運行Cisco IOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證示例

目錄

簡介

本檔案將說明如何在以本機模式(適用於Supervisor Engine和MSFC的單一Cisco IOS®軟體映像)執行的Catalyst 6500/6000上設定IEEE 802.1x，以及在遠端驗證撥入使用者服務(RADIUS)伺服器上進行驗證和VLAN指派。

必要條件

需求

本文檔的讀者應瞭解以下主題：

- Windows 4.1版Cisco Secure ACS安裝指南
- 思科安全訪問控制伺服器4.1使用手冊
- RADIUS 如何運作？
- Catalyst交換和ACS部署指南

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 在Supervisor Engine上執行Cisco IOS軟體版本12.2(18)SXF的Catalyst 6500**注意：**您需要使用Cisco IOS軟體版本12.1(13)E或更高版本來支援基於802.1x埠的身份驗證。
- 此範例使用Cisco Secure Access Control Server(ACS)4.1作為RADIUS伺服器。**注意：**在交換機上啟用802.1x之前，必須指定RADIUS伺服器。
- 支援802.1x身份驗證的PC客戶端**注意：**此示例使用Microsoft Windows XP客戶端。

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

IEEE 802.1x標準定義了基於客戶端伺服器的訪問控制和身份驗證協定，限制未經授權的裝置通過可公開訪問的埠連線到LAN。802.1x通過在每個埠建立兩個不同的虛擬接入點來控制網路訪問。一個接入點是非受控埠；另一個是受控埠。通過單個埠的所有流量對兩個接入點都可用。802.1x會驗證連線到交換器連線埠的每個使用者裝置，並將連線埠分配到VLAN，然後才可使用交換器或LAN提供的任何服務。在裝置通過身份驗證之前，802.1x訪問控制僅允許區域網可擴展身份驗證協定(EAPOL)流量通過裝置所連線的埠。驗證成功後，正常流量可以通過該連線埠。

注意：如果交換機從未配置802.1x身份驗證的連線埠接收EAPOL封包，或者如果交換機不支援802.1x身份驗證，則EAPOL封包會被捨棄，而且不會轉發到任何上游裝置。

設定

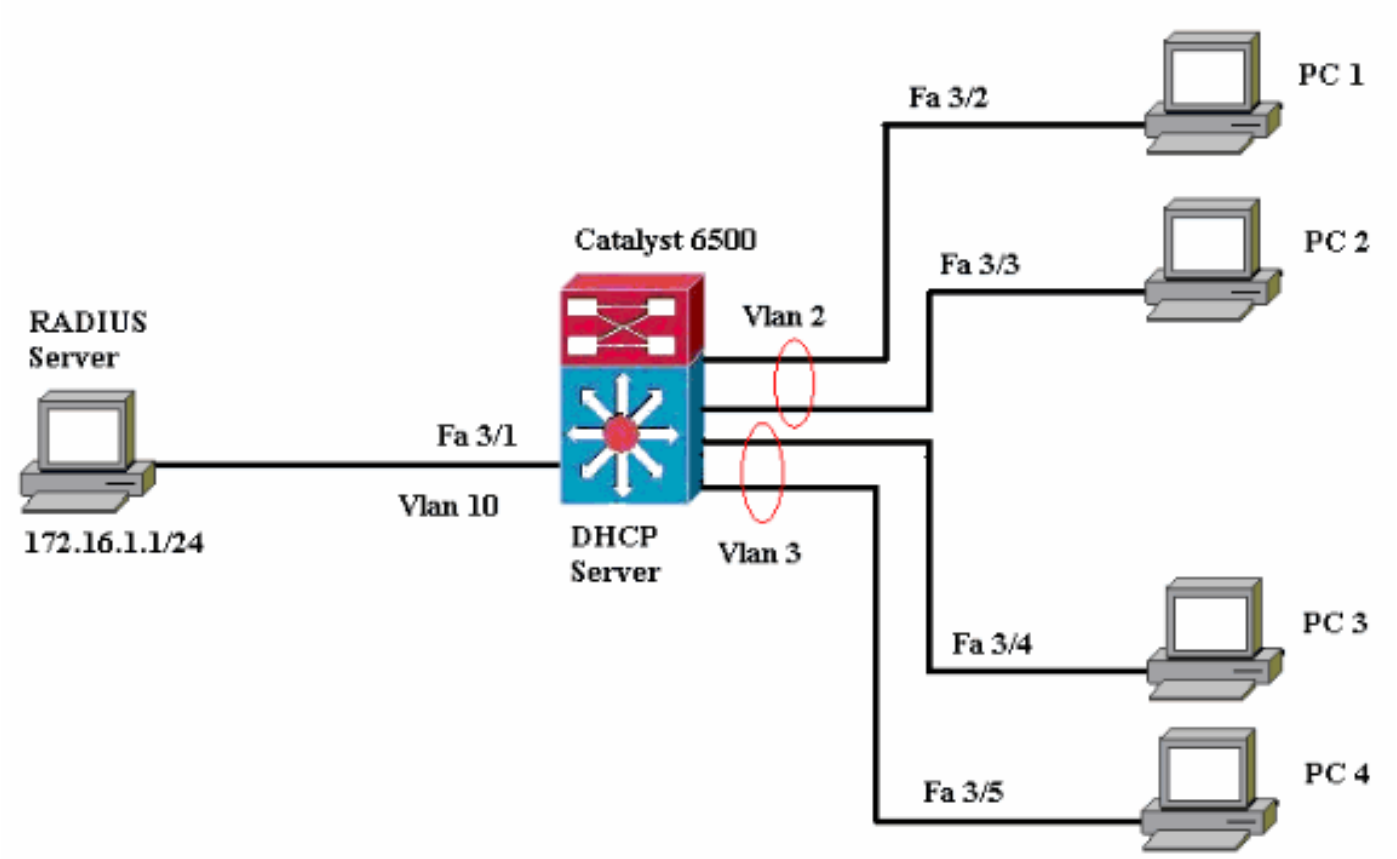
本節提供用於設定本檔案中所述802.1x功能的資訊。

此配置需要執行以下步驟：

- 為Catalyst交換機配置802.1x身份驗證。
- 設定RADIUS伺服器。
- 將PC客戶端配置為使用802.1x身份驗證。

網路圖表

本檔案會使用以下網路設定：



- RADIUS伺服器 — 執行客戶端的實際身份驗證。RADIUS伺服器會驗證使用者端的身分，並通知交換器使用者端是否獲得存取區域網路和交換器服務的授權。此處，RADIUS伺服器配置為身份驗證和VLAN分配。
- Switch — 根據客戶端的身份驗證狀態控制對網路的物理訪問。交換器充當使用者端和RADIUS伺服器之間的中繼（代理）。它從客戶端請求身份資訊，通過RADIUS伺服器驗證該資訊，並將響應中繼到客戶端。此處，Catalyst 6500交換機也被配置為DHCP伺服器。對動態主機配置協定(DHCP)的802.1x身份驗證支援允許DHCP伺服器通過將經過身份驗證的使用者身份新增到DHCP發現過程中來將IP地址分配給不同的終端使用者類別。
- 客戶端 — 請求訪問LAN和交換機服務並響應交換機請求的裝置（工作站）。這裡，PC 1到4是請求通過身份驗證的網路訪問的客戶端。PC 1和2使用與VLAN 2相同的登入憑據。同樣，PC 3和4使用VLAN 3的登入憑據。PC客戶端配置為從DHCP伺服器獲取IP地址。

配置Catalyst交換機以進行802.1x身份驗證

此交換機配置示例包括：

- 如何在快速乙太網埠上啟用802.1x身份驗證。
- 如何將RADIUS伺服器連線到FastEthernet連線埠3/1後面的VLAN 10。
- 兩個IP池的DHCP伺服器配置，一個用於VLAN 2中的客戶端，另一個用於VLAN 3中的客戶端。
- VLAN間路由，在身份驗證後實現客戶端之間的連線。

有關如何配置802.1x身份驗證的准則，請參閱802.1x基於埠的身份驗證准則和限制。

注意：確保RADIUS伺服器始終在授權埠後連線。

Catalyst 6500
`Router#configure terminal`

```
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname Cat6K
!--- Sets the hostname for the switch.
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
!--- This is a dedicated VLAN for the RADIUS server.
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut
!--- Assigns the port connected to the RADIUS server to
VLAN 10. !--- Note:- All the active access ports are in
VLAN 1 by default.

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat6K(config)#interface
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
!--- Enables 802.1x on all the FastEthernet interfaces.
Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model
!--- Enables AAA. Cat6K(config)#aaa authentication dot1x
default group radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat6K(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat6K(config)#radius-server host
172.16.1.1
!--- Sets the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco
!--- The key must match the key used on the RADIUS
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.2.1
!--- This pool assigns ip address for clients in VLAN 2.
Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
```

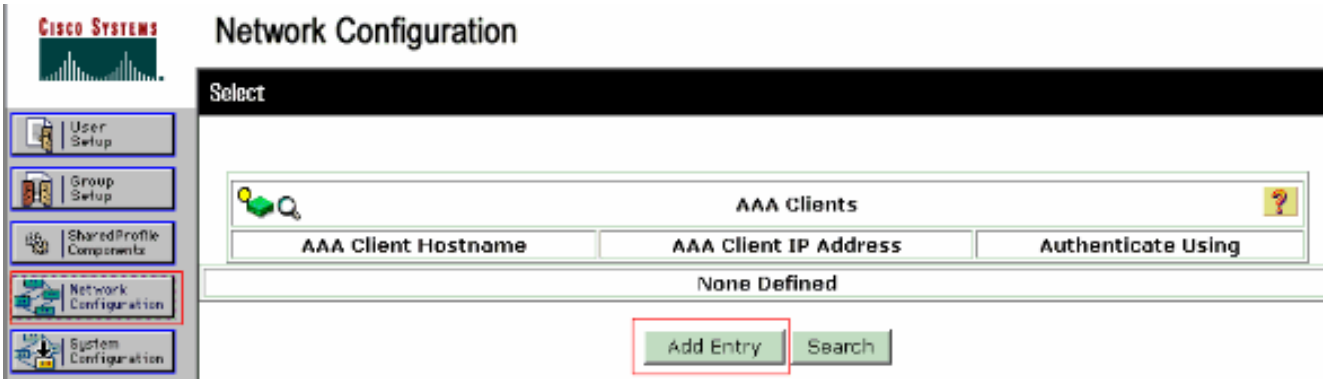
```
Cat6K(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
----------------------
1    default                           active    Fa3/2,
Fa3/3, Fa3/4, Fa3/5
                                                 Fa3/6,
Fa3/7, Fa3/8, Fa3/9
                                                 Fa3/10,
Fa3/11, Fa3/12, Fa3/13
                                                 Fa3/14,
Fa3/15, Fa3/16, Fa3/17
                                                 Fa3/18,
Fa3/19, Fa3/20, Fa3/21
                                                 Fa3/22,
Fa3/23, Fa3/24, Fa3/25
                                                 Fa3/26,
Fa3/27, Fa3/28, Fa3/29
                                                 Fa3/30,
Fa3/31, Fa3/32, Fa3/33
                                                 Fa3/34,
Fa3/35, Fa3/36, Fa3/37
                                                 Fa3/38,
Fa3/39, Fa3/40, Fa3/41
                                                 Fa3/42,
Fa3/43, Fa3/44, Fa3/45
                                                 Fa3/46,
Fa3/47, Fa3/48
2    VLAN2                             active
3    VLAN3                             active
10   RADIUS_SERVER                     active    Fa3/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

註：使用 Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

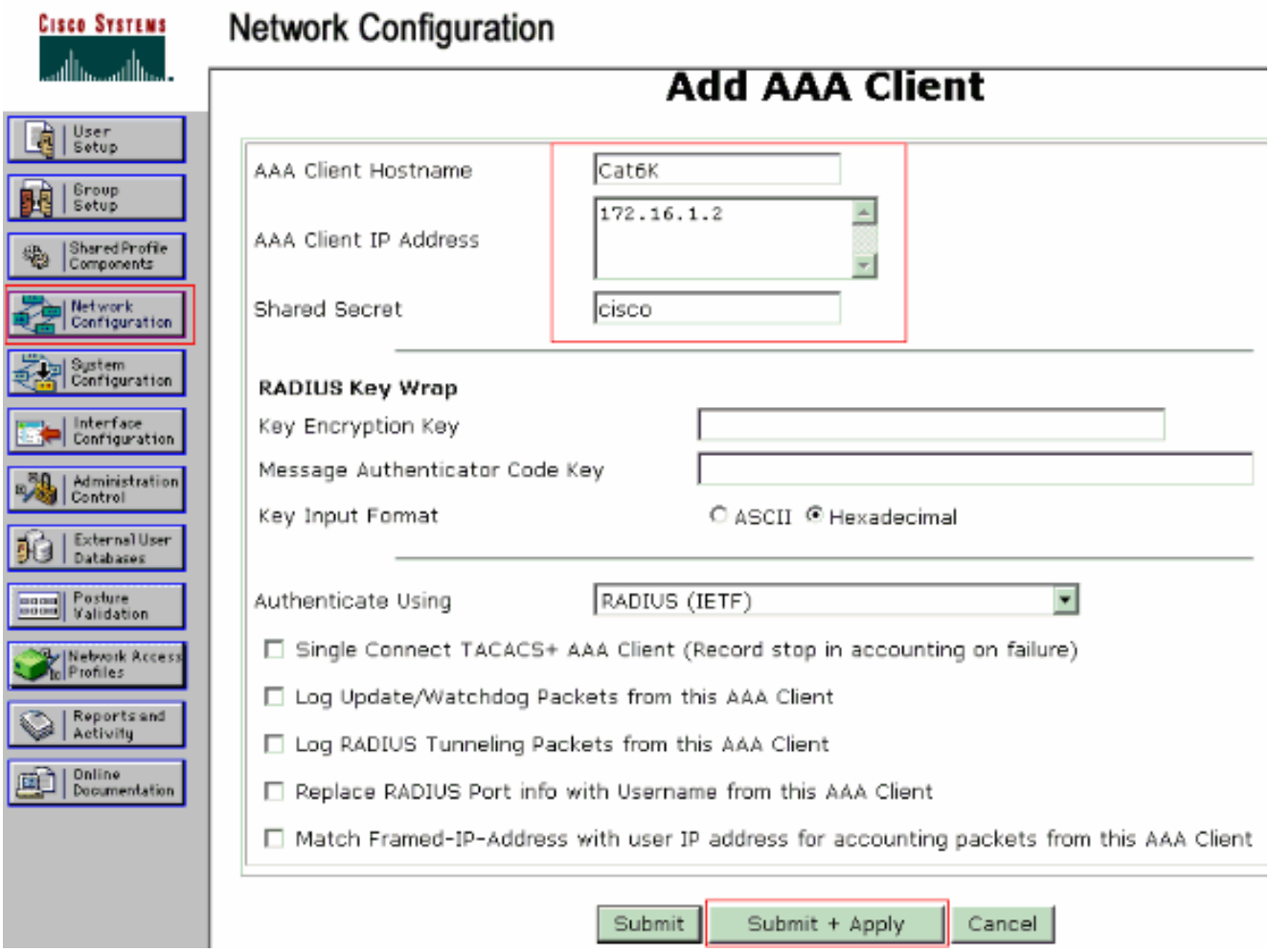
設定RADIUS伺服器

RADIUS伺服器配置了靜態IP地址172.16.1.1/24。要為AAA客戶端配置RADIUS伺服器，請完成以下步驟：

1. 在ACS管理視窗中按一下**Network Configuration**以配置AAA客戶端。
2. 按一下AAA clients部分下的**Add Entry**。



3. 將AAA客戶端主機名、IP地址、共用金鑰和身份驗證型別配置為：AAA客戶端主機名=交換機主**機名(Cat6K)**。AAA客戶端IP地址=交換機的管理介面IP**地址(172.16.1.2)**。共用金鑰=交換機上配置的RADIUS金鑰(cisco)。使用= **RADIUS** IETF**進行驗證**。**注意**：為了正確操作，AAA客戶端和ACS上的共用金鑰必須相同。金鑰區分大小寫。
4. 按一下**Submit + Apply**以使這些更改生效，如下例所示：

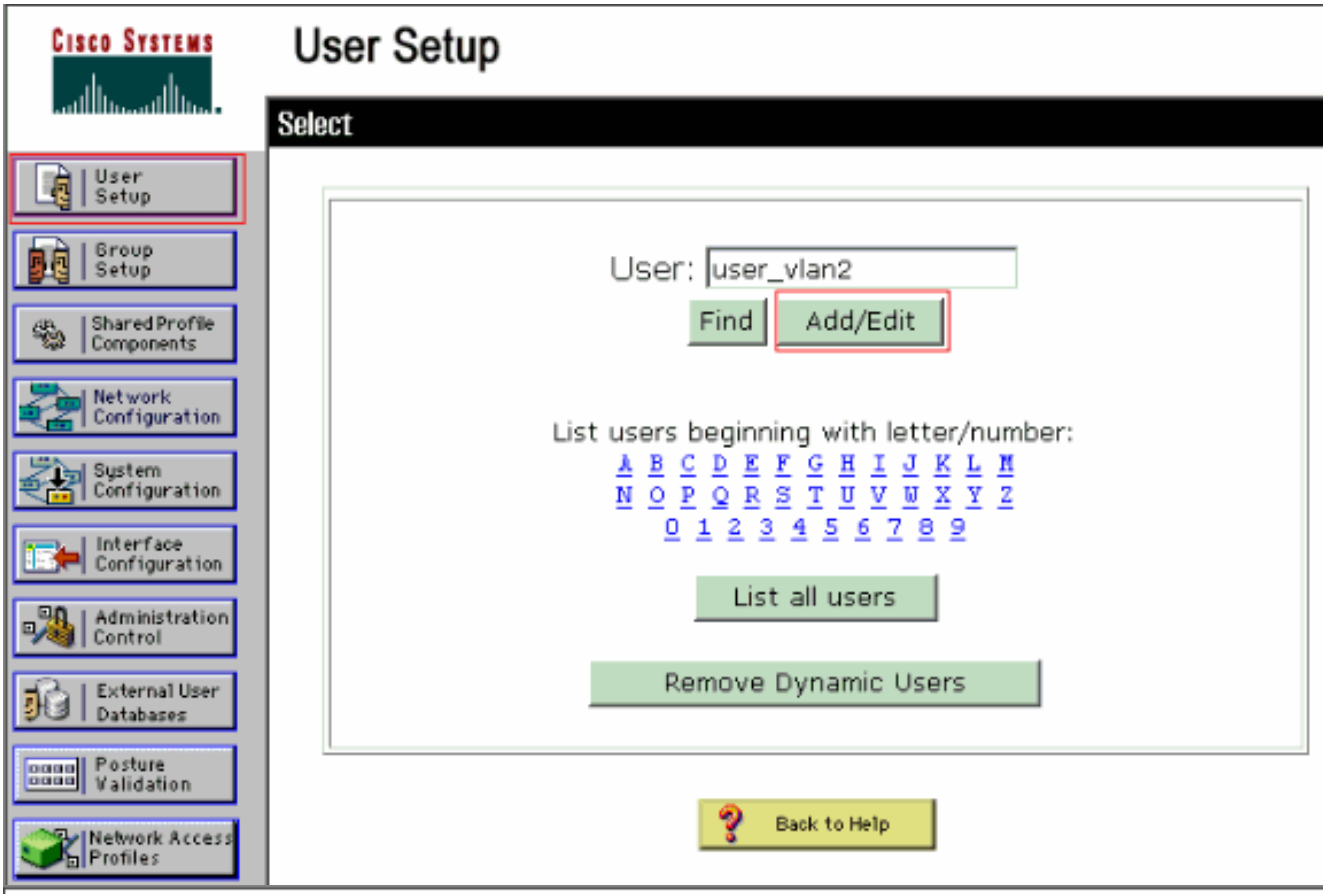


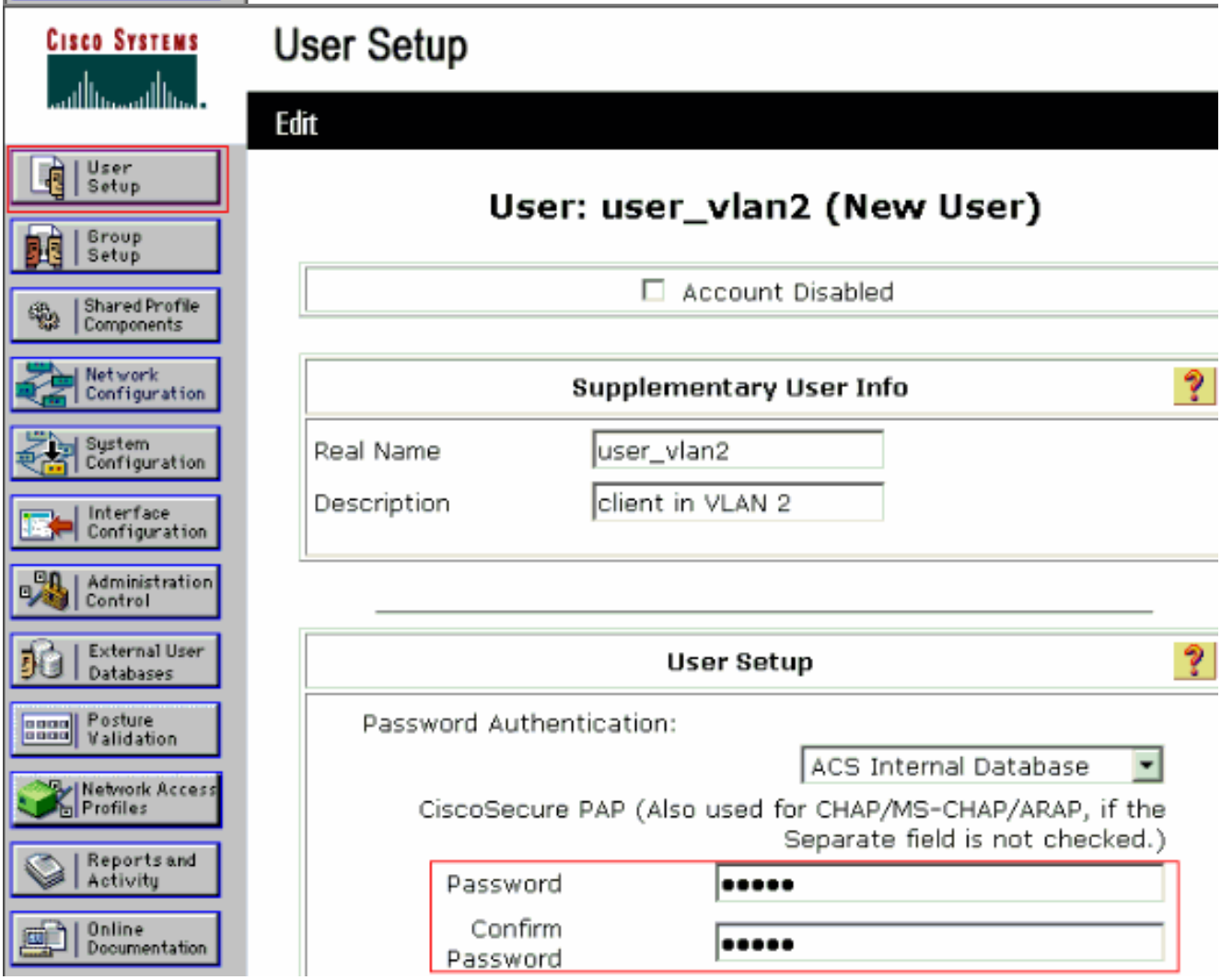
完成以下步驟，設定RADIUS伺服器以進行驗證、VLAN和IP位址分配。

必須為連線到VLAN 2的客戶端以及VLAN 3的客戶端分別建立兩個使用者名稱。為此，將為連線到VLAN 2的客戶端建立一個使用者**user_vlan2**，並為連線到VLAN 3的客戶端建立另一個使用者**user_vlan3**。

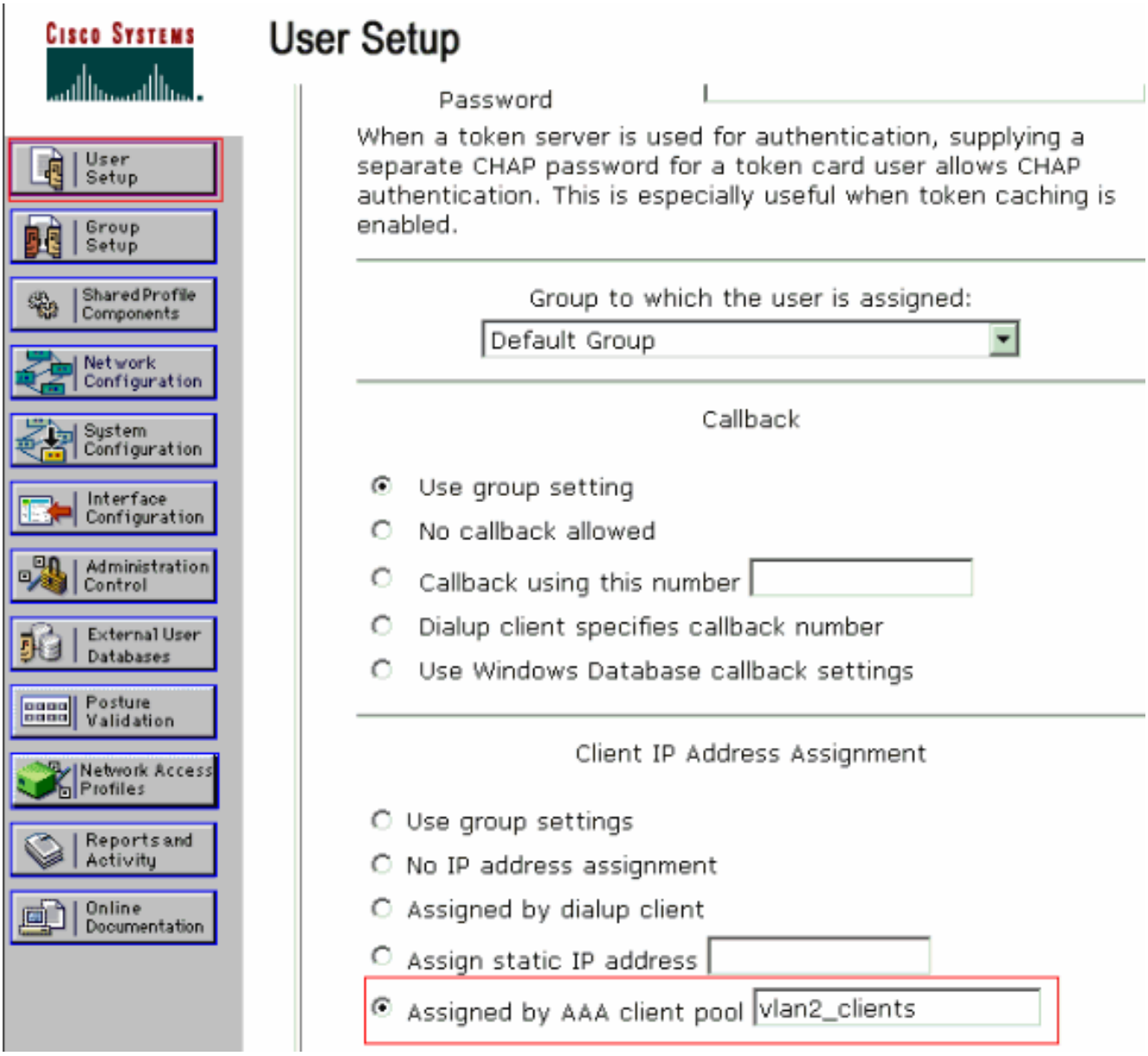
注意：在此處顯示僅連線到VLAN 2的客戶端的使用者配置。對於連線到VLAN 3的使用者，請遵循相同的步驟。

1. 要新增和配置使用者，請按一下**User Setup**並定義使用者名稱和密碼。



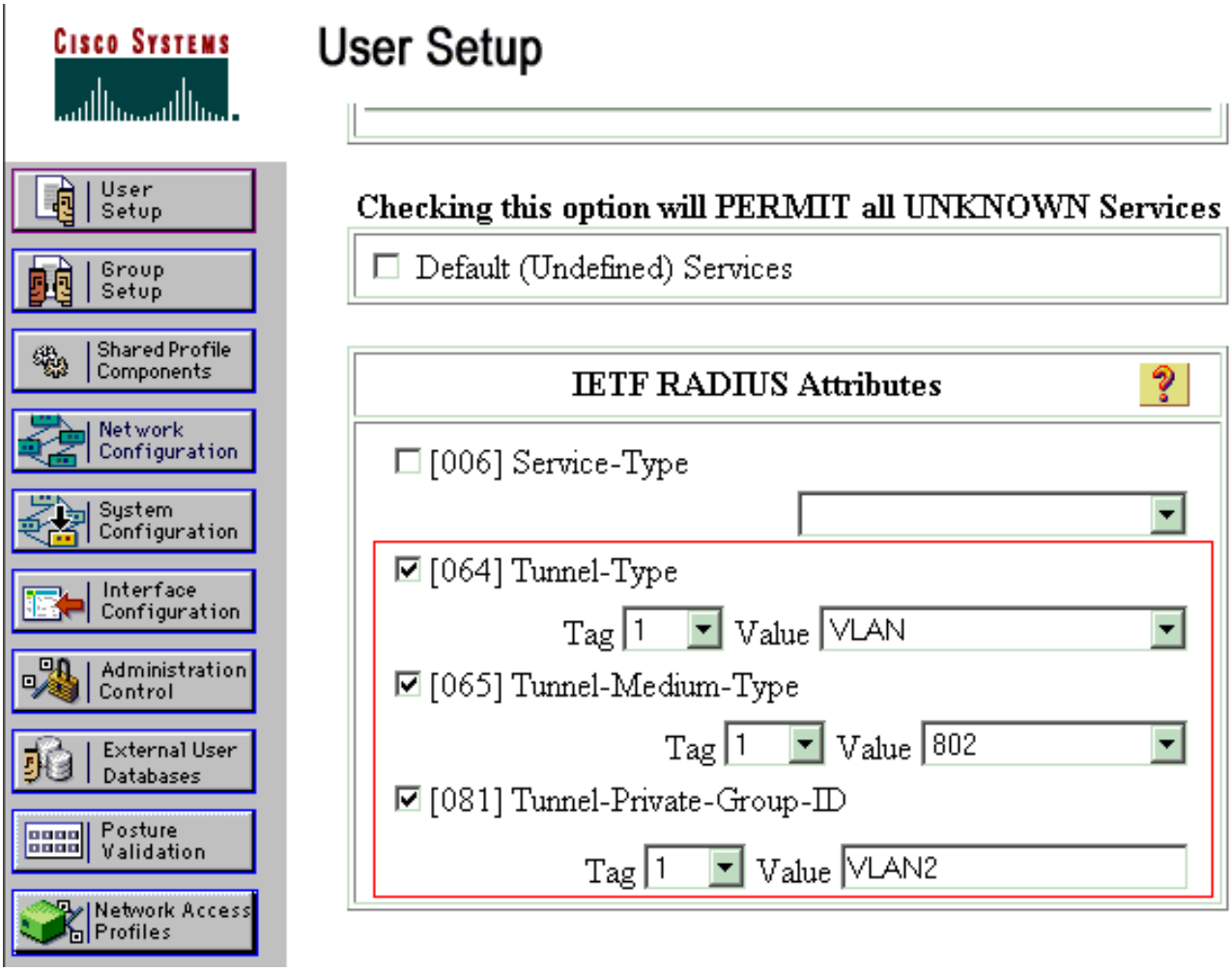


2. 將客戶端IP地址分配定義為**由AAA客戶端池分配**。輸入在交換機上為VLAN 2客戶端配置的IP地址池的名稱。



注意：只有在此使用者要通過AAA客戶端上配置的IP地址池分配IP地址時，才選擇此選項，並在框中鍵入AAA客戶端IP地址池名稱。

3. 定義Internet工程任務組(IETF)屬性**64**和**65**。確保將值的標籤設定為**1**，如以下示例所示。Catalyst將忽略除1以外的任何標籤。為了將使用者分配到特定的VLAN，還必須使用對應的VLAN *name*或VLAN *編號*定義屬性**81**。**注意**：如果使用VLAN *name*，則應該與交換器中設定的名稱完全相同。



附註： 有關這些IETF屬性的詳細資訊，請參閱RFC 2868:適用於通道通訊協定支援的RADIUS屬性 。**注意：**在ACS伺服器的初始配置中，IETF RADIUS屬性可能無法顯示在使用者設**置中**。要在使用者配置螢幕中啟用IETF屬性，請選擇**Interface configuration > RADIUS(IETF)**。 然後，在「使用者」和「組」列中檢查屬性**64**、**65**和**81**。**注意：**如果未定義IETF屬性**81**，並且埠是處於訪問模式的交換機埠，則客戶端可以分配到該埠的訪問VLAN。如果您已為動態VLAN分配定義了屬性**81**，並且該埠是處於接入模式的交換機埠，則需要在交換機上發出命令**aaa authorization network default group radius**。此命令將連線埠指定給RADIUS伺服器提供的VLAN。否則，802.1x會在使用者驗證之後將連線埠移至AUTHORIZED狀態；但埠仍位於埠的預設VLAN中，連線可能會失敗。如果您已定義屬性**81**，但您已將連線埠設定為路由連線埠，則會發生存取阻絕。系統會顯示以下錯誤消息：

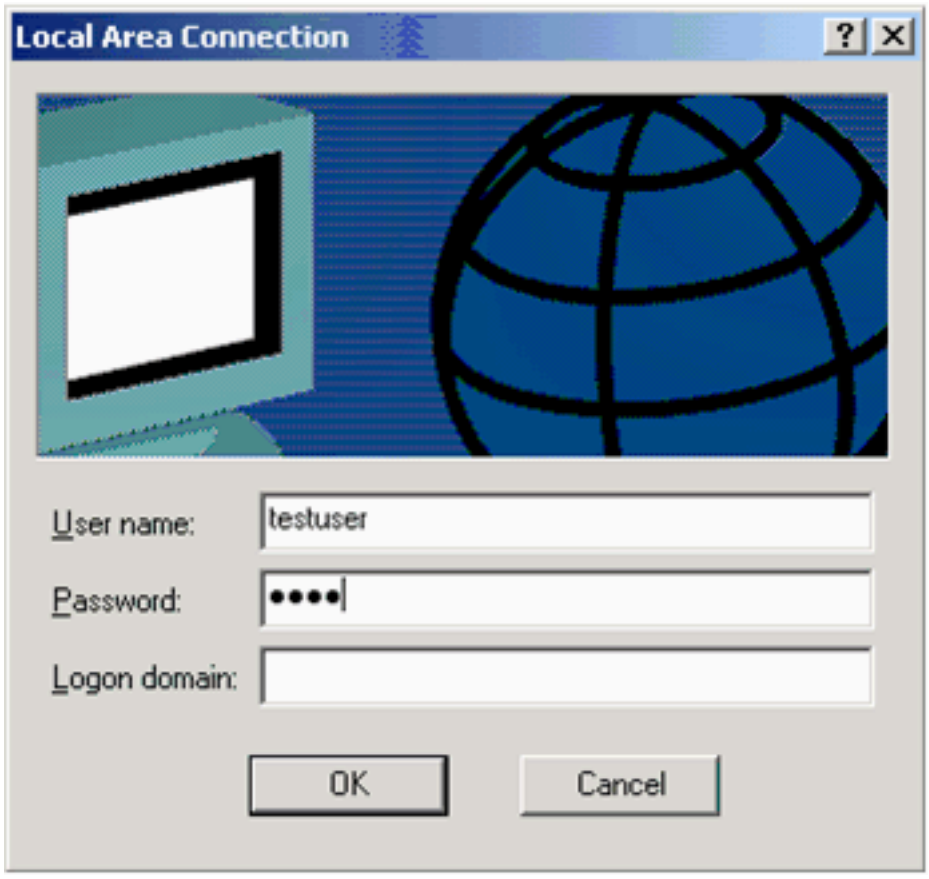
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

將PC客戶端配置為使用802.1x身份驗證

此範例特定於Microsoft Windows XP Extensible Authentication Protocol(EAP)over LAN(EAPOL)使用者端：

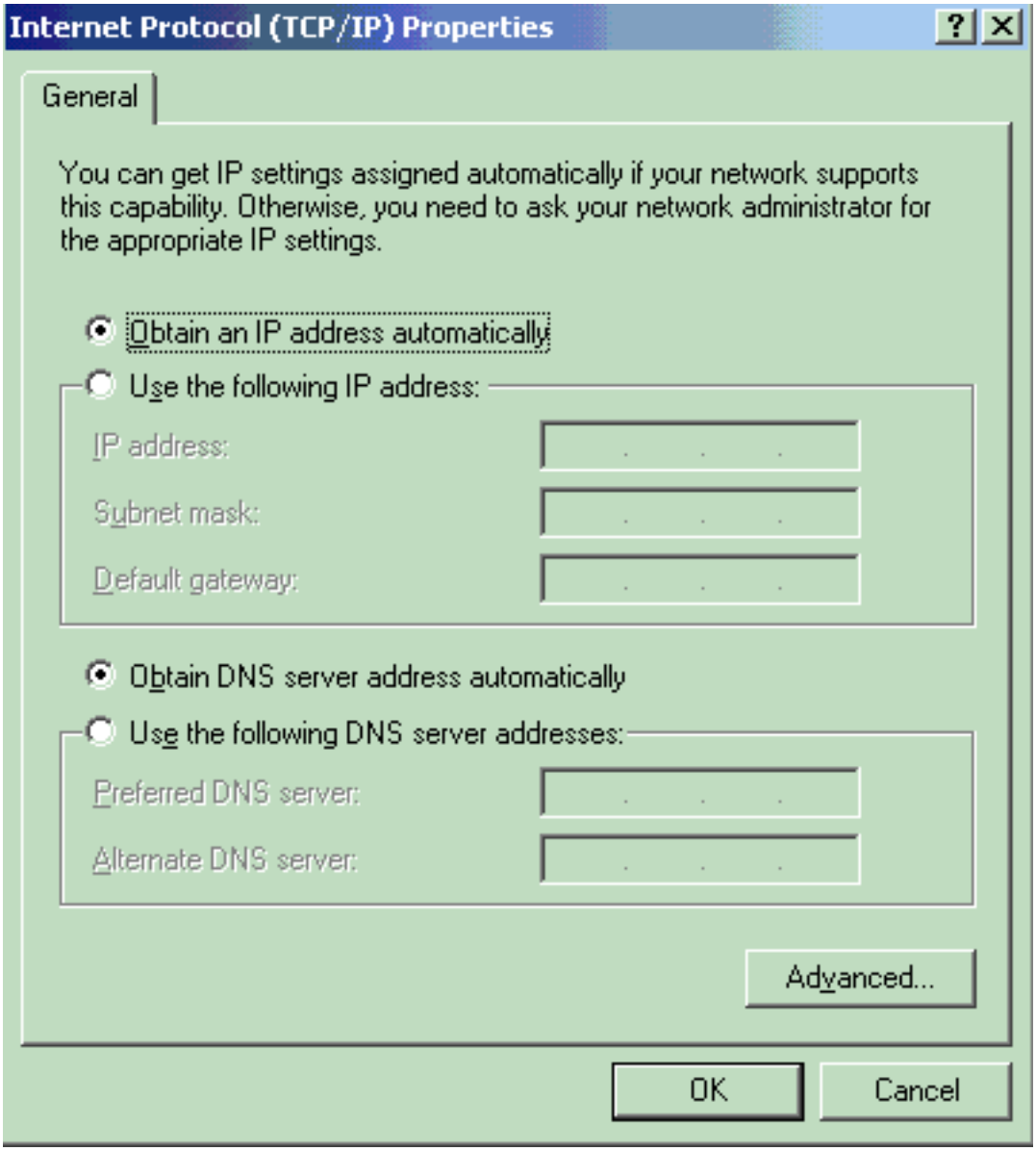
1. 選擇**Start > Control Panel > Network Connections**，然後按一下右鍵**Local Area Connection**並選擇**Properties**。
2. 在「General」頁籤下連線時，選中**Show icon in notification area**。
3. 在Authentication頁籤下，選中**Enable IEEE 802.1x authentication for this network**。
4. 將EAP型別設定為**MD5-Challenge**，如以下示例所示

:



完成這些步驟，配置客戶端以從DHCP伺服器獲取IP地址。

1. 選擇**Start > Control Panel > Network Connections**，然後按一下右鍵**Local Area Connection**並選擇**Properties**。
2. 在General頁籤下，按一下**Internet Protocol(TCP/IP)**，然後按一下**Properties**。
3. 選擇**Obtain an IP address automatically**。



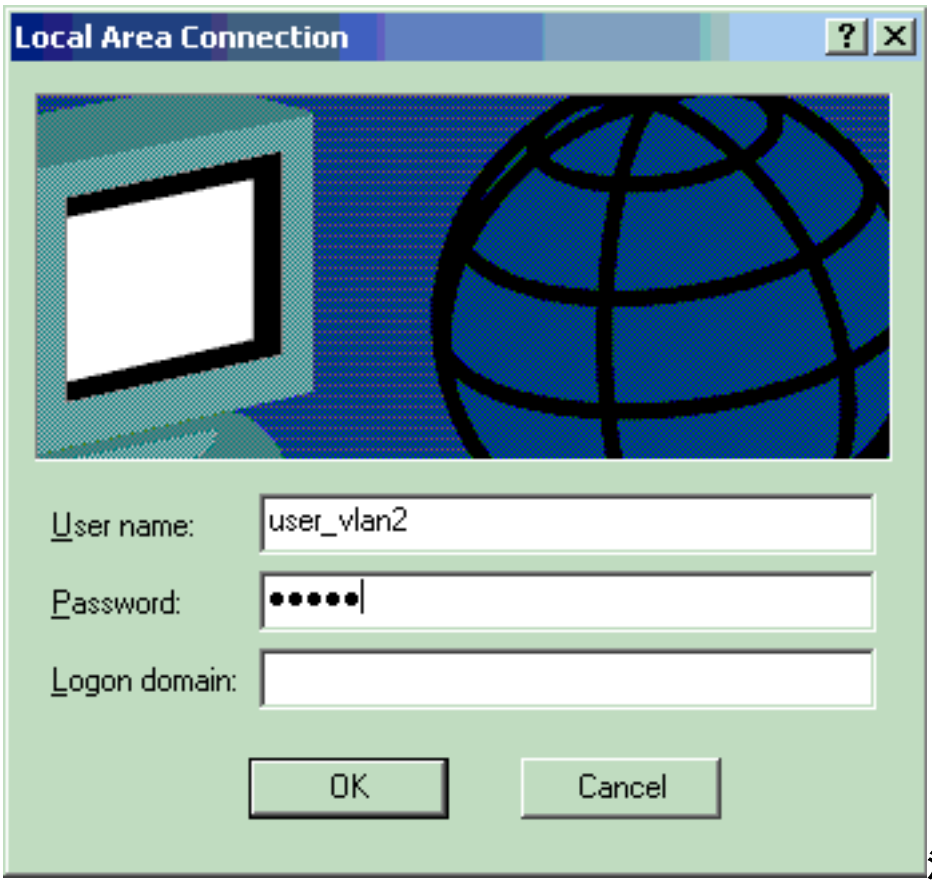
驗證

PC客戶端

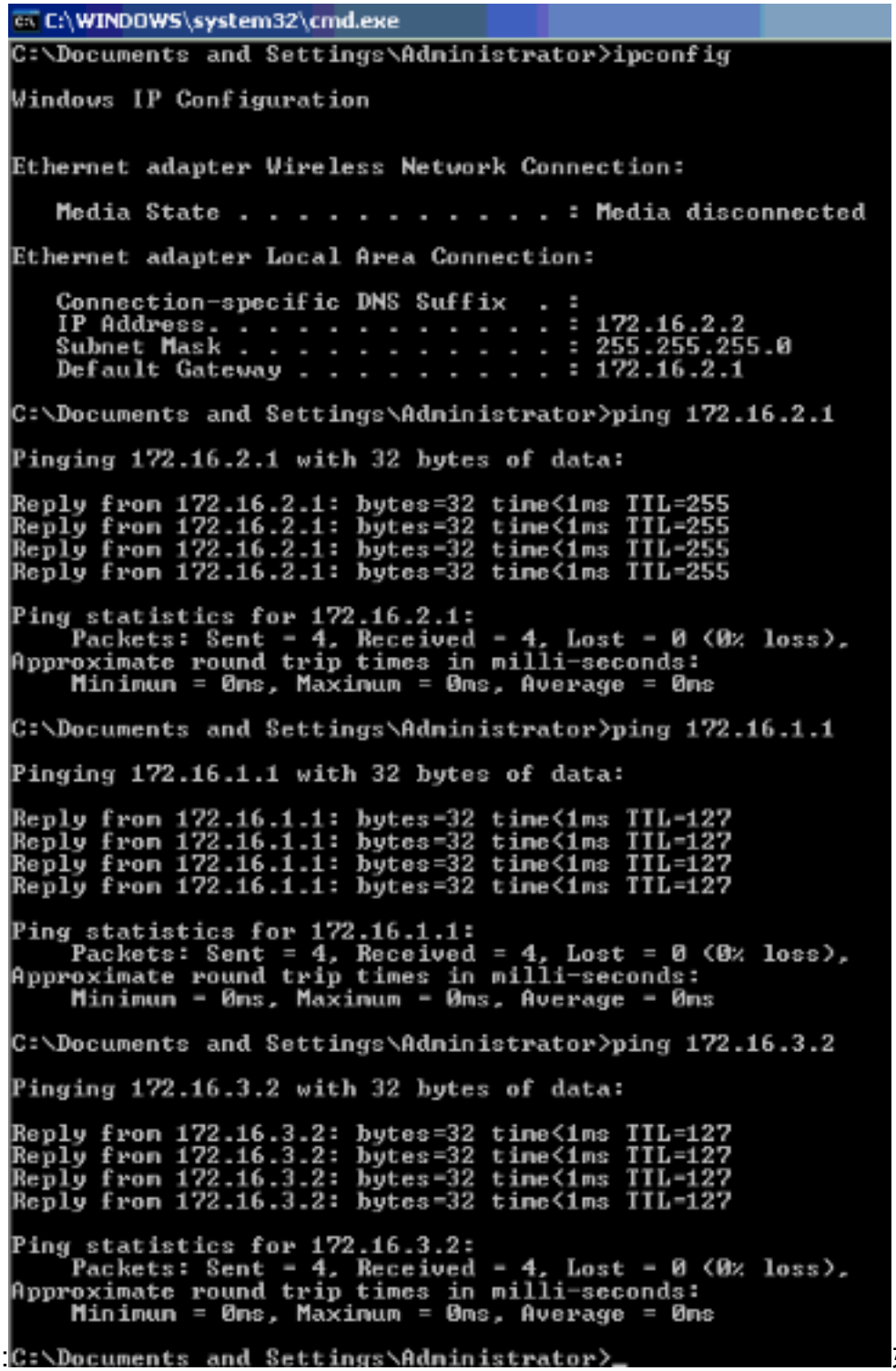
如果配置已正確完成，PC客戶端將顯示彈出提示以輸入使用者名稱和密碼。

1. 按一下提示，此示例顯示

：將顯示使用者名稱和密碼輸入視窗。

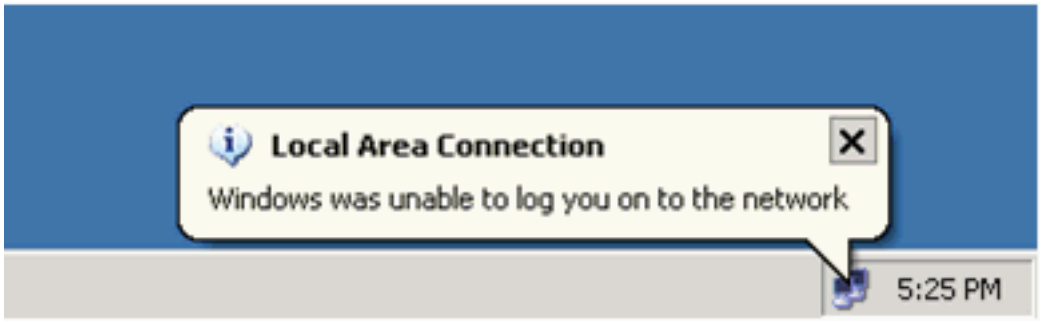


2. 輸入使用者名稱和密碼。**注意：**在PC 1和2中輸入VLAN 2使用者憑證，在PC 3和4中輸入VLAN 3使用者憑證。
3. 如果未顯示錯誤訊息，請透過常見方法(例如透過存取網路資源和ping)驗證連線。此輸出來自PC 1，顯示對PC 4成功



ping:如果出現此錯誤，請驗證使用者名稱和密碼是否正確

:



Catalyst 6500

如果密碼和使用者名稱正確，請驗證交換機上的802.1x埠狀態。

1. 尋找表示AUTHORIZED的連線埠狀態。

```
Cat6K#show dot1x

Sysauthcontrol                  = Enabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both


Cat6K#show dot1x interface fastEthernet 3/2
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/4
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/1
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
PortControl       = Force Authorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

驗證成功後確認VLAN狀態。

```
Cat6K#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa3/6, Fa3/7, Fa3/8, Fa3/9,
                                                Fa3/10, Fa3/11, Fa3/12, Fa3/13,
                                                Fa3/14, Fa3/15, Fa3/16, Fa3/17,
                                                Fa3/18, Fa3/19, Fa3/20, Fa3/21,
                                                Fa3/22, Fa3/23, Fa3/24, Fa3/25,
                                                Fa3/26, Fa3/27, Fa3/28, Fa3/29,
                                                Fa3/30, Fa3/31, Fa3/32, Fa3/33,
```

```
                                                Fa3/34, Fa3/35, Fa3/36, Fa3/37,
                                                Fa3/38, Fa3/39, Fa3/40, Fa3/41,
                                                Fa3/42, Fa3/43, Fa3/44, Fa3/45,
                                                Fa3/46, Fa3/47, Fa3/48
2    VLAN2                          active     Fa3/2, Fa3/3
3    VLAN3                          active     Fa3/4, Fa3/5
10   RADIUS_SERVER                  active     Fa3/1
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
!--- Output suppressed.
```

2. 身份驗證成功後，從驗證DHCP繫結狀態。

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.2.2       0100.1636.3333.9c       Mar 04 2007 06:35 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Mar 04 2007 06:43 AM    Automatic
172.16.3.2       0100.145e.945f.99       Mar 04 2007 06:50 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Mar 04 2007 06:57 AM    Automatic
```

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

疑難排解

收集以下debug命令的輸出，以排解疑難問題：

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

- debug dot1x events — 啟用由dot1x事件標誌保護的列印語句的調試。

```
Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
   is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
    this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
   this id 13
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
   id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
```

```
   will pick up any pending requests from the queue
Cat6K#
Cat6K#
!--- Debug output for PC 3 connected to Fa3/4. 00:19:58: dot1x-ev:Got a Request from SP to
send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0
00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 00:19:58: dot1x-
ev:The Interface on which we got this AAA
   Request is FastEthernet3/4
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
```

- **debug radius** — 顯示與RADIUS關聯的資訊。

```
Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-
login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit
FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6
AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36:
Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18
CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79
00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18
172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80
18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104
00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36:
```

```
Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18
11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# !--- Debug
output for PC 3 connected to Fa3/4. 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11
172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute
61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58:
Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from
id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58:
Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

相關資訊

- 運行CatOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證配置示例
- 在Cisco Catalyst交換機環境中部署適用於Windows NT/2000伺服器的Cisco Secure ACS的准則
- RFC 2868:適用於通道通訊協定支援的RADIUS屬性
- 配置IEEE 802.1X基於埠的身份驗證
- LAN 產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems