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

Contents

Introduction

当在适当的语音和数据VLAN时，放置他们多域认证在同一个交换端口允许IP电话和PC验证。本文解释如何配置IEEE 802.1x多域认证(MDA)在Cisco Catalyst层3固定配置交换机。

Prerequisites

Requirements

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

Components Used

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 Series Switch**Note:** 多域认证支持从Cisco IOS Software Release 12.2(35)SE是和以后仅可得到。
- 此示例使用思科安全访问控制服务器(ACS) 4.1作为RADIUS服务器。**Note:** 在交换机前必须指定RADIUS服务器，在您enable (event) 802.1x。
- 支持802.1x认证的PC客户端**Note:** 此示例使用Microsoft Windows XP客户端。
- 与SCCP固件版本8.2(1)的思科统一IP电话7970G
- 与SCCP固件版本8.2(2)的思科统一IP电话7961G
- 媒体收敛服务器(MCS)有Cisco Unified通信管理器的(Cisco CallManager) 4.1(3)sr2

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

相关产品

此配置可能也与这些硬件一起使用：

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

Note: Cisco Catalyst 3550 Series Switch不支持802.1x多域认证。

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

背景信息

IEEE 802.1x标准定义了从连接限制未授权的设备到LAN通过公共可访问的端口的一个客户端服务器基于访问控制和认证协议。802.1x由两个明显的虚拟访问访问接入点的创建控制网络访问在每个端口。一接入点是一个未管制的端口;其他是控制端口。所有数据流通过单个端口对两接入点是可用的。802.1x验证被连接到交换端口的每用户设备并且分配端口到VLAN，在使可用交换机或LAN提供的所有服务前。直到设备验证， 802.1x访问控制通过设备被连接的端口允许仅LAN上的可扩展认证协议(EAPOL)数据流。在认证是成功的以后，正常数据流能穿过端口。

802.1x包括三个主要组件。其中每一指端口访问实体(PAE)。

- 请求方—请求网络访问，例如， IP电话和附上个人计算机的客户端设备
- 证明人—实现请求方授权请求，例如， Cisco Catalyst 3560的网络设备
- 认证服务器—远程认证拨入用户服务(RADIUS)，提供认证业务，例如，思科安全访问控制服务器

Cisco Unified IP电话也包含一802.1X请求方。此请求方允许网络管理员控制IP电话连接到局域网交换端口。IP电话802.1X请求方的最初版本实现802.1X认证的EAP-MD5选项。在多域配置中， IP电话和附上PC必须由用户名和密码的规格独立地请求对网络的访问。证明人设备能要求从RADIUS被呼叫的属性的信息。属性指定另外的授权信息例如对特定VLAN的访问是否允许请求方。这些属性

可以卖方细节。Cisco使用RADIUS属性cisco-av-pair为了告诉证明人(Cisco Catalyst 3560)请求方(IP电话)在语音VLAN允许。

Configure

在此部分，向您介绍信息配置在本文描述的802.1x多域认证功能。

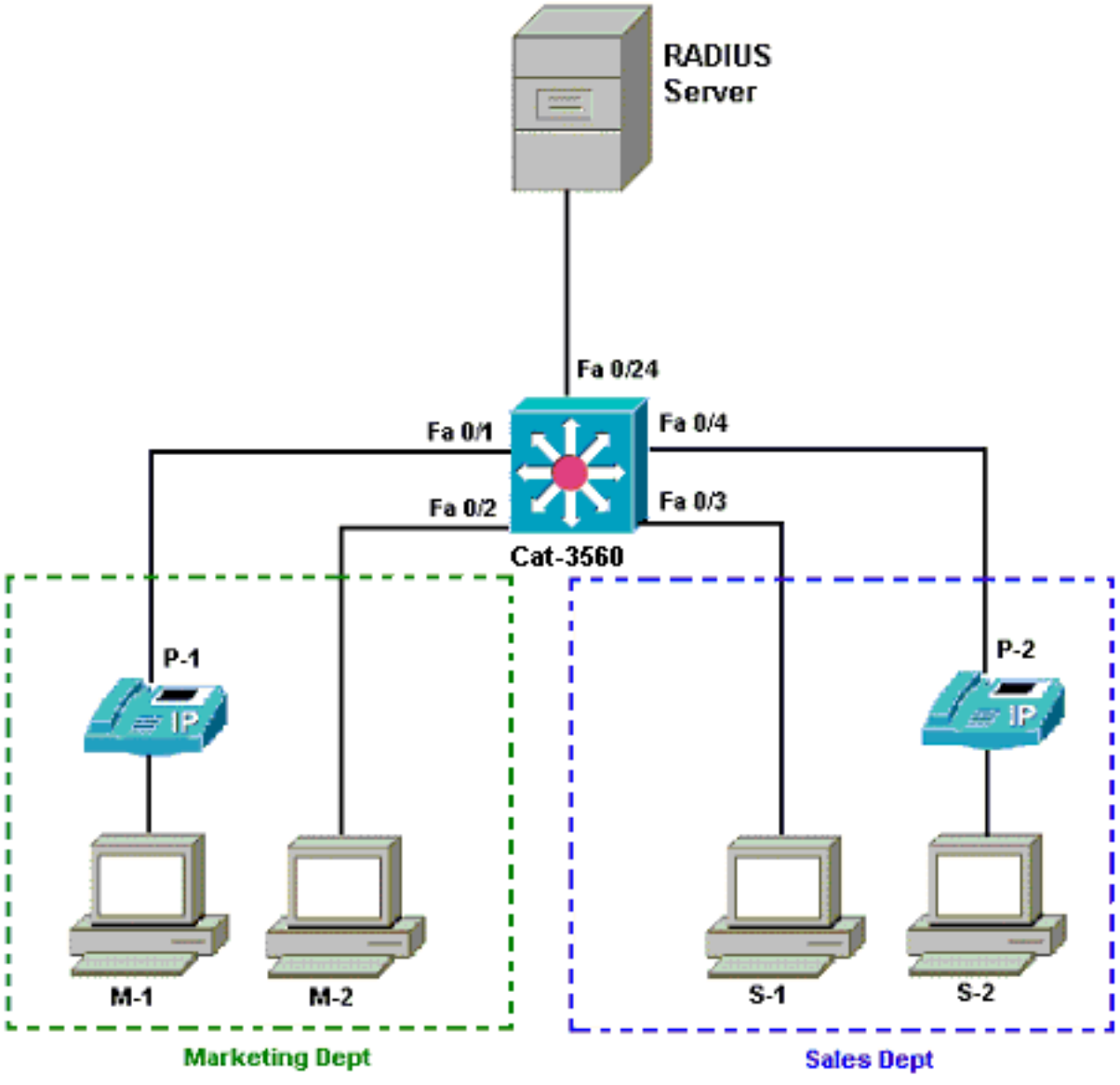
此配置要求执行下列步骤：

- 配置802.1x多域认证的Catalyst交换机。
- 配置RADIUS服务器。
- 配置PC客户端使用802.1x认证。
- 配置IP电话使用802.1x认证。

Note: 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。

Network Diagram

本文档使用以下网络设置：



- RADIUS服务器—这进行客户端的实际认证。RADIUS服务器验证客户端的身份并且通知交换机客户端是否被核准访问LAN和交换服务。这里， Cisco ACS在一个媒体收敛服务器(MCS)安装并且被配置的认证和VLAN分配。MCS也是TFTP server和Cisco Unified通信管理器(Cisco CallManager) IP电话的。
- 交换机—这控制对根据客户端的认证状态的网络的物理访问。交换机作为一中间(代理)在客户端和RADIUS服务器之间。它请求从客户端的身份信息，验证该信息用RADIUS服务器，并且传递对客户端的一种回应。这里， Catalyst 3560 switch也被配置作为DHCP服务器。动态主机配置协议(DHCP)的802.1x认证支持允许DHCP服务器分配IP地址到终端用户不同的组。为了执行此，它添加认证的用户身份到DHCP发现进程。端口FastEthernet0/1和0/4是为802.1x多域认证配置的唯一的端口。端口FastEthernet0/2和0/3在默认802.1x单个主机模式下。端口FastEthernet0/24连接到RADIUS服务器。**Note:** 如果使用一个外部DHCP服务器，请勿忘记添加在SVI (VLAN)接口的**ip helper-address命令**，客户端驻留，指向DHCP服务器。
- 客户端—这些是设备，例如， IP电话或工作站，对LAN和交换机服务的该请求访问并且回答自交换机的请求。这里，配置客户端为了获得从DHCP服务器的IP地址。设备M-1、M-2、S-1和S-2是要求对网络的访问的工作站客户端。P-1和P-2是要求对网络的访问的IP电话客户端。M-1、M-2和P-1是客户端设备在营销部门中。S-1、S-2和P-2是客户端设备在销售部中。配置IP电话P-1和P-2在同样语音VLAN (VLAN 3)。配置工作站M-1和M-2在同样数据VLAN (在一个成功的验证以后的VLAN 4)。也配置工作站S-1和S-2在同样数据VLAN (在一个成功的验证以后的VLAN 5)。**Note:** 您能仅使用从RADIUS服务器的动态VLAN分配数据装置。

配置802.1x多域认证的Catalyst交换机

此示例交换机配置包括：

- 如何对enable (event) 802.1x在交换端口的多域认证
- RADIUS服务器相关的配置
- IP地址分配的DHCP服务器配置
- VLAN间路由有客户端之间的连接在认证以后

请参见使用多域认证关于关于怎样的指南的更多信息配置MDA。

Note: 切记RADIUS服务器在一个被核准的端口后总是连接。

Note: 仅相关配置显示得这里。

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
```

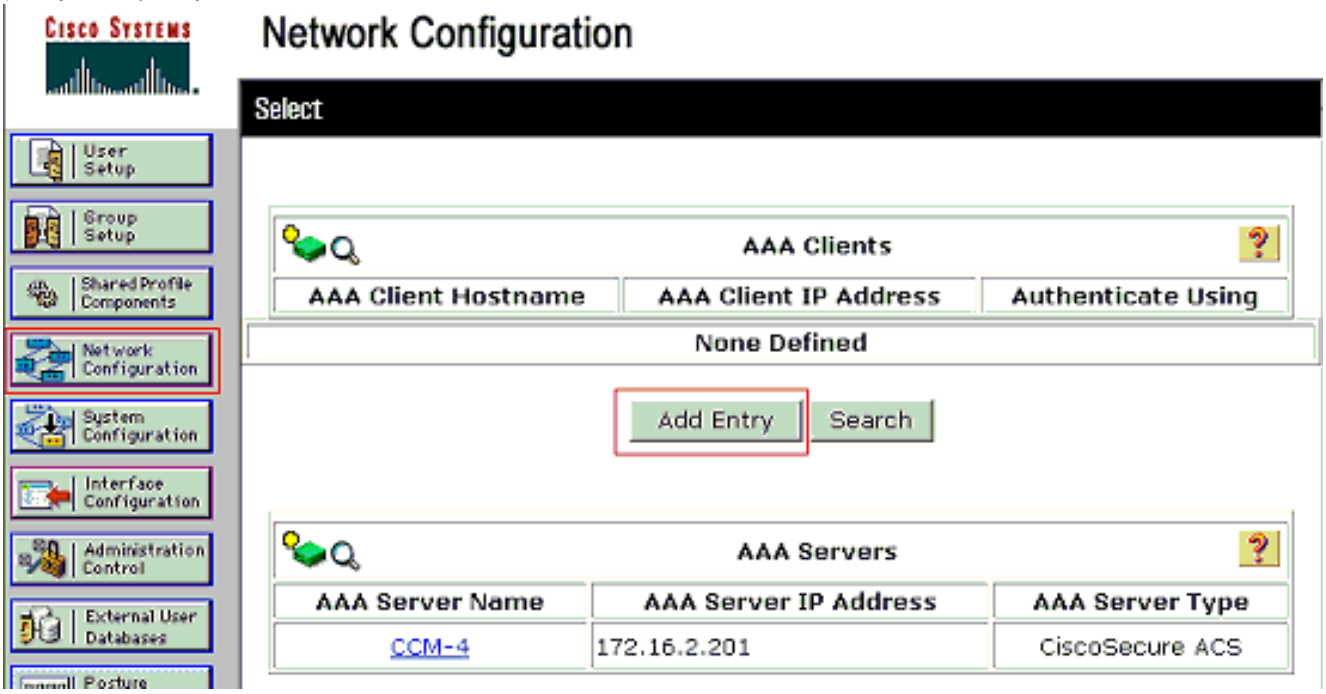
```
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- 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
```

Note: 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。

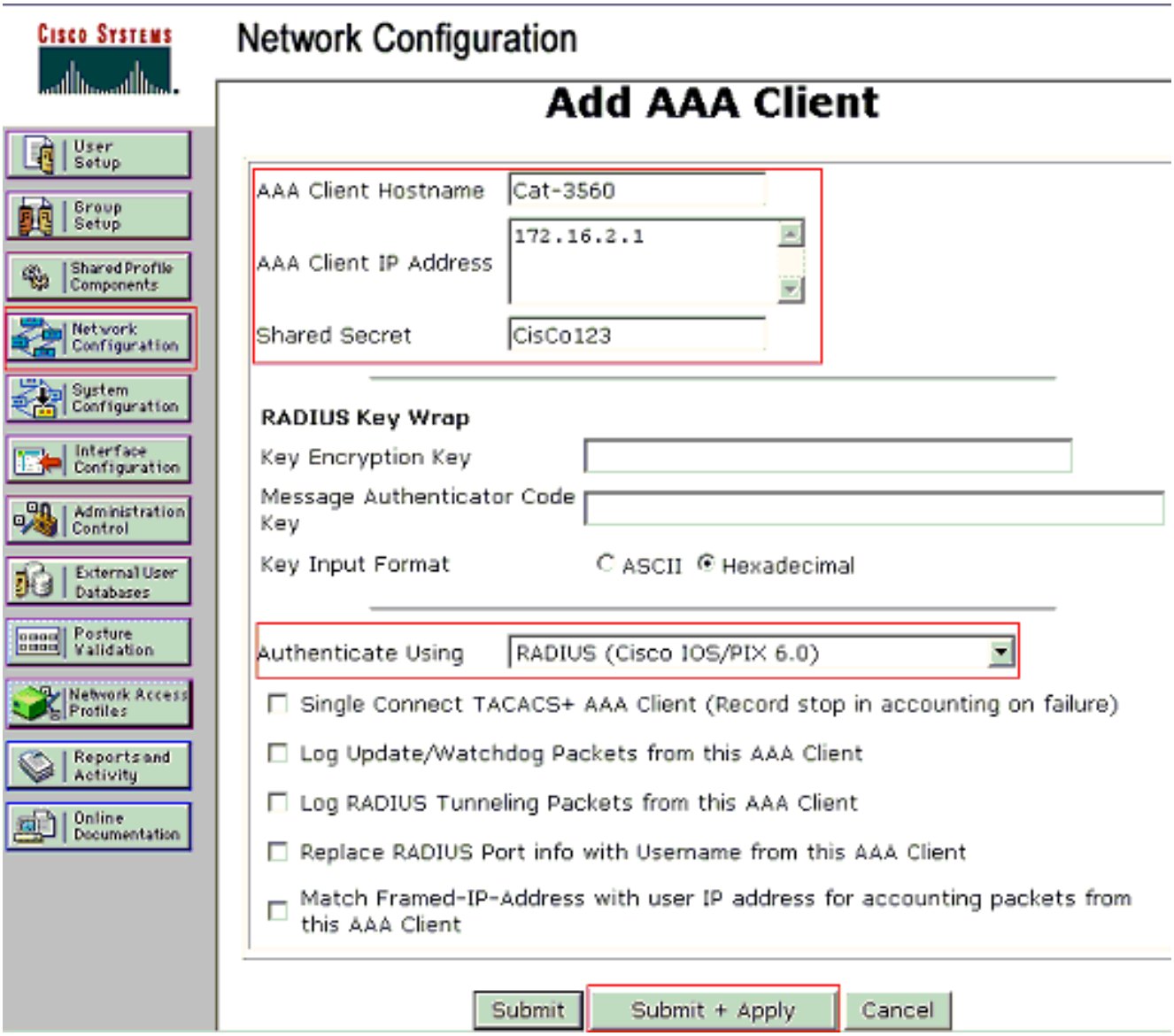
配置RADIUS服务器

RADIUS服务器配置有静态IP地址172.16.2.201/24。完成这些步骤为了配置AAA客户端的RADIUS服务器：

1. 点击在ACS管理窗口的**网络配置**为了配置AAA客户端。
2. 点击**Add条目**在AAA clients部分下。



3. 配置AAA客户端主机名-， IP地址、被共享的密钥和认证类型如下：AAA客户端主机名- =交换机主机名(**Cat-3560**)。AAA交换机(**172.16.2.1**)的客户端IP地址=管理接口IP地址。共有的秘密=在交换机配置的RADIUS键(**Cisco123**)。**Note:** 对于正确的操作，被共享的密钥一定是相同的在AAA客户端和ACS。键区分大小写。验证使用= **RADIUS (Cisco IOS/PIX 6.0)**。**Note:** Cisco attribute-value (AV)对属性是可用的在此选项下。
4. 点击**Submit+Apply**为了做这些变动有效，此示例显示
   ：



组建立

请参见此表为了配置认证的RADIUS服务器。

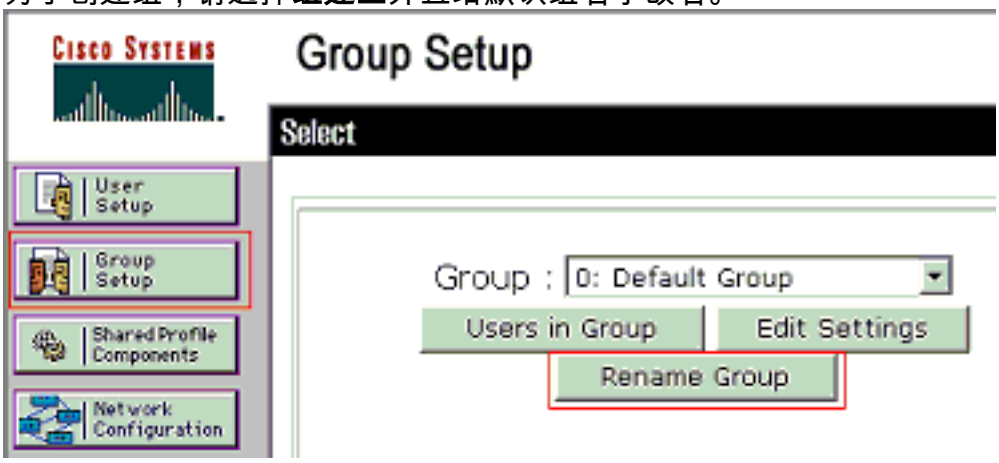
设备	部门	组	用户	密码	VLAN	DHCP池
M-1	销售	销售	市场管理人员	MMcisco	销售	销售
M-2	销售	销售	mkt-staff	MScisco	销售	销售
S-2	销售额	销售额	销售经理	SMcisco	销售额	销售额
S-1	销售额	销售额	销售人员	SScisco	销售额	销售额

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

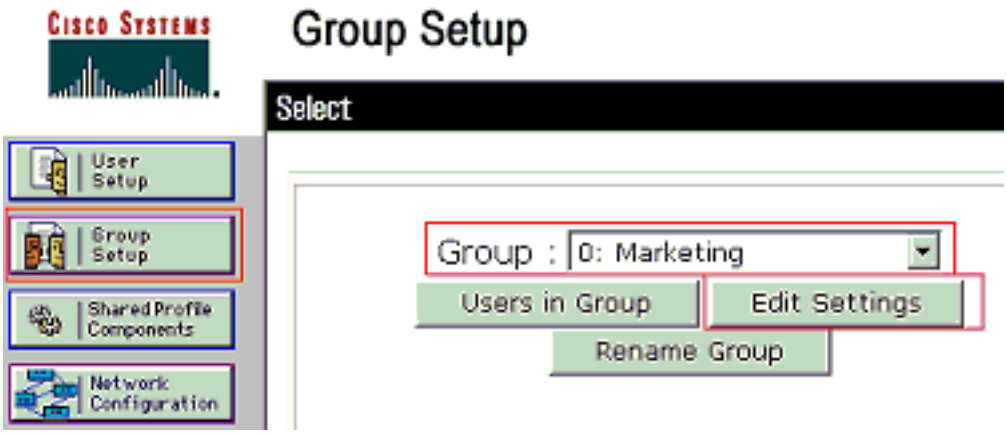
创建连接到VLAN 3的客户端的组(语音)， 4 (营销)和5 (销售额)。这里，组**IP电话**、**营销**和**销售额**为此被创建。

Note: 这是**营销**和**IP电话**组的配置。对于**销售额**组配置，请完成营销人员的步骤。

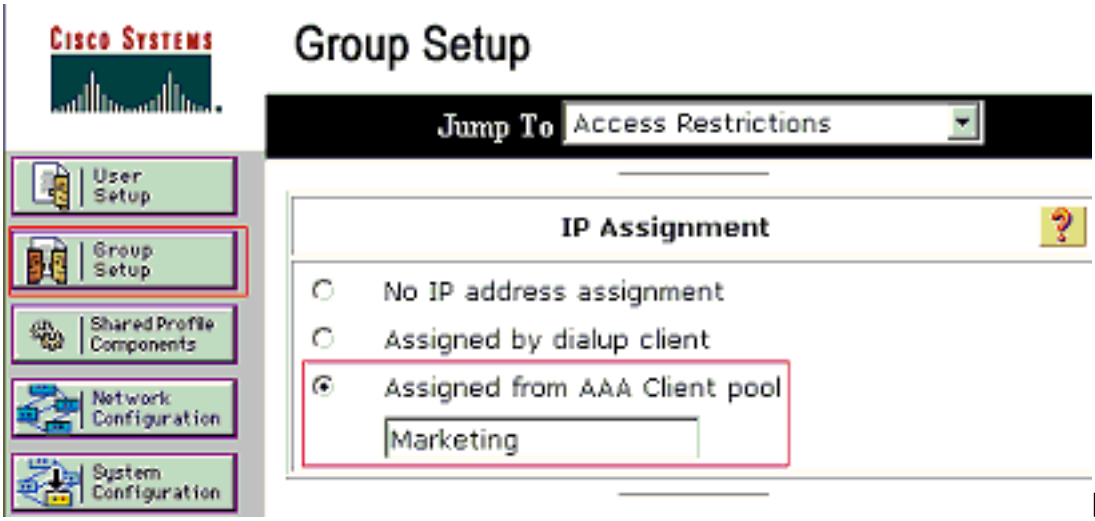
1. 为了创建组，请选择**组建立**并且给默认组名字改名。



2. 为了配置组，从列表选择组和点击**编辑设置**

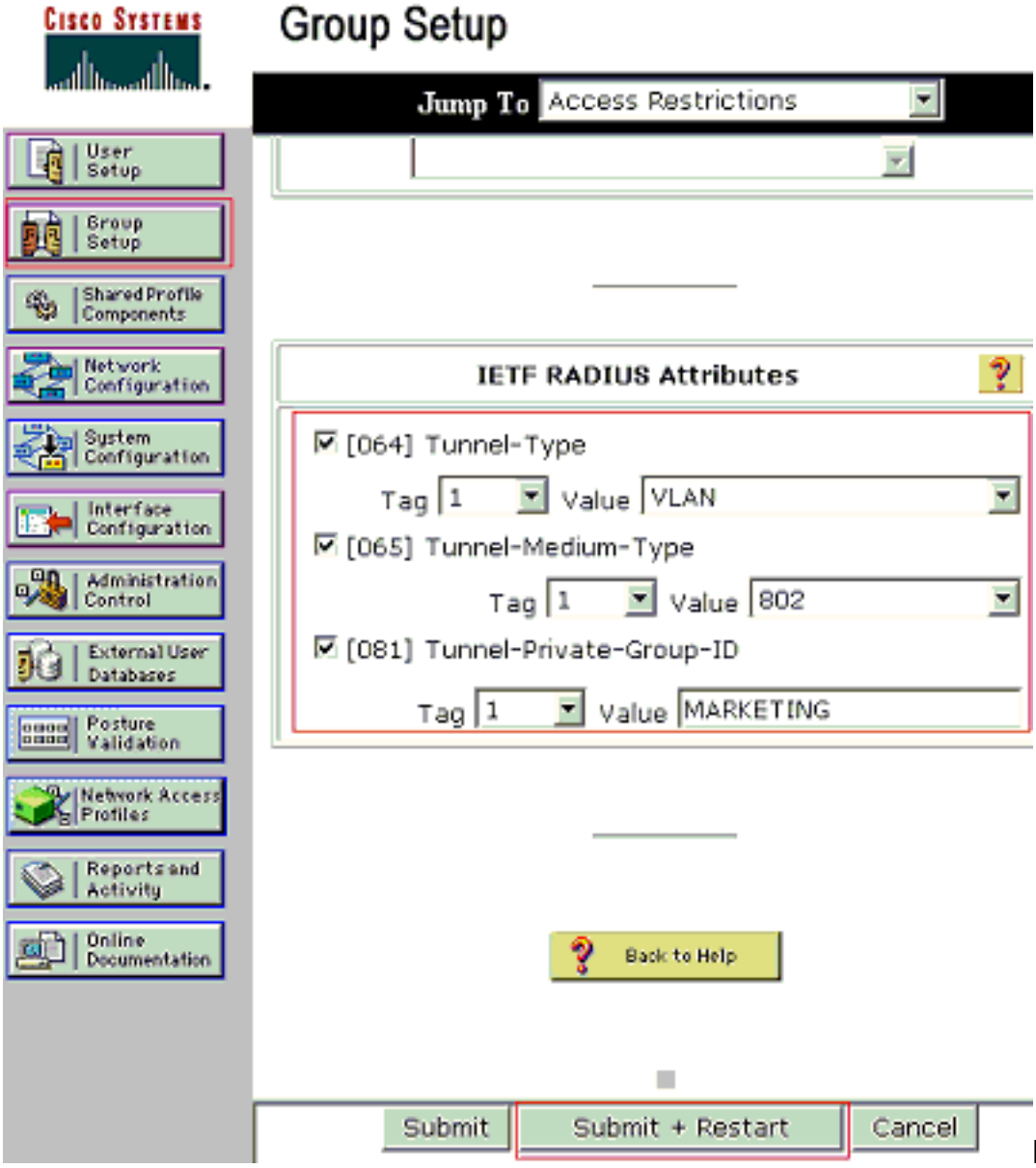


3. 定义客户端IP地址分配如**分配由AAA客户端池**。输入在此组客户端的交换机配置的IP地址池的



名字。**Note:** 只有如果此用户将安排IP地址分配由在AAA客户端，配置的IP地址池请选择此选项并且键入在机箱的AAA客户端IP池名字。**Note:** 对于**IP电话**单独组配置，请跳过下一步，第4步，并且进入步骤5。

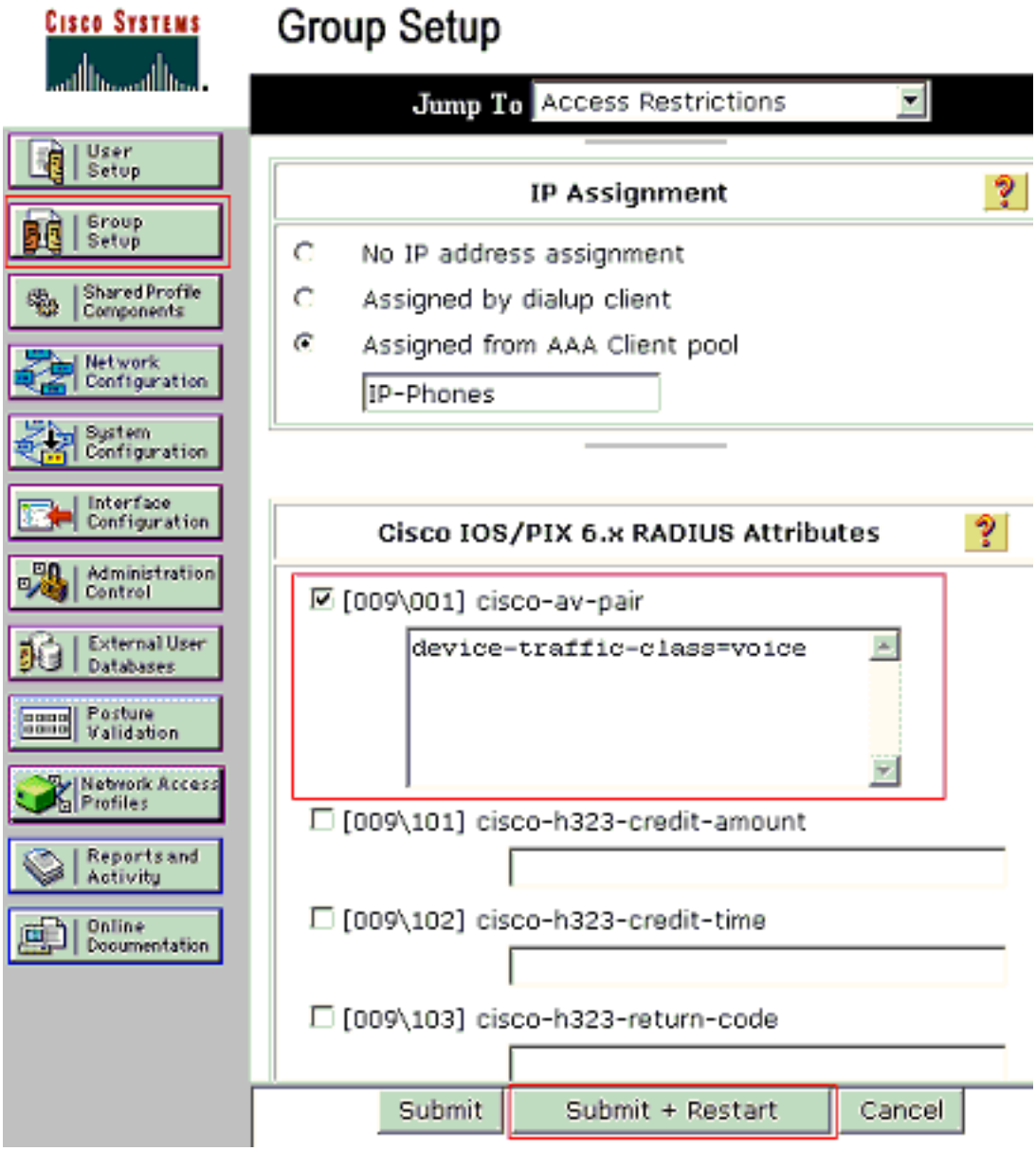
4. 定义互联网工程任务组(IETF)属性**64**， **65**和**81**然后点击**Submit+Restart**。切记值的标记设置到**1**，因为此示例显示。Catalyst忽略所有标记除1.之外为了分配用户到特定VLAN，您必须也定义属性**81**用对应的VLAN名称或VLAN号。**Note:** 如果使用VLAN名称，应该正确地是同在交换机配置的那个一样。



Note: 参考RFC

2868 ：隧道协议技术支持的RADIUS属性 关于这些IETF属性的更多信息。**Note:** 在ACS服务器的初始配置中， IETF RADIUS属性在**用户设置**可以不能显示。为了enable (event)在用户配置屏幕的IETF属性，选择**接口配置> RADIUS (IETF)**。然后，在用户和组列的检查属性**64**，**65**和**81**。**Note:** 如果不定义了IETF属性**81**，并且端口是在接入模式的一个交换端口，客户端被分配到端口的访问VLAN。如果定义了动态VLAN分配的属性**81**，并且端口是在接入模式的一个交换端口，您需要发出**AAA授权网络默认值group radius命令**在交换机。此命令分配端口到该的VLAN RADIUS服务器提供。否则， 802.1x移动端口向`Authorized State`在用户的认证以后;但是端口仍然在端口的默认VLAN，并且连接可以发生故障。**Note:** 下一步只是可适用的对**IP电话**组。

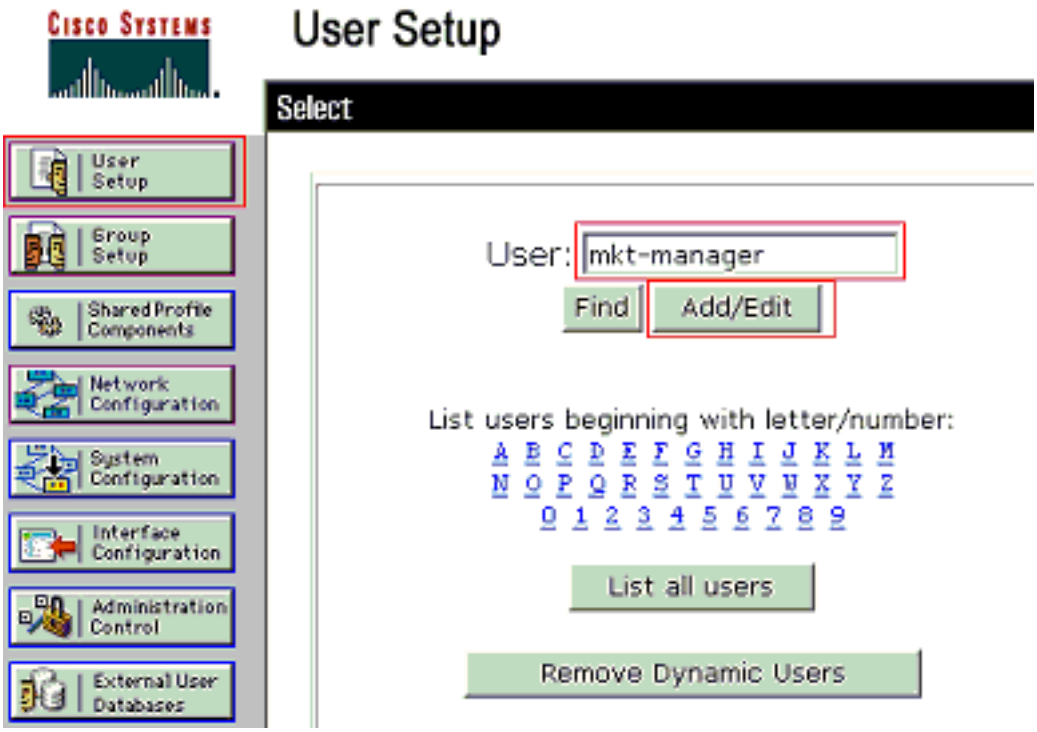
5. 配置RADIUS服务器发送Cisco attribute-value (AV)对属性核准语音设备。没有此，交换机对待语音设备作为数据装置。定义Cisco attribute-value (AV)与*device-traffic-class=voice*的值的对属性并且点击**Submit+Restart**。



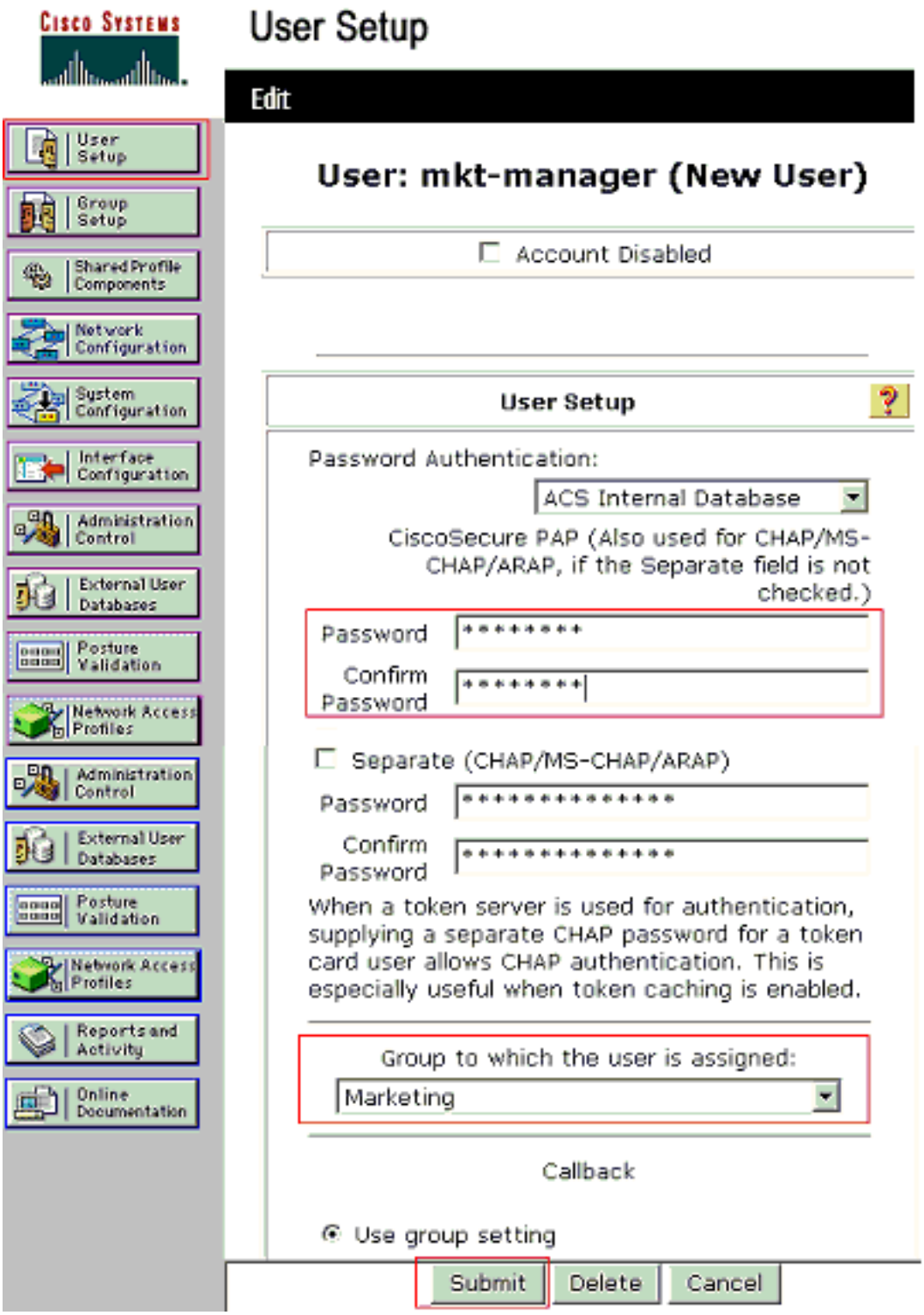
用户设置

完成这些步骤为了添加和配置用户。

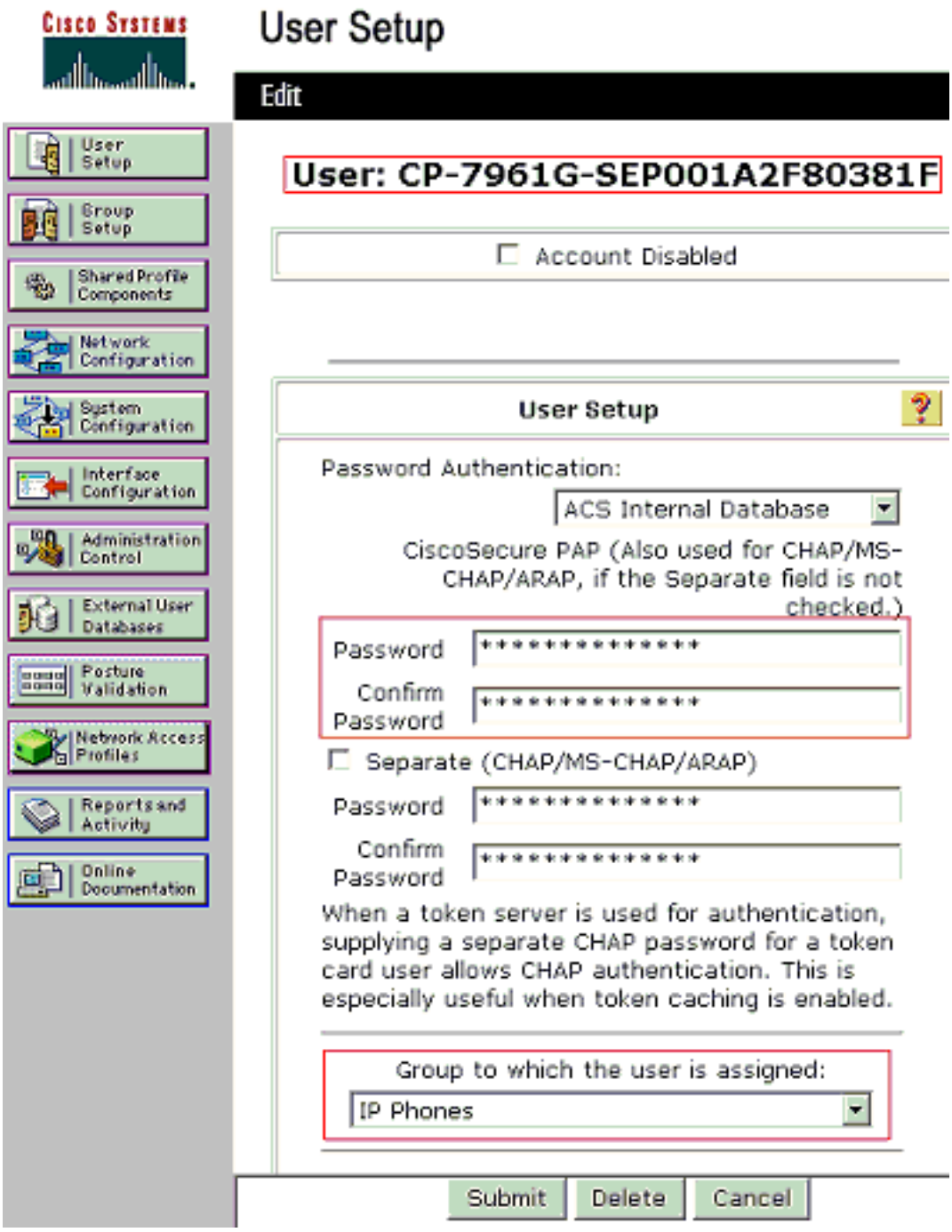
1. 为了添加和配置用户，请选择**用户设置**。输入用户名并且点击**添加/编辑**



2. 定义用户名、密码和组用户的。



3. IP电话使用其设备ID作为用户名和共有的秘密作为密码认证。这些值在RADIUS服务器应该配比。对于IP电话P-1和P-2请创建用户名同他们的设备ID和密码一样同被配置的共有的秘密一样。请参阅[配置IP电话使用802.1x Authentication部分]关于设备ID和共有的秘密的更多信息在

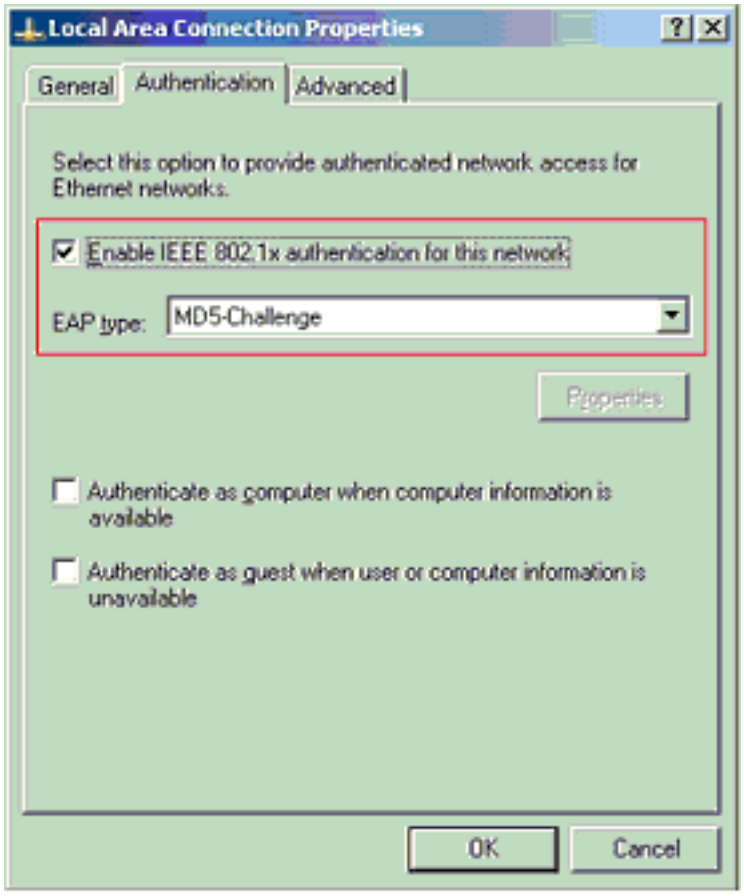


IP电话。

配置PC客户端使用802.1x认证

此示例是特定的对在LAN (EAPOL)客户端的Microsoft Windows XP可扩展的认证协议(EAP) ：

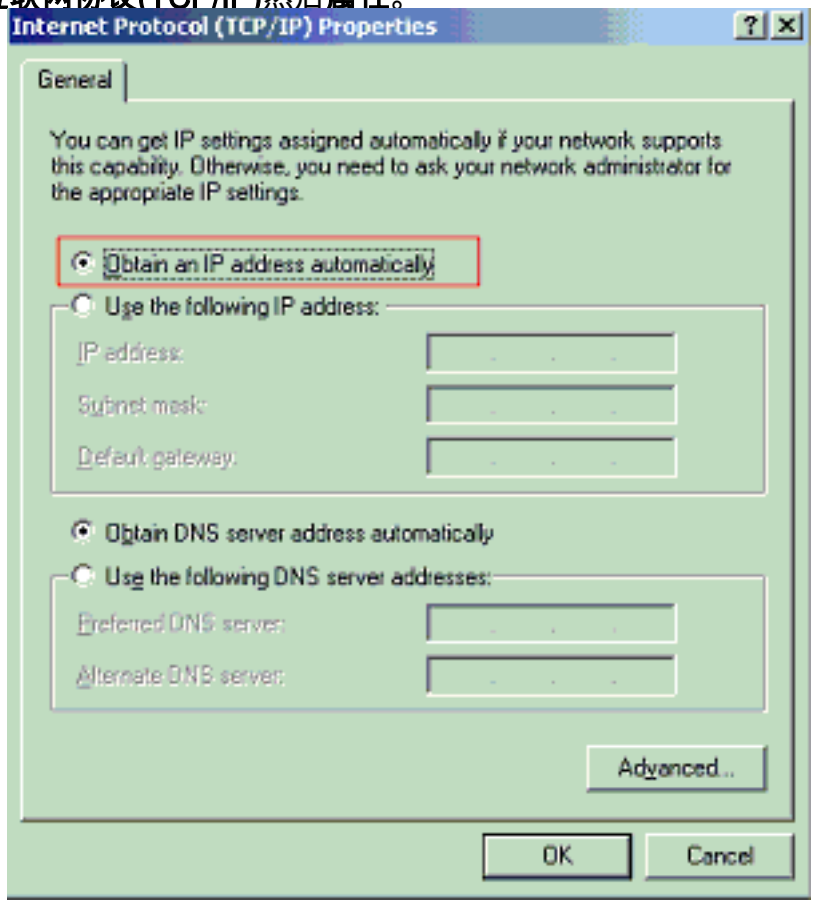
1. 选择**Start > Control Panel > Network Connections**，然后用鼠标右键单击在您**本地区域的连接**并且选择**属性**。
2. 检查**在通知区域显示图标，当连接**在一般选项下。
3. 在Authentication选项下，请检查**Enable (event) IEEE 802.1X验证此网络**。
4. 设置EAP类型为**信息-摘要算法**，此示例显示



:

完成这些步骤为了配置客户端获得从DHCP服务器的IP地址。

1. 选择**Start > Control Panel > Network Connections**，然后用鼠标右键单击在您**本地区域的连接**并且选择**属性**。
2. 在一般选项下，请点击**互联网协议(TCP/IP)**然后**属性**。



3. 选择**自动地获得IP地址**。

配置IP电话使用802.1x认证

完成这些步骤为了配置802.1x认证的IP电话。

1. 按**Settings按钮**为了访问**802.1X认证**设置和选择**安全配置> 802.1X认证>设备验证**。
2. 设置**设备验证**选项对**启用**。
3. 按**保存**Softkey。
4. 选择**802.1X认证> EAP-MD5 >共有的秘密**为了设置在电话的一个密码。
5. 输入共有的秘密并且按**保存**。**Note:** 密码必须在六个和32个字符之间，包括编号或字母的所有组合。消息显示，并且密码没有被保存，如果此情况不是满足的。**Note:** 如果在电话禁用802.1X认证或执行出厂重置，早先配置的MD5共有的秘密被删除。**Note:** 不可能配置其它选项、设备ID和领域。设备ID使用作为用户名802.1x认证。这是以此格式和唯一的MAC地址的显示的衍生商品电话的型号：CP-<model>-SEP-<MAC>。例如， **CP-7970G-SEP001759E7492C**。参考802.1X认证设置欲知更多信息。

完成这些步骤为了配置IP电话获得从DHCP服务器的IP地址。

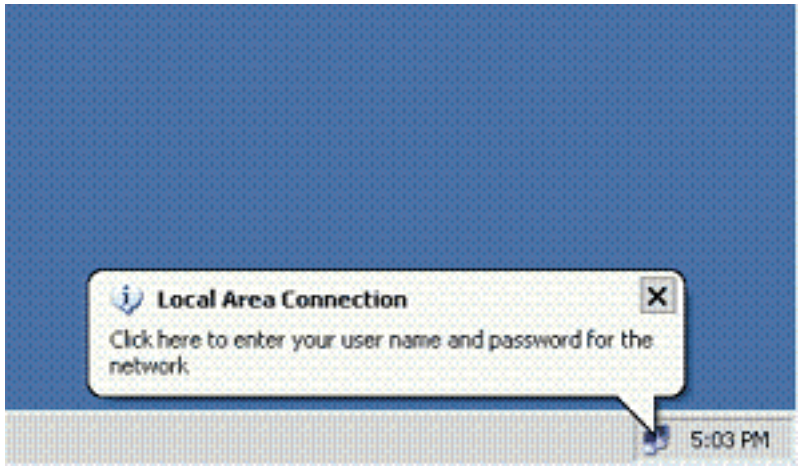
1. 按**Settings按钮**为了访问**网络配置**设置和选择**网络配置**。
2. 打开**网络配置**选项。为了开锁，请按**** #。**Note:** 请勿按**** #为了打开选项立即然后按**** #再为了锁定选择。电话解释此顺序和**** # ****，重置电话。为了锁定选择，在您打开他们后，等待至少10秒，在您按前**** #再。
3. 移动到启用DHCP选项并且按**是**Softkey为了enable (event) DHCP。
4. 按**保存**Softkey。

Verify

Use this section to confirm that your configuration works properly.

PC客户端

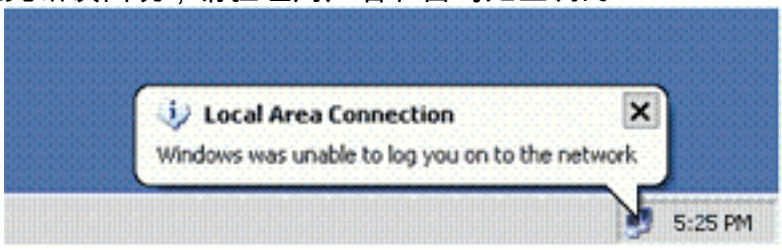
如果正确地完成了配置， PC客户端显示一个弹出式提示输入用户名和密码。

1. 点击提示，此示例显示： 

用户名和密码条目窗口显示。**Note:** MDA不强制执行设备验证顺序。但是，对于最佳的结果， Cisco建议语音设备在MDA可用的端口的数据装置前验证。

2. 输入用户名和密码。
3. 如果错误信息没出现，请验证连接与通常方法，例如网络资源的通过访问和与ping。**Note:** 如果此错误出现，请验证用户名和密码是正确的

:



IP电话

802.1X认证Status菜单在IP电话准许监控认证状态。

1. 按**Settings按钮**为了访问802.1X认证实时Stats和选择**安全配置> 802.1X认证状态**。
2. 应该**验证事务处理状态**。请参见802.1X认证实时状态欲知更多信息。**Note:** 认证状态可能从**设置>状态>状态消息**也被验证。

第3层交换机

如果密码和用户名看来是正确的，请验证在交换机的802.1x端口状态。

1. 寻找指示端口状态。

```
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
```

在成功的验证以后验证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. 在一个成功的验证以后验证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。

Troubleshoot

IP电话认证发生故障

IP电话状态显示IP或，如果802.1x认证发生故障。完成这些步骤为了排除此故障发出：

- 确认802.1x在IP电话被启用。
- 验证您有在认证(RADIUS)服务器输入的设备ID作为用户名。
- 确认共有的秘密在IP电话被配置。
- 如果配置共有的秘密，请验证您有在认证服务器输入的同一个共有的秘密。
- 验证您适当配置其他必需的设备，例如，交换机和认证服务器。

Related Information

- 配置IEEE 802.1x基于端口的认证
- 配置IP电话使用802.1x认证
- Cisco Secure ACS的配置指南Windows NT/2000服务器的在Cisco Catalyst交换机环境里
- RFC 2868 ：隧道协议技术支持的RADIUS属性
- IEEE 802.1X验证用运行Cisco IOS软件配置示例的Catalyst 6500/6000
- IEEE 802.1X验证用运行CatOS软件配置示例的Catalyst 6500/6000
- LAN 产品支持页
- LAN 交换技术支持页
- Technical Support & Documentation - Cisco Systems