: -1dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -
1vlanIfName: 'mac-client'
```

当 WLC（本地数据库）或 RADIUS 服务器上的 MAC 地址数据库中不存在的无线客户端尝试与 WLAN 关联时，将排除该客户端。以下是针对不成功 MAC 身份验证的 **debug aaa all enable** 命令的一个示例：

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657Wed May 23
11:05:06 2007: AuthenticationRequest: 0xa620e50Wed May 23 11:05:06 2007:
Callback.....................................0x807e724Wed May 23 11:05:06 2007:
protocolType.................................0x00000001Wed May 23 11:05:06 2007:
proxyState...................................                                    00:40:96:AC:E6:57-
00:00Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)Wed May 23 11:05:06 2007:
00:40:96:ac:e6:57 Returning AAA Error 'No Server' (-7)                          for mobile
00:40:96:ac:e6:57Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4Wed May 23 11:05:06
2007: structureSize..............................28Wed May 23 11:05:06 2007:
resultCode...................................-7Wed May 23 11:05:06 2007:
protocolUsed.................................0xffffffffWed May 23 11:05:06 2007:
proxyState...................................                                    00:40:96:AC:E6:57-
00:00Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

尝试通过 MAC 地址进行身份验证的无线客户端被拒绝；失败的身份验证报告显示内部错误

当使用在 Microsoft Windows 2003 Enterprise 服务器上运行的 ACS 4.1 时，尝试通过 MAC 地址进行身份验证的客户端将被拒绝。当 AAA 客户端向 AAA 服务器发送 Service-Type=10 属性值时会发生这种情况。这是因为 Cisco bug ID CSCsh62641（仅限注册用户）。受此 bug 影响的 AAA 客户端包括 WLC 和使用 MAC 身份验证旁路的交换机。

解决方法如下：

- 降级到 ACS 4.0。或
- 在内部 ACS DB MAC 地址表下，将要进行身份验证的 MAC 地址添加到网络访问保护 (NAP) 中。

不能使用 WLC GUI 添加 MAC 过滤器

这可能是由于 Cisco bug ID CSCsj98722（仅限注册用户）引起的。此 bug 在 4.2 代码版本中得到修复。如果运行的是早于 4.2 的版本，则可以将固件升级到 4.2 或使用下面两个解决方法来解决此问题。

- 使用 CLI，通过以下命令配置 MAC 过滤器：**config macfilter add** <MAC address> <WLAN ID#> <Interface>
- 在控制器的 Web GUI 中，在 Security 选项卡中选择 **Any WLAN** 并输入要过滤的 MAC 地址。

未将静默客户置于运行状态

如果未在控制器上配置必需的 DHCP，则当无线客户端发送出第一个 IP 数据包或 ARP 时，AP 可获知该无线客户端的 IP 地址。如果无线客户端是被动设备，例如，不启动通信的设备，则 AP 无法获知无线设备的 IP 地址。结果，控制器会等待十秒以等待客户端发送 IP 数据包。如果没有来自客户端的数据包响应，则控制器将丢弃发往被动无线客户端的任何数据包。Cisco bug ID CSCsq46427（仅限注册用户）中记录了此问题。

作为针对打印机、无线 PLC 泵等被动设备的建议解决方法，您需要针对 MAC 过滤设置 WLAN 并选中 AAA 覆盖以允许连接这些设备。

可以在将无线设备的 MAC 地址映射到 IP 地址的控制器上创建 MAC 地址过滤器。

注意： 这需要在 WLAN 配置上针对第 2 层安全启用 MAC 地址过滤。它还需要在 WLAN 配置的高级设置中启用 Allow AAA Overide。

在 CLI 中，请输入以下命令来创建 MAC 地址过滤器：

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

示例如下：

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

相关信息

- 无线 LAN 控制器中的 ACL 配置示例
- 无线局域网控制器认证的配置示例
- 无线局域网控制器上的 VLAN 配置示例
- Cisco 无线局域网控制器配置指南 4.1 版
- 无线技术支持页
- 技术支持和文档 - Cisco Systems