在Cisco Catalyst层3固定配置交换机上的IEEE 802.1x多域认证配置示例

目录

简介

使用多域身份验证功能，可以让 IP 电话和 PC 在同一交换机端口上进行身份验证（虽然它将它们置于相应的语音 VLAN 和数据 VLAN 上）。本文档说明了如何在 Cisco Catalyst 第 3 层固定配置交换机上配置 IEEE 802.1x 多域身份验证 (MDA)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- RADIUS 如何工作？
- Catalyst 交换和 ACS 部署指南
- **Cisco 安全访问控制服务器 4.1 用户指南**

- Cisco Unified IP 电话概述

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS软件版本12.2(37)SE1的Cisco Catalyst 3560系列交换机**注意：** 只有 Cisco IOS 软件版本 12.2(35)SE 及更高版本才提供多域身份验证支持。
- 此示例使用Cisco安全接入控制服务器(ACS) 4.1作为RADIUS服务器。**注意：** 您必须先指定 RADIUS 服务器，然后才能在交换机上启用 802.1x。
- 支持 802.1x 认证的 PC 客户端**注意：** 本示例使用 Microsoft Windows XP 客户端。
- 安装了 SCCP 固件版本 8.2(1) 的 Cisco Unified IP 电话 7970G
- 安装了 SCCP 固件版本 8.2(2) 的 Cisco Unified IP 电话 7961G
- 安装了 Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2 的媒体融合服务器 (MCS)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件：

- Cisco Catalyst 3560-E 系列交换机
- Cisco Catalyst 3750 系列交换机
- Cisco Catalyst 3750-E 系列交换机

注意： Cisco Catalyst 3550 系列交换机不支持 802.1x 多域身份验证。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

IEEE 802.1x 标准定义了一个基于客户端-服务器的访问控制和身份验证协议，以限制未经授权的设备通过可公共访问的端口连接到某个 LAN。802.1x 通过在每个端口创建两个不同的虚拟接入点来控制网络访问。一个接入点是非受控端口；另一个是受控端口。通过一个端口的所有流量对两个接入点均可用。802.1x 对连接到交换机端口的每个用户设备进行认证，并在实现该交换机或某个 LAN 所提供的任何服务之前将该端口分配到该 VLAN。在设备通过认证之前，802.1x 访问控制仅允许 LAN 的可扩展身份验证协议 (EAPOL) 数据流通过设备所连接的端口。认证成功后，普通流量可以通过该端口。

802.1x 包括三个主要组件。每个组件被称为端口访问实体 (PAE)。

- 请求方 — 一种可用于请求网络访问的客户端设备，例如 IP 电话及连接的 PC
- 身份验证器 — 一种便于进行请求方授权请求的网络设备，例如 Cisco Catalyst 3560
- 身份验证服务器 — 一种可提供身份验证服务的远程身份验证拨入用户服务器 (RADIUS)，例如 Cisco 安全访问控制服务器

Cisco Unified IP 电话也包含 802.1X 请求方。通过此请求方，网络管理员可以控制 IP 电话与 LAN

交换机端口之间的连接。IP 电话 802.1X 请求方的最初版本实现了用于 802.1X 身份验证的 EAP-MD5 选项。在多域配置中，IP 电话以及所连接的 PC 必须通过指定用户名和口令，以独立方式请求访问网络。身份验证器设备可能会要求用户提供来自 RADIUS 被叫方属性的信息。属性可用于指定其他授权信息，如是否允许请求方访问特定的 VLAN。这些属性可以是供应商特定的属性。Cisco 使用 RADIUS 属性 cisco-av-pair 告知身份验证器 (Cisco Catalyst 3560)，语音 VLAN 上已允许请求方（IP 电话）。

配置

此部分中将提供用于配置本文档中所述的 802.1x 多域身份验证功能的信息。

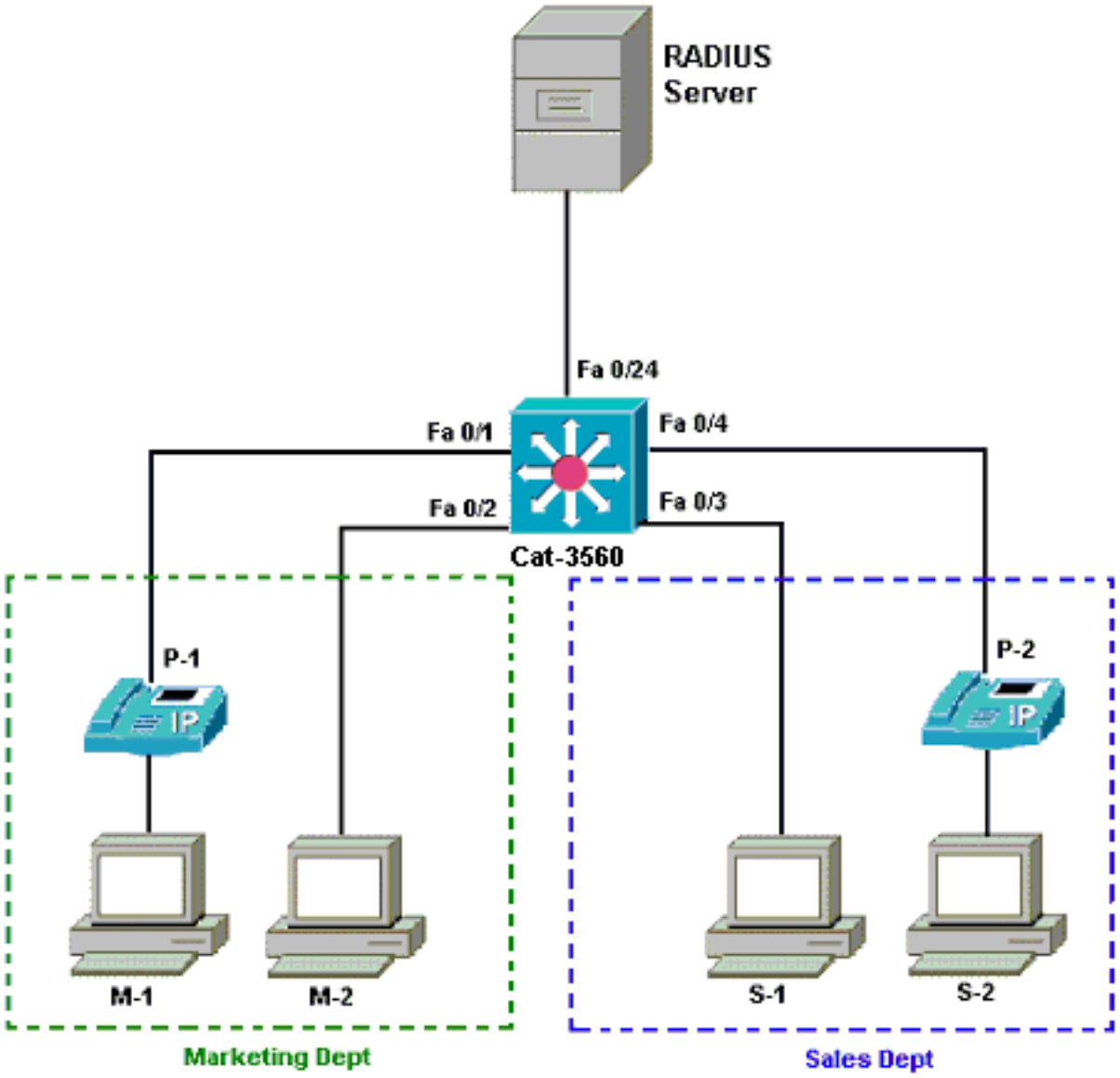
此配置要求执行下列步骤：

- 配置 Catalyst 交换机以进行 802.1x 多域身份验证。
- 配置 RADIUS 服务器。
- 配置 PC 客户端以使用 802.1x 认证。
- 将 IP 电话配置为使用 802.1x 身份验证。

注意： 使用命令查找工具（仅限注册用户）查找有关本文档所使用命令的详细信息。

网络图

本文档使用以下网络设置：



- RADIUS 服务器 — 该服务器将执行客户端的实际身份验证。RADIUS 服务器验证客户端的身份并通知交换机客户端是否获准访问 LAN 和交换机服务。在这里，已在媒体融合服务器 (MCS) 上安装并配置 Cisco ACS 以进行身份验证和 VLAN 分配。MCS 也充当 TFTP 服务器，并可作为 IP 电话的 Cisco Unified Communications Manager (Cisco CallManager)。
- 交换机 — 它可基于客户端身份验证状态控制对网络的物理访问。交换机充当客户端与 RADIUS 服务器之间的中介（代理）。它从客户端请求身份信息，向 RADIUS 服务器验证该信息，并将响应中继至客户端。这里的 Catalyst 3560 交换机还配置为 DHCP 服务器。对动态主机配置协议 (DHCP) 的 802.1x 身份验证支持允许 DHCP 服务器将 IP 地址分配给不同类别的最终用户。为此，它将经过身份验证的用户身份添加到 DHCP 发现过程中。端口 FastEthernet 0/1 和 0/4 是仅有的两个配置用于 802.1x 多域身份验证的端口。端口 FastEthernet 0/2 和 0/3 处于默认的 802.1x 单主机模式。端口 FastEthernet 0/24 连接到 RADIUS 服务器。**注意**： 如果使用的是外部 DHCP 服务器，请确保在 SVI (vlan) 接口上添加 **ip helper-address** 命令。客户端驻留在该接口中，并且该接口指向 DHCP 服务器。
- 客户端 — 这些是请求访问 LAN 和交换机服务并响应交换机请求的设备，例如 IP 电话或工作站。在这里，已将客户端配置为从 DHCP 服务器获取 IP 地址。设备 M-1、M-2、S-1 和 S-2 是可发出网络访问请求的工作站客户端。P-1 和 P-2 是可发出网络访问请求的 IP 电话客户端。M-1、M-2 和 P-1 是市场营销部门的客户端设备。S-1、S-2 和 P-2 是销售部门的客户端设备。IP 电话 P-1 和 P-2 已配置为处于同一语音 VLAN (VLAN 3) 中。工作站 M-1 和 M-2 已配置为在身份验证成功后处于同一数据 VLAN (VLAN 4) 中。工作站 S-1 和 S-2 也已配置为在身份验证成

功后处于同一数据 VLAN (VLAN 5) 中。**注意：** 只能对数据设备使用 RADIUS 服务器的动态 VLAN 分配。

配置 Catalyst 交换机以进行 802.1x 多域身份验证

此示例交换机配置包括：

- 如何在交换机端口上启用 802.1x 多域身份验证
- RADIUS 服务器相关配置
- 用于 IP 地址分配的 DHCP 服务器配置
- 身份验证后将在客户端之间实现连接的 Inter-VLAN Routing

有关 MDA 配置指南的详细信息，请参阅使用多域身份验证。

注意： 确保 RADIUS 服务器始终连接在获得授权的端口后面。

注意： 此处仅显示相关配置。

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
```

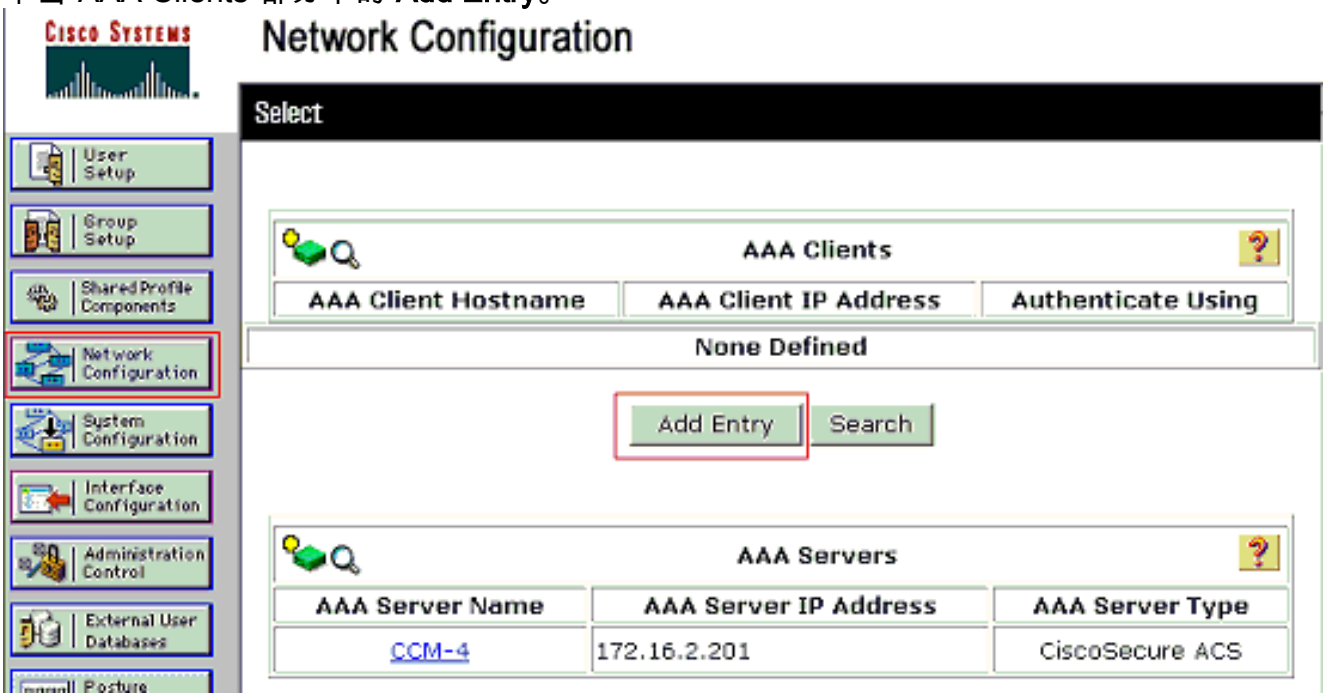
```
act/unsup 1003 token-ring-default act/unsup 1004
fddinet-default act/unsup 1005 trnet-default act/unsup
```

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

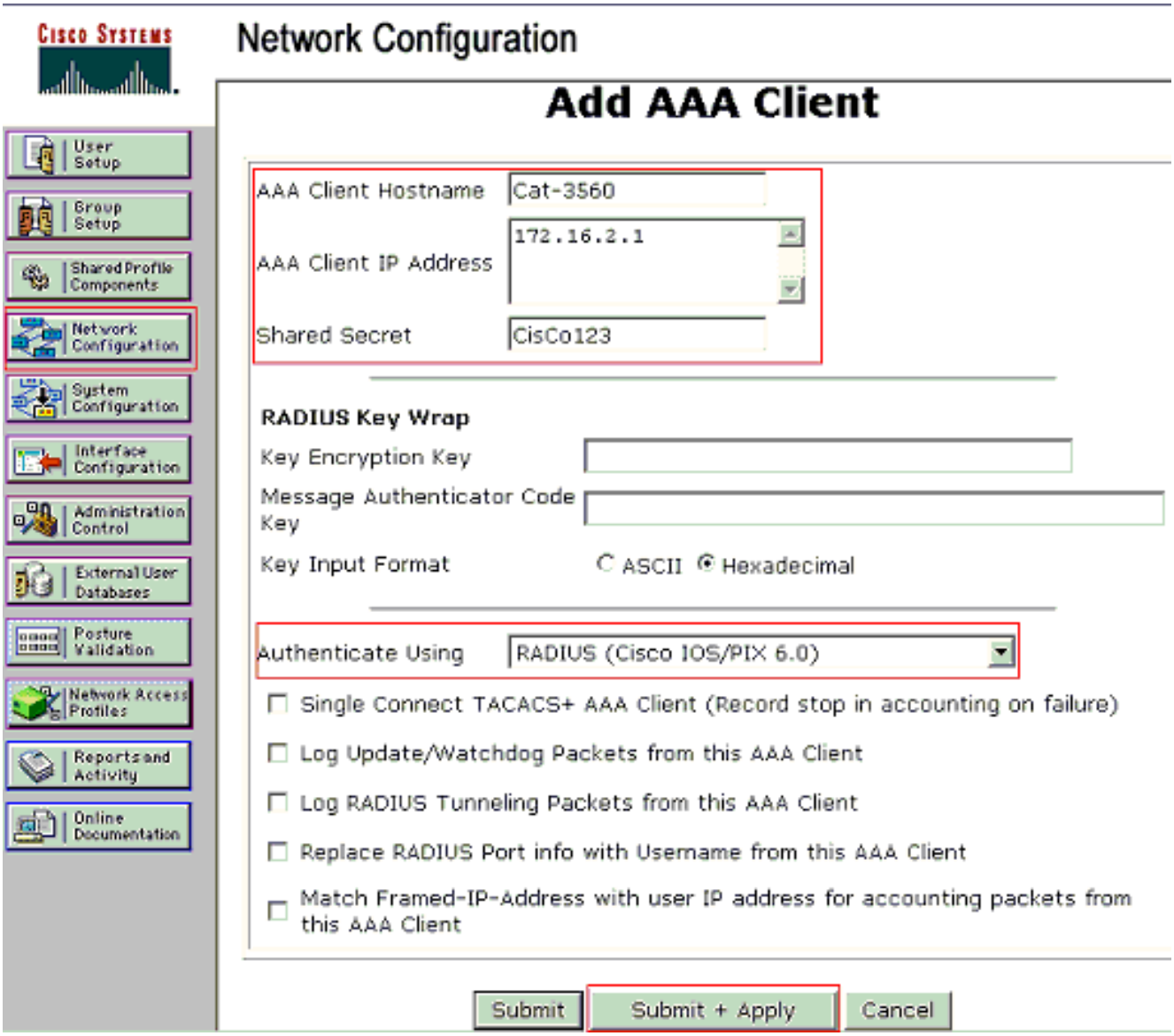
配置 RADIUS 服务器

RADIUS 服务器配置了静态 IP 地址 172.16.2.201/24。完成下列步骤以配置 RADIUS 服务器的 AAA 客户端：

1. 在 ACS 管理窗口中单击 **Network Configuration** 以配置 AAA 客户端。
2. 单击“AAA Clients”部分下的 **Add Entry**。



3. 如下配置 AAA 客户端的主机名、IP 地址、共享密钥和认证类型：AAA client hostname = 交换机主机名 (**Cat-3560**)。AAA Client IP Address = 交换机的管理接口 IP 地址 (**172.16.2.1**)。Shared Secret = 在交换机上配置的 RADIUS 密钥 (**CisCo123**)。**注意：** 要实现正确操作，AAA 客户端和 ACS 上的共享密钥必须相同。密钥区分大小写。Authenticate Using = **RADIUS (Cisco IOS/PIX 6.0)**。**注意：** 此选项下提供了 Cisco 属性/值 (AV) 对属性。
4. 单击 **Submit + Apply** 可使这些更改生效，如下面的示例所示：



组设置

要配置 RADIUS 服务器以进行身份验证，请参阅下表。

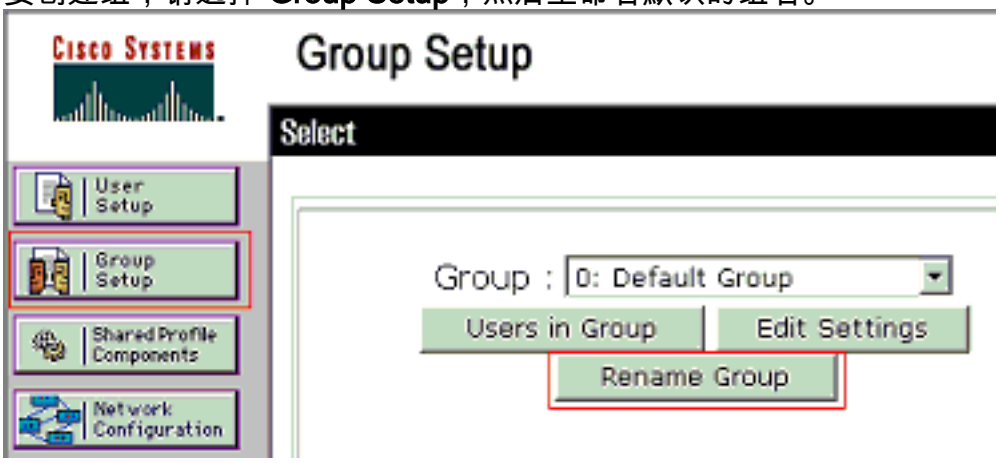
设备	部门	组	用户	密码	VLAN	DHCP 池
M-1	销售	销售	市场营销经理	MMcisco	销售	销售
M-2	销售	销售	mkt-staff	MScisco	销售	销售
S-2	塞尔斯	塞尔斯	销售经理	SMcisco	塞尔斯	塞尔斯
S-1	塞尔斯	塞尔斯	销售人员	SScisco	塞尔斯	塞尔斯

P-1	销售	IP 电话	CP-7970G-SEP001759E7492C	P1cisco	语音	IP 电话
P-2	塞尔斯	IP 电话	CP-7961G-SEP001A2F80381F	P2cisco	语音	IP 电话

请为连接到 VLAN 3 (VOICE)、VLAN 4 (MARKETING) 和 VLAN 5 (SALES) 的客户端创建组。在这里，**IP 电话**、**市场营销**和**销售**组即是为实现此目的而创建的。

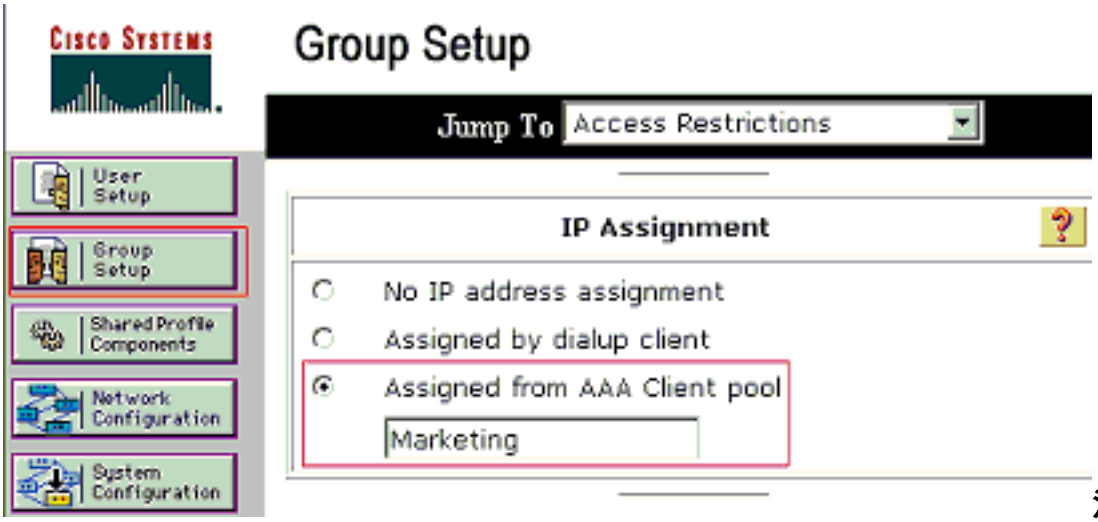
注意： 这是**市场营销**和 **IP 电话**组的配置。对于**销售**组配置，请完成**市场营销**组的步骤。

1. 要创建组，请选择 **Group Setup**，然后重命名默认的组名。



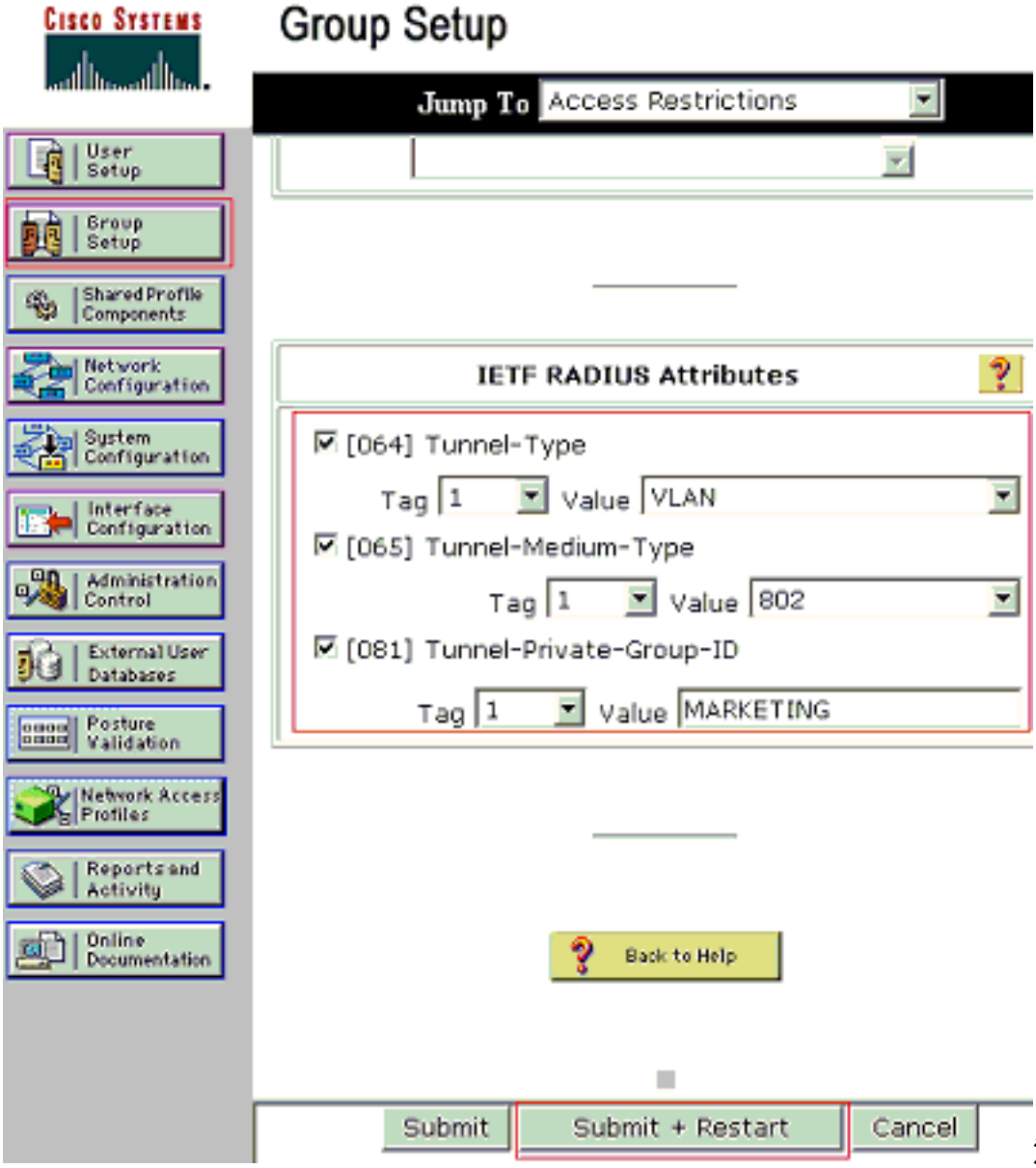
2. 要配置组，请从列表中选择组，然后单击 **Edit Settings**

3. 将客户端 IP 地址分配定义为 **Assigned by AAA client pool**。输入已在该组客户端的交换机上配置的 IP 地址池的名称。



注意： 仅当此用户将获得由 AAA 客户端上配置的 IP 地址池分配的 IP 地址时，才应选择此选项并在框中键入 AAA 客户端 IP 池名称。**注意：** 如果仅配置 **IP 电话**组，则可跳过下一步（即步骤 4），转到步骤 5。

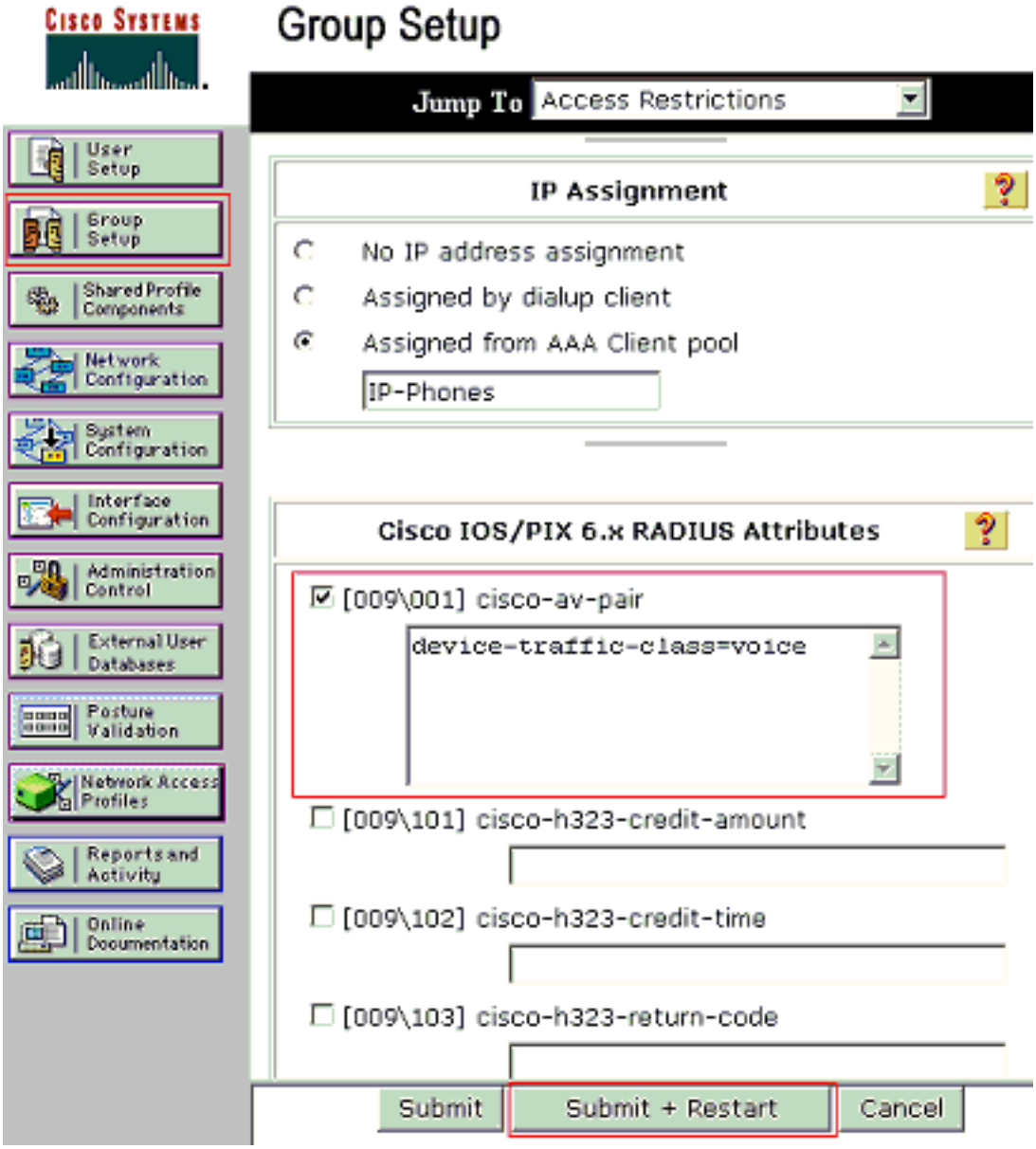
4. 定义 Internet 工程任务组 (IETF) 属性 **64**、**65** 和 **81**，然后单击 **Submit + Restart**。确保将“Values”的“Tags”设置为 **1**，如本例所示。Catalyst 将忽略所有 1 以外的标记。要将用户分配给特定 VLAN，还必须使用对应的 VLAN 名称 或 VLAN 编号 定义属性 **81**。**注意：** 如果使用 VLAN 名称，则该名称应与交换机中配置的名称完全相同。



注意： 请参阅

RFC 2868：用于支持隧道协议的 RADIUS 属性 以获得有关这些 IETF 属性的详细信息。**注意**：在 ACS 服务器的初始配置中，**User Setup** 中可能不会显示 IETF RADIUS 属性。要在用户配置屏幕中启用 IETF 属性，请选择 **Interface configuration > RADIUS (IETF)**。然后，检查 **64**， **65**和**81**在用户和群组栏。**注意**： 如果未定义 IETF 属性 **81** 且端口是处于接入模式的交换机端口，则会将客户端分配给该端口的接入 VLAN。如果为动态 VLAN 分配定义了属性 **81**，且端口是处于接入模式的交换机端口，则需在交换机上发出 **aaa authorization network default group radius** 命令。该命令将端口分配给 RADIUS 服务器提供的 VLAN。否则，802.1x 会在验证用户身份后将该端口转为 AUTHORIZED 状态；但该端口仍然位于端口的默认 VLAN 中，并且连接可能会失败。**注意**： 下一步仅适用于 **IP 电话**组。

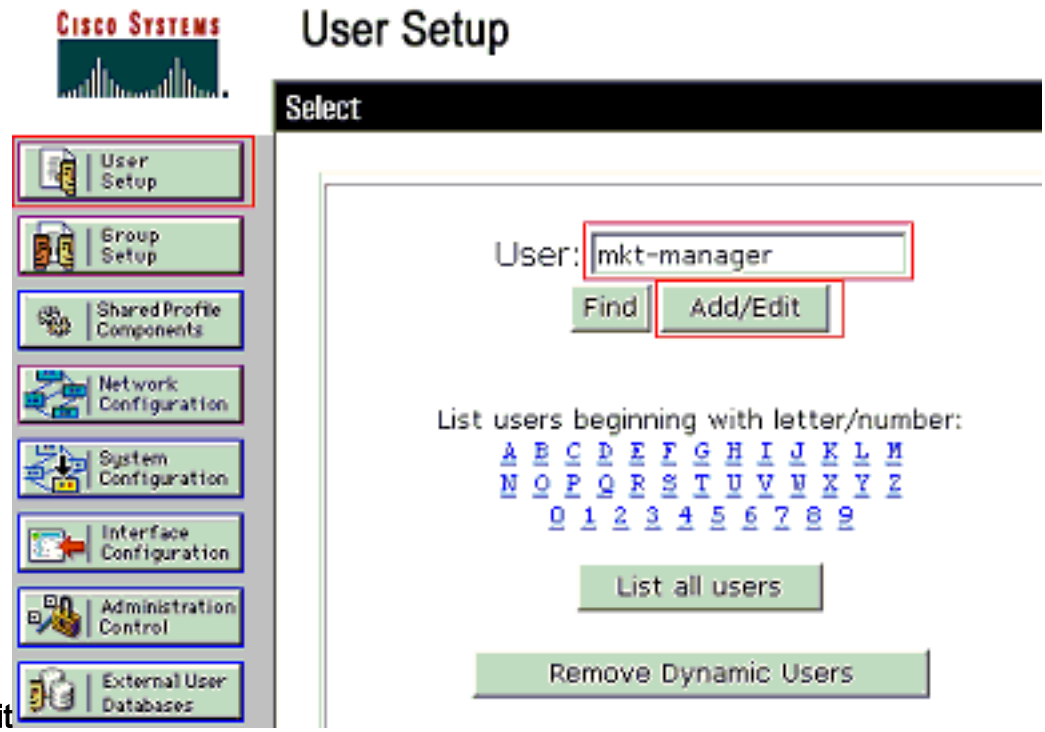
5. 配置 RADIUS 服务器，以便发送 Cisco 属性/值 (AV) 对属性，从而对语音设备授权。如果不进行此配置，交换机会将语音设备视为数据设备。使用值 *device-traffic-class=voice* 定义 Cisco 属性/值 (AV) 对属性，然后单击 **Submit + Restart**。



用户设置

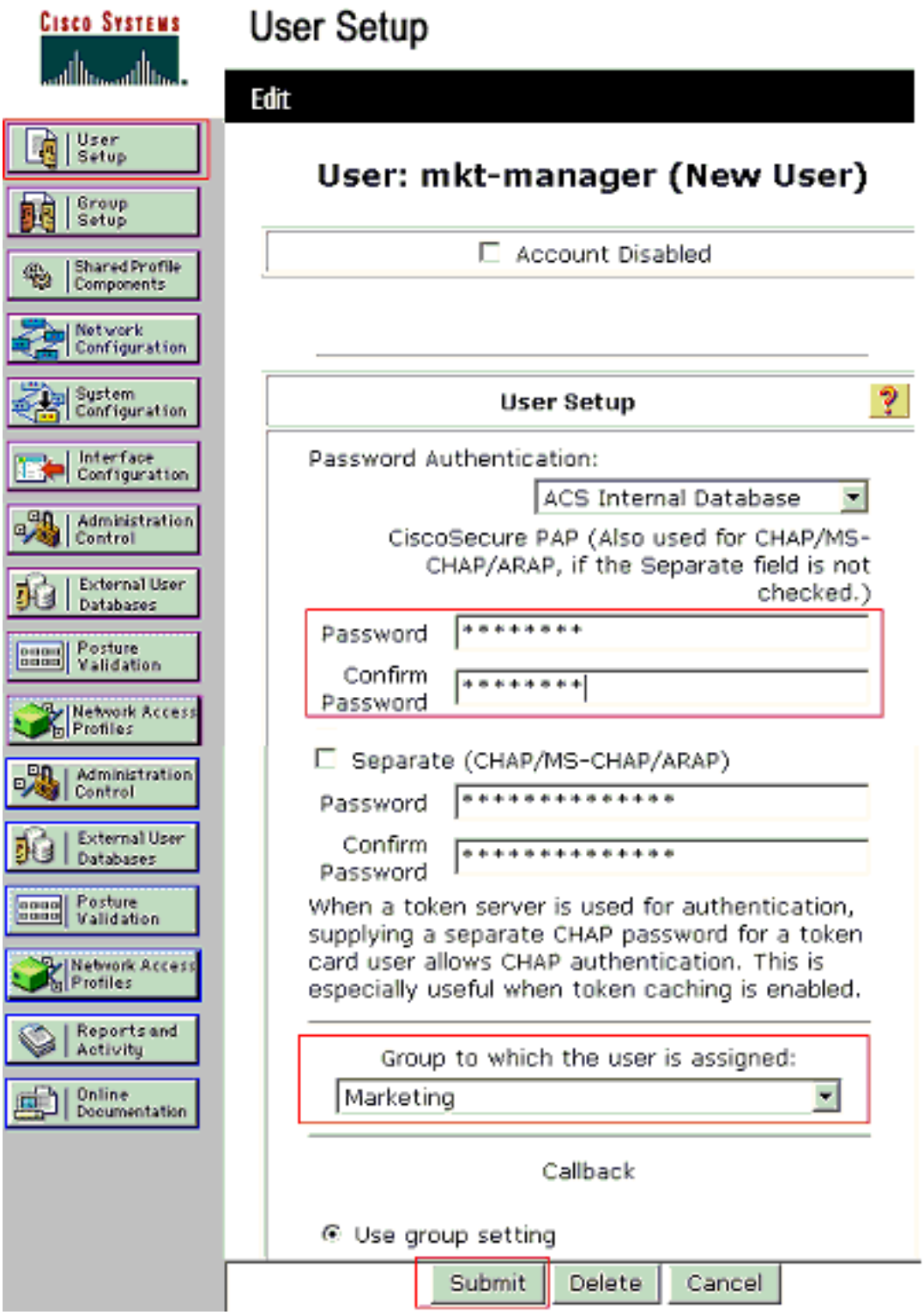
完成以下步骤可添加和配置用户。

1. 要添加和配置用户，请选择 **User Setup**。输入用户名，然后单击

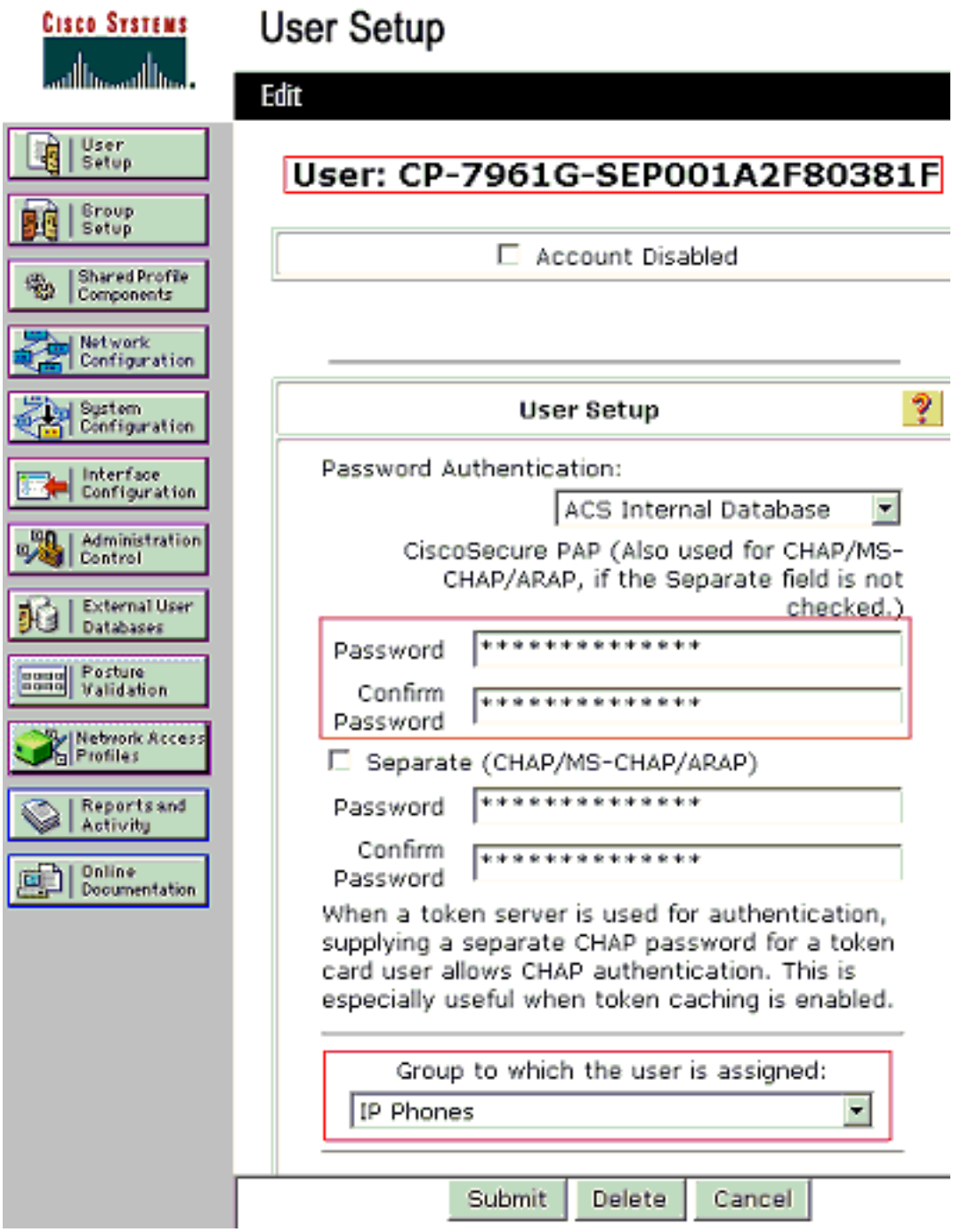


Add/Edit

2. 为用户定义用户名、口令和组。



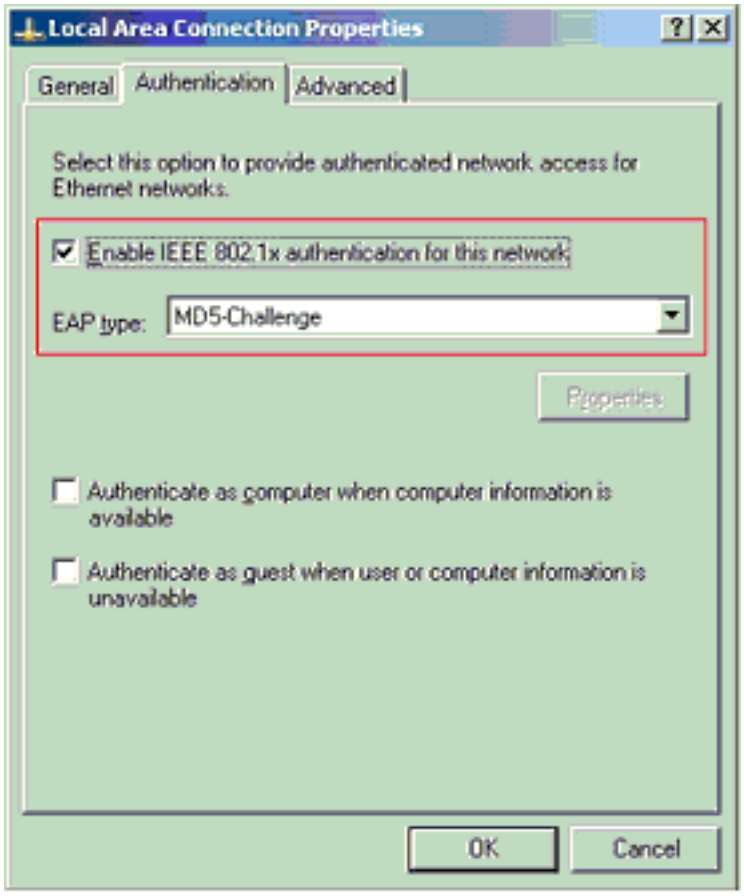
3. IP 电话将使用其设备 ID 作为用户名并使用共享密钥作为口令来进行身份验证。在 RADIUS 服务器上，这些值应该互相匹配。对于 IP 电话 P-1 和 P-2，在创建用户名和口令时，用户名应与设备 ID 相同，口令应与已配置的共享密钥相同。有关 IP 电话的设备 ID 和共享密钥的详细信息，请参阅将 IP 电话配置为使用 802.1x 身份验证部分。



配置 PC 客户端以使用 802.1x 认证

本示例是特定于 Microsoft Windows XP LAN 的可扩展认证协议 (EAPOL) 客户端的：

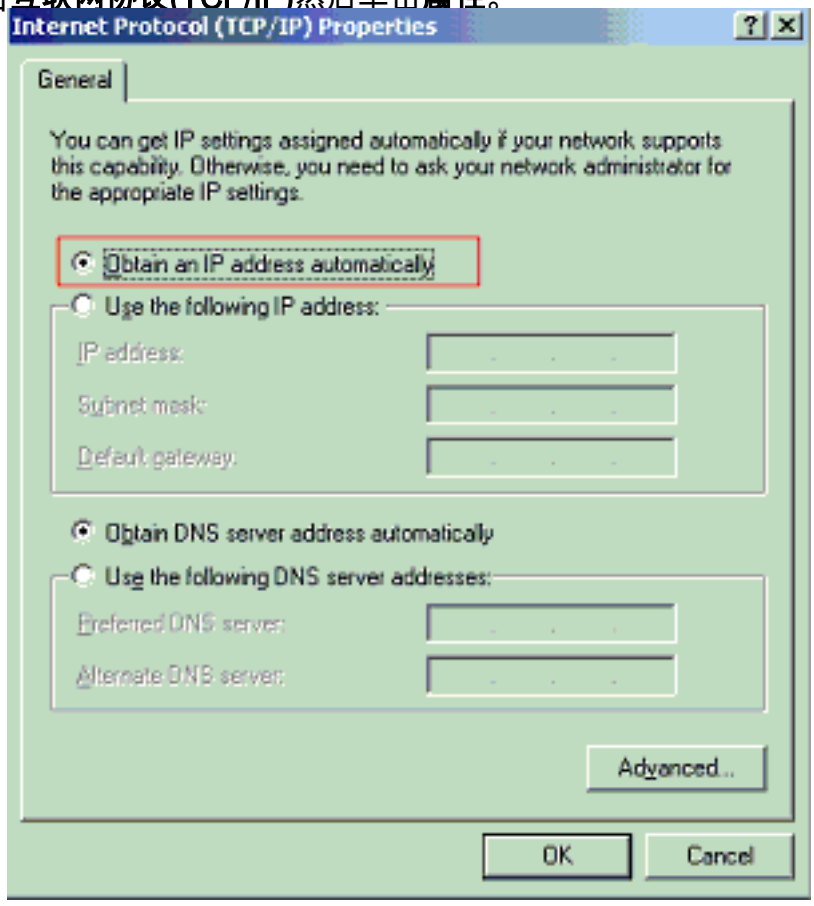
1. 选择**开始 > 控制面板 > 网络连接**，然后右键单击您的**本地连接**并选择**属性**。
2. 在“常规”选项卡下选中**连接后在通知区域显示图标**。
3. 在Authentication选项下，检查**启用此网络的IEEE 802.1X验证**。
4. 将 EAP 类型设置为 **MD5-质询**，如下面的示例所示



:

要将客户端配置为从 DHCP 服务器获取 IP 地址，请完成以下步骤。

1. 选择**开始 > 控制面板 > 网络连接**，然后右键单击您的**本地连接**并选择**属性**。
2. 在常规选项卡下，请单击**互联网协议(TCP/IP)**然后单击**属性**。



3. 选择**自动地获得IP地址**。

将 IP 电话配置为使用 802.1x 身份验证

要配置 IP 电话以进行 802.1x 身份验证，请完成以下步骤。

1. 按 **Settings** 按钮以访问 **802.1X Authentication** 设置，然后选择 **Security Configuration > 802.1X Authentication > Device Authentication**。
2. 将 **Device Authentication** 选项设置为 **Enabled**。
3. 按 **Save** 软键。
4. 选择 **802.1X Authentication > EAP-MD5 > Shared Secret** 以在电话上设置口令。
5. 输入共享密钥，然后按 **Save**。**注意：** 口令必须为 6 到 32 个字符，可以是数字或字母的任意组合。如果不满足此条件，则会显示 That key is not active here 消息，并且不会保存口令。**注意：** 如果禁用 802.1X 身份验证或在电话上执行恢复出厂设置的操作，则会删除以前配置的 MD5 共享密钥。**注意：** 无法配置其他选项、设备 ID 和领域。设备 ID 用作进行 802.1x 身份验证时所使用的用户名。该 ID 是从以下面的格式显示的电话型号和唯一 MAC 地址衍生而来的：CP-<model>-SEP-<MAC>。例如，**CP-7970G-SEP001759E7492C**。有关详细信息，请参阅 802.1X 身份验证设置。

要将 IP 电话配置为从 DHCP 服务器获取 IP 地址，请完成以下步骤。

1. 按 **Settings** 按钮以访问 **Network Configuration** 设置，然后选择 **Network Configuration**。
2. 解除 **Network Configuration** 选项锁定。要解除锁定，请按 ****#**。**注意：** 请不要按 ****#** 来解除选项锁定，然后又立即按 ****#** 来锁定选项。电话会将该序列解释为 ****#*?，这会重置电话。**要在解除选项锁定后锁定这些选项，必须至少等待 10 秒，然后再按 ****#**。
3. 滚动到“DHCP Enabled”选项，然后按 **Yes** 软键以启用 DHCP。
4. 按 **Save** 软键。

验证

使用本部分可确认配置能否正常运行。

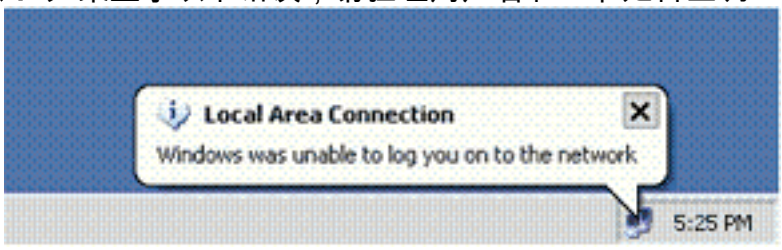
PC 客户端

如果配置已正确完成，PC 客户端将显示一个弹出提示框，提示您输入用户名和口令。

1. 单击该提示框，如下所示： 

此时将显示用户名和口令输入窗口。**注意：** 对于设备身份验证顺序，MDA 没有强制要求。但是，Cisco 建议您在启用了 MDA 的端口上先对语音设备进行身份验证，然后再对数据设备进行身份验证。

2. 输入用户名和密码。
3. 如果未显示错误消息，请采用常用方法验证连接，例如通过使用 ping 命令访问网络资源。**注意：** 如果显示以下错误，请验证用户名和口令是否正确



:

IP 电话

可使用 IP 电话中的 802.1X Authentication Status 菜单监控身份验证状态。

1. 按 **Settings** 按钮访问 802.1X Authentication Real-Time Stats，然后选择 **Security Configuration > 802.1X Authentication Status**。
2. **Transaction Status** 应为 **Authenticated**。有关详细信息，请参阅 802.1X 身份验证实时状态。**注意：** 也可以通过 **Settings > Status > Status Messages** 来验证身份验证状态。

第 3 层交换机

如果口令和用户名看起来正确，请验证交换机上的 802.1x 端口状态。

1. 查找 AUTHORIZED 端口状态。`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 在成功进行认证后验证 VLAN 状态。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. 在成功完成身份验证后，验证 DHCP 绑定状态。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 命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

IP 电话身份验证失败

如果 802.1x 身份验证失败，IP 电话状态将显示 Configuring IP 或 Registering。要对此问题进行故障排除，请执行以下步骤：

- 确认 802.1x 已在 IP 电话上启用。
- 验证您是否已在身份验证 (RADIUS) 服务器上输入设备 ID 作为用户名。
- 确认已在 IP 电话上配置共享密钥。
- 如果已配置共享密钥，请验证您是否在身份验证服务器上输入了相同的共享密钥。
- 验证您是否已对其他必需设备（例如交换机和身份验证服务器）进行了适当的配置。

相关信息

- 配置基于 IEEE 802.1x 端口的身份验证
- 将 IP 电话配置为使用 802.1x 身份验证
- 在 Cisco Catalyst 交换机环境中为 Windows NT/2000 服务器部署 Cisco Secure ACS 的指导原则
- RFC 2868：用于支持隧道协议的 RADIUS 属性
- 运行 Cisco IOS 软件的 Catalyst 6500/6000 IEEE 802.1x 认证示例
- 运行 CatOS 软件的 Catalyst 6500/6000 IEEE 802.1x 认证配置示例
- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems