

# Cisco Catalyst第3層固定配置交換機上的IEEE 802.1x多域身份驗證配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[為Catalyst交換機配置802.1x多域身份驗證](#)

[設定RADIUS伺服器](#)

[將PC客戶端配置為使用802.1x身份驗證](#)

[將IP電話配置為使用802.1x身份驗證](#)

[驗證](#)

[PC客戶端](#)

[IP電話](#)

[第3層交換機](#)

[疑難排解](#)

[IP電話身份驗證失敗](#)

[相關資訊](#)

## 簡介

多域身份驗證允許IP電話和PC在同一交換機埠上進行身份驗證，同時將它們放在適當的語音和資料VLAN上。本檔案將說明如何在Cisco Catalyst第3層固定組態交換器上設定IEEE 802.1x多網域驗證(MDA)。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- [RADIUS 如何運作？](#)
- [Catalyst交換和ACS部署指南](#)
- [思科安全訪問控制伺服器4.1使用手冊](#)

- [Cisco Unified IP電話概述](#)

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS®軟體版本12.2(37)SE1的Cisco Catalyst 3560系列交換器**注意**：多域身份驗證支援僅適用於Cisco IOS軟體版本12.2(35)SE及更高版本。
- 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。
- 採用SCCP韌體版本8.2(1)的Cisco整合IP電話7970G
- 採用SCCP韌體版本8.2(2)的Cisco整合IP電話7961G
- 媒體融合伺服器(MCS)，搭載思科整合通訊管理員(Cisco CallManager)4.1(3)sr2

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。

## 相關產品

此組態也可以用於以下硬體：

- Cisco Catalyst 3560-E系列交換器
- Cisco Catalyst 3750系列交換器
- Cisco Catalyst 3750-E系列交換器

**註**：Cisco Catalyst 3550系列交換機不支援802.1x多域身份驗證。

## 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。

802.1x由三個主要元件組成。每個埠稱為埠訪問實體(PAE)。

- 請求方 — 請求網路訪問的客戶端裝置，例如IP電話和連線的PC
- 驗證器 — 方便請求方授權請求的網路裝置，例如Cisco Catalyst 3560
- 驗證伺服器 — 遠端驗證撥入使用者伺服器(RADIUS)，提供驗證服務，例如思科安全存取控制伺服器

Cisco Unified IP電話還包含802.1X請求方。此請求方允許網路管理員控制IP電話與LAN交換機埠的連通性。IP電話802.1X請求方的初始版本為802.1X身份驗證實施了EAP-MD5選項。在多域配置中，IP電話和連線的PC必須根據使用者名稱和密碼的說明獨立請求訪問網路。驗證器裝置可以要求來

自RADIUS的資訊，稱為屬性。屬性指定其他授權資訊，例如請求方是否允許訪問特定VLAN。這些屬性可以是供應商特定的。思科使用RADIUS屬性cisco-av-pair告知驗證器(Cisco Catalyst 3560)語音VLAN上允許請求者 ( IP電話 )。

## 設定

本節提供用於設定本檔案中所述802.1x多網域驗證功能的資訊。

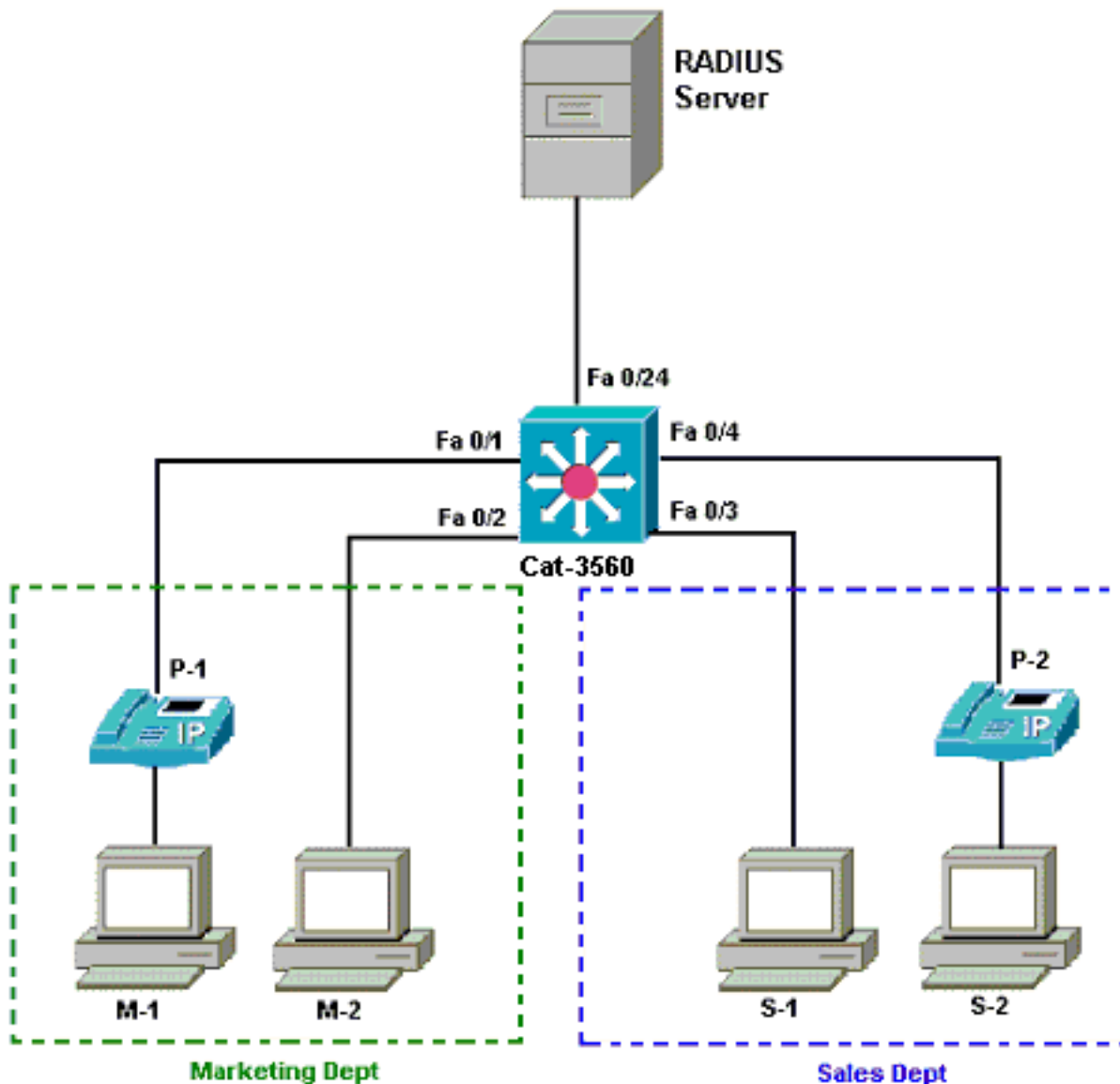
此配置需要執行以下步驟：

- [為Catalyst交換機配置802.1x多域身份驗證。](#)
- [設定RADIUS伺服器。](#)
- [將PC客戶端配置為使用802.1x身份驗證。](#)
- [將IP電話配置為使用802.1x身份驗證。](#)

註：使用[Command Lookup Tool](#)(僅限註冊客戶)可以查詢有關本文檔中使用的命令的詳細資訊。

## 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。在這裡，Cisco ACS安裝在媒體融合伺服器(MCS)上並配置為用於身份驗證和VLAN分配。MCS也是IP電話的TFTP伺服器和Cisco Unified Communications Manager(Cisco CallManager)。
- 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 3560交換機也被配置為DHCP伺服器。動態主機配置協定(DHCP)的802.1x身份驗證支援允許DHCP伺服器將IP地址分配給不同的終端使用者類別。為此，它將經過身份驗證的使用者身份新增到DHCP發現過程中。埠FastEthernet 0/1和0/4是為802.1x多域身份驗證配置的唯一埠。埠FastEthernet 0/2和0/3處於預設的802.1x單主機模式。埠FastEthernet 0/24連線到RADIUS伺服器。**注意：**如果使用外部DHCP伺服器，請不要忘記在客戶端所在的SVI(vlan)介面(指向DHCP伺服器)上新增**ip helper-address**命令。
- 客戶端 — 這些裝置(例如IP電話或工作站)請求訪問LAN和交換機服務並響應來自交換機的請求。在這裡，客戶端配置為從DHCP伺服器獲取IP地址。裝置M-1、M-2、S-1和S-2是請求訪問網路的工作站客戶端。P-1和P-2是請求訪問網路的IP電話客戶端。M-1、M-2和P-1是行銷部門的客戶裝置。S-1、S-2和P-2是銷售部門的客戶端裝置。IP電話P-1和P-2配置為位於同一個語音VLAN(VLAN 3)中。成功驗證後，工作站M-1和M-2配置為位於同一個資料VLAN(VLAN 4)中。在身份驗證成功後，工作站S-1和S-2也配置為位於同一個資料VLAN(VLAN 5)中。**注意：**只能對資料裝置使用RADIUS伺服器的動態VLAN分配。

## 為Catalyst交換機配置802.1x多域身份驗證

此交換機配置示例包括：

- 如何在交換機埠上啟用802.1x多域身份驗證
- RADIUS伺服器相關組態
- IP地址分配的DHCP伺服器配置
- 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MDA的指南的詳細資訊，請參閱[使用多域身份驗證](#)。

**注意：**確保RADIUS伺服器始終在授權埠後連線。

**注意：**此處僅顯示相關配置。

### Cat-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Sets the hostname for the switch. Cat-
3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- VLAN should already exist in the switch for a
successful authentication. Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
```

```

Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for the RADIUS Server.
Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for IP Phone clients in
VLAN 3. Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
4. Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
5. Cat-3560(config-if)#exit
Cat-3560(config)#ip routing
!--- Enables IP routing for interVLAN routing. Cat-
3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- This is a dedicated VLAN for the RADIUS server.
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- You must configure the voice VLAN for the IP phone
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
device fails authorization.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Enables IEEE 802.1x authentication on the port.
Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Allow both a host and a voice device to be !---
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- The guest VLAN and restricted VLAN features only
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
!--- Enables periodic re-authentication of the client.
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Set the number of seconds between re-authentication
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
!--- Specifies the number of authentication attempts to
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- By default a 802.1x authorized port allows only a
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60

```

```

Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- This pool assigns ip address for IP Phones. !---
Option 150 is for the TFTP server.
Cat-3560(dhcp-config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing Dept.
Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- This pool assigns ip address for PC clients in
Sales Dept.
Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
!--- Method list should be default. Otherwise dot1x does
not work.
Cat-3560(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS.
Cat-3560(config)#radius-server host
172.16.2.201 key CisCo123
!--- The key must match the key used on the RADIUS
server.
Cat-3560(config)#dot1x system-auth-control
!--- Globally enables 802.1x.
Cat-3560(config)#interface
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Gi0/1, Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1, Fa0/4
4 MARKETING	active	
5 SALES	active	
6 GUEST_and_AUTHFAIL	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

註：使用[Command Lookup Tool](#)(僅限註冊客戶)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172.16.2.201/24。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**。

**Network Configuration**

Select

**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

**Add Entry** Search

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
CCM-4	172.16.2.201	CiscoSecure ACS

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(Cat-3560)。AAA客戶端IP地址=交換機的管理介面IP地址(172.16.2.1)。共用金鑰=交換機上配置的RADIUS金鑰(CisCo123)。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。使用=RADIUS(Cisco IOS/PIX 6.0)進行身份驗證。注意：Cisco Attribute-Value(AV)pair attribute在該選項下可用。
4. 按一下「**Submit + Apply**」以使這些變更生效，如下例所示：



**CISCO SYSTEMS** Network Configuration

## Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

**RADIUS Key Wrap**

Key Encryption Key

Message Authenticator Code Key

Key Input Format       ASCII  Hexadecimal

Authenticate Using

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

### 組設定

請參閱下表以設定RADIUS伺服器進行驗證。

裝置	部門	群組	使用者	密碼	VLAN	DH CP 池
M-1	市場行銷	市場行銷	市場經理	Cisco	市場行銷	市場行銷
M-2	市場行銷	市場行銷	市場員工	MScisco	市場行銷	市場行銷
S-2	銷售	銷售	銷售經理	SMcisco	銷售	銷售
S-1	銷售	銷售	銷售人員	思科	銷售	銷售

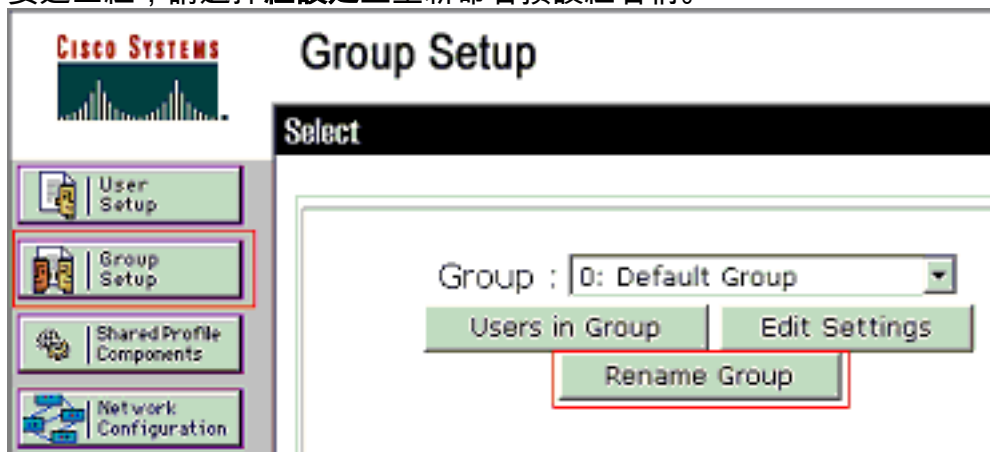


P-1	市場行銷	IP電話	CP-7970G-SEP001759E7492C	P1cisco	語音	IP電話
P-2	銷售	IP電話	CP-7961G-SEP001A2F80381F	P2cisco	語音	IP電話

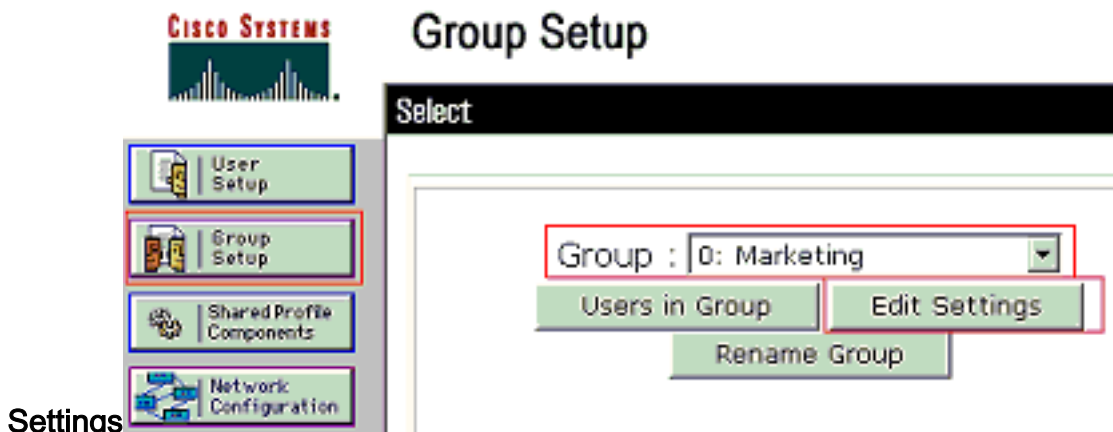
為連線到VLAN 3 ( 語音 )、4 ( 行銷 ) 和5 ( 銷售 ) 的客戶端建立組。這裡針對此目的建立了IP Phone、Marketing和Sales組。

**注意：**這是行銷和IP電話組的配置。對於Sales組配置，請完成Marketing組的步驟。

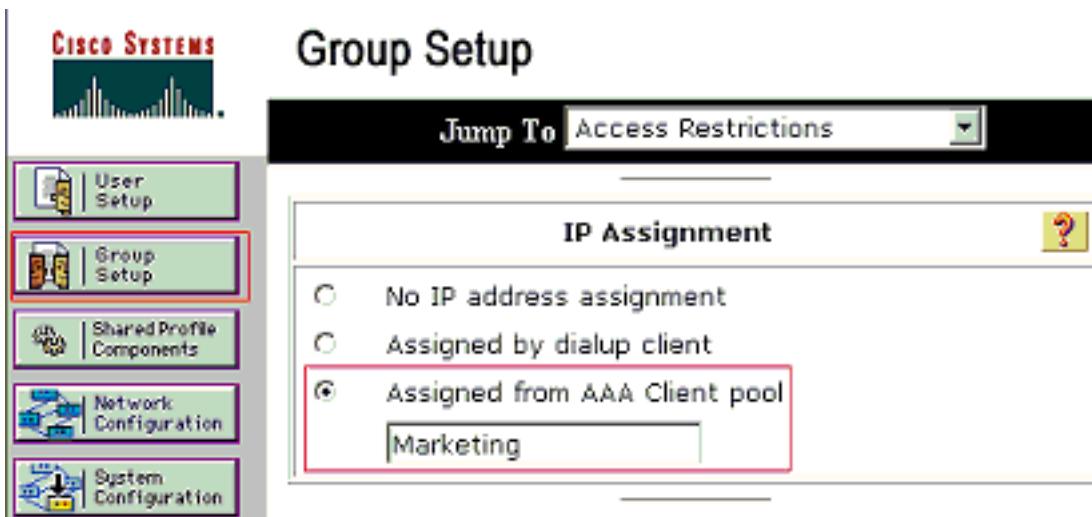
1. 要建立組，請選擇組設定並重新命名預設組名稱。



2. 若要配置組，請從清單中選擇該組，然後按一下Edit



3. 將客戶端IP地址分配定義為由AAA客戶端池分配。輸入在交換機上為此組客戶端配置的IP地址

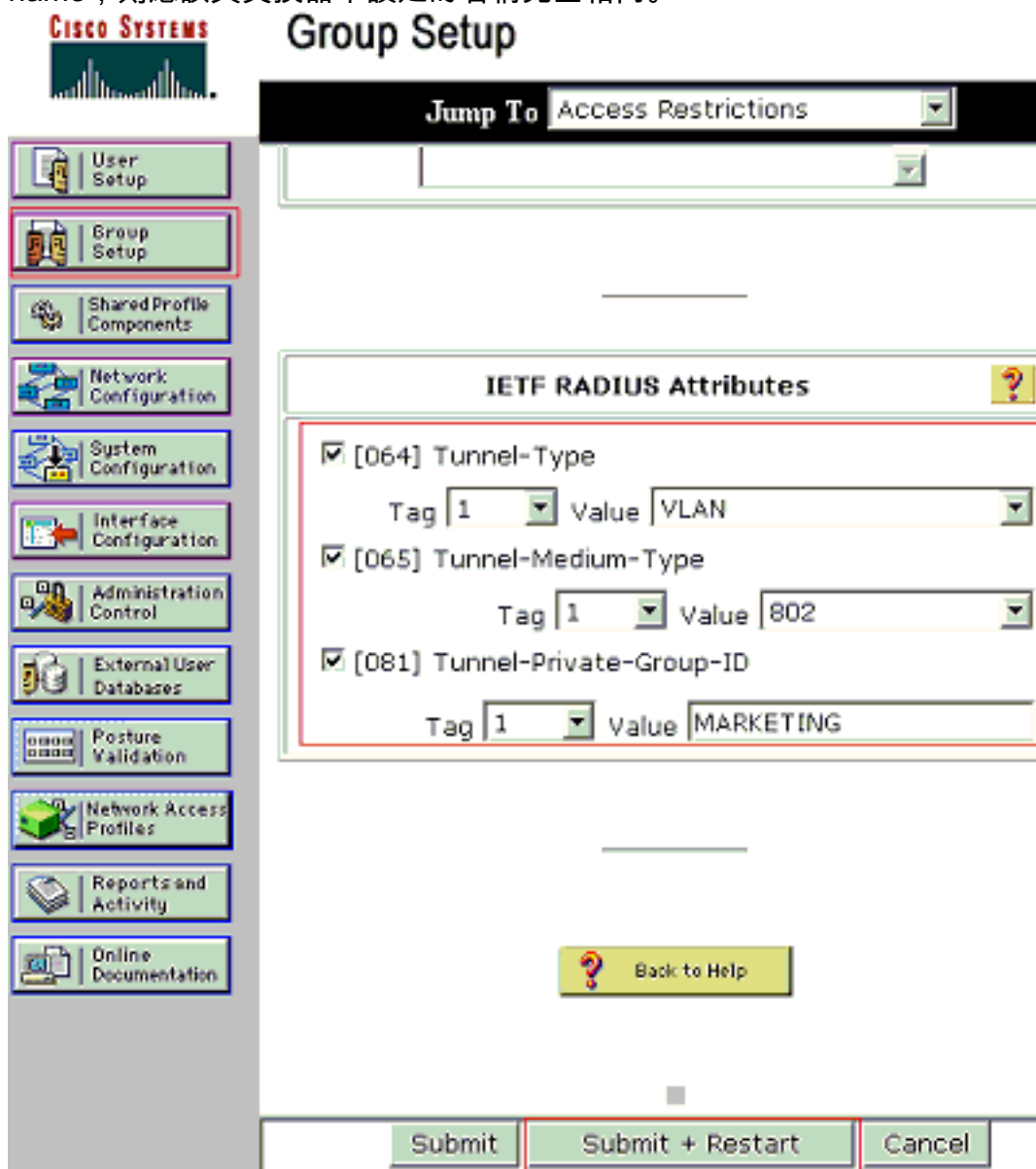


池的名稱。

**注意**

：僅當此使用者要通過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。**注意**：僅對於IP Phones組配置，請跳過下一步（步驟4）並轉到步驟5。

4. 定義Internet工程任務組(IETF)屬性64、65和81，然後按一下**提交+重新啟動**。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**：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。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，則客戶端將被分配到埠的訪問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**aaa authorization network default group radius**命令。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。**注意：**下一步僅適用於IP電話組。

5. 設定RADIUS伺服器以傳送思科屬性值(AV)配對屬性來授權語音裝置。否則交換器會將語音裝置視為資料裝置。使用**device-traffic-class=voice**的值定義Cisco屬性值(AV)配對屬性，然後點選**提交+重新啟動**。

The screenshot shows the 'Group Setup' configuration interface. On the left is a navigation sidebar with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Group Setup' and includes a 'Jump To' dropdown menu currently set to 'Access Restrictions'. Below this are two main sections: 'IP Assignment' and 'Cisco IOS/PIX 6.x RADIUS Attributes'. In the 'IP Assignment' section, the radio button for 'Assigned from AAA Client pool' is selected, and the text box below it contains 'IP-Phones'. In the 'Cisco IOS/PIX 6.x RADIUS Attributes' section, the checkbox for '[009\001] cisco-av-pair' is checked, and the text box below it contains 'device-traffic-class=voice'. Other attributes are unchecked. At the bottom of the form are three buttons: 'Submit', 'Submit + Restart' (which is highlighted with a red box), and 'Cancel'.

## 使用者設定

完成這些步驟，以便新增和配置使用者。

1. 要新增和配置使用者，請選擇**User Setup**。輸入使用者名稱，然後按一下「Add/Edit」



# User Setup

Select













- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

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](#)

2. 定義使用者的使用者名稱、密碼和組。

-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

## User: mkt-manager (New User)

Account Disabled

### User Setup

Password Authentication:

ACS Internal Database 

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

Password   
 Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password   
 Confirm 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:

Marketing 

Callback

Use group setting

Submit

Delete

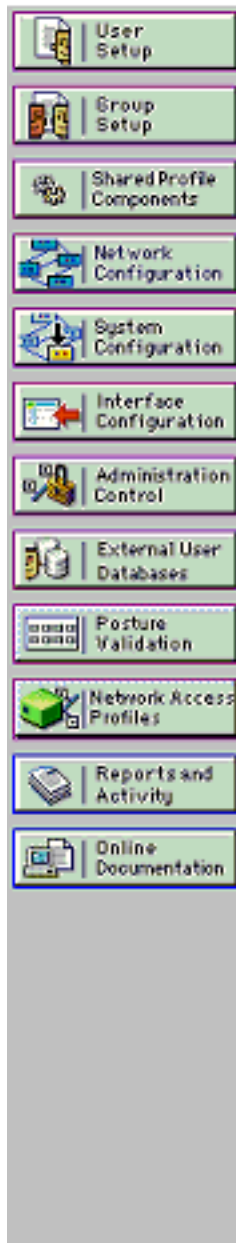
Cancel

3. IP電話使用其裝置ID作為使用者名稱，並使用共用金鑰作為身份驗證的密碼。RADIUS伺服器上的這些值應相符。對於IP電話，P-1和P-2建立與裝置ID相同的使用者名稱，建立與配置的共用金鑰相同的密碼。有關IP電話上的裝置ID和共用金鑰的詳細資訊，請參閱[配置IP電話以使用802.1x身份驗證](#)部分。



## User Setup

Edit



**User: CP-7961G-SEP001A2F80381F**

Account Disabled

### User Setup

Password Authentication:

ACS Internal Database

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

Password \*\*\*\*\*

Confirm Password \*\*\*\*\*

Separate (CHAP/MS-CHAP/ARAP)

Password \*\*\*\*\*

Confirm 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:

IP Phones

Submit

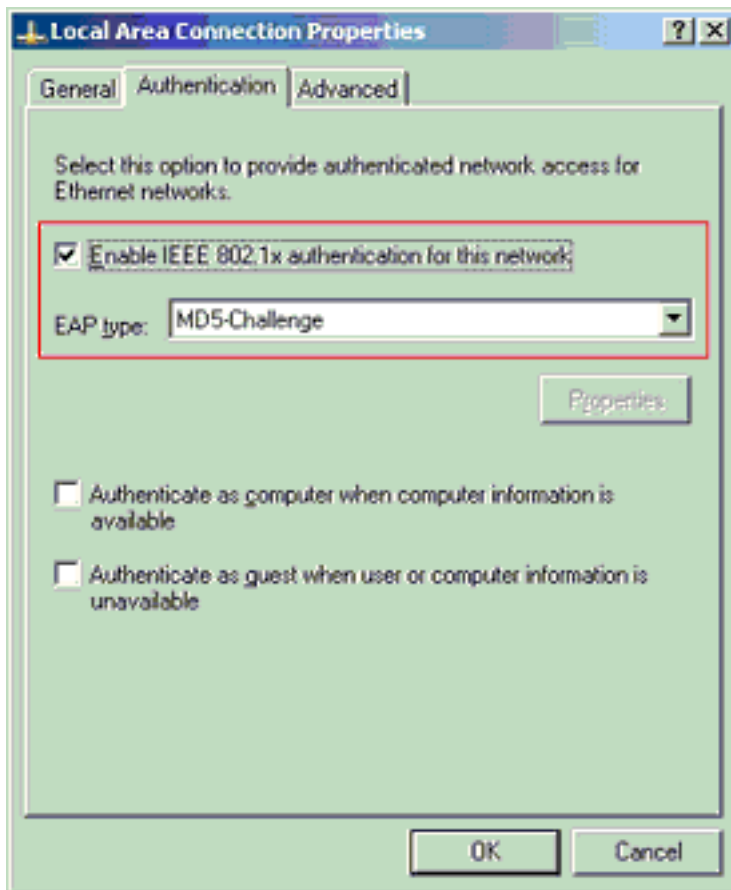
Delete

Cancel

### [將PC客戶端配置為使用802.1x身份驗證](#)

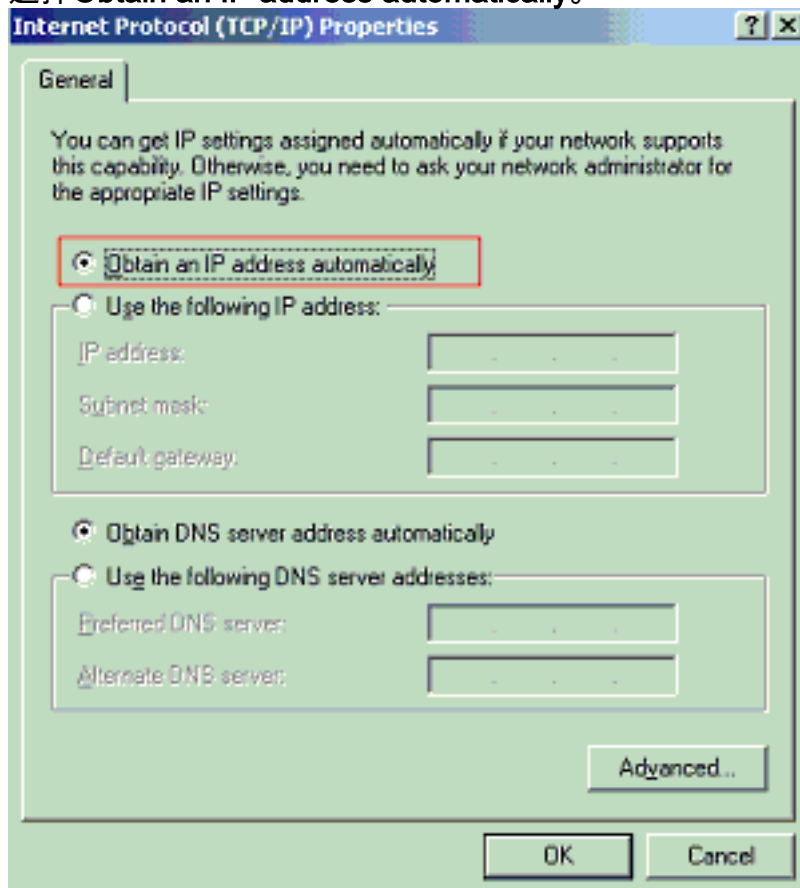
此範例特定於Microsoft Windows XP Extensible Authentication Protocol(EAP)over LAN(EAPOL)使用者端：

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，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**。





## 將IP電話配置為使用802.1x身份驗證

完成這些步驟，配置IP電話進行802.1x身份驗證。

1. 按Settings按鈕以訪問802.1X Authentication設定，然後選擇Security Configuration > 802.1X Authentication > Device Authentication。
2. 將Device Authentication選項設定為Enabled。
3. 按Save軟鍵。
4. 選擇802.1X Authentication > EAP-MD5 > Shared Secret，以在電話上設定密碼。
5. 輸入共用金鑰，然後按儲存。**注意：**密碼必須介於6到32個字元之間，由數字或字母的任意組合組成。，則顯示消息，並且不儲存密碼。**注意：**如果在電話上禁用802.1X身份驗證或執行出廠重置，則會刪除以前配置的MD5共用金鑰。**注意：**無法配置其他選項，即裝置ID和領域。裝置ID用作802.1x身份驗證的使用者名稱。這是電話型號和唯一MAC地址的衍生物，以以下格式顯示：CP-<model>-SEP-<MAC>。例如，CP-7970G-SEP001759E7492C。有關詳細資訊，請參閱[802.1X身份驗證設定](#)。

完成這些步驟，配置IP電話以從DHCP伺服器獲取IP地址。

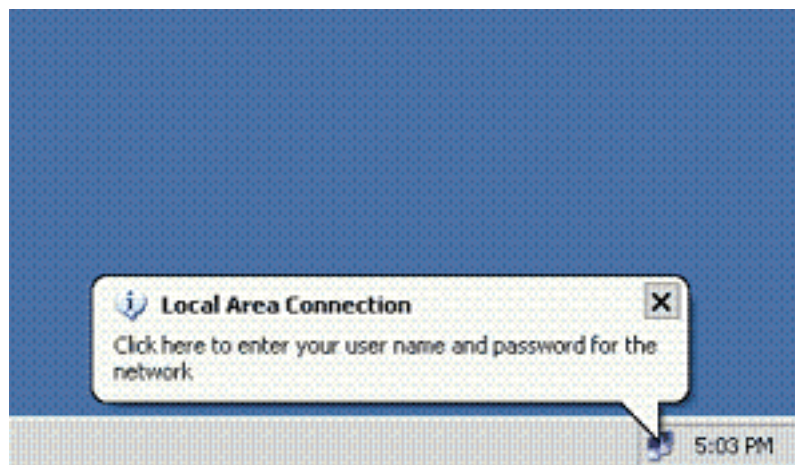
1. 按Settings按鈕以訪問Network Configuration設定，然後選擇Network Configuration。
2. 解鎖網路配置選項。要解鎖，請按\*\*#。附註：不要按\*\*#解鎖選項，然後立即再次按\*\*#鎖定選項。電話將此序列解釋為\*\*#\*\*，這將重置電話。若要在解鎖選項後將其鎖定，請至少等待10秒鐘，然後再按\*\*#。
3. 滾動到DHCP Enabled選項，然後按Yes軟鍵啟用DHCP。
4. 按Save軟鍵。

## 驗證

使用本節內容，確認您的組態是否正常運作。

## PC客戶端

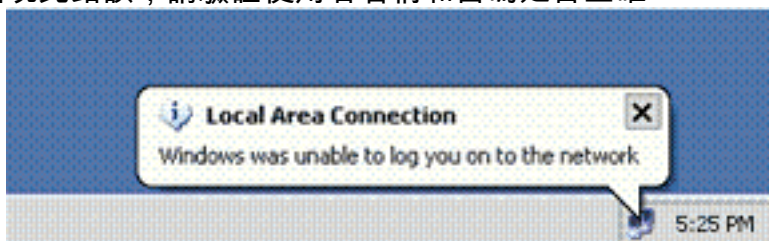
如果配置已正確完成，PC客戶端將顯示彈出提示以輸入使用者名稱和密碼。



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。**注意：**MDA不會強制裝置身份驗證的順序。但是，為了獲得最佳效果，思科建議在啟用MDA的連線埠上使用資料裝置之前，先對語音裝置進行驗證。



2. 輸入使用者名稱和密碼。
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。注意：如果出現此錯誤，請驗證使用者名稱和密碼是否正確



## IP電話

通過IP電話中的802.1X Authentication Status選單可以監控身份驗證狀態。

1. 按**Settings**按鈕以訪問802.1X Authentication Real-Time Stats，然後選擇**Security Configuration > 802.1X Authentication Status**。
2. **Transaction Status**應為**Authenticated**。如需詳細資訊，請參閱[802.1X驗證即時狀態](#)。注意：還可以通過**Settings > Status > Status Messages**驗證身份驗證狀態。

## 第3層交換機

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。

```
Cat-3560#show dot1x all summary
```

Interface	PAE	Client	Status
Fa0/1	AUTH	0016.3633.339c	AUTHORIZED
		0017.59e7.492c	AUTHORIZED
Fa0/2	AUTH	0014.5e94.5f99	AUTHORIZED
Fa0/3	AUTH	0011.858D.9AF9	AUTHORIZED
Fa0/4	AUTH	0016.6F3C.A342	AUTHORIZED
		001a.2f80.381f	AUTHORIZED

```
Cat-3560#show dot1x interface fastEthernet 0/1 details
```

Dot1x Info for FastEthernet0/1

```
-----  
PAE = AUTHENTICATOR  
PortControl = AUTO  
ControlDirection = Both  
HostMode = MULTI_DOMAIN  
ReAuthentication = Enabled  
QuietPeriod = 10  
ServerTimeout = 30  
SuppTimeout = 30  
ReAuthPeriod = 60 (Locally configured)  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30  
RateLimitPeriod = 0  
Auth-Fail-Vlan = 6  
Auth-Fail-Max-attempts = 2  
Guest-Vlan = 6
```

Dot1x Authenticator Client List

```
-----  
Domain = DATA  
Supplicant = 0016.3633.339c  
  Auth SM State = AUTHENTICATED  
  Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 29  
Authentication Method = Dot1x  
Authorized By = Authentication Server  
Vlan Policy = 4
```

```
Domain = VOICE  
Supplicant = 0017.59e7.492c  
  Auth SM State = AUTHENTICATED  
  Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 15  
Authentication Method = Dot1x  
Authorized By = Authentication Server
```

驗證成功後確認VLAN狀態。

Cat-3560#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Gi0/1 Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1, Fa0/4
4 MARKETING	active	Fa0/1, Fa0/2
5 SALES	active	Fa0/3, Fa0/4
6 GUEST_and_AUTHFAIL	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	

```
1005 trnet-default                               act/unsup
!--- Output suppressed.
```

## 2. 身份驗證成功後驗證DHCP繫結狀態。

```
Router#show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
172.16.3.2	0100.1759.e749.2c	Aug 24 2007 06:35 AM	Automatic
172.16.3.3	0100.1a2f.8038.1f	Aug 24 2007 06:43 AM	Automatic
172.16.4.2	0100.1636.3333.9c	Aug 24 2007 06:50 AM	Automatic
172.16.4.3	0100.145e.945f.99	Aug 24 2007 08:17 AM	Automatic
172.16.5.2	0100.166F.3CA3.42	Aug 24 2007 08:23 AM	Automatic
172.16.5.3	0100.1185.8D9A.F9	Aug 24 2007 08:51 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指令輸出的分析。

## 疑難排解

### IP電話身份驗證失敗

如果802.1x身份驗證失敗，IP電話狀態顯示IP或。完成以下步驟即可解決此問題：

- 確認IP電話上已啟用802.1x。
- 確認已在驗證(RADIUS)伺服器上輸入裝置ID作為使用者名稱。
- 確認已在IP電話上配置共用金鑰。
- 如果配置了共用金鑰，請驗證您在身份驗證伺服器上輸入的共用金鑰是否相同。
- 確認您已正確配置其他所需裝置，例如交換機和身份驗證伺服器。

## 相關資訊

- [配置IEEE 802.1x基於埠的身份驗證](#)
- [將IP電話配置為使用802.1x身份驗證](#)
- [在Cisco Catalyst交換機環境中部署適用於Windows NT/2000伺服器的Cisco Secure ACS的準則](#)
- [RFC 2868:適用於通道通訊協定支援的RADIUS屬性](#)
- [運行Cisco IOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證示例](#)
- [運行CatOS軟體的Catalyst 6500/6000的IEEE 802.1x身份驗證配置示例](#)
- [LAN 產品支援頁面](#)
- [LAN 交換支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)