

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[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](#)

[验证](#)

[PC 客户端](#)

[Catalyst 6500](#)

[故障排除](#)

[相关信息](#)

简介

本文档说明如何在以本地模式 (Supervisor 引擎和 MSFC 使用一个 Cisco IOS® 软件镜像) 运行的 Catalyst 6500/6000 上配置 IEEE 802.1x 和 Remote Authentication Dial-In User Service (RADIUS) 服务器以进行认证和 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 Cisco IOS 软件版本 12.2(18)SXF 的 Catalyst 6500**注意：**您需要 Cisco IOS 软件版本 12.1(13)E 或更高版本以支持 802.1x 基于端口的认证。
- 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。

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 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。

注意： 如果交换机接收到来自未配置 802.1x 认证的端口的 EAPOL 数据包，或者如果交换机不支持 802.1x 认证，则 EAPOL 数据包将丢包且不会转发到任何上游设备。

配置

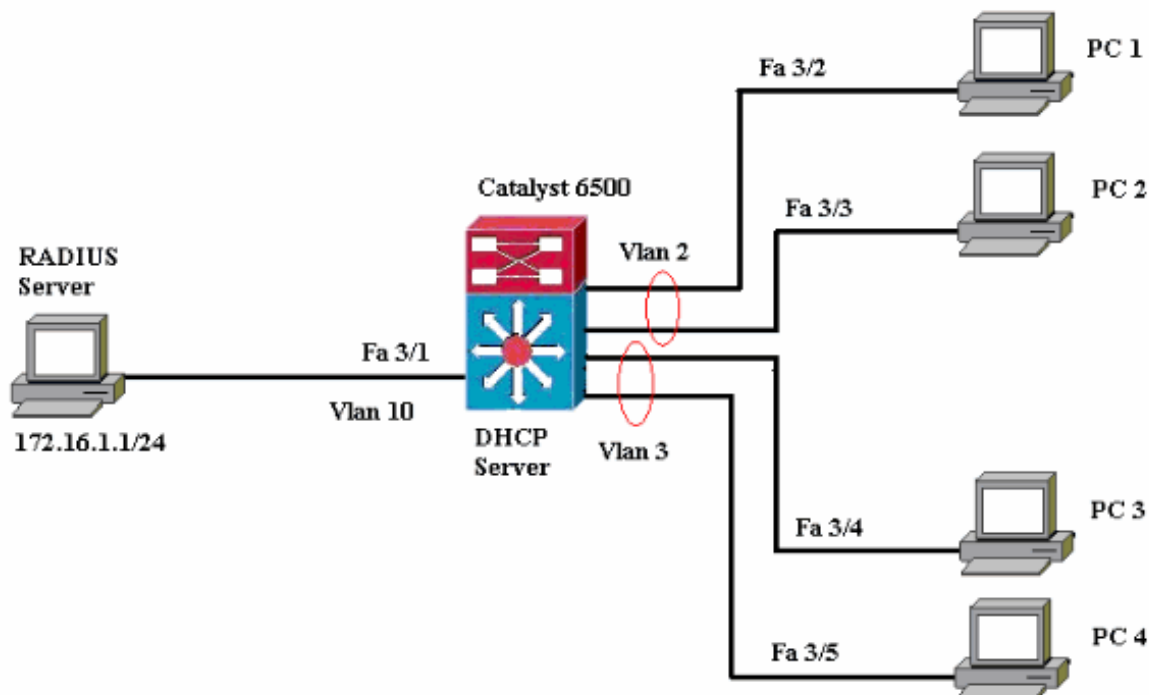
本部分将提供有关如何配置本文档中所述的 802.1x 功能的信息。

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？执行对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。这里的 RADIUS 服务器配置为进行认证和 VLAN 分配。
- 交换机？控制对根据客户端的认证状态的网络的物理访问。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 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？该的设备(工作站)请求对LAN和交换机服务的访问并且回答从交换机的请求。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 使用 VLAN 2 中的相同登录凭据。类似地，PC 3 和 PC 4 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。

为 Catalyst 交换机配置 802.1x 认证

此示例交换机配置包括：

- 如何在快速以太网端口上启用 802.1x 认证。
- 如何将 RADIUS 服务器连接到快速以太网端口 3/1 后面的 VLAN 10。
- 两个 IP 池的 DHCP 服务器配置，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 认证的指南，请参阅[基于 802.1x 端口的认证指南和限制](#)。

注意： 确保 RADIUS 服务器始终连接在获得授权的端口后面。

Catalyst 6500

```
Router#configure terminalEnter configuration commands, one
per line. End with CNTL/Z.Router(config)#hostname Cat6K!---
Sets the hostname for the switch.Cat6K(config)#vlan
2Cat6K(config-vlan)#name VLAN2Cat6K(config-vlan)#vlan
3Cat6K(config-vlan)#name VLAN3!--- VLAN should be existing in
the switch for a successful authentication.Cat6K(config-
vlan)#vlan 10Cat6K(config-vlan)#name RADIUS_SERVER!--- This
is a dedicated VLAN for the RADIUS server.Cat6K(config-
vlan)#exitCat6K(config-if)#interface
fastEthernet3/1Cat6K(config-if)#switchportCat6K(config-
if)#switchport mode accessCat6K(config-if)#switchport access
vlan 10Cat6K(config-if)#no shut!--- Assigns the port
connected to the RADIUS server to VLAN 10. !--- Note:- All
the active access ports are in VLAN 1 by
default.Cat6K(config-if)#exitCat6K(config)#dot1x system-auth-
control!--- Globally enables 802.1x.Cat6K(config)#interface
range fastEthernet3/2-48Cat6K(config-if-
range)#switchportCat6K(config-if-range)#switchport mode
accessCat6K(config-if-range)#dot1x port-control
autoCat6K(config-if-range)#no shut!--- Enables 802.1x on all
the FastEthernet interfaces.Cat6K(config-if-
range)#exitCat6K(config)#aaa new-model!--- Enables
AAA.Cat6K(config)#aaa authentication dot1x default group
radius!--- Method list should be default. Otherwise dot1x
does not work.Cat6K(config)#aaa authorization network default
group radius!--- You need authorization for dynamic VLAN
assignment to work with RADIUS. Cat6K(config)#radius-server
```

```

host 172.16.1.1!--- Sets the IP address of the RADIUS
server.Cat6K(config)#radius-server key cisco!--- The key must
match the key used on the RADIUS
server.Cat6K(config)#interface vlan 10Cat6K(config-if)#ip
address 172.16.1.2 255.255.255.0Cat6K(config-if)#no shut!---
This is used as the gateway address in RADIUS server !--- and
also as the client identifier in the RADIUS
server.Cat6K(config-if)#interface vlan 2Cat6K(config-if)#ip
address 172.16.2.1 255.255.255.0Cat6K(config-if)#no shut!---
This is the gateway address for clients in VLAN
2.Cat6K(config-if)#interface vlan 3Cat6K(config-if)#ip
address 172.16.3.1 255.255.255.0Cat6K(config-if)#no shut!---
This is the gateway address for clients in VLAN
3.Cat6K(config-if)#exitCat6K(config)#ip dhcp pool
vlan2_clientsCat6K(dhcp-config)#network 172.16.2.0
255.255.255.0Cat6K(dhcp-config)#default-router 172.16.2.1!---
This pool assigns ip address for clients in VLAN
2.Cat6K(dhcp-config)#ip dhcp pool vlan3_clientsCat6K(dhcp-
config)#network 172.16.3.0 255.255.255.0Cat6K(dhcp-
config)#default-router 172.16.3.1!--- This pool assigns ip
address for clients in VLAN 3.Cat6K(dhcp-
config)#exitCat6K(config)#ip dhcp excluded-address
172.16.2.1Cat6K(config)#ip dhcp excluded-address
172.16.3.1Cat6K(config-if)#endCat6K#show vlanVLAN Name
Status    Ports-----
-----1    default
active    Fa3/2, Fa3/3, Fa3/4, Fa3/5
Fa3/6, Fa3/7, Fa3/8, Fa3/9
Fa3/10, Fa3/11, Fa3/12, Fa3/13
Fa3/14, Fa3/15, Fa3/16, Fa3/17
Fa3/18, Fa3/19, Fa3/20, Fa3/21
Fa3/22, Fa3/23, Fa3/24, Fa3/25
Fa3/26, Fa3/27, Fa3/28, Fa3/29
Fa3/30, Fa3/31, Fa3/32, Fa3/33
Fa3/34, Fa3/35, Fa3/36, Fa3/37
Fa3/38, Fa3/39, Fa3/40, Fa3/41
Fa3/42, Fa3/43, Fa3/44, Fa3/45
Fa3/46, Fa3/47, Fa3/48/2    VLAN2
active3    VLAN3
RADIUS_SERVER          active    Fa3/11002 fddi-
default                act/unsup1003 token-ring-default
act/unsup1004 fddinet-default          act/unsup1005
trnet-default          act/unsup!--- Output
suppressed. !--- All active ports are in VLAN 1 (except 3/1)
before authentication.

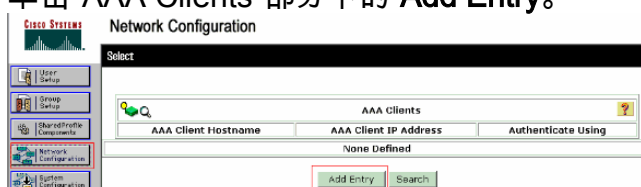
```

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 172.16.1.1/24。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**。



- 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 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。
- 单击 **Submit + Apply** 使上述更改生效，如下面的示例所示：

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

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，请遵循相同的过程。

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

User Setup

Select

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

User Setup

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

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

Password:

Confirm Password:

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。

CISCO SYSTEMS User Setup

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:

Callback

Use group setting
 No callback allowed
 Callback using this number
 Dialup client specifies callback number
 Use Windows Database callback settings

Client IP Address Assignment

Use group settings
 No IP address assignment
 Assigned by dialup client
 Assign static IP address
 Assigned by AAA client pool

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

CISCO SYSTEMS User Setup

Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes ?

[006] Service-Type _____

[064] Tunnel-Type
 Tag Value

[065] Tunnel-Medium-Type
 Tag Value

[081] Tunnel-Private-Group-ID
 Tag Value

中配置的名称完全相同。

注意： 有关这些

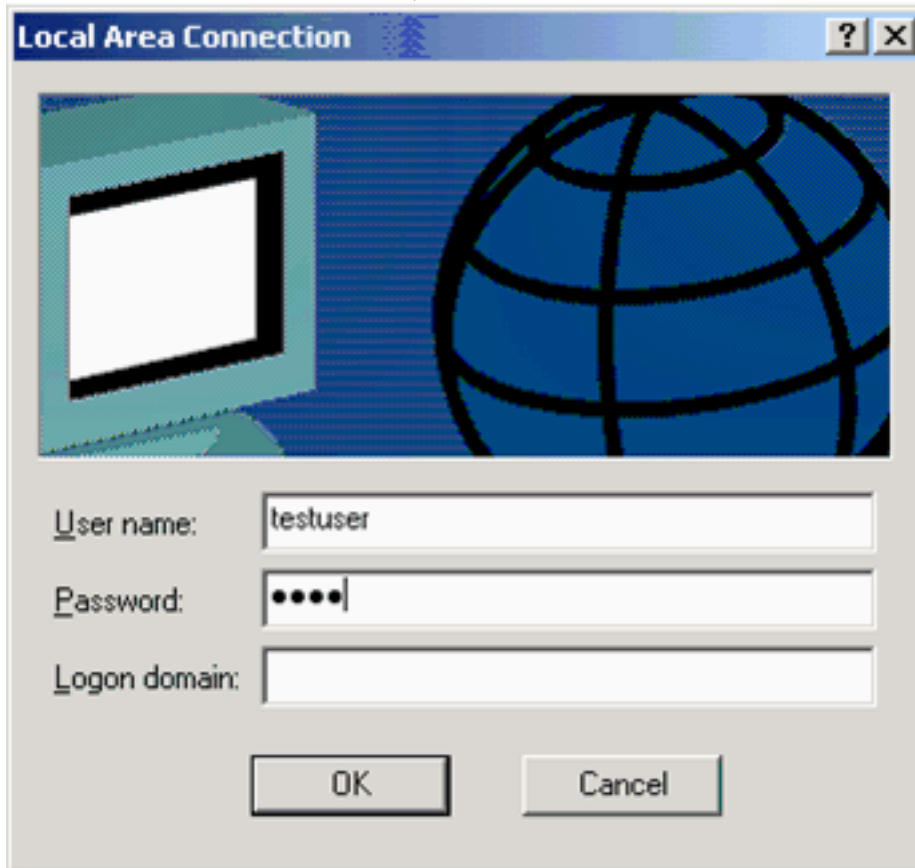
IETF 属性的详细信息，请参阅 [RFC 2868：用于支持隧道协议的 RADIUS 属性](#)。☑ **注意**：在 ACS 服务器的初始配置中，User Setup 中可能不会显示 IETF RADIUS 属性。要在用户配置屏幕中启用 IETF 属性，请选择 **Interface configuration > RADIUS (IETF)**。然后，检查 **64**，**65**和**81**在用户和群组栏。**注意**：如果未定义 IETF 属性 **81**，并且端口是接入模式的交换机端口，则客户端将分配给该端口的接入 VLAN。如果为动态 VLAN 分配定义了属性 **81**，并且端口是接入模式的交换机端口，则您需要在交换机上发出 **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。如果定义了属性 **81**，但您将端口配置为路由端口，则会拒绝接入。这时会显示以下错误消息：

```
Router#configure terminalEnter configuration commands, one per line.
End with CNTL/Z.Router(config)#hostname Cat6K!--- Sets the hostname for the
switch.Cat6K(config)#vlan 2Cat6K(config-vlan)#name VLAN2Cat6K(config-vlan)#vlan 3Cat6K(config-
vlan)#name VLAN3!--- VLAN should be existing in the switch for a successful
authentication.Cat6K(config-vlan)#vlan 10Cat6K(config-vlan)#name RADIUS_SERVER!--- This is a
dedicated VLAN for the RADIUS server.Cat6K(config-vlan)#exitCat6K(config-if)#interface
fastEthernet3/1Cat6K(config-if)#switchportCat6K(config-if)#switchport mode accessCat6K(config-
if)#switchport access vlan 10Cat6K(config-if)#no shut!--- Assigns the port connected to the RADIUS
server to VLAN 10. !--- Note:- All the active access ports are in VLAN 1 by default.Cat6K(config-
if)#exitCat6K(config)#dot1x system-auth-control!--- Globally enables 802.1x.Cat6K(config)#interface
range fastEthernet3/2-48Cat6K(config-if-range)#switchportCat6K(config-if-range)#switchport mode
accessCat6K(config-if-range)#dot1x port-control autoCat6K(config-if-range)#no shut!--- Enables
802.1x on all the FastEthernet interfaces.Cat6K(config-if-range)#exitCat6K(config)#aaa new-model!--
- Enables AAA.Cat6K(config)#aaa authentication dot1x default group radius !--- Method list should
be default. Otherwise dot1x does not work.Cat6K(config)#aaa authorization network default group
radius!--- You need authorization for dynamic VLAN assignment to work with RADIUS.
Cat6K(config)#radius-server host 172.16.1.1!--- Sets the IP address of the RADIUS
server.Cat6K(config)#radius-server key cisco!--- The key must match the key used on the RADIUS
server.Cat6K(config)#interface vlan 10Cat6K(config-if)#ip address 172.16.1.2
255.255.255.0Cat6K(config-if)#no shut!--- This is used as the gateway address in RADIUS server !---
and also as the client identifier in the RADIUS server.Cat6K(config-if)#interface vlan
2Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0Cat6K(config-if)#no shut!--- This is the
gateway address for clients in VLAN 2.Cat6K(config-if)#interface vlan 3Cat6K(config-if)#ip address
172.16.3.1 255.255.255.0Cat6K(config-if)#no shut!--- This is the gateway address for clients in
VLAN 3.Cat6K(config-if)#exitCat6K(config)#ip dhcp pool vlan2_clientsCat6K(dhcp-config)#network
172.16.2.0 255.255.255.0Cat6K(dhcp-config)#default-router 172.16.2.1!--- This pool assigns ip
address for clients in VLAN 2.Cat6K(dhcp-config)#ip dhcp pool vlan3_clientsCat6K(dhcp-
config)#network 172.16.3.0 255.255.255.0Cat6K(dhcp-config)#default-router 172.16.3.1!--- This pool
assigns ip address for clients in VLAN 3.Cat6K(dhcp-config)#exitCat6K(config)#ip dhcp excluded-
address 172.16.2.1Cat6K(config)#ip dhcp excluded-address 172.16.3.1Cat6K(config-if)#endCat6K#show
vlanVLAN Name                Status      Ports-----
-----
-----1          default
-----
Fa3/4, Fa3/5                    Fa3/6, Fa3/7, Fa3/8, Fa3/9
Fa3/10, Fa3/11, Fa3/12, Fa3/13  Fa3/14, Fa3/15,
Fa3/16, Fa3/17                    Fa3/18, Fa3/19, Fa3/20, Fa3/21
Fa3/22, Fa3/23, Fa3/24, Fa3/25  Fa3/26, Fa3/27,
Fa3/28, Fa3/29                    Fa3/30, Fa3/31, Fa3/32, Fa3/33
Fa3/34, Fa3/35, Fa3/36, Fa3/37  Fa3/38, Fa3/39,
Fa3/40, Fa3/41                    Fa3/42, Fa3/43, Fa3/44, Fa3/45
Fa3/46, Fa3/47, Fa3/482    VLAN2
active10    RADIUS_SERVER    active    Fa3/11002 fddi-default
act/unsup1003 token-ring-default    act/unsup1004 fddinet-default
act/unsup1005 trnet-default    act/unsup!--- Output suppressed. !--- All active
ports are in VLAN 1 (except 3/1) before authentication.
```

配置 PC 客户端以使用 802.1x 认证

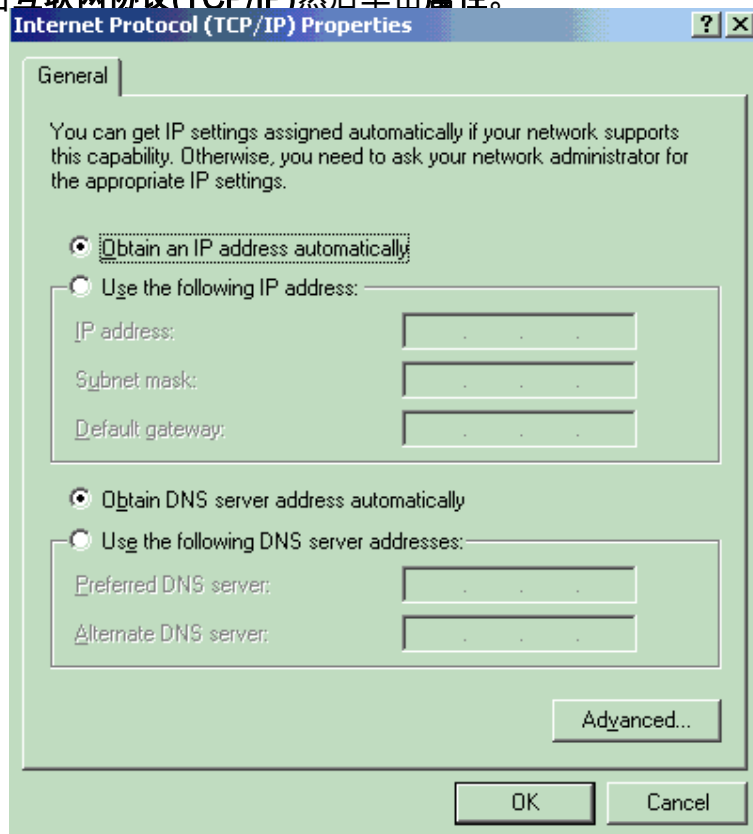
本示例是特定于 Microsoft Windows XP LAN 的可扩展认证协议 (EAPOL) 客户端的：

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



完成以下步骤以配置客户端从 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。



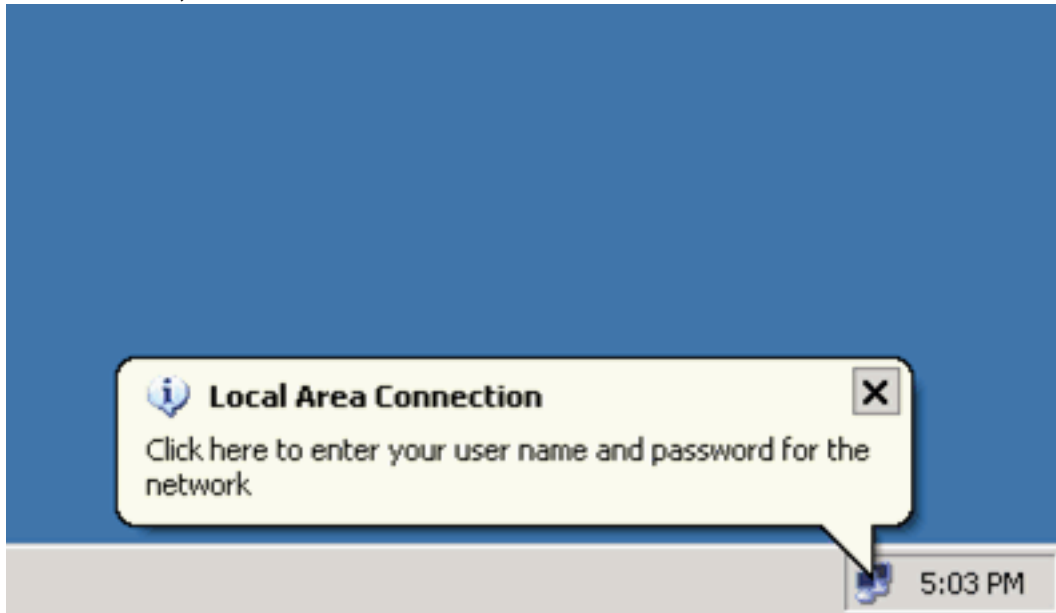
3. 选择自动地获得IP地址。

验证

PC 客户端

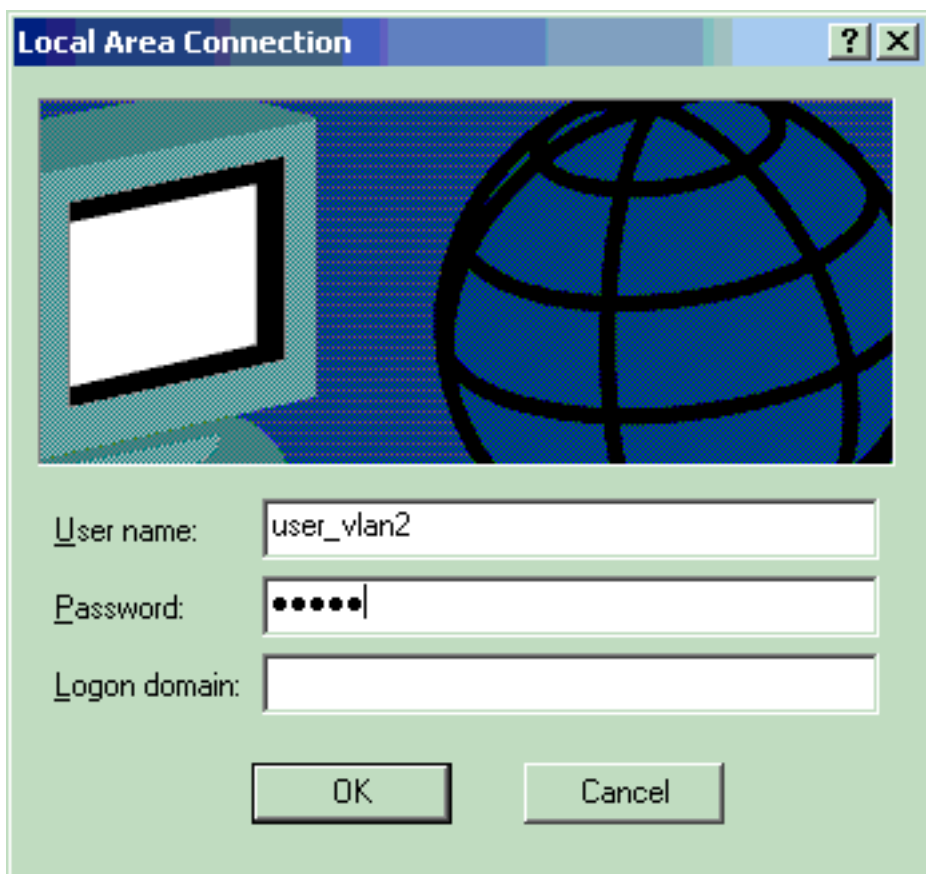
如果配置已正确完成，PC 客户端将显示一个弹出提示框，提示您输入用户名和口令。

1. 单击该提示框，如下所示



: 名和口令输入窗口。

此时将显示用户



2. 输入用户名和密码。

注意

: 在 PC 1 和 PC 2 中，输入 VLAN 2 用户凭据；在 PC 3 和 PC 4 中，输入 VLAN 3 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。以下输出来自 PC 1，显示了一个针对 PC 4 的成功 ping : ■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。Cat6K#**show dot1x**

```

Sysauthcontrol
Enabled Dot1x Protocol Version = 1 Dot1x Oper Controlled Directions = Both Dot1x Admin
Controlled Directions = Both Cat6K#show dot1x interface fastEthernet 3/2 AuthSM State =
AUTHENTICATEDBendSM State = IDLEPortStatus = AUTHORIZEDMaxReq = 2MultiHosts
= EnabledPort Control = AutoQuietPeriod = 60 SecondsRe-authentication =
DisabledReAuthPeriod = 3600 SecondsServerTimeout = 30 SecondsSuppTimeout = 30
SecondsTxPeriod = 30 SecondsCat6K#show dot1x interface fastEthernet 3/4 AuthSM State
= AUTHENTICATEDBendSM State = IDLEPortStatus = AUTHORIZEDMaxReq =
2MultiHosts = EnabledPort Control = AutoQuietPeriod = 60 SecondsRe-authentication
= DisabledReAuthPeriod = 3600 SecondsServerTimeout = 30 SecondsSuppTimeout = 30
SecondsTxPeriod = 30 SecondsCat6K#show dot1x interface fastEthernet 3/1Default Dot1x
Configuration Exists for this interface FastEthernet3/1AuthSM State = FORCE AUTHORIZEDBendSM
State = IDLEPortStatus = AUTHORIZEDMaxReq = 2MultiHosts =
DisabledPortControl = Force AuthorizedQuietPeriod = 60 SecondsRe-authentication =
DisabledReAuthPeriod = 3600 SecondsServerTimeout = 30 SecondsSuppTimeout = 30
SecondsTxPeriod = 30 Seconds

```

在成功进行认证后验证 VLAN 状态。Cat6K#**show vlan**

```

VLAN
Name Status Ports-----
-----1 default active Fa3/6, Fa3/7, Fa3/8,
Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13,
Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19,
Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25,
Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31,
Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37,
Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43,
Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/482 VLAN2
active Fa3/2, Fa3/33 VLAN3 active Fa3/4, Fa3/510
RADIUS_SERVER active Fa3/11002 fddi-default act/unsup1003
token-ring-default act/unsup1004 fddinet-default act/unsup1005
trnet-default act/unsup!--- Output suppressed.

```

2. 在成功进行认证后验证 DHCP 的绑定状态。Router#**show ip dhcp binding**

```

IP address Hardware
address Lease expiration Type172.16.2.2 0100.1636.3333.9c Mar 04 2007
06:35 AM Automatic172.16.2.3 0100.166F.3CA3.42 Mar 04 2007 06:43 AM
Automatic172.16.3.2 0100.145e.945f.99 Mar 04 2007 06:50 AM Automatic172.16.3.3
0100.1185.8D9A.F9 Mar 04 2007 06:57 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

收集以下 debug 命令的输出以进行故障排除：

注意：使用 debug 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- debug dot1x事件？启用打印语句调试dot1x事件标志守卫的。Cat6K#**debug dot1x events**
- ```

Dot1x
events debugging is onCat6K#!--- Debug output for PC 1 connected to Fa3/2.00:13:36: dot1x-ev:Got a
Request from SP to send it to Radius with id 1400:13:36: dot1x-ev:Couldn't Find a process thats
already handling the request for this id 300:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 100:13:36: dot1x-ev:Found a free slot at slot: 000:13:36: dot1x-
ev:AAA Client process spawned at slot: 000:13:36: dot1x-ev:AAA Client-process processing Request
Interface= Fa3/2, Request-Id = 14, Length = 1500:13:36: dot1x-ev:The Interface on which we got this
AAA Request is FastEthernet3/200:13:36: dot1x-ev:MAC Address is 0016.3633.339c00:13:36: dot1x-
ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA00:13:36: dot1x-ev:going to send to backend

```


on SP, length = 600:13:36: dot1x-ev:Sent to Bend00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 1500:13:36: dot1x-ev:Found a process thats already handling therequest for this id 1200:13:36: dot1x-ev:Username is user\_vlan2; eap packet length = 600:13:36: dot1x-ev:Dot1x Authentication Status:AAA\_AUTHEN\_STATUS\_GETDATA00:13:36: dot1x-ev:going to send to backend on SP, length = 3100:13:36: dot1x-ev:Sent to Bend00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 1600:13:36: dot1x-ev:Found a process thats already handling therequest for this id **1300:13:36: dot1x-ev:Username is user\_vlan2; eap packet length = 3200:13:36: dot1x-ev:Dot1x Authentication Status:AAA\_AUTHEN\_STATUS\_PASS00:13:36: dot1x-ev:Vlan name = VLAN200:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 16 EAP pkt len = 400:13:37: dot1x-ev:The process finished processing the request will pick up any pending requests from the queueCat6K#Cat6K#!---**

*Debug output for PC 3 connected to Fa3/4.00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 800:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 100:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 100:19:58: dot1x-ev:Found a free slot at slot: 000:19:58: dot1x-ev:AAA Client process spawned at slot: 000:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 1500:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/400:19:58: dot1x-ev:MAC Address is 0014.5e94.5f9900:19:58: dot1x-ev:Dot1x Authentication Status:AAA\_AUTHEN\_STATUS\_GETDATA00:19:58: dot1x-ev:going to send to backend on SP, length = 600:19:58: dot1x-ev:Sent to Bend00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 900:19:58: dot1x-ev:Found a process thats already handling therequest for this id 1000:19:58: dot1x-ev:Username is user\_vlan3; eap packet length = 600:19:58: dot1x-ev:Dot1x Authentication Status:AAA\_AUTHEN\_STATUS\_GETDATA00:19:58: dot1x-ev:going to send to backend on SP, length = 3100:19:58: dot1x-ev:Sent to Bend00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 1000:19:58: dot1x-ev:Found a process thats already handling therequest for this id **1100:19:58: dot1x-ev:Username is user\_vlan3; eap packet length = 3200:19:58: dot1x-ev:Dot1x Authentication Status:AAA\_AUTHEN\_STATUS\_PASS00:19:58: dot1x-ev:Vlan name = 300:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 400:19:58: dot1x-ev:The process finished processing the request will pick up any pending requests from the queueCat6K#***

- **debug radius ? 显示信息关联与RADIUS。** Cat6K#**debug radius** Radius protocol debugging is onCat6K#!--- *Debug output for PC 1 connected to Fa3/2.00:13:36: RADIUS: ustruct sharecount=100:13:36: RADIUS: Unexpected interface type in nas\_port\_format\_a00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 100:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 8500:13:36: Attribute 4 6 AC10020100:13:36: Attribute 61 6 0000000000:13:36: Attribute 1 12 7573657200:13:36: Attribute 12 6 000003E800:13:36: Attribute 24 33 4349534300:13:36: Attribute 79 17 0201000F00:13:36: Attribute 80 18 CCEE488900:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 7900:13:36: Attribute 79 8 010D000600:13:36: Attribute 24 33 4349534300:13:36: Attribute 80 18 C883376B00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius00:13:36: RADIUS: ustruct sharecount=100:13:36: RADIUS: Unexpected interface type in nas\_port\_format\_a00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 100:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 10900:13:36: Attribute 4 6 AC10020100:13:36: Attribute 61 6 0000000000:13:36: Attribute 1 12 7573657200:13:36: Attribute 12 6 000003E800:13:36: Attribute 24 33 4349534300:13:36: Attribute 79 8 020D000600:13:36: Attribute 80 18 1558248400:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 10400:13:36: Attribute 79 33 010E001F00:13:36: Attribute 24 33 4349534300:13:36: Attribute 80 18 0643D23400:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius00:13:36: RADIUS: ustruct sharecount=100:13:36: RADIUS: Unexpected interface type in nas\_port\_format\_a00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 100:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19 172.16.1.1:1812, Access-Request, len 13500:13:36: Attribute 4 6 AC10020100:13:36: Attribute 61 6 0000000000:13:36: Attribute 1 12 7573657200:13:36: Attribute 12 6 000003E800:13:36: Attribute 24 33 4349534300:13:36: Attribute 79 34 020E002000:13:36: Attribute 80 18 E8A6175100:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 12400:13:36: Attribute 64 6 0100000D00:13:36: Attribute 65 6 0100000600:13:36: Attribute 81 8 01564C4100:13:36: Attribute 88 15 766C616E00:13:36: Attribute 8 6 FFFFFFFFE00:13:36: Attribute 79 6 030E000400:13:36: Attribute 25 39 4349534300:13:36: Attribute 80 18 11A7DD4400:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K#Cat6K#!---* *Debug output for PC 3 connected to Fa3/4.00:19:58: RADIUS: ustruct sharecount=100:19:58: RADIUS: Unexpected interface type in nas\_port\_format\_a00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 100:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812, Access-Request, len 8500:19:58: Attribute 4 6 AC10020100:19:58: Attribute 61 6 0000000000:19:58: Attribute 1 12 7573657200:19:58: Attribute 12 6 000003E800:19:58: Attribute 79 17 0201000F00:19:58: Attribute 80 18 0001AC5200:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge, len 7900:19:58: Attribute 79 8 010B000600:19:58: Attribute 24 33 4349534300:19:58: Attribute 80 18 23B9C9E700:19:58: RADIUS: EAP-login: length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius00:19:58: RADIUS: ustruct sharecount=100:19:58: RADIUS: Unexpected*

```
interface type in nas_port_format_a00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 100:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request, len 10900:19:58: Attribute 4 6 AC10020100:19:58: Attribute 61 6 0000000000:19:58: Attribute 1 12 7573657200:19:58: Attribute 12 6 000003E800:19:58: Attribute 24 33 4349534300:19:58: Attribute 79 8 020B000600:19:58: Attribute 80 18 F4C8832E00:19:58: RADIUS: Received from id 12 172.16.1.1:1812, Access-Challenge, len 10400:19:58: Attribute 79 33 010C001F00:19:58: Attribute 24 33 4349534300:19:58: Attribute 80 18 45472A9300:19:58: RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from radius00:19:58: RADIUS: ustruct sharecount=100:19:58: RADIUS: Unexpected interface type in nas_port_format_a00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 100:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request, len 13500:19:58: Attribute 4 6 AC10020100:19:58: Attribute 61 6 0000000000:19:58: Attribute 1 12 7573657200:19:58: Attribute 12 6 000003E800:19:58: Attribute 24 33 4349534300:19:58: Attribute 79 34 020C002000:19:58: Attribute 80 18 37011E8F00:19:58: RADIUS: Received from id 13 172.16.1.1:1812, Access-Accept, len 12000:19:58: Attribute 64 6 0100000D00:19:58: Attribute 65 6 0100000600:19:58: Attribute 81 4 0133580F00:19:58: Attribute 88 15 766C616E00:19:58: Attribute 8 6 FFFFFFFFE0:19:58: Attribute 79 6 030C000400:19:58: Attribute 25 39 4349534300:19:58: Attribute 80 18 F5520A9500:19:58: RADIUS: EAP-login: length of eap packet = 4 Cat6K#
```

## 相关信息

- [运行 CatOS 软件的 Catalyst 6500/6000 IEEE 802.1x 认证配置示例](#)
- [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](#) 
- [配置基于 IEEE 802.1x 端口的身份验证](#)
- [LAN 产品支持](#)
- [LAN 交换技术支持](#)
- [技术支持和文档 - Cisco Systems](#)