Cisco Catalyst レイヤ 3 固定構成スイッチでの IEEE 802.1x マルチドメイン認証の設定例

目次

はじめに

マルチドメイン認証を使用すると、同じスイッチ ポート上での IP Phone と PC の認証が可能になる一方で、IP Phone と PC が適切な音声 VLAN とデータ VLAN に配置されます。 このドキュメントでは、Cisco Catalyst レイヤ 3 固定構成スイッチで IEEE 802.1x Multi-Domain Authentication（MDA; マルチドメイン認証）を設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- RADIUS はどのように動作しますか。
- Catalyst スイッチングおよび ACS 導入ガイド

- Cisco Secure Access Control Server 4.1 ユーザ ガイド
- Cisco Unified IP Phone の概要

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Catalyst 3560 シリーズはこと実行 Cisco IOS ® ソフトウェア リリース 12.2(37)SE1 切り替えます**注:** Cisco IOS　12.2(35)SE
- この例では、RADIUS サーバとして Cisco Secure Access Control Server（ACS）4.1 を使用します。**注:** 802.1x RADIUS
- 802.1x 認証をサポートする PC クライアント**注:** Microsoft Windows XP
- SCCP ファームウェア バージョン 8.2(1) を搭載した Cisco Unified IP Phone 7970G
- SCCP ファームウェア バージョン 8.2(2) を搭載した Cisco Unified IP Phone 7961G
- Cisco Unified Communications Manager（Cisco CallManager）4.1(3)sr2 を搭載した Media Covergence Server（MCS）

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

関連製品

この設定は、次のハードウェアにも使用できます。

- Cisco Catalyst 3560-E シリーズ スイッチ
- Cisco Catalyst 3750 シリーズ スイッチ
- Cisco Catalyst 3750-E シリーズ スイッチ

注: Cisco Catalyst 3550 シリーズ スイッチでは、802.1x マルチドメイン認証がサポートされません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IEEE 802.1x 標準では、認証されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアントサーバ ベースのアクセス制御と認証プロトコルが定義されています。 802.1x では、バーチャル アクセス ポイントを各ポートに 2 つ作成することで、ネットワーク アクセスが制御されます。 片方のアクセス ポイントは制御されないポートであり、 もう片方のアクセス ポイントは制御されたポートです。 単一のポートを通過するすべてのトラフィックは、どちらのアクセス ポイントでも使用できます。 802.1x では、スイッチ ポートに接続された各ユーザ デバイスが認証され、スイッチまたは LAN によって提供されるサービスが使用可能になる前にそのポートが VLAN に割り当てられます。 802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。 認証に成功すると、通常のトラフィックはポートを通過できるようになります。

802.1x は、次の 3 つの主要コンポーネントによって構成されます。 それぞれのコンポーネントは Port Access Entity（PAE）と呼ばれます。

- サプリカント：ネットワーク アクセスを要求するクライアント デバイス（IP Phone や PC など）。
- オーセンティケータ：サプリカント認証要求を容易にするネットワーク デバイス（Cisco Catalyst 3560 など）。
- 認証サーバ：認証サービスを提供する Remote Authentication Dial-in User Server（RADIUS）（Cisco Secure Access Control Server など）。

Cisco Unified IP Phone には、802.1X サプリカントも含まれています。 このサプリカントを使用すると、ネットワーク管理者は LAN スイッチ ポートへの IP Phone の接続を制御できるようになります。 IP phone 802.1X サプリカントの初期リリースでは、802.1X 認証に EAP-MD5 オプションが実装されています。 マルチドメイン設定では、IP Phone および接続された PC は ユーザ名とパスワードを指定してそれぞれ個別にネットワークへのアクセスを要求する必要があります。 オーセンティケータ デバイスには、アトリビュートと呼ばれる RADIUS からの情報が必要な場合があります。 アトリビュートによって、サプリカントに対して特定の VLAN へのアクセスが許可されるかどうかなど、追加的な認可情報が指定されます。 これらのアトリビュートは、ベンダー固有である場合があります。 Cisco では、サプリカント（IP Phone）が音声 VLAN 上で許可されていることをオーセンティケータ（Cisco Catalyst 3560）に伝えるために、RADIUS アトリビュート cisco-av-pair を使用します。

設定

このセクションでは、このドキュメントで説明する 802.1x マルチドメイン認証機能を設定するための情報を提供します。

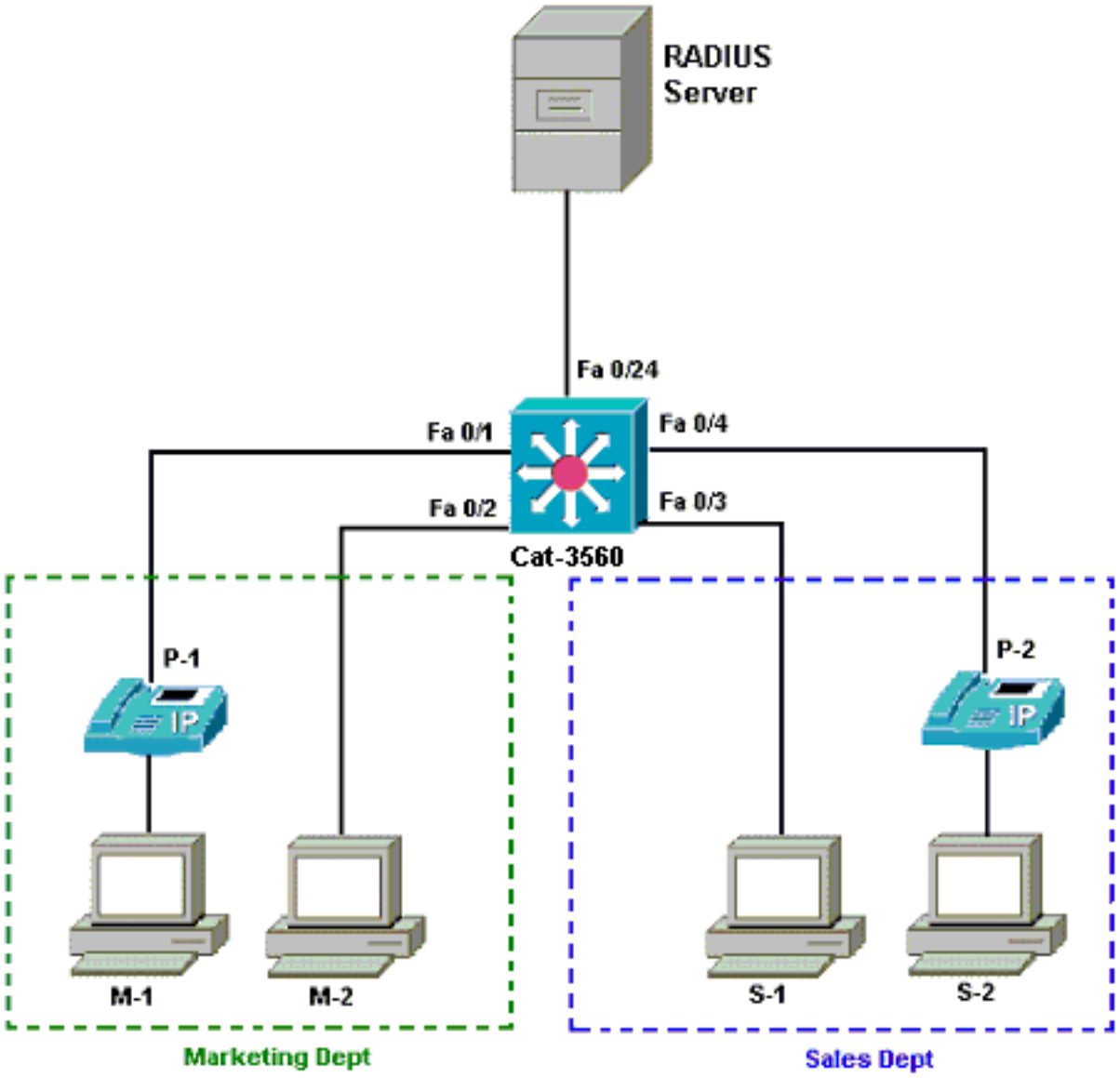
設定には次の手順が必要です。

- Catalyst スイッチで 802.1x マルチドメイン認証を使用するための設定
- RADIUS サーバの設定
- 802.1x 認証を使用するための PC クライアントの設定
- 802.1x 認証を使用するための IP Phone の設定

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



- RADIUS サーバ：クライアントの実際の認証を実行します。 RADIUS サーバは、クライアントの ID を検証し、クライアントが LAN およびスイッチ サービスにアクセスすることを承認されているかどうかをスイッチに通知します。 Cisco ACS は、認証および VLAN 割り当て用に Media Covergence Server（MCS）上にインストールされて設定されます。 また、MCS は IP Phone 用の TFTP サーバおよび Cisco Unified Communications Manager（Cisco CallManager）でもあります。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理的なアクセスを制御します。 スイッチは、クライアントと RADIUS サーバ間の中継要素（プロキシ）として動作します。 クライアントからの ID 情報を要求し、RADIUS サーバを使用してその情報を検証し、クライアントに応答を受け渡します。 Catalyst 3560 スイッチは DHCP サーバとしても設定されます。 Dynamic Host Configuration Protocol（DHCP）の 802.1x 認証サポートを使用すると、DHCP サーバでは異なるクラスのエンド ユーザに IP アドレスを割り当てることができます。 これを実行するために、認証済みのユーザ ID が DHCP ディスカバリ プロセスに追加されます。 802.1x マルチドメイン認証用に設定されるポートは、FastEthernet 0/1 および 0/4 のポートのみです。 FastEthernet 0/2 および 0/3 のポートは、デフォルトの 802.1x 単一ホスト モードです。 FastEthernet 0/24 ポートは、RADIUS サーバに接続します。**注:** DHCP DHCP SVIvlan **ip helper-address**
- クライアント：IP Phone やワークステーションなど、LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイスです。 クライアントは DHCP サー

バから IP アドレスを取得するように設定されています。 M-1、M-2、S-1、および S-2 の各デバイスは、ネットワークへのアクセスを要求するワークステーション クライアントです。 P-1 および P-2 は、ネットワークへのアクセスを要求する IP Phone クライアントです。 M-1、M-2、および P-1 は、マーケティング部門のクライアント デバイスです。 S-1、S-2、および P-2 は、営業部門のクライアント デバイスです。 P-1 および P-2 の IP Phone は、同じ音声 VLAN（VLAN 3）内に配置されるように設定されています。 M-1 および M-2 のワークステーションは、認証に成功した後、同じデータ VLAN（VLAN 4）内に配置されるように設定されています。 S-1 および S-2 のワークステーションも、認証に成功した後、同じデータ VLAN（VLAN 5）内に配置されるように設定されています。**注:** RADIUS VLAN

Catalyst スイッチで 802.1x マルチドメイン認証を使用するための設定

このスイッチ設定のサンプルには次のものが含まれます。

- スイッチ ポート上で 802.1x マルチドメイン認証を有効にする方法
- RADIUS サーバ関連の設定
- IP アドレス割り当てのための DHCP サーバの設定
- 認証後にクライアント間で接続を確立するためのインター VLAN ルーティング

MDA の設定方法のガイドラインについては、『マルチドメイン認証の使用』を参照してください。

注: RADIUS サーバは常に認証済みポートの背後に接続してください。

注: 関連する設定のみを次に示します。

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
```

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

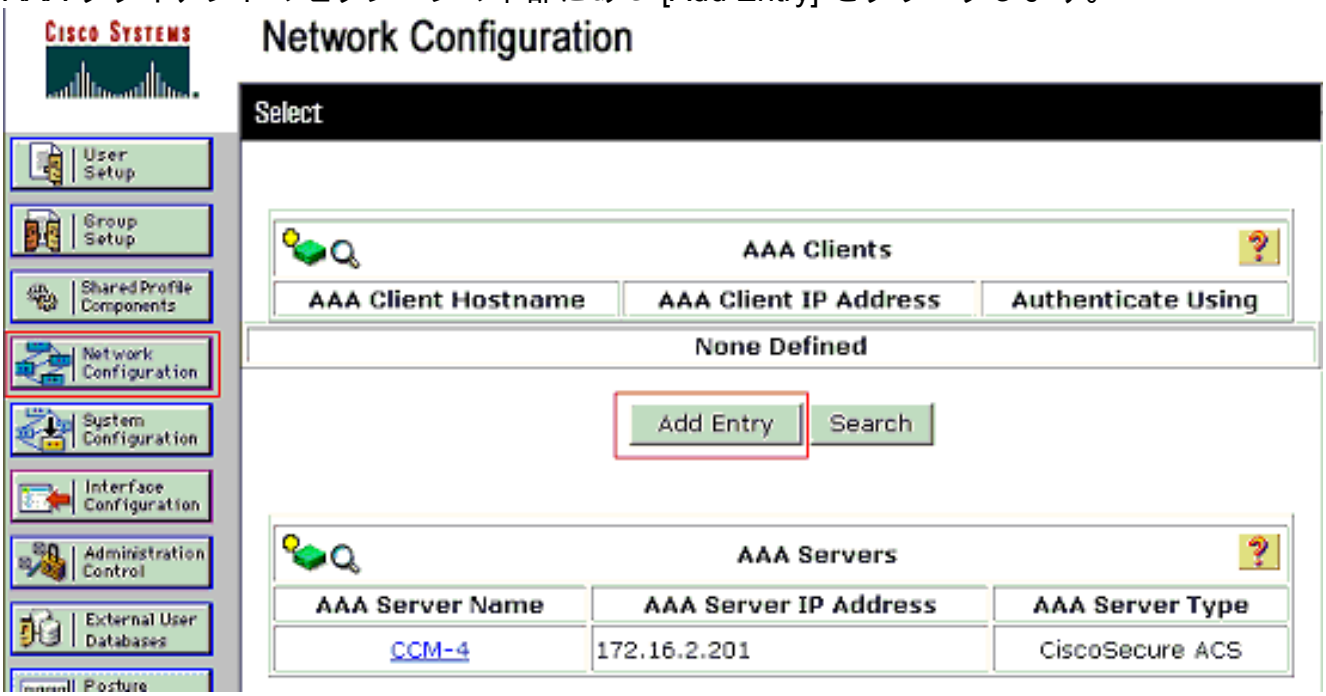
RADIUS サーバの設定

RADIUS サーバには、172.16.2.201/24 という固定 IP アドレスが割り当てられています。 AAA クライアントに RADIUS サーバを設定するには、次のステップを実行します。

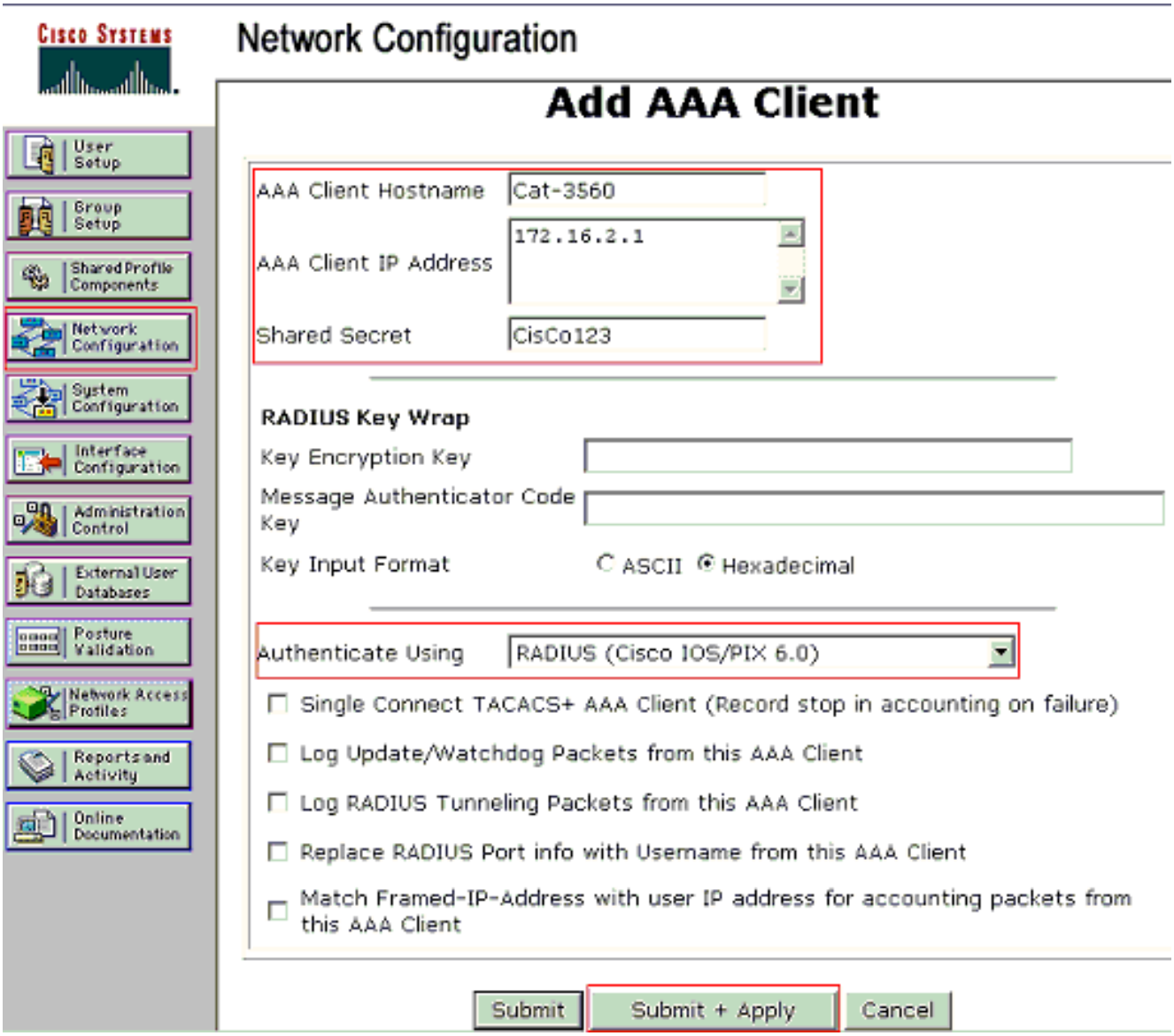
1. AAA クライアントを設定するには、ACS 管理ウィンドウで **Network Configuration** をクリッ

クします。

2. AAA クライアントのセクションの下部にある [Add Entry] をクリックします。



3. 次のように、AAA クライアント ホスト名、IP アドレス、共有秘密鍵、および認証タイプを設定します。AAA クライアント ホスト名 = スイッチ ホスト名（**Cat-3560**）AAA クライアントの IP アドレス = スイッチの管理インターフェイスの IP アドレス（**172.16.2.1**）共有秘密鍵 = スイッチで設定されている RADIUS キー（**CisCo123**）**注:** AAA ACS キーの大文字と小文字は区別されます。認証方法 = **RADIUS（Cisco IOS/PIX 6.0）注:** Cisco Attribute-ValueAV
4. これらの変更を有効にするには、次の例に示すように **Submit + Apply** をクリックします。



グループ セットアップ

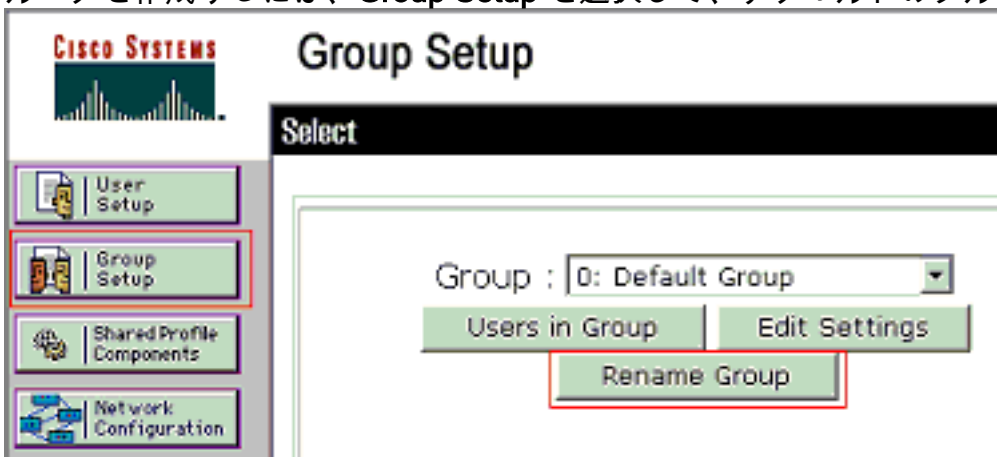
認証用に RADIUS サーバを設定するには、次の表を参照してください。

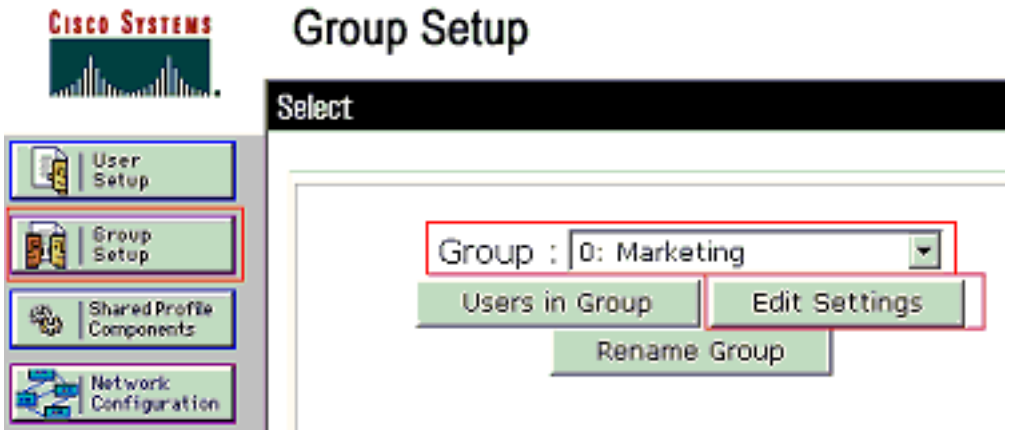
デバイス	部門	グループ	User	Password	VLAN	DHCP プール
M-1	Marketing	Marketing	mkt-manager	MMcisco	MARKETING	Marketing
M-2	Marketing	Marketing	mkt-staff	MScisco	MARKETING	Marketing
S-2	Sales	Sales	sales-manager	SMcisco	SALES	Sales
S-1	Sales	Sales	sales-	SScisc	SALES	Sale

			staff	o		s
P-1	Marketing	IP Phone	CP-7970G-SEP001759E7492C	P1cisco	音声	IP-Phones
P-2	Sales	IP Phone	CP-7961G-SEP001A2F80381F	P2cisco	音声	IP-Phones

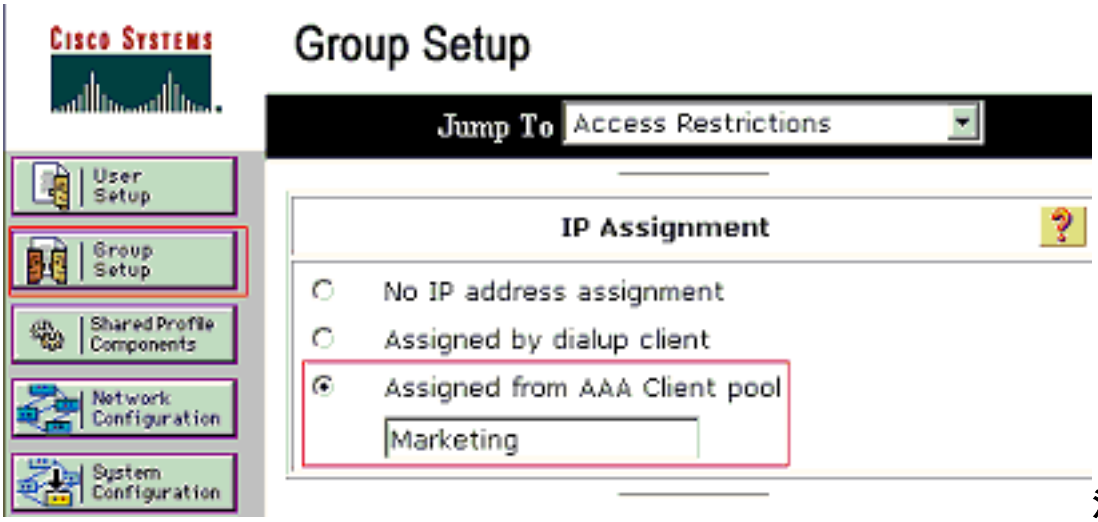
VLAN 3（VOICE）、VLAN 4（MARKETING）、および VLAN 5（SALES）に接続するクライアントのグループを作成します。 この例では、**IP Phones**、**Marketing**、および **Sales** の各グループが作成されます。

注: これは、**Marketing** グループおよび **IP Phones** グループの設定です。 **Sales** グループの設定には、**Marketing** グループの手順を実行します。

1. グループを作成するには、**Group Setup** を選択して、デフォルトのグループ名を変更します。


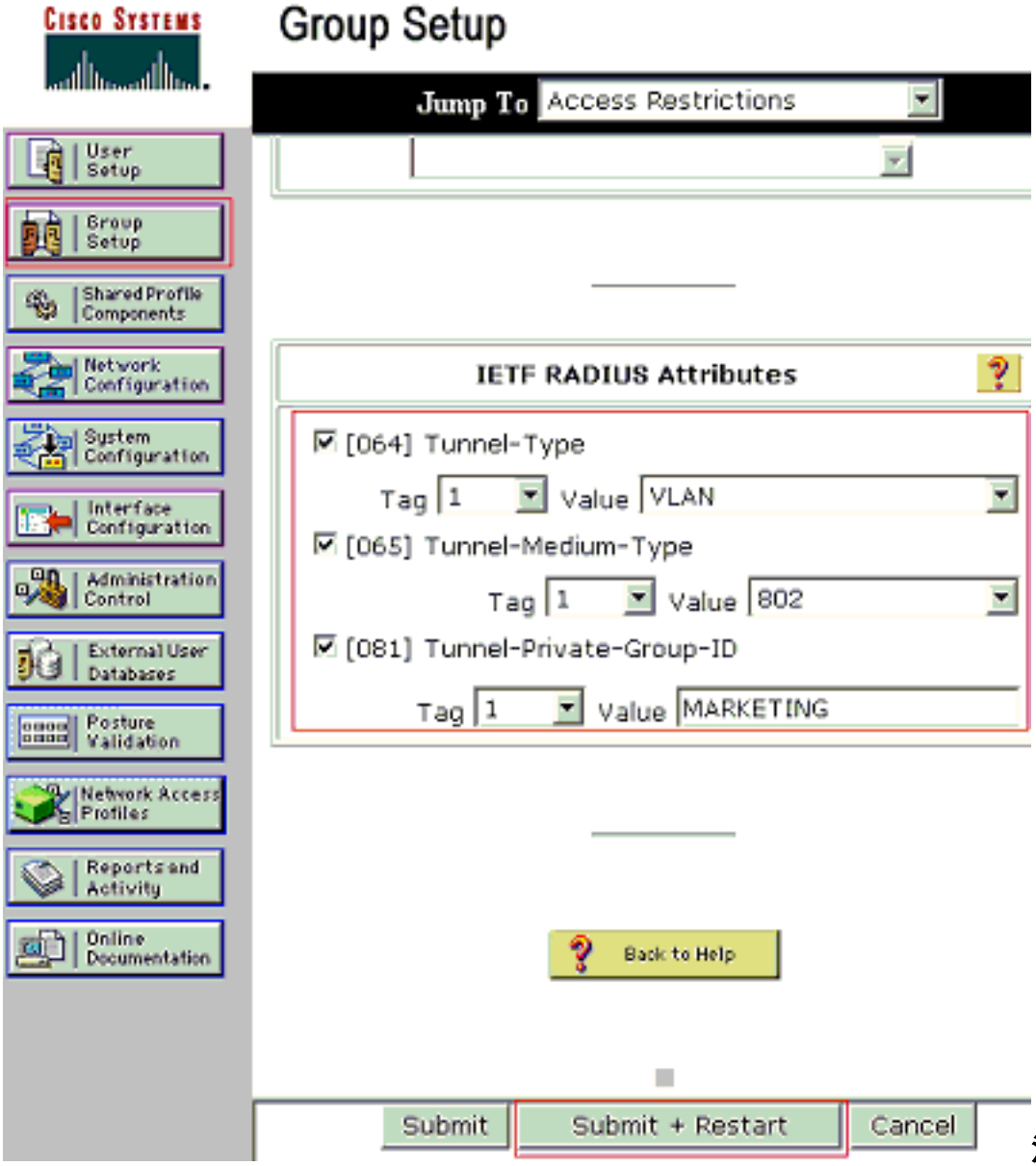
2. グループを設定するには、リストからグループを選択して、**Edit Settings** をクリックします。


3. **Assigned by AAA client pool** としてクライアント IP アドレス割り当てを定義します。 このグループ クライアントのスイッチ上で設定された IP アドレス プールの名前を入力します。



注: AAA IP IP AAA IP **注: IP Phones 4 5**

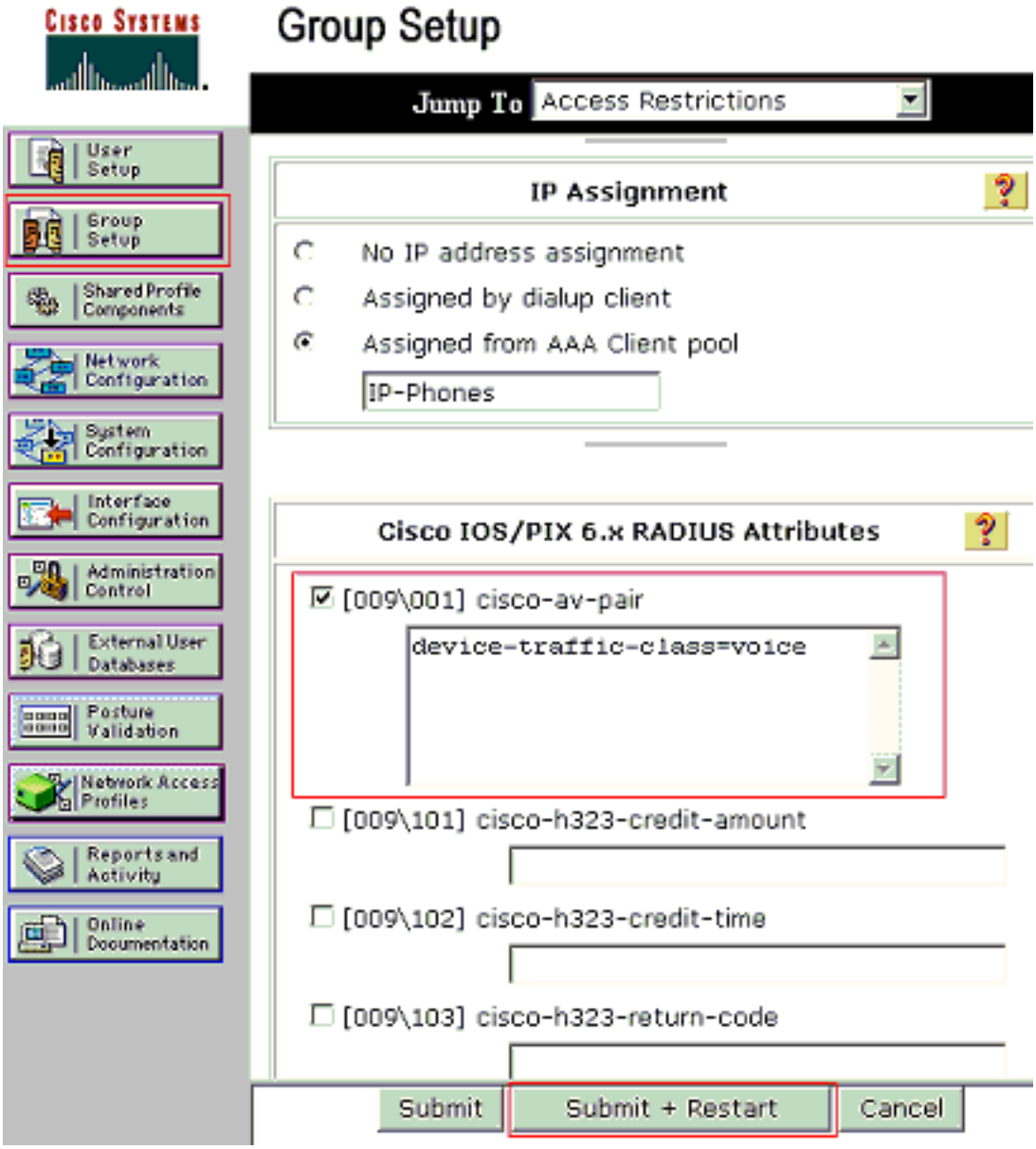
4. Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) アトリビュート **64**、**65**、および **81** を定義してから、**Submit + Restart** をクリックします。この例のように、値のタグには **1** を設定してください。 Catalyst では 1 以外のタグは無視されます。ユーザを特定の VLAN に割り当てるには、アトリビュート **81** で、対応する VLAN **名**または VLAN **番号**を指定します。**注:** VLAN VLAN



注: これらの IETF 属性の詳細については、『RFC 2868: これらの IETF 属性に関する 詳細については[ト

ンネルプロトコル サポートのための RADIUS特性。**注:** ACS サーバの初期設定では、IETF RADIUS 属性が **User Setup** に表示されない場合があります。 ユーザ設定の画面で IETF アトリビュートを有効にするには、**Interface configuration > RADIUS (IETF)** の順にクリックします。 次に、[User and Group] 列で属性 **64**、**65**、および **81** にチェックを付けます。**注 :** IETF **81** VLAN ダイナミック VLAN 割り当てのためにアトリビュート **81** を設定している場合で、ポートがアクセス モードのスイッチ ポートである場合、スイッチで **aaa authorization network default group radius** コマンドを発行する必要があります。 このコマンドによって、ポートが RADIUS サーバから提供される VLAN に割り当てられます。 さもなければ、802.1X はユーザの認証の後でにポートを移動します; しかしポートはポートのデフォルトVLAN にまだあり、接続は失敗する場合があります。**注: IP Phones**

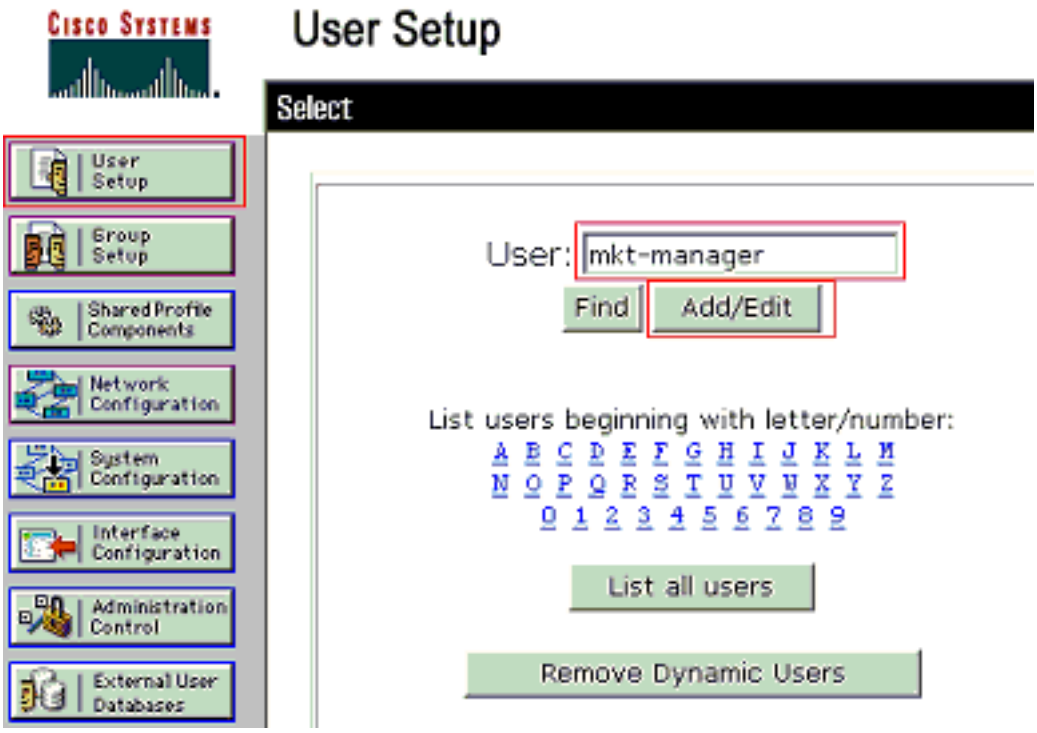
5. 音声デバイスを認可するために、Cisco AV ペア アトリビュートを送信するように RADIUS サーバを設定します。 これを行わないと、スイッチでは音声デバイスがデータ デバイスとして認識されます。 Cisco AV ペア アトリビュートの値を **device-traffic-class=voice** に設定し、**Submit + Restart** をクリックします。



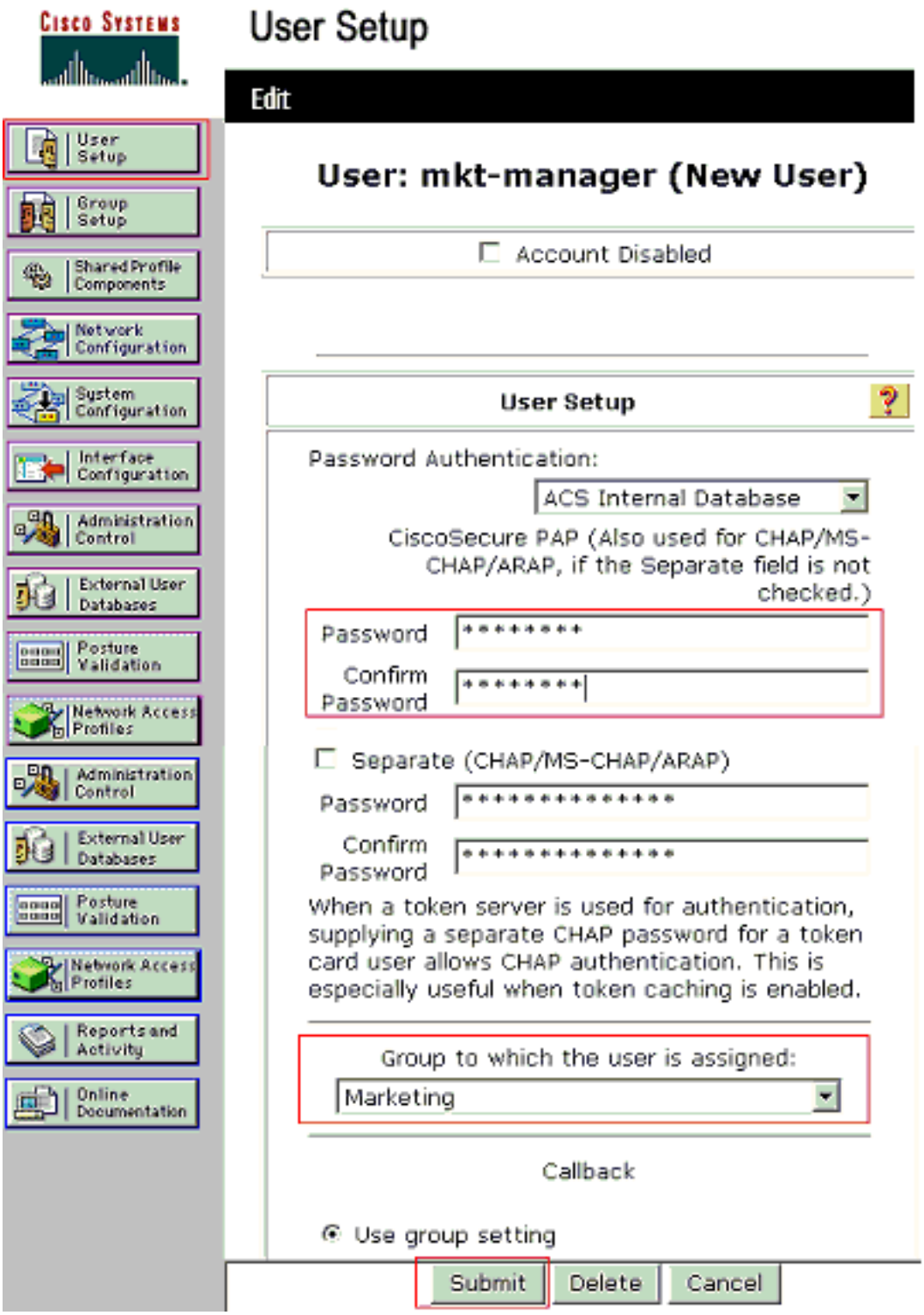
ユーザ設定

ユーザを追加して設定するには、次の手順を実行します。

1. ユーザを追加して設定するには、**User Setup** を選択します。 ユーザ名を入力して、**Add/Edit** をクリックします。

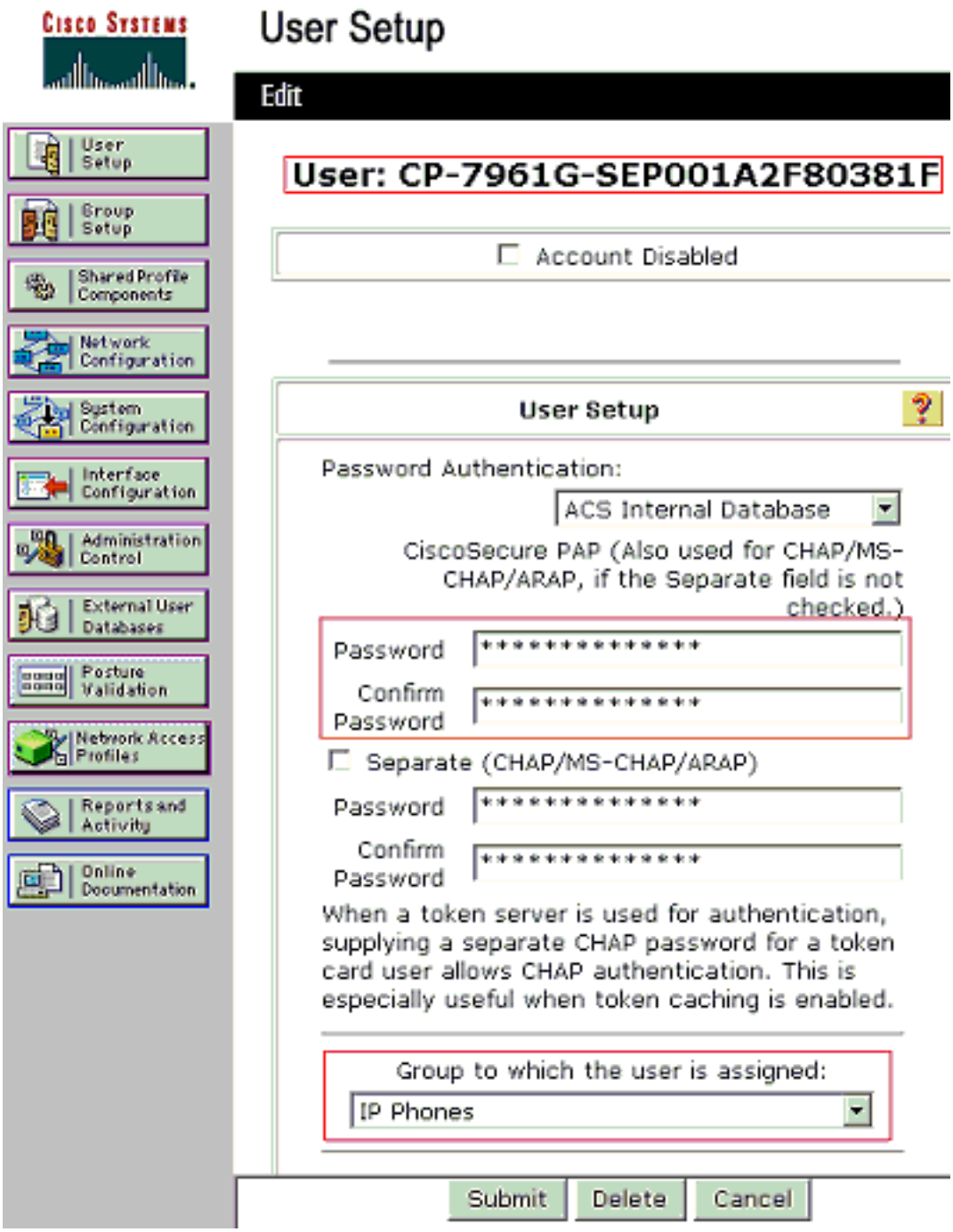


2. ユーザのユーザ名、パスワード、およびグループを定義します。



3. IP Phone は、自身のデバイス ID をユーザ名として使用し、共有秘密鍵を認証用のパスワードとして使用します。 これらの値は、RADIUS サーバ上で一致する必要があります。 P-1 および P-2 の IP Phone では、デバイス ID と一致するユーザ名を作成し、設定済みの共有秘密鍵と一致するパスワードを作成します。 IP Phone でのデバイス ID と共有秘密鍵の詳細については、「802.1x 認証を使用するための IP Phone の設定」セクションを参照してくだ

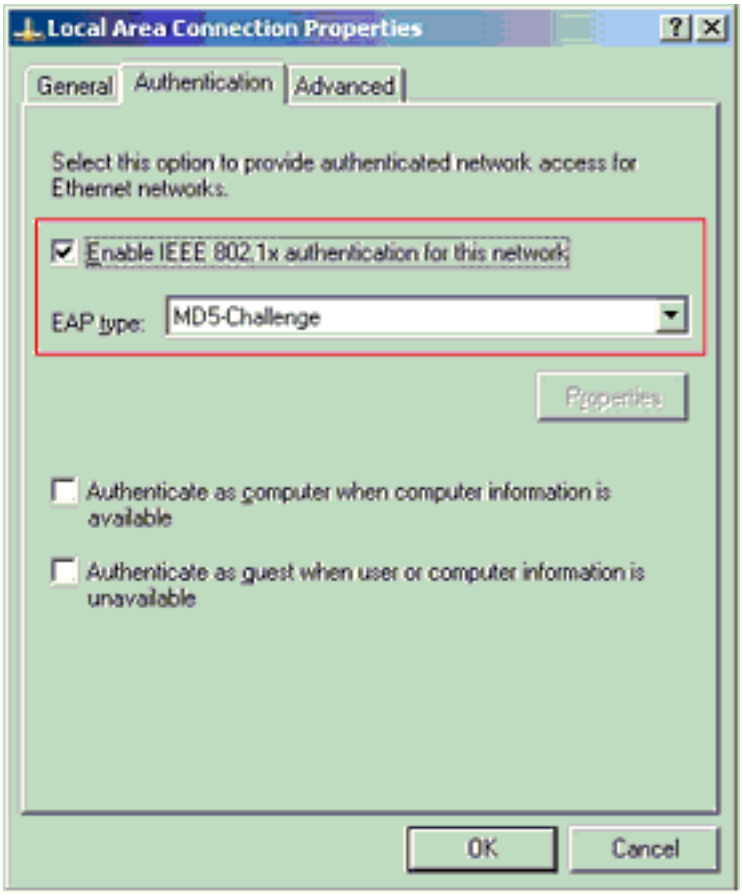
さい。



802.1x 認証を使用するための PC クライアントの設定

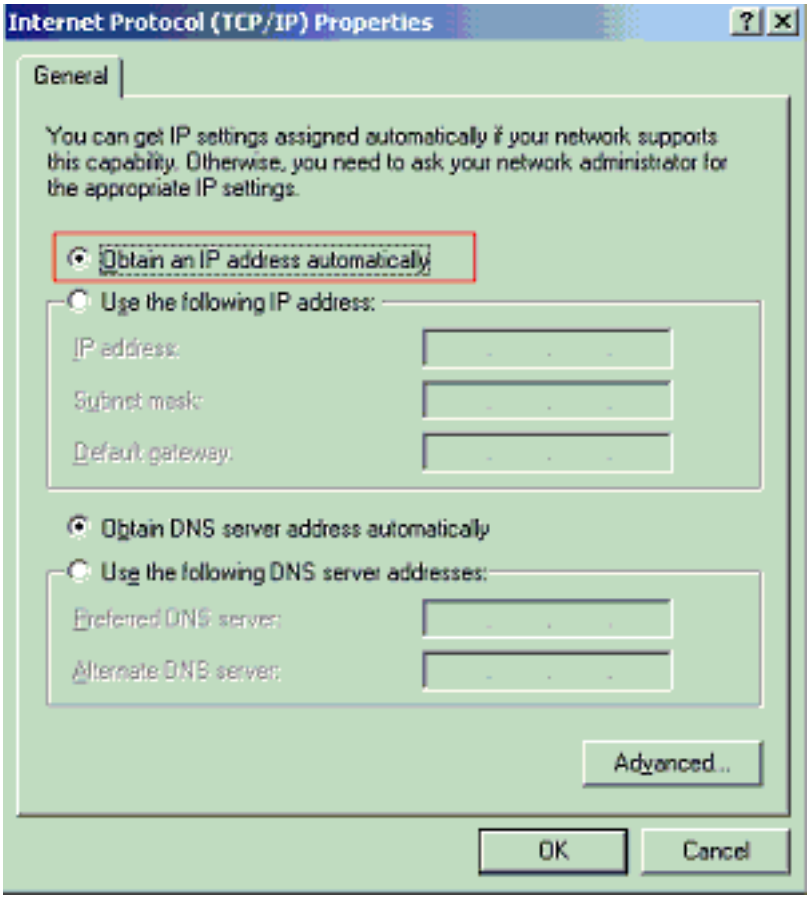
この設定例は、Microsoft Windows XP の Extensible Authentication Protocol（EAP）over LAN（EAPOL）クライアント固有のものです。

1. **[スタート] > [コントロールパネル] > [ネットワーク接続]** の順にクリックし、**[ローカルエリア接続]** を右クリックして **[プロパティ]** を選択します。
2. General タブで、**Show icon in notification area when connected** にチェックを付けます。
3. [Authentication] タブで、**[Enable IEEE 802.1x authentication for this network]** にチェックを付けます。
4. 次の例のように、EAP の種類に **[MD5-Challenge]** を選択します。



次の手順に従って、クライアントが DHCP サーバから IP アドレスを取得できるように設定します。

1. **[スタート] > [コントロールパネル] > [ネットワーク接続]** の順にクリックし、[**ローカルエリア接続**] を右クリックして [**プロパティ**] を選択します。
2. [General] タブで、**[Internet Protocol (TCP/IP)]** をクリックし、**[Properties]** をクリックします。
3. [Obtain an IP address automatically] を選択します。



802.1x 認証を使用するための IP Phone の設定

802.1x 認証を使用するように IP Phone を設定するには、次の手順に従います。

1. **Settings** ボタンを押して、**802.1X Authentication** 設定にアクセスし、**Security Configuration > 802.1X Authentication > Device Authentication** の順に選択します。
2. **Device Authentication** オプションを **Enabled** に設定します。
3. [Save] ソフトキーを押します。
4. **802.1X Authentication > EAP-MD5 > Shared Secret** の順に選択して、電話機にパスワードを設定します。
5. 共有秘密鍵を入力して、**Save** を押します。**注:** 6 32 この条件が満たされない場合、That key is not active here というメッセージが表示され、パスワードは保存されません。**注:** 802.1X MD5 **注: 別のオプションである Device ID and Realm は設定できません。** デバイス ID は、802.1x 認証用のユーザ名として使用されます。 これはこの形式で表示される電話の型番およびユニークな MAC アドレスの派生物です: CP-<model>-SEP-<MAC>。 たとえば、**CP-7970G-SEP001759E7492C** となります。 詳細については、『802.1X 認証の設定』を参照してください。

次の手順に従って、IP Phone が DHCP サーバから IP アドレスを取得できるように設定します。

1. **Settings** ボタンを押して、**Network Configuration** 設定にアクセスし、**Network Configuration** を選択します。
2. **Network Configuration** オプションのロックを解除します。 ロックを解除するには、****#** を押します。**注:** オプションのロックを解除するために ****#** を押した直後に、オプションをロックするために再度 ****#** を押さないでください。 電話機ではこのシーケンスが ****#*? として解釈され、電話機がリセットされます。** オプションのロックを解除した後にオプションをロックするには、少なくとも 10 秒間待機してから ****#** を再度押します。

3. DHCP Enabled オプションまでスクロールし、**Yes** ソフトキーを押して DHCP を有効にします。
4. [Save] ソフトキーを押します。

確認

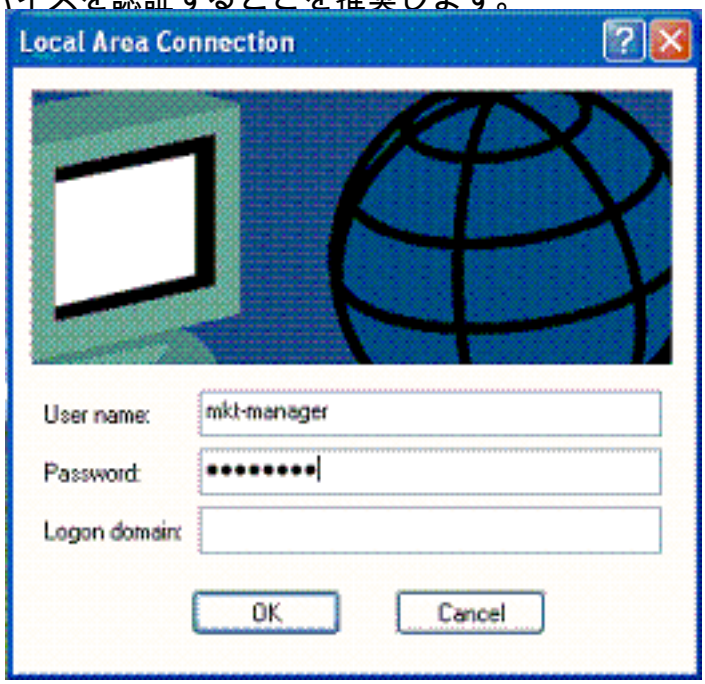
ここでは、設定が正常に動作していることを確認します。

PC クライアント

正しく設定が行われると、PC クライアントにポップアップが表示され、ユーザ名とパスワードの入力をユーザに要求します。

1. 次の例で示すプロンプトをクリックします。

ユーザ名とパスワードを入力するウィンドウが表示されます。**注:** MDA ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。



2. ユーザ名とパスワードを入力します。
3. エラー メッセージが表示されなければ、ネットワーク リソースにアクセスしたり、**ping** を発行したりするなど、通常の方法で接続を確認します。**注:**

IP Phone

IP Phone の 802.1X Authentication Status メニューを使用すると、認証のステータスを監視できます。

1. **Settings** ボタンを押して、802.1X Authentication Real-Time Stats にアクセスし、**Security Configuration > 802.1X Authentication Status** の順に選択します。
2. **Transaction Status** は、**Authenticated** である必要があります。 詳細については、『802.1X 認証リアルタイム ステータス』を参照してください。**注: Settings > Status > Status Messages**

レイヤ 3 スイッチ

パスワードとユーザ名が正しく入力されている場合は、スイッチの 802.1x ポートの状態を確認します。

1. AUTHORIZED を示すポート状態を探します。

```
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
```

認証に成功した後、VLAN ステータスを確認します。

```
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. 認証に成功した後、DHCP バインディング ステータスを確認します。

```
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
```

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

IP Phone 認証の失敗

802.1x 認証に失敗する場合、IP phone ステータスに Configuring IP または Registering が表示されます。 この問題のトラブルシューティングを行うには、次の手順を実行します。

- IP Phone で 802.1x が有効であることを確認します。
- 認証（RADIUS）サーバで入力したデバイス ID がユーザ名と一致していることを確認します。
- IP Phone で共有秘密鍵が設定されていることを確認します。
- 共有秘密鍵が設定されている場合、認証サーバにも同じ共有秘密鍵が設定されていることを確認します。
- 他の必要なデバイス（スイッチや認証サーバなど）を適切に設定していることを確認します。

関連情報

- IEEE 802.1x ポートベース認証の設定
- 802.1x 認証を使用するための IP Phone の設定
- Cisco Catalyst スイッチ環境で Windows NT/2000 Server 用 Cisco Secure ACS を導入する際のガイドライン
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support
- Cisco IOS ソフトウェアが稼動する Catalyst 6500/6000 での IEEE 802.1x 認証の設定例
- CatOS ソフトウェアが稼動する Catalyst 6500/6000 での IEEE 802.1x 認証の設定例
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems