Microsoft IAS Radius伺服器上的Cisco Airespace VSA配置示例

目錄

簡介

本文檔介紹如何配置Microsoft Internet身份驗證服務(IAS)伺服器以支援Cisco Airespace供應商特定屬性(VSA)。 Cisco Airespace VSA的供應商代碼為**14179**。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何配置IAS伺服器
- 輕量型存取點(LAP)和思科無線LAN控制器(WLC)的組態資訊
- 思科統一無線安全解決方案知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用IAS的Microsoft Windows 2000 Server
- Cisco 4400 WLC（執行軟體版本4.0.206.0）
- Cisco 1000系列LAP

- 採用韌體2.5的802.11 a/b/g無線使用者端配接器
- Aironet案頭公用程式(ADU)版本2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

注意：本文檔旨在為讀者提供在IAS伺服器上支援思科Airespace VSA所需的配置示例。本文檔中介紹的IAS伺服器配置已在實驗室經過測試，並且工作正常。如果配置IAS伺服器時遇到問題，請與Microsoft聯絡以獲取幫助。Cisco TAC不支援Microsoft Windows伺服器配置。

本檔案假設WLC已設定為基本操作，且LAP已註冊到WLC。如果您是嘗試設定WLC以使用LAP執行基本操作的新使用者，請參閱向無線LAN控制器(WLC)註冊輕量AP(LAP)。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

在大多數無線LAN(WLAN)系統中，每個WLAN都有一個靜態策略，該策略適用於與服務組識別碼(SSID)相關聯的所有使用者端。 此方法雖然功能強大，但也有侷限性，因為它要求客戶端與不同的SSID關聯以繼承不同的QoS和安全策略。

但是，Cisco無線LAN解決方案支援身份網路，允許網路通告單個SSID，並且特定使用者根據其使用者配置檔案繼承不同的QoS或安全策略。您可以使用身份網路控制的特定策略包括：

- **服務品質** — 當存在於RADIUS存取接受中時，QoS層級值會覆寫WLAN設定檔中指定的QoS值。
- **ACL** — 當RADIUS訪問接受中存在訪問控制清單(ACL)屬性時，系統會在客戶端工作站進行身份驗證後應用ACL名稱。這會覆蓋分配給介面的所有ACL。
- **VLAN** — 當RADIUS訪問接受中存在VLAN介面名稱或VLAN標籤時，系統將客戶端置於特定介面上。
- **WLAN ID** — 當RADIUS Access Accept中存在WLAN-ID屬性時，系統會在客戶端工作站進行身份驗證後應用WLAN-ID(SSID)。WLAN ID由WLC在除IPSec以外的所有驗證範例中傳送。在Web驗證的情況下，如果WLC在來自AAA伺服器的驗證回應中收到WLAN-ID屬性，並且該屬性與WLAN的ID不相符，則會拒絕驗證。其他型別的安全方法不執行此操作。
- **DSCP值** — 當存在於RADIUS訪問接受中時，DSCP值將覆蓋WLAN配置檔案中指定的DSCP值。
- **802.1p-Tag** — 當存在於RADIUS存取接受中時，802.1p值會覆蓋WLAN設定檔中指定的預設值。

注意：VLAN功能僅支援MAC過濾、802.1X和Wi-Fi保護訪問(WPA)。 VLAN功能不支援Web驗證或IPSec。作業系統的本地MAC過濾器資料庫已擴展為包含介面名稱。這允許本地MAC過濾器指定應該分配給客戶端的介面。也可以使用單獨的RADIUS伺服器，但必須使用安全選單定義RADIUS伺服器。

有關身份網路的詳細資訊，請參閱配置身份網路。

為Airespace VSA配置IAS

要為Airespace VSA配置IAS，您需要完成以下步驟：

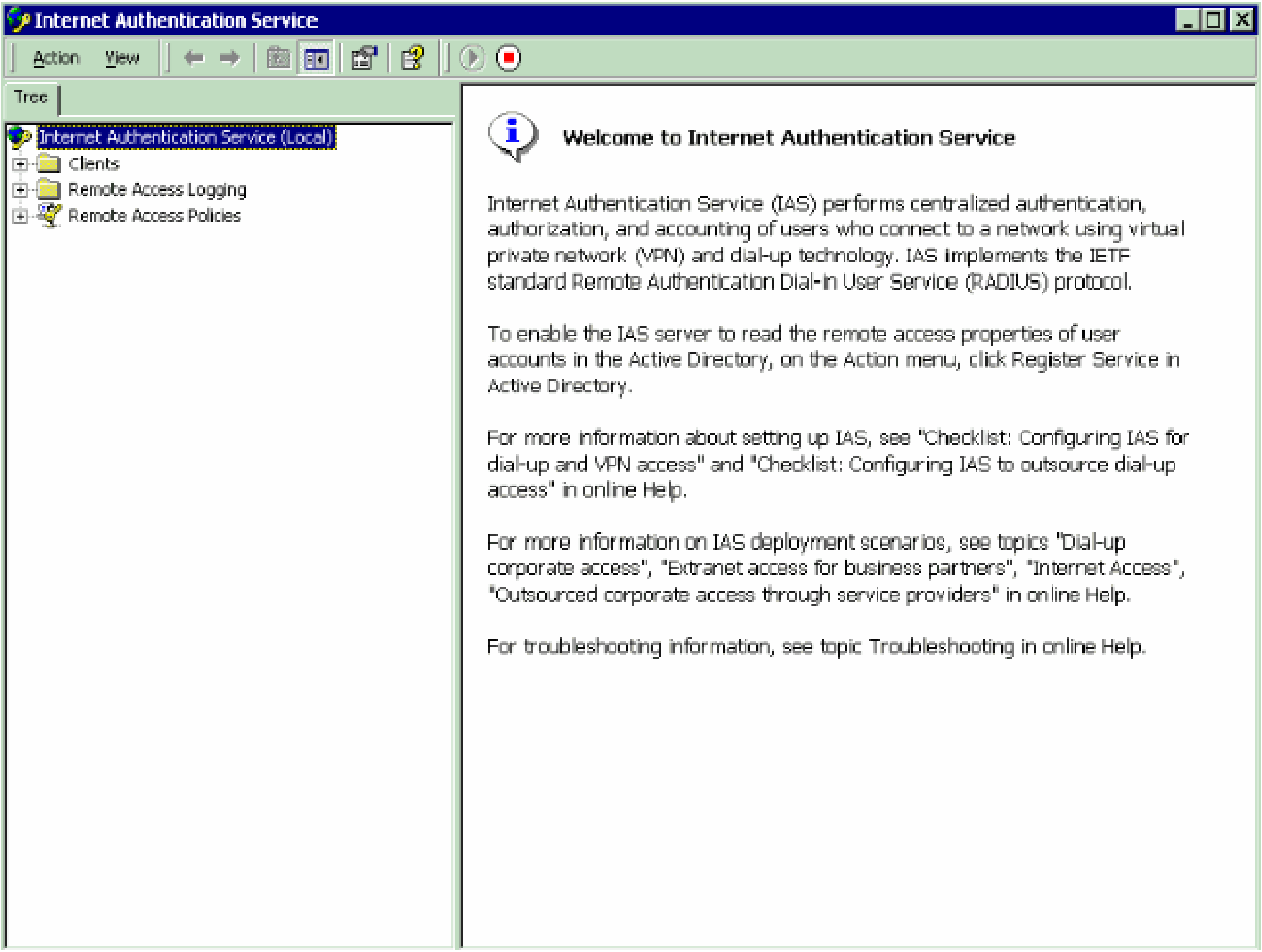
1. 將WLC配置為IAS上的AAA客戶端
2. 在IAS上配置遠端訪問策略

注意：VSA是在遠端訪問策略下配置的。

將WLC配置為IAS上的AAA客戶端

完成以下步驟，以便在IAS上將WLC設定為AAA使用者端：

1. 按一下**Programs > Administrative Tools > Internet Authentication Service**，以便在Microsoft 2000伺服器上啟動IAS。



Internet Authentication Service
Action
View
Tree
Internet Authentication Service (Local)
Clients
Remote Access Logging
Remote Access Policies

Welcome to Internet Authentication Service

Internet Authentication Service (IAS) performs centralized authentication, authorization, and accounting of users who connect to a network using virtual private network (VPN) and dial-up technology. IAS implements the IETF standard Remote Authentication Dial-In User Service (RADIUS) protocol.

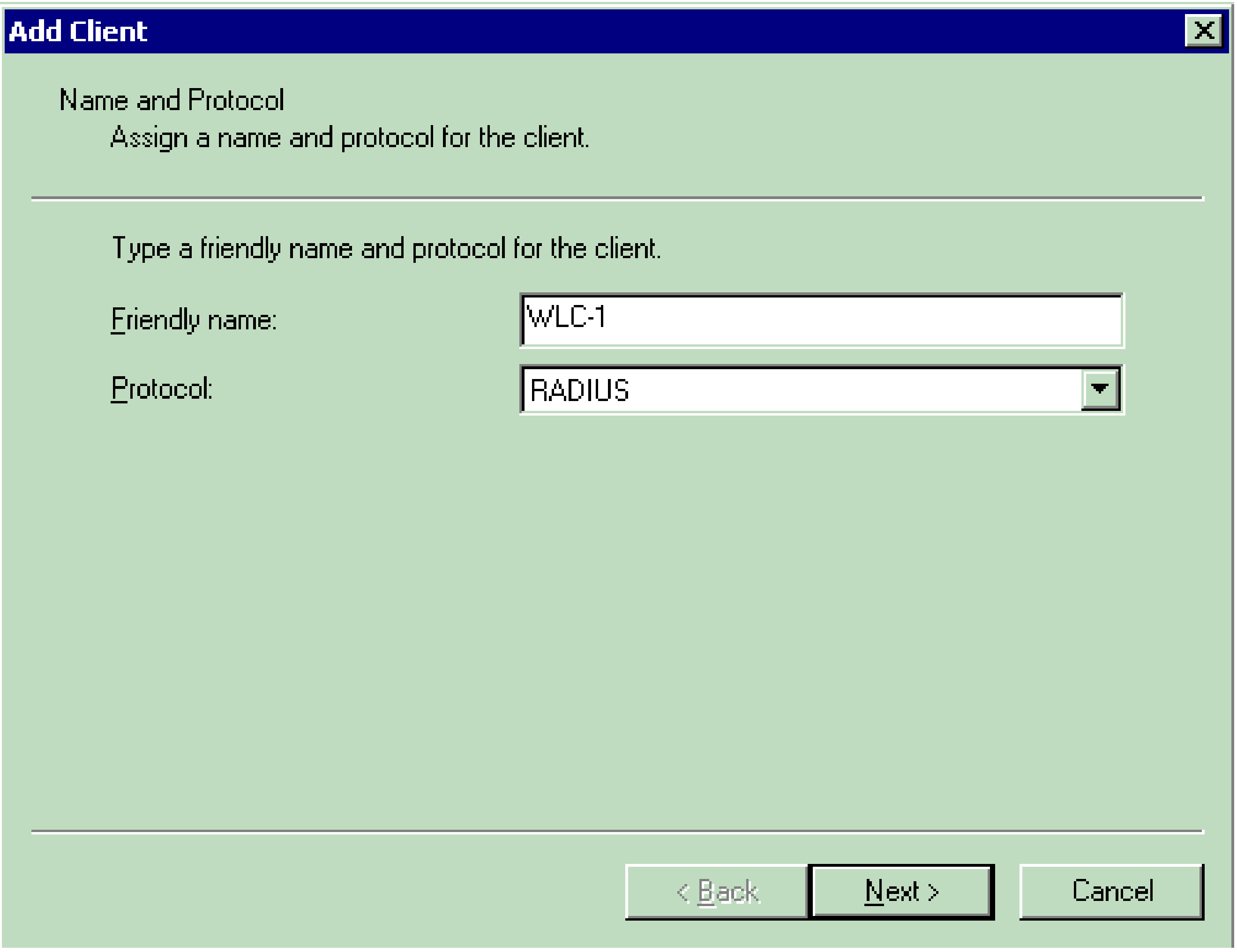
To enable the IAS server to read the remote access properties of user accounts in the Active Directory, on the Action menu, click Register Service in Active Directory.

For more information about setting up IAS, see "Checklist: Configuring IAS for dial-up and VPN access" and "Checklist: Configuring IAS to outsource dial-up access" in online Help.

For more information on IAS deployment scenarios, see topics "Dial-up corporate access", "Extranet access for business partners", "Internet Access", "Outsourced corporate access through service providers" in online Help.

For troubleshooting information, see topic Troubleshooting in online Help.

2. 按一下右鍵**Clients**資料夾並選擇**New Client**以新增新的RADIUS客戶端。
3. 在「新增客戶端」視窗中，輸入客戶端的名稱，然後選擇**RADIUS**作為協定。然後，按一下**下一步**。在本範例中，使用者端名稱是*WLC-1*。**注意**：預設情況下，協定設定為RADIUS。



Add Client

Name and Protocol

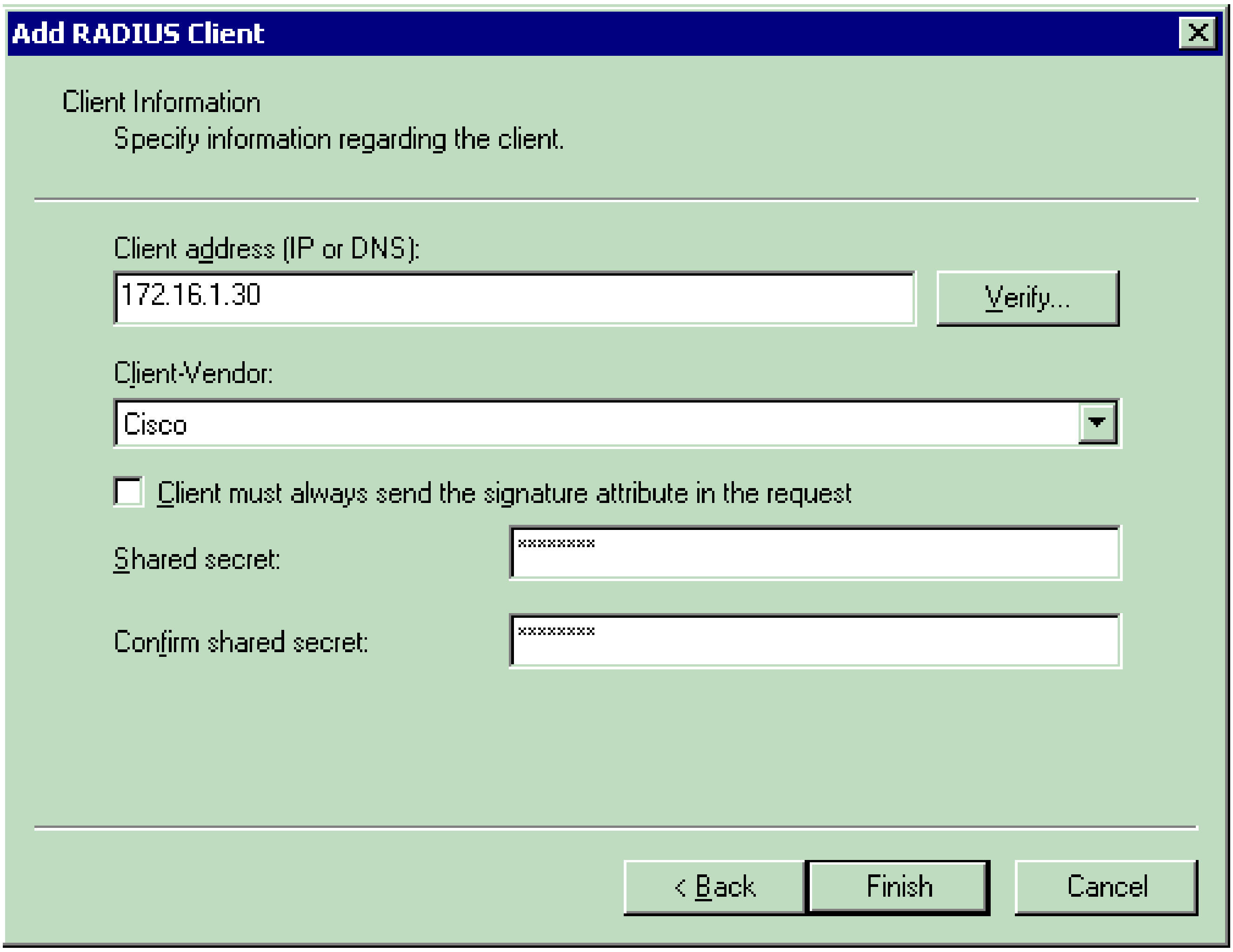
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

Friendly name: WLC-1

Protocol: RADIUS

4. 在「新增RADIUS客戶端」視窗中，輸入**客戶端IP地址、客戶端 — 供應商**和**共用金鑰**。輸入客戶端資訊後，按一下**Finish**。此範例顯示IP位址為*172.16.1.30*、Client-Vendor設定為*Cisco*、Shared secret設定為*cisco123*且名為*WLC-1*的使用者端
：



Add RADIUS Client

Client Information

Specify information regarding the client.

Client address (IP or DNS): 172.16.1.30

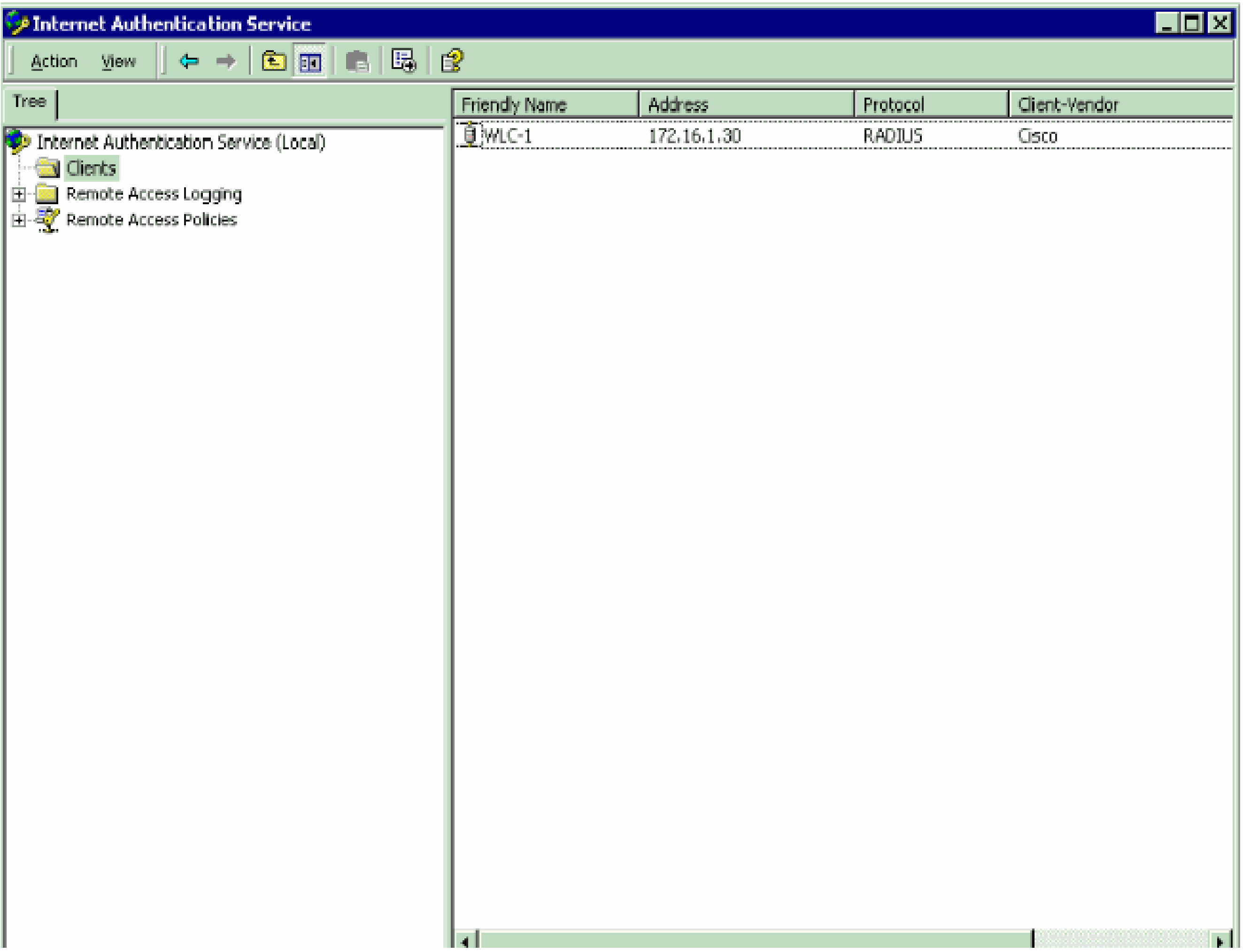
Client-Vendor: Cisco

□ Client must always send the signature attribute in the request

Shared secret: *********

Confirm shared secret: *********

透過此資訊，名為WLC-1的WLC會新增為IAS伺服器的AAA使用者端。


Internet Authentication Service
Action
View
Tree
Internet Authentication Service (Local)
Clients
Remote Access Logging
Remote Access Policies

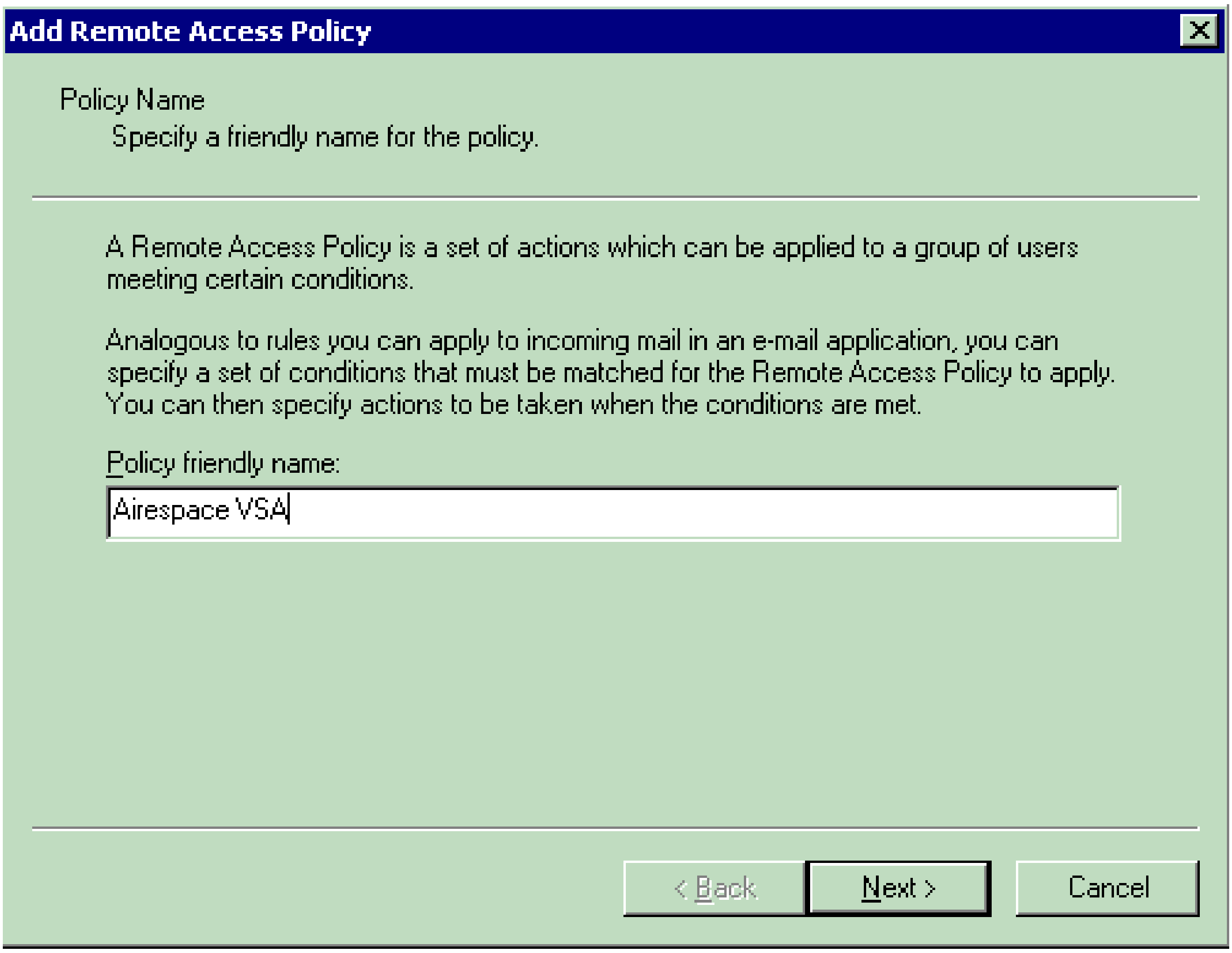
Friendly Name	Address	Protocol	Client-Vendor
WLC-1	172.16.1.30	RADIUS	Cisco

下一步是建立遠端訪問策略並配置VSA。

在IAS上配置遠端訪問策略

完成以下步驟，以便在IAS上配置新的遠端訪問策略：

1. 按一下右鍵**Remote Access Policies**，然後選擇**New Remote AccessMSss Policy**。系統將顯示Policy Name視窗。
2. 輸入策略名稱，然後按一下**Next**。



Add Remote Access Policy

Policy Name

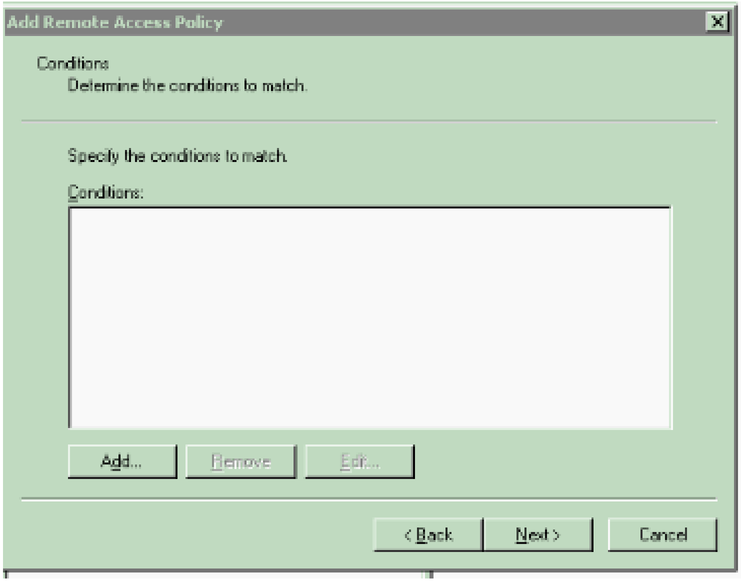
Specify a friendly name for the policy.

A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.

Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.

Policy friendly name: Airespace VSA

3. 在下一個視窗中，選擇將應用遠端訪問策略的條件。按一下**Add**以選擇條件。



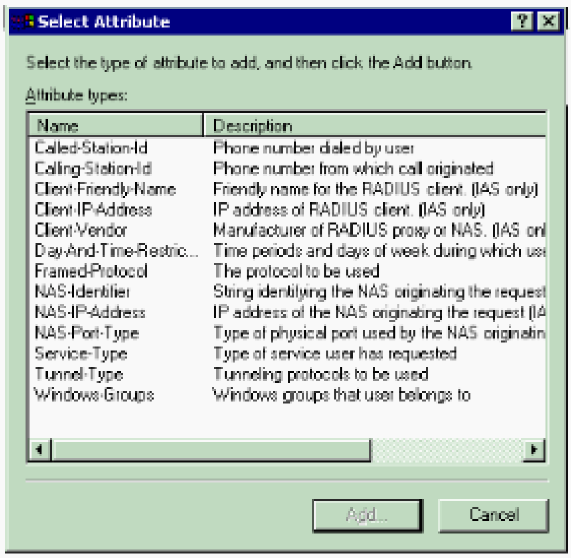
Add Remote Access Policy

Conditions

Determine the conditions to match.

Specify the conditions to match.

Conditions:



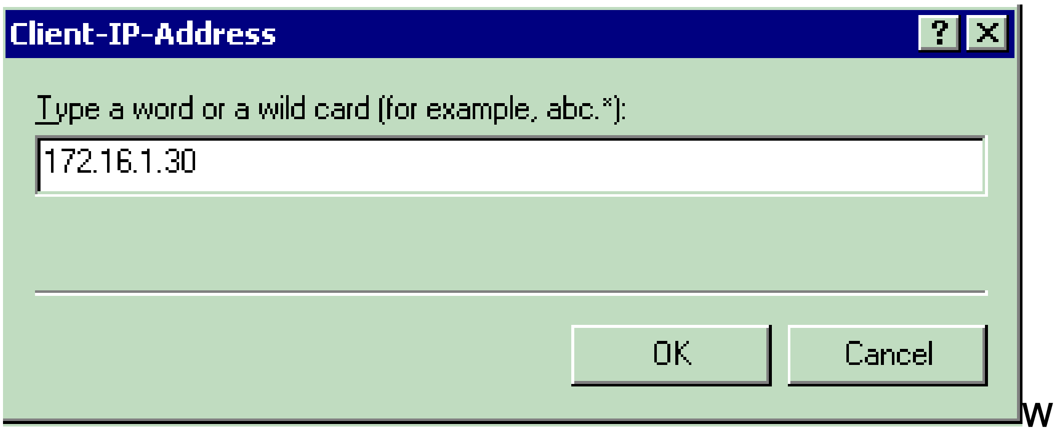
Select Attribute

Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only)
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (IAS onl
Day-And-Time-Restric...	Time periods and days of week during which use
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the request
NAS-IP-Address	IP address of the NAS originating the request (IA
NAS-Port-Type	Type of physical port used by the NAS originatin
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to

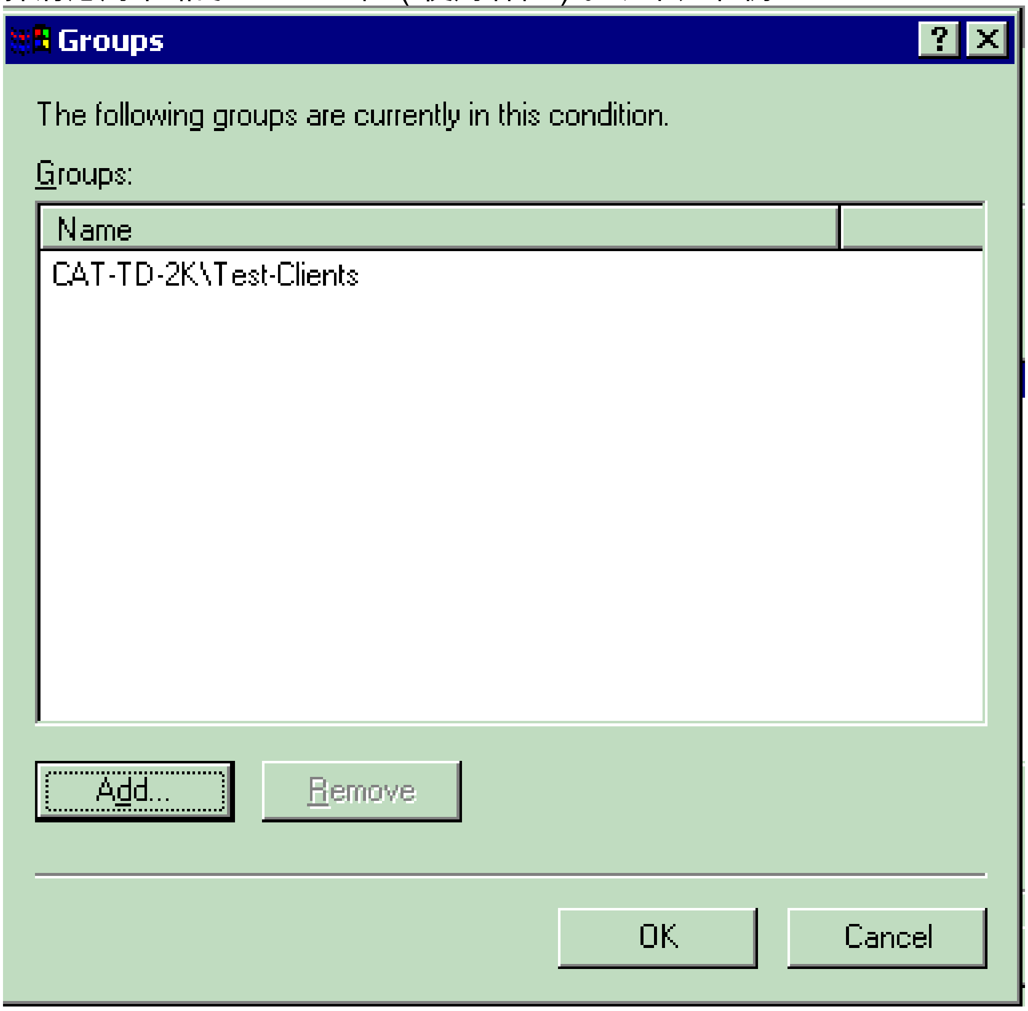
4. 從「屬性型別」選單中選擇以下屬性：**Client-IP-Address** — 輸入AAA客戶端的IP地址。在此範例中，輸入WLC的IP位址，以便原則適用於來自WLC的封包。


Client-IP-Address

Type a word or a wild card (for example, abc.*):

172.16.1.30

Windows Groups — 選擇將應用策略的Windows組（使用者組）。以下是範例

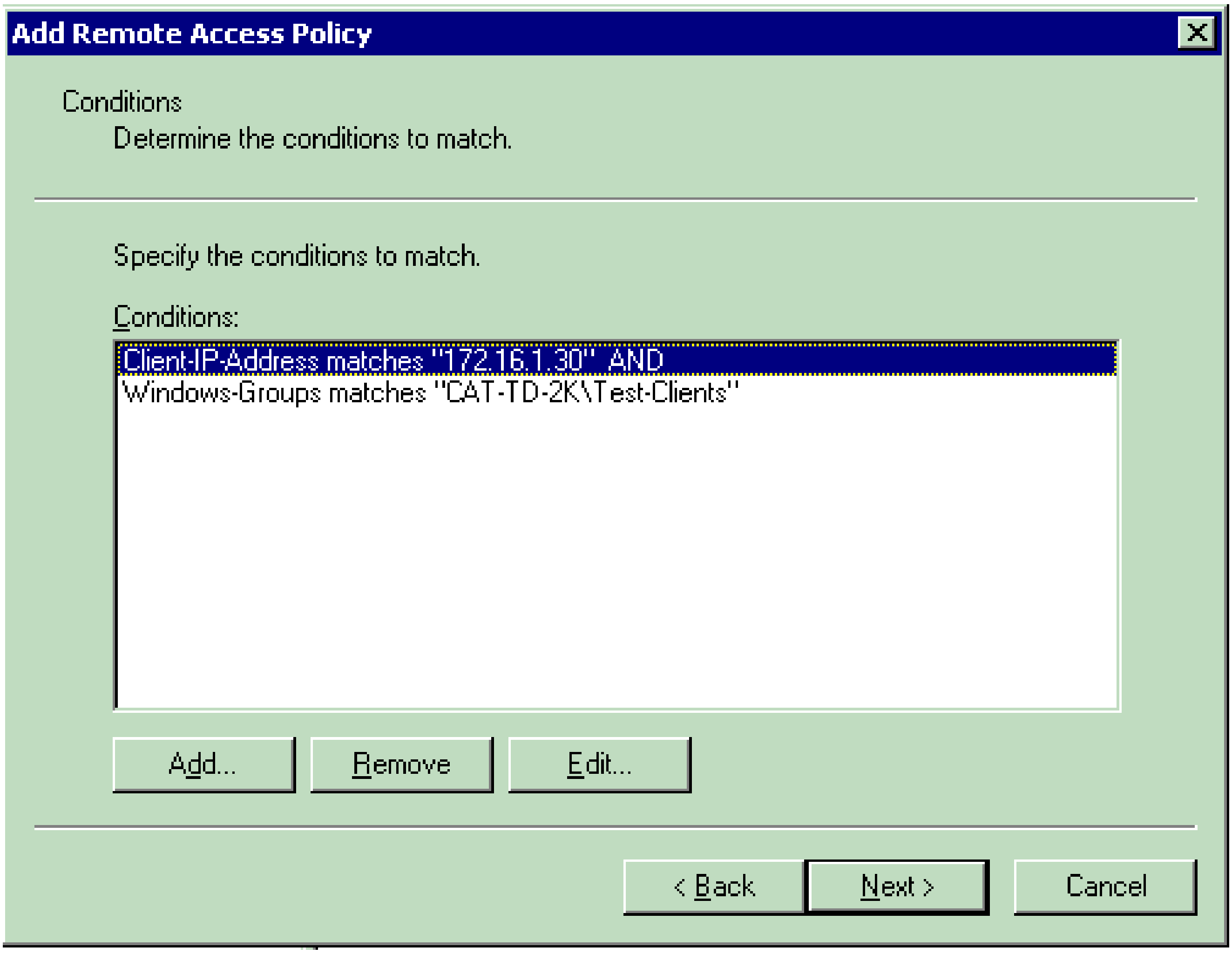

Groups

The following groups are currently in this condition.

Groups:

Name
CAT-TD-2K\Test-Clients

:



Add Remote Access Policy

Conditions

Determine the conditions to match.

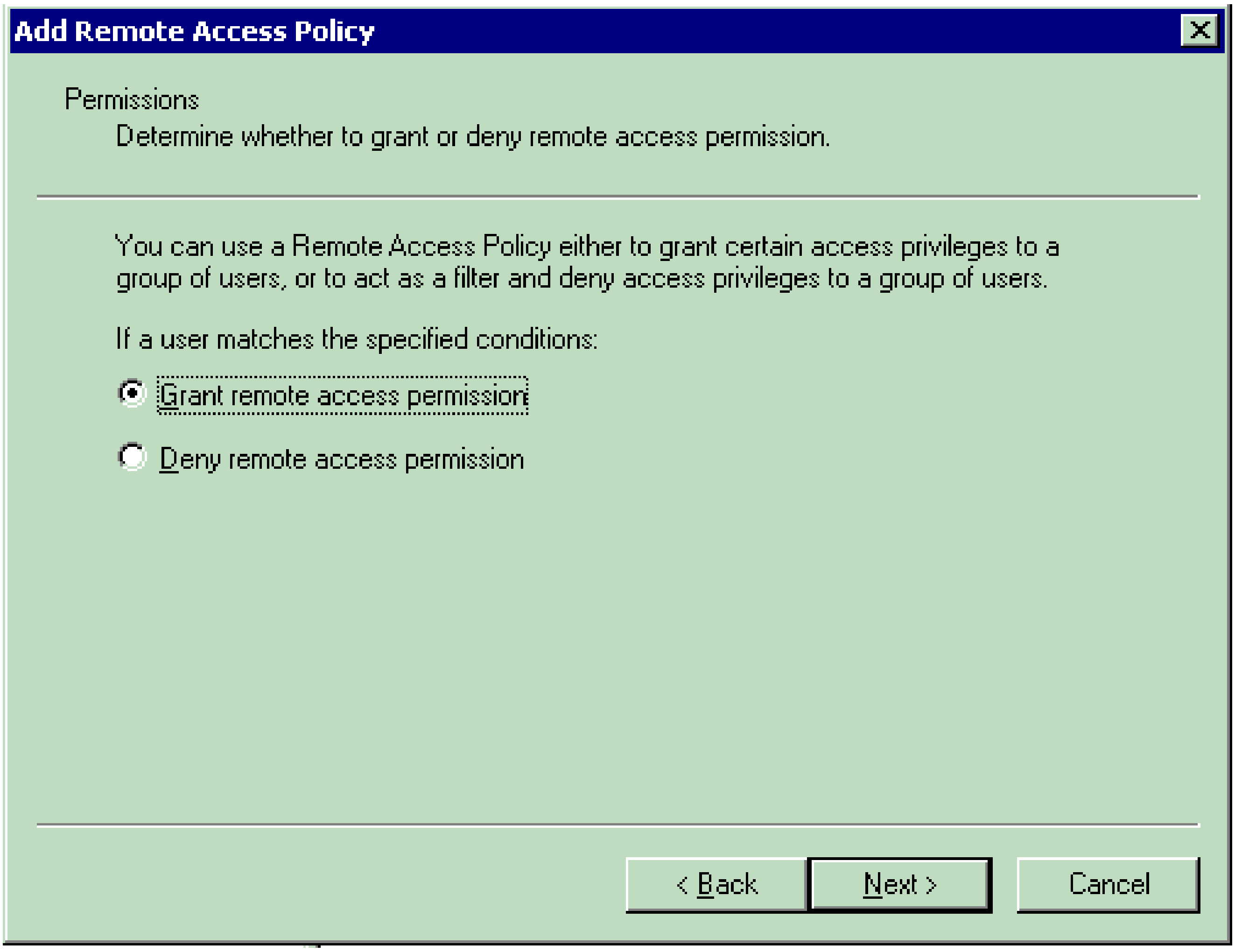
Specify the conditions to match.

Conditions:

```
Client-IP-Address matches "172.16.1.30"  AND
Windows-Groups matches "CAT-TD-2K\Test-Clients"
```

此範例僅顯示兩個條件。如果有更多條件，也新增這些條件，然後按一下**下一步**。出現「Permissions（許可權）」視窗。

5. 在「許可權」視窗中，選擇**「授予遠端訪問許可權」**。選擇此選項後，如果使用者符合指定的條件（在步驟2中），則授予使用者訪問許可權。



Add Remote Access Policy

Permissions

Determine whether to grant or deny remote access permission.

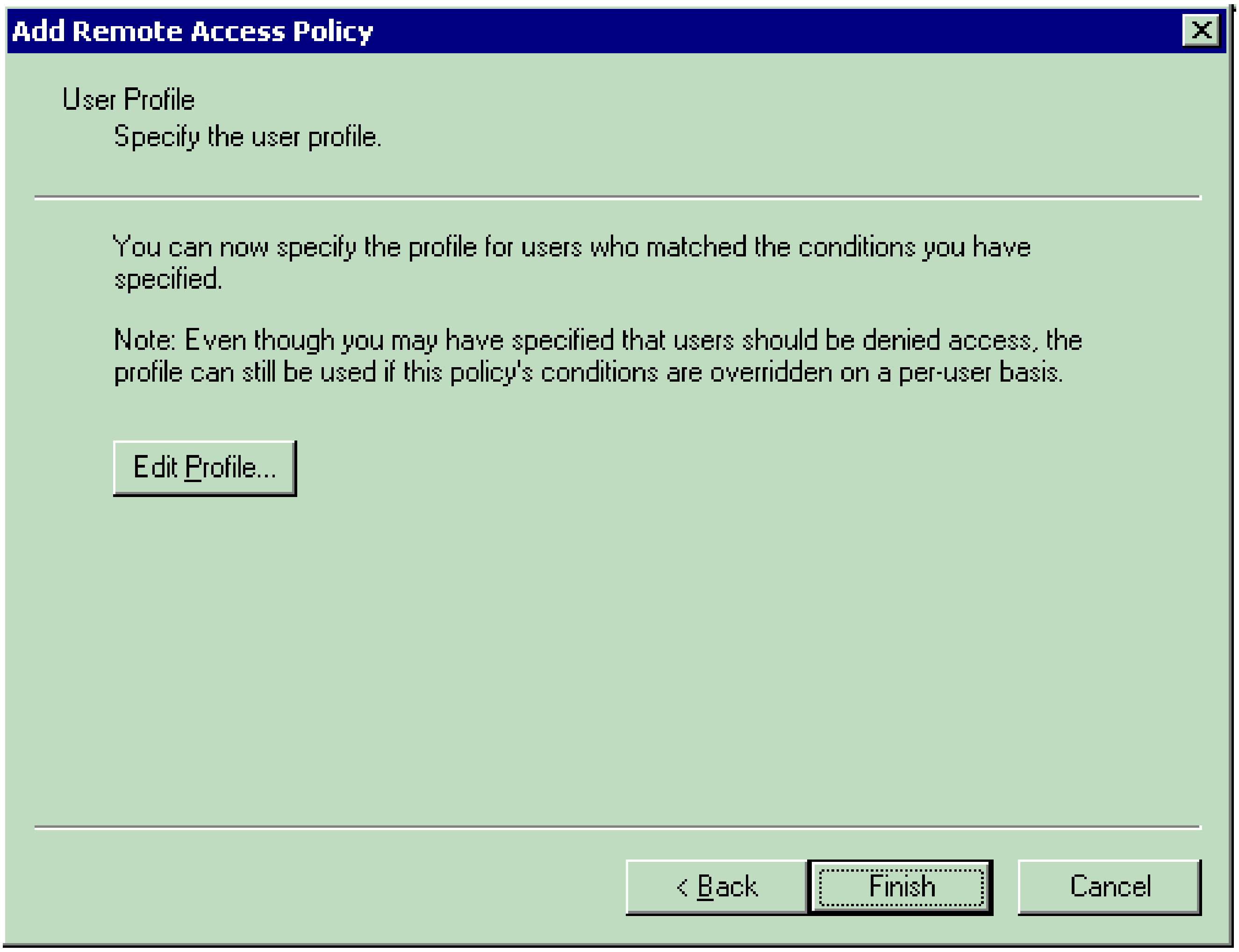
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

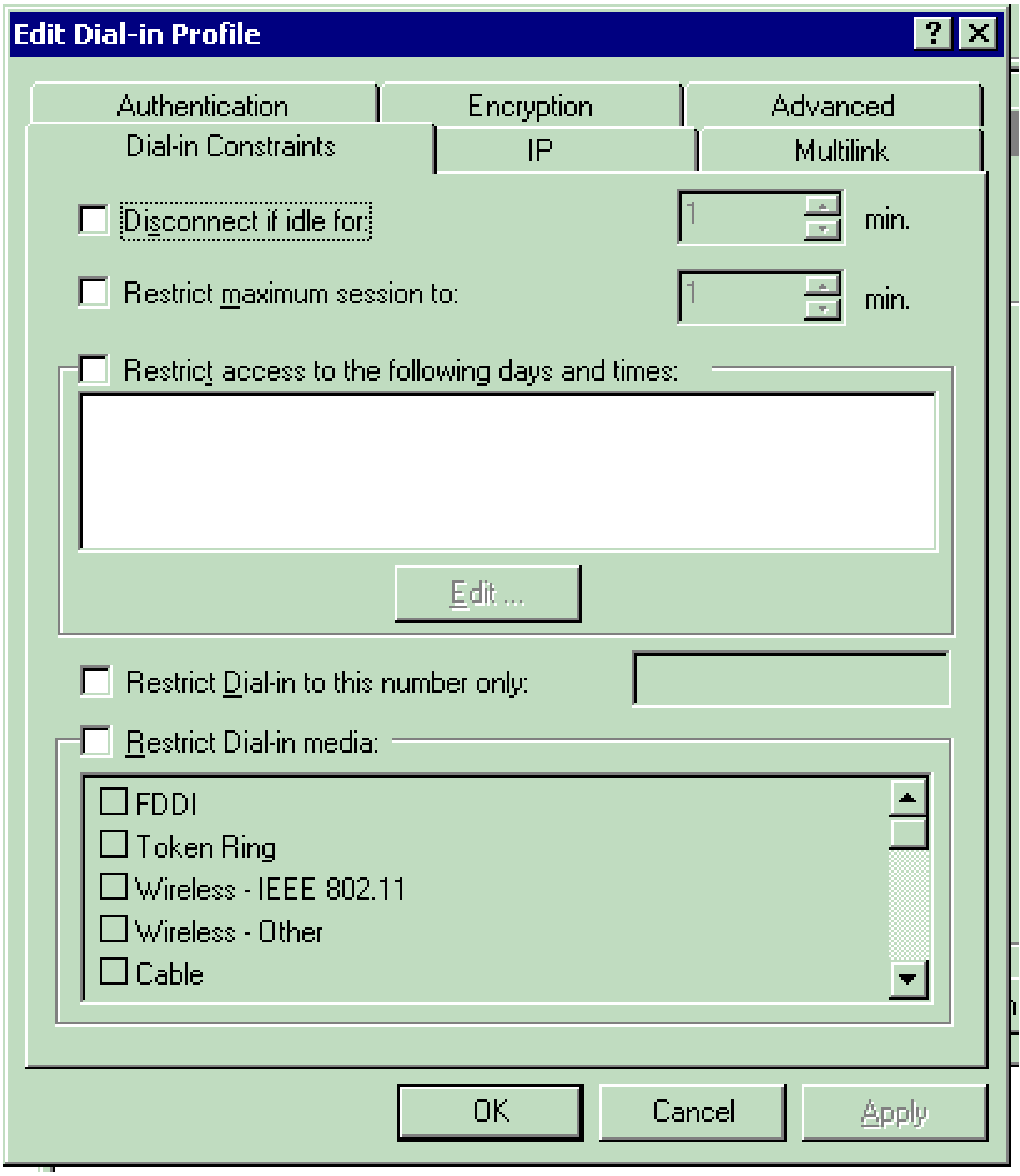
6. 按「**Next**」（下一步）。
7. 下一步是設定使用者配置檔案。儘管您可能已經指定應該根據條件拒絕或授予使用者訪問許可權，但是，如果此策略的條件被基於每個使用者覆蓋，則仍然可以使用配置檔案。



You can now specify the profile for users who matched the conditions you have specified.

Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.

若要配置使用者配置檔案，請在「使用者配置檔案」視窗中按一下**「編輯配置檔案」**。出現「Edit Dial-in Profile（編輯撥入配置檔案）」視窗。



Edit Dial-in Profile

□ Disconnect if idle for: 1 min.

□ Restrict maximum session to: 1 min.

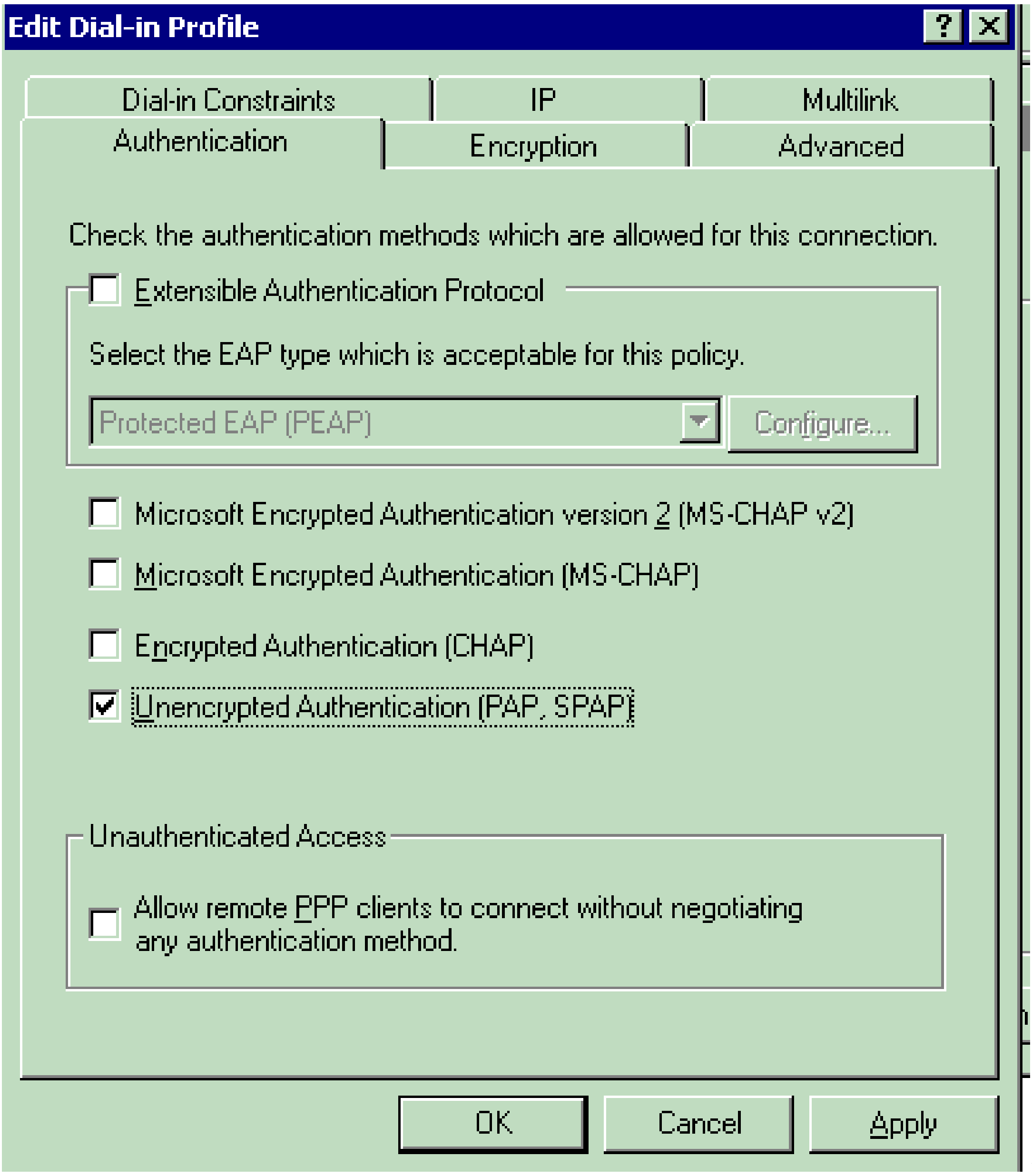
□ Restrict access to the following days and times:

□ Restrict Dial-in to this number only:

□ Restrict Dial-in media:

- □ FDDI
- □ Token Ring
- □ Wireless - IEEE 802.11
- □ Wireless - Other
- □ Cable

按一下**Authentication**索引標籤，然後選擇在WLAN中使用的驗證方法。此範例使用未加密驗證(PAP、SPAP)。



Check the authentication methods which are allowed for this connection.

☐ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Protected EAP (PEAP)

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ Microsoft Encrypted Authentication (MS-CHAP)

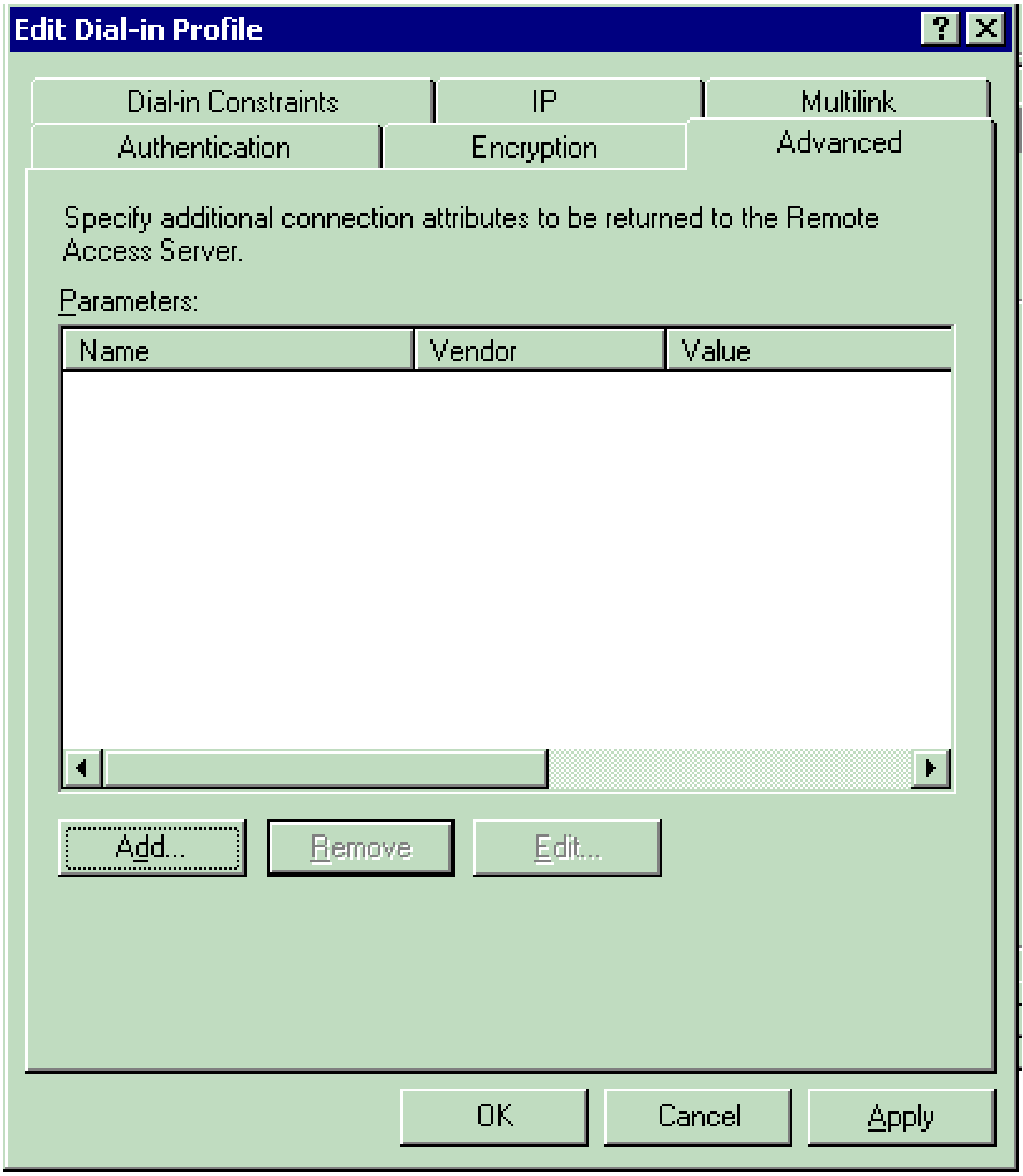
☐ Encrypted Authentication (CHAP)

☑ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

☐ Allow remote PPP clients to connect without negotiating any authentication method.

按一下 Advanced頁籤。移除所有預設引數，然後按一下「Add」。

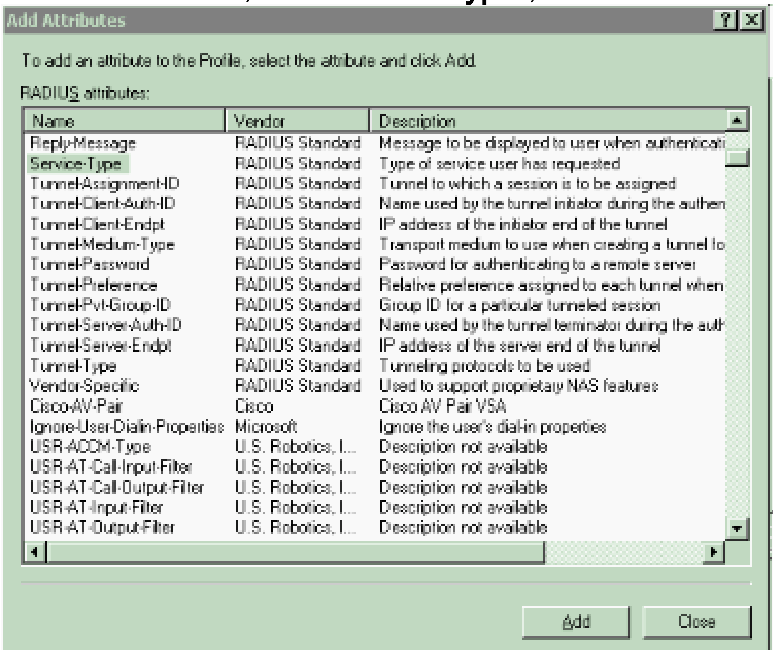


Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value

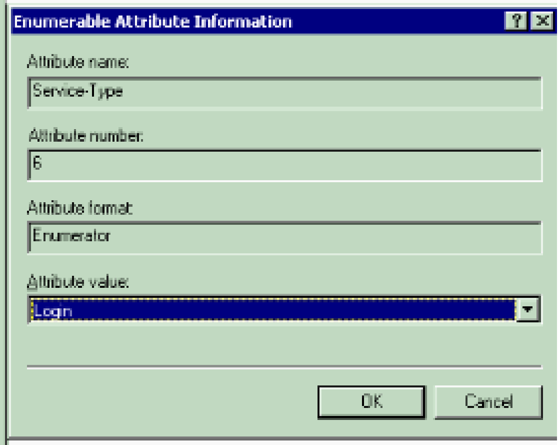
在Add Attributes視窗中，選擇Service-Type，然後從下一個視窗中選擇Login值。



To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties
USR-ACCM-Type	U.S. Robotics, I...	Description not available
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Output-Filter	U.S. Robotics, I...	Description not available



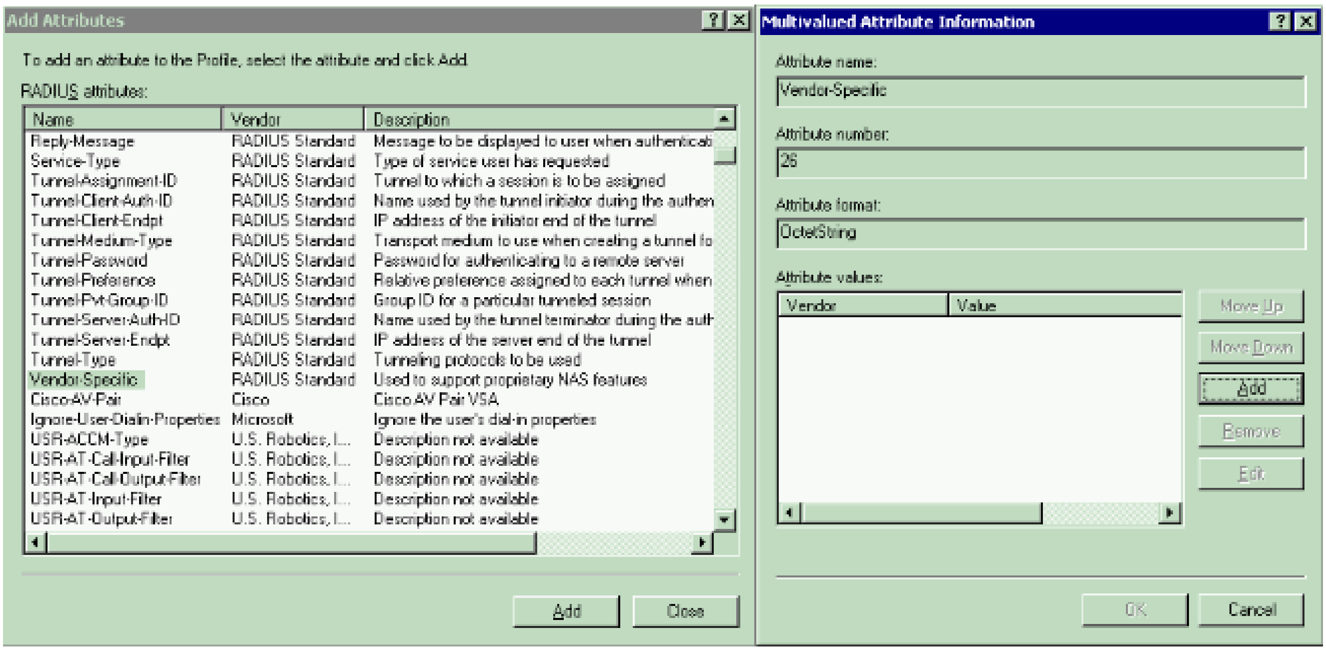
Attribute name: Service-Type

Attribute number: 6

Attribute format: Enumerator

Attribute value: Login

接下來，您需要從RADIUS屬性清單中選擇Vendor-Specific屬性。



Add Attributes

To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-AuthID	RADIUS Standard	Name used by the tunnel terminator during the auth
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties
USR-ACCM-Type	U.S. Robotics, I...	Description not available
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Output-Filter	U.S. Robotics, I...	Description not available

Multivalued Attribute Information

Attribute name: Vendor-Specific

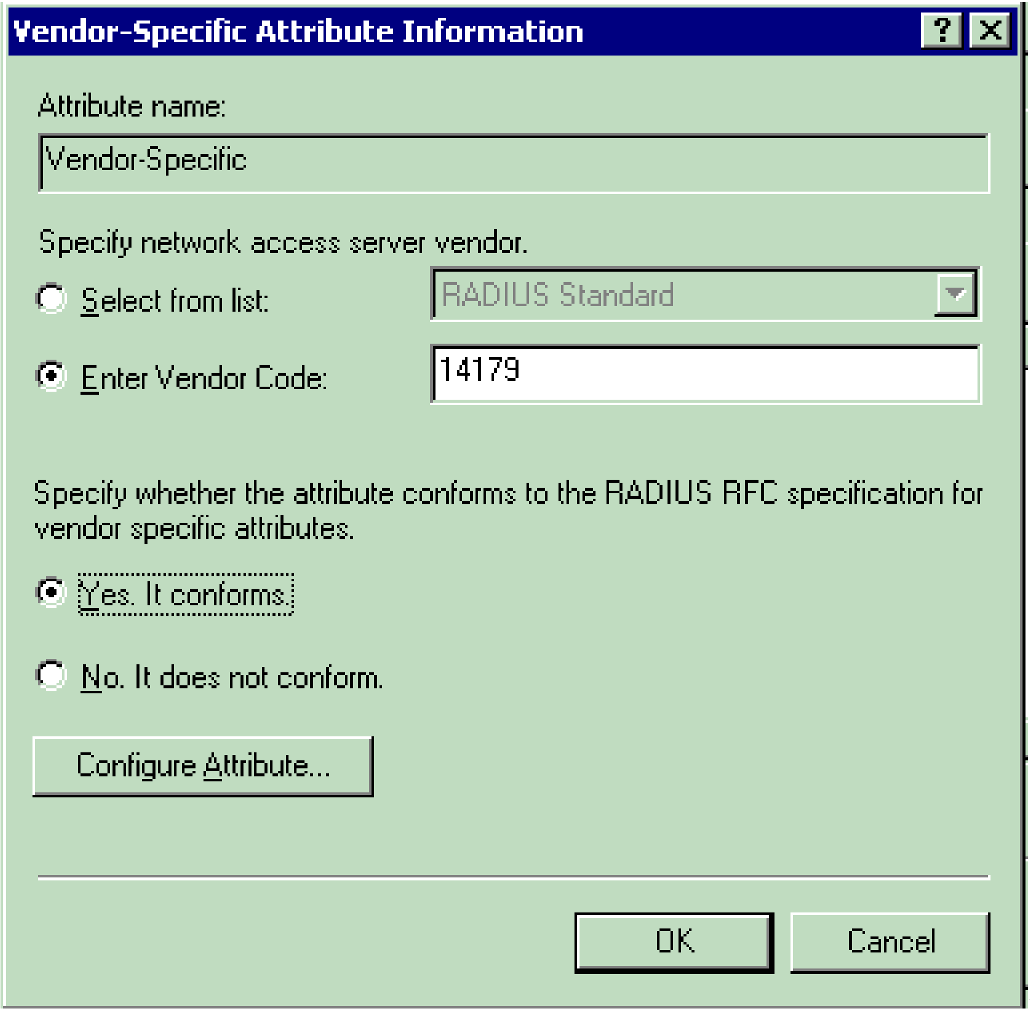
Attribute number: 26

Attribute format: OctetString

Attribute values:

Vendor	Value

在下一個視窗中，按一下**Add**以選擇新的VSA。此時將出現「供應商特定屬性資訊」視窗。在Specify network access server vendor下，選擇**Enter Vendor Code**。輸入Airespace VSA的供應商代碼。Cisco Airespace VSA的供應商代碼為**14179**。由於此屬性符合VSA的RADIUS RFC規範，請選擇**Yes。它符合。**



Vendor-Specific Attribute Information

Attribute name: Vendor-Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

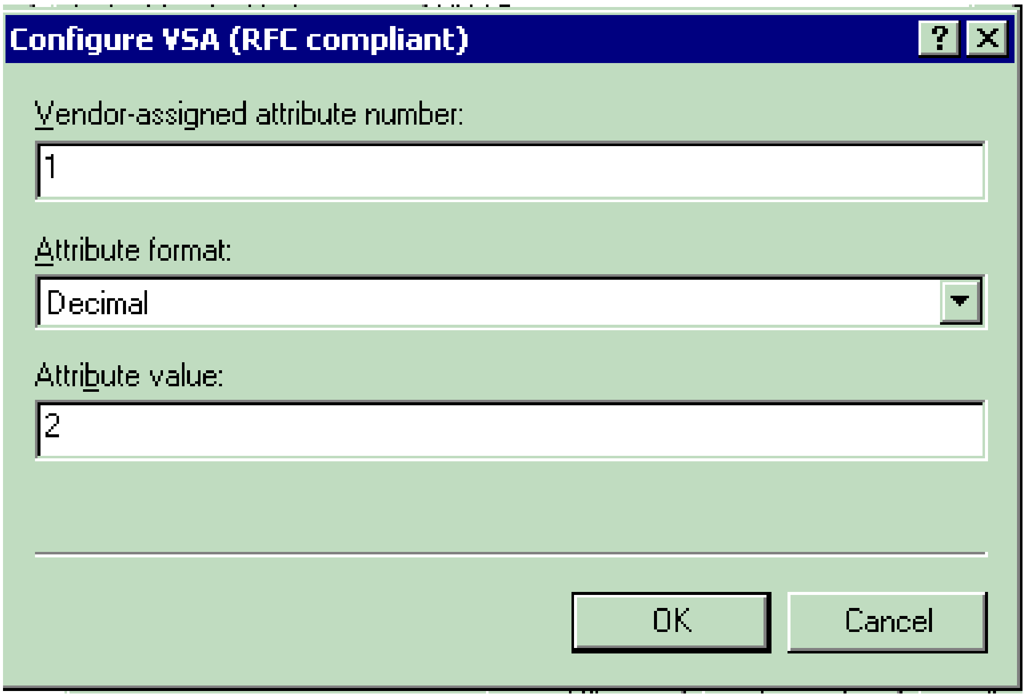
● Enter Vendor Code: 14179

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms.

○ No. It does not conform.

.按一下「**Configure Attribute**」。在配置VSA（符合RFC）視窗中，輸入供應商分配的屬性編號、屬性格式和屬性值，具體取決於您要使用的VSA。要按使用者設定WLAN-ID，請執行以下操作：**屬性名**稱 — Airespace-WLAN-Id**供應商分配的屬性編**號 — 1**屬性格式** — 整數/十進位制**值**- WLAN-ID**範例**



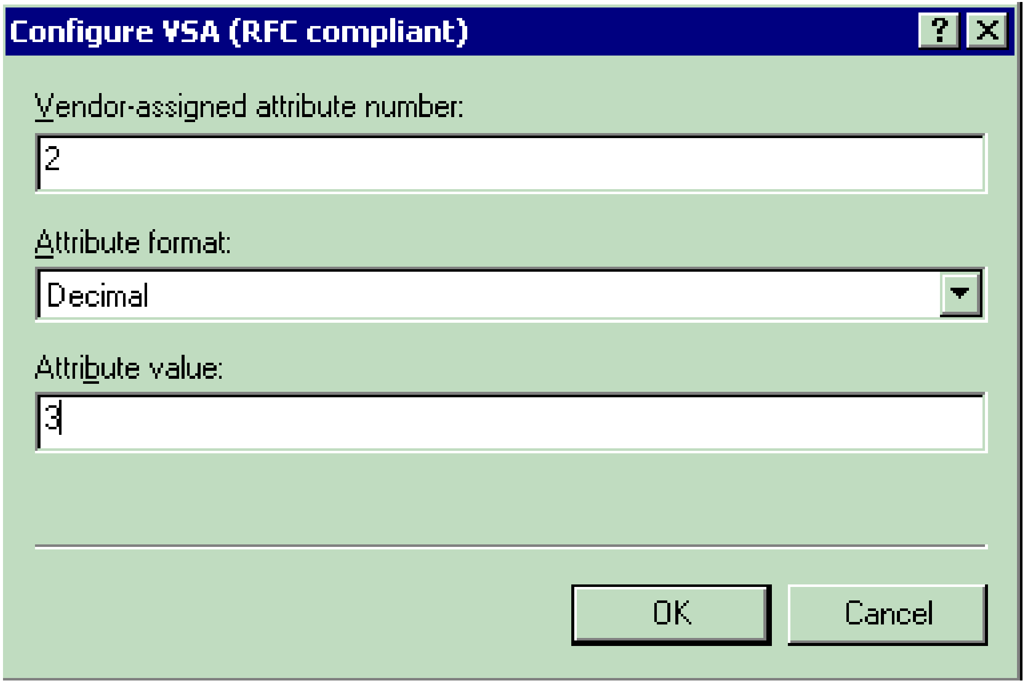
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 1

Attribute format: Decimal

Attribute value: 2

1 要按使用者設定QoS配置檔案，請執行以下操作：**屬性名稱** — Airespace-QoS-Level**供應商分配的屬性編**號 — 2**屬性格式** — 整數/十進位制**值**- 0 — 銀牌；1 — 黃金；2 — 白金；3 — 銅牌**範例 2**



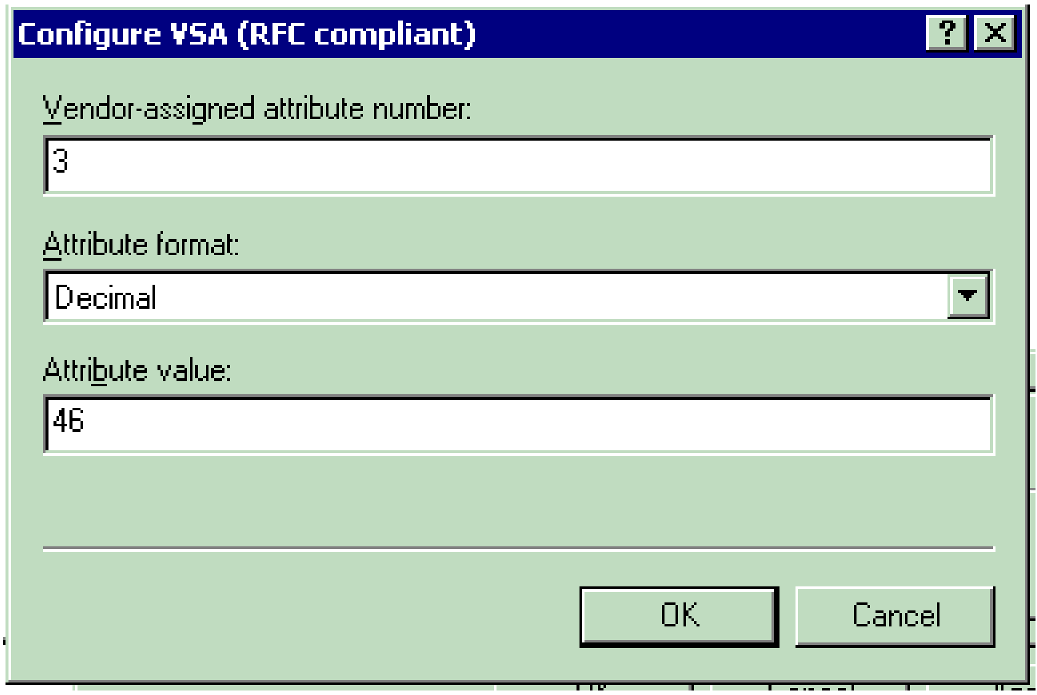
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 2

Attribute format: Decimal

Attribute value: 3

要按使用者設定DSCP值，請執行以下操作：**屬性名稱** — Airespace-DSCP**供應商分配的屬性編號**- 3**屬性格式** — 整數/十進位制**值**- DSCP值**範例 3**

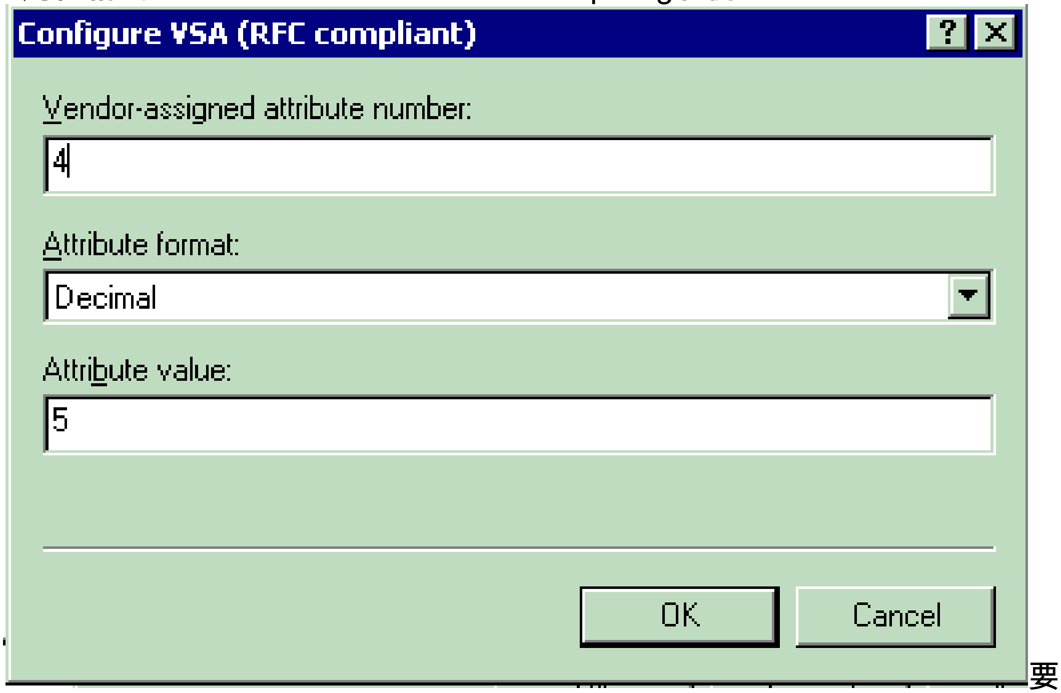

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 3

Attribute format: Decimal

Attribute value: 46

要按使用者設定802.1p-Tag，請執行以下操作：**屬性名稱** — Airespace-802.1p-Tag**供應商分配的屬性編**號 — 4**屬性格式** — 整數/十進位制**Value** - 802.1p-Tag**範例 4**

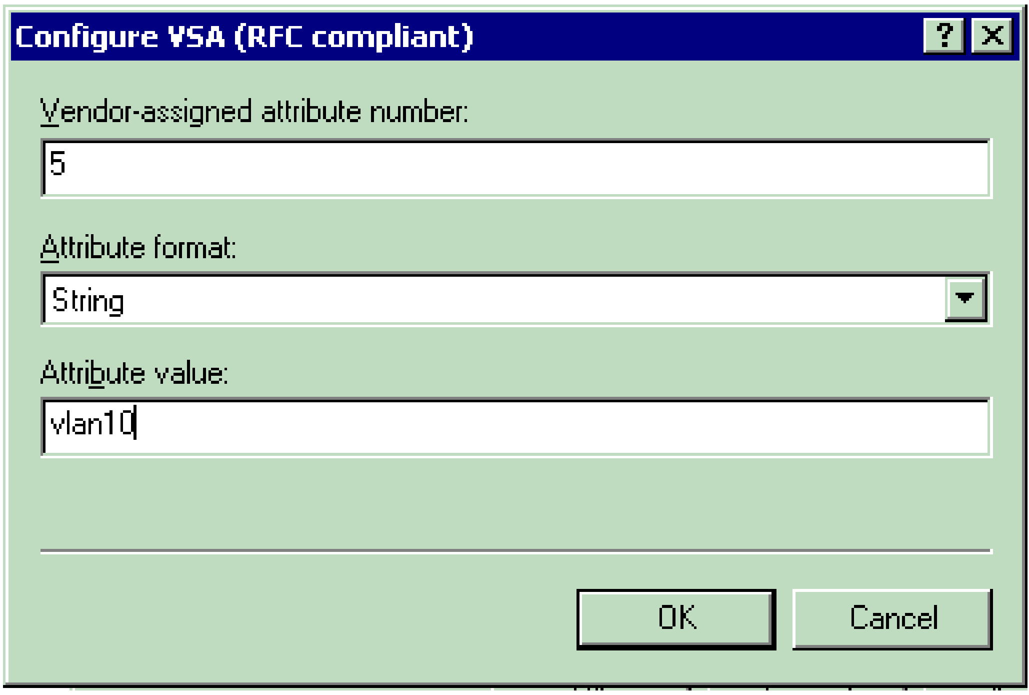

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 4

Attribute format: Decimal

Attribute value: 5

要針對每個使用者設定介面(VLAN):**Attribute Name** - Airespace-Interface-Name**供應商分配的屬性編**號 — 5**屬性格式** — 字串**Value** — 介面名稱**範例 5**

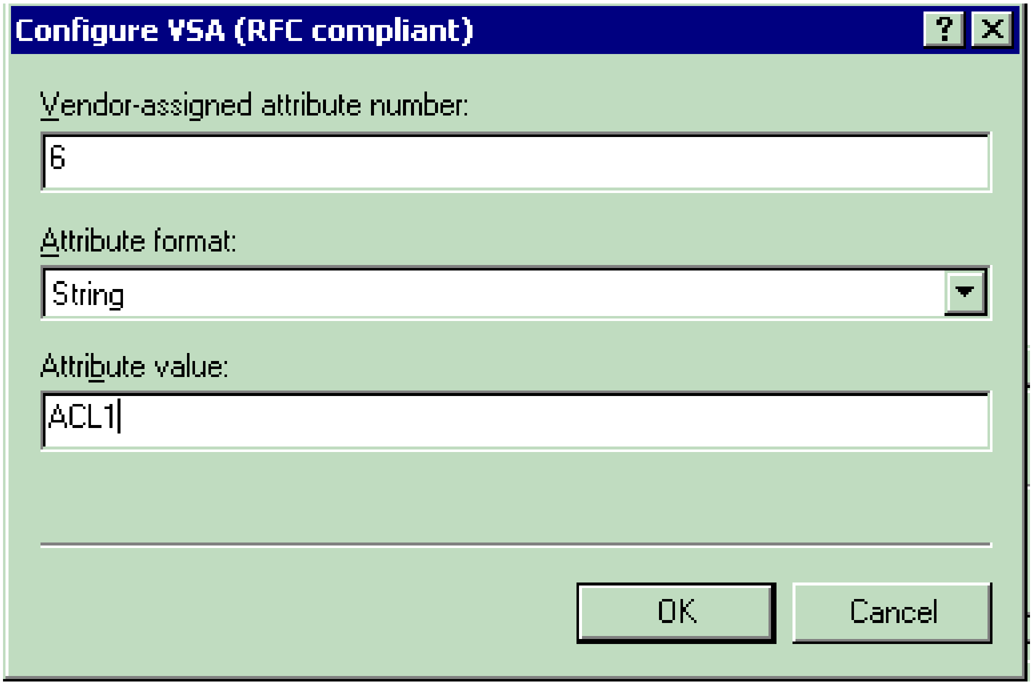


Vendor-assigned attribute number: 5

Attribute format: String

Attribute value: vlan10

要按使用者設定ACL，請執行以下操作：**屬性名稱** — Airespace-ACL-Name**供應商分配的屬性編**號 — 6**屬性格式** — 字串**Value** - ACL-Name**範例 6**

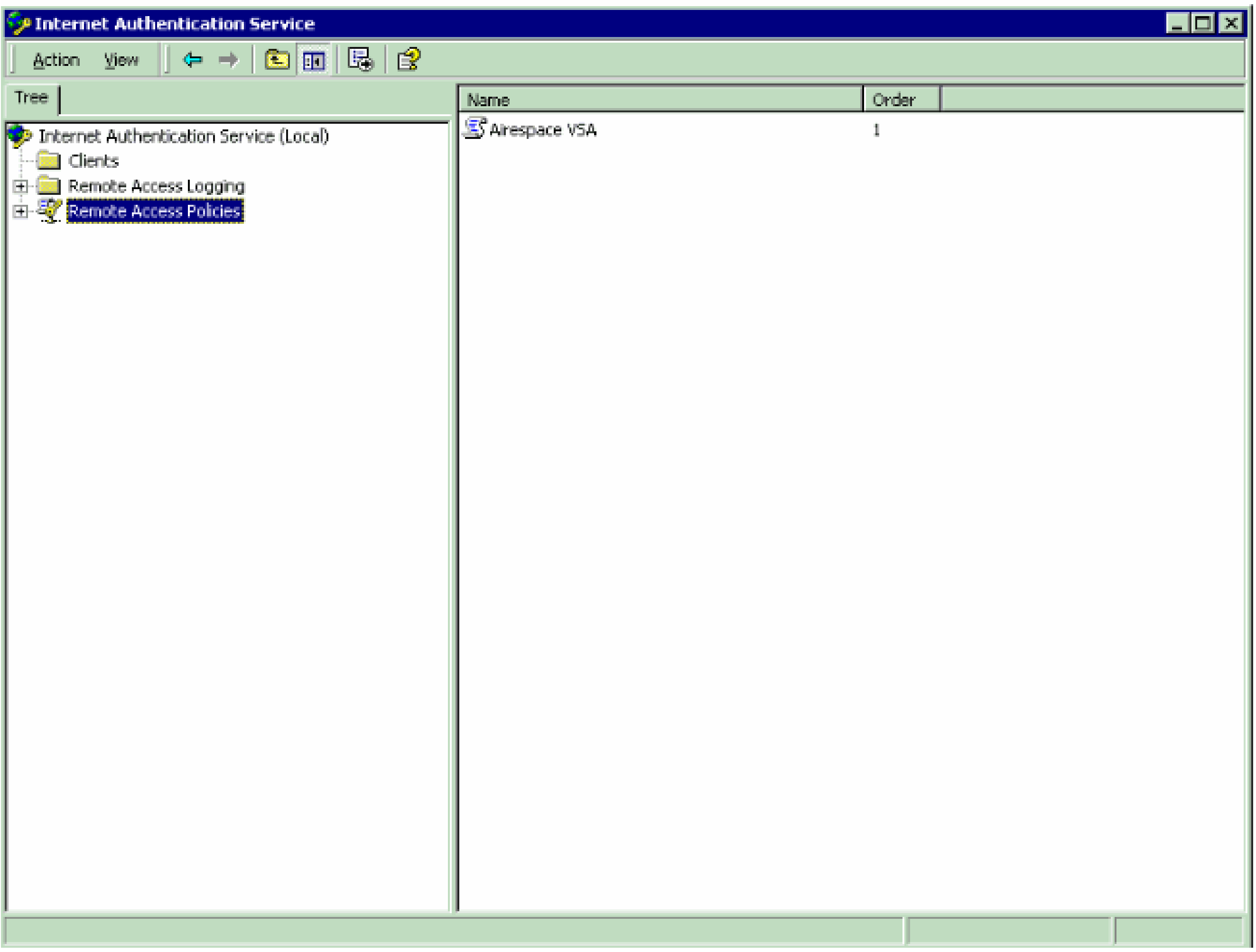


Vendor-assigned attribute number: 6

Attribute format: String

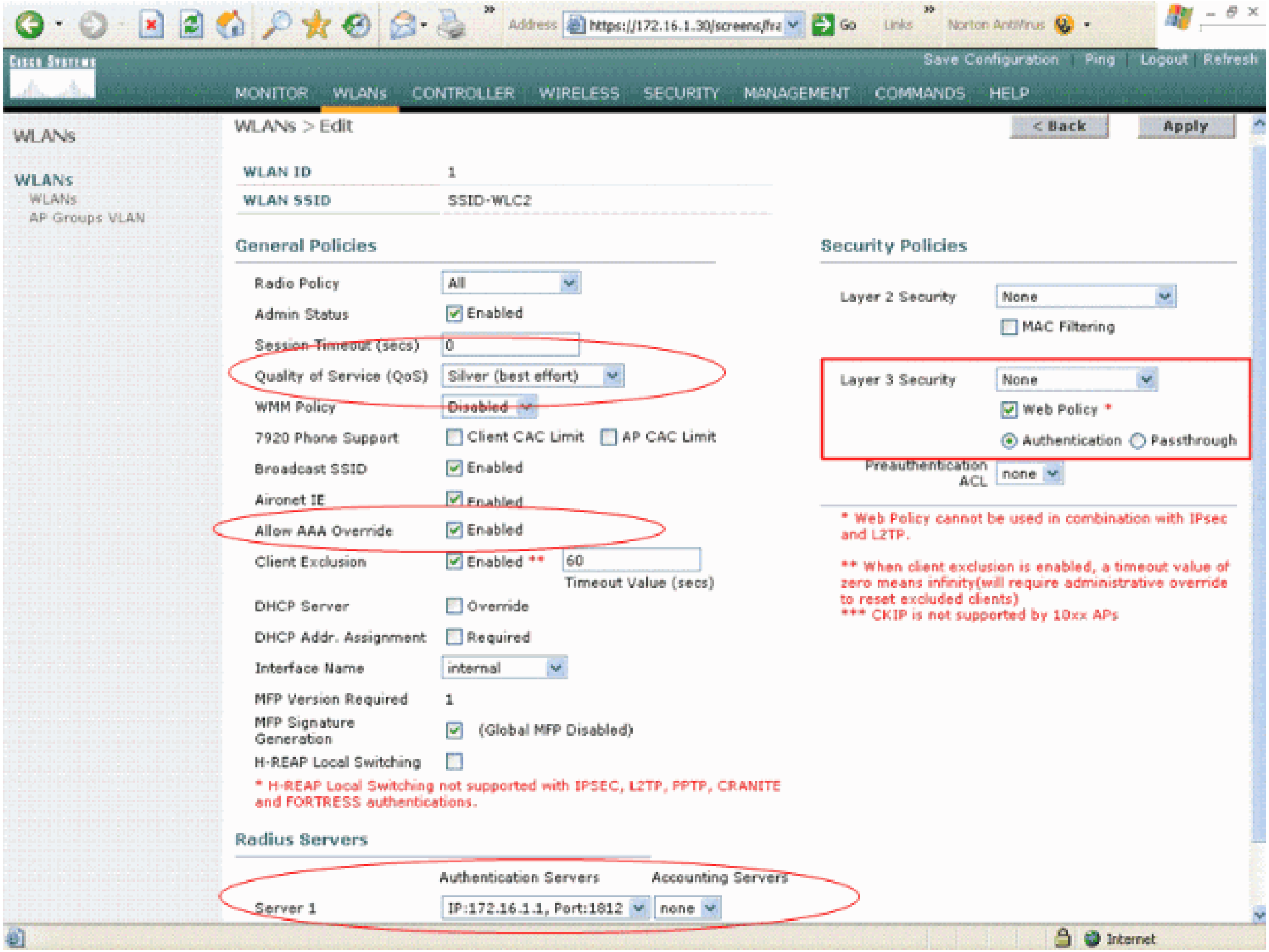
Attribute value: ACL1

8. 配置VSA後，按一下**OK**，直到看到User profile（使用者配置檔案）視窗。
9. 然後按一下**Finish**以完成配置。您可以在遠端訪問策略下看到新策略。



組態範例

在此範例中，WLAN設定為Web驗證。使用者由IAS RADIUS伺服器進行身份驗證，並且RADIUS伺服器配置為按使用者分配QoS策略。



WLANs > Edit

WLAN ID	1
WLAN SSID	SSID-WLC2

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	0
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Aironet IE	☑ Enabled
Allow AAA Override	☑ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	□ Required
Interface Name	internal
MFP Version Required	1
MFP Signature Generation	☑ (Global MFP Disabled)
H-REAP Local Switching	□

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.1.1, Port:1812	none

Security Policies

Layer 2 Security	None
	□ MAC Filtering
Layer 3 Security	None
	☑ Web Policy *
	● Authentication ○ Passthrough
Preauthentication ACL	none

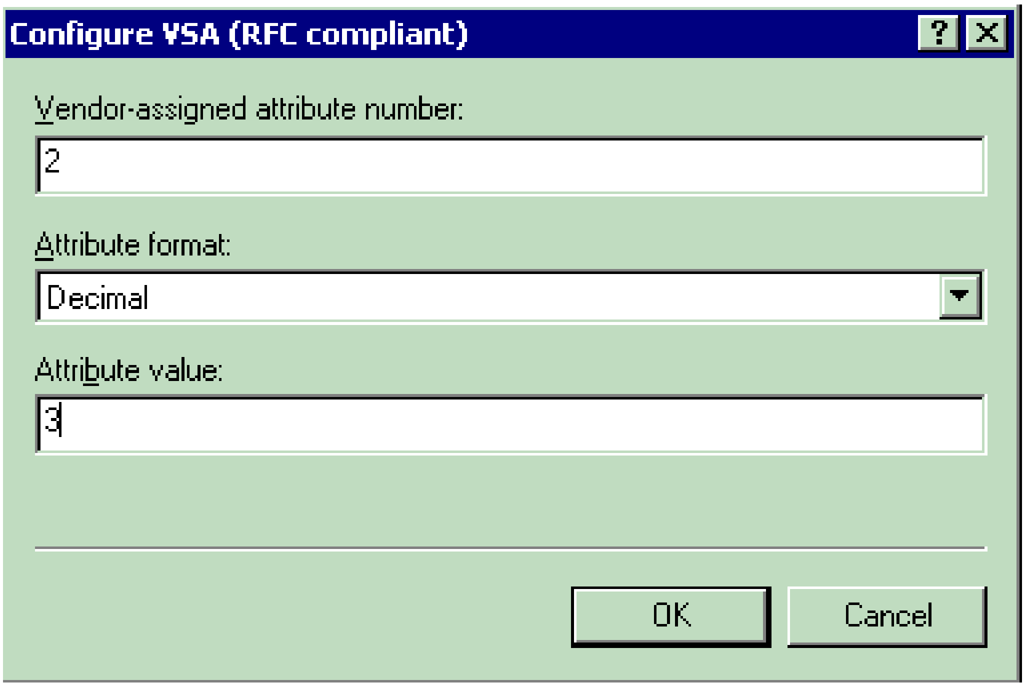
* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

*** CKIP is not supported by 10xx APs

您可以從該視窗看到，Web驗證已啟用，驗證伺服器為172.16.1.1，而且在WLAN上也啟用了AAA覆寫。此WLAN的預設QoS設定設定為Silver。

在IAS RADIUS伺服器上，配置了遠端訪問策略，該策略返回RADIUS接受請求中的QoS屬性Bronze。當您配置特定於QoS屬性的VSA時，會完成此操作。



Configure VSA (RFC compliant)

Vendor-assigned attribute number:

2

Attribute format:

Decimal

Attribute value:

3

有關如何在IAS伺服器上配置遠端訪問策略的詳細資訊，請參閱本文檔的在IAS上配置遠端訪問策略部分。

一旦為此設定配置了IAS伺服器、WLC和LAP，無線客戶端就可以使用Web身份驗證進行連線。

驗證

使用本節內容，確認您的組態是否正常運作。

當使用者使用使用者ID和密碼連線到WLAN時，WLC會將憑證傳遞到IAS RADIUS伺服器，該伺服器根據遠端訪問策略中配置的條件和使用者配置檔案對使用者進行身份驗證。如果使用者驗證成功，RADIUS伺服器會傳回也包含AAA覆寫值的RADIUS接受要求。在這種情況下，將返回使用者的QoS策略。

您可以發出**debug aaa all enable**命令來檢視身份驗證期間發生的事件順序。以下是輸出範例：

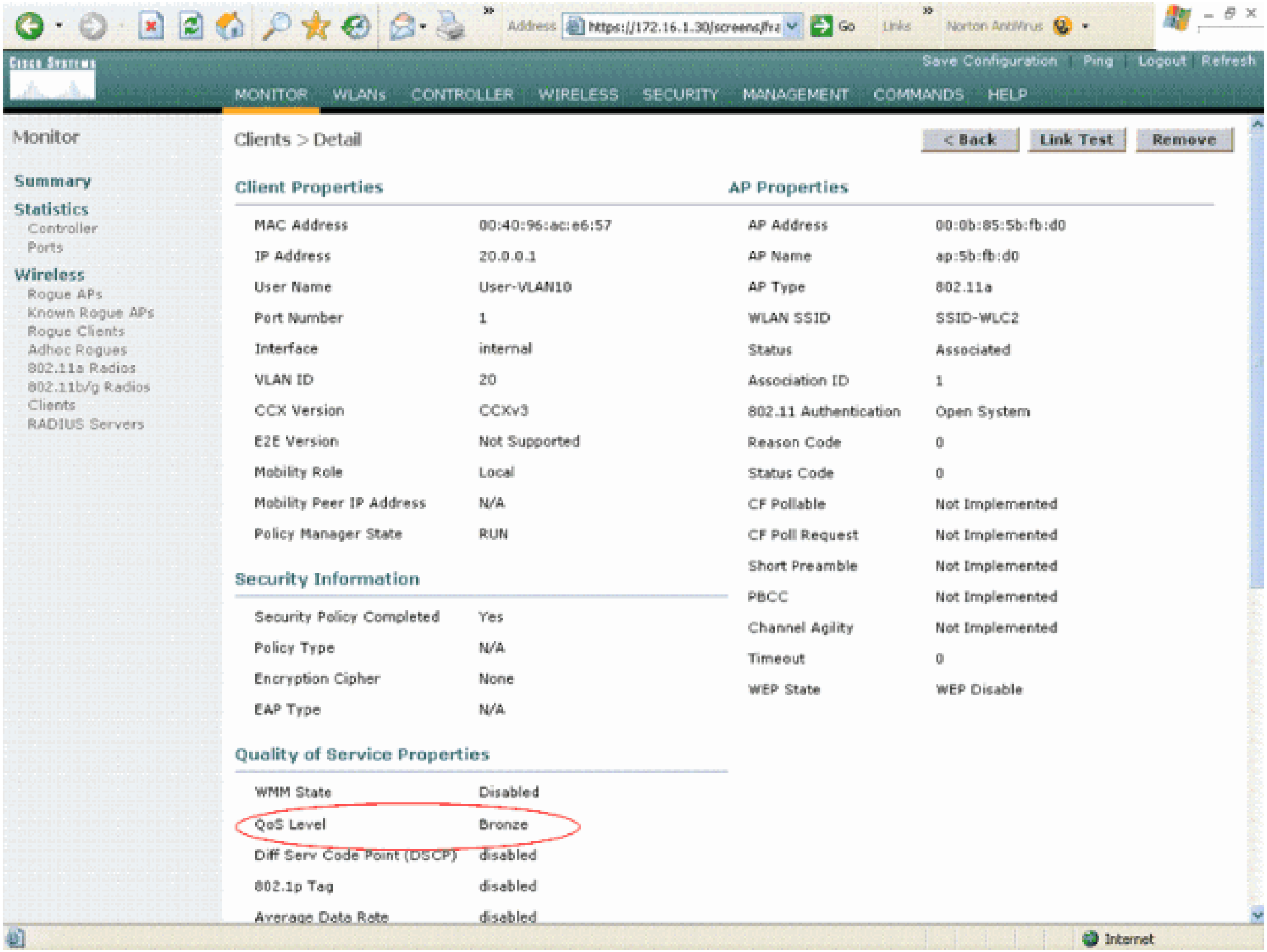
```
(Cisco Controller) > debug aaa all enable
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 28:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 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)
```

從輸出中您可以看到，使用者已進行驗證。接著，AAA覆寫值會與RADIUS接受訊息一起傳回。在這種情況下，使用者將獲得Bronze的QoS策略。

您也可在WLC GUI上驗證這點。以下是範例：



Clients > Detail

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

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

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

注意：此SSID的預設QoS配置檔案是Silver。但是，由於選擇了AAA覆蓋，並且使用者在IAS伺服器上配置了Bronze的QoS配置檔案，因此預設的QoS配置檔案將被覆蓋。

疑難排解

您可以在WLC上使用**debug aaa all enable**指令對組態進行疑難排解。本檔案的驗證一節將提供在正常網路中此偵錯輸出的範例。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

相關資訊

- **思科無線LAN控制器組態設定指南4.0版**

- 使用WLC和Cisco Secure ACS配置示例根據SSID限制WLAN訪問
- 無線產品支援
- 技術支援與文件 - Cisco Systems