无线域服务配置

目录

简介

本文档介绍 Wireless Domain Services (WDS) 的概念。 本文档还介绍如何将一个接入点 (AP) 或无线 LAN 服务模块 (WLSM) 配置为 WDS 以及将至少另一个配置为基础设施 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。本文档旨在使读者掌握基本的知识，了解如何配置快速安全漫游或将无线 LAN 解决方案引擎 (WLSE) 引入网络，从而使用其功能。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 全面了解无线 LAN 网络和无线安全问题。
- 了解最新可扩展的身份验证协议 (EAP) 安全方法。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 装有 Cisco IOS® 软件的 AP
- Cisco IOS 软件版本 12.3(2)JA2 或更高版本
- Catalyst 6500 系列无线 LAN 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。本文中用到的所有设备在接口BVI1上开始都有一个缺省（默认）配置和在接口BVI1上的IP地址，因此可以从Cisco IOS软件GUI或命令行界面(CLI)都可以访问设备。 如果使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

无线域服务

WDS 是 Cisco IOS 软件中的 AP 的新功能，也是 Catalyst 6500 系列 WLSM 的基础。WDS 是启用类似如下的其他特性的核心功能：

- 快速安全漫游
- WLSE 交互
- 无线电管理

您必须在参与 WDS 和 WLSM 的 AP 之间建立关系，其他任何基于 WDS 的功能才能起作用。WDS 的用途之一是使身份验证服务器不必验证用户凭据，并可缩短客户端身份验证所需要的时间。

为了使用 WDS，必须指定一个 AP 或 WLSM 作为 WDS。WDS AP 必须使用 WDS 用户名和密码才能与身份验证服务器建立关系。身份验证服务器可以是外部 RADIUS 服务器或 WDS AP 中的本地 RADIUS 服务器功能。WLSM 必须与身份验证服务器存在关系，即使 WLSM 不需要向该服务器验证身份。

其他 AP（称为基础设施 AP）可与 WDS 通信。在进行注册之前，基础设施 AP 必须向 WDS 进行身份验证。WDS 中的基础设施服务器组定义了此基础设施身份验证。

WDS 中的一个或多个客户端服务器组用于定义客户端身份验证。

当客户端尝试与基础设施 AP 关联时，基础设施 AP 会将用户的凭据传递给 WDS 进行验证。如果 WDS 第一次看到凭据，WDS 将转向身份验证服务器来验证凭据。然后 WDS 会缓存凭据，这样，当同一用户再次尝试身份验证时，便无需返回身份验证服务器。重新验证示例包括：

- 重新获取密钥
- 漫游
- 当用户启动客户端设备时

所有基于 RADIUS 的 EAP 验证协议均可通过 WDS 进行隧道传输，例如：

- 轻量 EAP (LEAP)
- 受保护的 EAP (PEAP)
- EAP 传输层安全 (EAP-TLS)
- 通过安全隧道的 EAP 灵活身份验证 (EAP-FAST)

MAC 地址验证还可通过隧道传输到外部身份验证服务器或 WDS AP 本地的列表。WLSM 不支持 MAC 地址验证。

WDS 和基础设施 AP 基于名为 WLAN 上下文控制协议 (WLCCP) 的组播协议进行通信。 这些组播

消息无法路由，因此 WDS 和关联的基础设施 AP 必须在同一 IP 子网和同一 LAN 网段中。在 WDS 和 WLSE 之间，WLCCP 在端口 2887 上使用 TCP 和用户数据报协议 (UDP)。当 WDS 和 WLSE 位于不同的子网中时，网络地址转换 (NAT) 之类的协议无法转换数据包。

配置为 WDS 设备的 AP 最多支持 60 个参与的 AP。配置为 WDS 设备的集成多业务路由器 (ISR) 最多支持 100 个参与的 AP。配备 WLSM 的交换机最多支持 600 个参与的 AP 和 240 个移动组。单个 AP 最多支持 16 个移动组。

注意：思科建议基础设施AP运行与WDS设备相同的IOS版本。如果使用 IOS 的早期版本，AP 可能无法向 WDS 设备验证身份。另外，Cisco 建议您使用 IOS 的最新版本。无线下载页提供了 IOS 的最新版本。

WDS 设备的角色

WDS 设备可在无线 LAN 中执行多个任务：

- 通告其 WDS 功能并参与为无线 LAN 选择最佳 WDS 设备。在为 WDS 配置无线 LAN 时，将一个设备设置为主要 WDS 候选，然后将一个或多个其他设备设置为备份 WDS 候选。如果主要 WDS 设备脱机，则由其中一个备份 WDS 设备替代它。
- 对子网中的所有 AP 进行验证并与每个 AP 均建立安全通信信道。
- 从子网中的 AP 收集无线数据，聚合数据，并将其转发给网络上的 WLSE 设备。
- 用作与参与的 AP 关联的所有 802.1x 已验证身份的客户端设备的穿透。
- 在使用动态密钥的子网中注册所有客户端设备，为其建立会话密钥，并缓存其安全凭据。当客户端漫游至另一个 AP 时，WDS 设备会将客户端的安全凭据转发给新 AP。

使用 WDS 设备的接入点的角色

无线 LAN 中的 AP 可在以下活动中与 WDS 设备交互：

- 发现并跟踪当前 WDS 设备并将 WDS 通告中继至无线 LAN。
- 对 WDS 设备进行身份验证并建立到 WDS 设备的安全通信信道。
- 注册与 WDS 设备关联的客户端设备。
- 向 WDS 设备报告无线数据。

配置

WDS 通过有序的模块化方式呈现配置。每个概念均以之前的概念为基础来建立。为了清晰并关注核心主题，WDS 会省略其他配置项，例如密码、远程访问和无线设置。

本部分提供配置本文档中介绍的功能所需的信息。

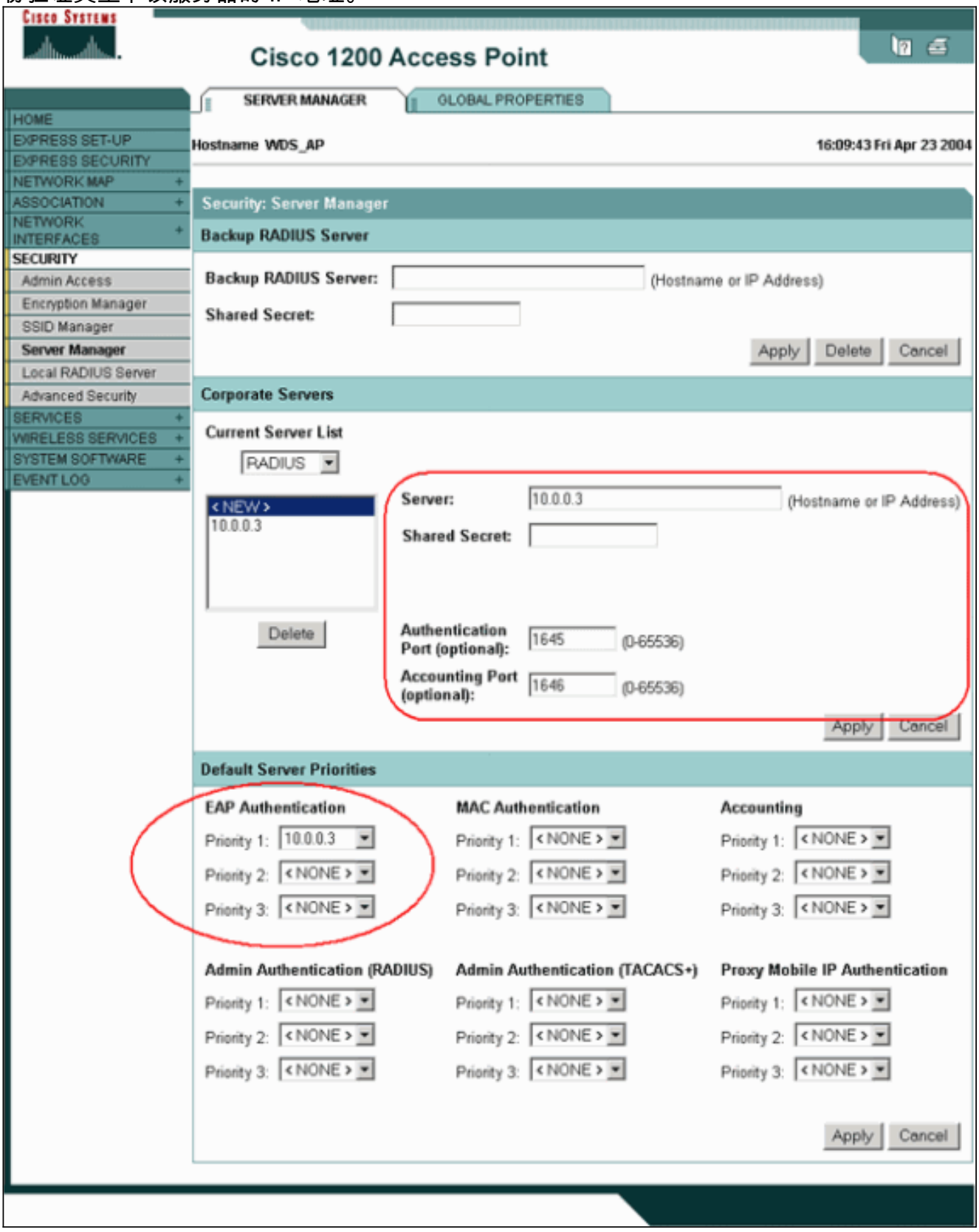
注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

指定 AP 作为 WDS

第一步是将一个 AP 指定为 WDS。WDS AP 是可与身份验证服务器通信的唯一一个 AP。

完成以下步骤，以将 AP 指定为 WDS：

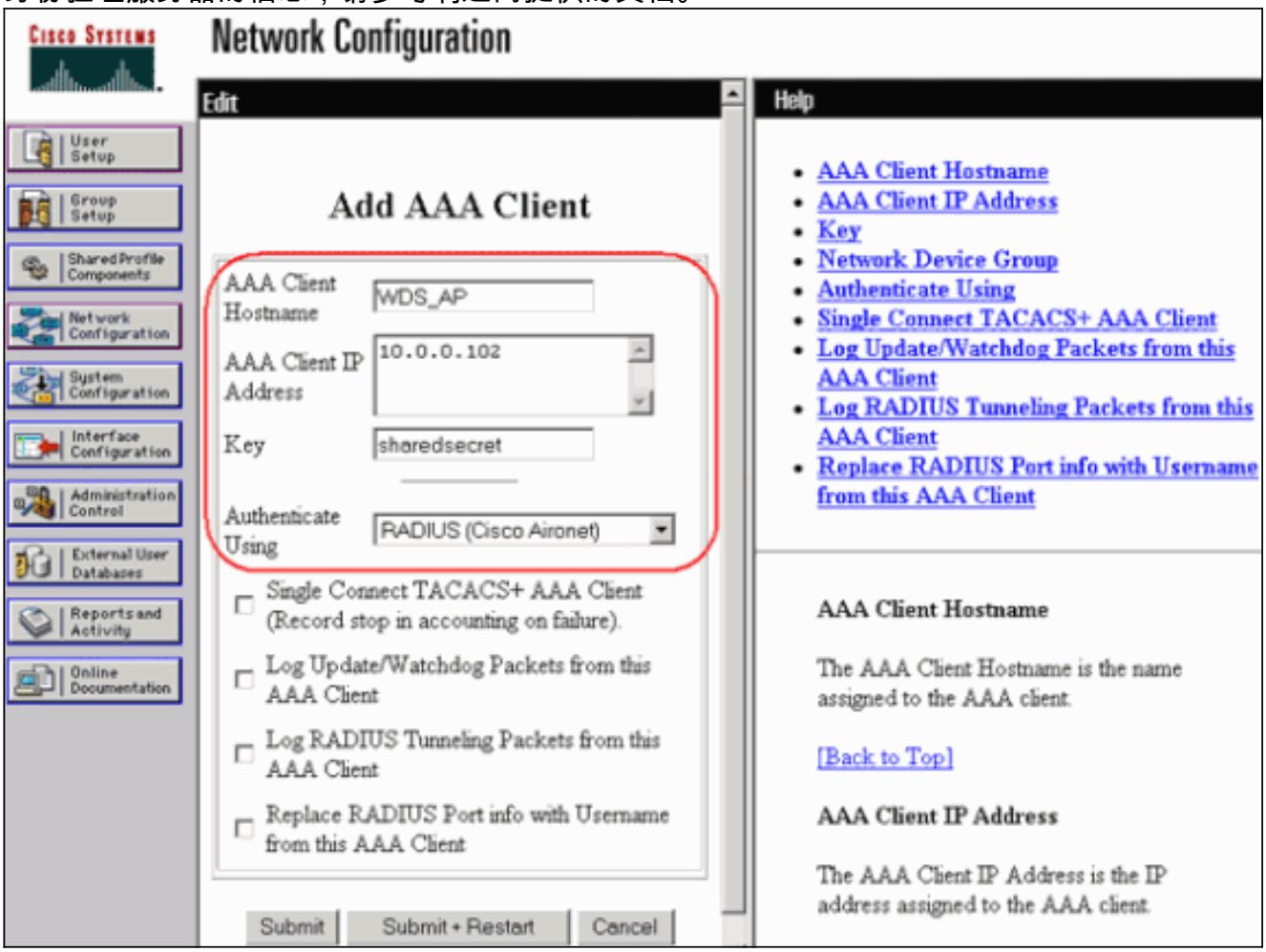
1. 为了在 WDS AP 中配置身份验证服务器，请选择 **Security > Server Manager，以转至 Server Manager 选项卡：**在 Corporate Servers 下的 Server 字段中键入身份验证服务器的 IP 地址。指定 Shared Secret 和端口。在 Default Server Priorities 下，将 Priority 1 字段设置为相应身份验证类型下该服务器的 IP 地址。



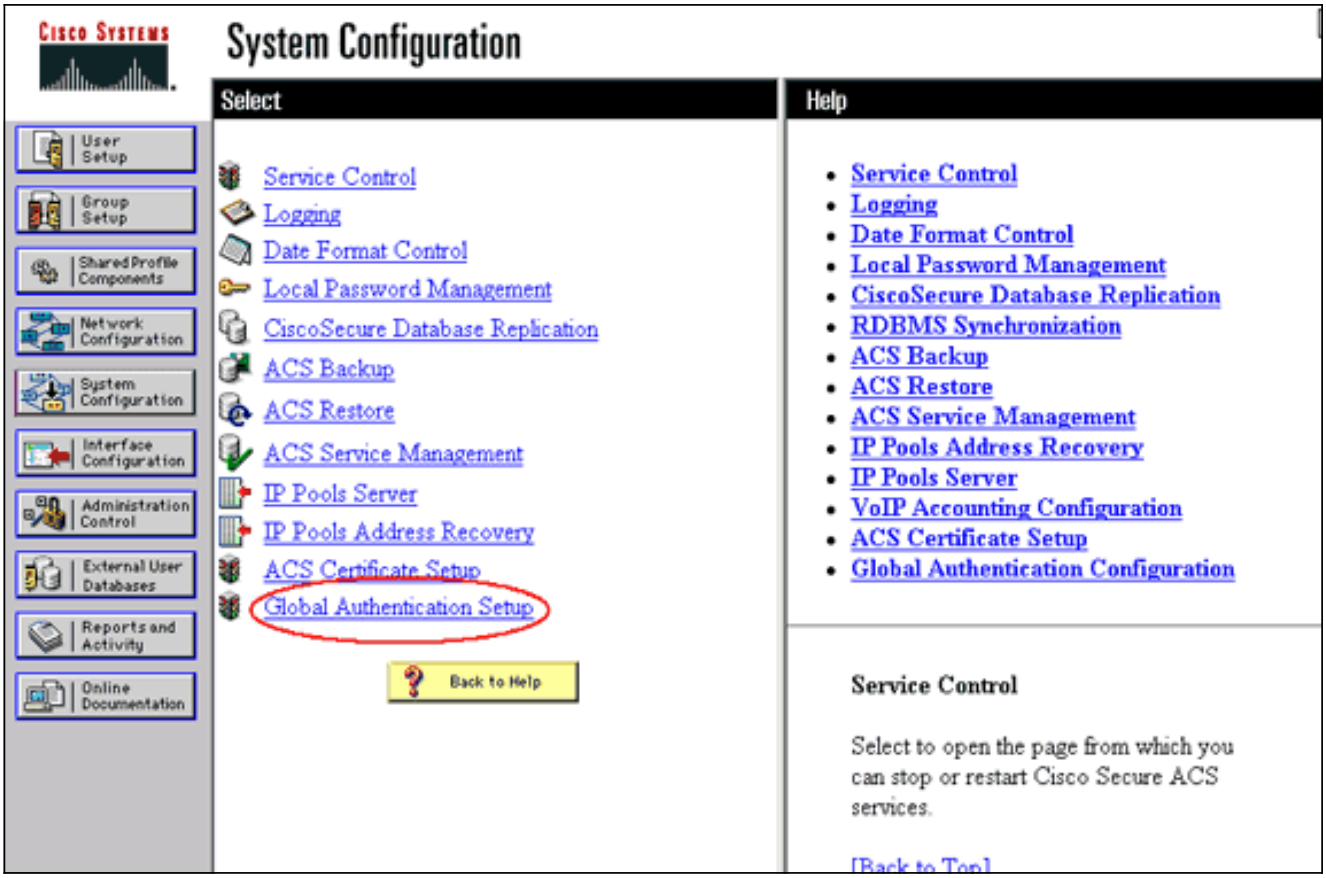
也可从 CLI 中发出以下命令：

2. 下一步是在身份验证服务器中将 WDS AP 配置为身份验证、授权和记帐 (AAA) 客户端。为此，您需要将该 WDS AP 添加为 AAA 客户端。请完成以下步骤：**注意：**本文档使用Cisco Secure ACS服务器作为身份验证服务器。在 Cisco 安全访问控制服务器 (ACS) 中，此操作发生于为 WDS AP 定义这些属性所在的 Network Configuration 页： 名称IP 地址共享密钥认证方

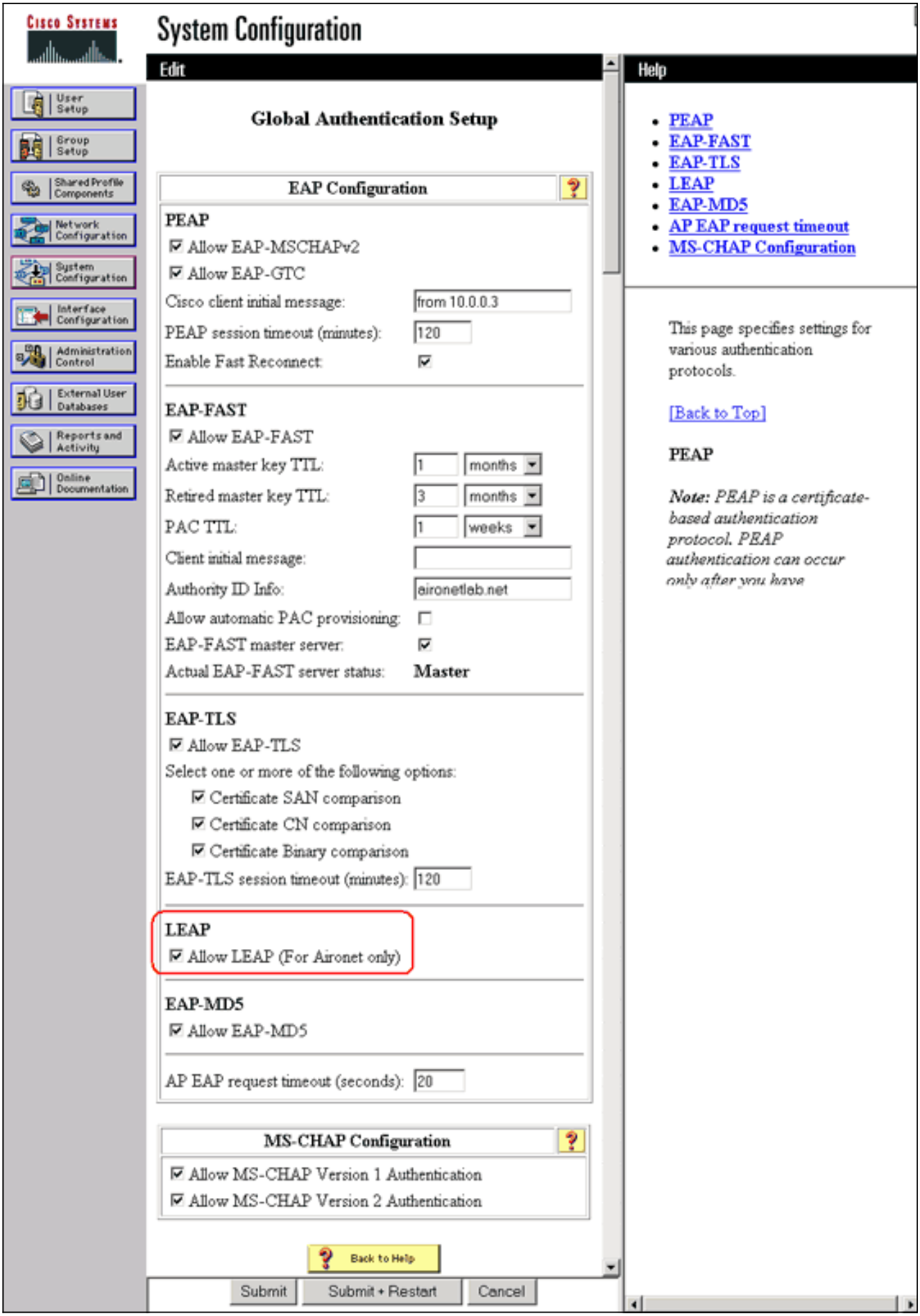
法RADIUS Cisco AironetRADIUS Internet 工程任务组 [IETF]单击 **Submit**。有关其他非 ACS 身份验证服务器的信息，请参考制造商提供的文档。



而且，在 Cisco Secure ACS 中，还要确保在 System Configuration - Global Authentication Setup 页中将 ACS 配置为执行 LEAP 身份验证。首先，单击 **System Configuration**，然后单击 **Global Authentication Setup**。



将该页向下滚动到 LEAP 设置。当您选中该框时，ACS 将对 LEAP 进行身份验证。

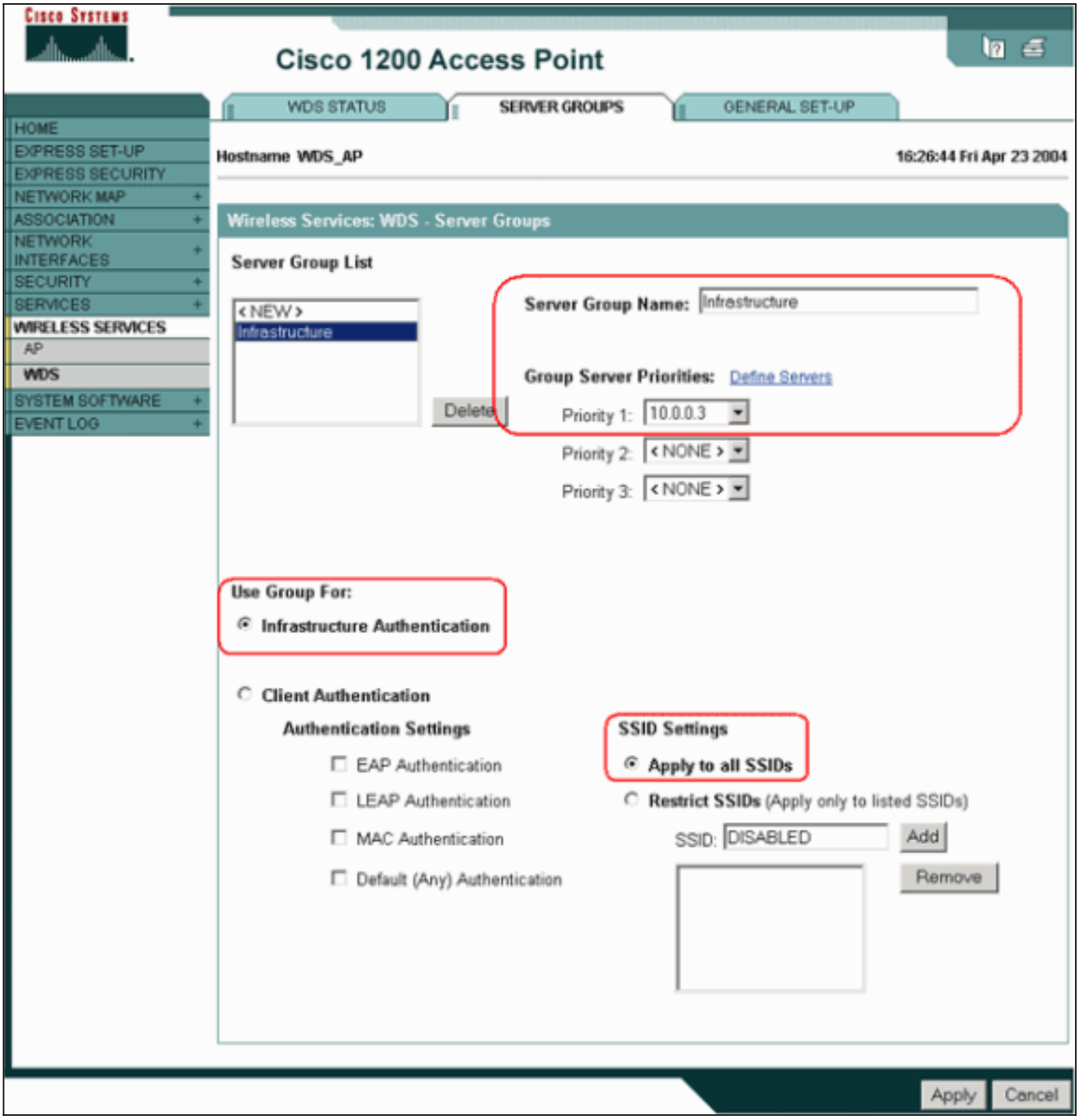


3. 为了在 WDS AP 中配置 WDS 设置，请在 WDS AP 中选择 **Wireless Services > WDS，然后单击 General Set-Up 选项卡。**请执行以下步骤：在 WDS-Wireless Domain Services - Global Properties 下，选中 **Use this AP as Wireless Domain Services**。将 Wireless Domain

Services Priority 字段的值设置为大约 **254**，因为这是第一个值。可将一个或多个 AP 或交换机配置为候选，以提供 WDS。优先级最高的设备提供 WDS。

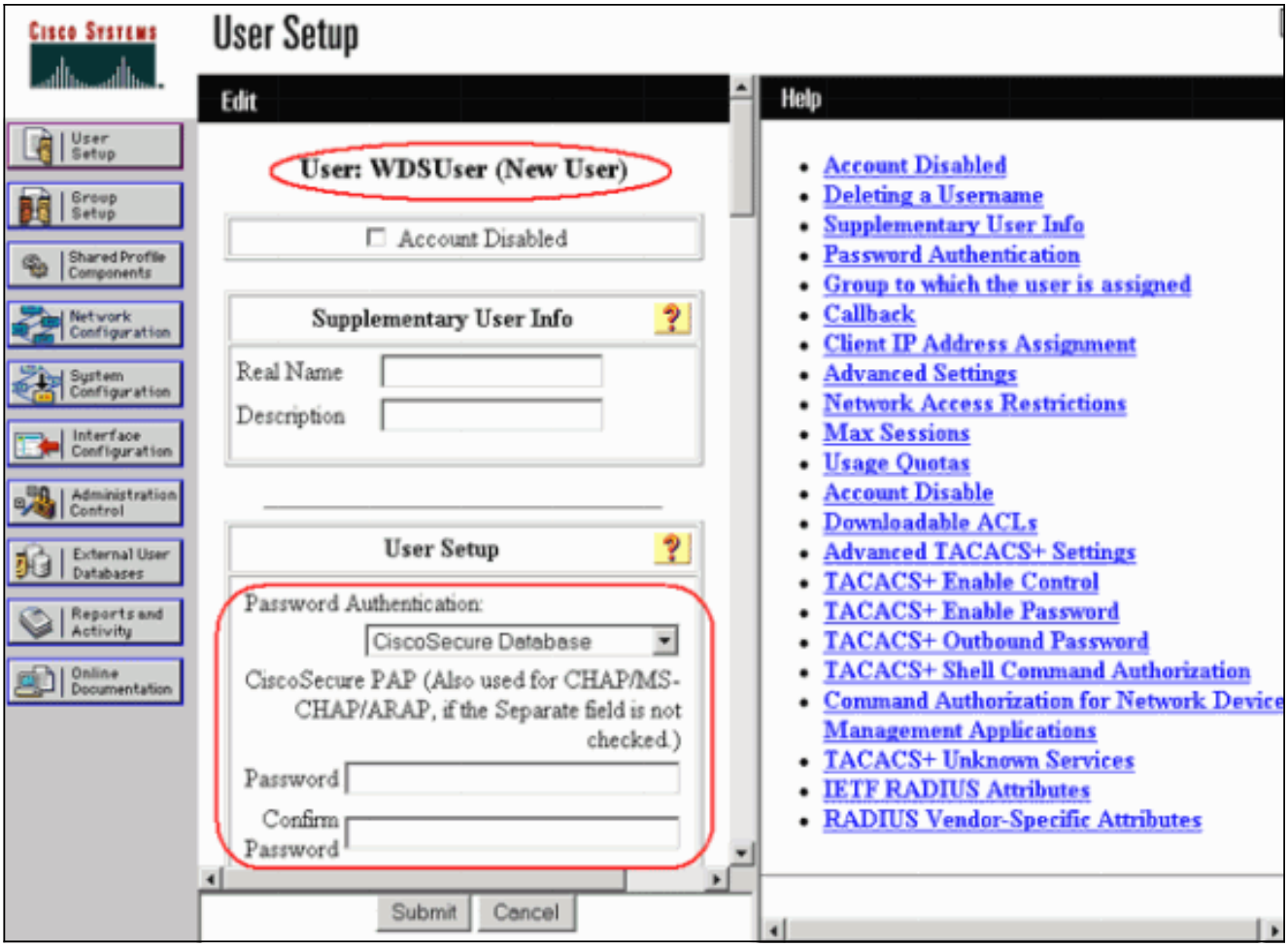
也可从 CLI 中发出以下命令：

4. 选择 **Wireless Services > WDS**，转到 **Server Groups 选项卡**：将对其他 AP 进行身份验证的服务器组名称定义为基础设施组。将 Priority 1 设置为以前配置的身份验证服务器。单击 **Use Group For:Infrastructure Authentication 单选按钮。**将设置应用于相关服务集标识符 (SSID)。



也可从 CLI 中发出以下命令：

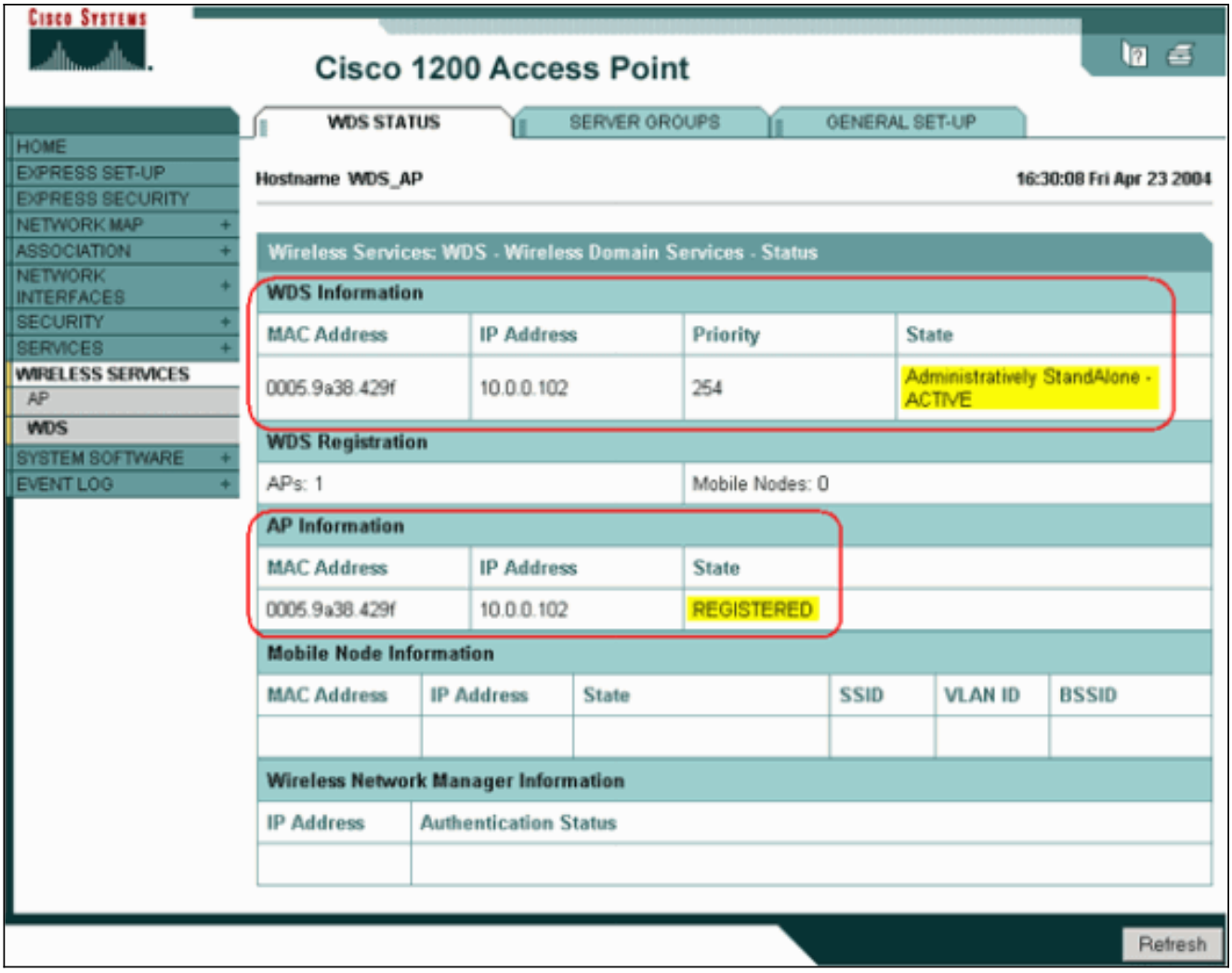
5. 将 WDS 用户名和密码配置为身份验证服务器中的一个用户。在 Cisco Secure ACS 中，此操作发生在 User Setup 页，您可在其中定义 WDS 用户名和密码。有关其他非 ACS 身份验证服务器的信息，请参考制造商提供的文档。**注意：**请勿将WDS用户置于分配了许多权限和权限的组中 — WDS仅需要有限的身份验证。



6. 选择 **Wireless Services > AP**，然后为 Participate in SWAN infrastructure 选项单击 **Enable**。然后键入 WDS 用户名和密码。您必须在身份验证服务器上为指定为 WDS 成员的所有设备定义一个 WDS 用户名和密码。

也可从 CLI 中发出以下命令：

7. 选择 **Wireless Services > WDS**。在 WDS AP WDS Status 选项卡中，检查 WDS AP 是否出现在 WDS Information 区域中并显示为 ACTIVE State。AP 还必须出现在 AP Information 区域中，并且状态为 REGISTERED。如果 AP 未显示为 REGISTERED 或 ACTIVE，请为所有错误或失败的身份验证尝试检查身份验证服务器。正确注册 AP 后，添加基础设施 AP 以使用该 WDS 的服务。



也可从 CLI 中发出以下命令：**注意：**您无法测试客户端关联，因为客户端身份验证尚未设置。

指定 WLSM 作为 WDS

本部分说明如何将 WLSM 配置为 WDS。WDS 是可与身份验证服务器通信的唯一设备。

注：在WLSM的`enable` 命令提示符下发出以下命令，而不是在Supervisor引擎720的enable命令提示符下。要进入WLSM的命令提示符，请在Supervisor引擎720的`enable`命令提示符下发出以下命令：

```
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#
```

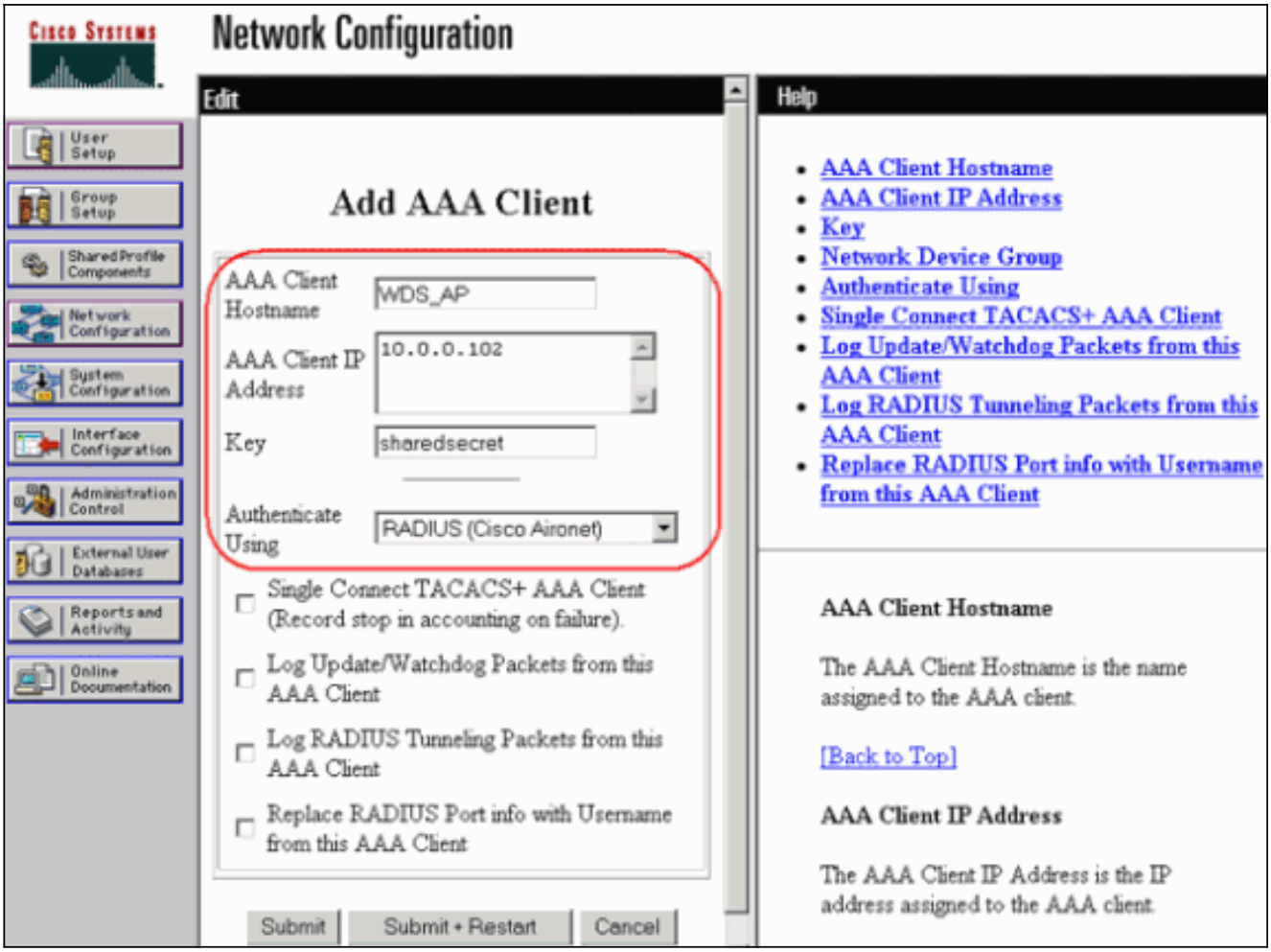
注意：为了更轻松地对WLSM进行故障排除和维护，请配置对WLSM的Telnet远程访问。请参考配置 Telnet 远程访问。

为了指定 WLSM 作为 WDS：

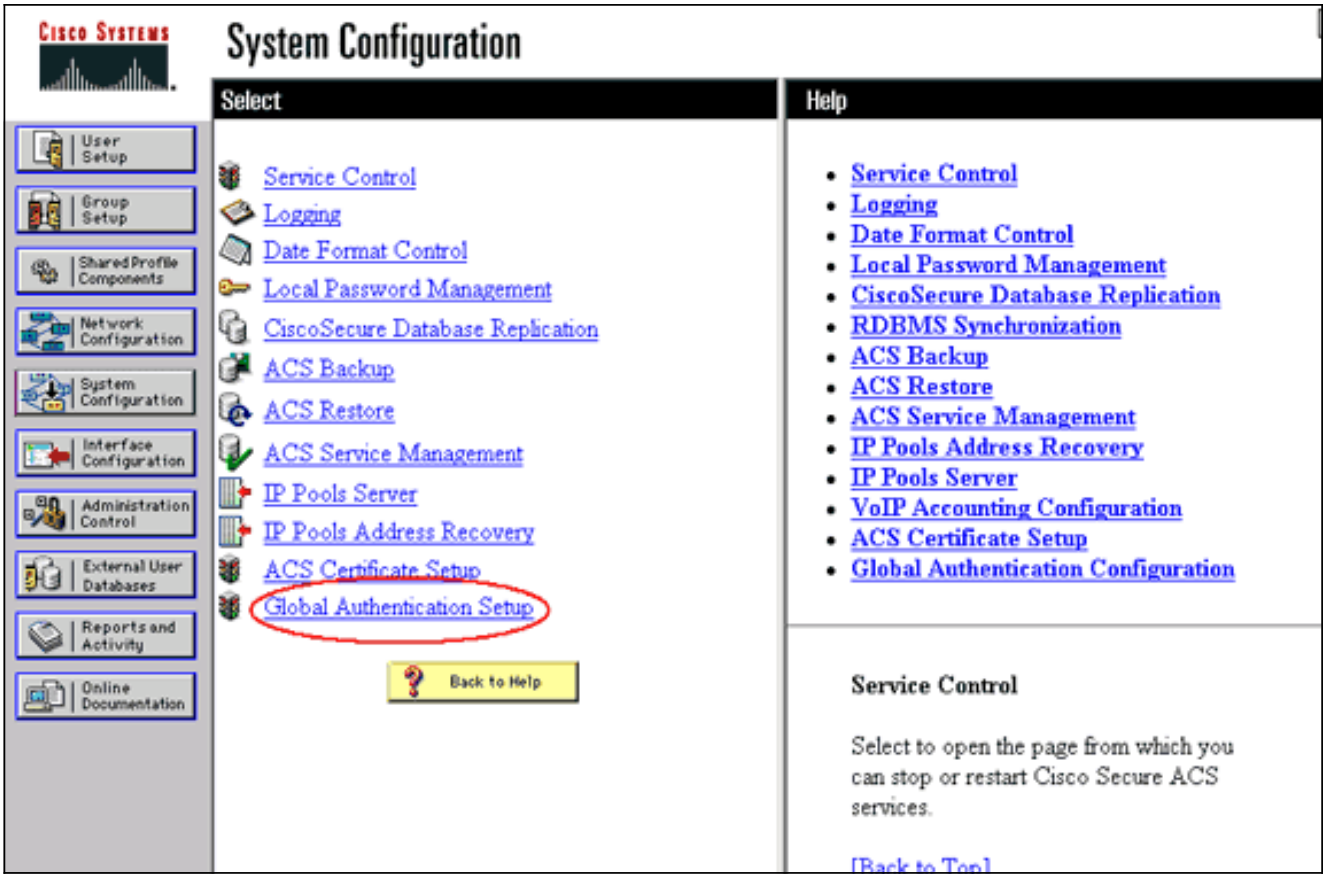
1. 从 WLSM 的 CLI 中，发出以下命令，并与身份验证服务器建立关系：**注意：**WLSM中没有优

先级控制。如果网络包含多个 WLSM 模块，WLSM 将使用冗余配置来确定主要模块。

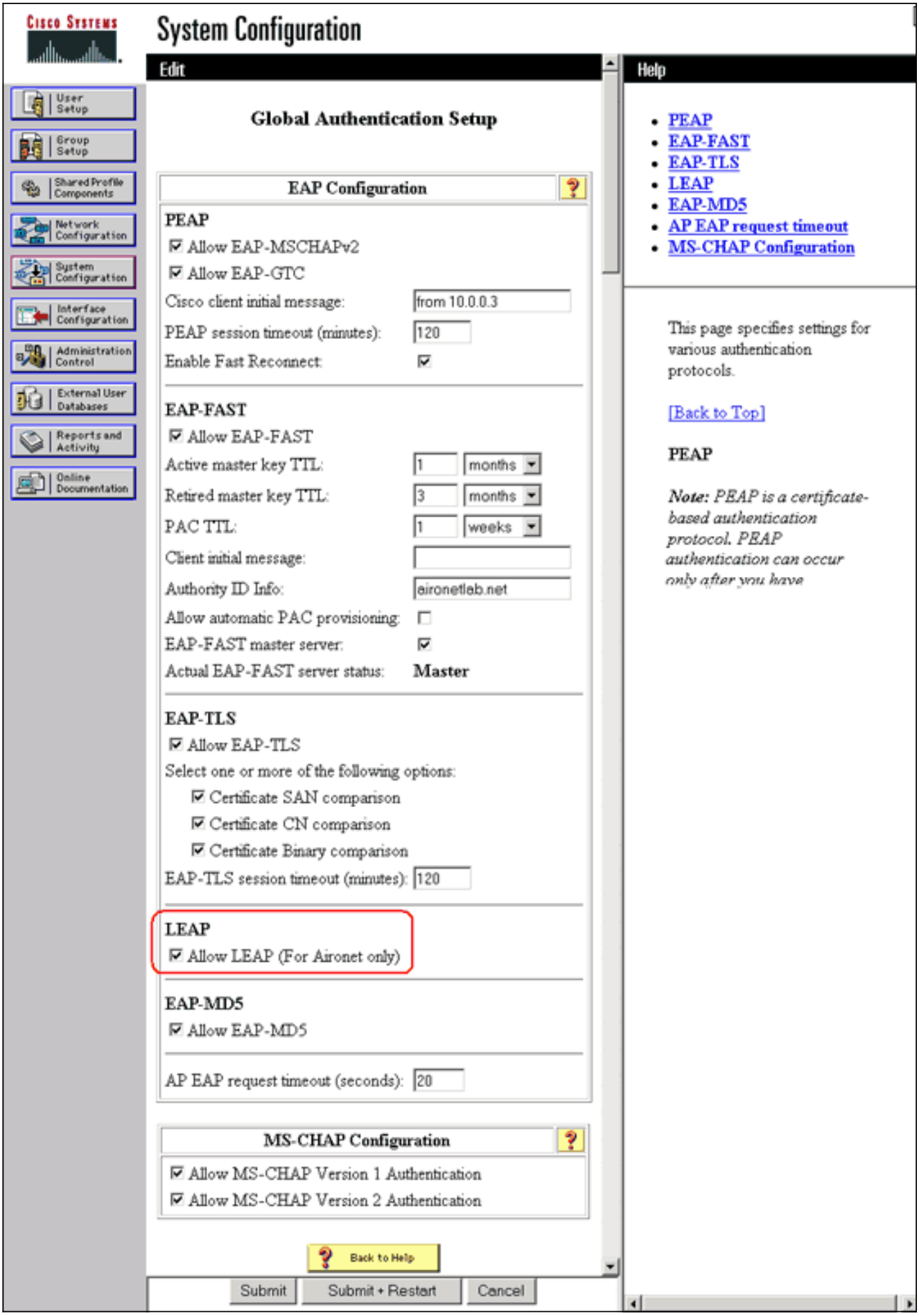
2. 在身份验证服务器中将 WLSM 配置为 AAA 客户端。在 Cisco Secure ACS 中，此操作发生于 Network Configuration 页，您可在此为 WLSM 定义这些属性：名称IP 地址共享密钥认证方法RADIUS Cisco AironetRADIUS IETF有关其他非 ACS 身份验证服务器的信息，请参考制造商提供的文档。



并且，在 Cisco Secure ACS 中，请在 System Configuration - Global Authentication Setup 页上配置 ACS 以执行 LEAP 身份验证。首先，单击 **System Configuration**，然后单击 **Global Authentication Setup**。



将该页向下滚动到 LEAP 设置。当您选中该框时，ACS 将对 LEAP 进行身份验证。



3. 在 WLSM 中，定义可对其他 AP（基础设施服务器组）进行身份验证的方法。
4. 在 WLSM 中，定义对客户端设备（客户端服务器组）进行身份验证的方法以及这些客户端使用的 EAP 类型。**注意**：此步骤无需定义客户端身份验证方法。

5. 在 Supervisor 引擎 720 和 WLSM 之间定义唯一 VLAN，以允许 WLSM 与 AP 和身份验证服务器等外部条目进行通信。此 VLAN 不在其他任何位置使用，也不在网络中用于其他用途。首先在 Supervisor 引擎 720 中创建 VLAN，然后发出以下命令：在 Supervisor 引擎 720 上：在 WLSM 上：
6. 通过以下命令验证 WLSM 的功能：在 WLSM 上：在 Supervisor 引擎 720 上：

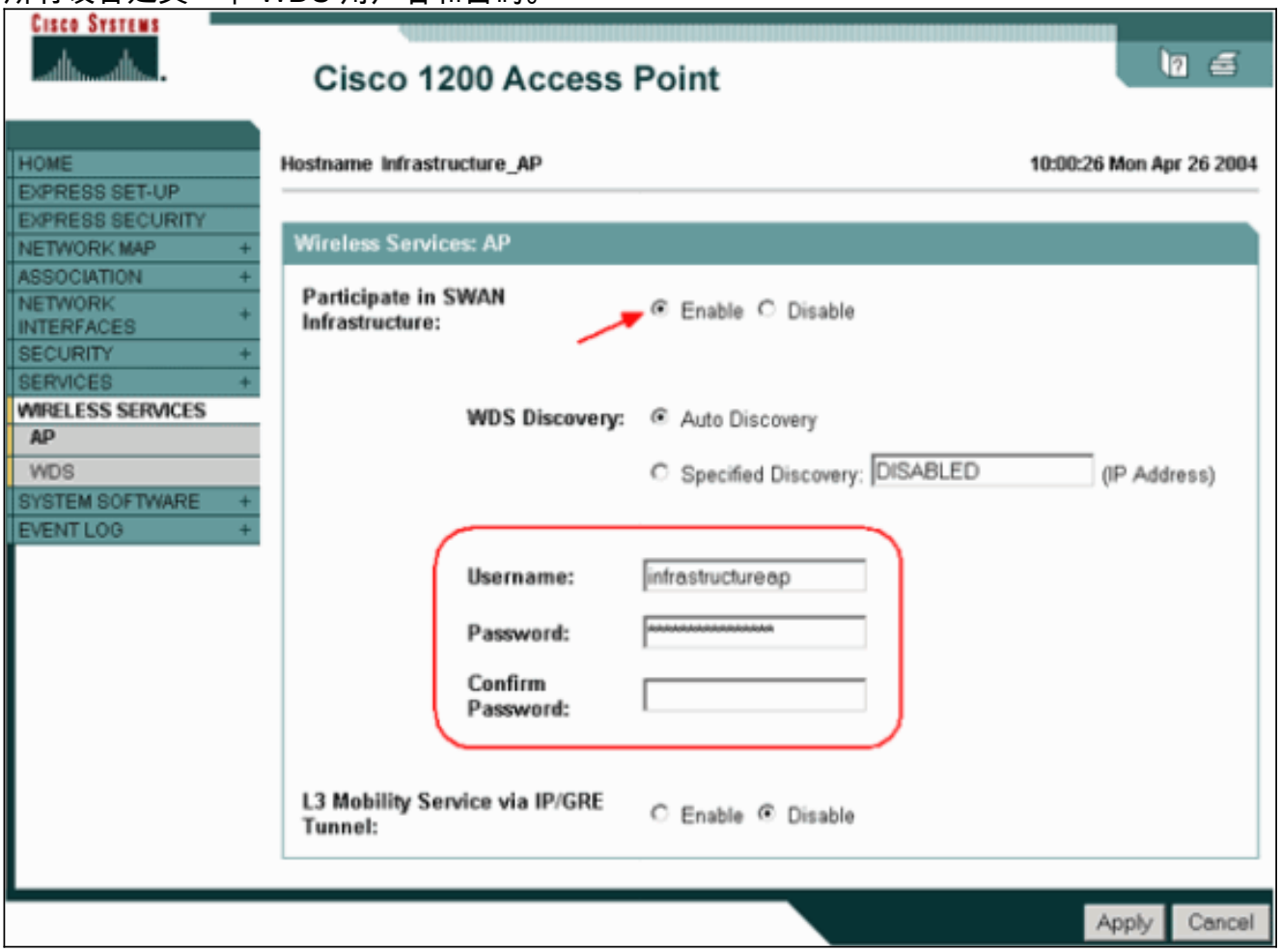
指定 AP 作为基础设施设备

接下来，必须至少指定一个基础设施 AP 并将该 AP 与 WDS 相关。客户端与基础设施 AP 关联。基础设施 AP 请求 WDS AP 或 WLSM 为其执行身份验证。

完成这些步骤，以添加使用 WDS 的服务的基础设施 AP：

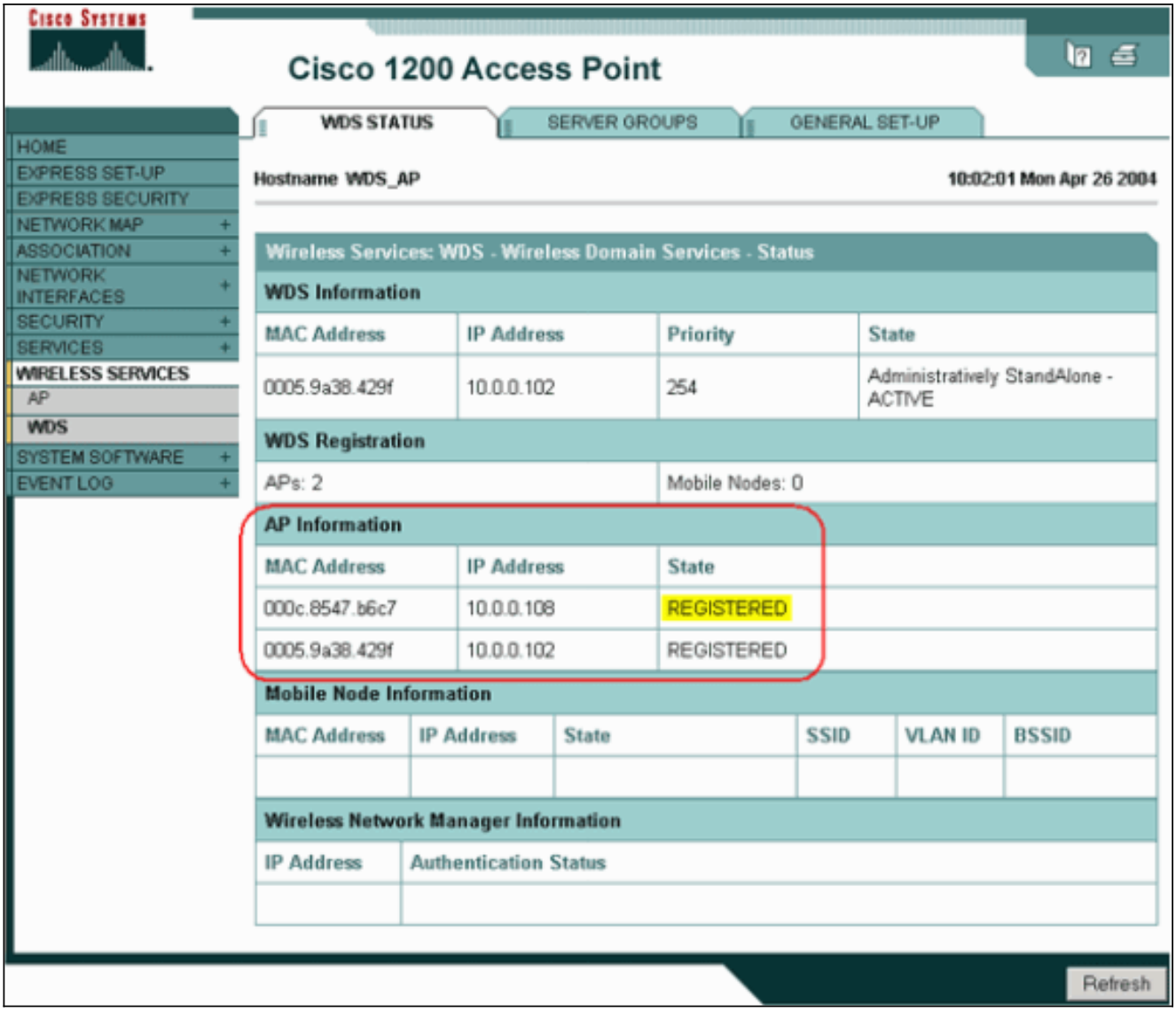
注意：此配置仅适用于基础设施AP，而不适用于WDS AP。

1. 选择 **Wireless Services > AP**。在基础设施 AP 中，选择 Wireless Services 选项对应的 **Enable**。然后键入 WDS 用户名和密码。您必须在身份验证服务器上为将要成为 WDS 成员的所有设备定义一个 WDS 用户名和密码。



也可从 CLI 中发出以下命令：

2. 选择 **Wireless Services > WDS**。在 WDS AP WDS Status 选项卡上，新的基础设施 AP 出现在 WDS Information 区域中时状态为 ACTIVE，出现在 AP Information 区域时状态为 REGISTERED。如果 AP 未显示为 ACTIVE 和/或 REGISTERED，请为所有错误或失败的身份验证尝试检查身份验证服务器。在 AP 显示为 ACTIVE 和/或 REGISTERED 后，请向 WDS 中添加一个客户端身份验证方法。



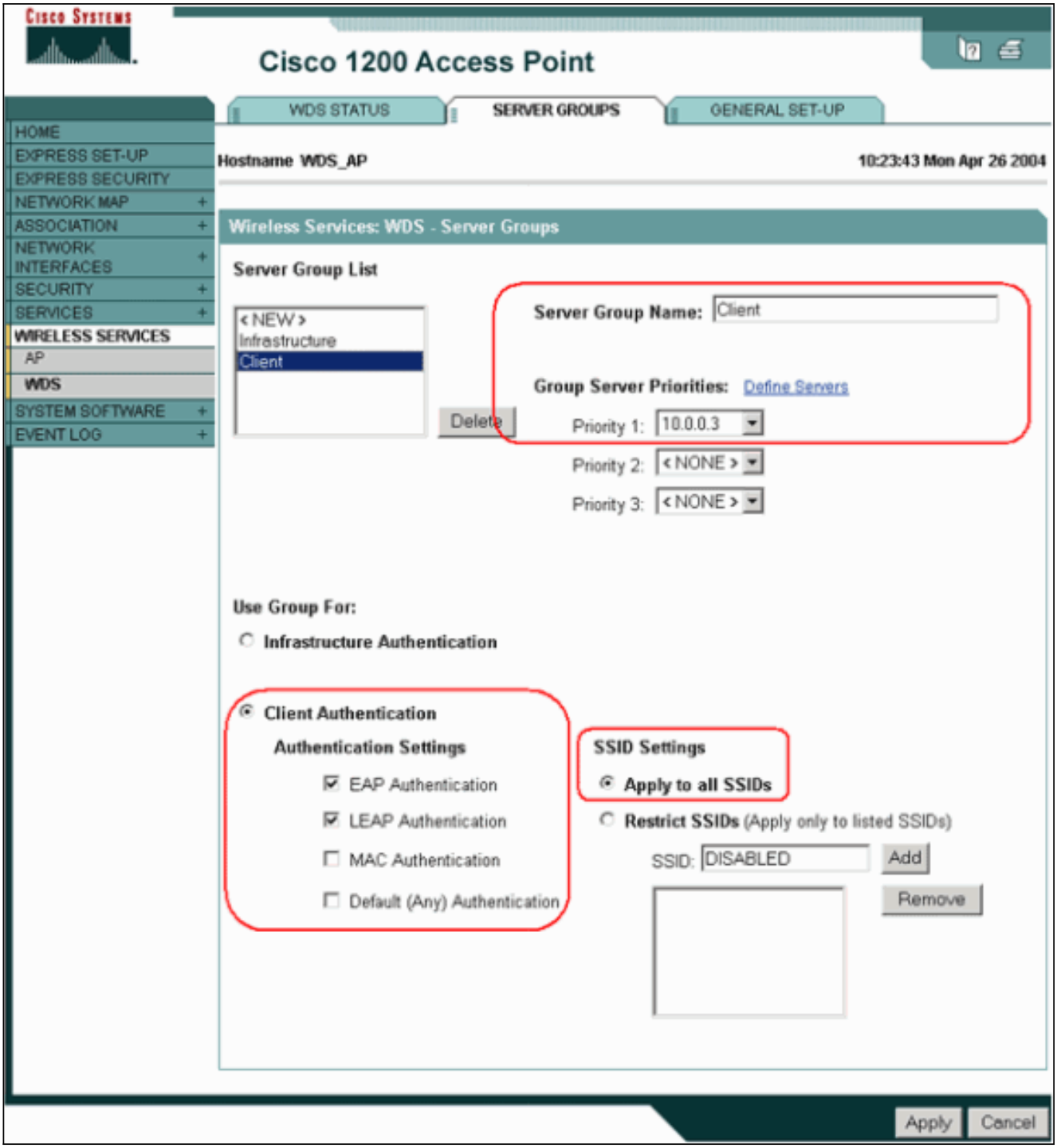
也可以从 CLI 发出以下命令：也可以从 WLSM 发出以下命令：然后，在基础设施 AP 中发出以下命令：**注意：**您无法测试客户端关联，因为客户端身份验证尚未设置。

定义客户端身份验证方法

最后，定义客户端身份验证的方法。

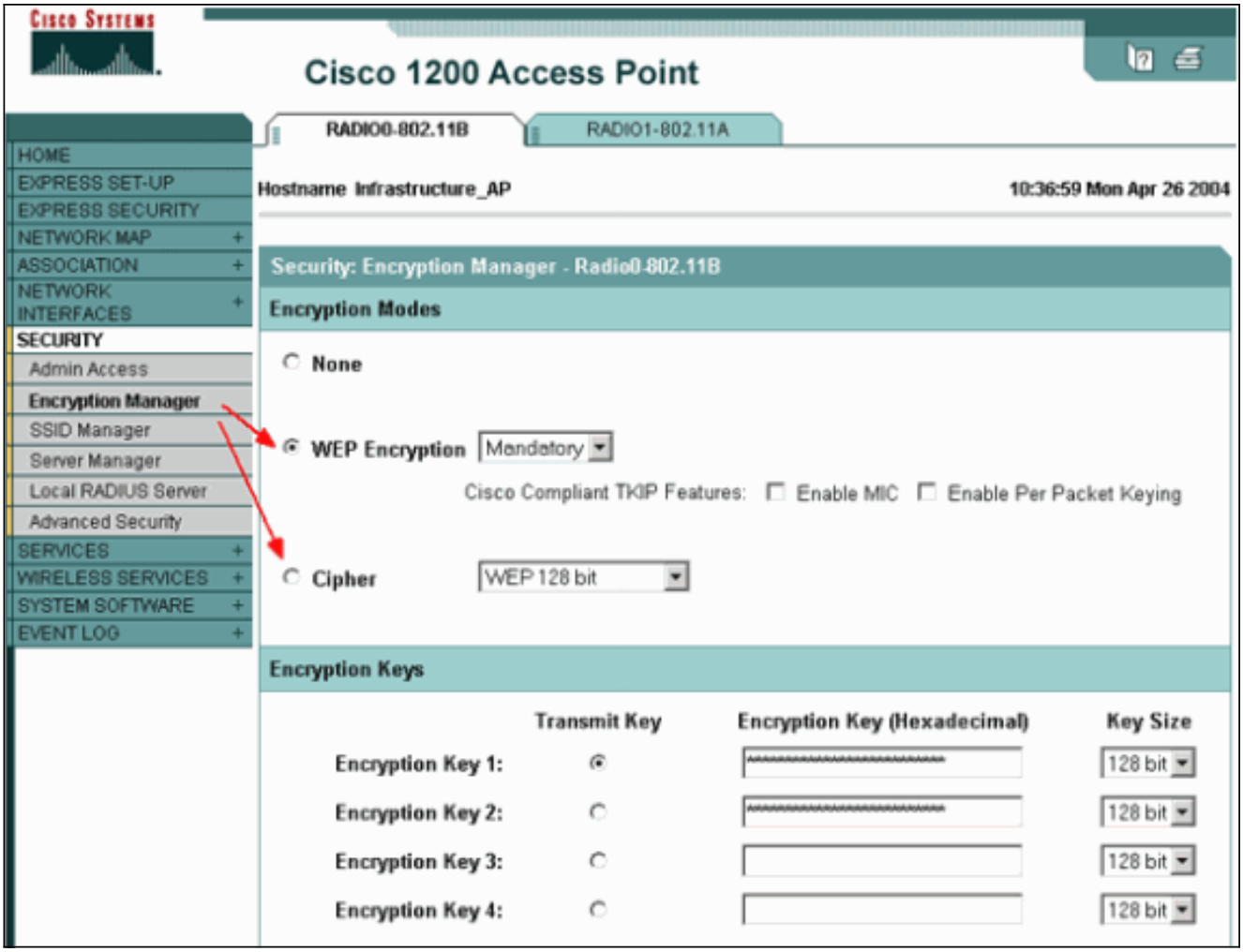
完成以下步骤，以添加客户端身份验证方法：

1. 选择 **Wireless Services > WDS**。在 WDS AP Server Groups 选项卡中执行以下步骤：定义对客户端进行身份验证的服务器组（客户端组）。将 Priority 1 设置为以前配置的身份验证服务器。设置身份验证的适用类型（LEAP、EAP、MAC 等）。将设置应用于相关的 SSID。

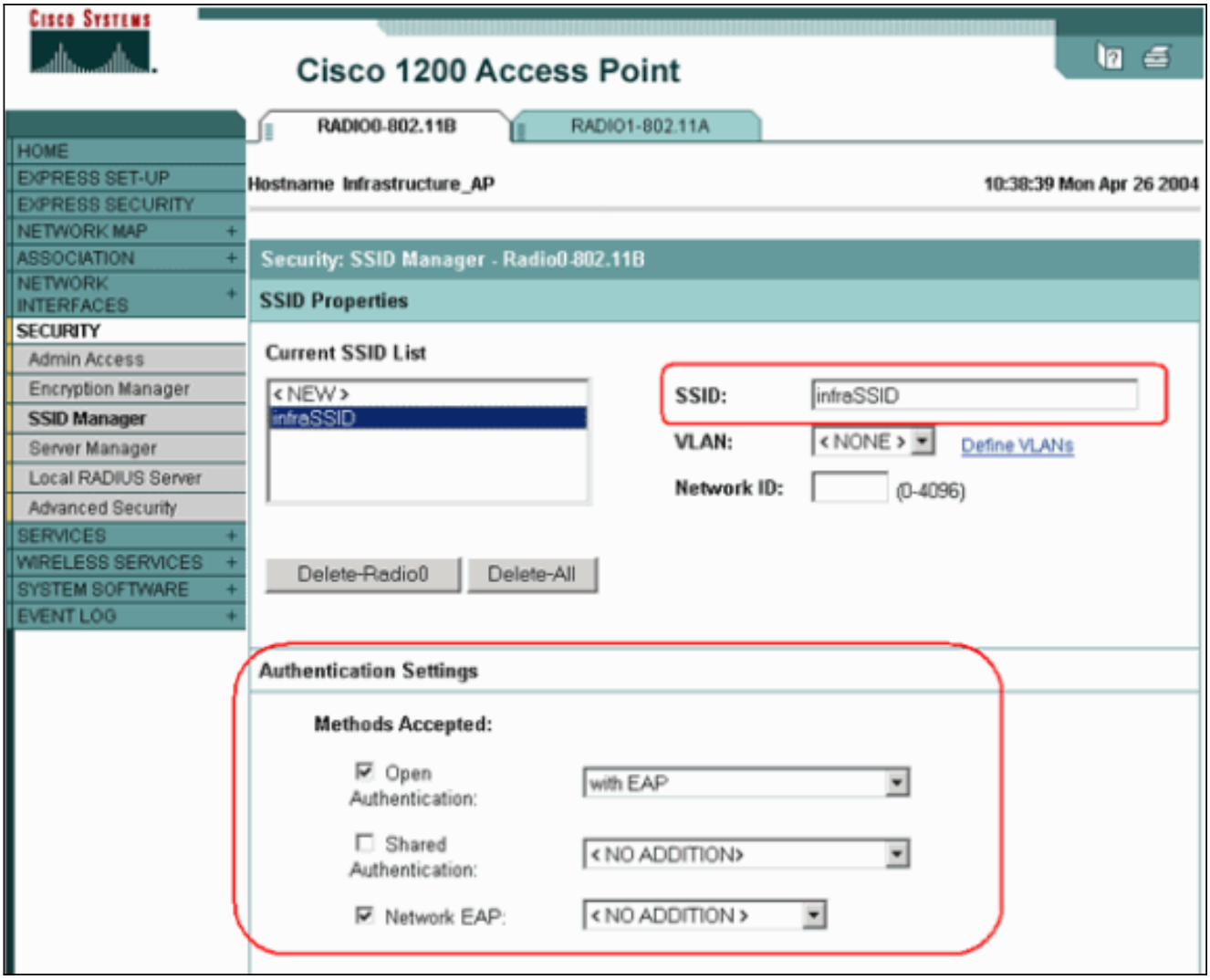


也可从 CLI 中发出以下命令：**注意：**示例WDS AP是专用的，不接受客户端关联。**注意：**请勿在基础设施AP上为服务器组配置，因为基础设施AP会将任何请求转发到要处理的WDS。

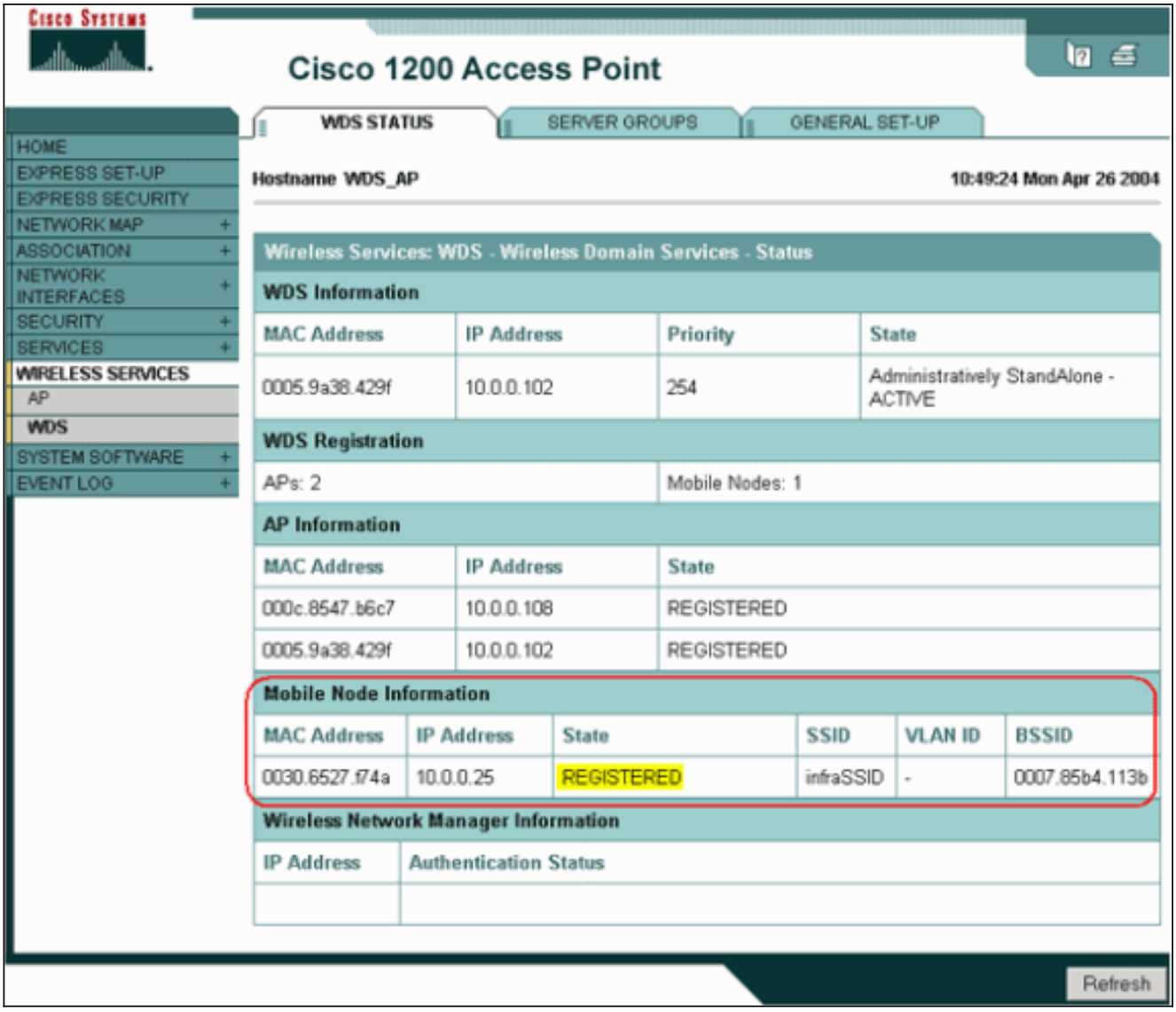
2. 在基础设施 AP 中：根据您使用的身份验证协议的要求，在 **Security > Encryption Manager 菜单项下单击 WEP Encryption 或 Cipher**。



在 Security > SSID Manager 菜单项下，根据您使用的身份验证协议的要求选择身份验证方法。



3. 现在，您可以成功测试客户端是否可向基础设施 AP 验证身份。WDS Status 选项卡（在 **Wireless Services > WDS 菜单项下）中 WDS 的 AP指示客户端出现在 Mobile Node Information 区域中，并且状态为 REGISTERED。**如果客户端未出现，请检查身份验证服务器，以确定客户端是否遇到任何错误或进行了失败的身份验证尝试。



也可从 CLI 中发出以下命令：**注意：**如果需要调试身份验证，请确保在WDS AP上调试，因为WDS AP是与身份验证服务器通信的设备。

验证

当前没有可用于此配置的验证过程。

故障排除

此部分提供您能使用故障排除您的配置的信息。此列表显示与 WDS 命令相关的一些常见问题，以进一步阐明这些命令的用处：

- **问题：在 WDS AP 中，这些项目的建议设置是什么？radius-server timeoutradius-server deadtimeTemporal Key Integrity Protocol (TKIP) 消息完整性检查 (MIC) 故障保持断开时间客户端保持断开时间EAP 或 MAC 重新身份验证间隔EAP 客户端超时（可选）答案：**建议您保留与这些特殊设置有关的配置的默认设置，同时考虑特殊设置并只在存在计时问题时使用这些特殊设置。以下是 WDS AP 的建议设置：禁用 **radius-server timeout**。这是 AP 在重新发送 RADIUS 请求之前等待该请求答复的秒数。默认时间为 5 秒钟。禁用 **radius-server deadtime**。除非将所有服务器都标记为无用，否则在数分钟的持续时间内，其他请求将跳过 RADIUS。默认情况下，启用 TKIP MIC Failure Holdoff Time 并将其设置为 60 秒。如果启用保持断开时间

，则可输入以秒为单位的间隔。如果 AP 在 60 秒内检测到两次 MIC 故障，它将在此处指定的保持断开时间段内阻止该接口上的所有 TKIP 客户端。默认情况下应禁用 Client Holdoff Time。如果启用保持断开，请输入 AP 在身份验证失败之后、处理后续身份验证请求之前等待的秒数。默认情况下禁用 EAP 或 MAC Reauthentication Interval。如果启用重新身份验证，则可指定间隔或接受身份验证服务器给定的间隔。如果您选择指定间隔，请输入 AP 在强制通过身份验证的客户端重新进行身份验证之前等待的间隔秒数。EAP Client Timeout（可选）默认情况下设置为 120 秒。输入 AP 应等待无线客户端响应 EAP 身份验证请求的时间。

- **问题：关于 TKIP 保持断开时间，我认为应设置为 100 毫秒而不是 60 秒。我假设在浏览器中将其设置为一秒，因为这是可以选择的最小值？答案：**除非故障报告唯一的解决方案是增加此时间，否则不会特别建议将其设置为 100 毫秒。一秒是最低设置。
- **问题：以下两个命令是否会对客户端身份验证有所帮助，WDS 或基础设施 AP 中是否需要这两个命令？radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multiple答案：**这两个命令不会对身份验证过程有帮助，WDS 或 AP 中也不需要这两个命令。
- **问题：在基础设施 AP 中，假设 AP 会接收来自 WDS 的信息，所以不需要任何服务器管理器和全局属性设置。基础设施 AP 是否需要其中的任何特定命令？radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtime答案：**不需要将服务器管理器和全局属性用于基础设施 AP。WDS 将处理该任务，无需使用以下设置：**radius-server attribute 6 on-for-login-authradius-server attribute 6 support-multipleradius-server timeoutradius-server deadtime**默认情况下，**radius-server attribute 32 include-in-access-req format %h 设置会保留并且是必需的。**

AP 是第 2 层设备。所以，在将 AP 配置为充当 WDS 设备时，AP 不支持第 3 层移动性。只有在将 WLSM 配置为 WDS 设备时，才能获得第 3 层移动性。请参阅Cisco *Catalyst 6500系列无线LAN服*务模块的第3层移动架构部分：白皮书中。

因此，在将 AP 配置为 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，并且您需要用 WLSM 作为 WDS 设备，才能正确配置第 3 层移动性。如果不正确地使用 **mobility network-id 命令，则会看到下列某些症状：**

- 无线客户端无法与 AP 关联。
- 无线客户端可与 AP 关联，但是收不到来自 DHCP 服务器的 IP 地址。
- 当您部署了 Voice over WLAN 时，无法对无线电话进行身份验证。
- 未进行 EAP 身份验证。配置 **mobility network-id 后，AP 会尝试构建通用路由封装 (GRE) 隧道来转发 EAP 数据包。**如果未建立隧道，数据包将留在原地。
- 已配置为 WDS 设备的 AP 运行不正常，并且 WDS 配置也不起作用。**注意：**您不能将Cisco Aironet 1300 AP/网桥配置为WDS主设备。1300 AP/Bridge 不支持此功能。1300 AP/Bridge 可以作为基础设施设备参与 WDS 网络，在其中将一些 AP 或 WLSM 配置为 WDS 主控。

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。

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

- **debug dot11 aaa authenticator all** — 显示客户端在通过802.1x或EAP进程关联和身份验证时所经历的各种协商。这个debug在Cisco IOS软件版本12.2(15)JA介绍过。此命令在该版本和更高版本中废弃 **debug dot11 aaa dot1x all。**
- **debug aaa authentication - 从通用 AAA 的角度显示身份验证过程。**
- **debug wlccp ap - 显示作为 AP 加入 WDS 的 WLCCP 协商。**

- debug wlccp packet - 显示关于 WLCCP 协商的详细信息。
- debug wlccp leap-client - 显示作为基础设备加入 WDS 的详细信息。

相关信息

- 配置 WDS、快速安全漫游和无线管理
- Catalyst 6500 系列无线 LAN 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
- 技术支持和文档 - Cisco Systems