运行 CatOS 软件的 Catalyst 6500/6000 IEEE 802.1x 认证配置示例

目录

简介

本文档说明如何在以混合模式运行（在 Supervisor 引擎上运行 CatOS，在 MSFC 上运行 Cisco IOS® 软件）的 Catalyst 6500/6000 上配置 IEEE 802.1x，以及如何配置 Remote Authentication Dial-In User Service (RADIUS) 服务器的认证和 VLAN 分配。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 在 Supervisor 引擎上运行 CatOS 软件版本 8.5(6) 并在 MSFC 上运行 Cisco IOS 软件版本 12.2(18)SXF 的 Catalyst 6500**注意：** 您需要有 CatOS 版本 6.2 或更高版本，才能支持 802.1x 基于端口的认证。**注意：** 如果软件版本低于 7.2(2)，则一旦对 802.1x 主机进行认证，它便会加入经过 NVRAM 配置的 VLAN。使用软件版本 7.2(2) 和更高版本，802.1x 主机在进行认证后可以从 RADIUS 服务器收到其 VLAN 分配。
- 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：** 必须先指定 RADIUS 服务器，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。

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。

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认证协议，用于限制未经授权的设备通过公共访问端口连接到某个 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 (EAPOL) 流量的可扩展的认证协议 (EAP) 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。

配置

本部分将提供有关如何配置本文档中所述的 802.1x 功能的信息。

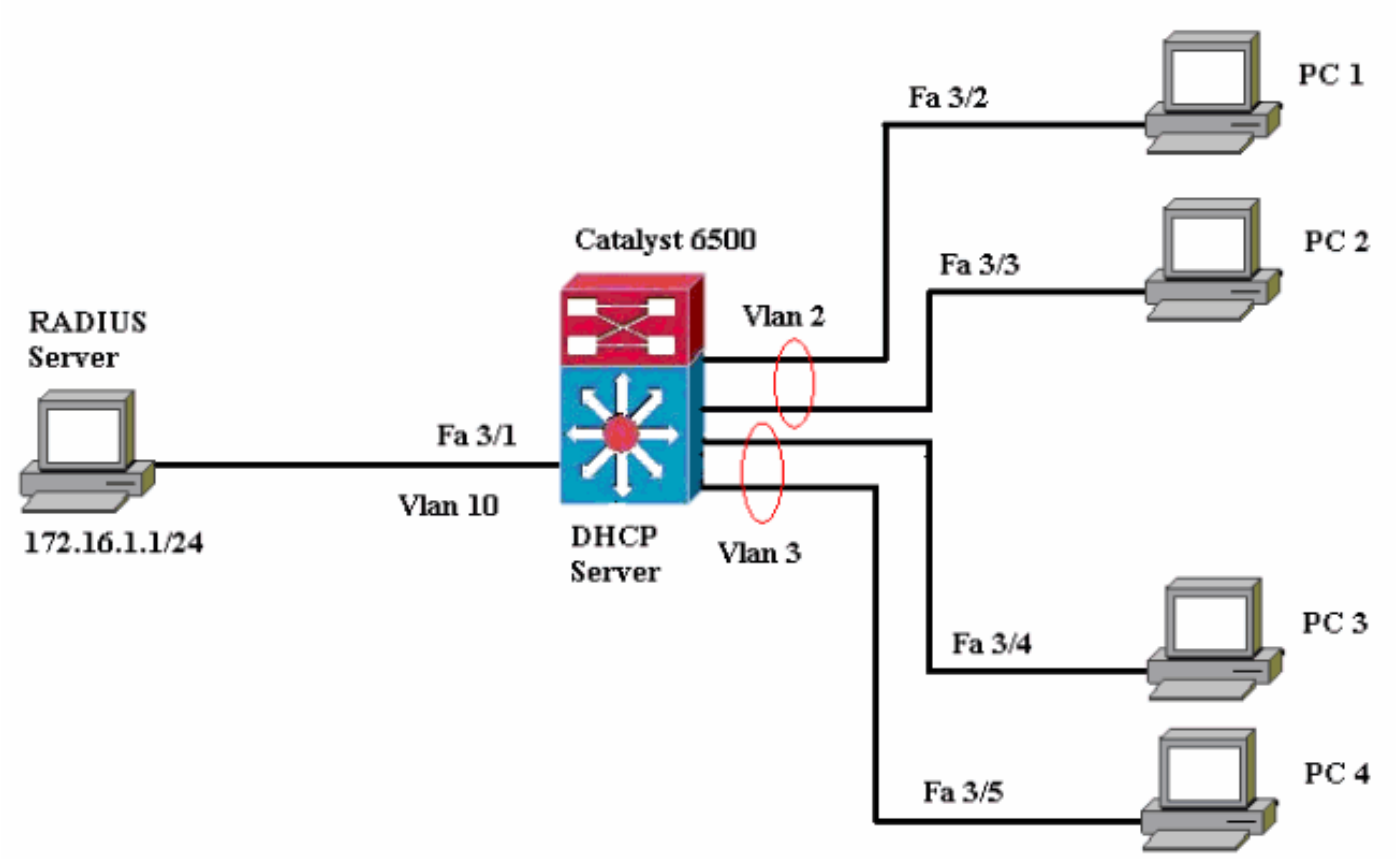
注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

此配置要求执行下列步骤：

- 为 Catalyst 交换机配置 802.1x 认证
- 配置 RADIUS 服务器
- 配置 PC 客户端以使用 802.1x 认证

网络图

本文档使用以下网络设置：



- RADIUS 服务器 — 执行客户端的实际认证。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。这里的 RADIUS 服务器配置为进行认证和 VLAN 分配。
- 交换机 — 根据客户端的认证状态控制对网络的物理访问。该交换机充当客户端与 RADIUS 服务器之间的中间设备（代理），它从客户端请求身份信息，然后通过 RADIUS 服务器验证此信息，再向客户端转发响应。这里的 Catalyst 6500 交换机还配置为 DHCP 服务器。利用动态主机配置协议 (DHCP) 的 802.1x 认证支持，DHCP 服务器可以将经过认证的用户身份添加到 DHCP 发现进程中，从而将 IP 地址分配给不同类别的最终用户。
- 客户端 — 请求对 LAN 和交换机服务的访问并响应来自交换机的请求的设备（工作站）。这里的 PC 1 到 PC 4 是请求带认证的网络访问的客户端。PC 1 和 PC 2 将使用同一登录凭据登录 VLAN 2。同样，PC 3 和 PC 4 将使用 VLAN 3 的登录凭据。PC 客户端配置为从 DHCP 服务器获取 IP 地址。**注意：** 在这种配置下，将拒绝任何未通过认证的客户端或任何连接到交换机的不支持 802.1x 的客户端进行网络访问，方法是使用认证失败和访客 VLAN 功能将这些客户端移至未使用的 VLAN（VLAN 4 或 VLAN 5）。

为 Catalyst 交换机配置 802.1x 认证

此示例交换机配置包括：

- 在快速以太网端口启用 802.1x 认证和相关功能。
- 将 RADIUS 服务器连接到快速以太网端口 3/1 后的 VLAN 10。
- DHCP 服务器配置为采用两个 IP 池，其中一个用于 VLAN 2 中的客户端，另一个用于 VLAN 3 中的客户端。
- 认证后将在客户端之间实现连接的 Inter-VLAN Routing。

有关如何配置 802.1x 认证的准则，请参阅认证配置指南。

注意： 确保 RADIUS 服务器始终连接在获得授权的端口后面。

Catalyst 6500

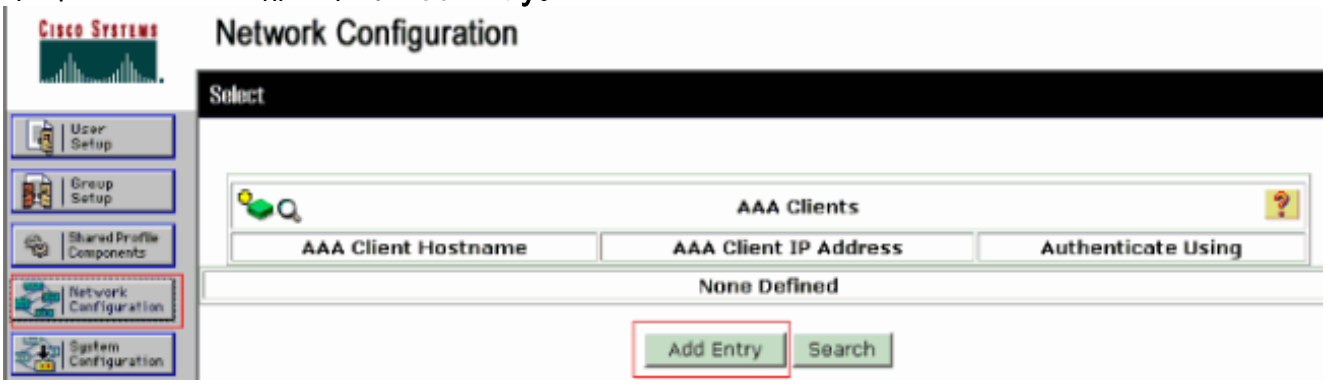
Console (enable) **set system name Cat6K** System name set. *!--- Sets the hostname for the switch.* Cat6K> (enable) **set localuser user admin password cisco** Added local user admin. Cat6K> (enable) **set localuser authentication enable** LocalUser authentication enabled *!--- Uses local user authentication 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 successsful 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)
```

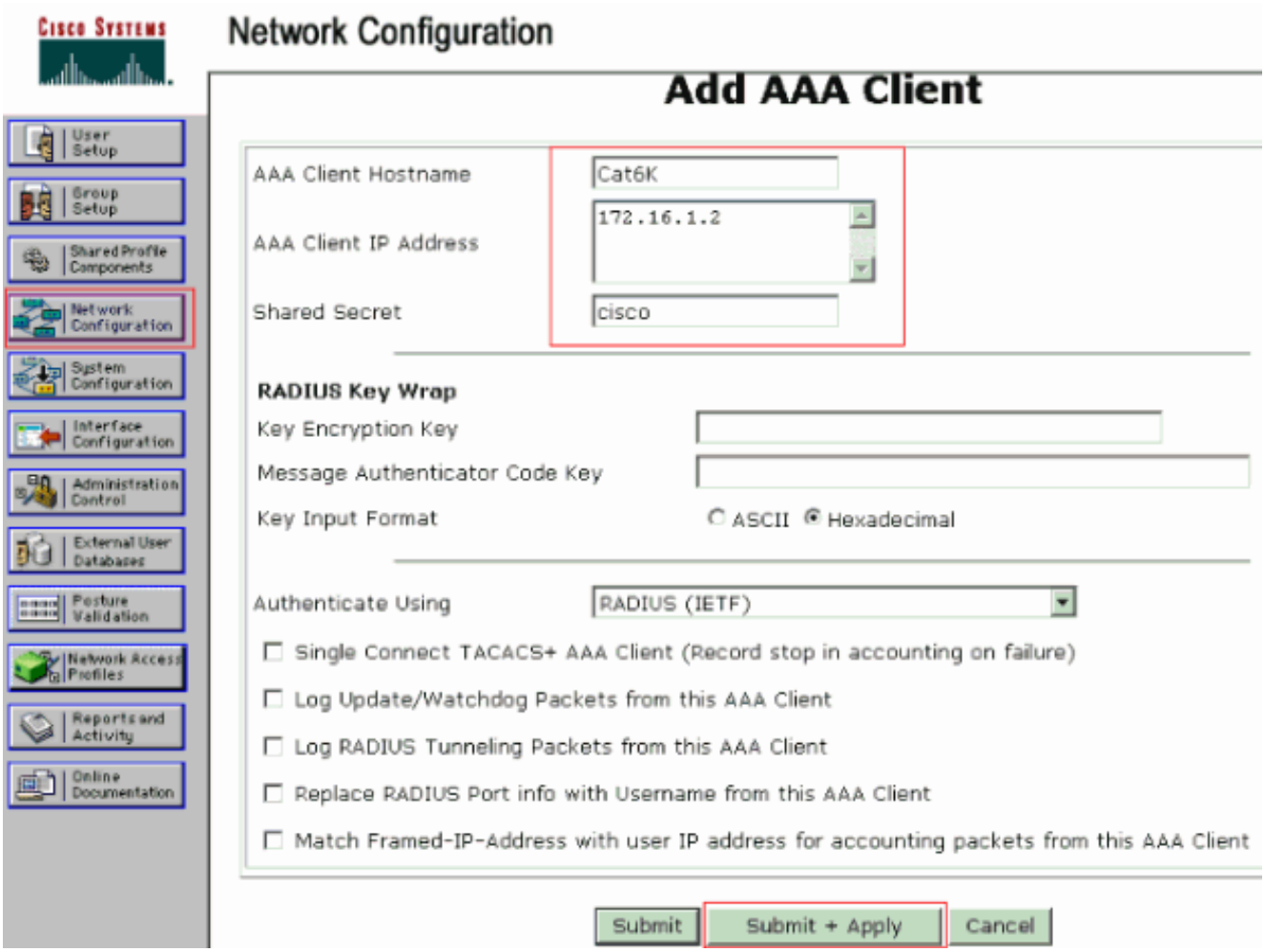
配置 RADIUS 服务器

RADIUS 服务器配置了静态 IP 地址 172.16.1.1/24。完成下列步骤以配置 RADIUS 服务器的 AAA 客户端：

1. 要配置 AAA 客户端，请单击 ACS 管理窗口中的 **Network Configuration**。
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 (**Cat6k**)。“AAA client IP address”= 交换机的管理接口 (sc0) IP 地址 (**172.16.1.2**)。Shared Secret = 在交换机上配置的 Radius 密钥 (**cisco**)。Authenticate Using = **RADIUS IETF**。**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。
4. 单击 **Submit + Apply** 使上述更改生效，如下面的示例所示：



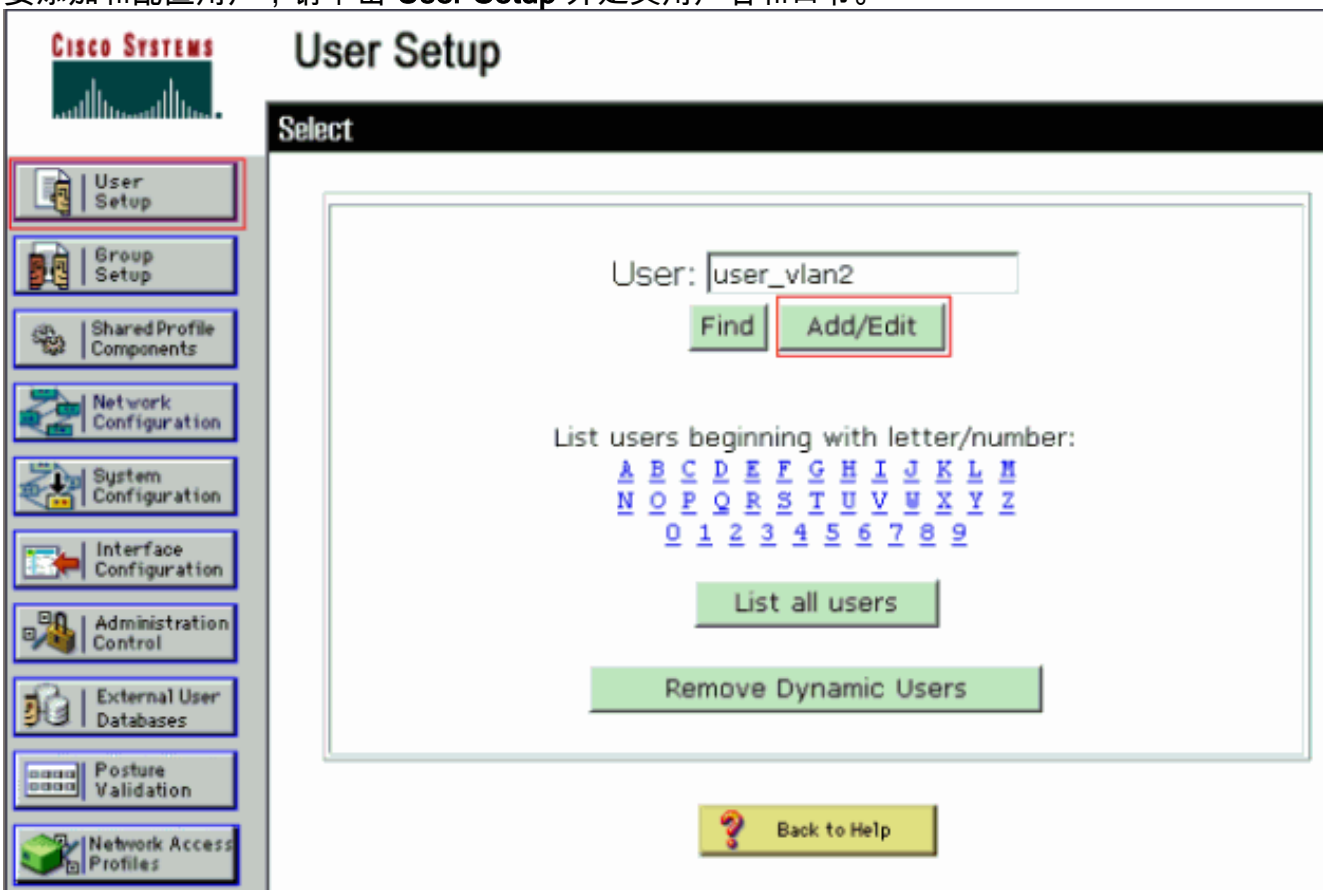
完成下列步骤以配置 RADIUS 服务器的认证、VLAN 和 IP 地址分配：

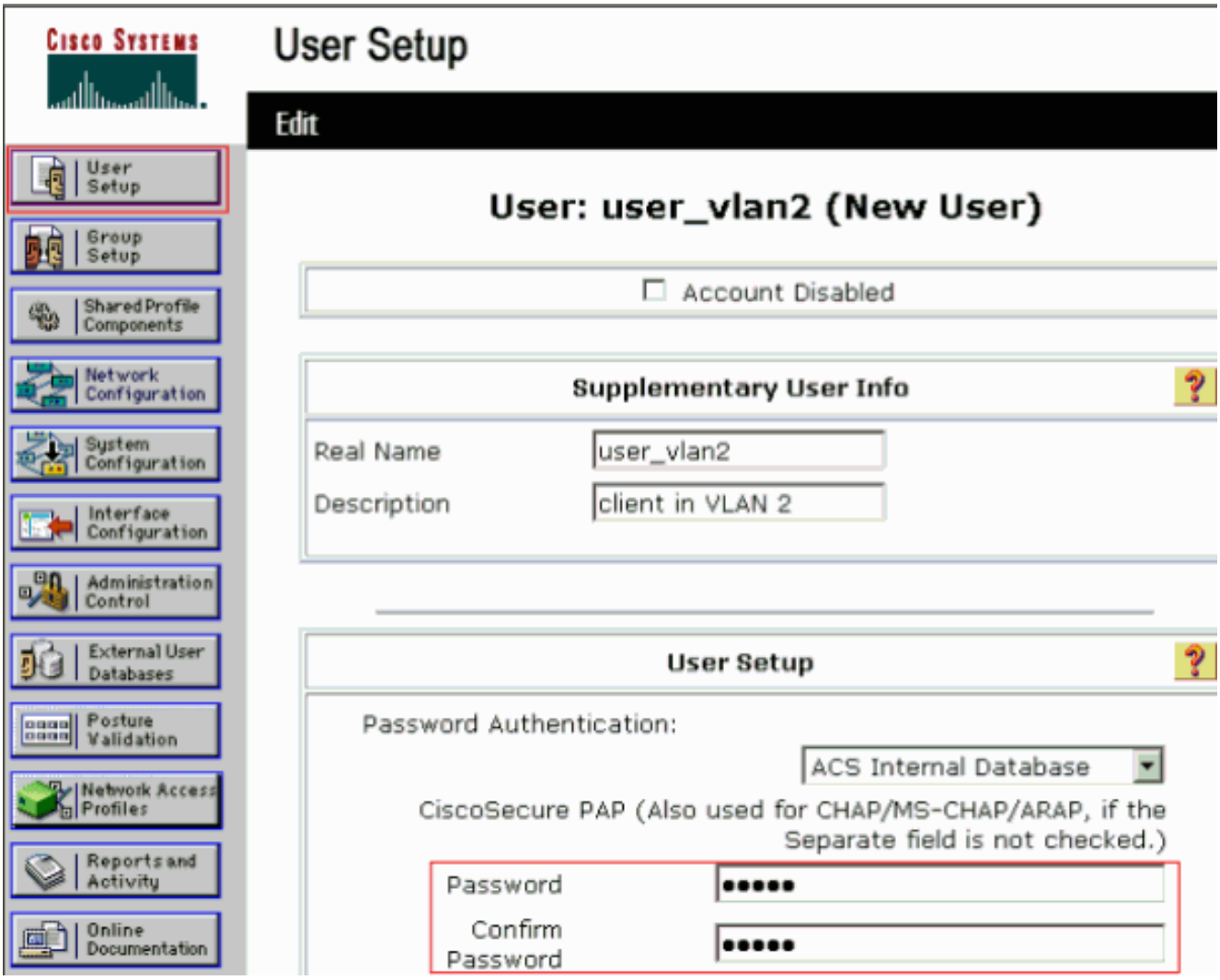
必须为连接到 VLAN 2 以及连接到 VLAN 3 的客户端分别创建两个用户名。为此，在这里为连接到 VLAN 2 的客户端创建一个用户 **user_vlan2**，为连接到 VLAN 3 的客户端创建另一个用户 **user_vlan3**。

注意： 这里仅显示连接到 VLAN 2 的客户端的用户配置。对于连接到 VLAN 3 的用户，完成相同的

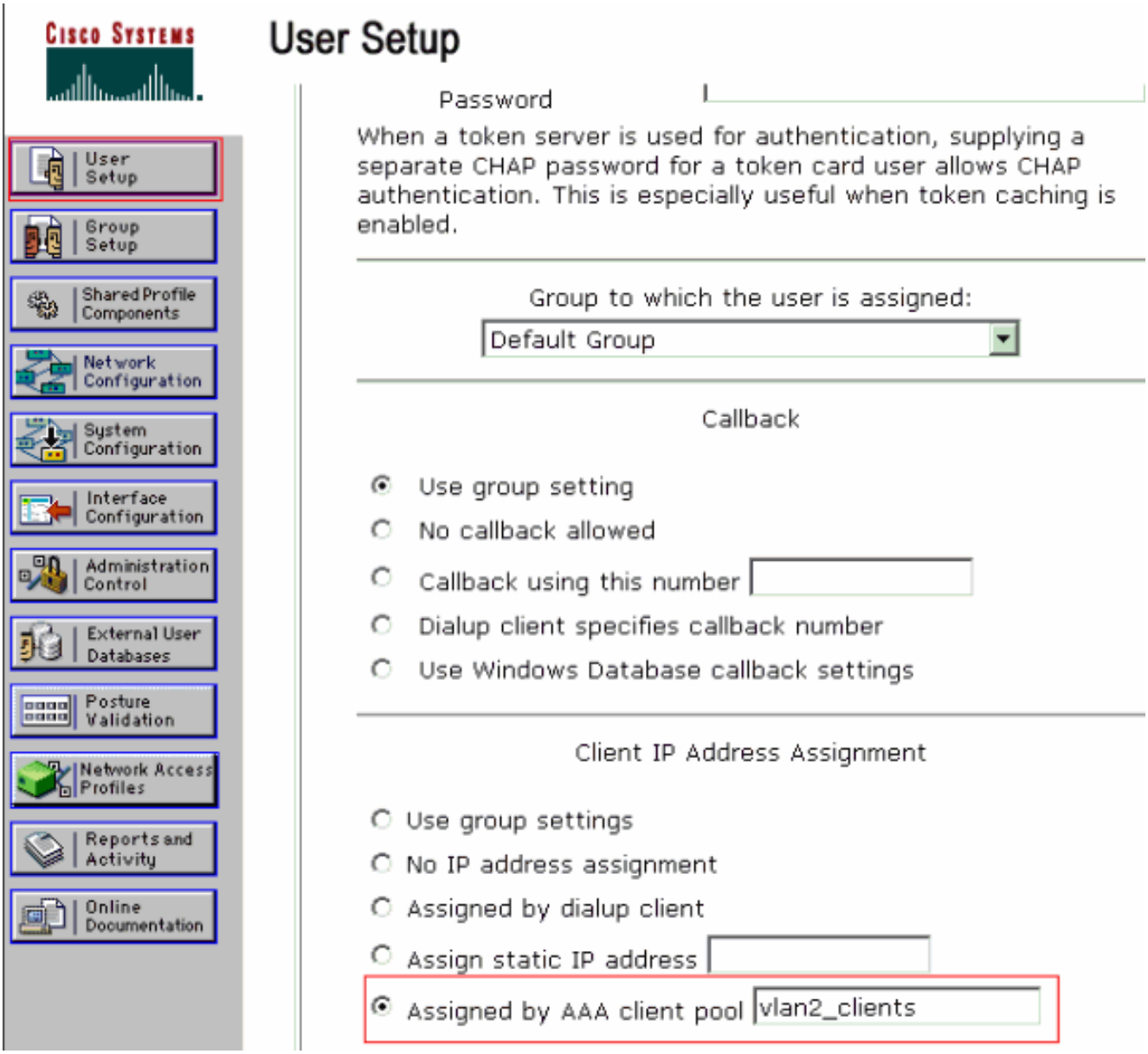
步骤。

1. 要添加和配置用户，请单击 **User Setup** 并定义用户名和口令。



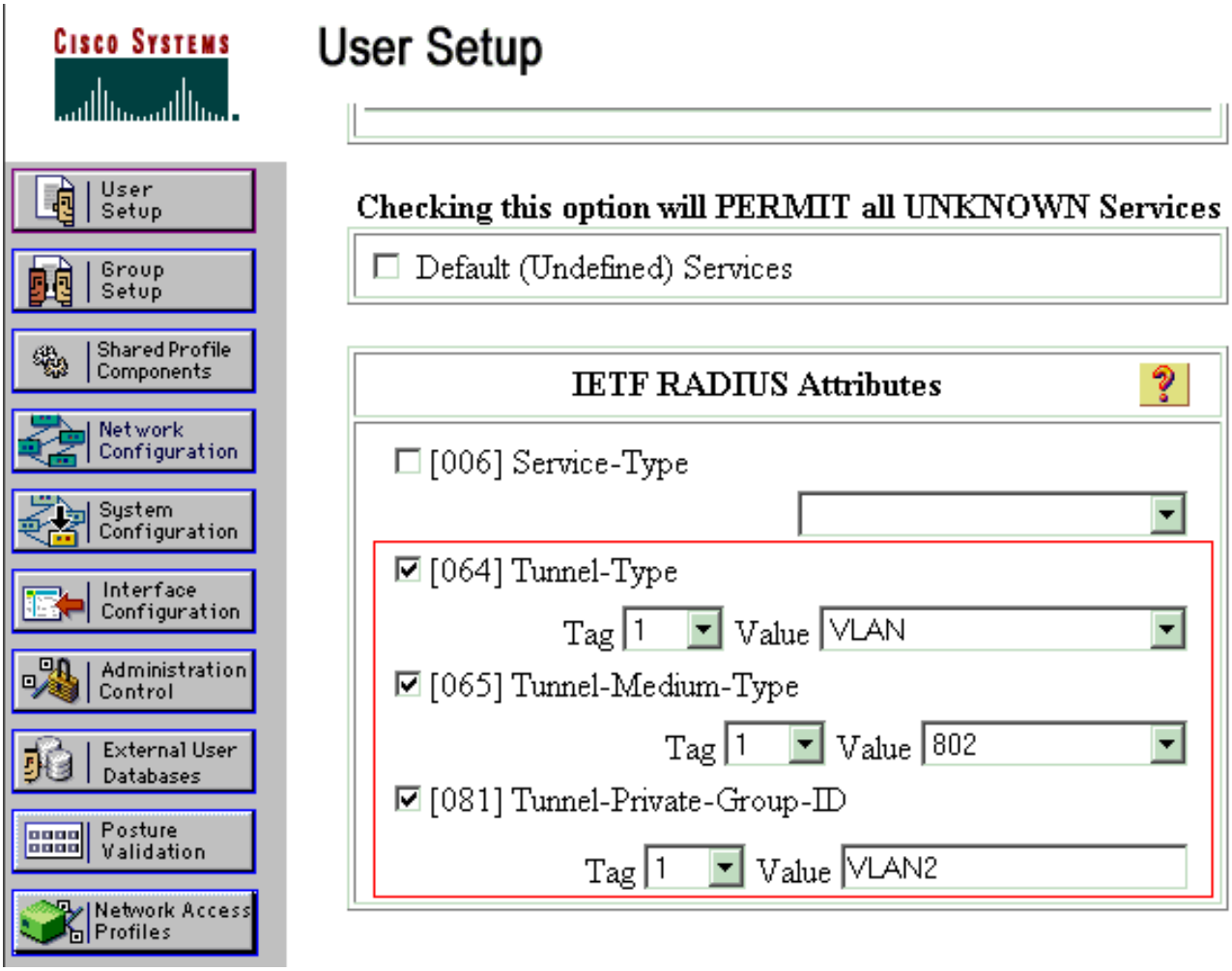


2. 将客户端 IP 地址分配定义为 **Assigned by AAA client pool**。输入在交换机上为 VLAN 2 客户端配置的 IP 地址池的名称。



注意： 只有此用户将获得由 AAA 客户端上配置的 IP 地址池分配的 IP 地址时，才能选择此选项并在框中键入 AAA 客户端 IP 池名称。

3. 定义 Internet 工程任务组 (IETF) 属性 64 和 65。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。要将用户分配到特定的 VLAN，还必须定义具有对应 VLAN 名称的属性 81。**注意：** 该 VLAN 名称应与交换机中配置的名称完全相同。**注意：** CatOS 不支持基于 VLAN 号的 VLAN 分配。

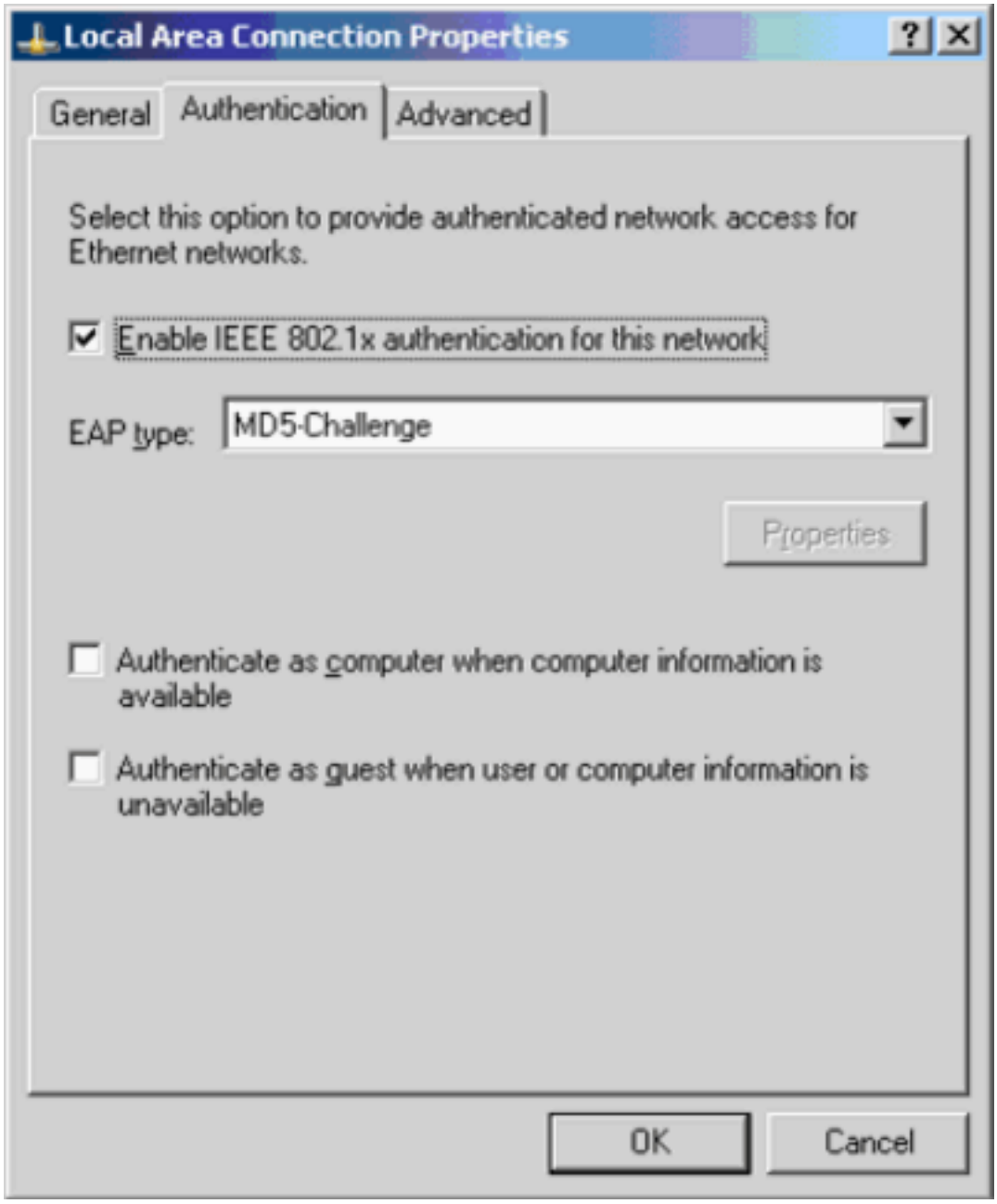


请参阅 RFC 2868：用于支持隧道协议的 RADIUS 属性 以获得有关这些 IETF 属性的详细信息。**注意：** 在 ACS 服务器的初始配置中，**User Setup** 中可能不会显示 IETF RADIUS 属性。选择 **Interface configuration > RADIUS (IETF)** 可启用用户配置屏幕中的 IETF 属性。然后，检查 **64**， **65**和**81**在用户和群组栏。

配置 PC 客户端以使用 802.1x 认证

此示例特定于 LAN (EAPOL) 客户端的 Microsoft Windows XP 可扩展的认证协议 (EAP)。完成这些步骤：

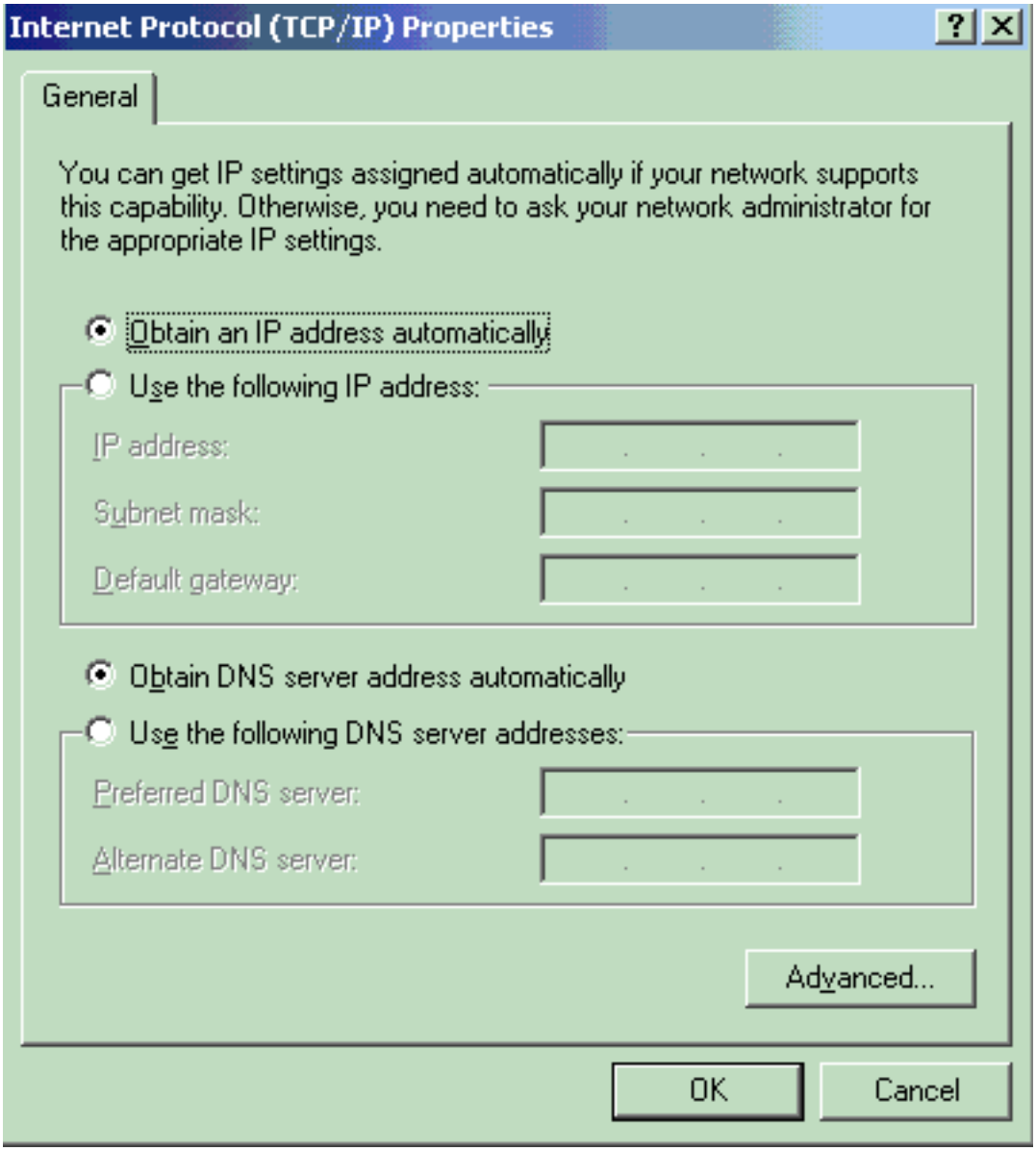
1. 选择**开始 > 控制面板 > 网络连接**，然后右键单击您的**本地连接**并选择**属性**。
2. 在“常规”选项卡下选中**连接后在通知区域显示图标**。
3. 在Authentication选项下，检查**启用此网络的IEEE 802.1X验证**。
4. 将 EAP 类型设置为 **MD5-质询**，如下面的示例所示



:

完成下列步骤，将客户端配置为从 DHCP 服务器获取 IP 地址：

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**。



验证

使用本部分可确认配置能否正常运行。

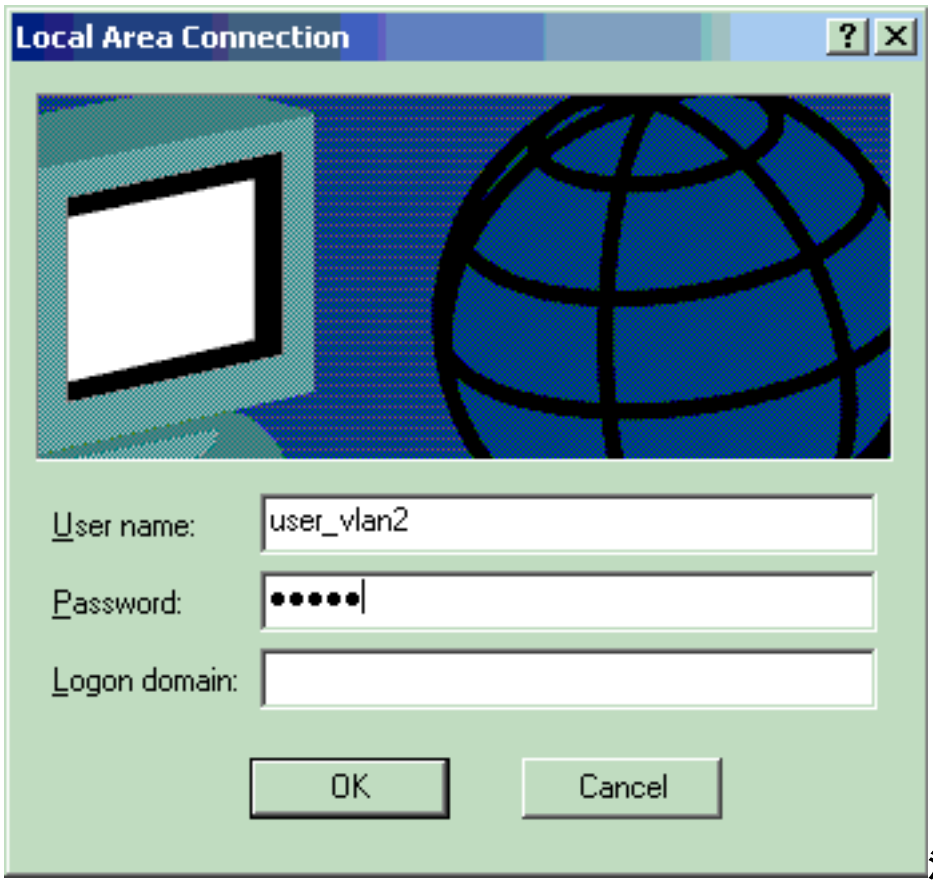
命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

PC 客户端

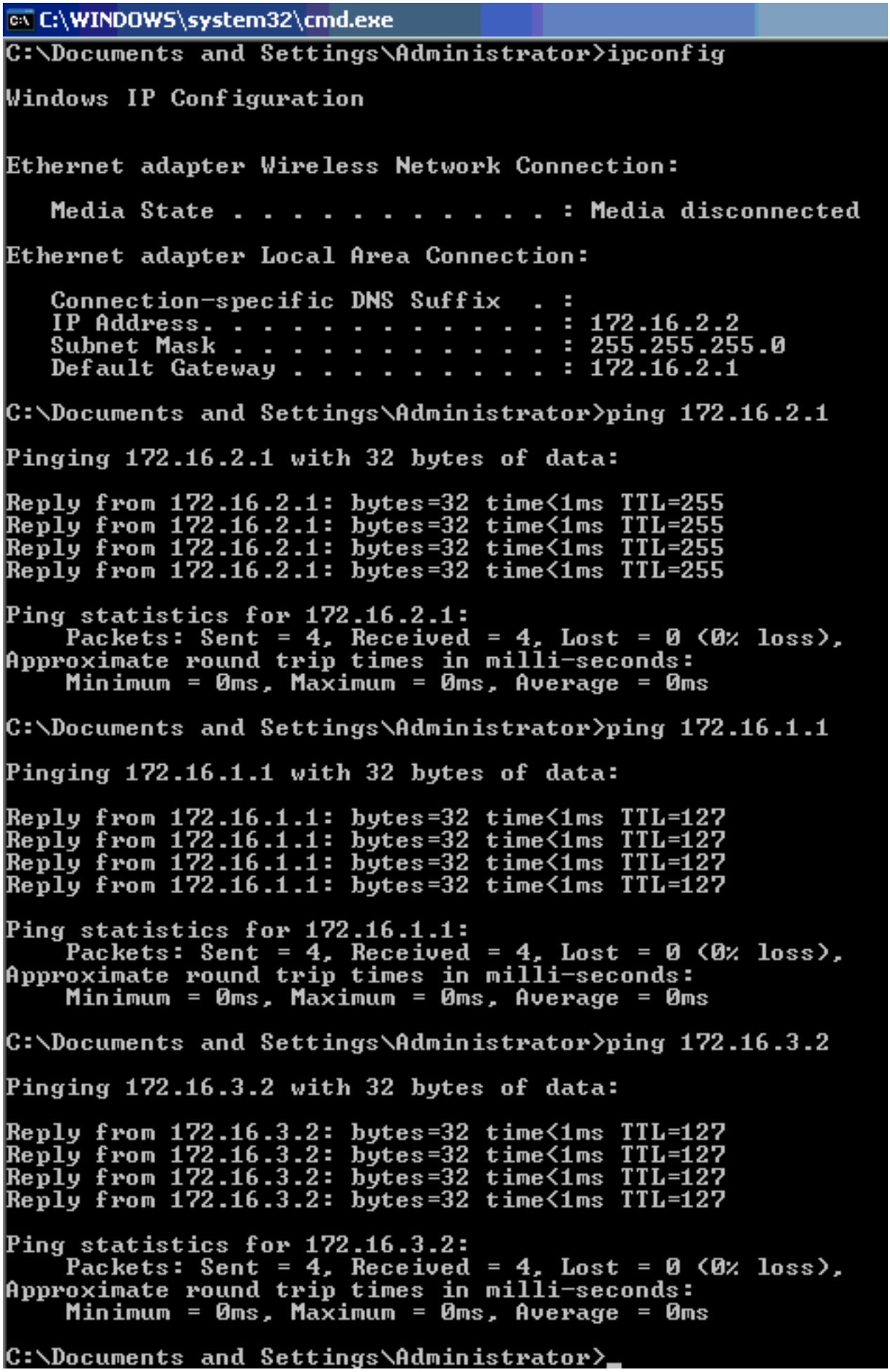
如果配置已正确完成，PC 客户端将显示一个弹出提示框，提示您输入用户名和口令。

1. 单击该提示框，如下所示

：此时显示用户名和口令输入窗口。



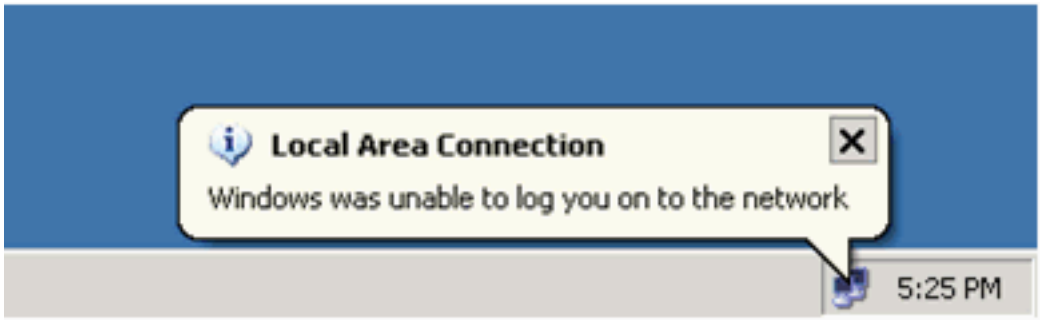
2. 输入用户名和口令。**注意**：在 PC 1 和 PC 2 中，输入 VLAN 2 的用户凭据。在 PC 3 和 PC 4 中，输入 VLAN 3 的用户凭据。
3. 如果未显示错误消息，请采用常用方法验证连接，例如通过使用 **ping 命令**访问网络资源。下面来自 PC 1 的输出，显示对 PC 4 执行 ping 成功



：

如果显示以下错误，请验证用户名和口令是否正确

:



Catalyst 6500

如果口令和用户名看来正确，请验证交换机上的 802.1x 端口状态。

1. 查找表示 authorized 的端口状态。`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** *!--- This is the port to which RADIUS server is connected.* 3/2 **authenticated** idle 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` 在成功进行认证后验证 VLAN 状态。`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. 认证成功后，通过路由模块 (MSFC) 验证 DHCP 绑定状态。`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`

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 运行 Cisco IOS 软件的 Catalyst 6500/6000 IEEE 802.1x 认证示例
- Catalyst 交换和 ACS 部署指南
- RFC 2868：用于支持隧道协议的 RADIUS 属性
- 配置 802.1x 认证
- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems