

配置轻量级接入点作为802.1x请求方

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[配置LAP](#)

[配置交换机](#)

[配置 RADIUS 服务器](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

本文描述如何配置一轻量级接入点作为802.1x请求方验证RADIUS服务器。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- Cisco Aironet 1130，1240或者1250系列接入点
- 运行IOS®版本5.1的WLC
- Cisco Catalyst 3560系列交换机用Cisco IOS版本12.2(35)SE5
- Cisco Catalyst 3750系列交换机用Cisco IOS版本12.2(40)SE
- Cisco Catalyst 4500系列交换机用Cisco IOS版本12.2(40)SG
- Cisco Catalyst 6500系列交换机用Supervisor引擎运行Cisco IOS版本12.2(33)SXH的32

使用的组件

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](#)。

背景信息

拉普设备安装X.509证书，签字由专用密钥，烧录到设备在制造时。拉普使用此证书验证与WLC在加入进程。欲知更多信息，参考[保护部署思科440X系列无线局域网控制器的](#)本文的[LWAPP控制层面](#)。此方法描述另一个方式验证拉普。使用WLC版本5.1，您能配置在Cisco Aironet接入点和Cisco交换机之间的802.1x验证。接入点作为802.1x请求方和由该的RADIUS服务器(ACS)的交换机验证EAP-FAST的用途与匿名PAC设置。一旦它为802.1x验证配置，交换机不允许任何流量除802.1x流量之外穿过端口，直到设备连接对端口成功验证。接入点可以验证或者，在加入WLC前或，在加入WLC后，在您配置在交换机情况下的802.1x，在LAP加入WLC后。

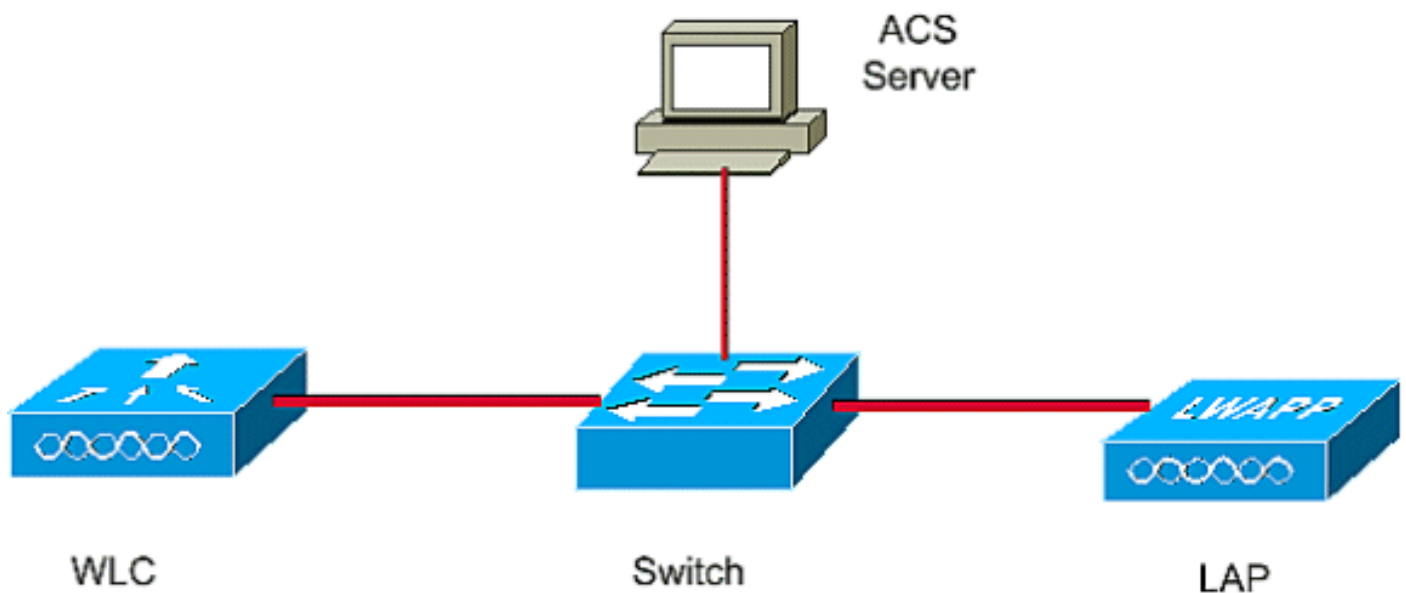
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用以下网络设置：



配置

本文使用这些IP地址：

- 交换机的IP地址是10.77.244.210
- ACS服务器的IP地址是10.77.244.196
- WLC的IP地址是10.77.244.204

配置LAP

在此部分，您提交以信息配置LAP作为802.1x请求方。

完成这些步骤：

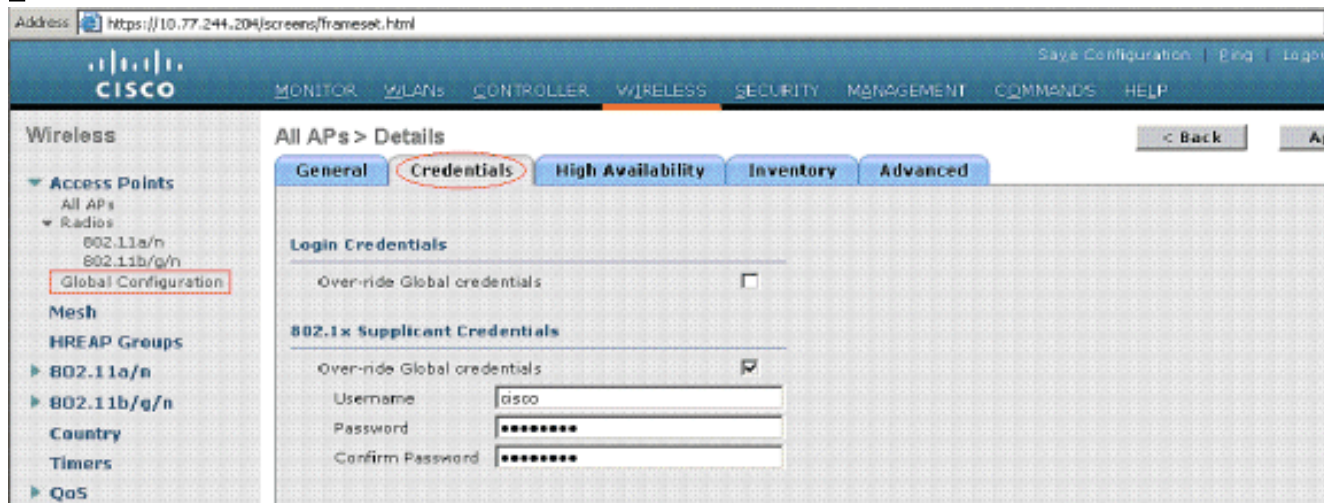
1. 确保接入点装载与一个轻量级恢复镜像。
2. 连接LAP到交换机。
3. LAP通过加入进程并且向WLC登记。如图1所显示，这可以从WLC的无线菜单被检查。图

1



4. 点击接入点，并且点击凭证选项卡。
5. 在朝向802.1x请求方的凭证下，请检查改写全局凭证方框设置此接入点的802.1x用户名和密码。您能也设置用户名和密码共同兴趣为加入与全局配置菜单的一WLC的所有接入点。图2显示如何设置接入点的802.1x凭证。图

2



注意： 您能也设置一接入点的802.1x用户名和密码有CLI命令设置ap dot1xuser添加用户名 <user>密码<password> Cisco_AP的WLC的(AP名称)。

6. 单击 **Apply** 以提交更改。
7. 点击**保存配置**保存凭证。**注意：** 一旦保存，这些凭证在WLC和AP重启间保留。只有当LAP加入一新的WLC时，他们更改。在新的WLC配置的LAP假设用户名和密码。
8. 如果接入点未加入WLC，您在特权模式必须控制到LAP设置凭证和使用CLI命令的此
：LAP#lwapp ap dot1x username <username> password <password> **注意：** 此命令为运行5.1恢复镜像的接入点是仅可用的。

配置交换机

交换机作为LAP的一验证器并且利用RADIUS服务器验证LAP。如果交换机没有兼容软件，请[升级交换机](#)。在交换机CLI，请输入这些命令启用在交换机端口的802.1x验证：

```

switch#configure terminal
switch(config)aaa new-model
group radius
switch(config)dot1x system-auth-control
switch(config)aaa authentication dot1x default
switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret
switch(config)interface gigabitEthernet 1/0/43!---
43 is the port number on which the access point is connected.
switch(config-if)switchport
mode access
switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x authentication.

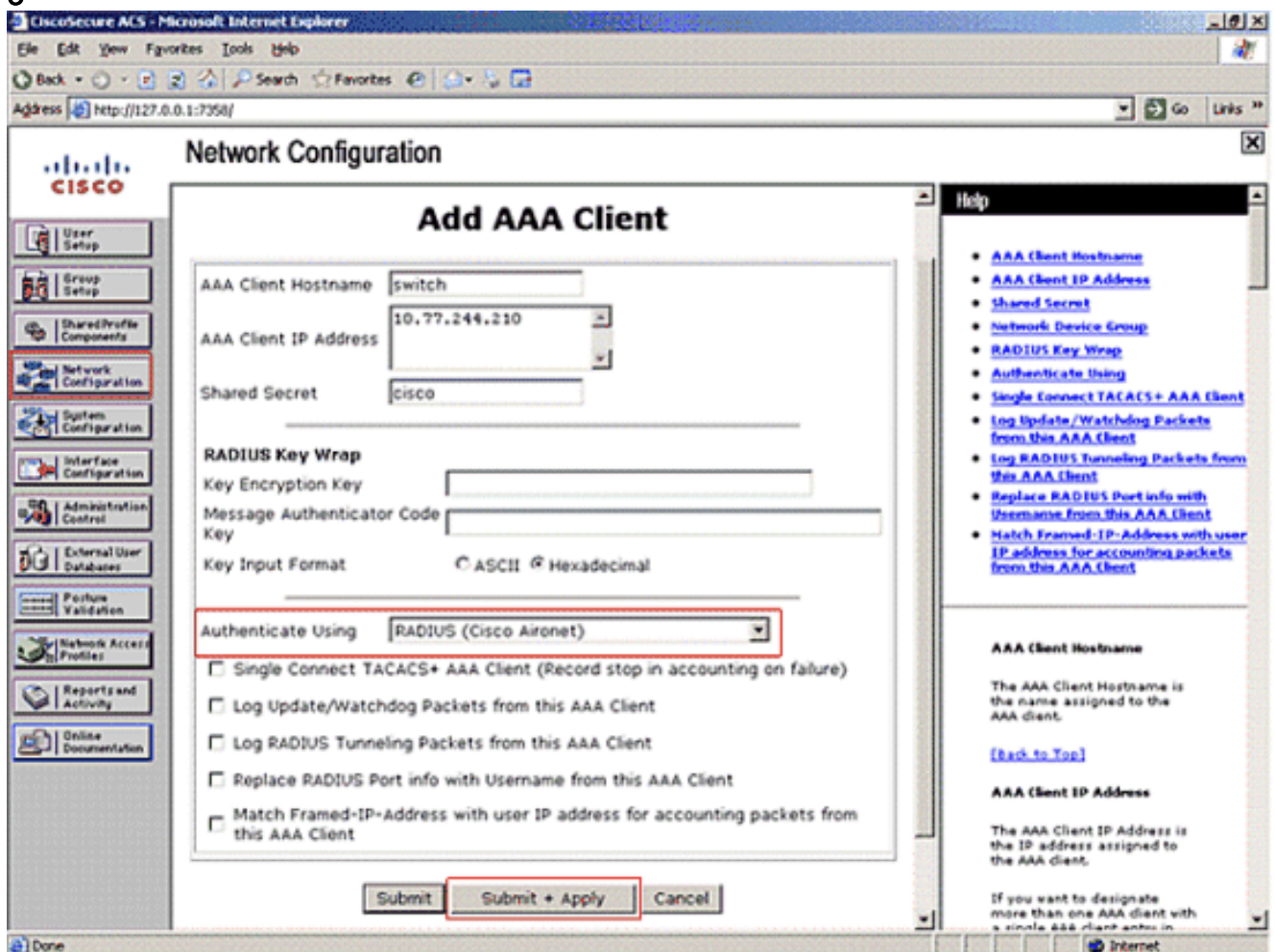
```

配置 RADIUS 服务器

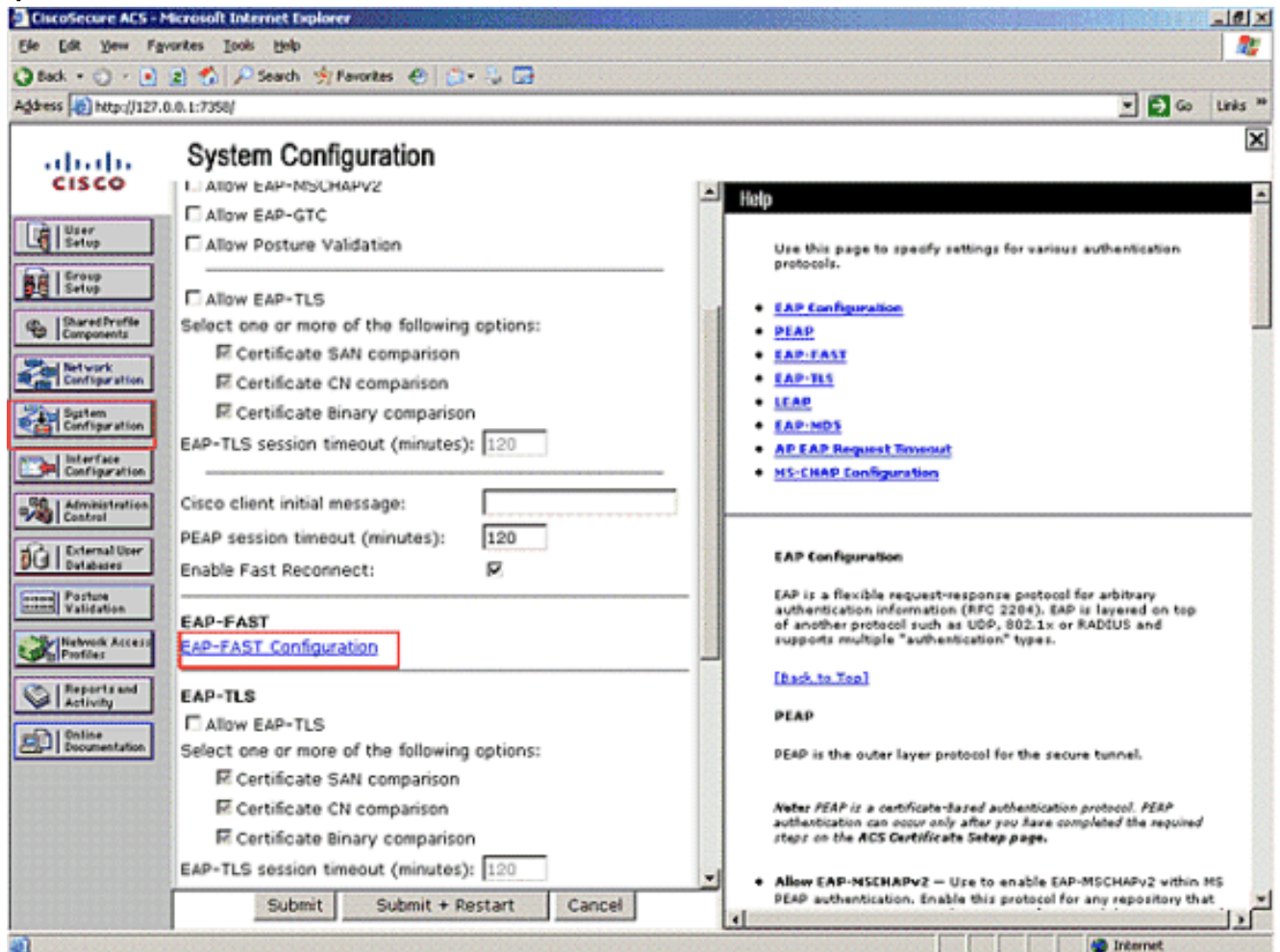
LAP验证与EAP-FAST。确保RADIUS服务器您使用支持此EAP方法。在本例中，ACS服务器使用验证。完成在ACS服务器的这些步骤：

1. 启动ACS admin屏幕。
2. 配置LAP的用户名和密码在ACS数据库的。为了添加在ACS的一个用户帐户，参考本文[用户指南的用户管理部分](#) [思科安全访问控制服务器的4.2](#)。
3. 配置交换机作为AAA客户端到ACS服务器。在ACS admin屏幕，请点击**Network Configuration**菜单。
4. 在**AAA客户端**部分下，请单击**添加新的条目**。输入这些参数：在AAA客户端IP地址字段输入交换机的IP地址。输入交换机的共享机密。这必须正确地是相同的在交换机和ACS服务器。使用字段，选择在验证的一个**RADIUS**协议。默认情况下，它是TACACS+。注意：检查ACS服务器RADIUS协议的说明。请参阅图 3。图

3

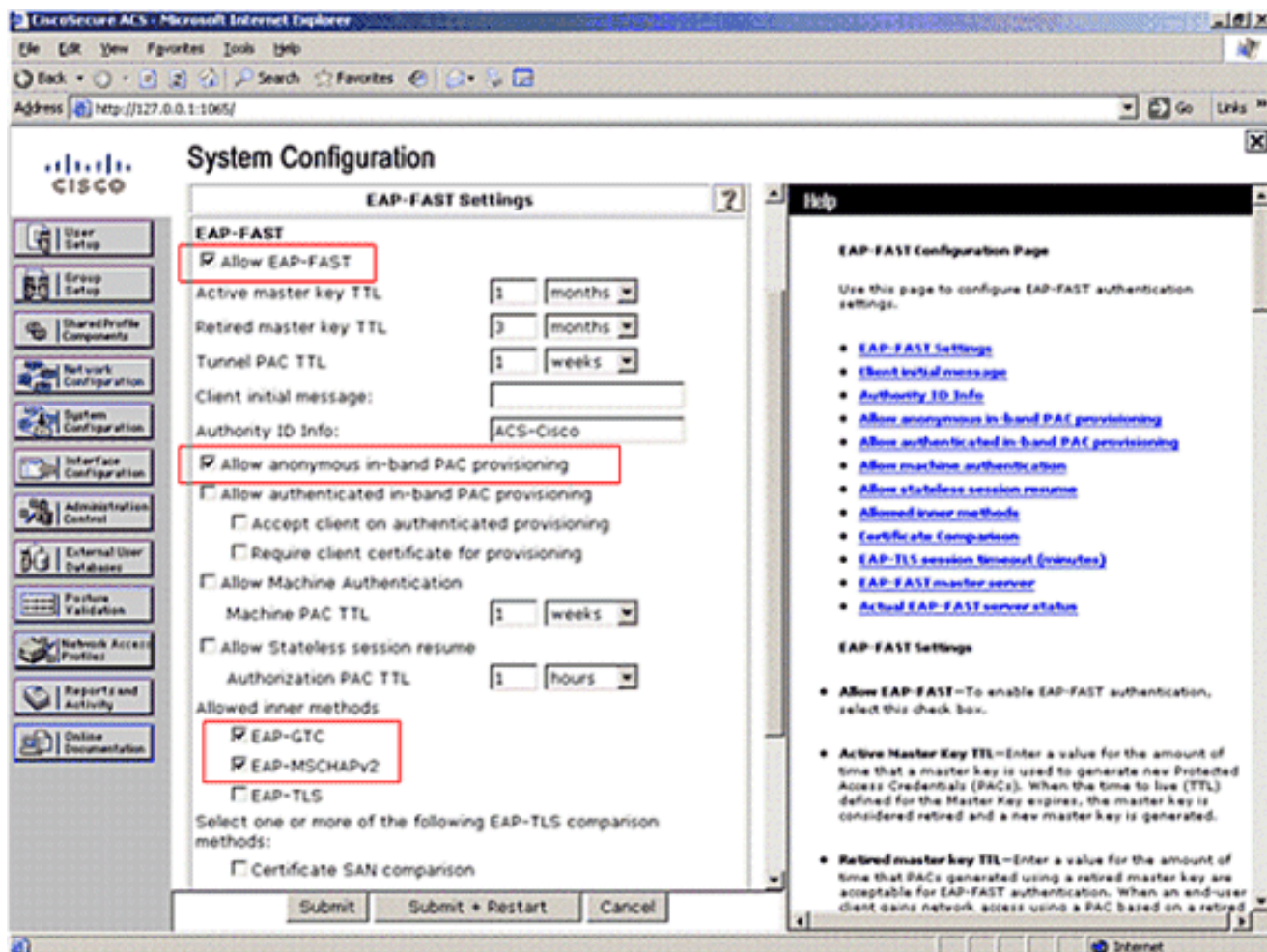


5. 点击**Submit+Apply**救AAA客户端。
6. EAP-FAST在RADIUS服务器必须启用。点击在左手边的**System Configuration**菜单。点击**全局验证设置**选项。图



7. 如图4.所显示，单击EAP-FAST配置。

8. 在EAP-FAST Settings页，请检查允许EAP-FAST方框。LAP以匿名PAC设置使用EAP-FAST。检查设置方框的允许匿名带内PAC。欲知更多信息，参考[与无线局域网控制器和外部RADIUS服务器配置示例的本文EAP-FAST验证](#)。图



9. 确保EAP-GTC和EAP-MSCHAPv2被检查得下允许内在方法。图5显示配置示例步骤8和9。

验证

使用本部分可确认配置能否正常运行。

[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。

一旦802.1x在交换机端口启用，所有流量，除了802.1x流量通过端口阻塞。LAP，已经注册对WLC，获得不相关。在一成功的802.1x之后验证是通过通过的其他允许的流量。LAP的成功的注册对WLC的，在802.1x在交换机后启用表明LAP验证是成功的。

您能从ACS也检查此。从ACS主屏幕，请点击**报告和验证**菜单。点击**Failed Attempts**选项。如果验证是成功的，您查找与如图6.所显示，*EAP-FAST*用户配置有新的PAC用交换机的IP地址在nas-ip-address字段的代码的一个**验证失败**消息。您能也确认与日期和时间验证。

图 6

故障排除

使用本部分可排除配置故障。

1. 请使用ping命令并且检查ACS服务器是否从交换机是可及的。
2. 确保交换机配置作为ACS服务器的一个AAA客户端。
3. 保证共享机密是相同的在交换机和ACS服务器之间。
4. 检查EAP-FAST是否在ACS服务器启用。
5. 检查在设备的软件标准。
6. 检查802.1x凭证是否为LAP配置并且是同样在ACS服务器。注意：用户名和密码区分大小写。

故障排除命令

当前没有此功能的调试可以使用的命令。

相关信息

- [控制轻量接入点](#)
- [配置基于 IEEE 802.1x 端口的身份验证](#)
- [技术支持和文档 - Cisco Systems](#)