

思科在Microsoft IAS RADIUS服务器配置示例的Airespace VSAs

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置Airespace的VSAs IAS](#)

[配置WLC作为IAS的一个AAA客户端](#)

[配置在IAS的Remote access Policy](#)

[配置示例](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文显示您如何配置Microsoft互联网认证服务(IAS)服务器支持思科Airespace卖方细节属性(VSAs)。思科的Airespace VSAs厂商代码是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：

- 知识如何配置IAS服务器
- 轻量级接入点(拉普)和Cisco无线LAN控制器(WLCs)的配置的知识
- 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：

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

- 802.11 a/b/g无线客户端适配器固件2.5
- 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： 本文打算提供读者在IAS服务器要求的配置的一示例支持思科Airespace VSAs。在本文提交的IAS服务器配置在实验室里测试了并且工作正如所料。如果有麻烦配置IAS服务器的，与帮助的Microsoft联系。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

在多数无线局域网(WLAN)系统中，每WLAN有适用于所有客户端关联与服务集标识(SSID)的一项静态策略。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。

然而，Cisco无线LAN解决方案支持标识网络，允许网络通告单个SSID和特定用户继承根据他们的用户配置文件或安全策略的另外QoS。您能控制使用标识网络的特定策略包括：

- **服务质量**—当在RADIUS访问的存在接受时，QoS-Level值改写在WLAN配置文件指定的QoS值。
- **ACL** —当访问控制表(ACL)属性是存在RADIUS访问时请接受，系统运用ACL名称到客户端工作站，在验证后。这撤销的所有ACL都被分配到接口上。
- **VLAN** —当VLAN Interface-Name或VLAN标记是存在RADIUS访问时请接受，系统放置客户端在一个特定接口。
- **WLAN ID** —当WLAN-ID属性是存在RADIUS访问时请接受，系统应用WLAN-ID (SSID)到客户端工作站，在验证后。WLAN ID由在验证所有实例的WLC发送除了IPSec的。在Web验证，如果WLC接收在验证答复的一个ID属性从AAA服务器和它的情况下不匹配WLAN的ID，验证拒绝。安全方法的其他类型不执行此。
- **DSCP值**—当在RADIUS访问的存在接受时，DSCP值改写在WLAN配置文件指定的DSCP值。
- **802.1p TAG** —当在RADIUS访问的存在接受时，802.1p值改写在WLAN配置文件指定的默认。

注意： VLAN功能只支持MAC过滤，802.1X和Wi-Fi保护访问(WPA)。VLAN功能不支持Web验证或IPSec。操作系统的本地MAC过滤器数据库被延伸包括接口名称。这允许建立接口客户端应该分配的本地MAC过滤器指定。可能也使用一个分开的RADIUS服务器，使用安全菜单，但是必须定义RADIUS服务器。

参考[配置标识网络](#)关于标识网络的更多信息。

配置Airespace的VSAs IAS

为了配置Airespace的VSAs IAS，您需要完成这些步骤：

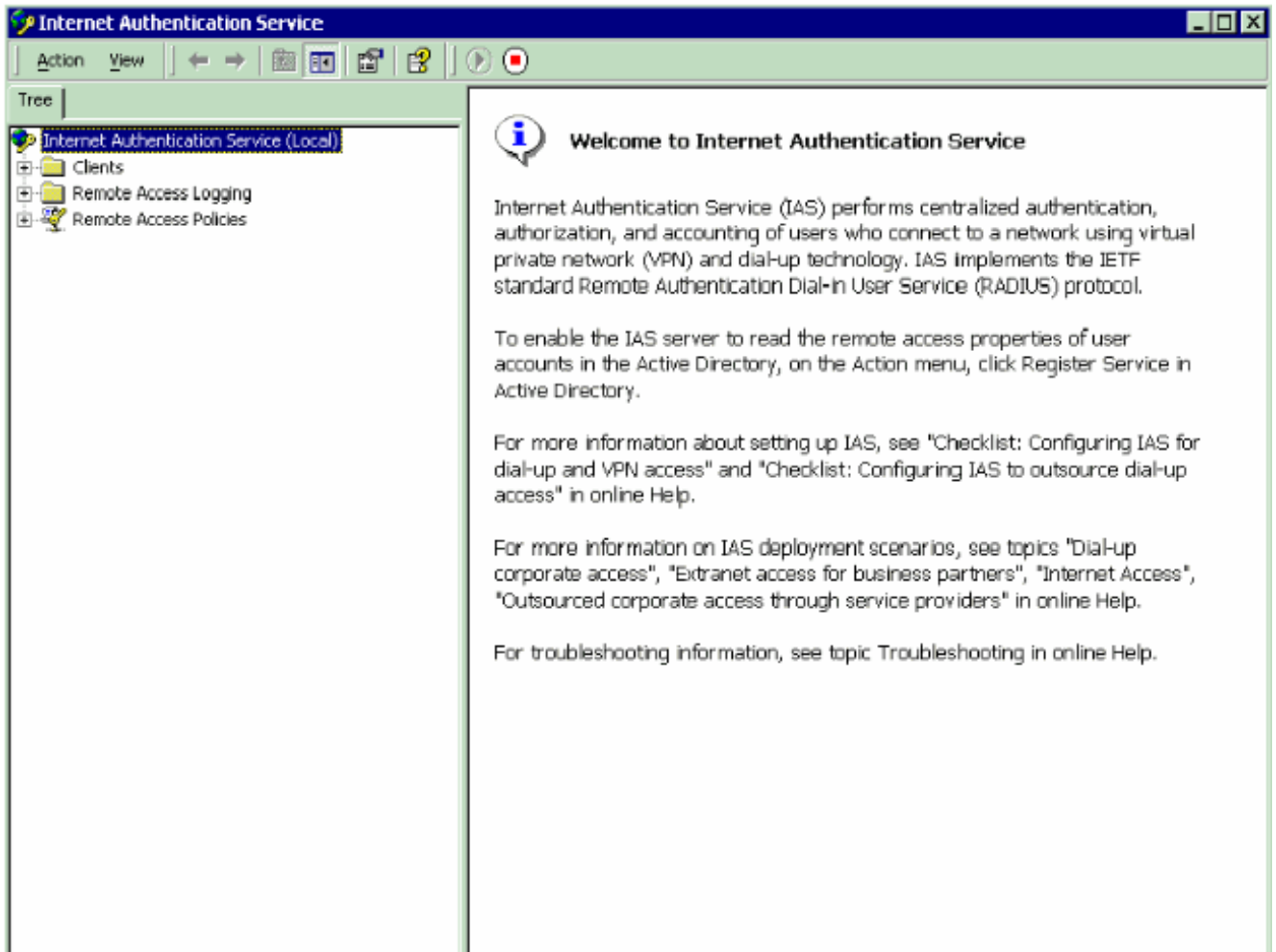
1. [配置WLC作为IAS的一个AAA客户端](#)
2. [配置在IAS的Remote access Policy](#)

注意：VSAs根据Remote access Policy配置。

[配置WLC作为IAS的AAA客户端](#)

完成这些步骤为了配置WLC作为IAS的一个AAA客户端：

1. 点击**Programs > Administrative工具> Internet验证服务**为了启动在Microsoft 2000服务器的IAS。



2. 用鼠标右键单击客户端文件夹并且选择**新的客户端**为了添加一个新的RADIUS客户端。
3. 在添加客户端窗口，请输入客户端的名称并且选择**RADIUS**作为协议。然后单击 **Next**。在本例中，客户端名称是**WLC-1**。**注意**：默认情况下，协议设置为RADIUS。

Add Client [X]

Name and Protocol
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

Friendly name:

Protocol:

< Back Next > Cancel

4. 在添加RADIUS客户端窗口，请输入**客户端IP地址**，**客户端供应商**和**共享机密**。在您输入客户端信息后，请点击**芬通社**。此示例显示客户端名为WLC-1用172.16.1.30的IP地址，客户端供应商设置为**思科**，并且共享机密是cisco123

:

Add RADIUS Client [X]

Client Information
Specify information regarding the client.

Client address (IP or DNS):
172.16.1.30 [Verify...]

Client-Vendor:
Cisco [v]

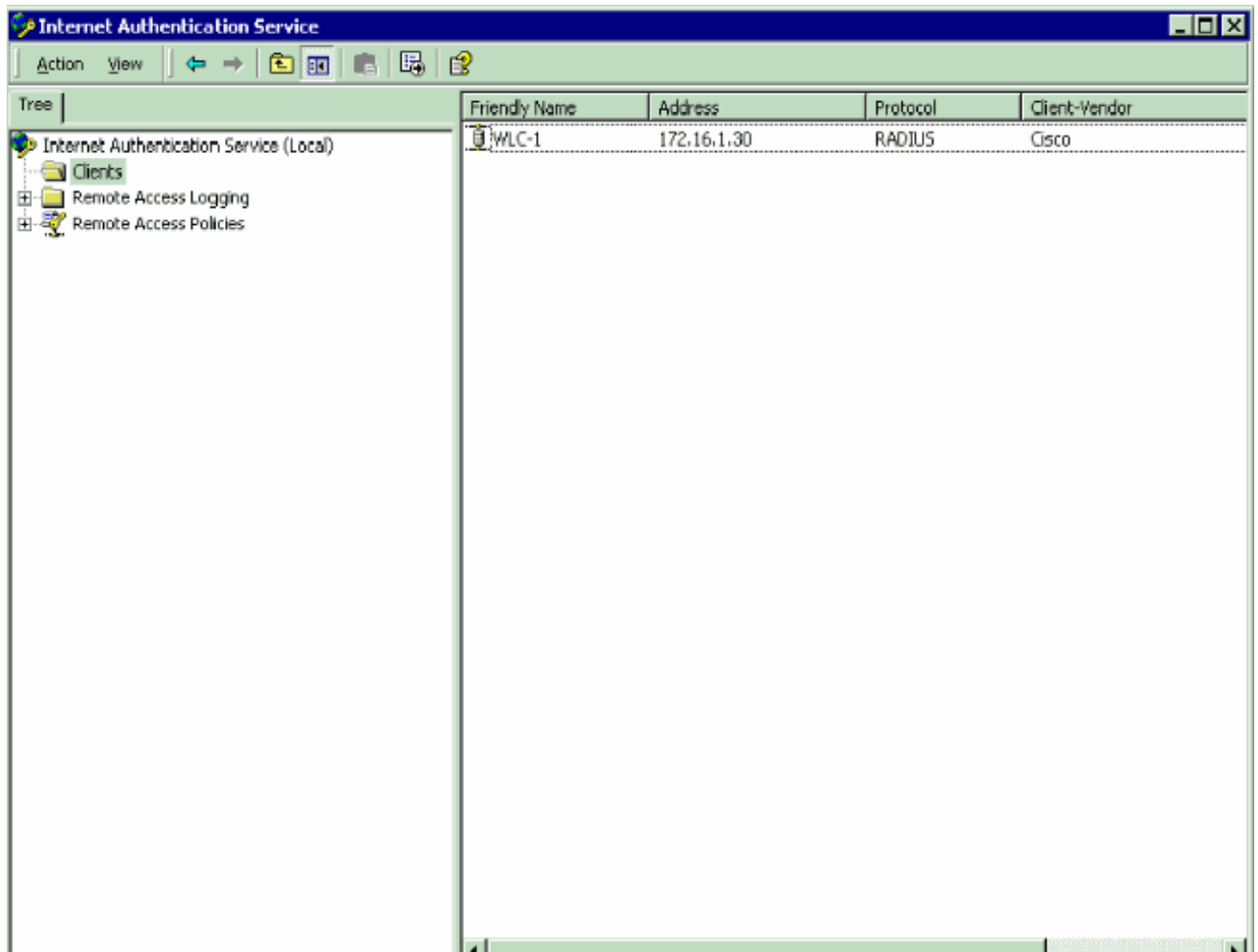
Client must always send the signature attribute in the request

Shared secret: [xxxxxxxx]

Confirm shared secret: [xxxxxxxx]

< Back Finish Cancel

有此信息，名为WLC-1的WLC被添加作为IAS服务器的AAA客户端。

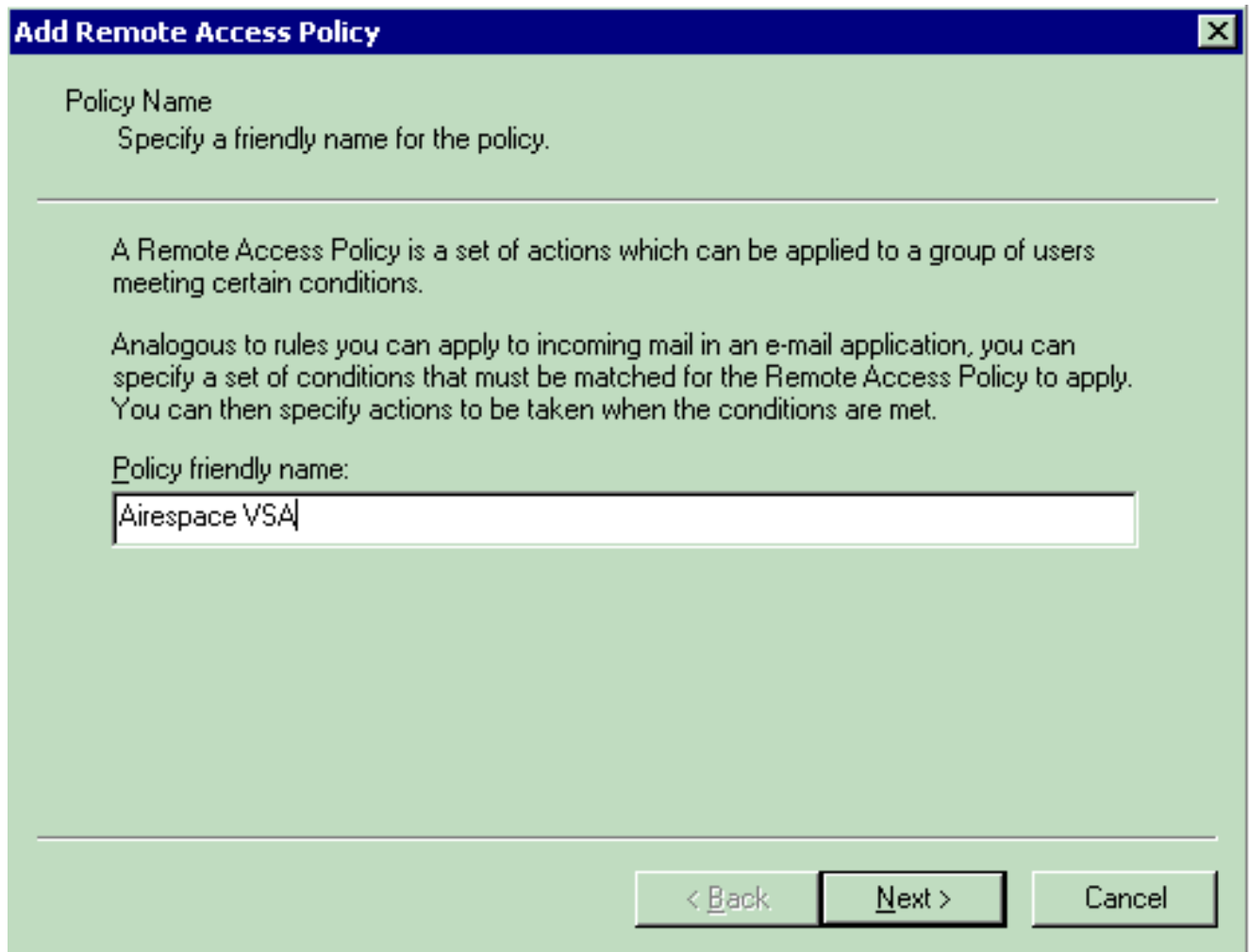


下一步是创建Remote access Policy和配置VSAs。

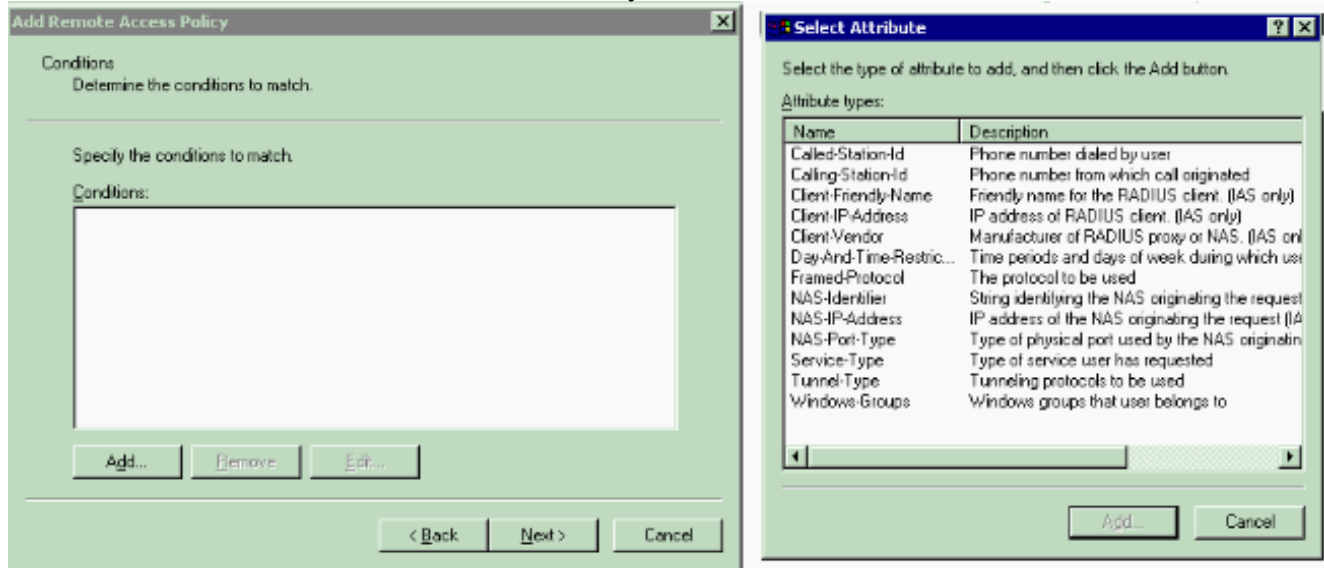
[配置在IAS的Remote access Policy](#)

完成这些步骤为了配置在IAS的一新的Remote access Policy：

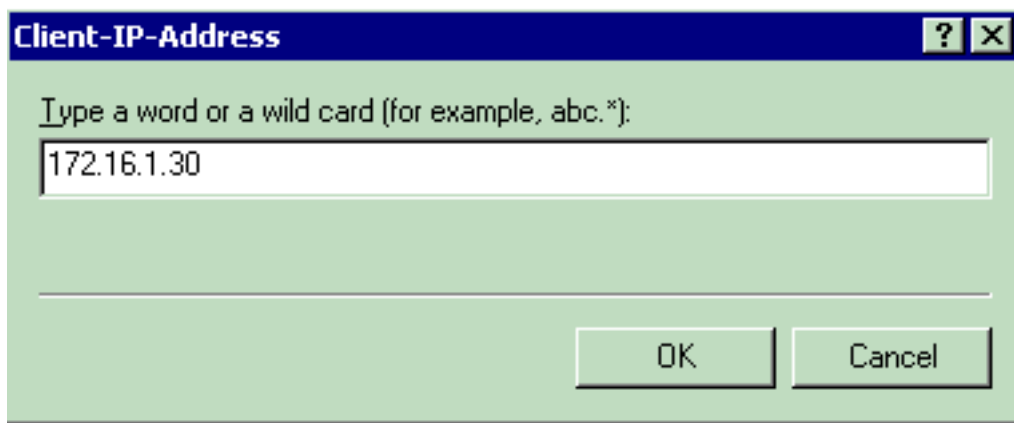
1. 用鼠标右键单击Remote access Policy并且选择新的远程AcceMSss策略。策略名称窗口出现。
2. 输入策略的名称并且其次单击。



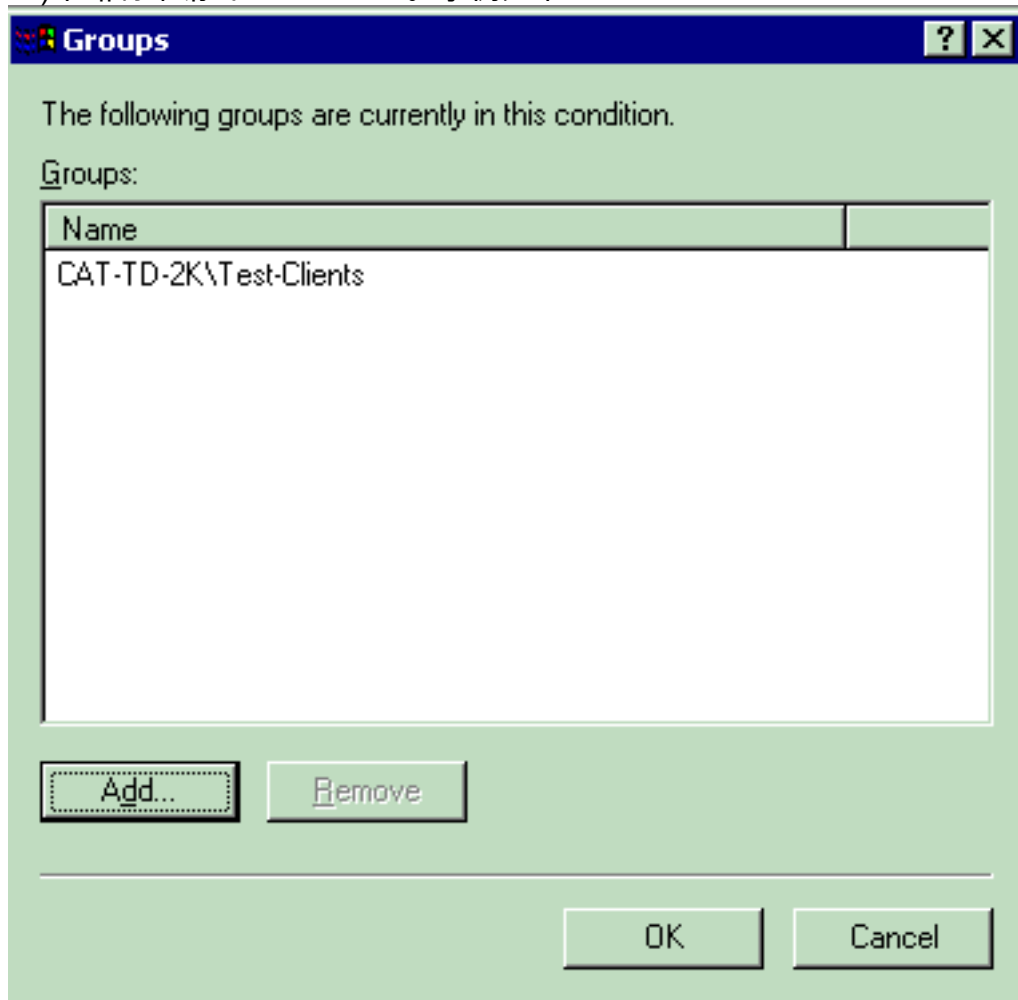
3. 在下一个窗口，请选择Remote access Policy将申请的条件。单击添加为了选择条件。

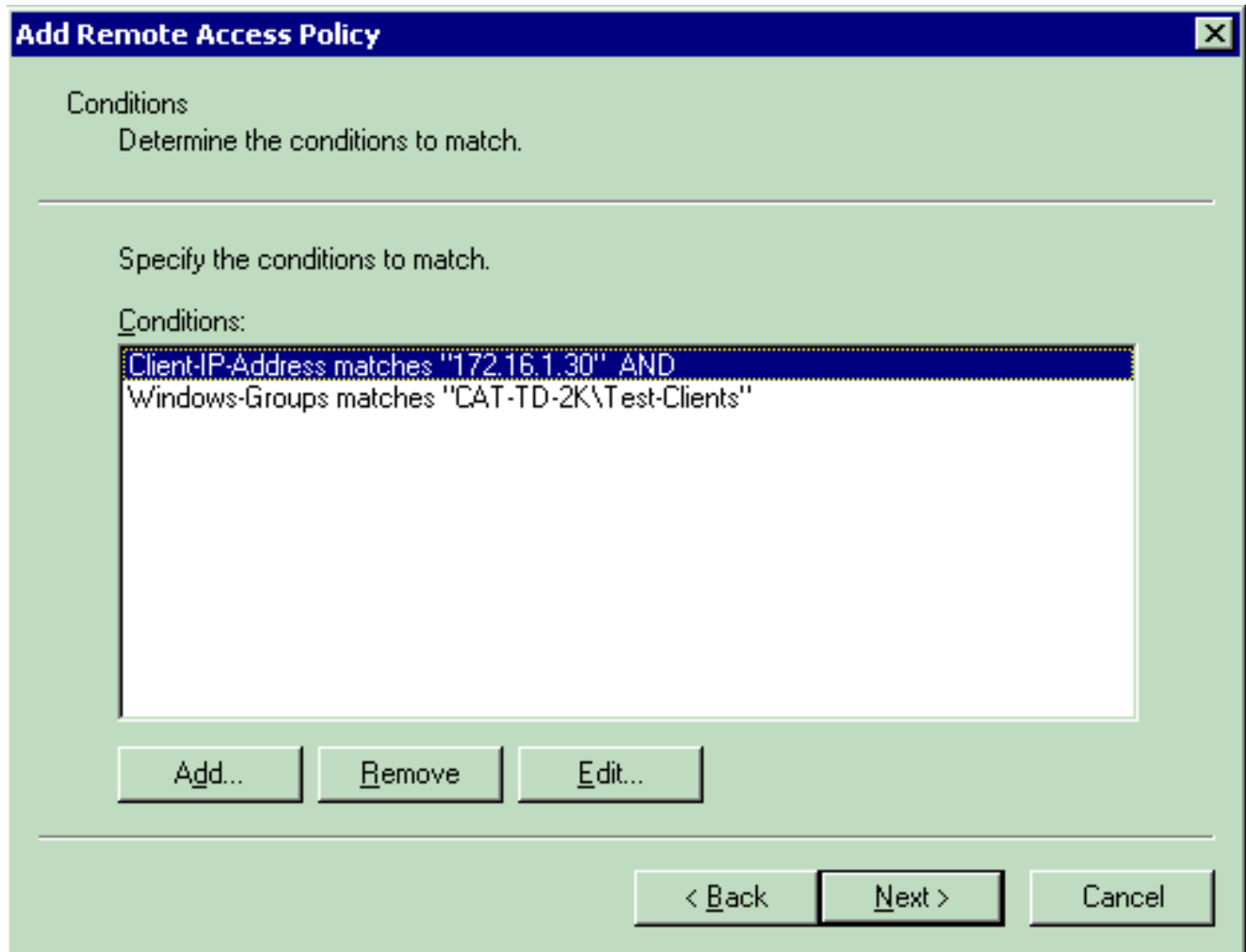


4. 从Attribute type菜单，请选择这些属性：**客户端IP地址**—输入AAA客户端的IP地址。在本例中，WLCs IP地址被输入，以便策略适用于从WLC的数据包。



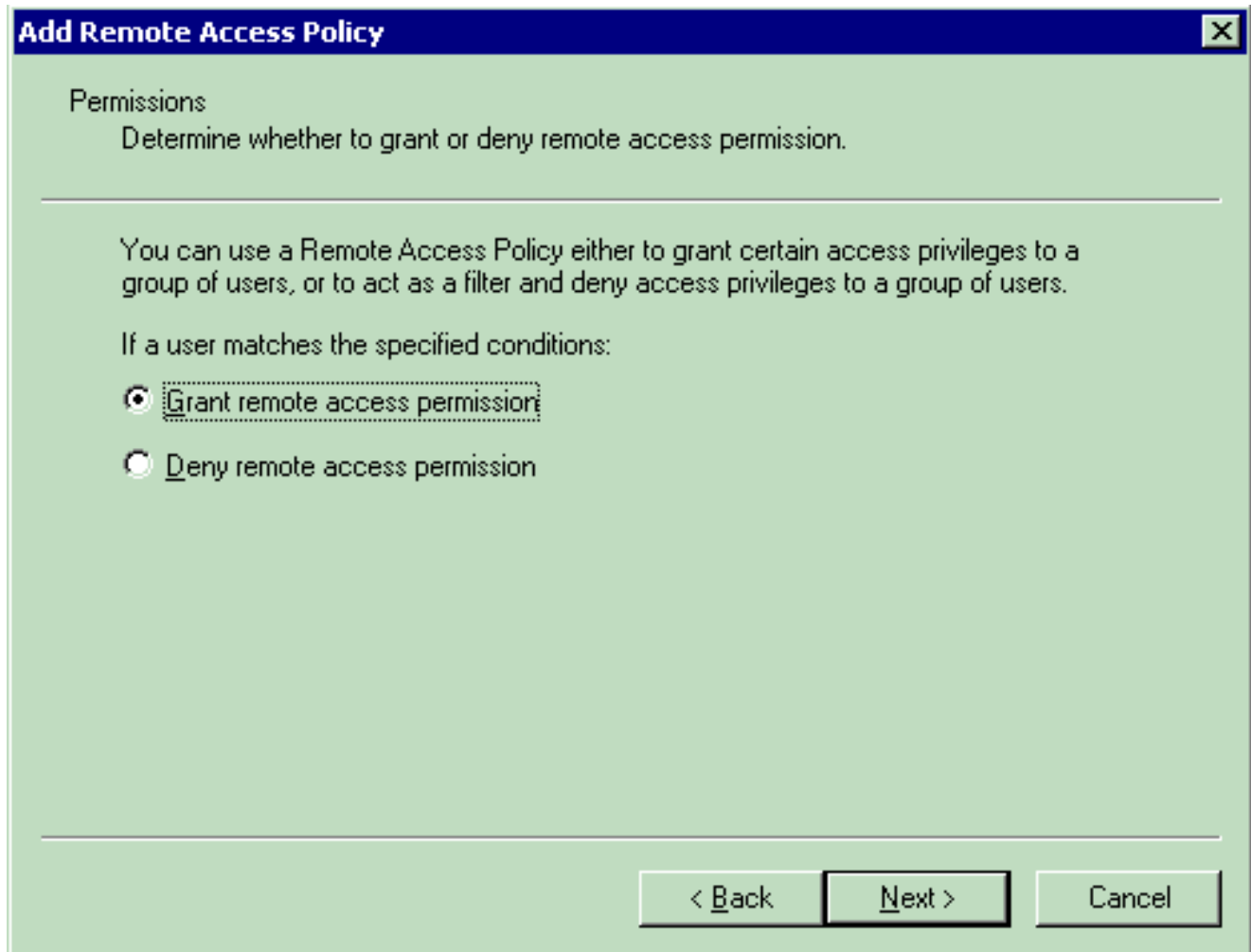
Windows组—选择(用户组)策略将申请的Windows组。示例如下





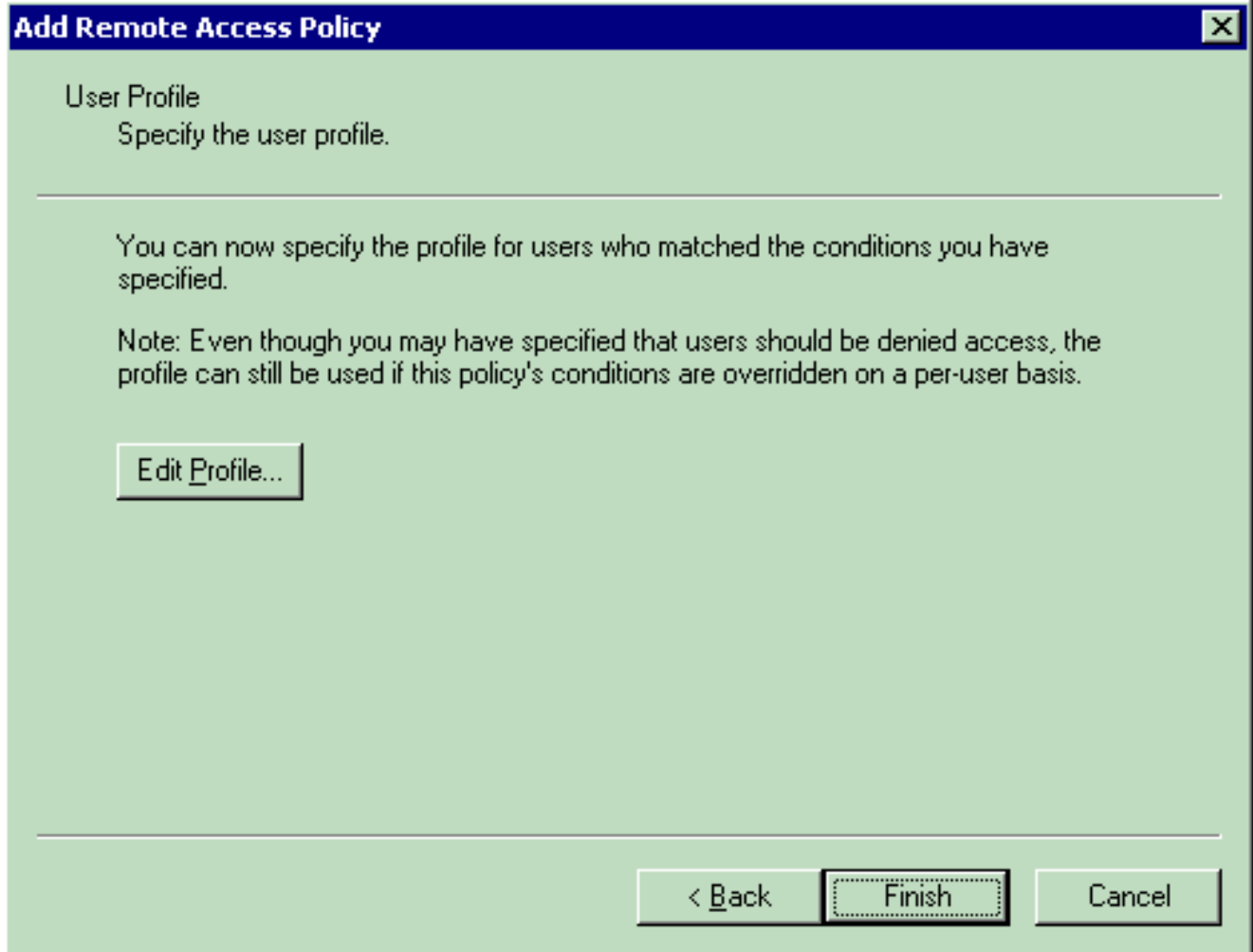
此示例只显示两个情况。如果有更多情况，请添加那些情况并且其次单击。Permissions窗口出现。

5. 在Permissions窗口，请选择**批准远程接入**。在您选择此选项后，用户给访问，假设用户匹配指定的条件(从步骤2)。

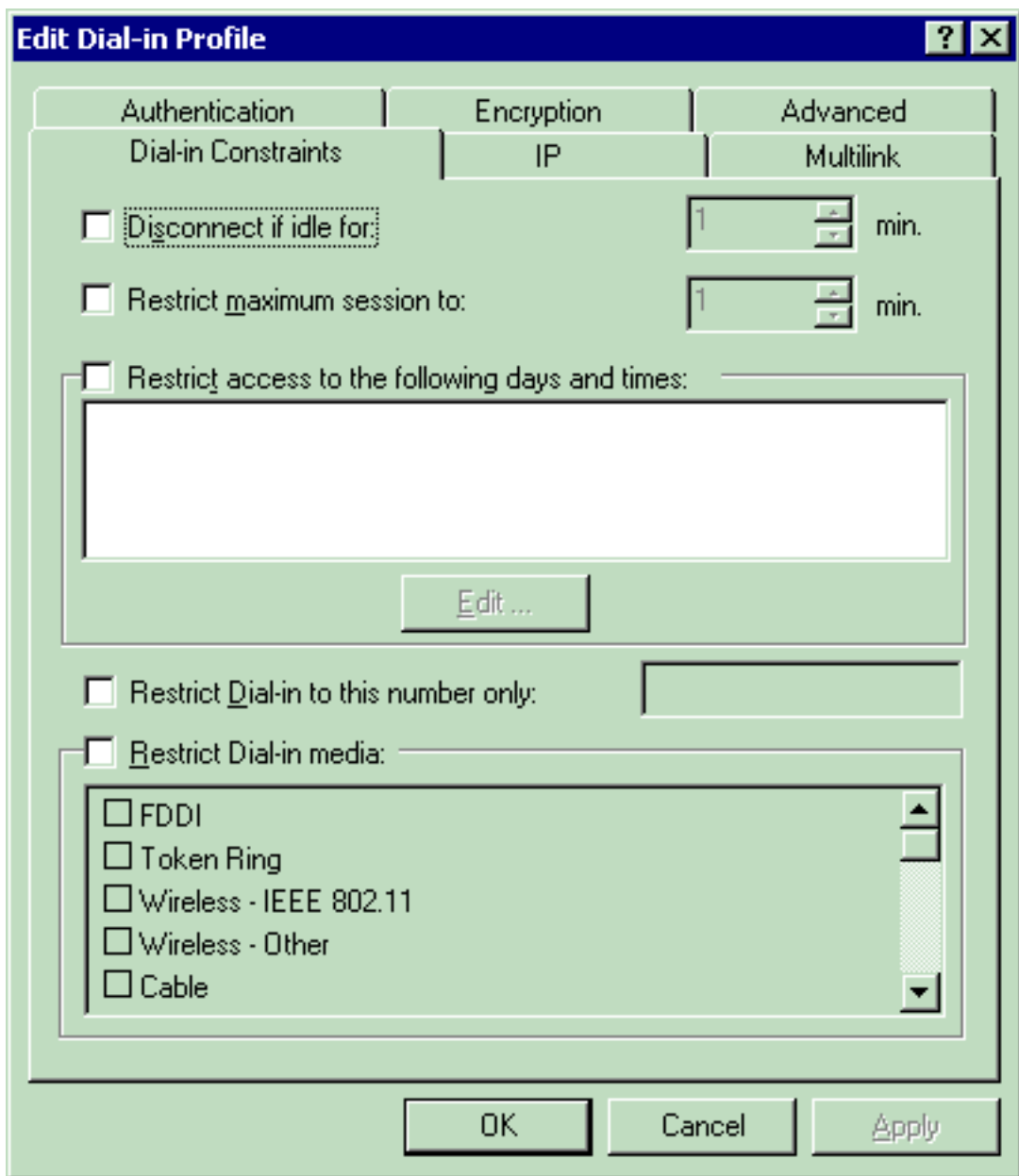


6. 单击 **Next**。

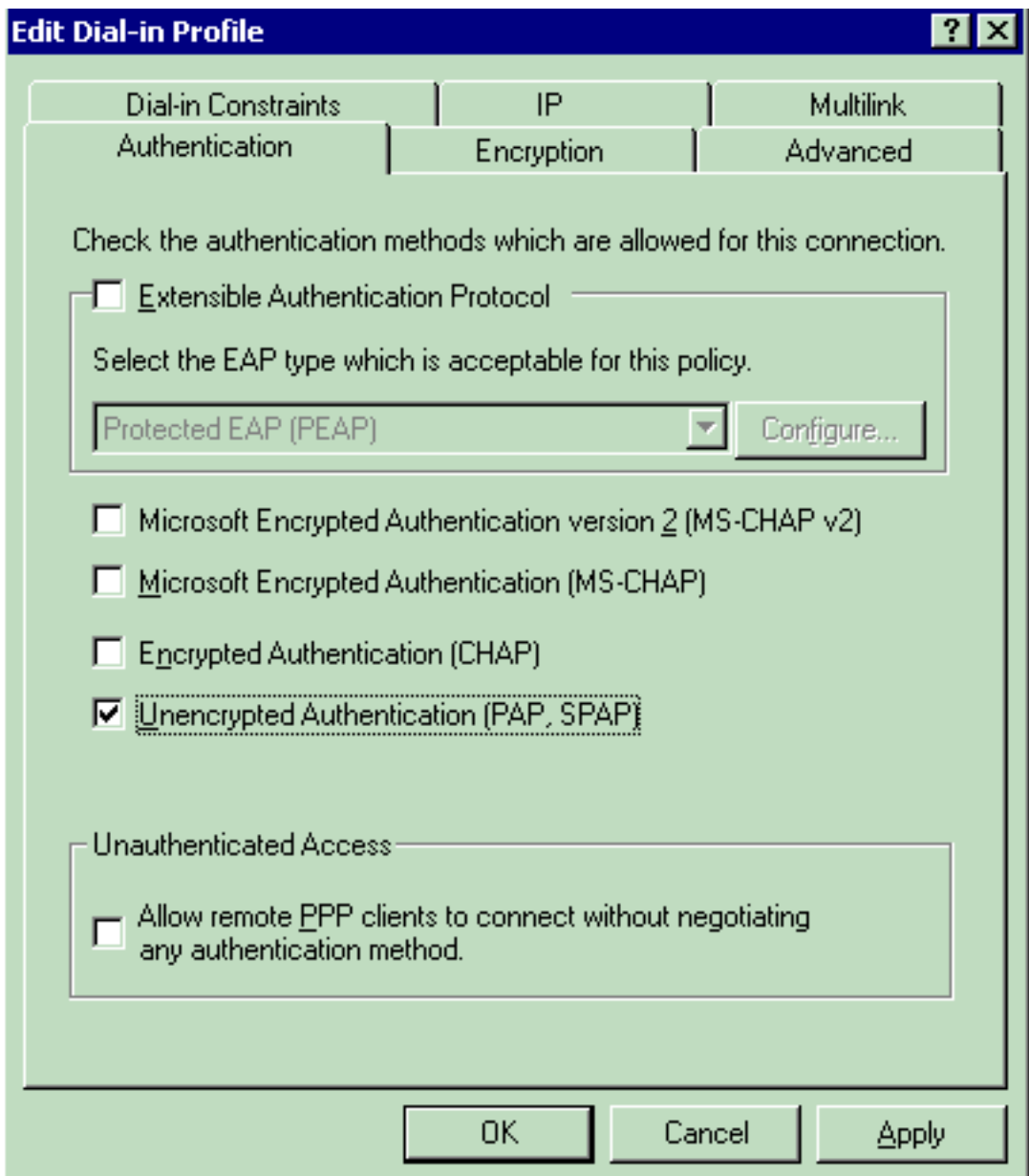
7. 下一步是设置用户配置文件。即使您也许已经指定用户应该拒绝或授权访问根据条件，可能仍然使用配置文件，如果此策略的情况逐个用户被改写。



为了配置用户配置文件，请单击**编辑**在用户配置文件窗口的**配置文件**。Edit Dial-in Profile窗口



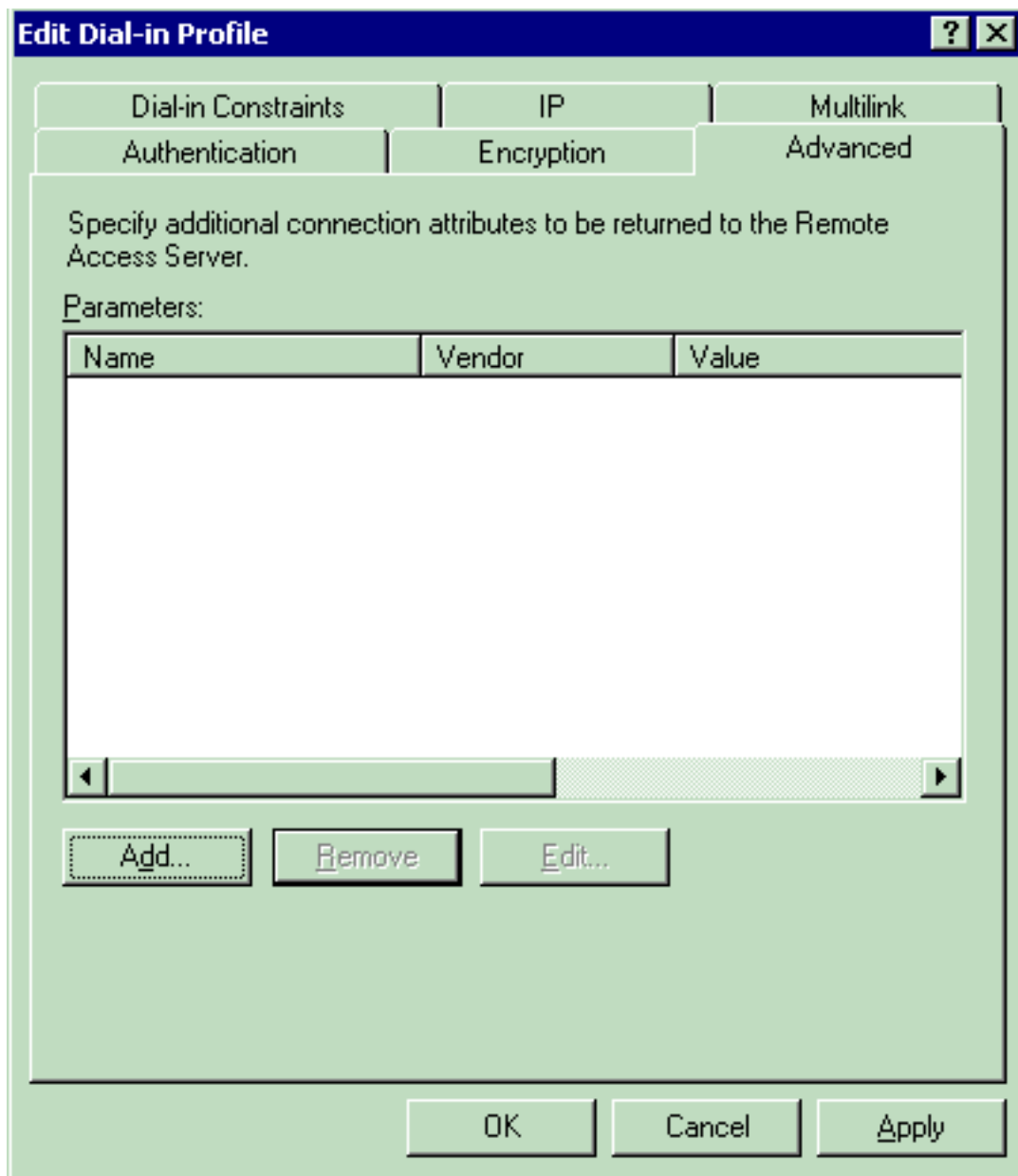
出现。 单击 **Authentication** 选项，然后选择在WLAN使用的认证方法。此示例使用未加密的认证(PAP，



SPAP)。

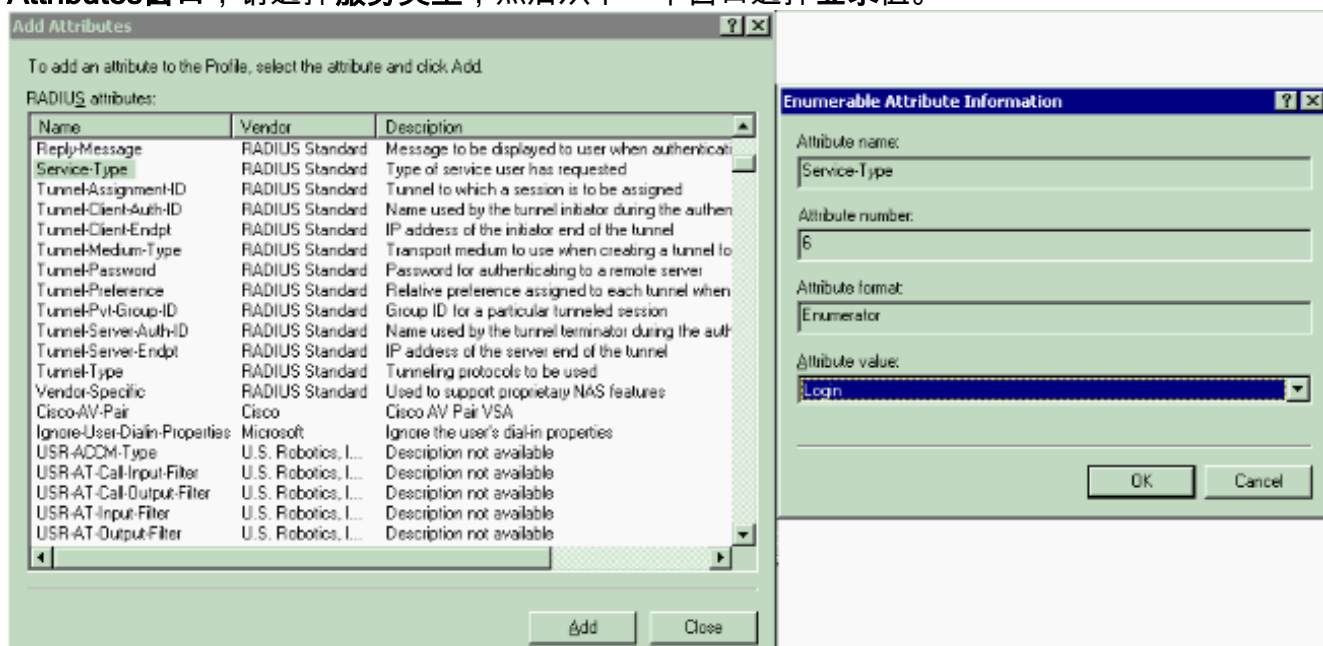
Advanced 选项卡。删除所有默认参数并且单击**添加**。

单击

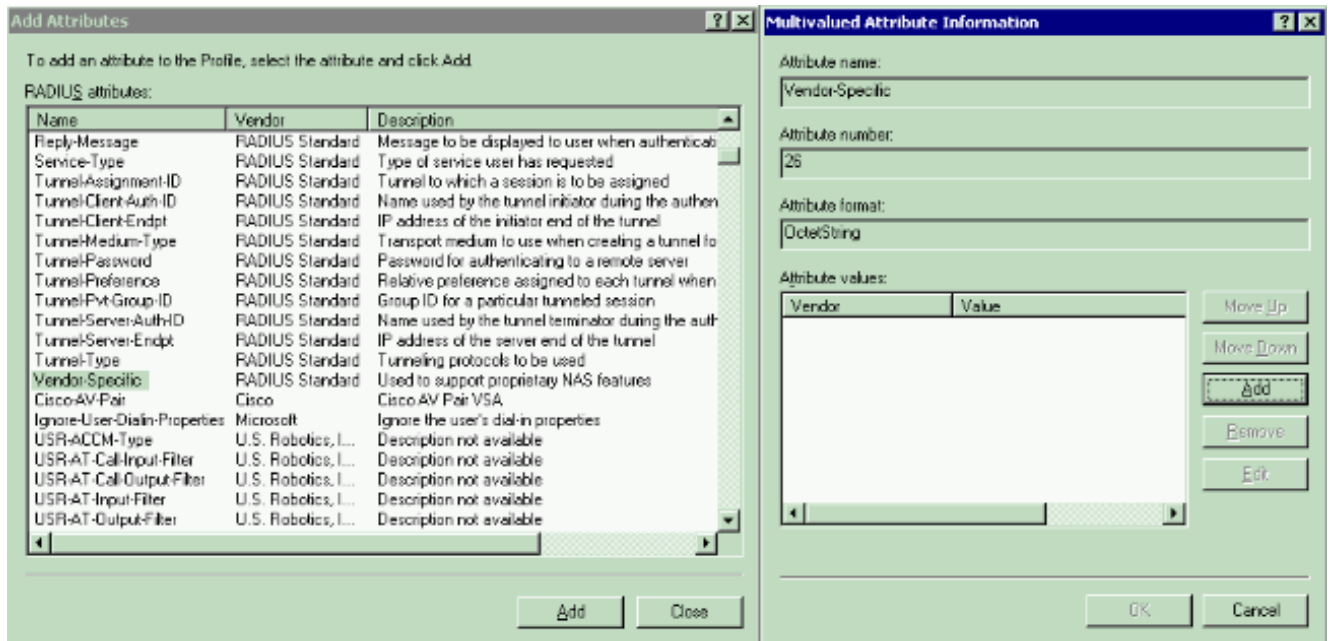


从添加

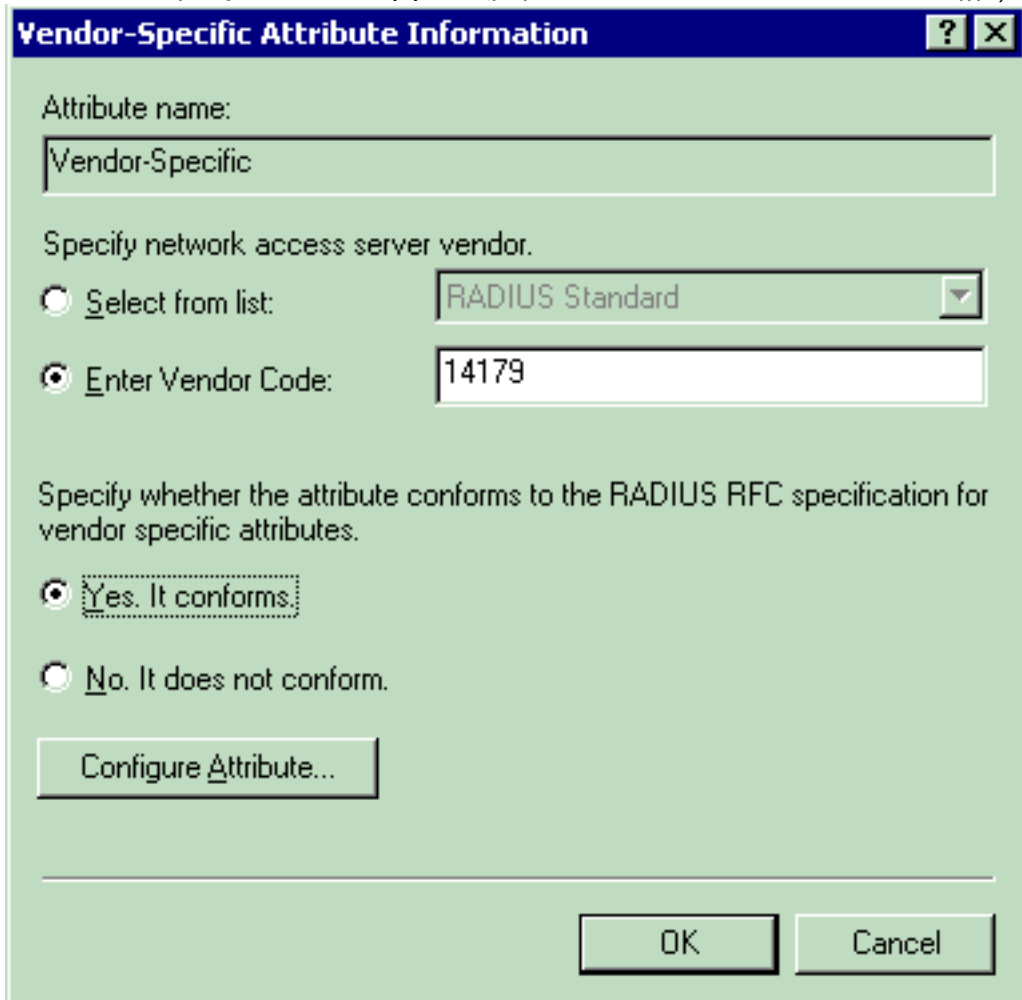
Attributes窗口，请选择服务类型，然后从下一个窗口选择登录值。



其次，您需要选择从RADIUS属性属性列表的供应商专用属性。



在下一个窗口，请单击**添加**以选择新的VSA。供应商专用属性信息窗口出现。下面请指定网络接入服务器供应商，选择**回车厂商代码**。输入Airespace的VSAs厂商代码。思科的Airespace VSAs厂商代码是**14179**。由于此属性遵守VSAs的RADIUS RFC规格，请选择**是**。



它一致。单击**配置属性**。在配置VSA (兼容的RFC)窗口，请输入供应商赋值的属性编号、属性格式和属性值，取决于VSA您要使用。逐个用户设置WLAN-ID：**属性名称— Airespace-WLAN-Id 供应商赋值的属性编号— 1 属性格式— 整数/十进制值— WLAN-ID 示例**

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
1

Attribute format:
Decimal

Attribute value:
2

OK Cancel

1 逐个用户设置

QoS配置文件：属性名称— Airespace-QoS-Level 供应商赋值的属性编号— 2 属性格式— 整数/十进制值— 0 -西尔弗;1 -金牌服务;2 -白金服务;3 -铜牌服务示例

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
2

Attribute format:
Decimal

Attribute value:
3

OK Cancel

2 逐个用户设置

DSCP值：属性名称— Airespace DSCP 供应商赋值的属性number — 3 属性格式— 整数/十进制值— DSCP值示例

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

3

逐个用户设置

802.1p TAG : 属性名称— Aireospace-802.1p-Tag 供应商赋值的属性编号— 4 属性格式— 整数 / 十进制值— 802.1p TAG 示例

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
4

Attribute format:
Decimal

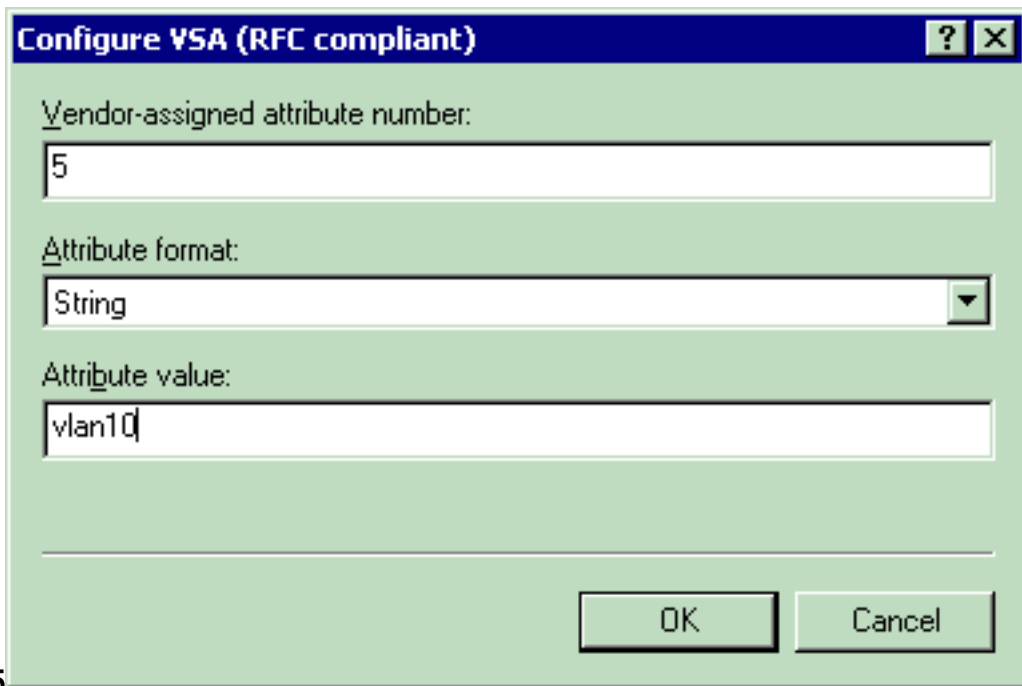
Attribute value:
5

OK Cancel

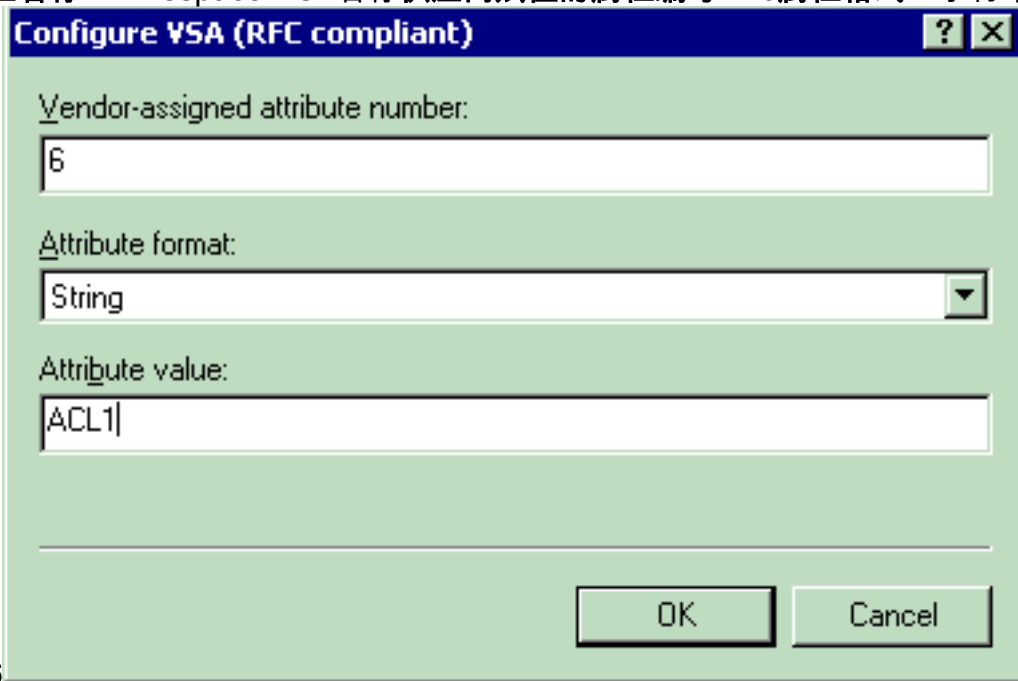
4

逐个用户设置

Interface (VLAN) : 属性名称— Aireospace 接口名称 供应商赋值的属性编号— 5 属性格式— 字符串值— Interface-Name 示例

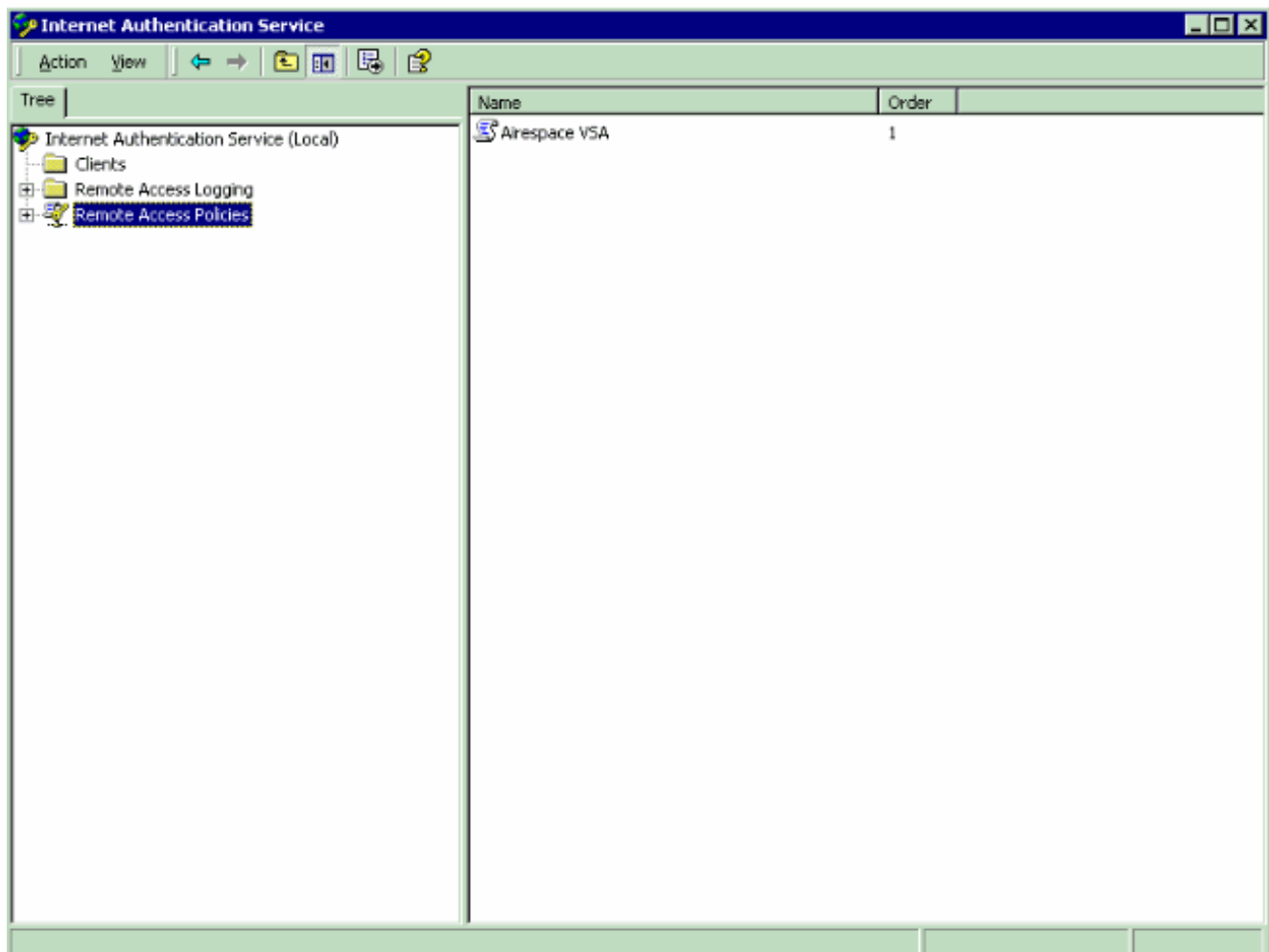


5 逐个用户设置ACL
: 属性名称— Airespace ACL名称 供应商赋值的属性编号— 6 属性格式— 字符串值— ACL名称



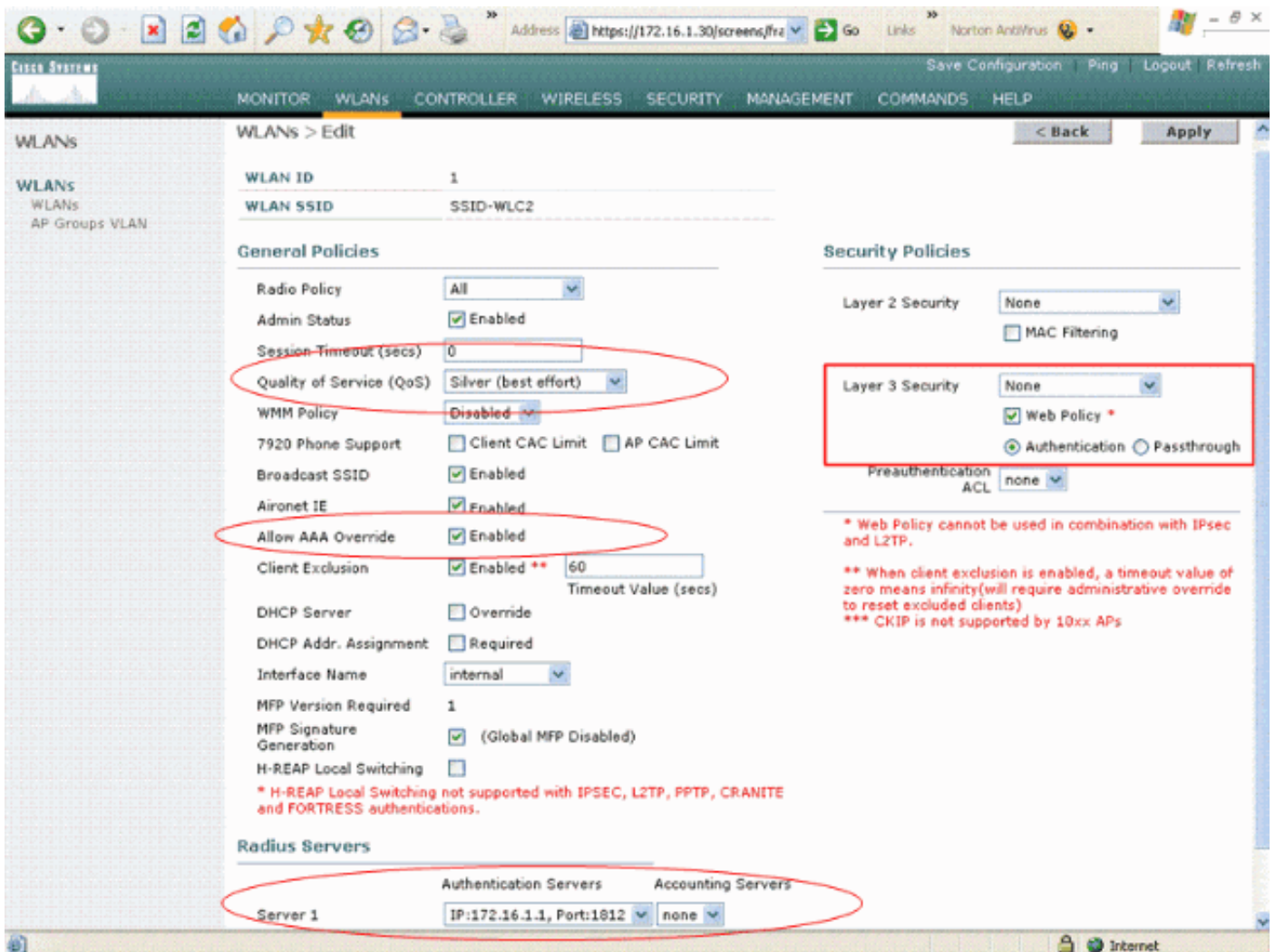
示例6

8. 一旦配置VSAs，请点击OK键，直到您看到用户配置文件窗口。
9. 然后，请点击芬通社为了完成配置。您能根据Remote access Policy看到新的策略。



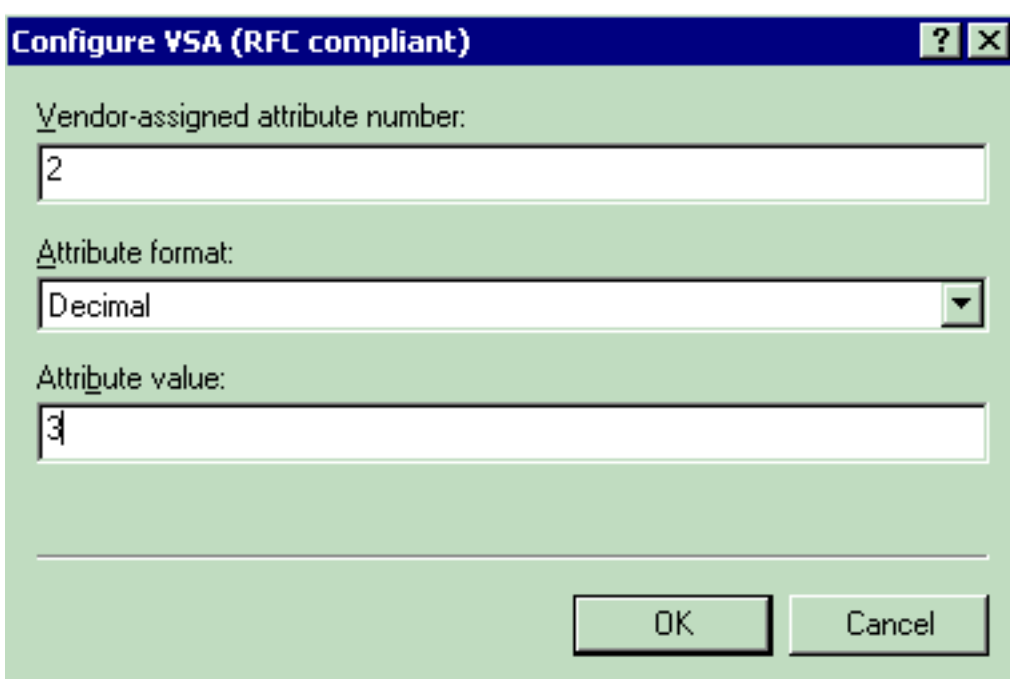
配置示例

在本例中，WLAN为Web验证配置。用户由IAS RADIUS服务器验证，并且RADIUS服务器配置逐个用户定量QoS策略。



正如你从此窗口看到，Web验证启用，认证服务器是172.16.1.1，并且AAA覆盖在WLAN也启用。此WLAN的默认QoS设置变成银色。

在IAS RADIUS服务器上，返回在Accept请求的RADIUS的QoS属性铜牌服务的Remote access Policy配置。当您配置VSA特定对QoS属性时，这执行。




```

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)

```

正如你从输出看到，用户验证。然后，AAA覆盖值返回与RADIUS接受消息。在这种情况下，用户给铜牌服务QoS策略。

您在WLC GUI能验证此。示例如下：

The screenshot shows the Cisco WLC configuration interface. The left sidebar contains navigation options like Monitor, Summary, Statistics, and Wireless. The main content area is titled 'Clients > Detail' and is divided into several sections:

- Client Properties:**

MAC Address	00:40:96:ac:e6:57
IP Address	20.0.0.1
User Name	User-VLAN10
Port Number	1
Interface	internal
VLAN ID	20
CCX Version	CCXv3
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
- AP Properties:**

AP Address	00:0b:85:5b:fb:d0
AP Name	ap:5b:fb:d0
AP Type	802.11a
WLAN SSID	SSID-WLC2
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable
- Security Information:**

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A
- Quality of Service Properties:**

WMM State	Disabled
QoS Level	Bronze
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled

注意：此SSID的默认QoS配置文件是银色的。然而，因为AAA覆盖选择，并且用户配置与铜牌服务QoS配置文件在IAS服务器的，默认QoS配置文件被改写。

故障排除

您能使用 `debug aaa all enable` 命令在WLC排除故障配置。此调试输出的示例在工作的网络的在本文的 [Verify部分](#) 显示。

注意：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](#)