无线域服务配置

Contents

Introduction

本文档介绍 Wireless Domain Services (WDS) 的概念。本文也描述如何配置一接入点(AP)或无线局域网服务模块(WLSM)作为WDS和一至少其他作为基础设施AP。本文档中的过程将指导您使用正在运行的 WDS，它允许客户端与 WDS AP 或基础设施 AP 关联。本文打算设立的您能快速地配置安全漫游或介绍无线LAN解决方案引擎的一个基本类型(WLSE)到网络，因此您能使用功能。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 有无线LAN网络和无线安全安全性问题详尽的知识。
- 有当前可扩展的认证协议(EAP)安全方法知识。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 与Cisco IOS软件的APs
- Cisco IOS Software Release 12.3(2)JA2或以上
- Catalyst 6500 Series无线局域网服务模块

本文档中的信息都是基于特定实验室环境中的设备创建的。用于本文的所有设备开始与一原始和一个IP地址在接口BVI1，因此单元从Cisco IOS软件GUI或命令行界面(CLI)是可访问的。如果在一个真实网络工作，请保证您了解所有命令的潜在影响。

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

无线域服务

WDS是APs的一个新功能在Cisco IOS软件和Catalyst 6500 Series WLSM的基本类型。WDS是该核心的功能enable (event)其它功能类似这些：

- 快速地请获取漫游
- WLSE交互作用
- 无线电管理

您必须建立参加WDS和WLSM APs之间的关系，在所有其他基于WDS的功能运作前。其中一个WDS的目的是排除需要对于认证服务器验证用户凭证和减少客户端验证的所需的时间。

为了使用WDS，您必须选定一个AP或WLSM作为WDS。WDS AP必须使用WDS用户名和密码建立与认证服务器的一个关系。认证服务器可以是一个外部RADIUS服务器或本地RADIUS服务器功能在WDS AP。WLSM必须有与认证服务器的关系，即使WLSM不需要验证到服务器。

其他APs，称为基础设施APs，与WDS联络。在注册发生前，基础设施APs必须验证自己到WDS。WDS的基础设施服务器组定义了此基础设施认证。

在WDS的一个或更多客户端服务器组定义了客户端验证。

当客户端尝试联合到基础设施AP时，基础设施AP通过用户的证件对验证的WDS。如果WDS第一次看到证件， WDS转向认证服务器验证证件。当同一个用户再时，尝试认证WDS然后缓存证件，为了排除需要返回到认证服务器。再验证示例包括：

- 键变更
- 漫游
- 当用户启动客户端设备

所有基于RADIUS的EAP认证协议可以通过WDS被以隧道传输例如这些：

- 轻量级EAP (LEAP)
- Protected EAP (PEAP)
- EAP 传输层安全 (EAP-TLS)
- EAP灵活认证通过获取建立隧道(EAP-FAST)

MAC地址验证能也建立隧道到一个外部认证服务器或列表本地到WDS AP。WLSM不支持MAC地址验证。

WDS和基础设施APs在称为WLAN上下文控制协议的组播协议沟通(WLCCP)。这些组播消息不可能路由，因此WDS和相关的基础设施APs必须在同一个IP子网和在同一LAN段。在WDS和WLSE，

WLCCP在端口2887的用途TCP和用户数据报协议(UDP)之间。当WDS和WLSE在不同的子网时，一个协议类似网络地址转换(NAT)不能转换信息包。

作为WDS设备支持被配置的AP至60参与的APs。作为WDS设备支持(ISR)被配置的集成业务路由器至100参与的APs。并且一台WLSM被装备的交换机支持600参与的APs和240移动组。单个AP支持16移动组。

Note: Cisco建议基础设施APs运行IOS版本和WDS设备一样。如果使用IOS早版本， APs也许不能验证到WDS设备。另外， Cisco建议您使用IOS的新版本。您能找到IOS新版本在无线下载页的。

WDS设备的角色

WDS设备执行在您的无线局域网的几项任务：

- 通知其WDS功能并且参加选择您的无线局域网的最佳的WDS设备。当您配置您的WDS的时无线局域网，您设置一个设备作为主要WDS候选和一个或更多另外的设备作为备份的WDS候选。如果主要WDS设备脱机，其中一个备份的WDS设备采取其地方。
- 验证在子网的所有APs并且设立有每一个的安全通信通信通道。
- 从在子网的APs收集无线电数据，聚集数据，并且寄它给在您的网络的WLSE设备。
- 作为所有802.1X验证的客户端设备的转接被关联对参与的APs。
- 注册使用动态密钥在子网的所有客户端设备，设立他们的对话键，并且缓存他们的安全证件。当客户端漫游对另一个AP时， WDS设备转发客户端的安全证件到新的AP。

接入点的角色使用WDS设备

在您的无线局域网的APs与在这些活动的WDS设备呼应：

- 发现并且跟踪当前WDS设备和中继WDS广告对无线局域网。
- 用WDS设备验证并且设立安全通信通信通道到WDS设备。
- 注册相关的客户端设备用WDS设备。
- 无线电数据向WDS设备报告。

配置

WDS在一个被定购的，模块化方式呈现配置。在先于的概念的每个概念修造。WDS为了清晰省略其他配置条目例如密码、远程访问和在核心主题的无线电设置和重点。

此部分引见必要的信息配置在本文描述的功能。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

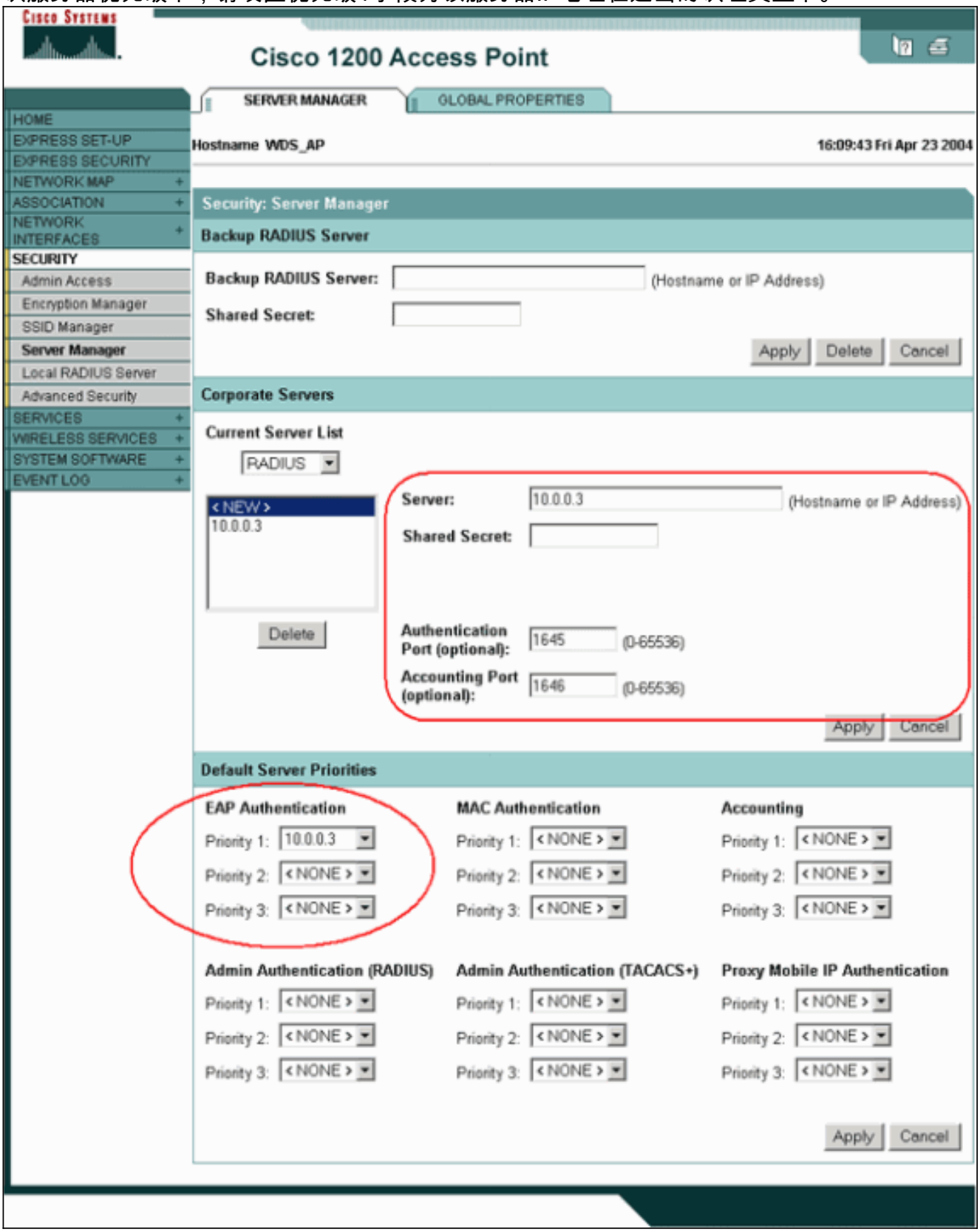
选定AP作为WDS

第一步将选定AP作为WDS。WDS AP是与认证服务器联络的只那个。

完成这些步骤为了选定AP作为WDS ：

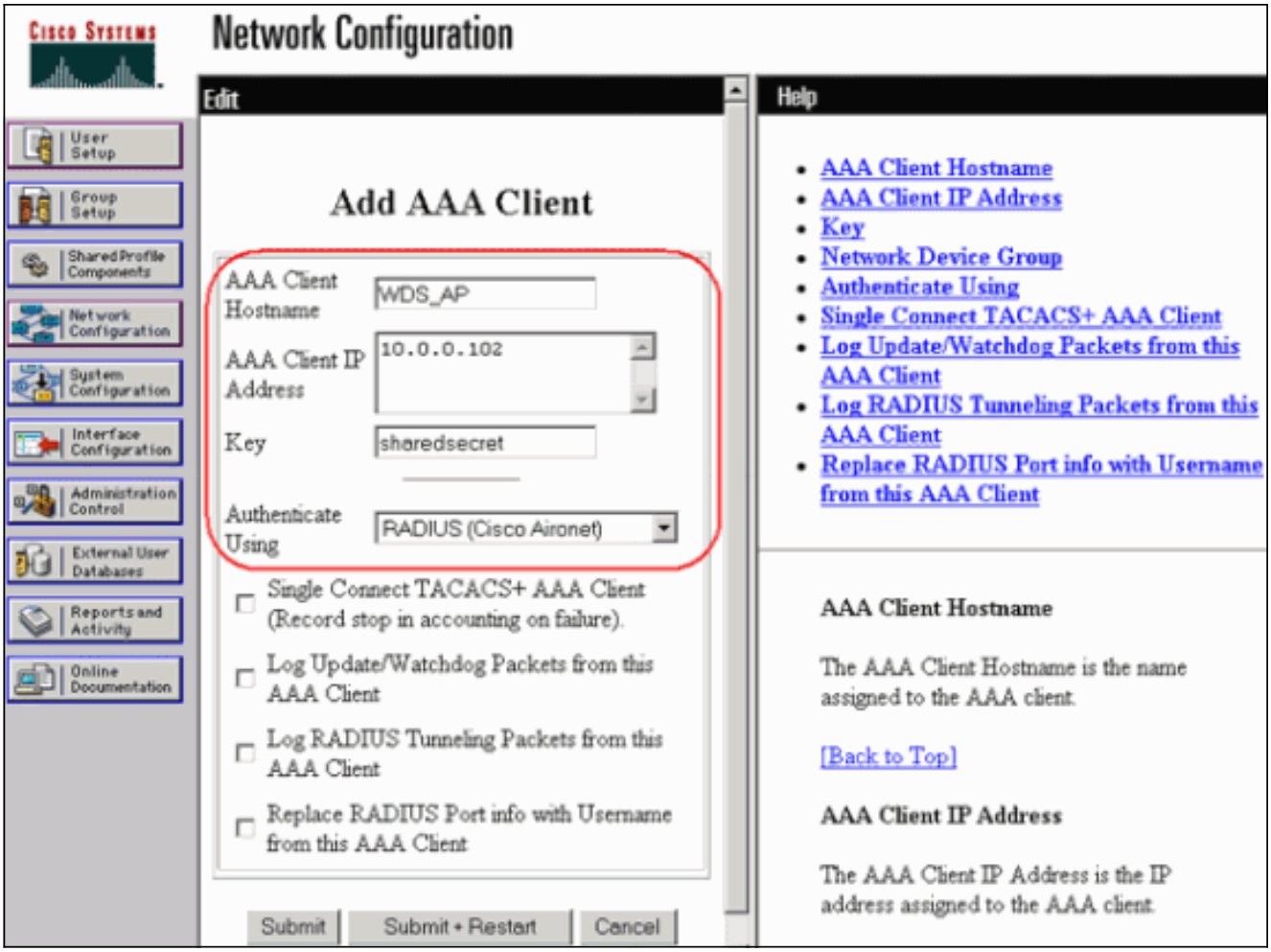
1. 为了配置在WDS AP的认证服务器，请选择**安全>Server管理器**去Server Manager选项：在公

司服务器下，请键入认证服务器的IP地址在服务器领域的。指定 Shared Secret 和端口。在默认服务器优先级下，请设置优先级1字段为该服务器IP地址在适当的认证类型下。

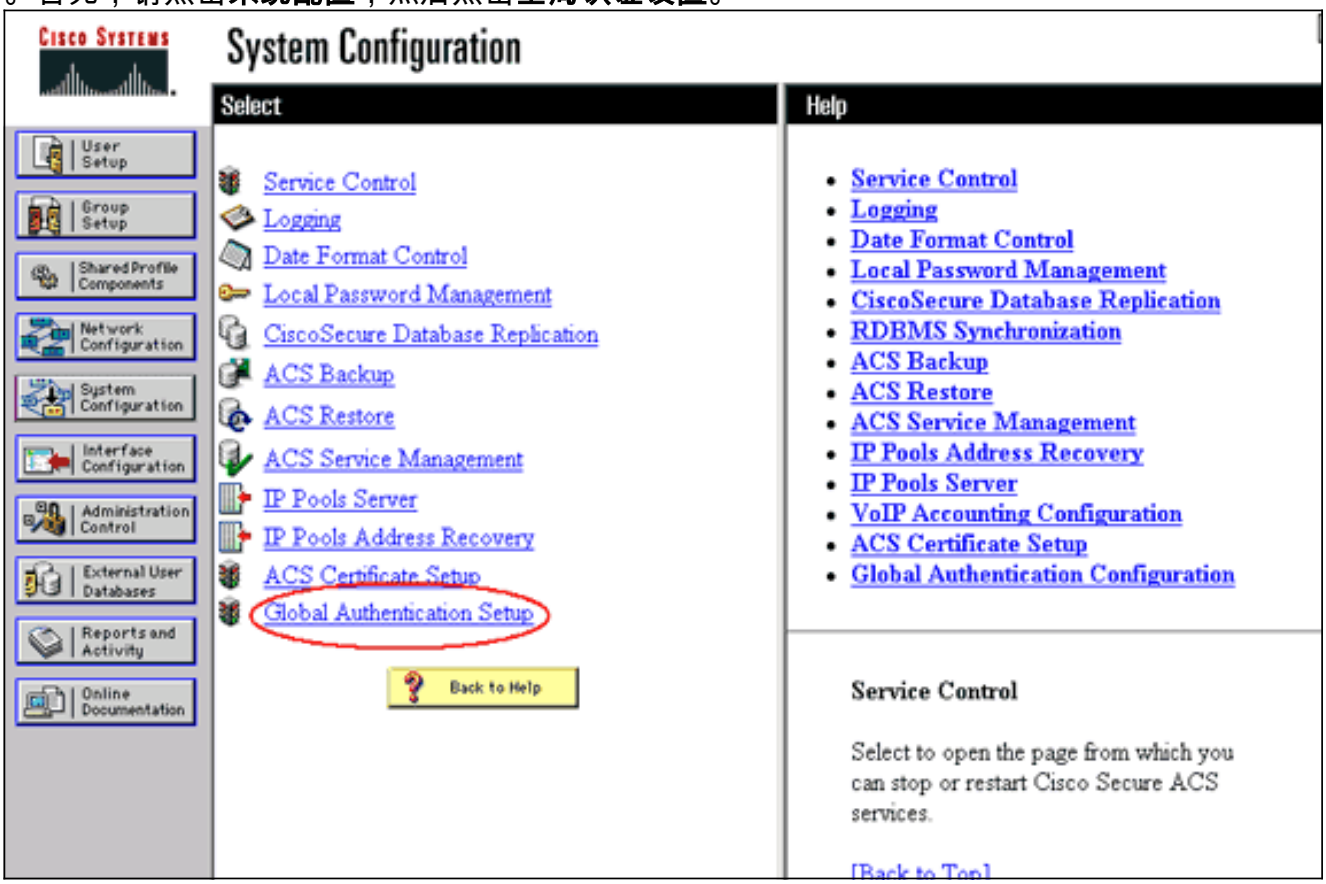


或者，请发出从CLI的这些命令：

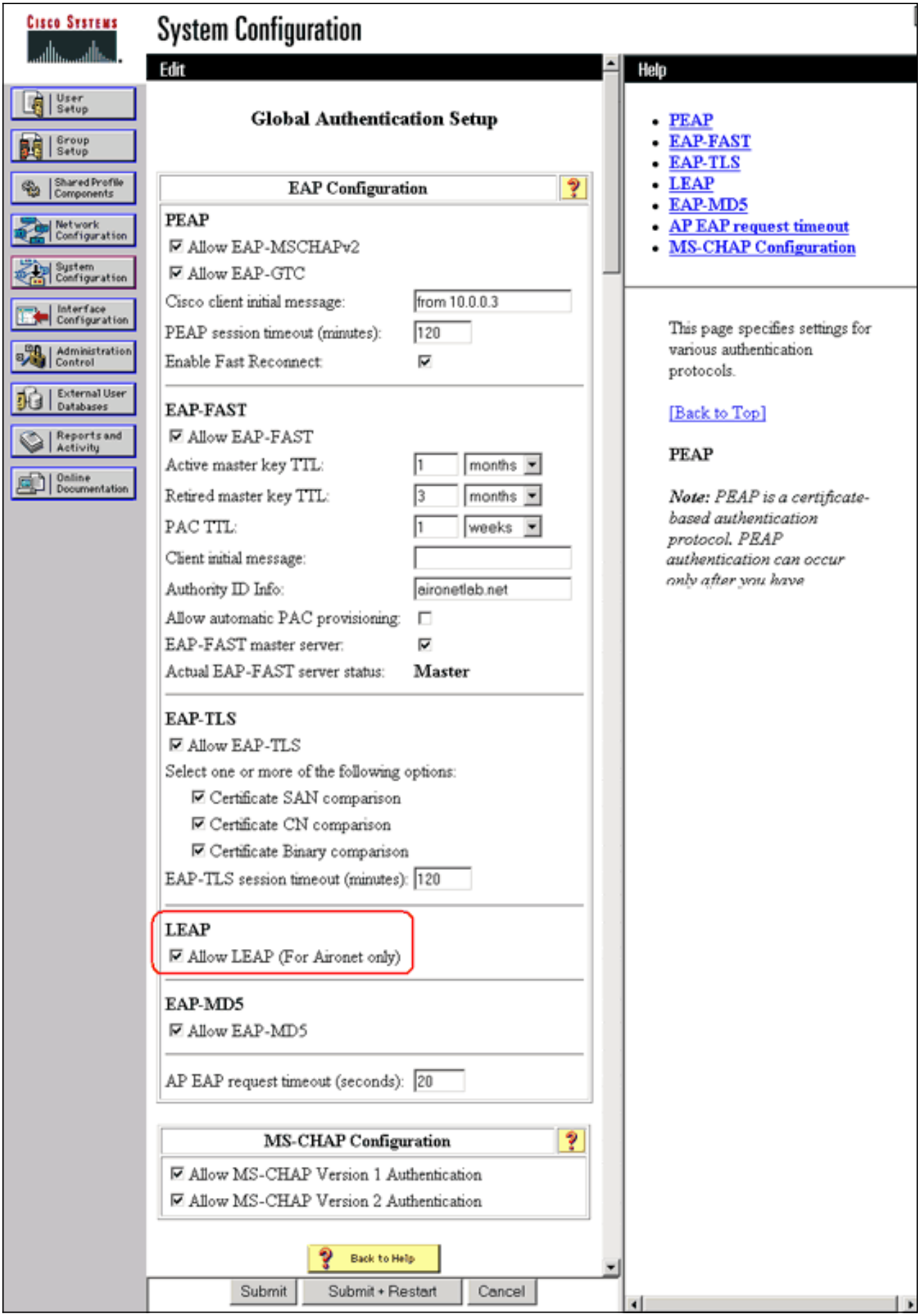
2. 下一步是配置在认证服务器的WDS AP作为验证、授权和统计(AAA)客户端。对于此，您需要添加WDS AP作为AAA客户端。完成这些步骤：**Note:** 本文使用Cisco Secure ACS服务器作为认证服务器。在思科安全访问控制服务器(ACS)中，这在您定义了WDS AP的这些属性的Network Configuration页发生：名字IP地址共有的秘密认证方法RADIUS Cisco AironetRADIUS互联网工程任务组[IETF]点击**提交**。关于其他非ACS认证服务器，请参见从制造商的文档。



并且，在Cisco Secure ACS，请保证您配置ACS进行在系统配置的LEAP认证-全局认证设置页。首先，请点击**系统配置**，然后点击**全局认证设置**。



把页移下来到LEAP设置。当您检查机箱时， ACS验证LEAP。

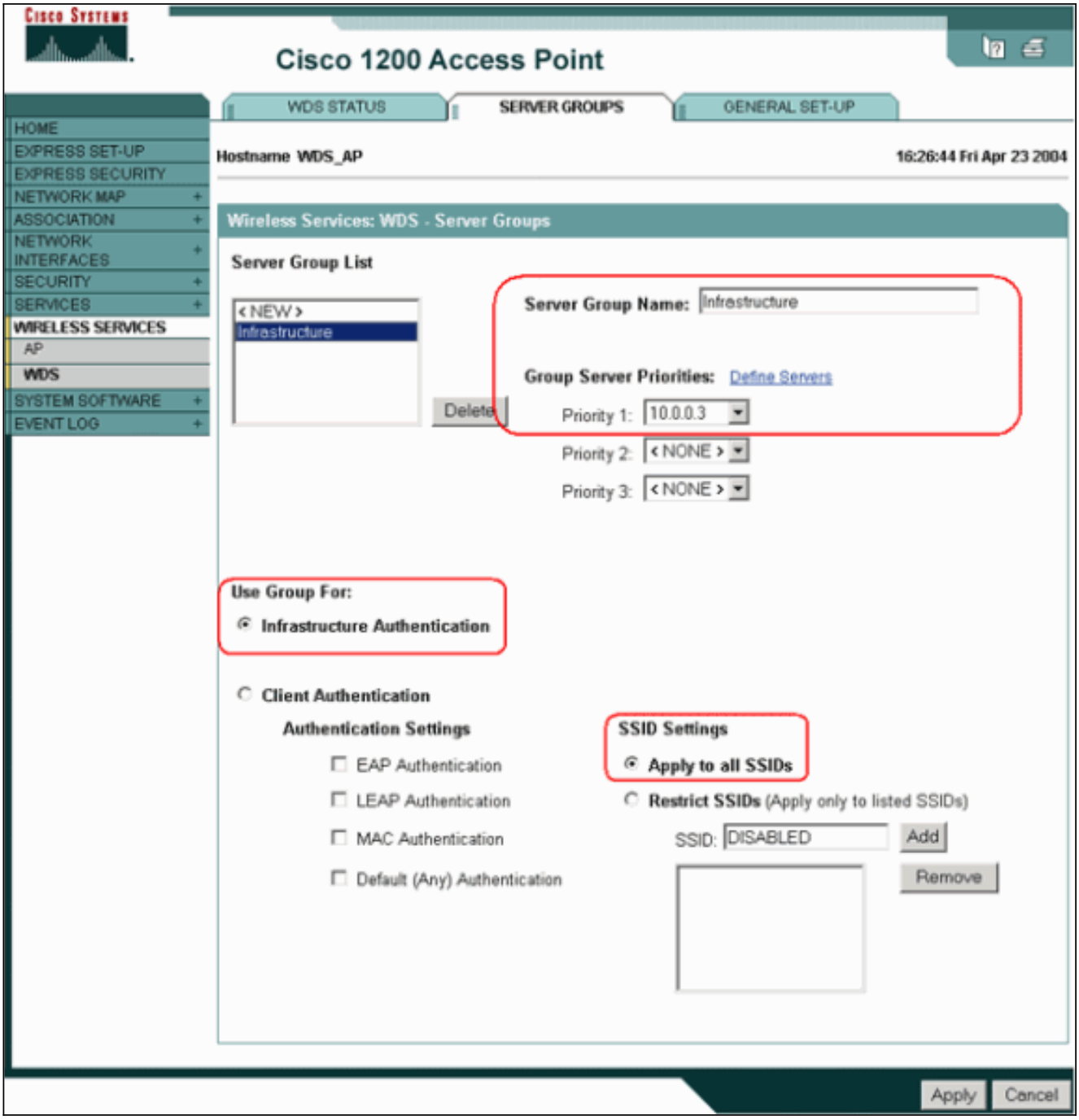


3. 为了配置在WDS AP的WDS setttings，请选择在WDS AP的**无线服务> WDS**，并且点击**一般设置**选项。执行这些步骤：在WDS无线域服务下-全局属性，检查**使用此AP作为无线域服务**。因为这是第一个，设置无线域服务优先级字段的值为值为大约**254**。您能配置一个或更多

APs或交换机作为提供WDS的候选。有最高优先级的提供WDS的设备。

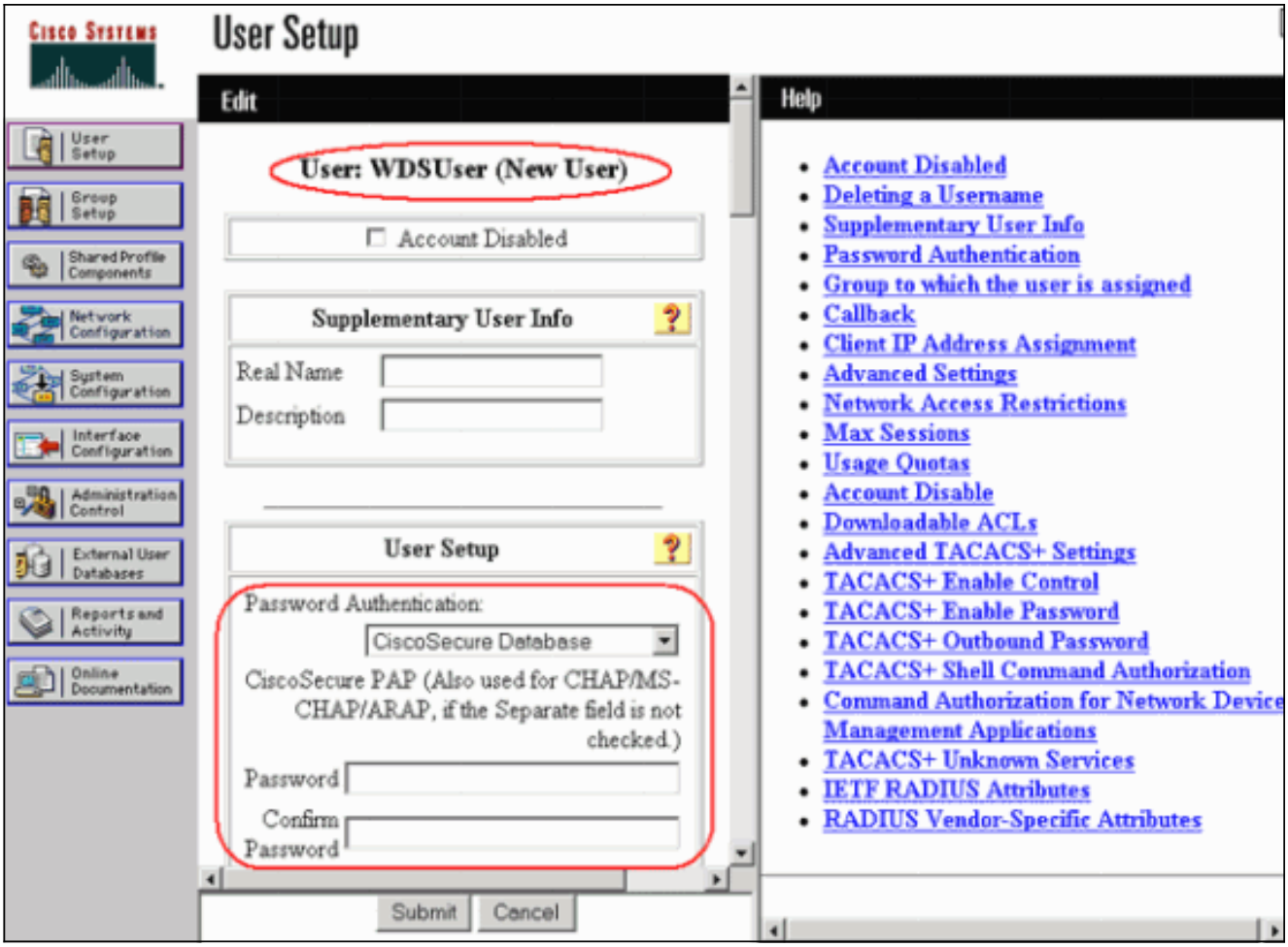
或者，请发出从CLI的这些命令：

4. 选择**无线服务> WDS**，并且去**Server Groups选项**：定义验证另一个APs的服务器组组名，基础设施组。设置优先权1为早先配置的认证服务器。点击**使用组为：基础设施认证**单选按钮。应用设置于相关服务集标识(Ssid)。



或者，请发出从CLI的这些命令：

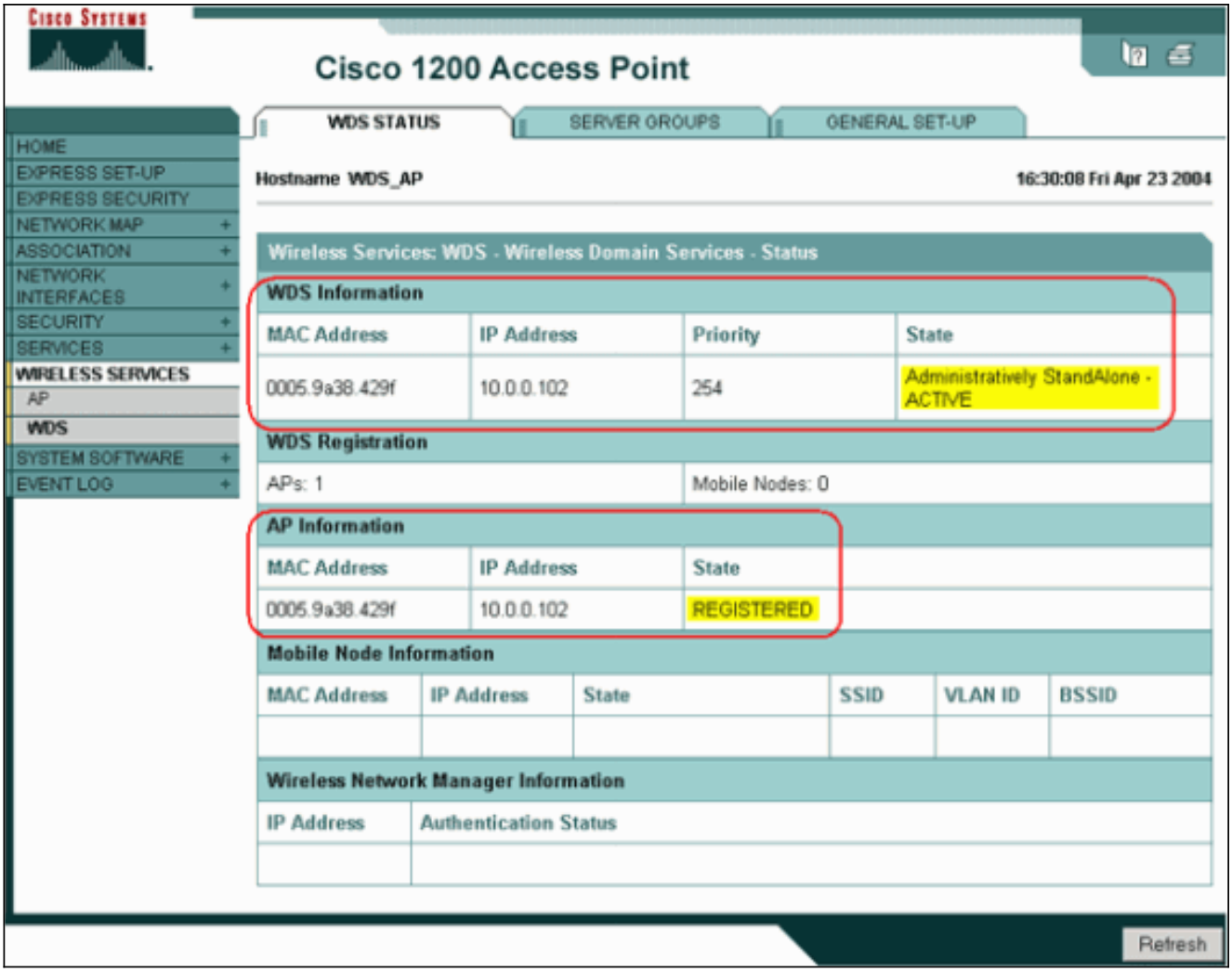
5. 配置WDS用户名和密码作为您的认证服务器的一个用户。在Cisco Secure ACS，这在User Setup页发生，您定义了WDS用户名和密码。关于其他非ACS认证服务器，请参见从制造商的文档。**Note:** 请勿放置WDS用户在分配许多权利和权限—的组WDS只要求有限的认证。



6. 选择**无线服务> AP**，并且点击参加的**Enable (event)** SWAN基础设施选项。然后请键入WDS用户名和密码。您必须定义一个WDS用户名和密码在认证服务器所有设备的您选定WDS的成员。

或者，请发出从CLI的这些命令：

7. 选择**无线服务> WDS**。在WDS AP WDS Status选项，检查WDS AP是否在WDS信息地区出现，在激活状态。AP在AP信息地区必须也出现，以状态如注册。如果AP不看上去注册或活动，请检查认证服务器所有错误或失败的认证尝试。当AP适当地时注册，请添加基础设施AP使用WDS的服务。



或者，请发出从CLI的这些命令：**Note:** 因为客户端验证没有提供，您不能测试客户端关联。

选定WLSM作为WDS

此部分说明如何配置WLSM作为WDS。WDS是与认证服务器联络的唯一的设备。

Note: 发出这些at命令WLSM的`enable`提示，不Supervisor引擎720。为了达到WLSM的prompt命令，请发出这些at命令在Supervisor引擎720的一个`enable`提示：

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

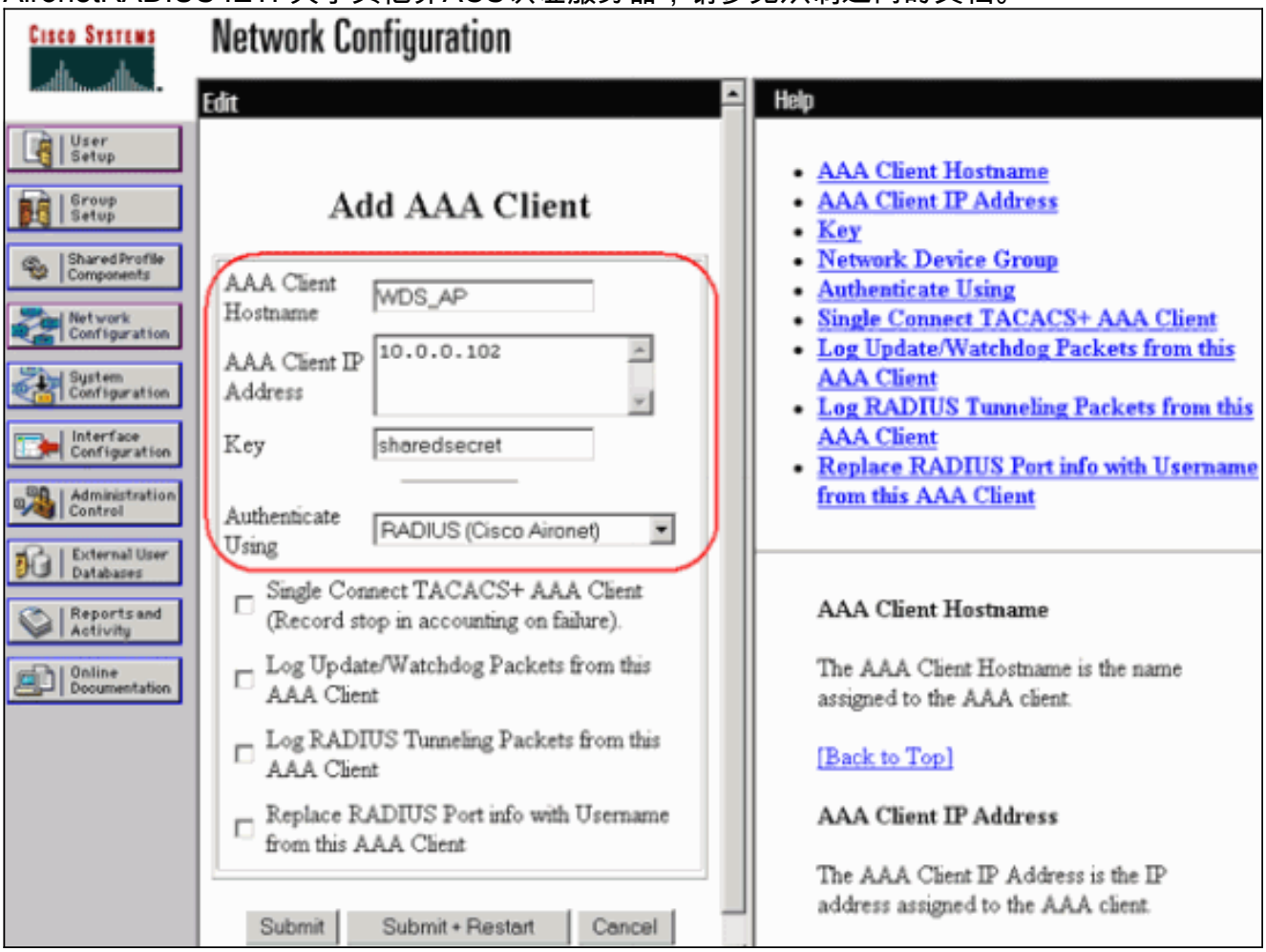
Note: 为了更加容易地排除和维护您的WLSM故障，请配置对WLSM的Telnet远程访问。参考配置Telnet远程访问。

为了选定WLSM作为WDS ：

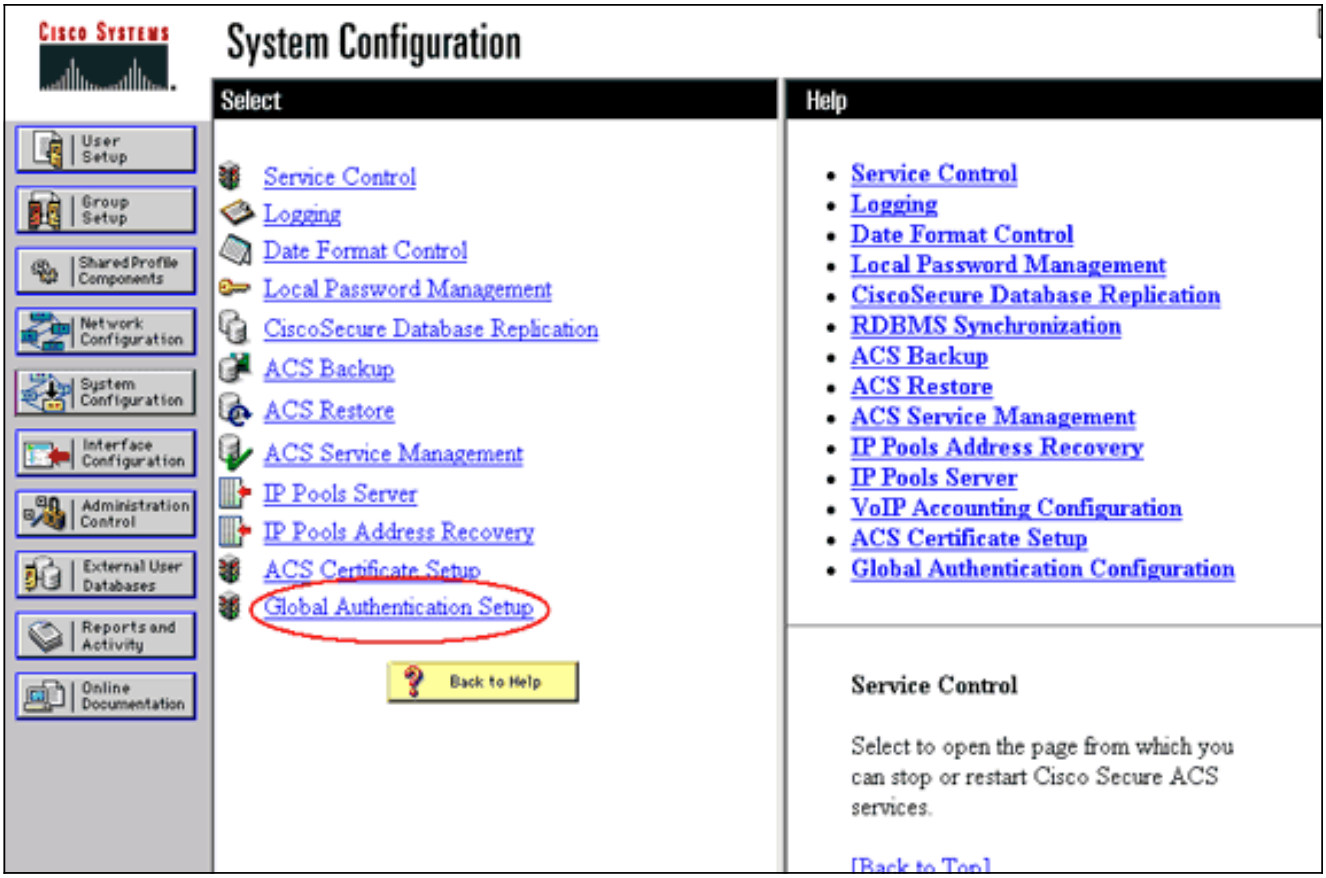
1. 从WLSM的CLI，请发出这些命令，并且建立与认证服务器的一个关系：**Note:** 没有在WLSM的

优先级控制。如果网络包含多个WLSM模块， WLSM使用冗余配置为了确定主要的模块。

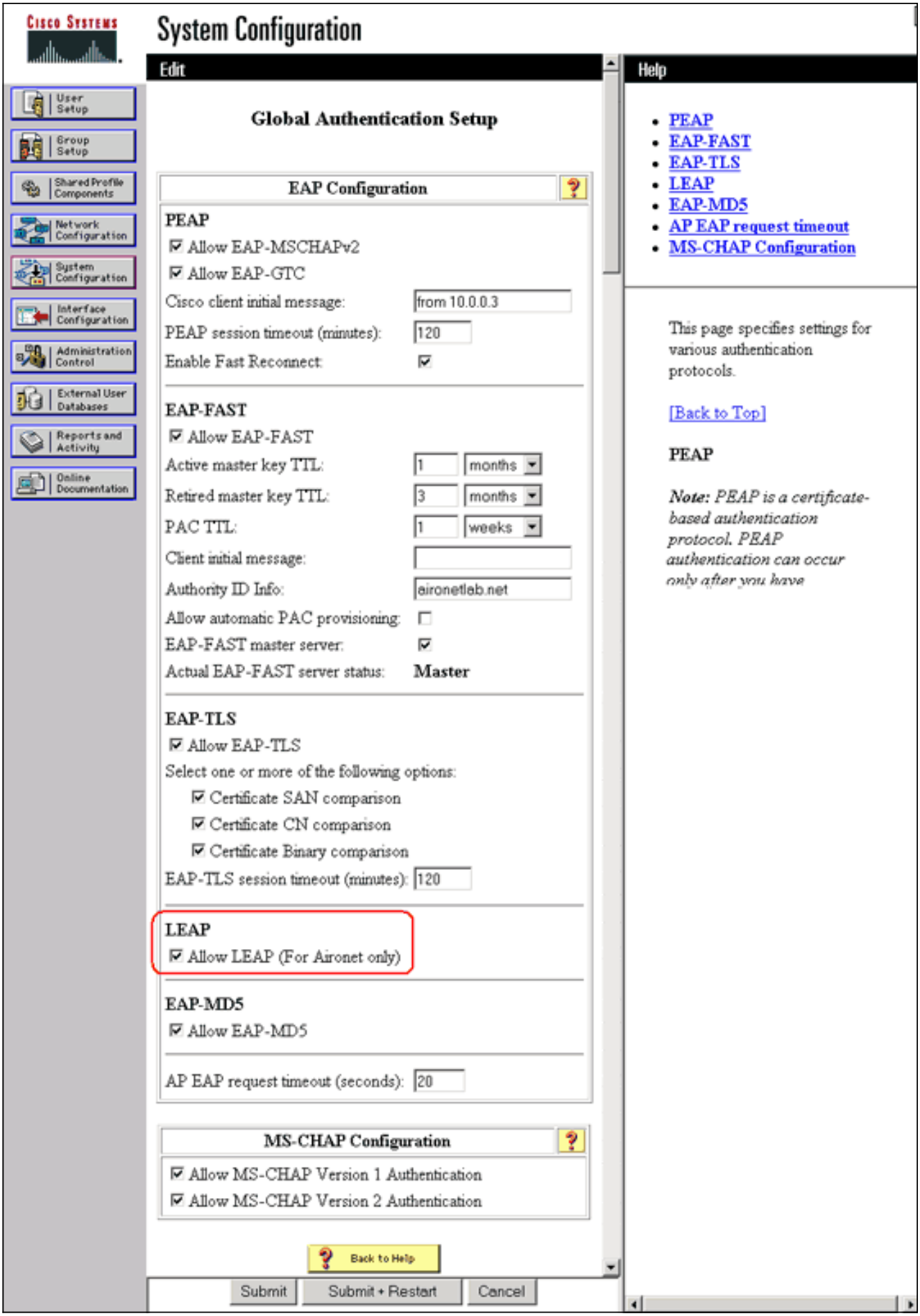
2. 配置在认证服务器的WLSM作为AAA客户端。在Cisco Secure ACS，这在您定义了WLSM的这些属性的Network Configuration页发生：名字IP地址共有的秘密认证方法RADIUS Cisco AironetRADIUS IETF关于其他非ACS认证服务器，请参见从制造商的文档。



并且，在Cisco Secure ACS，请配置ACS进行在系统配置的LEAP认证-全局认证设置页。首先，请点击**系统配置**，然后点击**全局认证设置**。



把页移下来到LEAP设置。当您检查机箱时，ACS验证LEAP。



3. 在WLSM，请定义验证另一个APs的一个方法(基础设施服务器组)。
4. 在WLSM，请定义验证客户端设备的一个方法(客户端服务器组)，并且什么EAP键入那些客户端使用。**Note:** 此步骤排除对定义客户端验证方法进程的需要。

5. 定义在Supervisor引擎720和WLSM之间的一唯一的VLAN为了允许WLSM沟通以外部实体类似APs和认证服务器。此VLAN是未使用的别处或为在网络的其他目的。首先创建在Supervisor引擎720的VLAN，然后发出这些命令：在 Supervisor 引擎 720 上：在WLSM ：
6. 验证WLSM的功能用这些命令：在WLSM ：在 Supervisor 引擎 720 上：

选定AP作为基础设施设备

其次，您必须选定至少一个基础设施AP和与WDS涉及AP。客户端联合对基础设施APs。基础设施APs请求WDS AP或WLSM进行他们的认证。

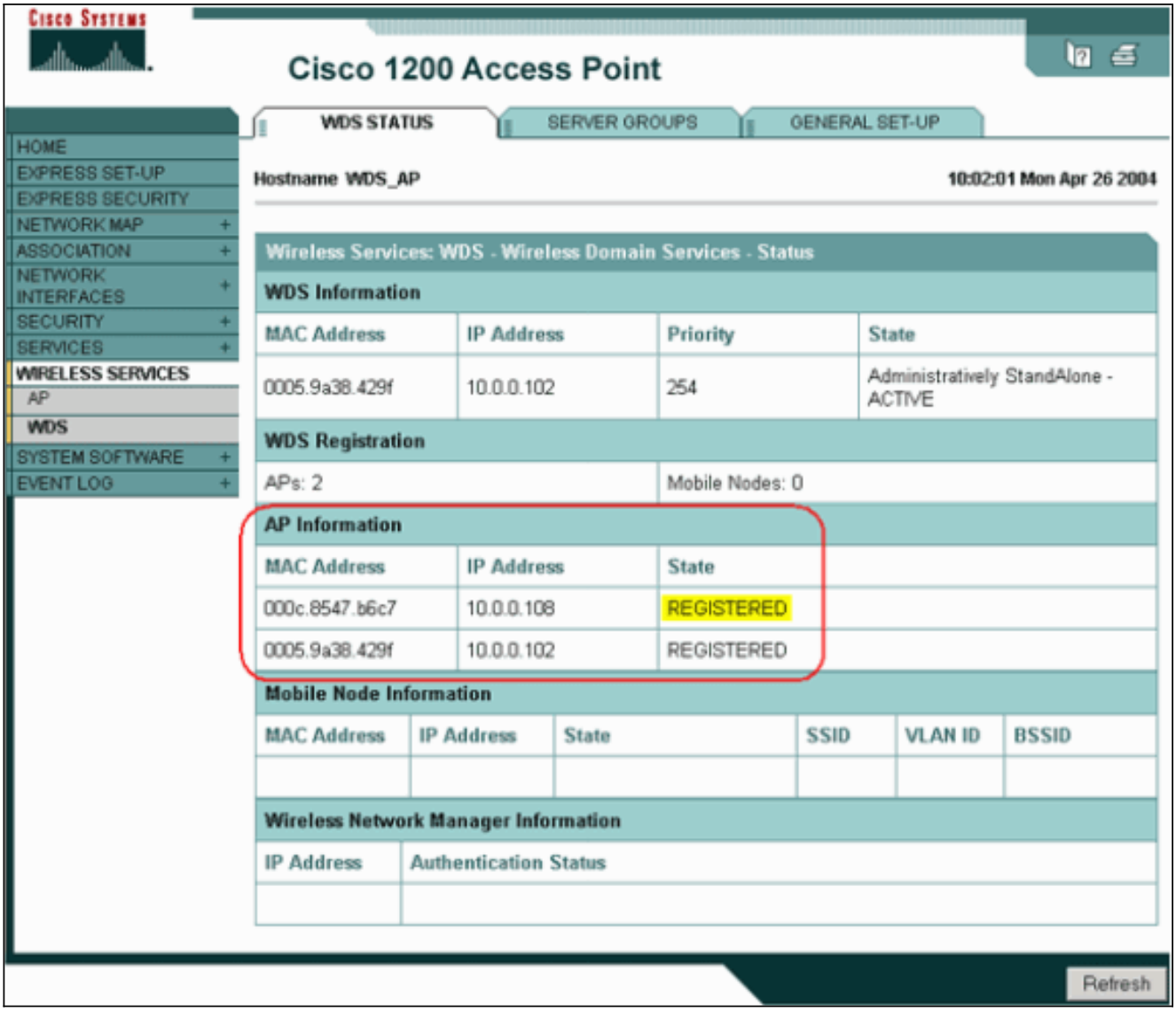
完成这些步骤为了添加使用WDS的服务的基础设施AP ：

Note: 此配置仅适用于基础设施APs而不是WDS AP。

1. 选择**无线服务> AP**。在基础设施AP，为Wireless Services选项请选择**Enable (event)**。然后请键入WDS用户名和密码。您必须定义一个WDS用户名和密码在认证服务器是WDS的成员的所有设备的。

或者，请发出从CLI的这些命令：

2. 选择**无线服务> WDS**。在WDS AP WDS Status选项，新的基础设施AP出现在WDS信息地区，以状态一样活动和在AP信息地区，以状态象注册。如果AP不看上去活动并且/或者注册，请检查认证服务器所有错误或失败的认证尝试。在AP看上去活动并且/或者注册后，请添加一个客户端验证方法到WDS。



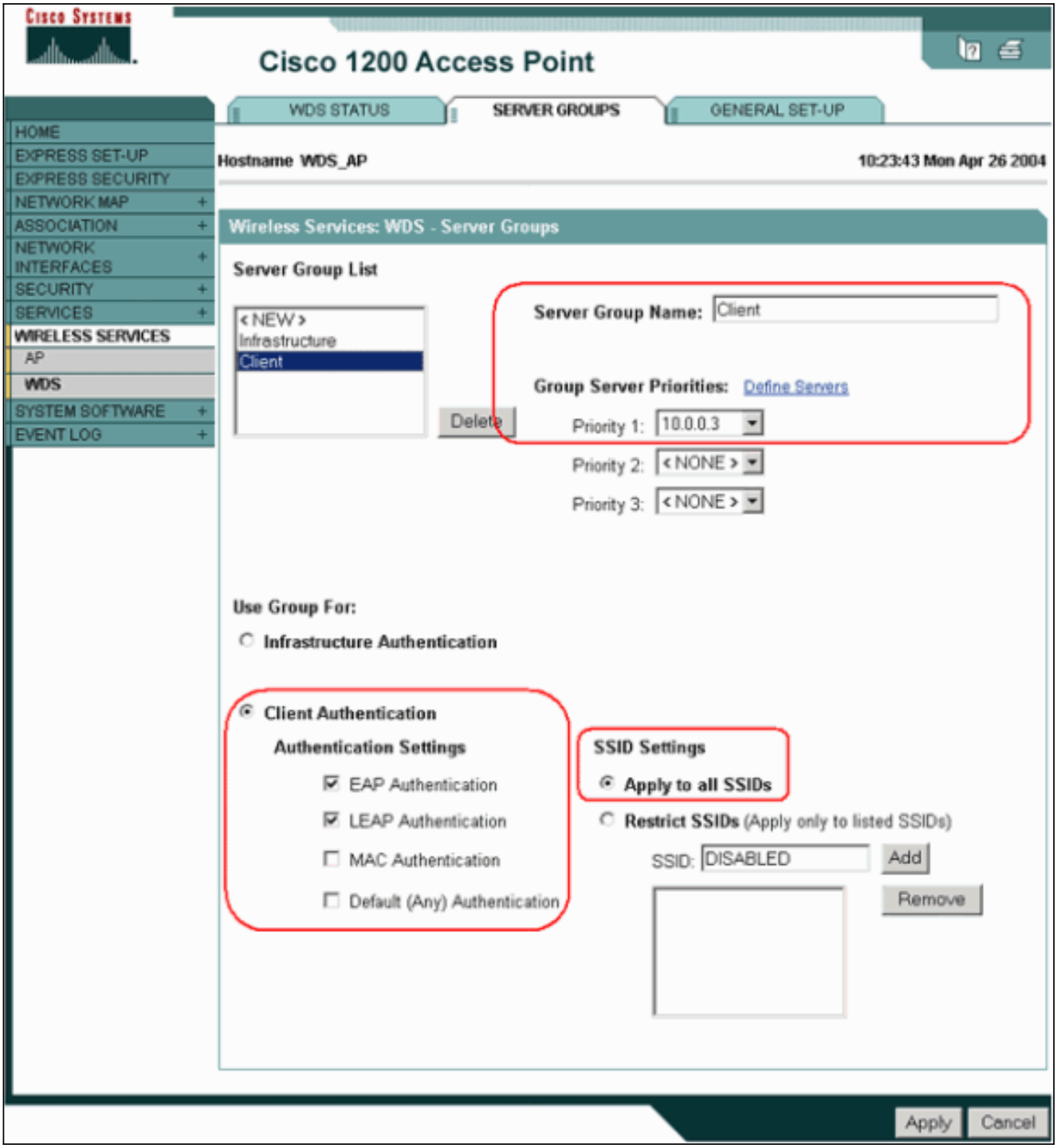
或者，请发出从CLI的此命令：或者，请发出从WLSM的此命令：然后，请发出此on命令基础设施AP ：**Note:** 因为客户端验证没有提供，您不能测试客户端关联。

定义客户端验证方法

最后，请定义客户端验证方法。

完成这些步骤为了添加客户端验证方法：

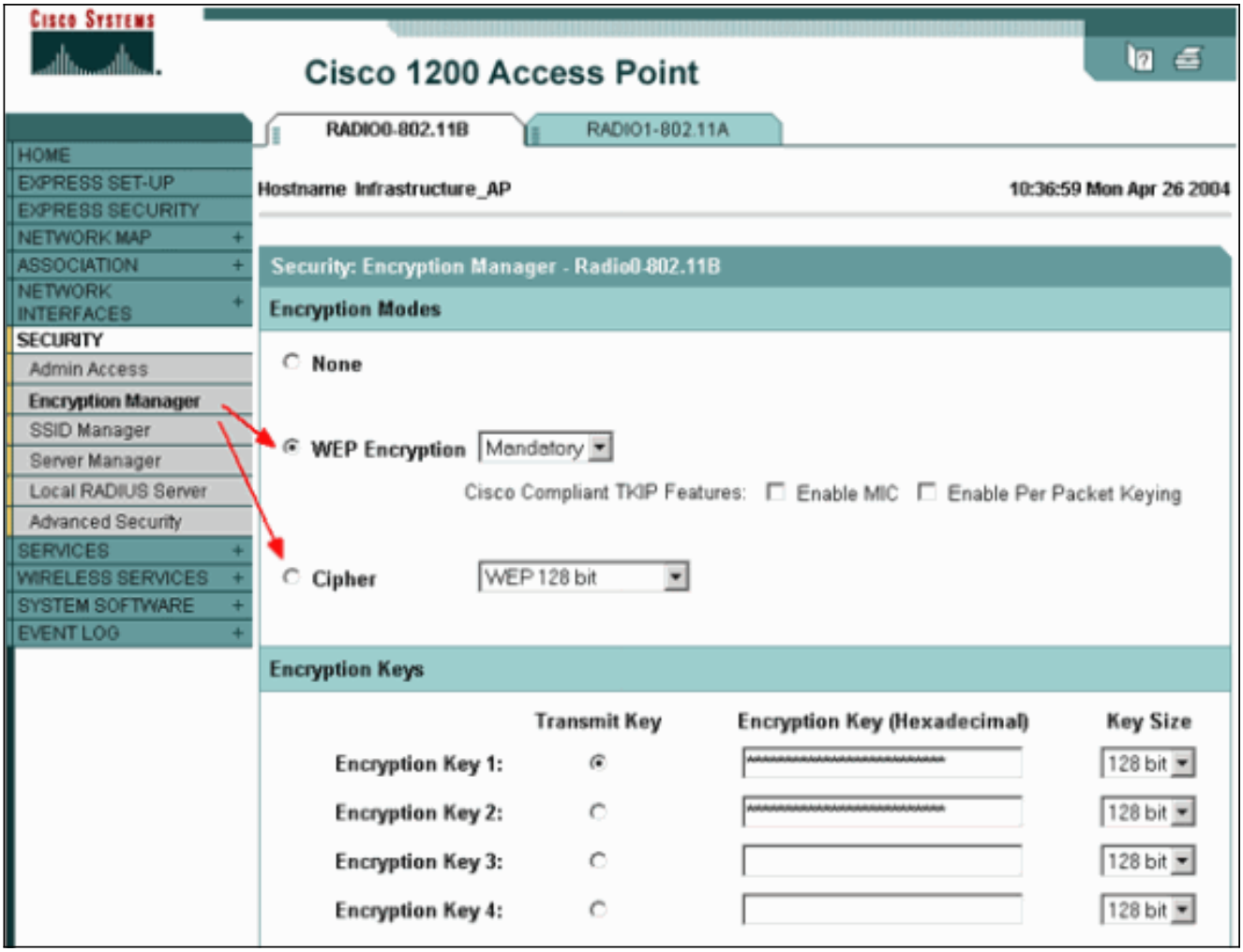
1. 选择**无线服务> WDS**。执行在WDS AP Server Groups选项的这些步骤：定义验证客户端的一个服务器组(客户端组)。设置优先权1为早先配置的认证服务器。设置认证(LEAP的可适用的类型， EAP， MAC，等等)。应用设置于相关Ssid。



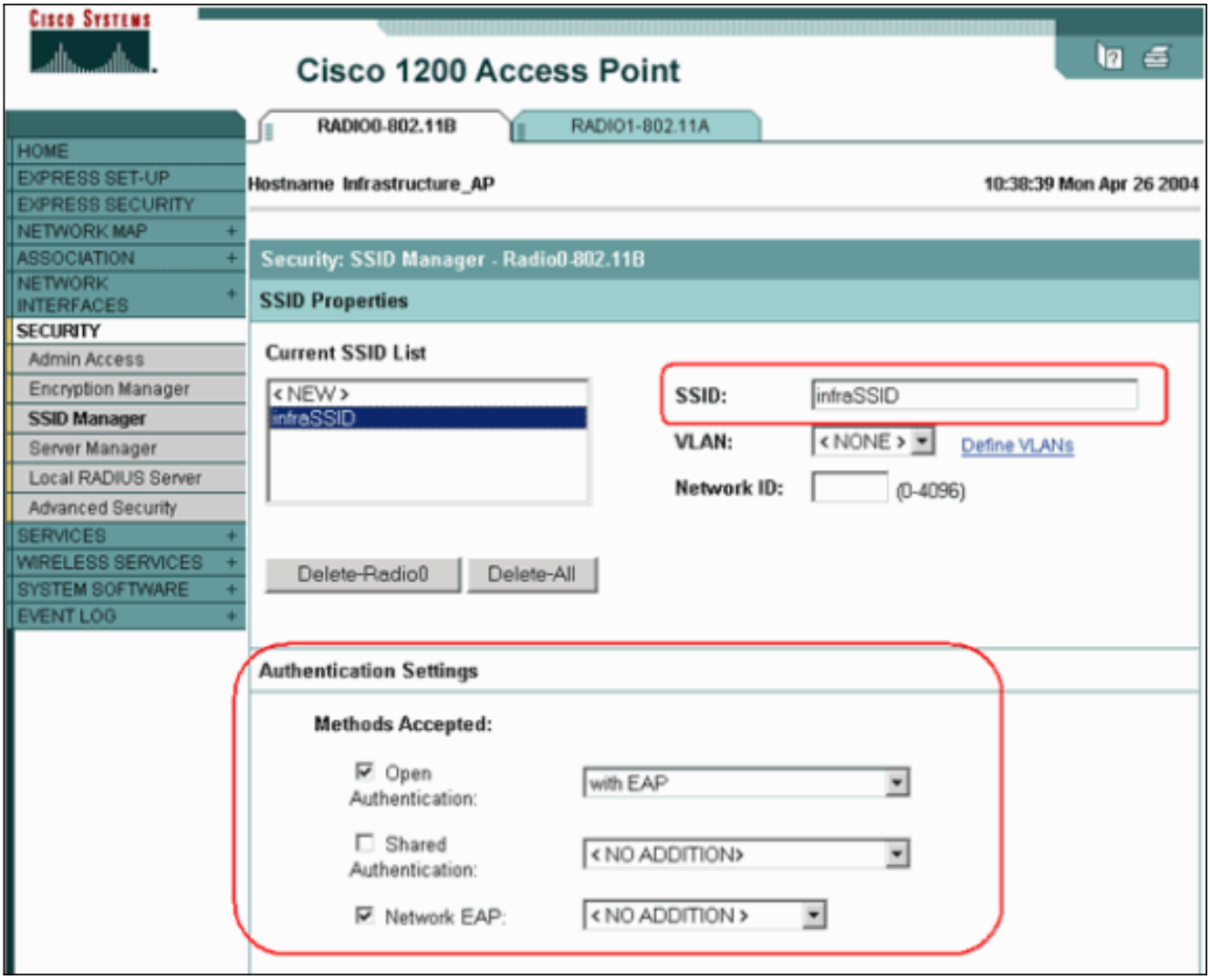
或者，请发出从CLI的这些命令：**Note:** 示例WDS AP是专用的，并且不接受客户端关联。

Note: 因为基础设施APs寄所有请求给WDS被处理，请勿配置在服务器组的基础设施APs。

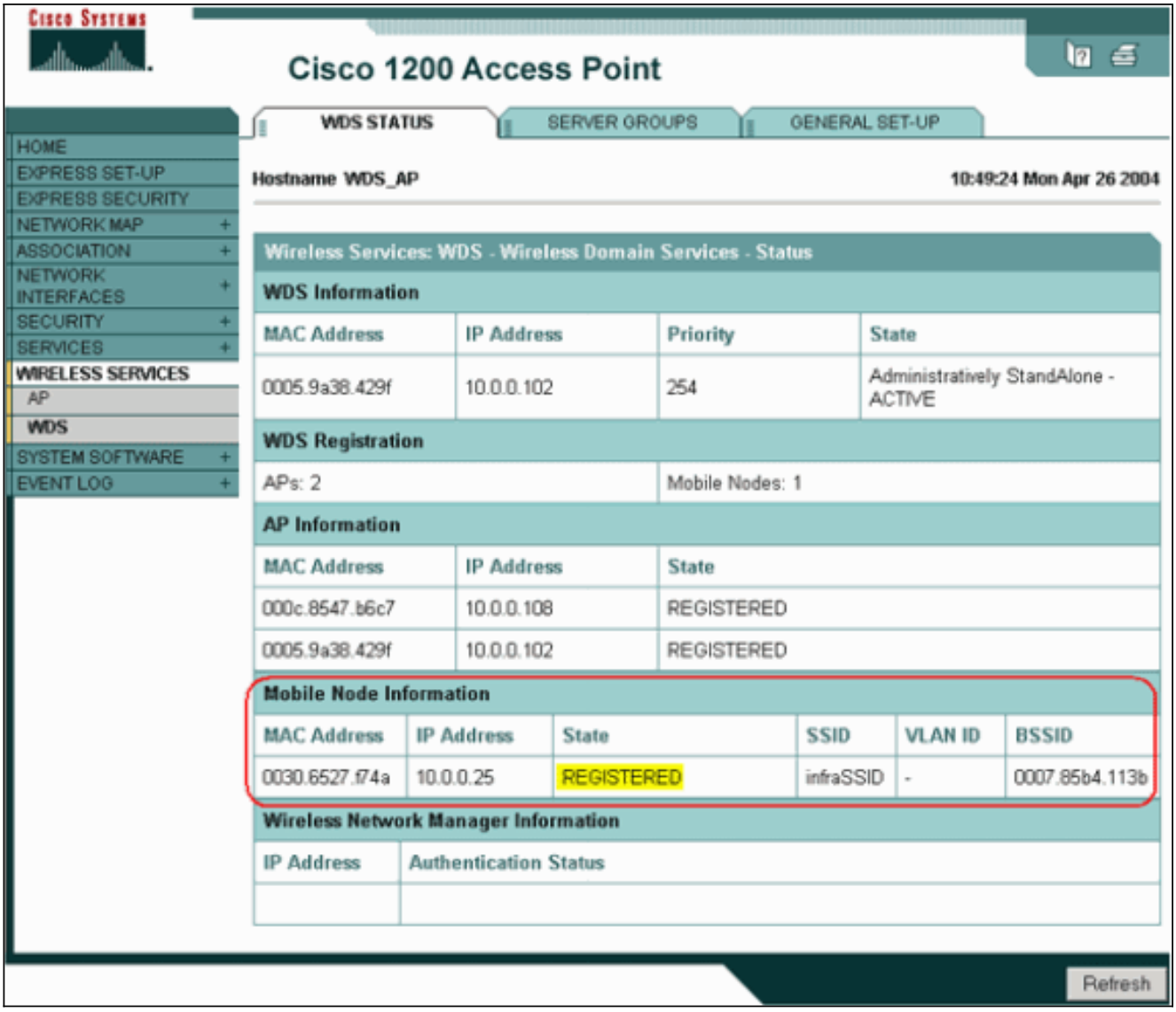
2. 在基础设施AP或APs ：在**安全>加密管理器**菜单项下，请点击**WEP加密**或据您使用的认证协议要求**加密**。



在**安全> SSID管理器**菜单项下，据您使用的认证协议要求的挑选认证方法。



3. 您能成功当前测试客户端是否验证对基础设施APs。WDS的AP在WDS Status选项的(在**无线服务> WDS**菜单项下)表明客户端在移动节点信息地区出现并且有一个注册的状态。如果客户端没出现，请检查认证服务器所有错误或失败的认证尝试由客户端。



或者，请发出从CLI的这些命令：**Note:** 如果需要debug authentication，请保证您在WDS AP调试，因为WDS AP是与认证服务器联络的设备。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

此部分提供您能使用排除您的配置故障的信息。此列表显示某些常见问题与WDS命令有关为了进一步澄清这些命令的实用性：

- **问题：在WDS AP，什么是这些项目的推荐的设置？RADIUS服务器超时RADIUS服务器deadtime临时密钥完整性协议(TKIP) Message Integrity Check (MIC)故障Holdoff时间客户端Holdoff时间EAP或MAC再验证间隔EAP客户机超时(可选)答案：**被建议您保持与默认设置的配置关于这些特殊设置和只使用他们，当有关于定时时的一个问题。这些是WDS AP的推荐的设置：功能失效**RADIUS服务器超时**。这是AP等待给RADIUS请求的一个回复秒钟的数量，在再发出请求前。默认值是5秒。功能失效**RADIUS服务器deadtime**。除非所有服务器被标记得死，RADIUS由另外的要求跳过分钟的期限。默认情况下TKIP MIC故障Holdoff时间被启用对60秒。如果enable (event) holdoff时间，您能以秒钟输入间隔。如果AP在60秒以内发现两个MIC故障

，阻拦该接口的所有TKIP客户端指定的holdoff时间的这里。默认情况下客户端应该禁用Holdoff时间。如果enable (event) holdoff，输入AP应该等秒钟的数量，在随后的认证请求前的认证失败被处理后。默认情况下EAP或MAC再验证间隔被禁用。如果enable (event)再验证，您能指定间隔或接受认证服务器产生的间隔。如果选择指定间隔，请以AP等的秒钟输入间隔，在迫使一个验证的客户端重新鉴别前。EAP客户机超时(可选)默认情况下是120秒。输入AP应该等待无线客户端回答EAP认证请求的时间。

- **问题：关于TKIP holdoff时间，我读应该设置这为100毫秒和没有60秒。我假设它设置为从浏览器的一秒钟，因为那是您能精选的低数值？答案：**没有特定推荐设置它为100毫秒，除非有报告的故障唯一的解决方案将增加这次的地方。一秒钟是最低的设置。
- **问题：这两help命令客户端验证在任何情况下，并且他们是否是需要的在WDS或基础设施AP？RADIUS服务器属性6在为洛金auth技术支持多个的RADIUS服务器属性6答案：**这些命令不帮助认证过程，并且他们在WDS或AP没有必要。
- **问题：在基础设施AP，我假设，服务器管理器都和全局属性设置不是需要的，因为AP从WDS获得信息。这些特定命令中的任一个为基础设施AP必要？RADIUS服务器属性6在为洛金auth技术支持多个的RADIUS服务器属性6RADIUS服务器超时RADIUS服务器deadtime答案**：没有需要有服务器管理器和全局属性基础设施的APs。WDS照料该任务，并且没有需要有这些设置：**RADIUS服务器属性6在为洛金auth技术支持多个的RADIUS服务器属性6RADIUS服务器超时RADIUS服务器deadtime**默认情况下**RADIUS服务器属性32包括在访问req格式%h**设置依然是和需要。

AP是第2层设备。所以，当配置AP作为WDS设备时， AP不支持第3层移动性。只有当您配置WLSM作为WDS设备时，您能达到第3层移动性。请参见Cisco Catalyst 6500 Series无线局域网服务模块的*第3层移动性体系结构*部分：白皮书欲知更多信息。

所以，当您配置AP作为WDS设备时，请勿使用**mobility network-id命令**。此命令适用于第3层移动性，并且您需要有WLSM，当您的WDS设备为了适当配置第3层移动性。如果不正确地使用**mobility network-id命令**，您能看到其中一些症状：

- 无线客户端无法与 AP 关联。
- 无线客户端能联合到AP，但是从DHCP服务器不收到IP地址。
- 当您有在WLAN部署时的一语音一个无线电话没有验证。
- EAP验证不出现。使用被配置的**移动性网络id**， AP设法构建通用路由封装(GRE)隧道转发EAP信息包。如果隧道没有设立，信息包任何地方不去。
- 作为WDS设备被配置的AP不作用正如所料，并且WDS配置不工作。**Note:** 您不能配置Cisco Aironet 1300 AP/bridge作为WDS主设备。1300 AP/bridge不支持此功能。1300 AP/bridge能参加WDS网络，当某个其他AP或WLSM被配置作为WDS主设备的基础设施设备。

故障排除命令

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。

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

- **调试全dot11 aaa的证明人**表示多种协商，客户端经历，当客户端通过802.1x或EAP进程联合并且验证。此调试在Cisco IOS Software Release 12.2(15)JA被引入。此命令废弃**debug dot11 aaa dot1x all**由于及以后版本。
- **debug aaa authentication** —显示认证过程从一个通用的AAA方面。
- **debug wlccp ap** —显示作为AP介入的WLCCP协商加入WDS。
- **debug wlccp packet** —显示关于WLCCP协商的详细信息。

- **调试wlccp LEAP客户端**—，当基础设施设备加入WDS，显示详细资料。

Related Information

- 配置WDS，快速地请巩固漫游和无线电管理
- Catalyst 6500 Series无线局域网服务模块配置注释
- 配置密码套件和WEP
- 配置身份验证类型
- 无线LAN支持页
- Technical Support & Documentation - Cisco Systems