Microsoft IAS Radius服务器上的Cisco Airespace VSA配置示例

目录

简介

本文档介绍如何配置Microsoft Internet Authentication Service(IAS)服务器以支持Cisco Airespace供应商特定属性(VSA)。 Cisco Airespace VSA的供应商代码为**14179**。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置IAS服务器
- 了解轻量接入点(LAP)和思科无线局域网控制器(WLC)的配置
- Cisco Unified无线安全解决方法知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 具有 IAS 的 Microsoft Windows 2000 服务器
- 运行软件版本 4.0.206.0 的 Cisco 4400 WLC
- Cisco 1000 系列 LAP

- 具有固件 2.5 的 802.11 a/b/g 无线客户端适配器
- Aironet Desktop Utility (ADU) 版本 2.5

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。

注意：本文档旨在向读者提供IAS服务器上支持Cisco Airespace VSA所需配置的示例。本文档中介绍的IAS服务器配置已在实验中测试并按预期工作。如果配置IAS服务器时遇到问题，请联系Microsoft获取帮助。Cisco TAC 不支持 Microsoft Windows 服务器配置。

本文档假设已配置 WLC 进行基本操作，并且已在 WLC 中注册 LAP。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)。

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

在大多数无线LAN(WLAN)系统中，每个WLAN都有一个静态策略，该策略适用于与服务集标识符(SSID)关联的所有客户端。 虽然此方法功能强大，但也具有局限性，这是因为，它要求客户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

但是，思科无线局域网解决方案支持身份网络，它允许网络通告单个SSID和特定用户根据其用户配置文件继承不同的QoS或安全策略。您可以使用身份网络控制的特定策略包括：

- **服务质量**(QoS) — 当在RADIUS访问接受(RADIUS Access Accept)中出现时，QoS级别值将覆盖WLAN配置文件中指定的QoS值。
- **ACL** — 当RADIUS Access Accept中存在访问控制列表(ACL)属性时，系统在对客户端站进行身份验证后将ACL-Name应用到客户端站。这撤销的所有ACL都被分配到接口上。
- **VLAN** — 当VLAN接口名称或VLAN标记存在于RADIUS接入接受中时，系统将客户端置于特定接口上。
- **WLAN ID** — 当WLAN-ID属性存在于RADIUS Access Accept中时，系统在进行身份验证后将WLAN-ID(SSID)应用到客户端站。WLC在除IPSec之外的所有身份验证实例中发送WLAN ID。在Web身份验证中，如果WLC从AAA服务器收到身份验证响应中的WLAN-ID属性，并且与WLAN的ID不匹配，则身份验证被拒绝。其他类型的安全方法不执行此操作。
- **DSCP值** — 当RADIUS访问接受中存在时，DSCP值将覆盖WLAN配置文件中指定的DSCP值。
- **802.1p-Tag** — 当在RADIUS访问接受中存在时，802.1p值将覆盖WLAN配置文件中指定的默认值。

注意：VLAN功能仅支持MAC过滤、802.1X和Wi-Fi保护访问(WPA)。 VLAN功能不支持Web身份验证或IPSec。操作系统的本地MAC过滤器数据库已扩展为包括接口名称。这允许本地MAC过滤器指定应分配客户端的接口。也可以使用单独的RADIUS服务器，但必须使用安全菜单定义RADIUS服务器。

有关身份网络的详细信息，请参阅配置身份网络。

为Airespace VSA配置IAS

要配置Airespace VSA的IAS，您需要完成以下步骤：

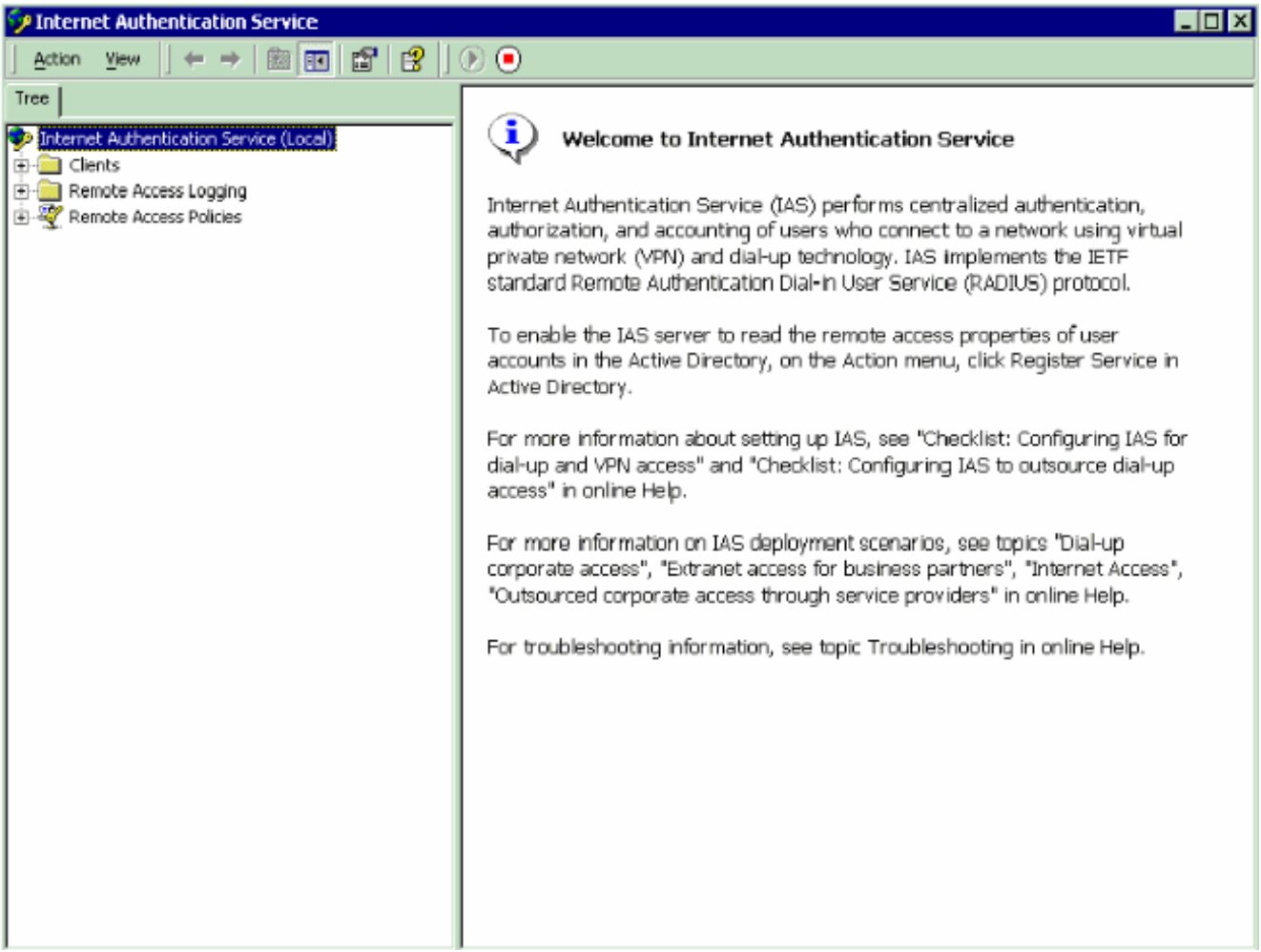
1. 在IAS上将WLC配置为AAA客户端
2. 在IAS上配置远程访问策略

注意：VSA在远程访问策略下配置。

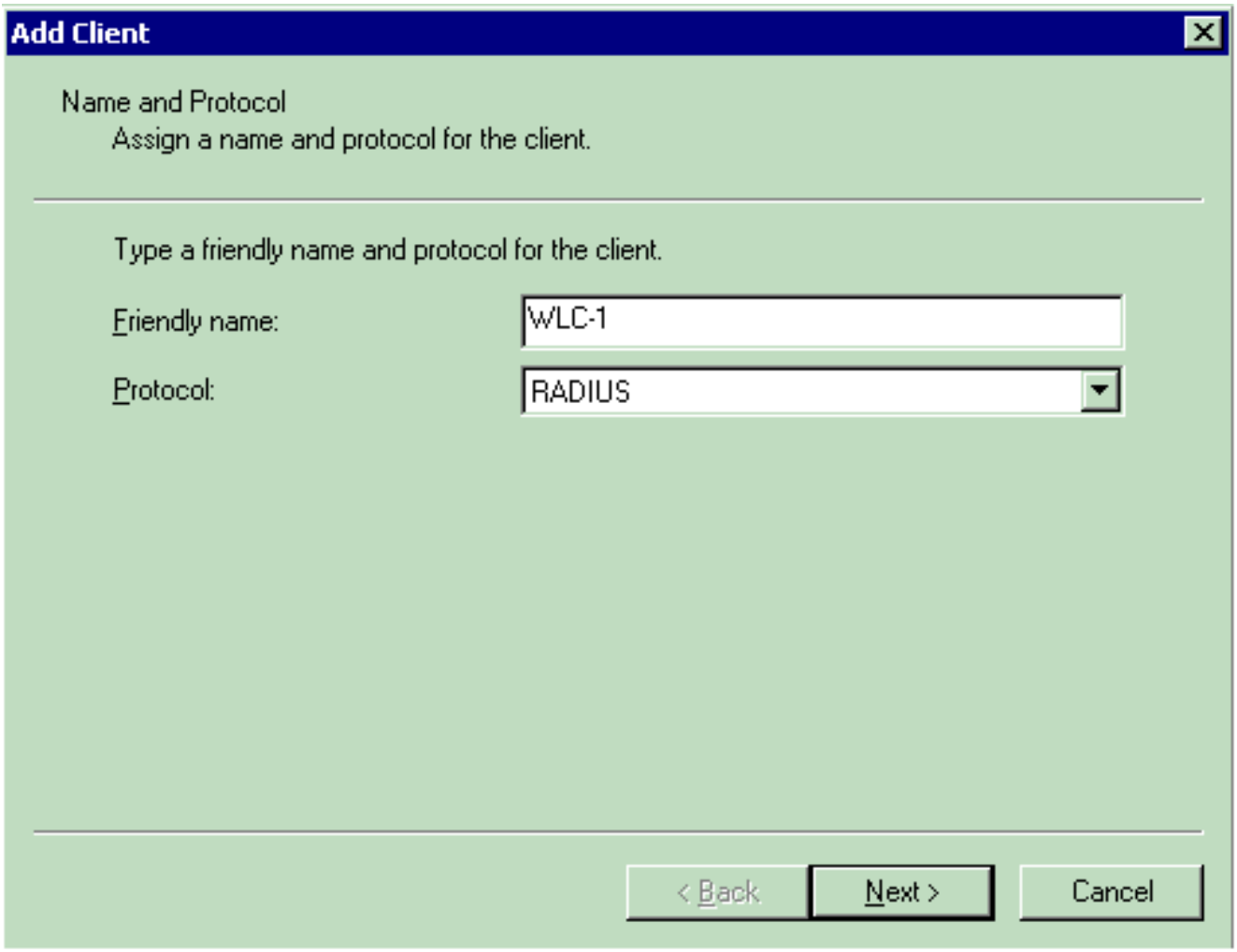
在IAS上将WLC配置为AAA客户端

要在IAS上将WLC配置为AAA客户端，请完成以下步骤：

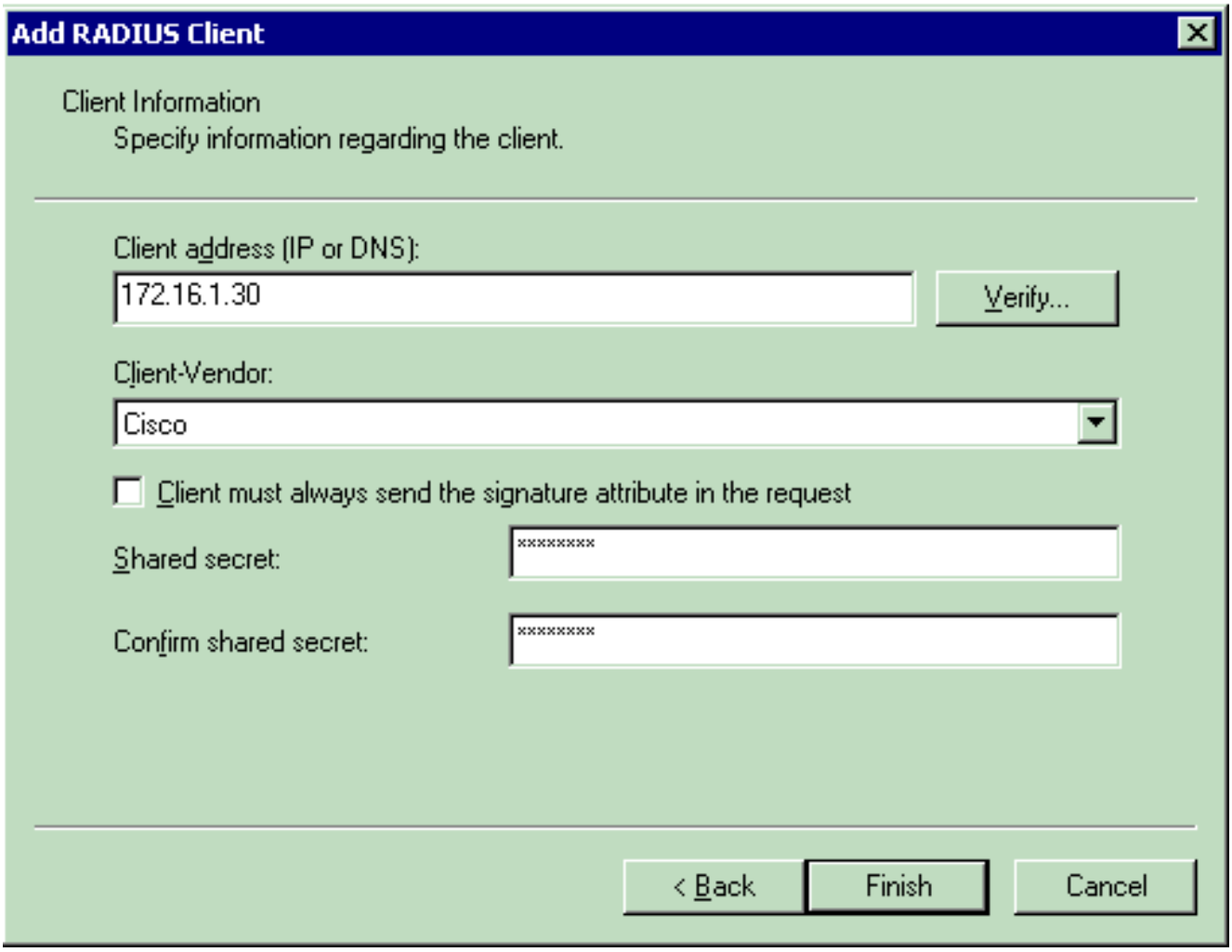
1. 单击**程序>管理工具> Internet身份验证服务**以在Microsoft 2000服务器上启动IAS。



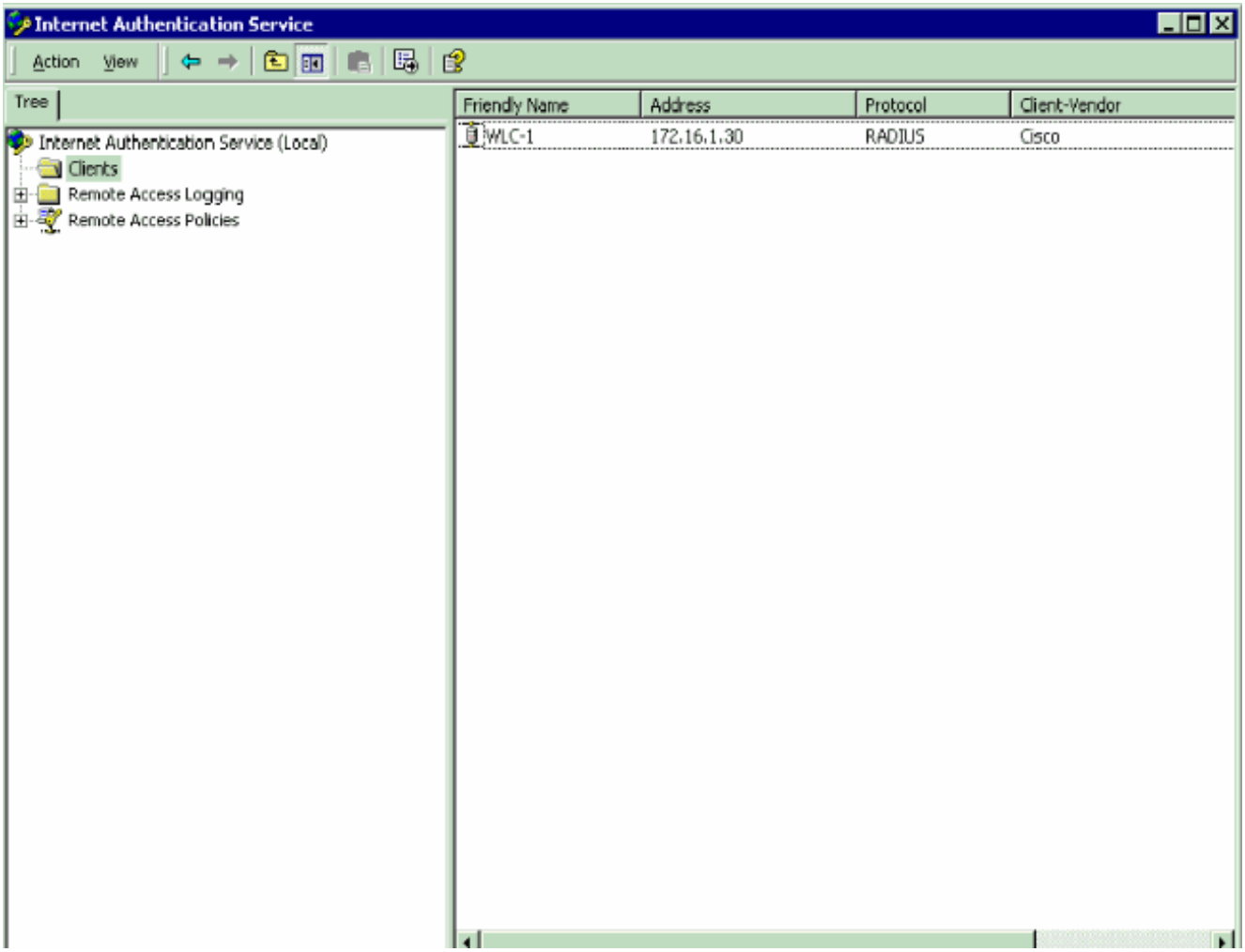
2. 右键单击“Clients”**文**件夹，然**后选择“New Client**”以添加新的RADIUS客户端。
3. 在Add Client（添加客户端）窗口中，输入客户端的名称，然后选择**RADIUS**作为协议。然后单击 **Next**。在本示例中，客户端名称为*WLC-1*。**注意**：默认情况下，协议设置为RADIUS。



4. 在Add RADIUS Client（添加RADIUS客户端）窗口中，输入**Client IP address（客户端IP地址）**、**Client-Vendor（客户端 — 供应商）**和**Shared secret（共享密钥）**。输入客户端信息后，单击**Finish**。本示例显示IP地址为*172.16.1.30*的名为*WLC-1*的客户端，Client-Vendor设置为*Cisco*,Shared secret为
cisco123:



使用此信息，名为WLC-1的WLC将添加为IAS服务器的AAA客户端。

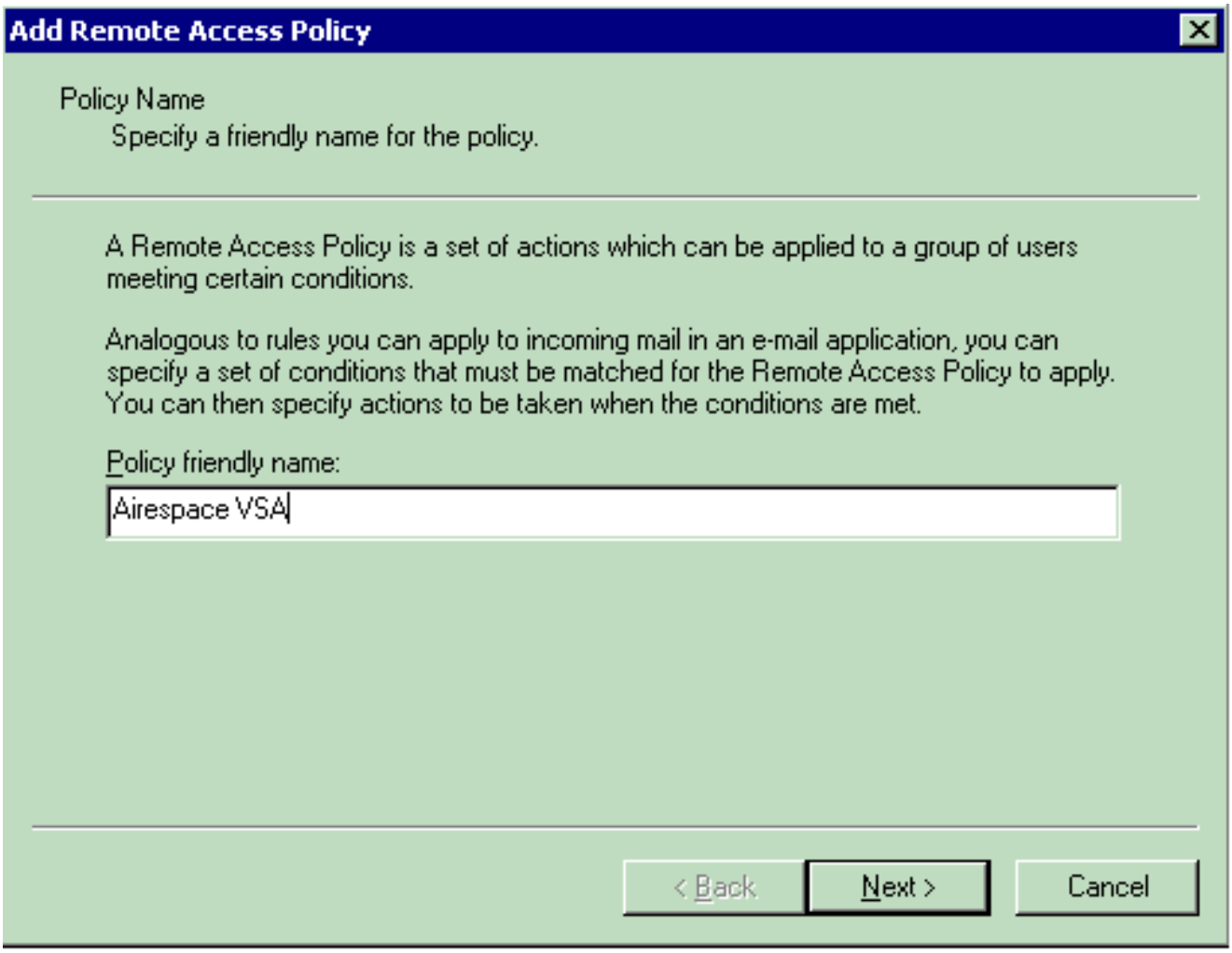


下一步是创建远程访问策略并配置VSA。

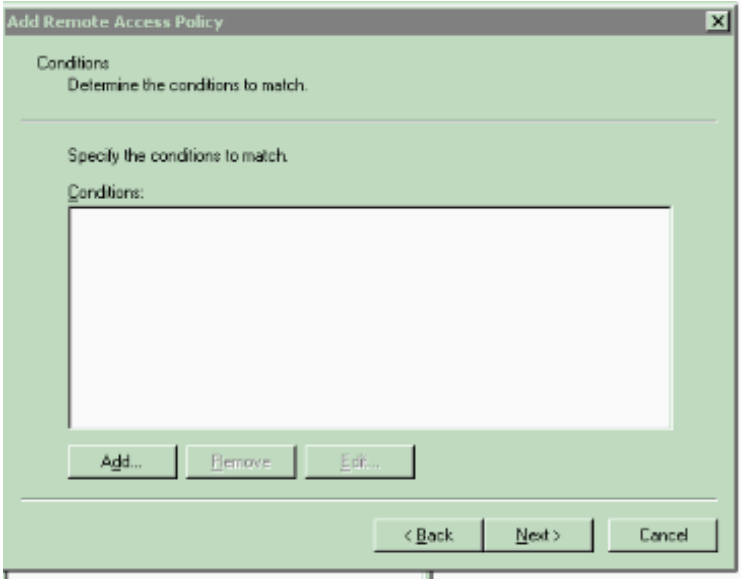
在IAS上配置远程访问策略

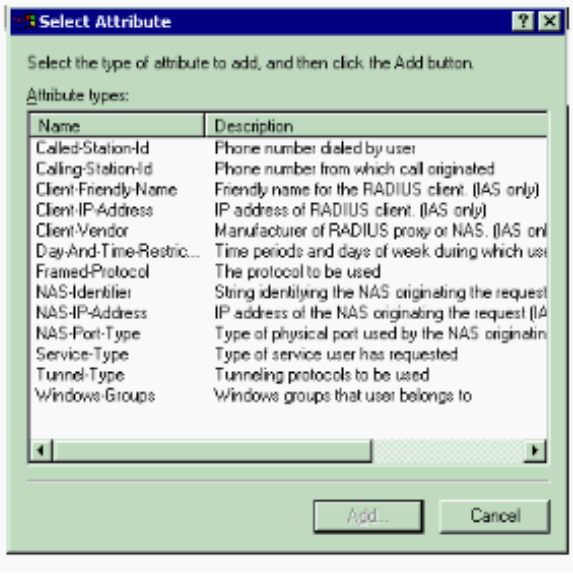
要在IAS上配置新的远程访问策略，请完成以下步骤：

1. 右键单击“远**程访问策略”**，然后选**择“新建远程访问策略**”。系统将显示Policy Name窗口。
2. 输入策略的名称，然后单击**Next**。

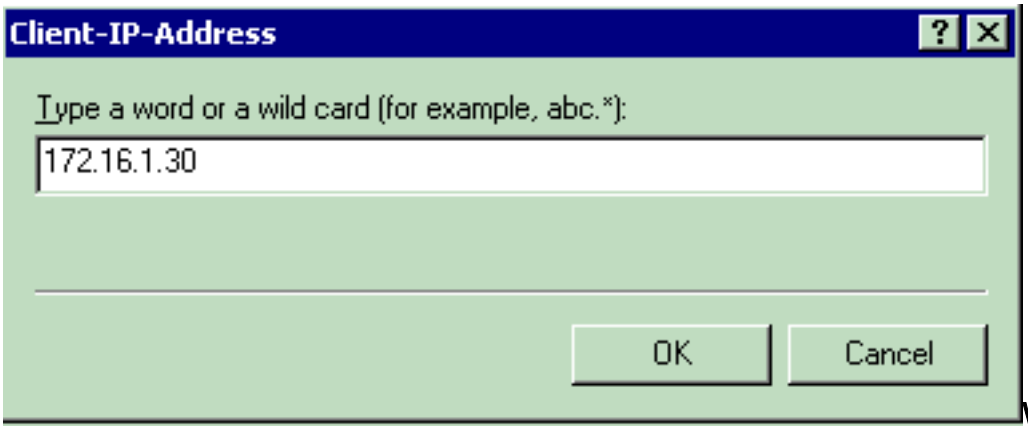


3. 在下一个窗口中，选择远程访问策略将应用的条件。单击**Add**以选择条件。

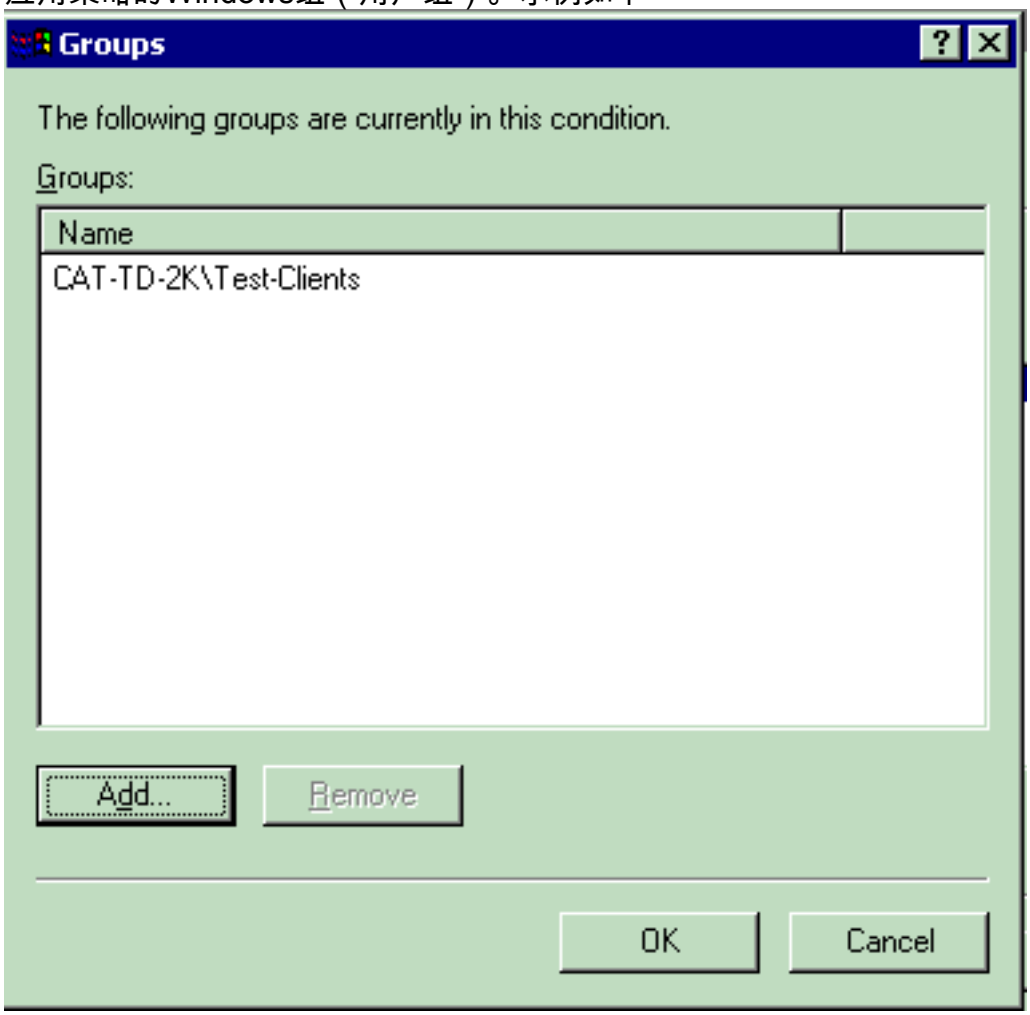




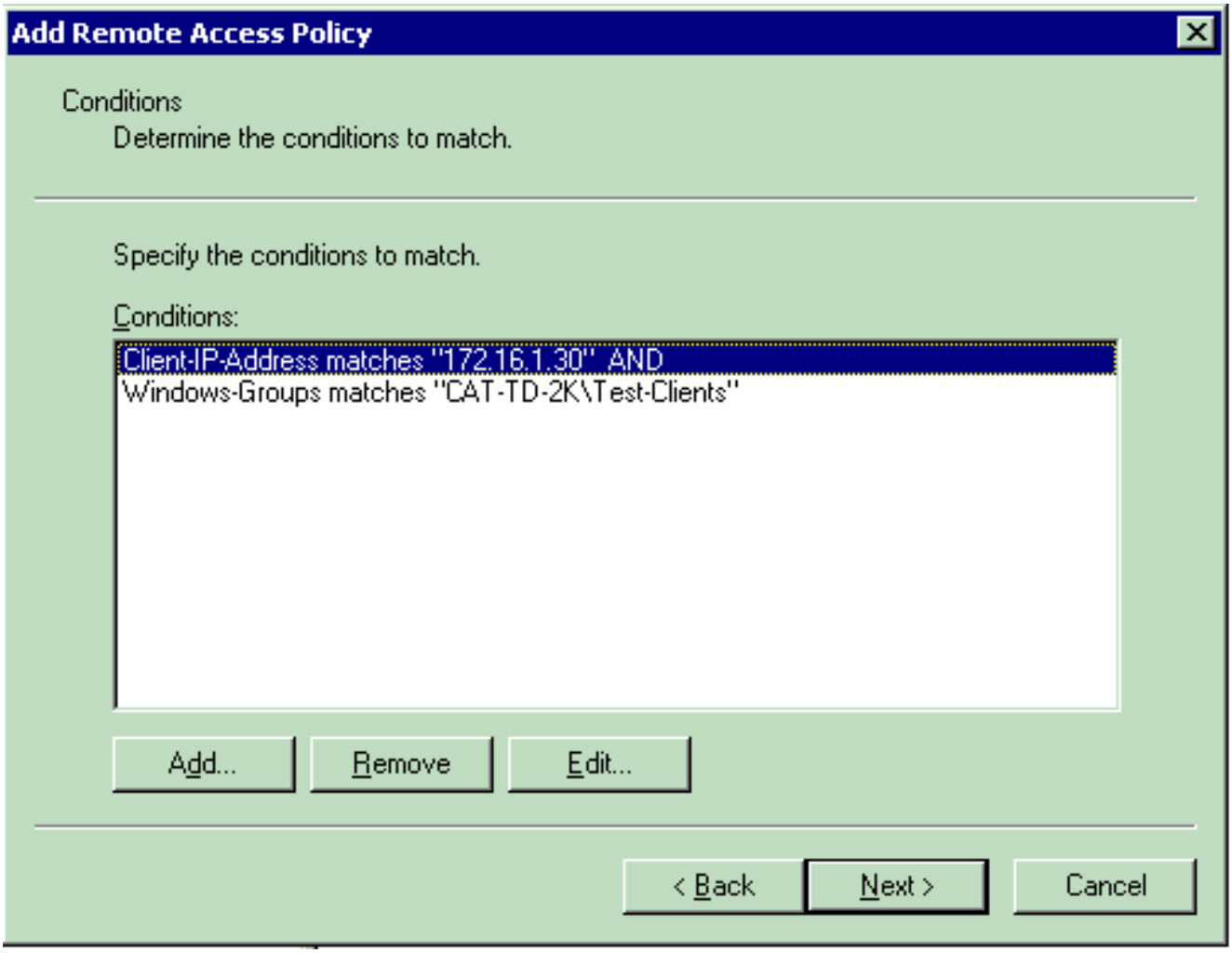
4. 从“属性类型”(Attribute types)菜单中，选择以下属性：**Client-IP-Address** — 输入AAA客户端的IP地址。在本例中，输入WLC IP地址，以便策略应用于来自WLC的数据包。



Windows组 — 选择将应用策略的Windows组（用户组）。示例如下

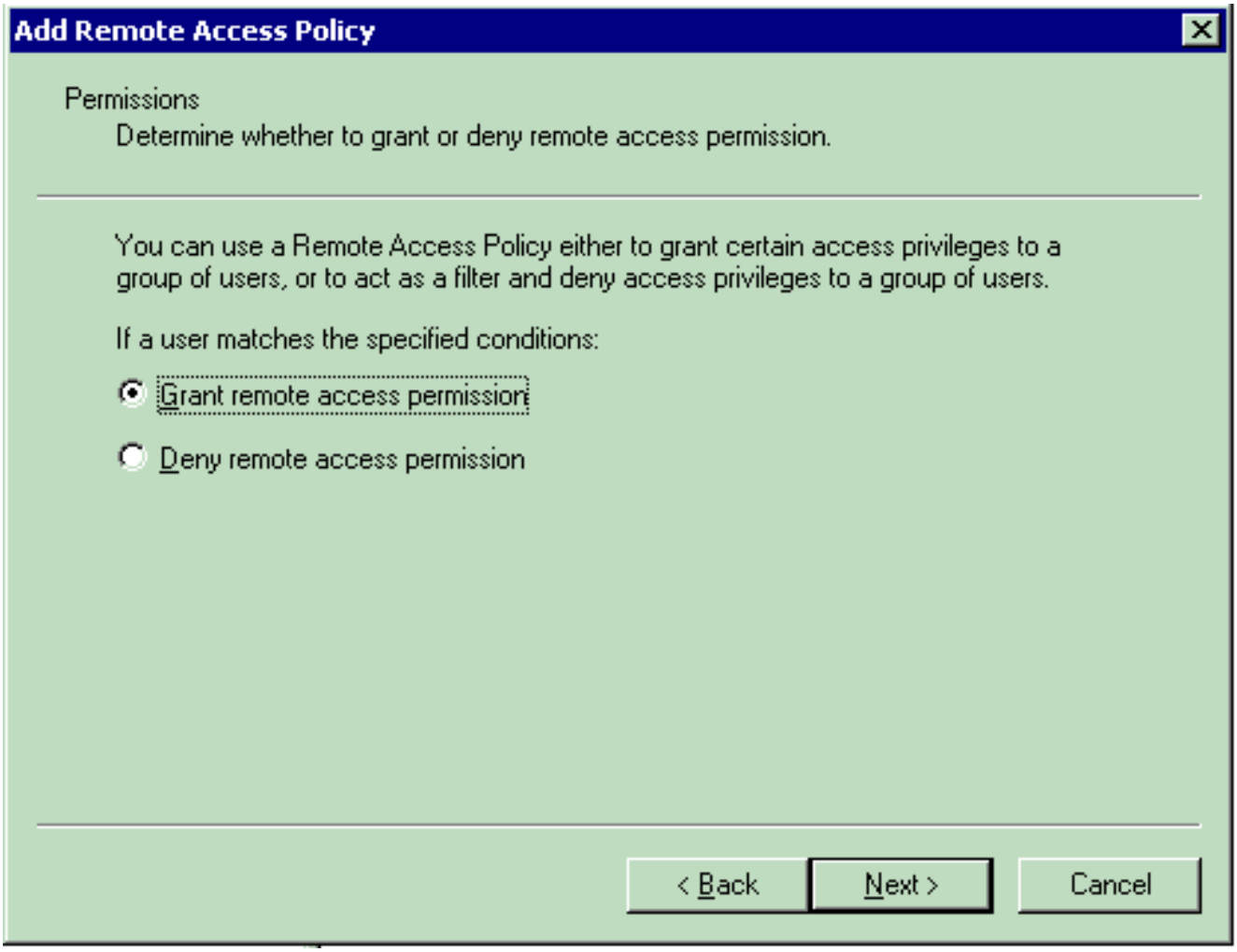


:

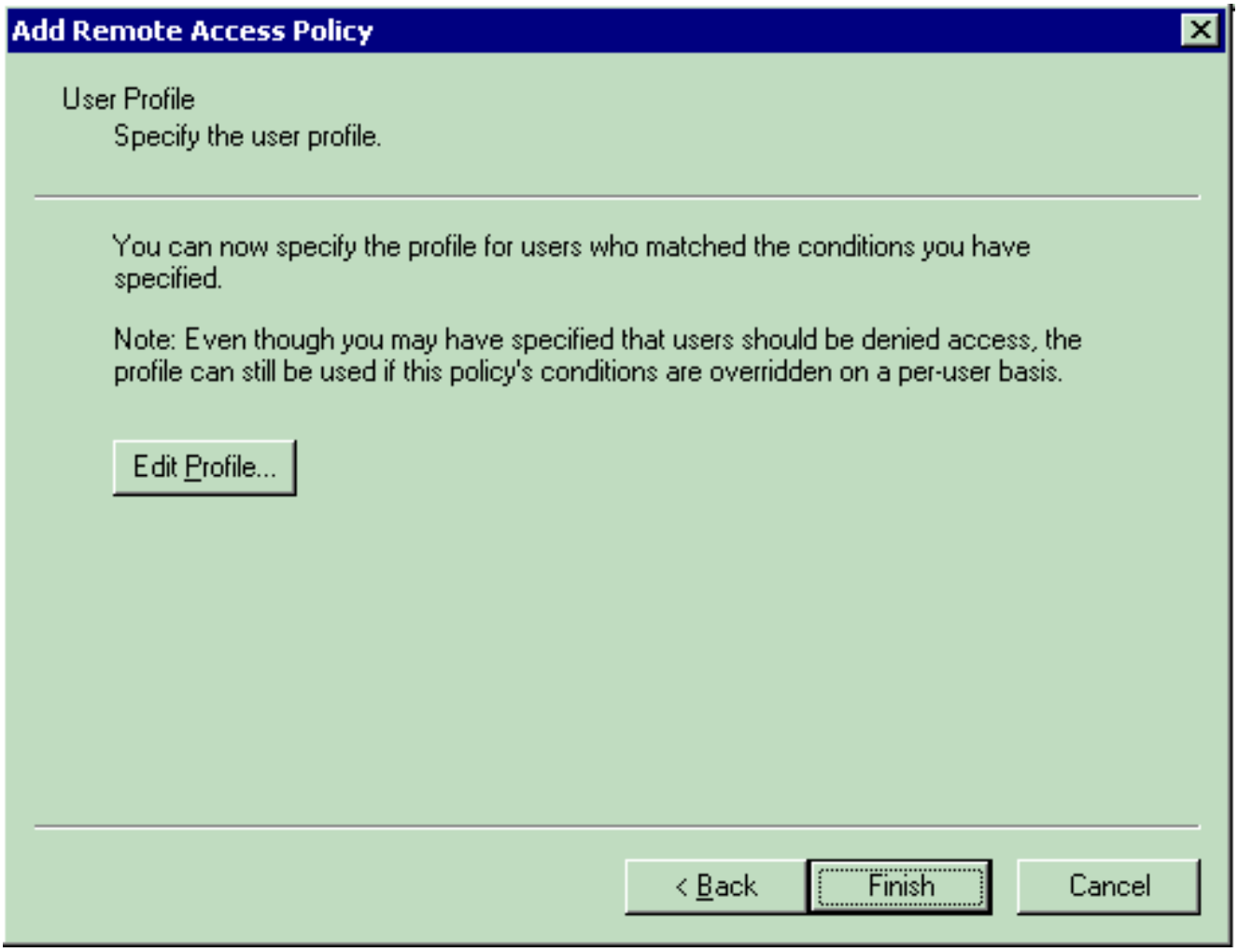


此示例仅显示两个条件。如果有更多条件，请添加这些条件，然后单击**Next**。系统将显示“权限”窗口。

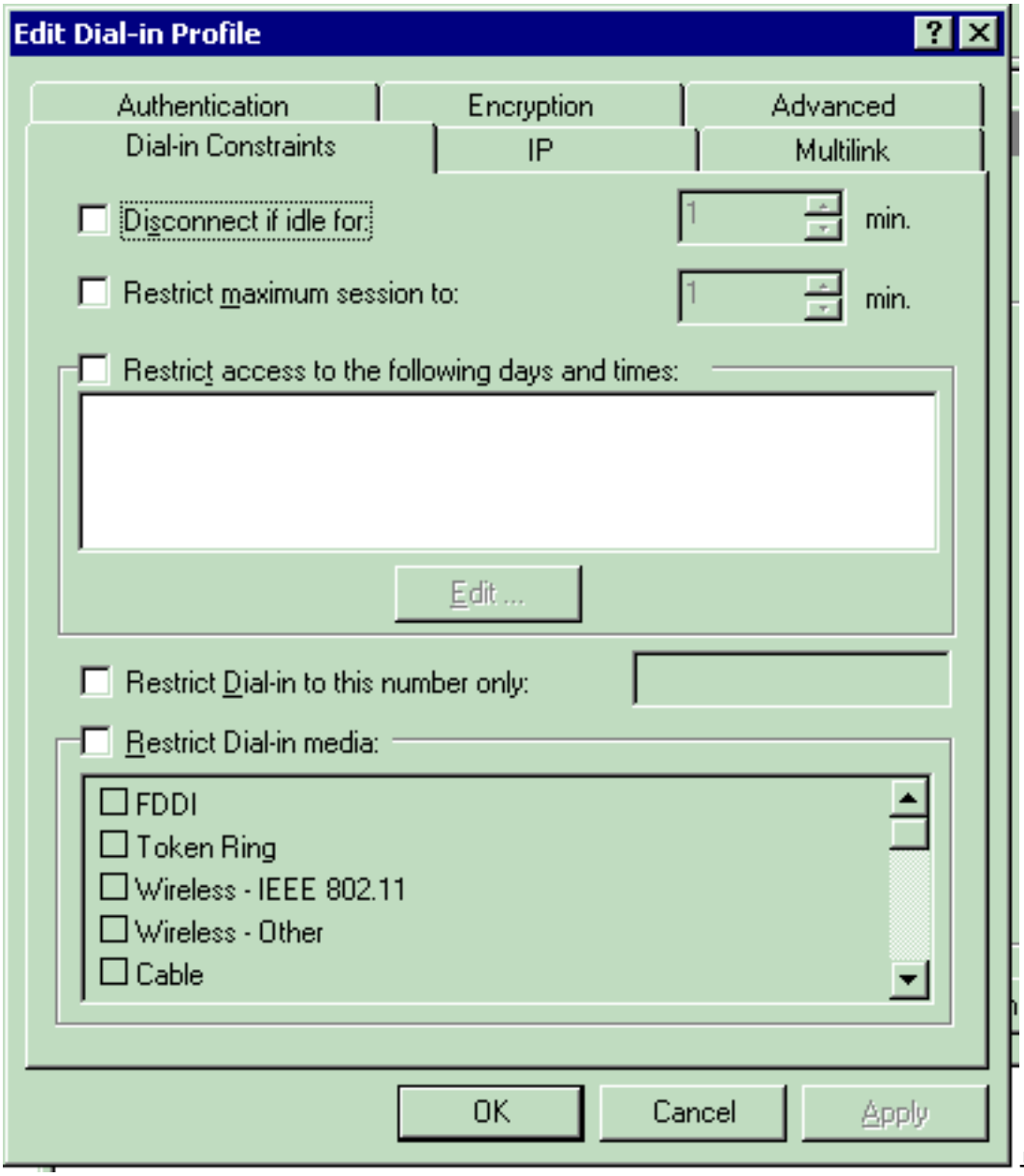
5. 在“权限”窗口中，选择“授**予远程访问权限”**。选择此选项后，如果用户符合指定条件（从步骤2开始），则用户将获得访问权限。



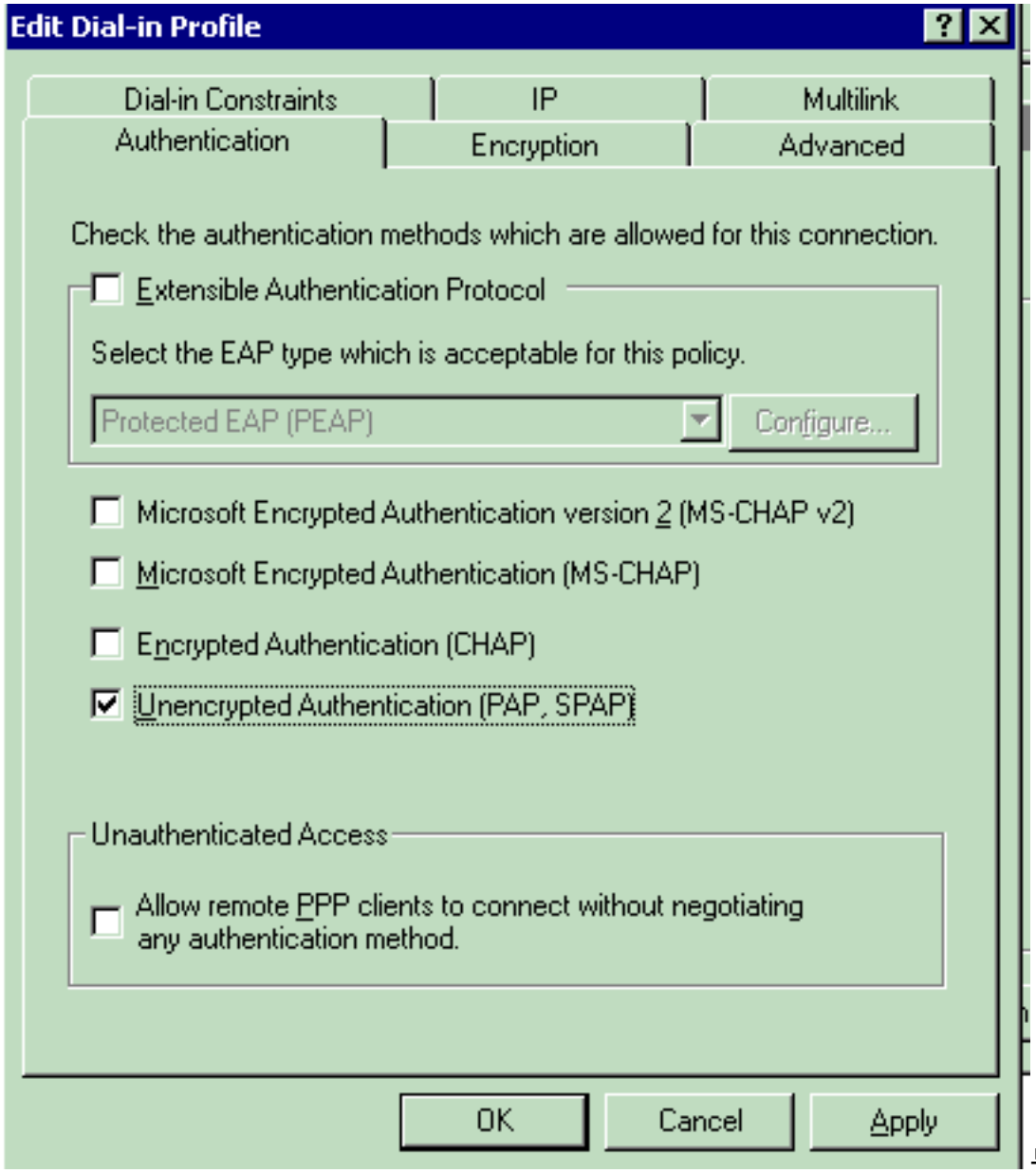
6. 单击 **Next**。
7. 下一步是设置用户配置文件。即使您可能已指定应根据条件拒绝用户或授予用户访问权限，但是，如果此策略的条件基于每个用户被覆盖，则仍然可以使用配置文件。



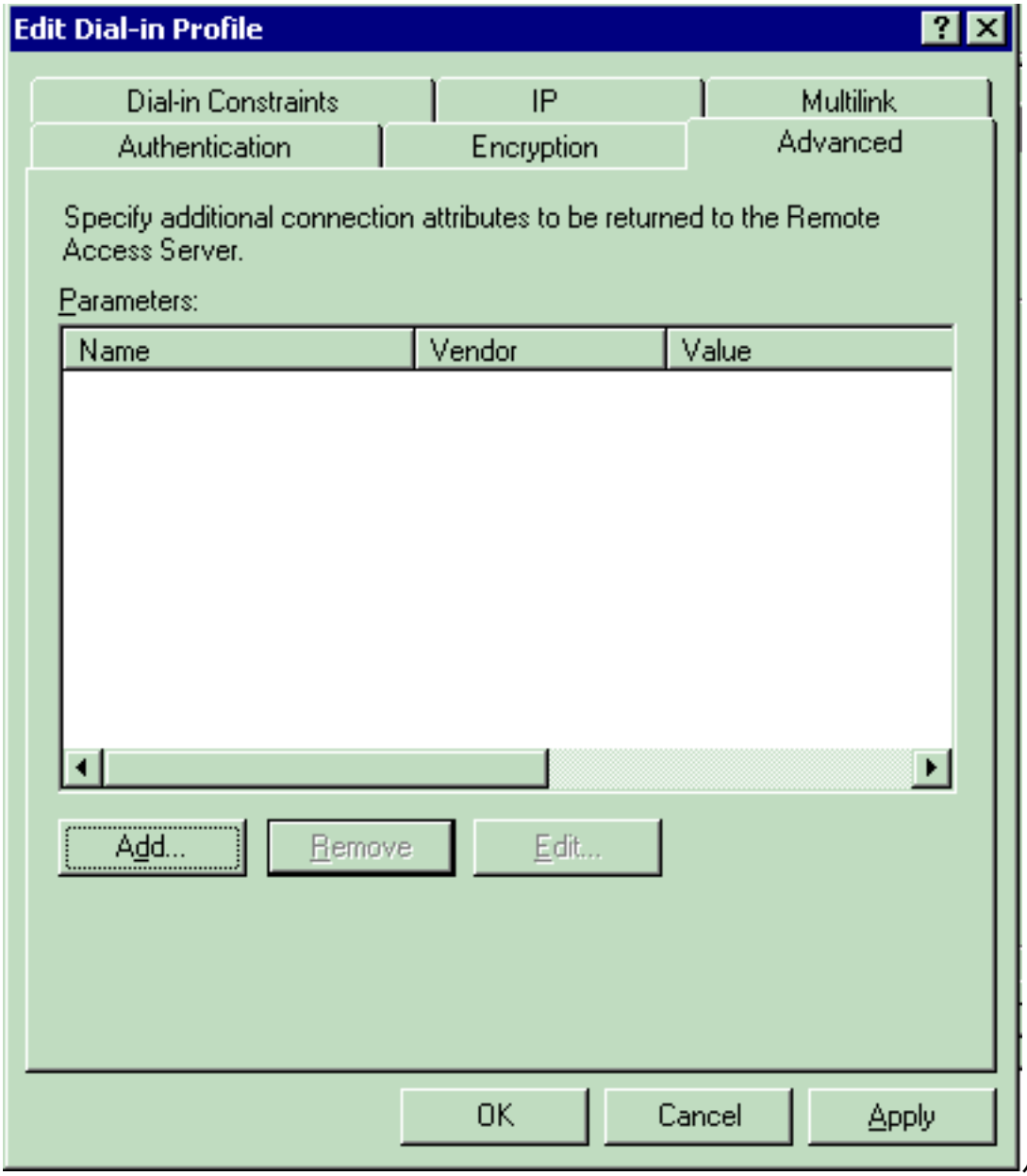
要配置用户配置文件，请在“用户配置文件”(User Profile)窗口中单击“编辑配置文件”(Edit Profile)。系统将显示Edit Dial-in Profile窗口。



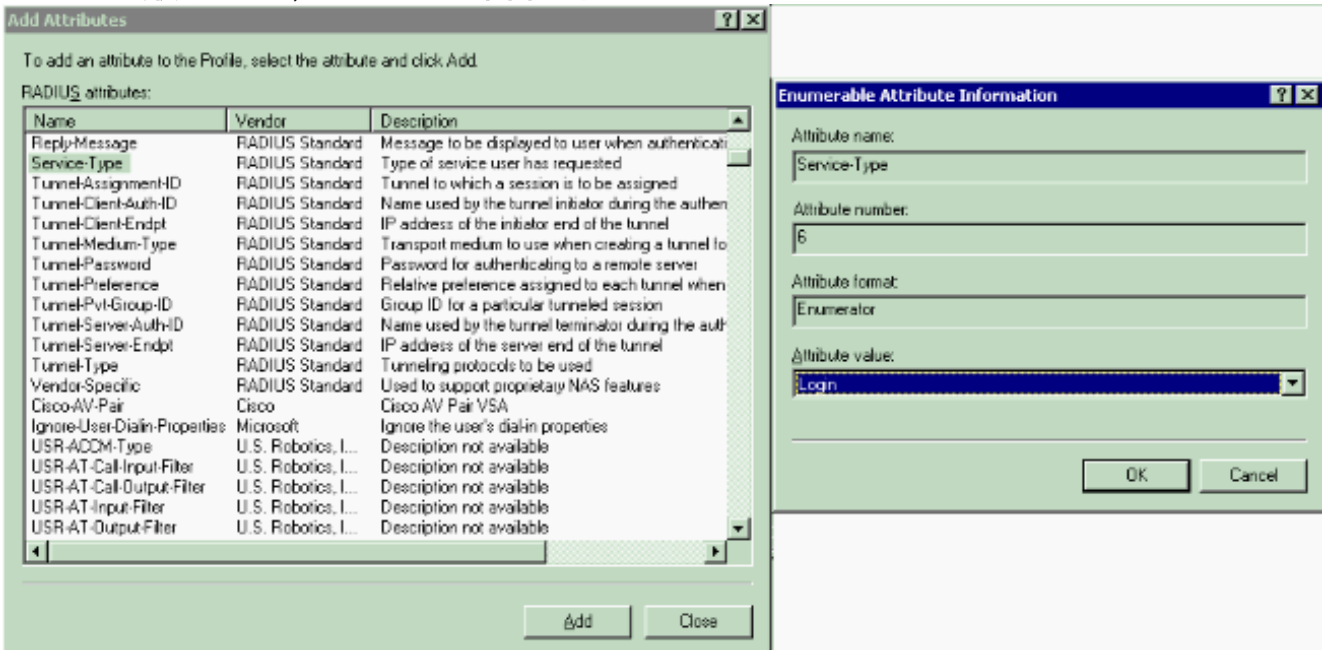
单击**Authentication**选项卡，然后选择WLAN中使用的身份验证方法。本示例使用未加密身份验证(PAP，SPAP)。



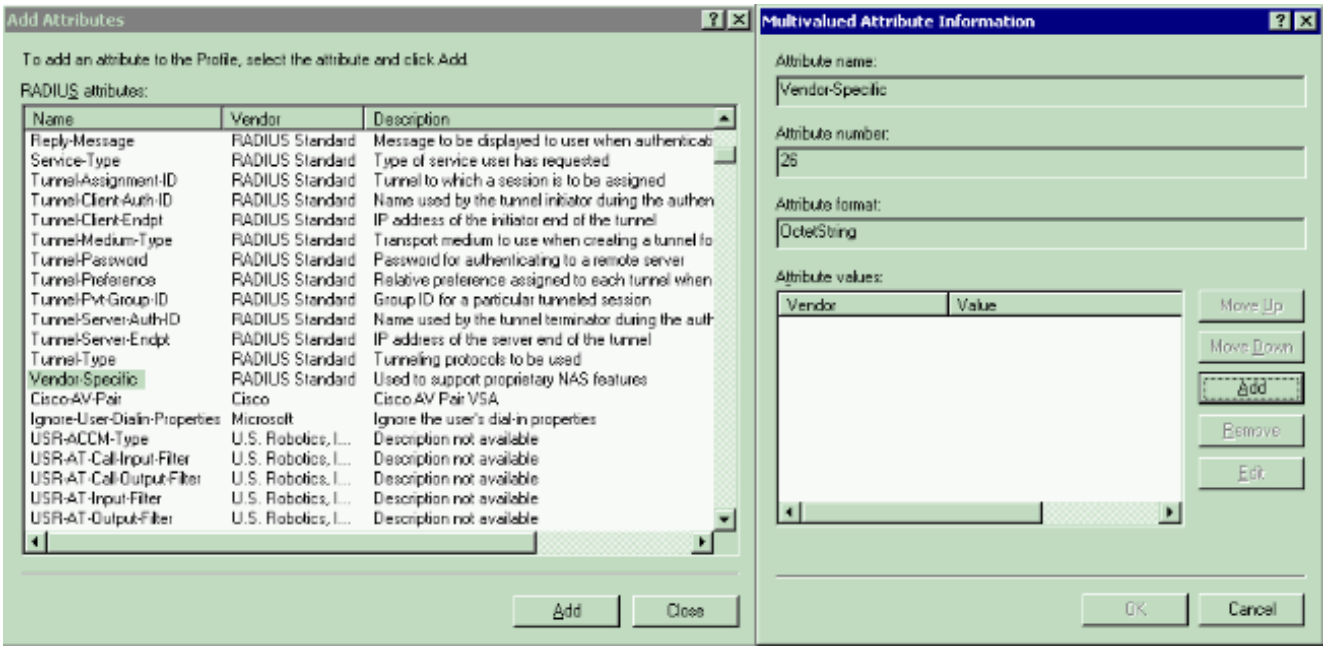
单击 **Advanced 选项卡。**删除所有默认参数，然后单击“**添加”**。



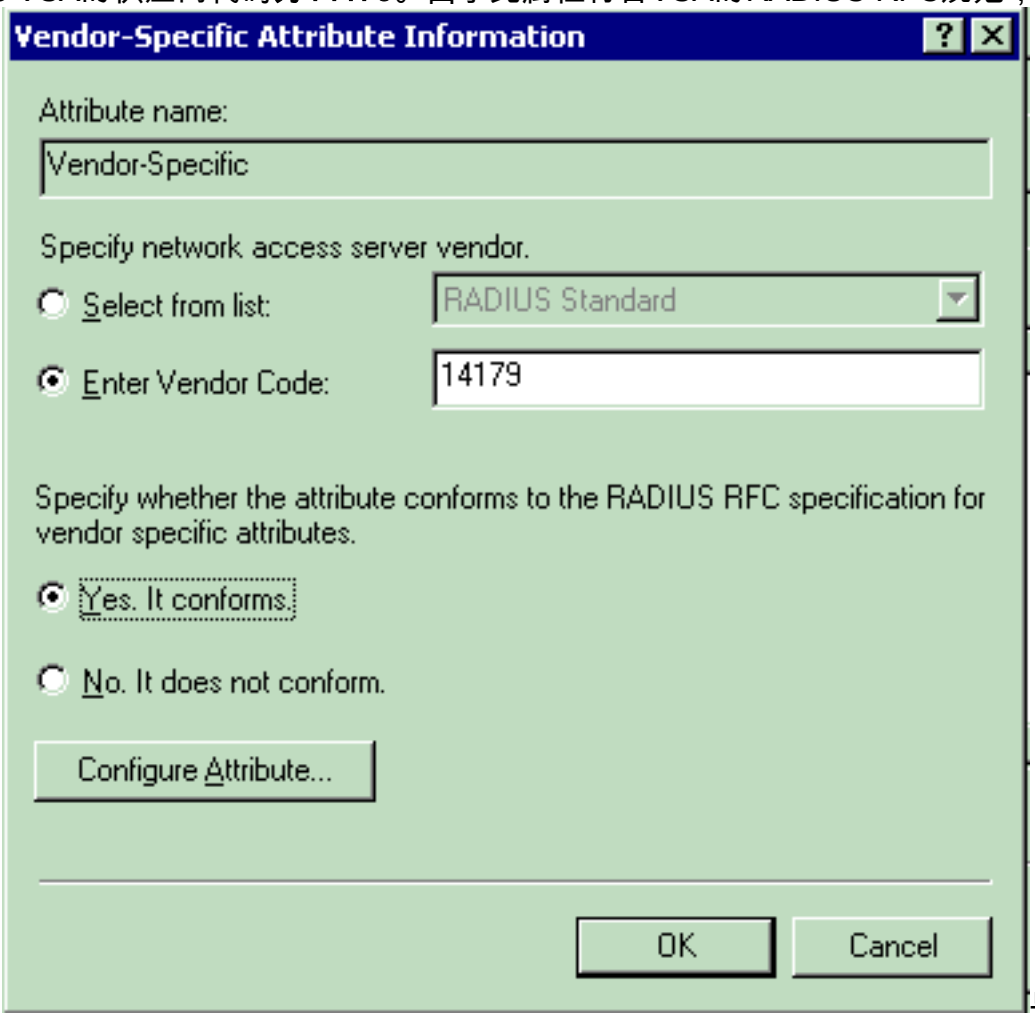
从“添**加属性**”窗口中**选择“服务类**型”，然后从下一**个窗口中选**择“登录”值。



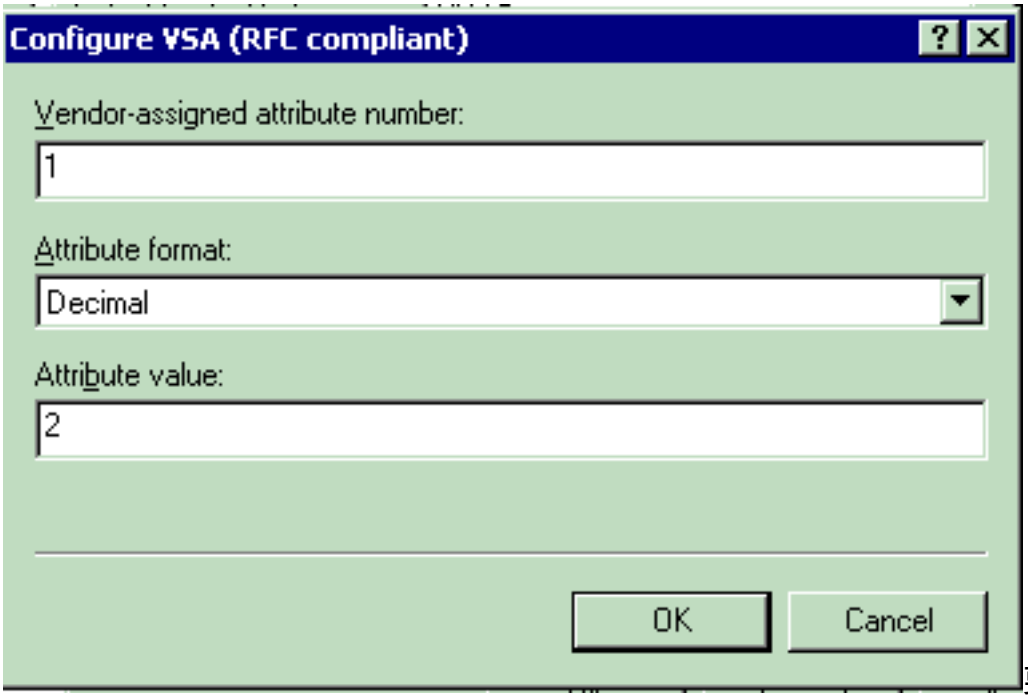
接下来，您需要从RADIUS**属性列表中选择**供应商特定属性。



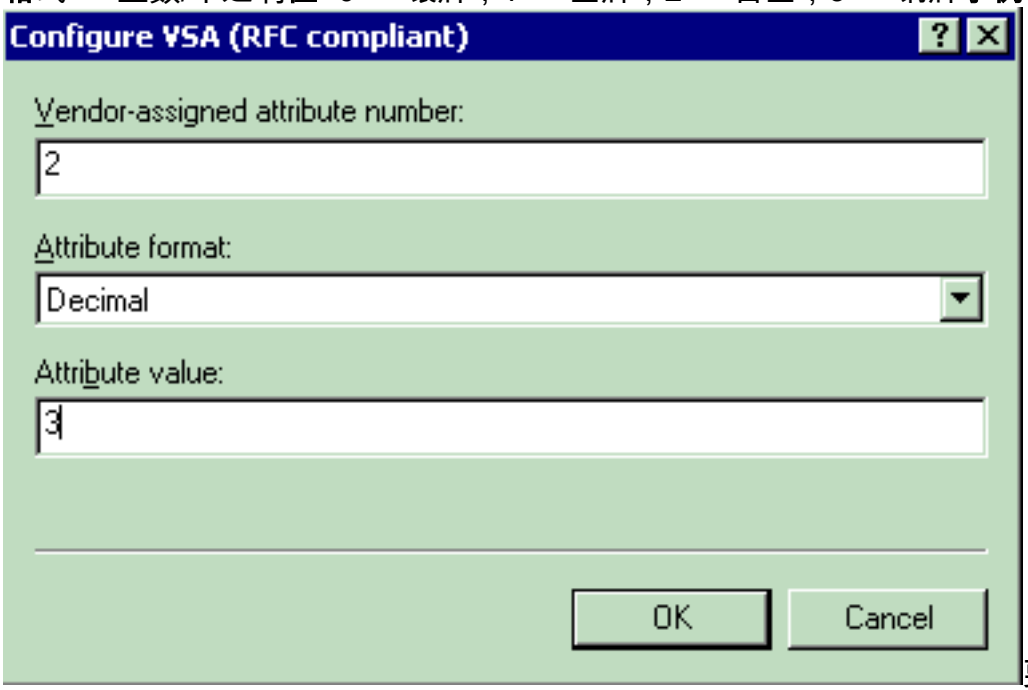
在下一个窗口中，单击**Add**以选择新的VSA。系统将显示供应商特定属性信息窗口。在“指定网络访问服务器供应商”下，选择**输入供应商代码**。输入Airespace VSA的供应商代码。Cisco Airespace VSA的供应商代码**为14179**。由于此属性符合VSA的RADIUS RFC规范，请选择**是。符合。**



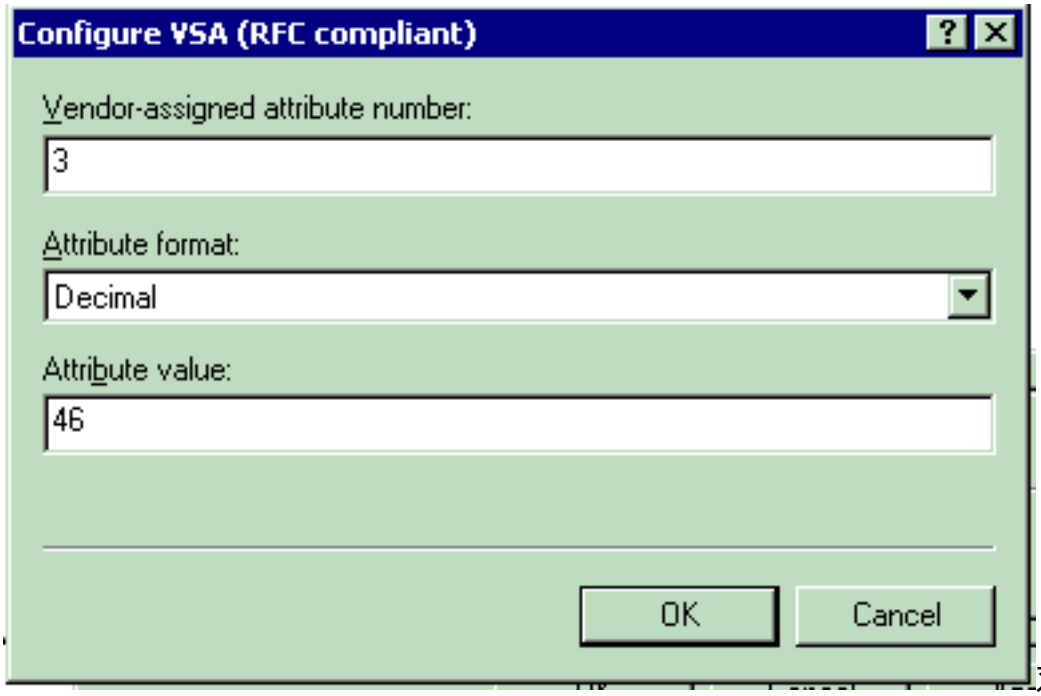
单击**Configure Attribute**。在Configure VSA（RFC兼容）窗口中，输入供应商分配的属性编号、属性格式和属性值，这取决于要使用的VSA。对于按用户设置WLAN-ID:**属性名**称 — Airespace-WLAN-Id**供应商分配的属性编**号 — 1**属性格**式 — 整数/十进制**值**— WLAN-ID**示例 1**



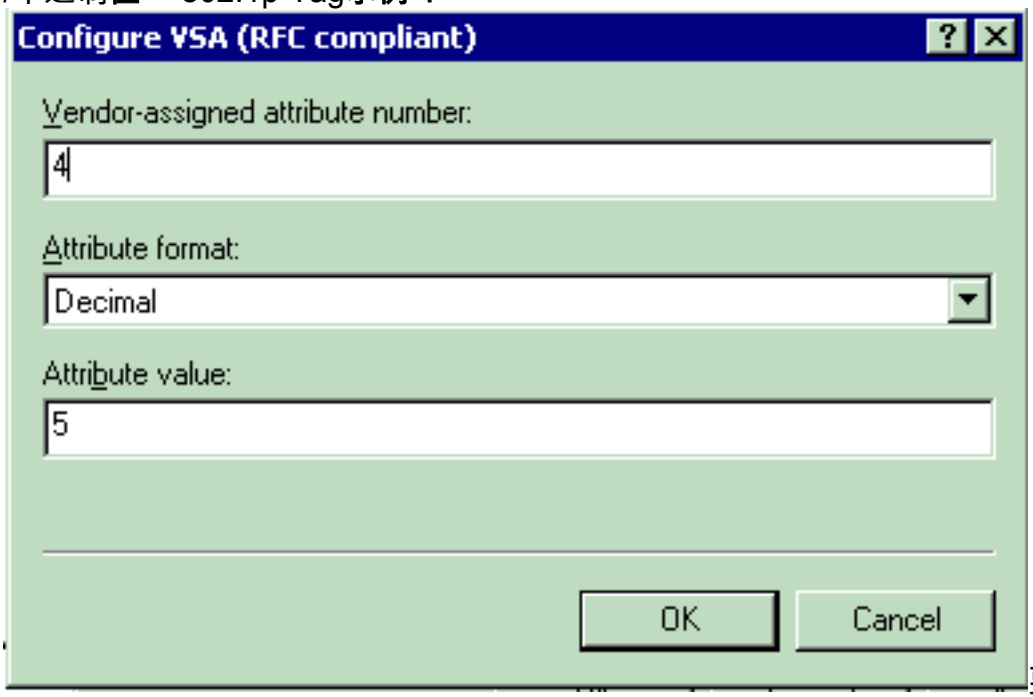
要按用户设置QoS配置文件，请执行以下操作：**属性名**称 — Airespace-QoS级别**供应商分配的属性编**号 — 2**属性格**式 — 整数/十进制**值**- 0 — 银牌；1 — 金牌；2 — 白金；3 — 铜牌**示例 2**



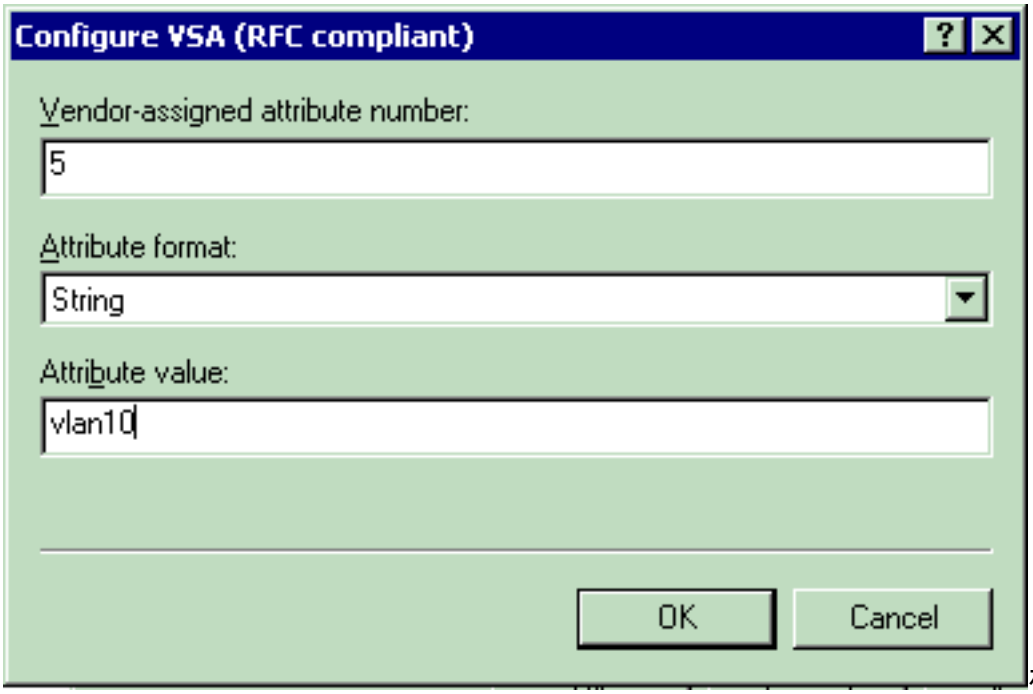
要按用户设置DSCP值，请执行以下操作：**属性名**称 — Airespace-DSCP**供应商分配的属性编号**- 3**属性格**式 — 整数/十进制**值**— DSCP值**示例 3**



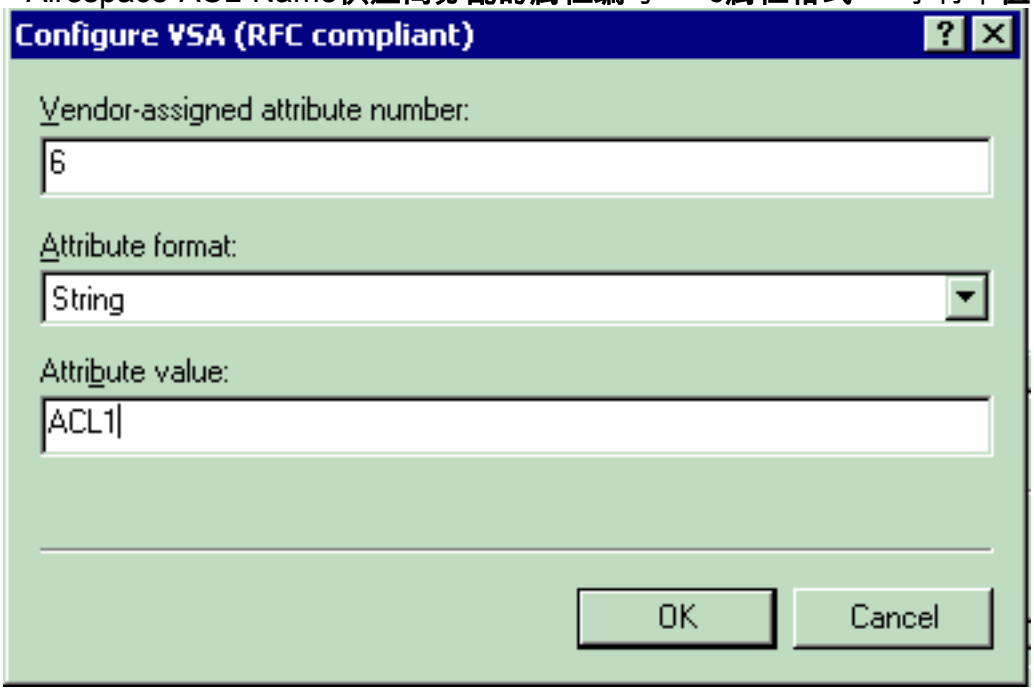
对于按用户设置802.1p-Tag:**属性名**称 — Airespace-802.1p-Tag**供应商分配的属性编**号 — 4**属性格**式 — 整数/十进制**值**— 802.1p-Tag**示例 4**



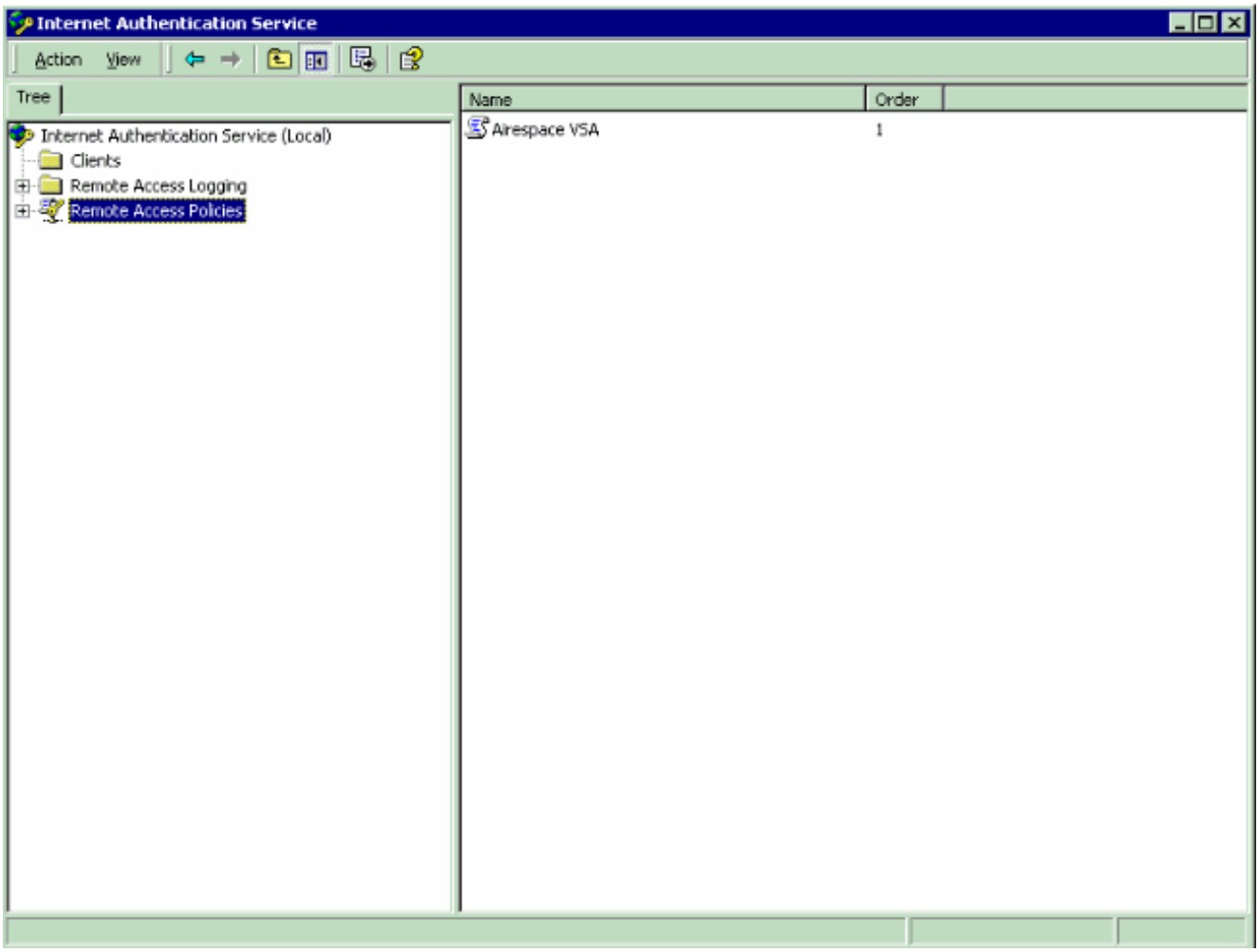
要按用户设置接口(VLAN)，请执行以下操作：**属性名**称 — Airespace-Interface-Name**供应商分配的属性编**号 — 5**属性格式** — 字符串**值** — 接口名称**示例 5**



根据每个用户设置ACL:**属性名**称 — Airespace-ACL-Name**供应商分配的属性编**号 — 6**属性格式** — 字符串**值**— ACL名称**示例 6**

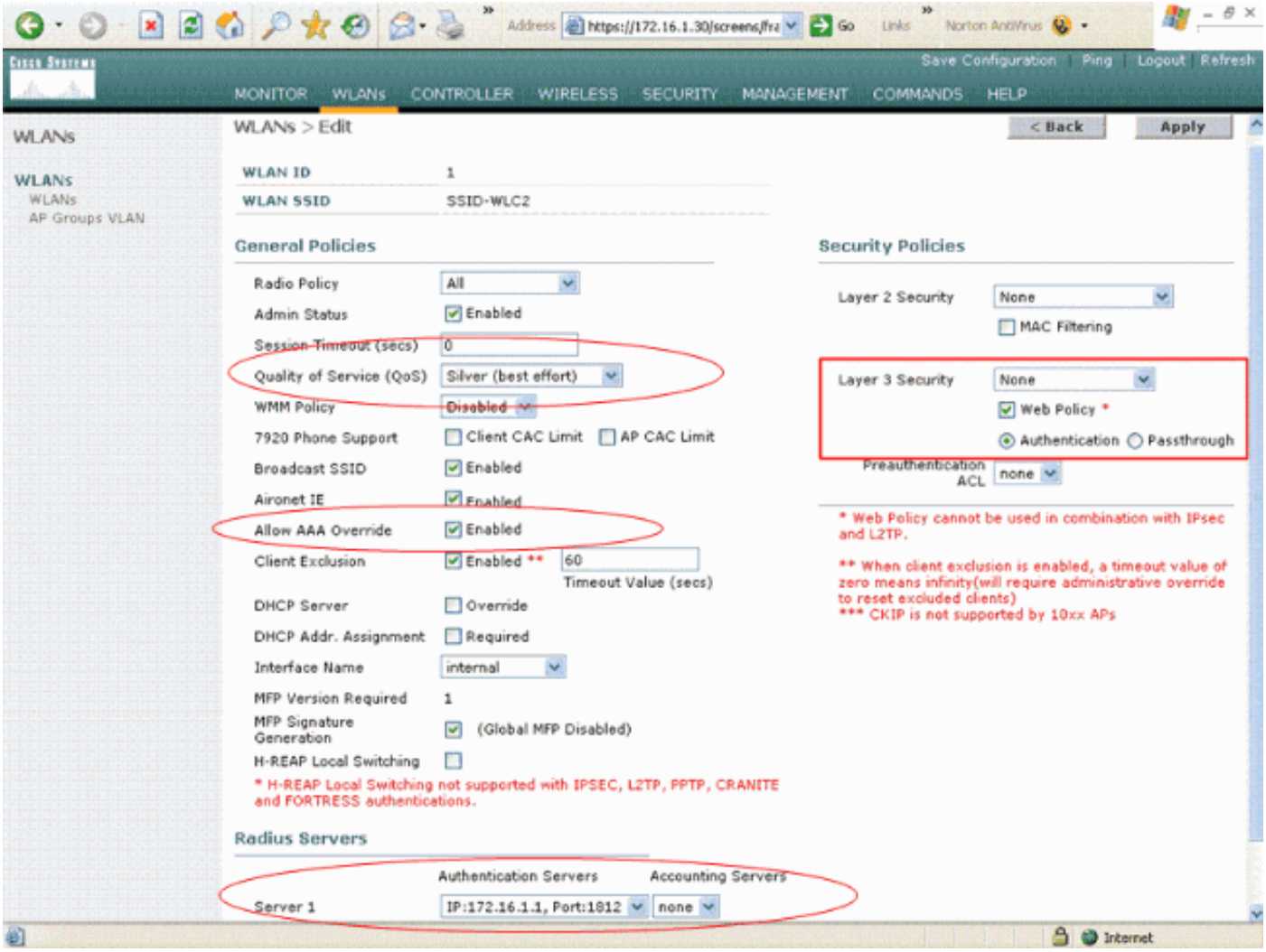


8. 配置VSA后，单击**OK**，直到看到User profile窗口。
9. 然后，单击**Finish**以完成配置。您可以在远程访问策略下看到新策略。



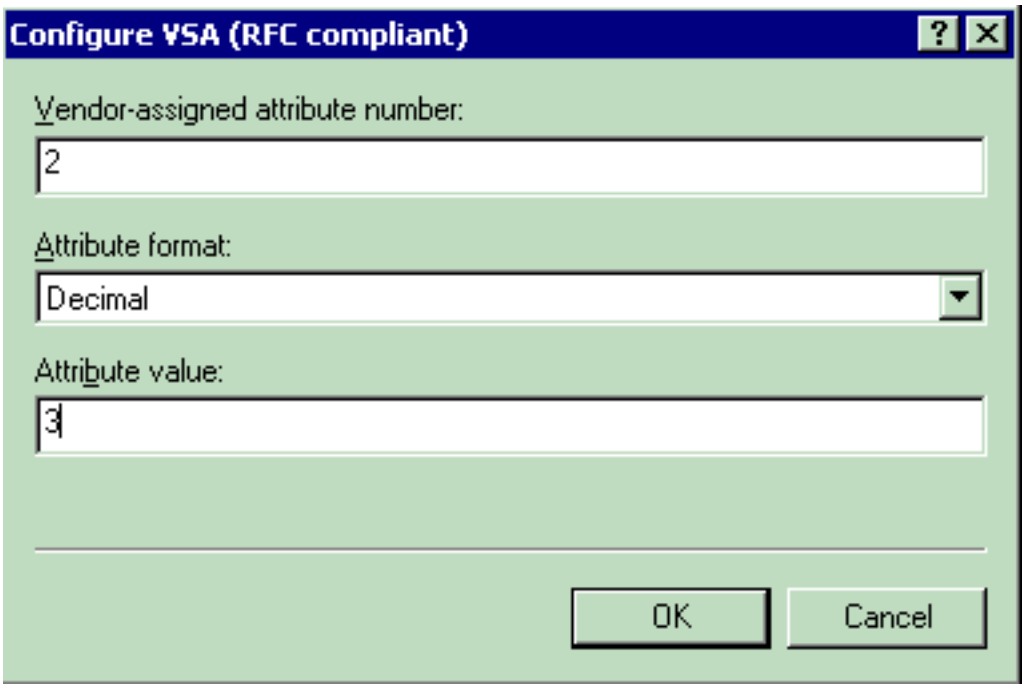
配置示例

在本例中，为Web身份验证配置了WLAN。用户由IAS RADIUS服务器进行身份验证，并且RADIUS服务器配置为按用户分配QoS策略。



从此窗口中您可以看到，Web身份验证已启用，身份验证服务器为172.16.1.1,WLAN上也启用了AAA覆盖。此WLAN的默认QoS设置设置为银牌。

在IAS RADIUS服务器上，配置远程访问策略，该策略返回RADIUS接受请求中的QoS属性Bronze。当您配置特定于QoS属性的VSA时，会执行此操作。



有关如何在IAS服务器上配置远程访问策略的详细信息，请参阅本文档的在IAS上配置远程访问策略部分。

为此设置配置IAS服务器、WLC和LAP后，无线客户端可以使用Web身份验证进行连接。

验证

使用本部分可确认配置能否正常运行。

当用户使用用户ID和密码连接到WLAN时，WLC将凭证传递到IAS RADIUS服务器，该服务器根据远程访问策略中配置的条件和用户配置文件对用户进行身份验证。如果用户身份验证成功，RADIUS服务器会返回RADIUS接受请求，该请求还包含AAA覆盖值。在这种情况下，将返回用户的QoS策略。

您可以发出**debug aaa all enable**命令，以查看身份验证期间发生的事件顺序。以下为示例输出：

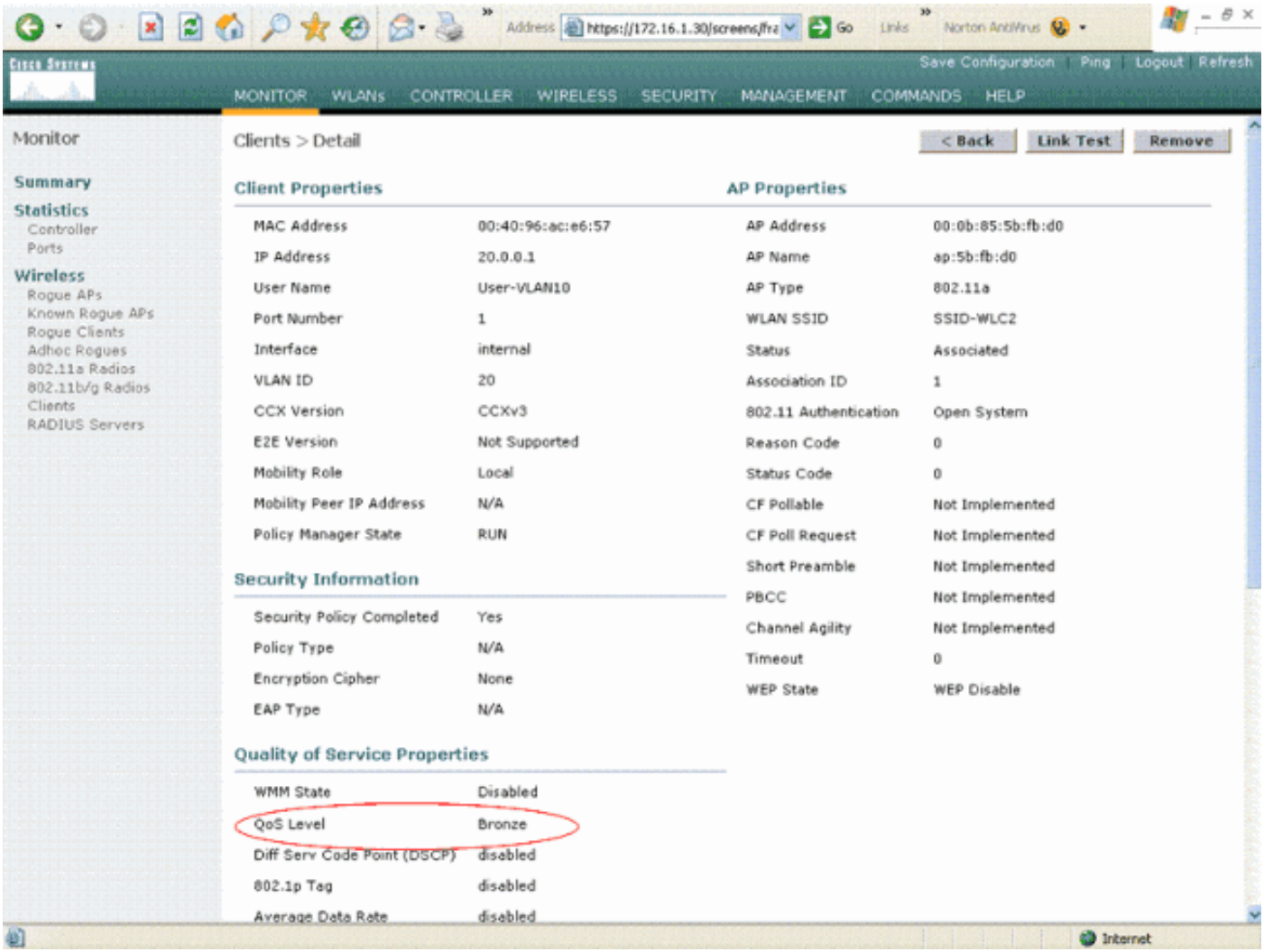
```
(Cisco Controller) > debug aaa all enable
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 28:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 18:14:24 2007:       structureSize.............................70
Wed Apr 18 18:14:24 2007:       resultCode................................0
Wed Apr 18 18:14:24 2007:       protocolUsed..............................0x00000008
Wed Apr 18 18:14:24 2007:       proxyState................................
                                28:1F:00:00:00:00-00:00
Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs:
Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type..........................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier..............
                                    0x00000000 (0) (4 bytes)
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 29:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 18:14:24 2007:       structureSize.............................70
Wed Apr 18 18:14:24 2007:       resultCode................................0
Wed Apr 18 18:14:24 2007:       protocolUsed..............................0x00000008
Wed Apr 18 18:14:24 2007:       proxyState................................
                                29:1F:00:00:00:00-00:00
Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs:
Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type..........................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier..............
                                    0x00000000 (0) (4 bytes)
Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10
Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc
Wed Apr 18 18:15:08 2007:       Callback.....................................0x8250c40
Wed Apr 18 18:15:08 2007:       protocolType.................................0x00000001
Wed Apr 18 18:15:08 2007:       proxyState...................................
                                00:40:96:AC:E6:57-00:00
Wed Apr 18 18:15:08 2007:       Packet contains 8 AVPs (not shown)
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Packet
                          (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-96:ac
Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00  00 00 00 00 00 00 00 00
                          ...h............
Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73  65 72 2d 56 4c 41 4e 31
                          ......User-VLAN1
```

```
Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a  ba 57 38 11 bc 9a 5d 59
                          0...2W.*.W8...]Y
Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00  01 04 06 ac 10 01 1e 20
                          ..#.............
Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00  00 37 63 01 06 00 00 00
                          .WLC2....7c.....
Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e 30 2e  30 2e 31 1e 0d 31 37 32
                          ...20.0.0.1..172
Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e 31 2e 33 30 .16.1.30
Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc  e4 ea 41 3e 28 7e cc bc
                          ...F?.....A>(~..
Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00  37 63 02 06 00 00 00 03
                          ..a.....7c......
Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20  37 d0 03 e6 00 00 01 37
                          ........7......7
Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01 c7  7a 8b 35 20 31 80 00 00
                          ........z.5.1...
Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00 1b      ......
Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2
Wed Apr 18 18:15:08 2007: ****Enter processRadiusResponse: response code=2
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Access-Accept received from RADIUS server
                          172.16.1.1 for mobile 00:40:96:ac:e6:57 receiveId = 0
Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520
Wed Apr 18 18:15:08 2007:       structureSize.............................114
Wed Apr 18 18:15:08 2007:       resultCode................................0
Wed Apr 18 18:15:08 2007:       protocolUsed..............................0x00000001
Wed Apr 18 18:15:08 2007:       proxyState................................
                                00:40:96:AC:E6:57-00:00
Wed Apr 18 18:15:08 2007:       Packet contains 3 AVPs:
Wed Apr 18 18:15:08 2007:           AVP[01] Airespace / QOS-Level...................
                                    0x00000003 (3) (4 bytes)
Wed Apr 18 18:15:08 2007:           AVP[02] Service-Type............................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:08 2007:           AVP[03] Class...................................
                                    DATA (30 bytes)
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station
                          00:40:96:ac:e6:57
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
        source: 48, valid bits: 0x3
        qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
        vlanIfName: '', aclName: '
Wed Apr 18 18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc
Wed Apr 18 18:15:12 2007:       Packet contains 13 AVPs:
Wed Apr 18 18:15:12 2007:           AVP[01] User-Name...............................
                                    User-VLAN10 (11 bytes)
Wed Apr 18 18:15:12 2007:           AVP[02] Nas-Port................................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[03] Nas-Ip-Address..........................
                                    0xac10011e (-1408237282) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[04] NAS-Identifier..........................
                                    0x574c4332 (1464615730) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[05] Airespace / WLAN-Identifier.............
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[06] Acct-Session-Id.........................
                                    4626602c/00:40:96:ac:e6:57/16 (29 bytes)
Wed Apr 18 18:15:12 2007:           AVP[07] Acct-Authentic..........................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[08] Tunnel-Type.............................
                                    0x0000000d (13) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[09] Tunnel-Medium-Type......................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[10] Tunnel-Group-Id.........................
                                    0x3230 (12848) (2 bytes)
```

```
Wed Apr 18 18:15:12 2007:          AVP[11] Acct-Status-Type.....................
                                   0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:          AVP[12] Calling-Station-Id.....................
                                   20.0.0.1 (8 bytes)
Wed Apr 18 18:15:12 2007:          AVP[13] Called-Station-Id.....................
                                   172.16.1.30 (11 bytes)
```

从输出中您可以看到，用户已通过身份验证。然后，AAA覆盖值随RADIUS接受消息返回。在这种情况下，为用户提供铜级服务的QoS策略。

您也可以在WLC GUI上验证这一点。示例如下：



注意：此SSID的默认QoS配置文件为银牌。但是，由于选择了AAA覆盖，并且用户在IAS服务器上配置了铜级QoS配置文件，因此默认QoS配置文件被覆盖。

故障排除

您可以在WLC上**使用debug aaa all enable**命令排除配置故障。本文档的“验证”部分显示了此调试在工作网络中的输出示例。

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

相关信息

- Cisco 无线 LAN 控制器配置指南 4.0 版

- 根据 WLC 和 Cisco Secure ACS 的 SSID 限制 WLAN 访问的配置示例
- 无线产品支持
- 技术支持和文档 - Cisco Systems