

運行CatOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[配置Catalyst交換機以進行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](#)

[驗證](#)

[PC客戶端](#)

[Catalyst 6500](#)

[疑難排解](#)

[相關資訊](#)

[簡介](#)

本文說明如何在混合模式下運行的Catalyst 6500/6000(Supervisor Engine上使用CatOS , MSFC上使用Cisco IOS®軟體)和遠端驗證撥入使用者服務(RADIUS)伺服器上設定IEEE 802.1x，以進行驗證和VLAN分配。

[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CatOS軟體版本8.5(6)和MSFC上執行Cisco IOS軟體版本12.2(18)SXF的Catalyst 6500**注意**：您需要使用CatOS 6.2版或更高版本來支援802.1x基於埠的身份驗證。**注意**：在軟體版本7.2(2)之前，一旦對802.1x主機進行驗證，它就會加入已設定NVRAM的VLAN。透過軟體版本7.2(2)和更新版本，經過驗證後，802.1x主機可以從RADIUS伺服器接收其VLAN指派。
- 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

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

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訪問控制僅允許通過裝置所連線的埠的LAN可擴展身份驗證協定(EAP)流量(EAPOL)。驗證成功後，正常流量可以通過該連線埠。

設定

本節提供用於設定本檔案中所述802.1x功能的資訊。

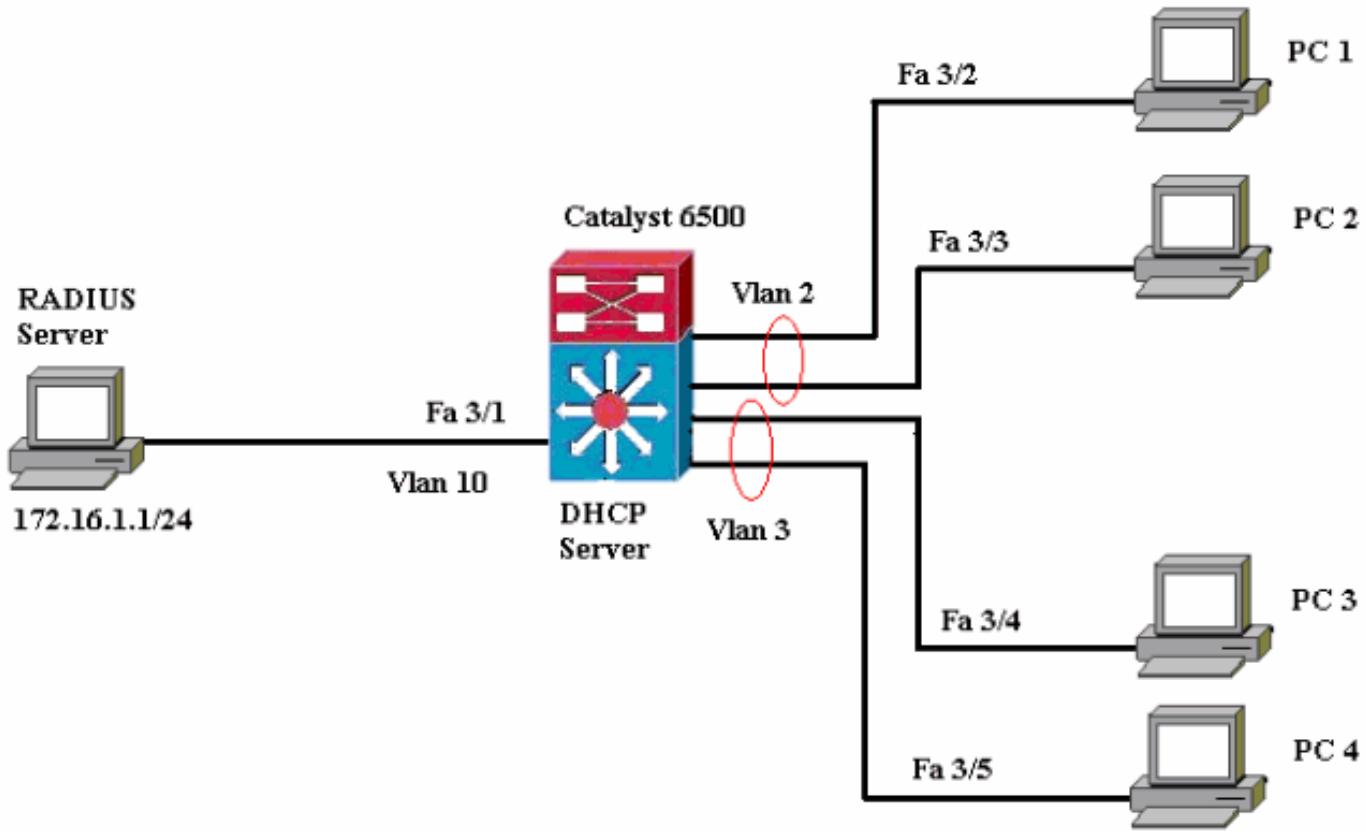
註：使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

此配置需要執行以下步驟：

- [配置Catalyst交換機以進行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份，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），從使用者端要求身分資訊，使用RADIUS伺服器驗證該資訊，以及將回應轉送到使用者端。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PC 2將在VLAN 2中使用相同的登入憑據。同樣，PC 3和PC 4將使用VLAN 3的登入憑據。PC客戶端配置為從DHCP伺服器獲取IP地址。**註意**：在此配置中，任何未通過身份驗證的客戶端或任何連線到交換機的不支援802.1x的客戶端都會被拒絕網路訪問，方法是使用身份驗證失敗和訪客VLAN功能將它們移到未使用的VLAN（VLAN 4或5）。

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：

- 在快速乙太網埠上啟用802.1x身份驗證和相關功能。
- 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身份驗證的準則，請參閱[身份驗證配置準則](#)。

注意：確保RADIUS伺服器始終在授權埠後連線。

Catalyst 6500

```
Console (enable) set system name Cat6K
System name set.
!--- Sets the hostname for the switch. Cat6K> (enable)
set localuser user admin password cisco
Added local user admin.
Cat6K> (enable) set localuser authentication enable
LocalUser authentication enabled
!--- Uses local user authentication to access the
switch. Cat6K> (enable) set vtp domain cisco
VTP domain cisco modified
!--- Domain name must be configured for VLAN
configuration. Cat6K> (enable) set vlan 2 name VLAN2
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 2 configuration successful
!--- VLAN should be existing in the switch !--- for a
successful authentication. Cat6K> (enable) set vlan 3
name VLAN3
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
!--- VLAN names will be used in RADIUS server for VLAN
assignment. Cat6K> (enable) set vlan 4 name
AUTHFAIL_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful
!--- A VLAN for non-802.1x capable hosts. Cat6K>
(enable) set vlan 5 name GUEST_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful
!--- A VLAN for failed authentication hosts. Cat6K>
(enable) set vlan 10 name RADIUS_SERVER
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 10 configuration successful
!--- This is a dedicated VLAN for the RADIUS Server.
Cat6K> (enable) set interface sc0 10 172.16.1.2
255.255.255.0
Interface sc0 vlan set, IP address and netmask set.
!--- Note: 802.1x authentication always uses the !---
sc0 interface as the identifier for the authenticator !-
-- when communicating with the RADIUS server.

Cat6K> (enable) set vlan 10 3/1
VLAN 10 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
10 3/1
!--- Assigns port connecting to RADIUS server to VLAN
10. Cat6K> (enable) set radius server 172.16.1.1 primary
172.16.1.1 with auth-port 1812 acct-port 1813
added to radius server table as primary server.
!--- Sets the IP address of the RADIUS server. Cat6K>
(enable) set radius key cisco
Radius key set to cisco
!--- The key must match the key used on the RADIUS
server. Cat6K> (enable) set dot1x system-auth-control
enable
```

```
dot1x system-auth-control enabled.  
Configured RADIUS servers will be used for dot1x  
authentication.  
!--- Globally enables 802.1x. !--- You must specify at  
least one RADIUS server before !--- you can enable  
802.1x authentication on the switch. Cat6K> (enable) set  
port dot1x 3/2-48 port-control auto  
Port 3/2-48 dot1x port-control is set to auto.  
Trunking disabled for port 3/2-48 due to Dot1x feature.  
Spantree port fast start option enabled for port 3/2-48.  
!--- Enables 802.1x on all FastEthernet ports. !--- This  
disables trunking and enables portfast automatically.  
Cat6K> (enable) set port dot1x 3/2-48 auth-fail-vlan 4  
Port 3/2-48 Auth Fail Vlan is set to 4  
!--- Ports will be put in VLAN 4 after three !--- failed  
authentication attempts. Cat6K> (enable) set port dot1x  
3/2-48 guest-vlan 5  
Ports 3/2-48 Guest Vlan is set to 5  
!--- Any non-802.1x capable host connecting or 802.1x !-  
-- capable host failing to respond to the username and  
password !--- authentication requests from the  
Authenticator is placed in the !--- guest VLAN after 60  
seconds. !--- Note: An authentication failure VLAN is  
independent !--- of the guest VLAN. However, the guest  
VLAN can be the same !--- VLAN as the authentication  
failure VLAN. If you do not want to !--- differentiate  
between the non-802.1x capable hosts and the !---  
authentication failed hosts, you can configure both  
hosts to !--- the same VLAN (either a guest VLAN or an  
authentication failure VLAN). !--- For more information,  
refer to !--- Understanding How 802.1x Authentication  
for the Guest VLAN Works. Cat6K> (enable) switch console  
Trying Router-16...  
Connected to Router-16.  
Type ^C^C^C to switch back...  
!--- Transfers control to the routing module (MSFC).  
Router>enable  
Router#conf t  
Enter configuration commands, one per line. End with  
CNTL/Z.  
Router(config)#interface vlan 10  
Router(config-if)#ip address 172.16.1.3 255.255.255.0  
!--- This is used as the gateway address in RADIUS  
server. Router(config-if)#no shut  
Router(config-if)#interface vlan 2  
Router(config-if)#ip address 172.16.2.1 255.255.255.0  
Router(config-if)#no shut  
!--- This is the gateway address for clients in VLAN 2.  
Router(config-if)#interface vlan 3  
Router(config-if)#ip address 172.16.3.1 255.255.255.0  
Router(config-if)#no shut  
!--- This is the gateway address for clients in VLAN 3.  
Router(config-if)#exit  
Router(config)#ip dhcp pool vlan2_clients  
Router(dhcp-config)#network 172.16.2.0 255.255.255.0  
Router(dhcp-config)#default-router 172.16.2.1  
!--- This pool assigns ip address for clients in VLAN 2.  
Router(dhcp-config)#ip dhcp pool vlan3_clients  
Router(dhcp-config)#network 172.16.3.0 255.255.255.0  
Router(dhcp-config)#default-router 172.16.3.1  
!--- This pool assigns ip address for clients in VLAN 3.  
Router(dhcp-config)#exit  
Router(config)#ip dhcp excluded-address 172.16.2.1  
Router(config)#ip dhcp excluded-address 172.16.3.1
```

```

!--- In order to go back to the Switching module, !---
enter Ctrl-C three times. Router# Router#^C Cat6K>
(enable) Cat6K> (enable) show vlan VLAN Name Status
IfIndex Mod/Ports, Vlans -----
----- 1 default
active 6 2/1-2

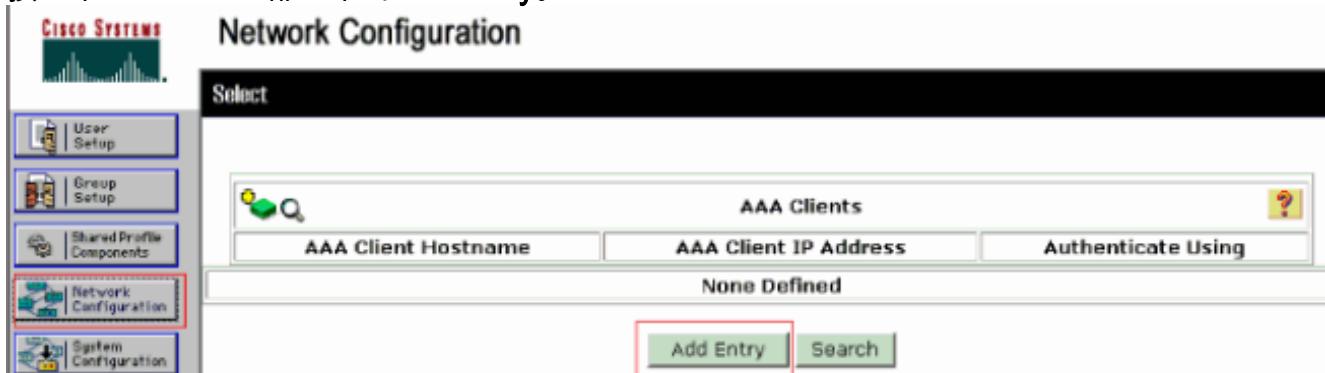
3/2-48
2 VLAN2 active 83
3 VLAN3 active 84
4 AUTHFAIL_VLAN active 85
5 GUEST_VLAN active 86
10 RADIUS_SERVER active 87
3/1
1002 fddi-default active 78
1003 token-ring-default active 81
1004 fddinet-default active 79
1005 trnet-default active 80
!--- Output suppressed. !--- All active ports will be in
VLAN 1 (except 3/1) before authentication. Cat6K>
(enable) show dot1x
PAE Capability Authenticator Only
Protocol Version 1
system-auth-control enabled
max-req 2
quiet-period 60 seconds
re-authperiod 3600 seconds
server-timeout 30 seconds
shutdown-timeout 300 seconds
supp-timeout 30 seconds
tx-period 30 seconds
!--- Verifies dot1x status before authentication. Cat6K>
(enable)

```

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：

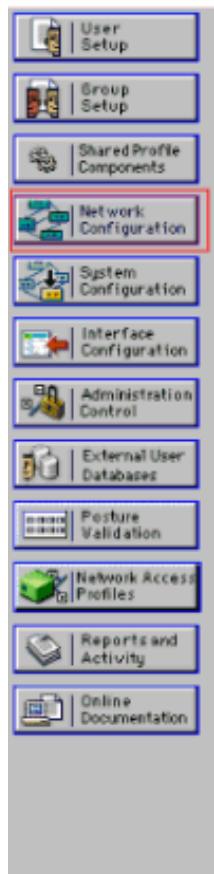
1. 要配置AAA客戶端，請在ACS管理視窗中按一下**Network Configuration**。
2. 按一下AAA clients部分下的**Add Entry**。



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=管理介面(sc0)交換機(172.16.1.2)的IP地址。共用金鑰=在交換機(cisco)上配置的Radius金鑰。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



Network Configuration



Add AAA Client

AAA Client Hostname

Cat6K

AAA Client IP Address

172.16.1.2

Shared Secret

cisco

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

ASCII Hexadecimal

Authenticate Using

RADIUS (IETF)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit

Submit + Apply

Cancel

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user_vlan2，並為連線到VLAN 3的客戶端建立另一個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，請完成相同的過程。

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。

CISCO SYSTEMS

User Setup

Select

User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles

User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			

CISCO SYSTEMS

User Setup

Edit

User: **user_vlan2 (New User)**

Account Disabled

Supplementary User Info

Real Name	<input type="text" value="user_vlan2"/>
Description	<input type="text" value="client in VLAN 2"/>

User Setup

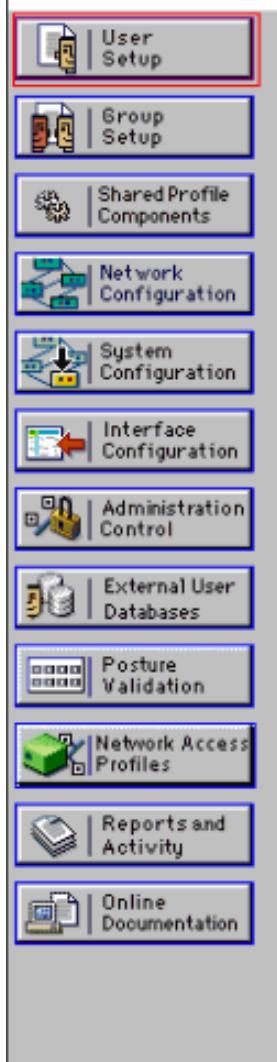
Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

- 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。

User Setup



Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Default Group

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

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Values的Tags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名稱定義屬性81。**注意：**VLAN name應與交換機中配置的名稱完全相同。**注意**：CatOS不支援基於VLAN編號的VLAN分配。

User Setup

Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes

[006] Service-Type

[064] Tunnel-Type
Tag 1 Value VLAN

[065] Tunnel-Medium-Type
Tag 1 Value 802

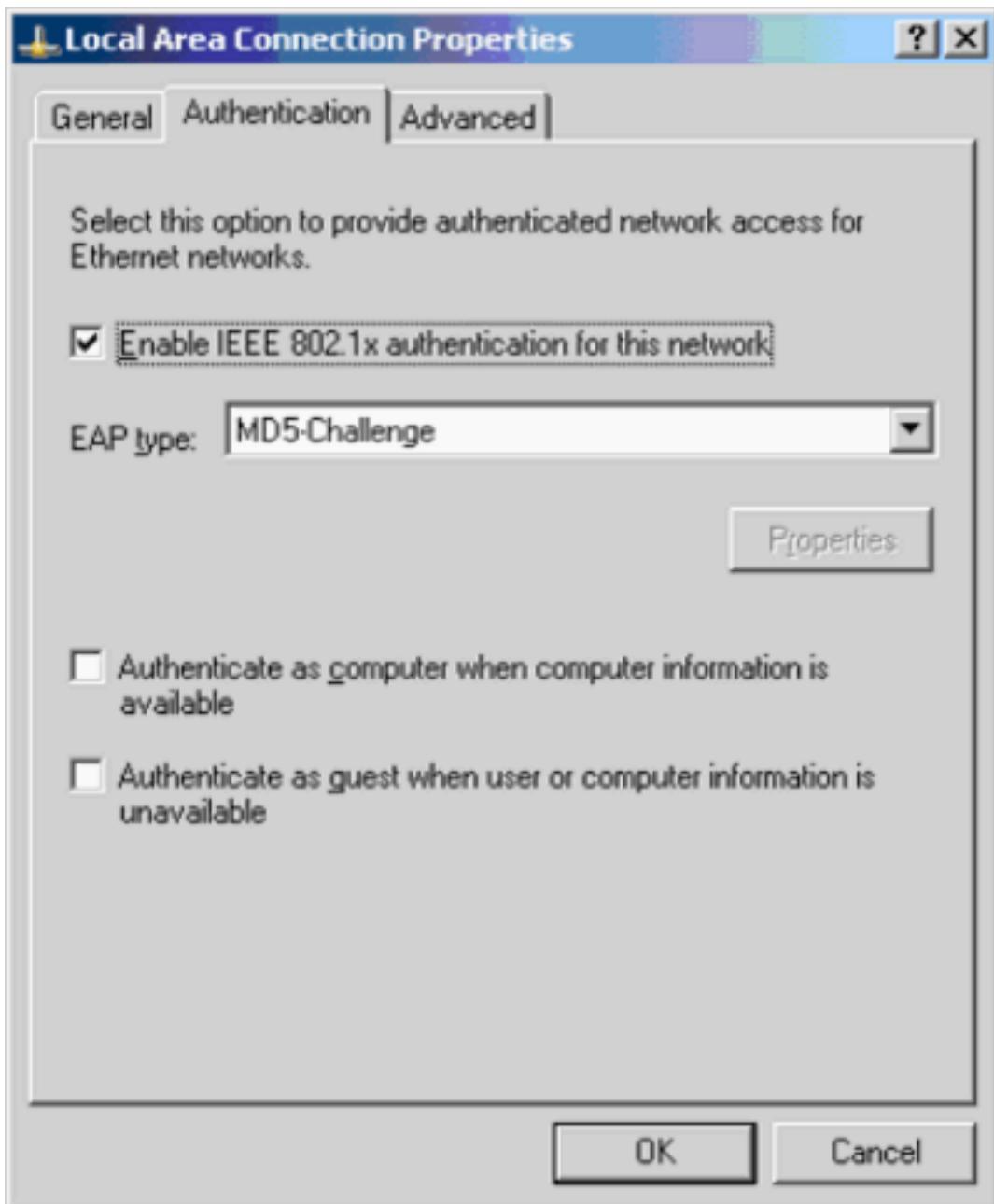
[081] Tunnel-Private-Group-ID
Tag 1 Value VLAN2

請參閱[RFC 2868:適用於通道通訊協定支援的RADIUS屬性](#)，以瞭解更多有關這些IETF屬性的資訊。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。依序選擇「Interface configuration > RADIUS(IETF)」，以在使用者組態畫面中啟用IETF屬性。然後，在「使用者」和「組」列中檢查屬性64、65和81。

將PC客戶端配置為使用802.1x身份驗證

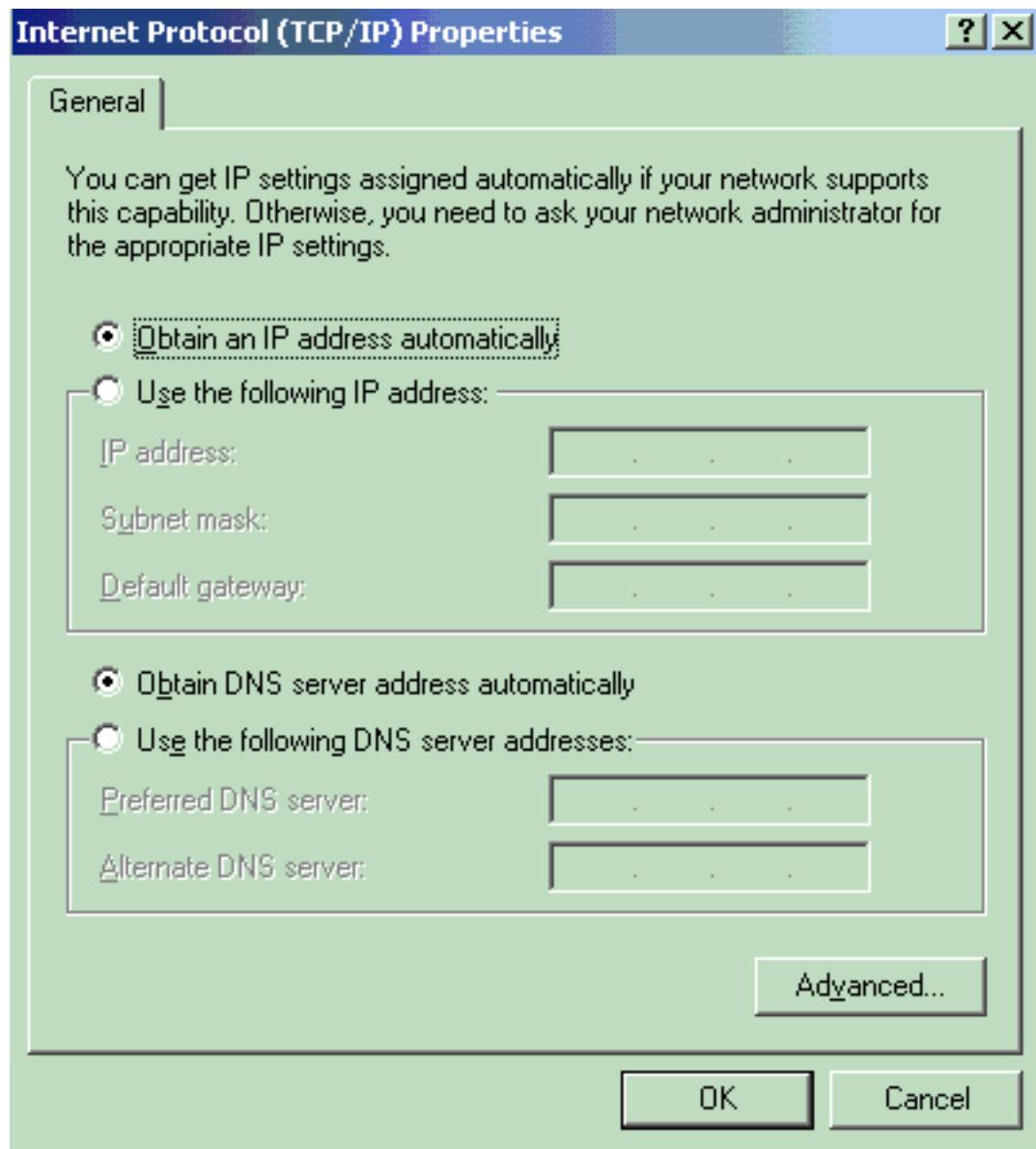
此範例特定於Microsoft Windows XP Extensible Authentication Protocol(EAP)over LAN(EAPOL)使用者端。請完成以下步驟：

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



完成以下步驟，將客戶端配置為從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

使用本節內容，確認您的組態是否正常運作。

[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。

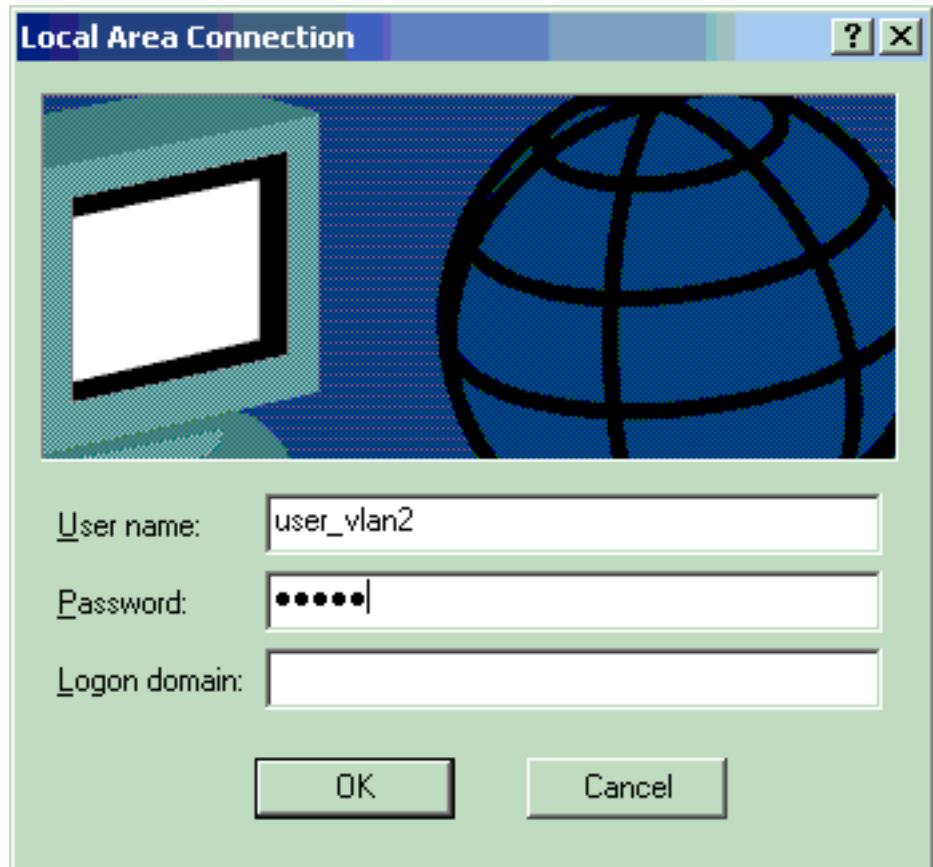
PC客戶端

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指令驗證連線。這是PC 1的輸出，其中顯示對PC 4的ping操作成功

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Wireless Network Connection:
    Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . :
    IP Address . . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\Documents and Settings\Administrator>ping 172.16.2.1
Pinging 172.16.2.1 with 32 bytes of data:
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.1.1
Pinging 172.16.1.1 with 32 bytes of data:
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

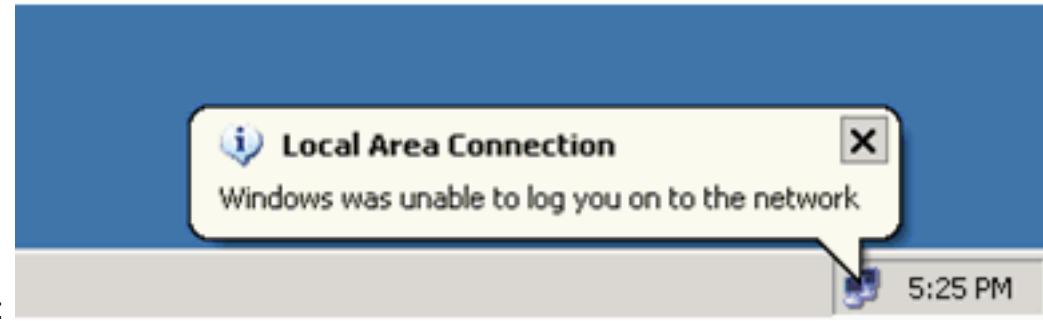
Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2
Pinging 172.16.3.2 with 32 bytes of data:
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

: C:\Documents and Settings\Administrator>

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> (enable) show port dot1x 3/1-5
```

Port	Auth-State	BEnd-State	Port-Control	Port-Status
3/1	force-authorized	idle	force-authorized	authorized
	<i>!--- This is the port to which RADIUS server is connected.</i>			
auto		authorized		
3/3	authenticated	idle	auto	authorized
3/4	authenticated	idle	auto	authorized
3/5	authenticated	idle	auto	authorized

Port	Port-Mode	Re-authentication	Shutdown-timeout
3/1	SingleAuth	disabled	disabled
3/2	SingleAuth	disabled	disabled
3/3	SingleAuth	disabled	disabled
3/4	SingleAuth	disabled	disabled
3/5	SingleAuth	disabled	disabled

驗證成功後確認VLAN狀態。

```
Cat6K> (enable) show vlan
```

VLAN	Name	Status	IfIndex	Mod/Ports, Vlans
1	default	active	6	2/1-2 3/6-48
2	VLAN2	active	83	3/2-3
3	VLAN3	active	84	3/4-5
4	AUTHFAIL_VLAN	active	85	
5	GUEST_VLAN	active	86	
10	RADIUS_SERVER	active	87	3/1
1002	fddi-default	active	78	
1003	token-ring-default	active	81	
1004	fddinet-default	active	79	
1005	trnet-default	active	80	

!--- Output suppressed.

2. 在身份驗證成功後，從路由模組(MSFC)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	Feb 14 2007 03:00 AM	Automatic
172.16.2.3	0100.166F.3CA3.42	Feb 14 2007 03:03 AM	Automatic
172.16.3.2	0100.145e.945f.99	Feb 14 2007 03:05 AM	Automatic
172.16.3.3	0100.1185.8D9A.F9	Feb 14 2007 03:07 AM	Automatic

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [運行Cisco IOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證示例](#)
- [Catalyst交換和ACS部署指南](#)
- [RFC 2868:適用於通道通訊協定支援的RADIUS屬性](#)
- [配置802.1x身份驗證](#)
- [LAN 產品支援頁面](#)
- [LAN 交換支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)