Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o Cisco IOS Software Configuration Example

Contents

Introduction

Este documento explica como configurar o IEEE 802.1X em um Catalyst 6500/6000 que é executado no modo nativo (uma única imagem do software Cisco IOS® para o Supervisor Engine e o MSFC) e um servidor Remote Authentication Dial-In User Service (RADIUS) para autenticação e atribuição de VLAN.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- Guia de instalação do Cisco Secure ACS para Windows 4.1
- Guia do usuário do Cisco Secure Access Control Server 4.1
- Como funciona o RADIUS?
- Guia de implantação do Catalyst Switching e ACS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 6500 que executa o Cisco IOS Software Release 12.2(18)SXF no Supervisor Engine**Observação:** você precisa do Cisco IOS Software Release 12.1(13)E ou posterior para suportar a autenticação baseada em porta 802.1x.
- Este exemplo usa o Cisco Secure Access Control Server (ACS) 4.1 como o servidor RADIUS.**Observação:** um servidor RADIUS deve ser especificado antes de habilitar 802.1x no switch.
- Clientes PC que suportam autenticação 802.1x**Observação:** este exemplo usa clientes Microsoft Windows XP.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O padrão IEEE 802.1x define um controle de acesso baseado em cliente-servidor e um protocolo de autenticação que restringe a conexão de dispositivos não autorizados a uma LAN através de portas acessíveis publicamente. O 802.1x controla o acesso à rede criando dois pontos de acesso virtuais distintos em cada porta. Um ponto de acesso é uma porta não controlada; a outra é uma porta controlada. Todo o tráfego através de uma única porta está disponível para ambos os pontos de acesso. O 802.1x autentica cada dispositivo de usuário conectado a uma porta de switch e atribui a porta a uma VLAN antes de disponibilizar quaisquer serviços oferecidos pelo switch ou pela LAN. Até que o dispositivo seja autenticado, o controle de acesso 802.1x permite somente o tráfego Extensible Authentication Protocol over LAN (EAPOL) através da porta à qual o dispositivo está conectado. Após a autenticação ser bem-sucedida, o tráfego normal pode passar pela porta.

Observação: se o switch receber pacotes EAPOL da porta que não está configurada para autenticação 802.1x ou se o switch não suportar autenticação 802.1x, os pacotes EAPOL serão descartados e não serão encaminhados a nenhum dispositivo upstream.

Configurar

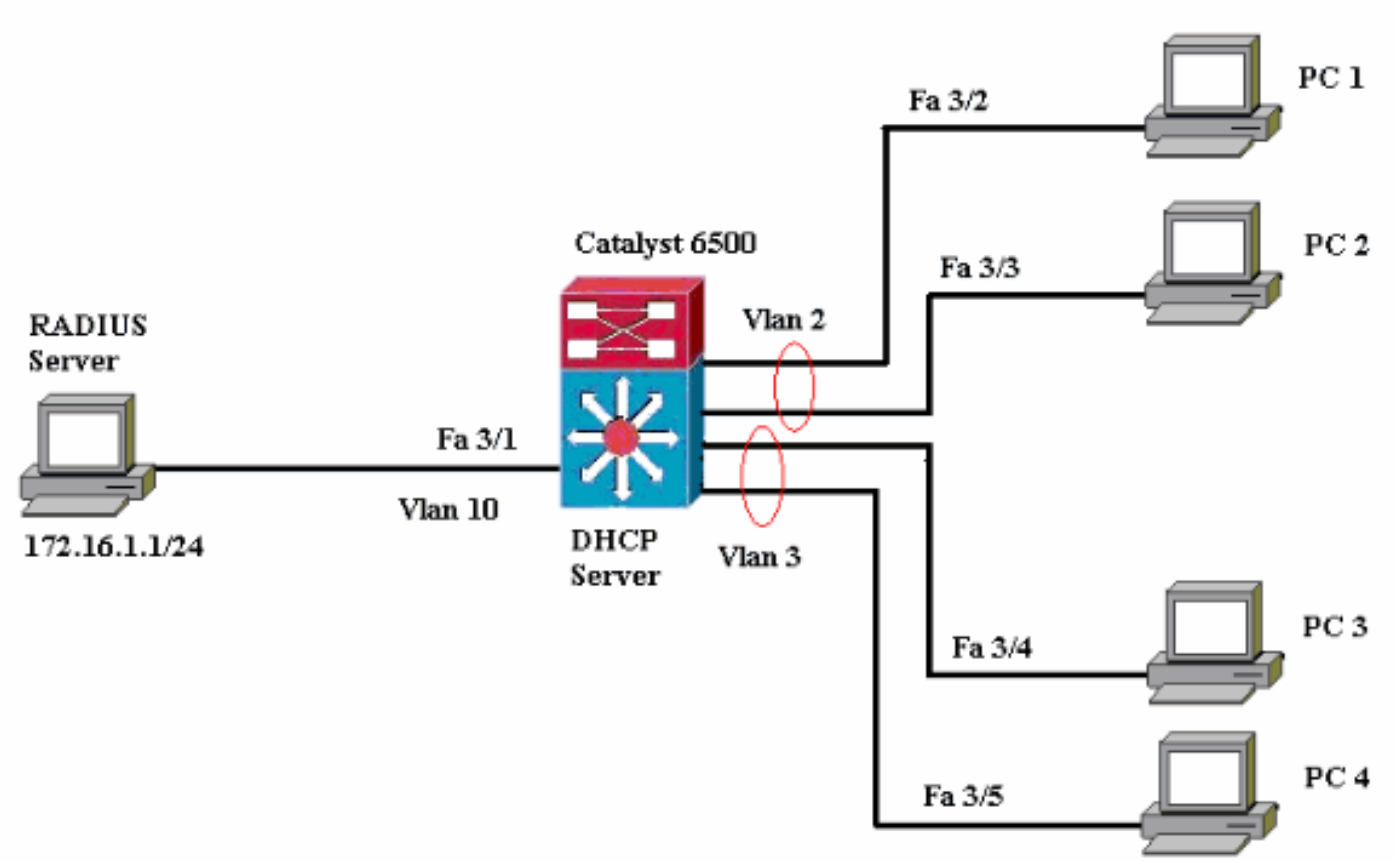
Nesta seção, você recebe as informações para configurar o recurso 802.1x descrito neste documento.

Essa configuração requer estes passos:

- Configure o switch Catalyst para autenticação 802.1x.
- Configure o servidor RADIUS.
- Configure os clientes PC para usar a autenticação 802.1x.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



- Servidor RADIUS—Executa a autenticação real do cliente. O servidor RADIUS valida a identidade do cliente e notifica o switch se o cliente está autorizado a acessar os serviços de LAN e switch. Aqui, o servidor RADIUS está configurado para autenticação e atribuição de VLAN.
- Switch—Controla o acesso físico à rede com base no status de autenticação do cliente. O switch atua como um intermediário (proxy) entre o cliente e o servidor RADIUS. Ele solicita informações de identidade do cliente, verifica essas informações com o servidor RADIUS e retransmite uma resposta ao cliente. Aqui, o switch Catalyst 6500 também é configurado como um servidor DHCP. O suporte à autenticação 802.1x para o DHCP (Dynamic Host Configuration Protocol) permite que o servidor DHCP atribua os endereços IP às diferentes classes de usuários finais adicionando a identidade de usuário autenticado ao processo de descoberta de DHCP.
- Clientes—Os dispositivos (estações de trabalho) que solicitam acesso à LAN e aos serviços do switch e respondem às solicitações do switch. Aqui, os PCs 1 a 4 são os clientes que solicitam um acesso autenticado à rede. Os PCs 1 e 2 usam a mesma credencial de logon que está na VLAN 2. Da mesma forma, os PCs 3 e 4 usam uma credencial de login para a VLAN 3. Os clientes PC são configurados para obter o endereço IP de um servidor DHCP.

Configurar o Switch Catalyst para autenticação 802.1x

Este exemplo de configuração de switch inclui:

- Como ativar a autenticação 802.1x em portas FastEthernet.

- Como conectar um servidor RADIUS à VLAN 10 atrás da porta FastEthernet 3/1.
- Uma configuração de servidor DHCP para dois pools IP, um para clientes na VLAN 2 e outro para clientes na VLAN 3.
- Roteamento entre VLANs para ter conectividade entre clientes após a autenticação.

Consulte Diretrizes e Restrições de Autenticação Baseada em Porta 802.1x para obter as diretrizes sobre como configurar a autenticação 802.1x.

Observação: verifique se o servidor RADIUS sempre se conecta atrás de uma porta autorizada.

Catalyst 6500

```
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname Cat6K
!--- Sets the hostname for the switch.
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
!--- This is a dedicated VLAN for the RADIUS server.
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(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)#exit
Cat6K(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat6K(config)#interface
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
!--- Enables 802.1x on all the FastEthernet interfaces.
Cat6K(config-if-range)#exit
Cat6K(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 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
```

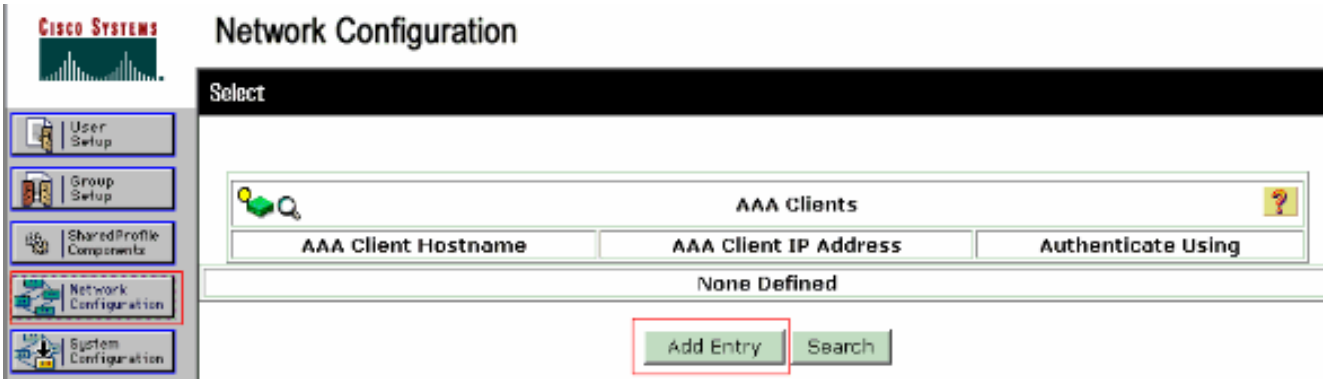
```
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(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_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

VLAN 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                             active
3    VLAN3                             active
10   RADIUS_SERVER                     active    Fa3/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

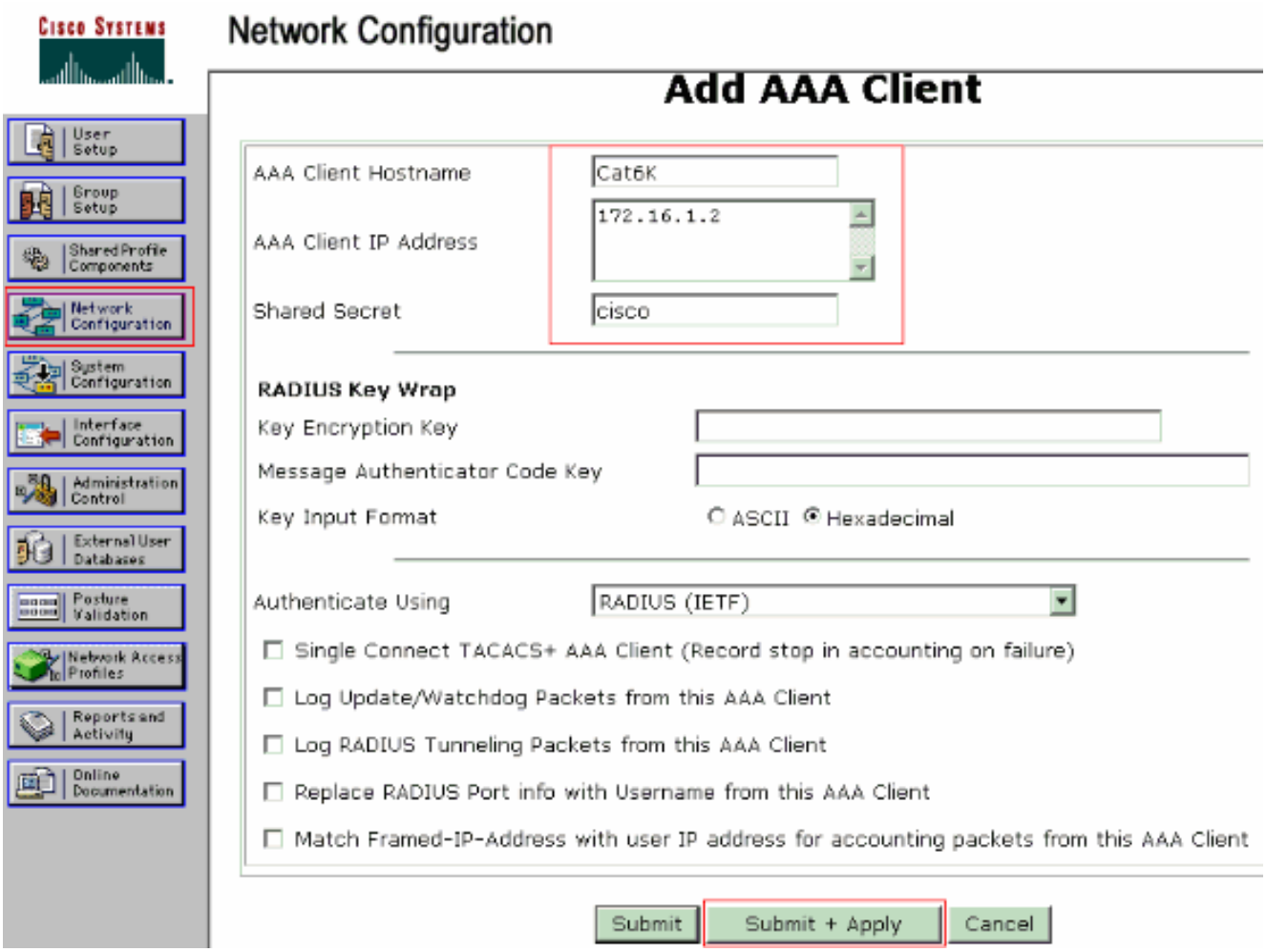
Configurar o servidor RADIUS

O servidor RADIUS é configurado com um endereço IP estático de 172.16.1.1/24. Conclua estes passos para configurar o servidor RADIUS para um cliente AAA:

1. Clique em **Network Configuration** na janela de administração do ACS para configurar um cliente AAA.
2. Clique em **Add Entry** na seção AAA clients.



3. Configure o nome de host do cliente AAA, o endereço IP, a chave secreta compartilhada e o tipo de autenticação como:Nome de host do cliente AAA = Nome de host do switch (**Cat6K**).Endereço IP do cliente AAA = Endereço IP da interface de gerenciamento do switch (**172.16.1.2**).Segredo compartilhado = chave RADIUS configurada no switch (**cisco**).Autentique Usando = **RADIUS IETF**.**Observação:** para uma operação correta, a chave secreta compartilhada deve ser idêntica no cliente AAA e no ACS. As chaves diferenciam maiúsculas e minúsculas.
4. Clique em **Enviar + Aplicar** para tornar essas alterações efetivas, como mostrado neste exemplo:

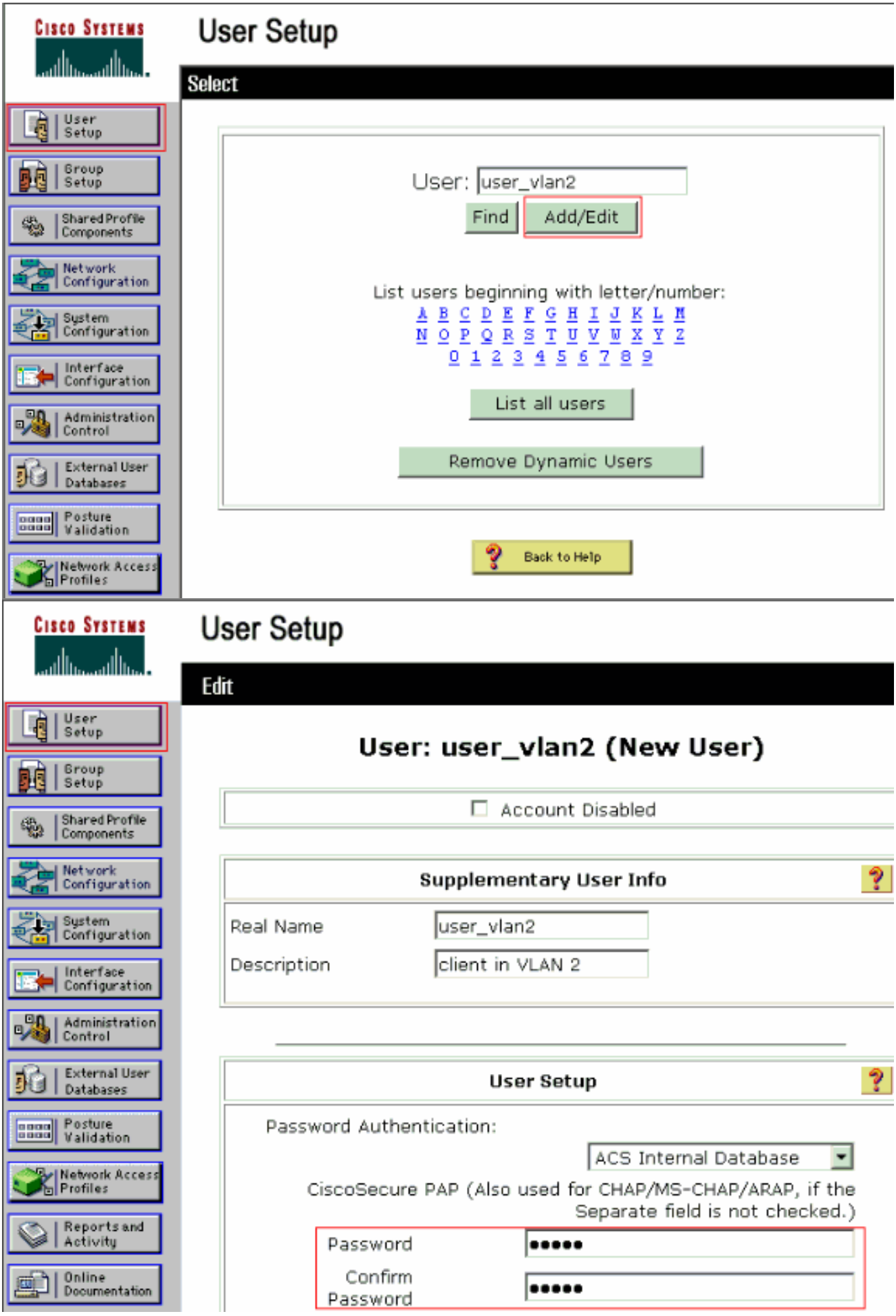


Conclua estes passos para configurar o servidor RADIUS para autenticação, VLAN e atribuição de endereços IP.

Dois nomes de usuário devem ser criados separadamente para clientes que se conectam à VLAN 2 e à VLAN 3. Aqui, um usuário **user_vlan2** para clientes que se conectam à VLAN 2 e a outro usuário **user_vlan3** para clientes que se conectam à VLAN 3 são criados para essa finalidade.

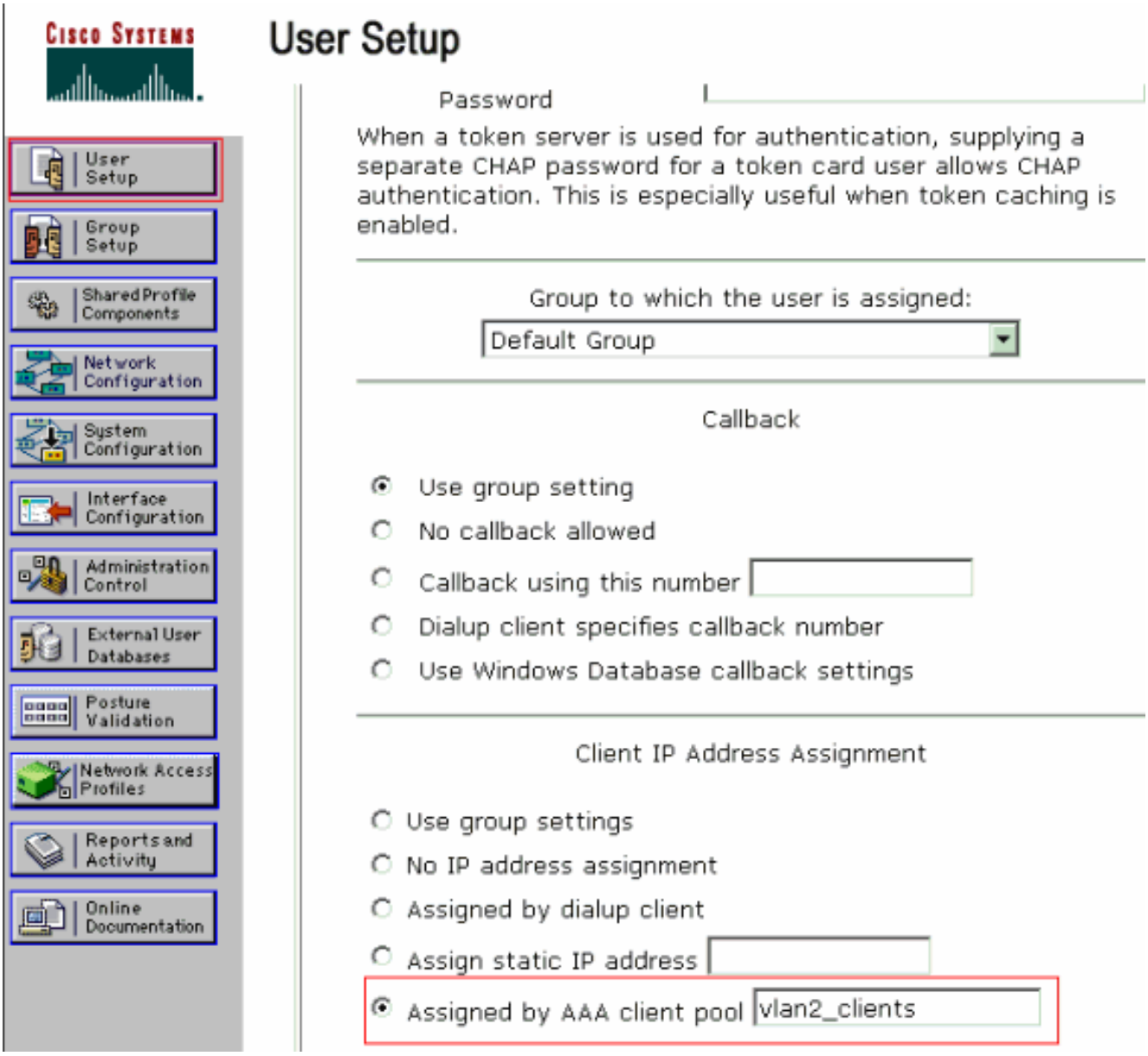
Observação: aqui, a configuração do usuário é mostrada somente para clientes que se conectam à VLAN 2. Para os usuários que se conectam à VLAN 3, siga o mesmo procedimento.

1. Para adicionar e configurar usuários, clique em **User Setup** e defina o nome de usuário e a senha.



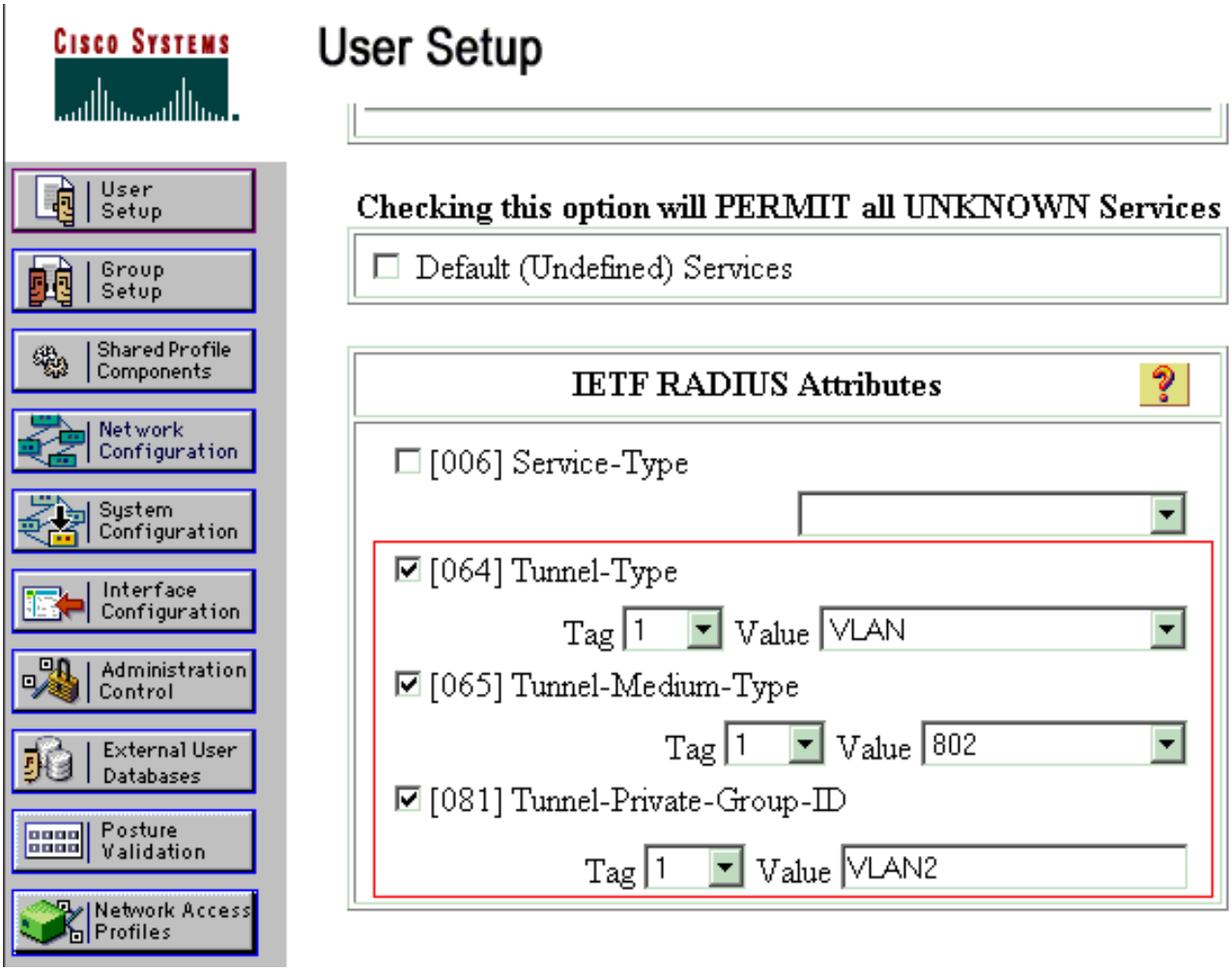
2. Defina a atribuição do endereço IP do cliente como **atribuído pelo pool de clientes AAA**. Insira o nome do pool de endereços IP configurado no switch para clientes VLAN

2.



Observação: selecione esta opção e digite o nome do pool IP do cliente AAA na caixa, somente se esse usuário tiver o endereço IP atribuído por um pool de endereços IP configurado no cliente AAA.

3. Defina os atributos da IETF (Internet Engineering Task Force) **64** e **65**.Certifique-se de que as Marcas dos Valores estejam definidas como **1**, como mostrado neste exemplo. O Catalyst ignora qualquer marca diferente de 1. Para atribuir um usuário a uma VLAN específica, você também deve definir o atributo **81** com um *nome* de VLAN ou *número de* VLAN que corresponda.**Observação:** se você usar o *nome* da VLAN, ele deve ser exatamente o mesmo configurado no
switch.



Observação: para obter mais informações sobre esses atributos IETF, consulte RFC 2868: Atributos do RADIUS para suporte de protocolo de túnel.**Observação:** na configuração inicial do servidor ACS, os atributos IETF RADIUS podem não ser exibidos na **configuração do usuário**. Para habilitar os atributos IETF nas telas de configuração do usuário, escolha **Interface configuration > RADIUS (IETF)**. Em seguida, verifique os atributos 64, 65 e 81 nas colunas User e Group.**Observação:** se você não definir o atributo IETF **81** e a porta for uma porta de switch no modo de acesso, o cliente terá atribuição à VLAN de acesso da porta. Se você definiu o atributo **81** para atribuição dinâmica de VLAN e a porta é uma porta de switch no modo de acesso, é necessário emitir o comando **aaa authorization network default group radius** no switch. Este comando atribui a porta à VLAN que o servidor de RADIUS fornece. Caso contrário, 802.1x move a porta para o estado AUTORIZADO após a autenticação do usuário; mas a porta ainda está na VLAN padrão da porta, e a conectividade pode falhar. Se você definiu o atributo **81**, mas configurou a porta como uma porta roteada, ocorre a negação de acesso. Esta mensagem de erro é exibida:

```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

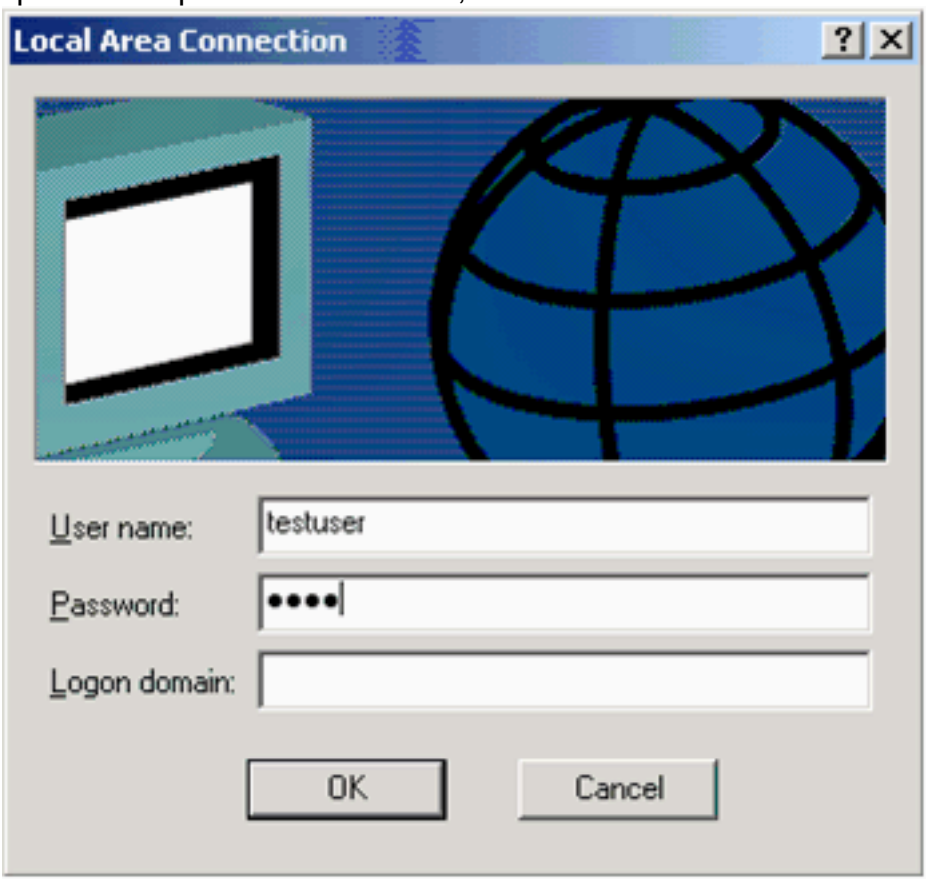
Configurar os PC Clients para Usar a Autenticação 802.1x

Este exemplo é específico do cliente do Protocolo de Autenticação Extensível (EAP - Extensible Authentication Protocol) sobre LAN (EAPOL - Microsoft Windows XP Extensible Authentication Protocol):

1. Escolha **Iniciar > Painel de controle > Conexões de rede**, clique com o botão direito do

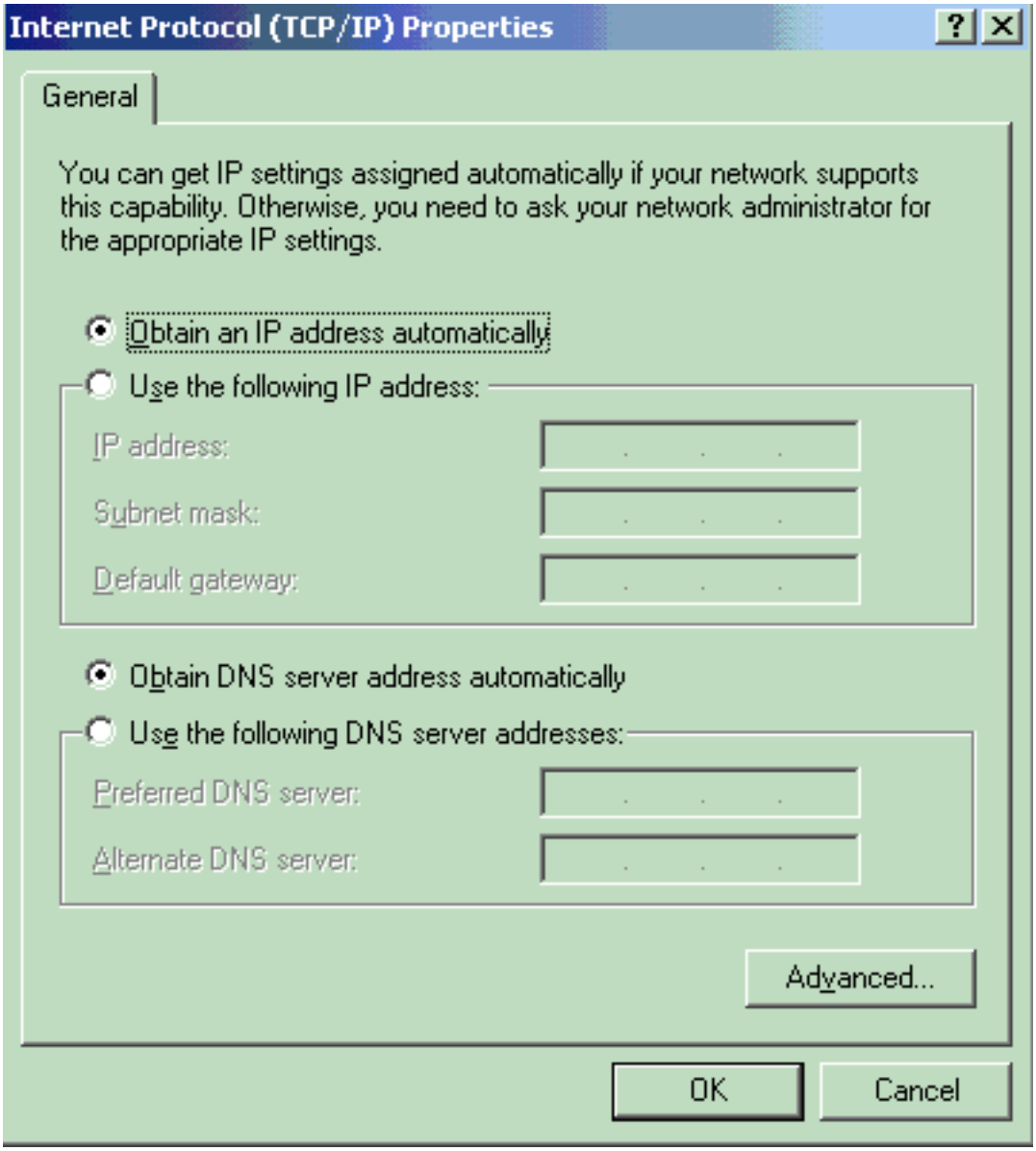
mouse em sua **Conexão local** e escolha **Propriedades**.

2. Marque **Mostrar ícone na área de notificação quando conectado** na guia Geral.
3. Na guia Authentication (Autenticação), marque Enable IEEE 802.1x authentication for this network (Habilitar autenticação 802.1x de IEEE para essa rede).
4. Defina o tipo de EAP para o desafio MD5, como mostra este exemplo:



Conclua estes passos para configurar os clientes para obter o endereço IP de um servidor DHCP.

1. Escolha **Iniciar > Painel de controle > Conexões de rede**, clique com o botão direito do mouse em sua **Conexão local** e escolha **Propriedades**.
2. Na guia Geral, clique em **Protocolo Internet (TCP/IP)** e em **Propriedades**.
3. Escolha **Obter um endereço IP automaticamente**.

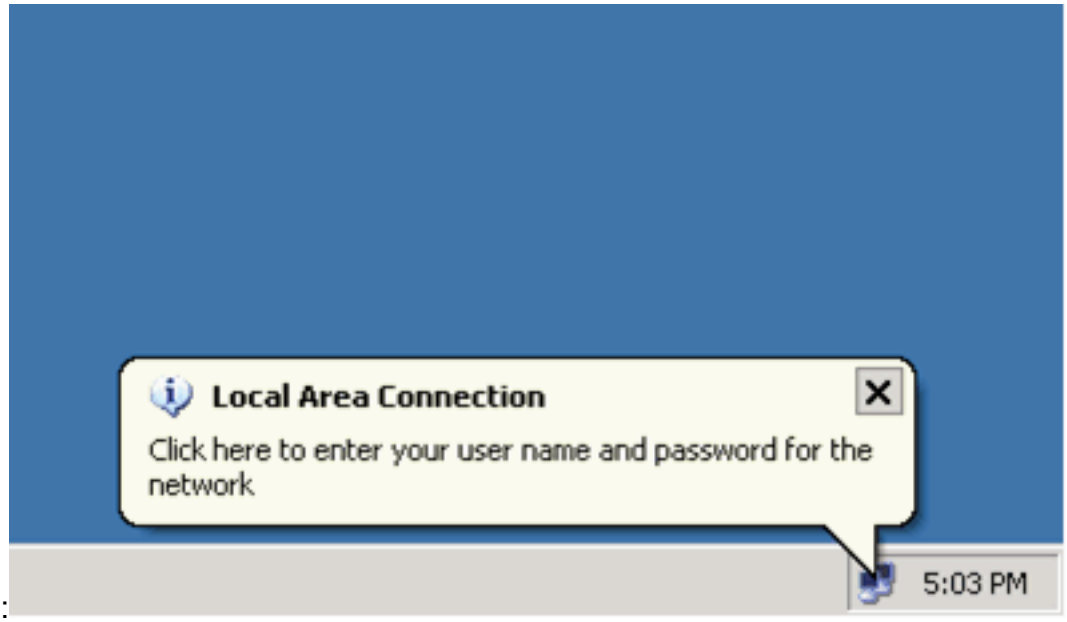


Verificar

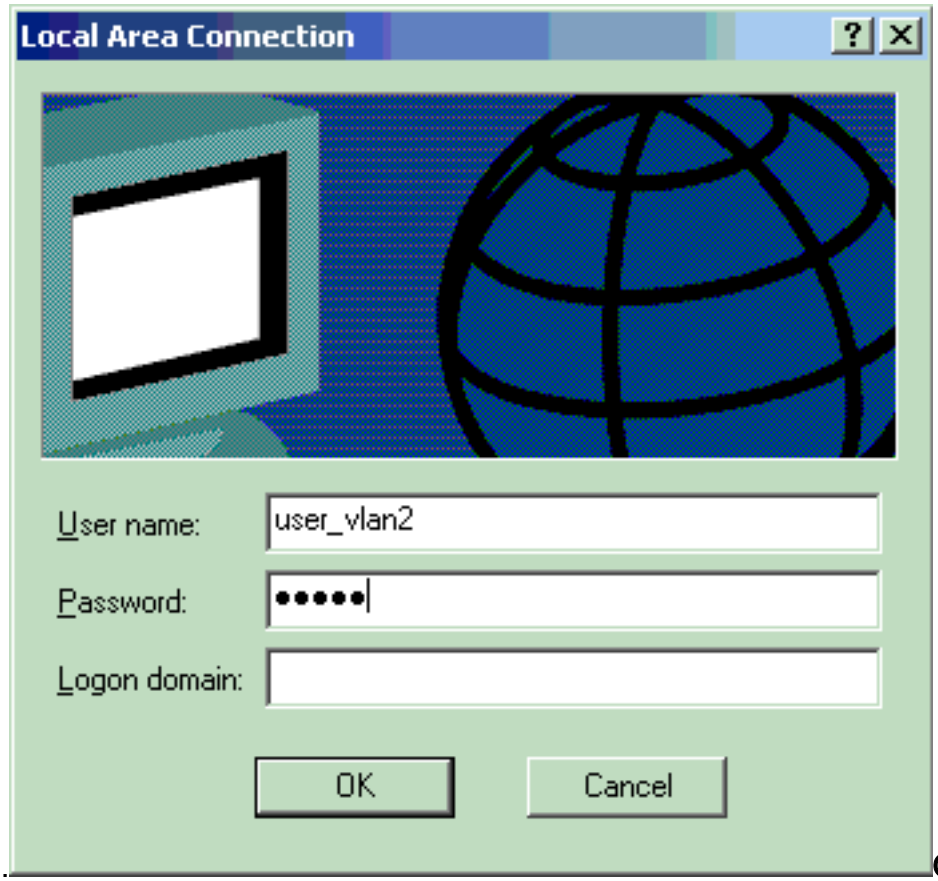
Clientes PC

Se você concluiu corretamente a configuração, os clientes do PC exibem um prompt pop-up para inserir um nome de usuário e uma senha.

1. Clique no prompt que este exemplo

mostra: 

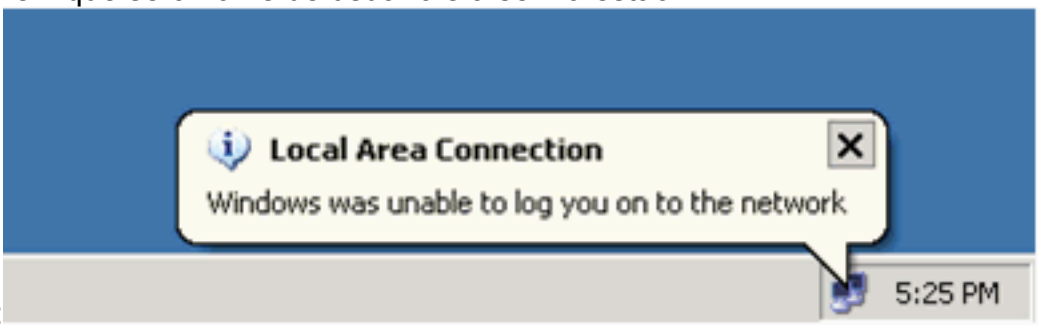
Uma janela de entrada de nome de usuário e senha é exibida.

2. Digite o nome de usuário e a 

senha. **Observação:** nos PCs 1 e 2, insira as credenciais de usuário da VLAN 2 e nos PCs 3 e 4 insira as credenciais de usuário da VLAN 3.
3. Se nenhuma mensagem de erro for exibida, verifique a conectividade com os métodos comuns, como por meio do acesso aos recursos da rede e com o **ping**. Esta saída é do PC 1 e mostra um **ping** bem-sucedido para o PC

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Wireless Network Connection:

   Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 172.16.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.2.1

C:\Documents and Settings\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:

Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

4: Se esse erro for exibido, verifique se o nome de usuário e a senha estão corretos:



Catalyst 6500

Se a senha e o nome de usuário parecerem estar corretos, verifique o estado da porta 802.1x no

switch.

1. Procure o status de uma porta que indica AUTORIZADO.

```
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      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/4
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/1
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
PortControl       = Force Authorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

Verifique o status da VLAN após a autenticação bem-sucedida.

```
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, Fa3/48
2    VLAN2                          active    Fa3/2, Fa3/3
3    VLAN3                          active    Fa3/4, Fa3/5
10   RADIUS_SERVER                  active    Fa3/1
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
!--- Output suppressed.
```

2. Verifique o status da associação DHCP no após a autenticação bem-sucedida.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.2.2       0100.1636.3333.9c       Mar 04 2007 06:35 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Mar 04 2007 06:43 AM    Automatic
172.16.3.2       0100.145e.945f.99       Mar 04 2007 06:50 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Mar 04 2007 06:57 AM    Automatic
```

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshoot

Colete a saída desses comandos **debug** para solucionar problemas:

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug dot1x events** —Habilita a depuração de instruções de impressão protegidas pelo flag de eventos dot1x.

```
Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- 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 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
   is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
    this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
   this id 13
```

```
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
   id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
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 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/4**

```
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
```

- **debug radius** — Exibe informações associadas ao RADIUS.

```
Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
```

!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18 CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79 00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80 18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104 00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19

```
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36:
Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18
11A7DD44 00:13:36: 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=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11
172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute
61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58:
Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from
id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58:
Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

Informações Relacionadas

- Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o exemplo de configuração de software CatOS
- Diretrizes para a implantação dos servidores Cisco Secure ACS para Windows NT/2000 em um ambiente de switch Cisco Catalyst
- RFC 2868: Atributos de RADIUS para suporte a protocolo de túnel
- Configurando a autenticação baseada em porta IEEE 802.1X
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems