

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o Catalyst Switch para a autenticação do 802.1x](#)

[Configurar o servidor Radius](#)

[Configurar os clientes PC para usar a autenticação do 802.1x](#)

[Verificar](#)

[Clientes PC](#)

[Catalyst 6500](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

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.

[Pré-requisitos](#)

[Requisitos](#)

Os leitores deste documento devem estar cientes destes tópicos:

- [Guia de Instalação para o Cisco Secure ACS for Windows 4.1](#)
- [Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1](#)
- [Como o RAIIO trabalha?](#)
- [Interruptor do catalizador e guia de distribuição 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 **Nota:** É necessário o software Cisco IOS versão 12.1(13)E ou posterior para suportar a autenticação 802.1x baseada em porta.
- Este exemplo usa o Serviço de controle de acesso Cisco Secure (ACS) 4.1 como o servidor Radius. **Nota:** Um servidor Radius deve ser especificado antes que você permita o 802.1x no interruptor.
- Clientes PC que apoia a autenticação do 802.1x **Nota:** Este exemplo usa clientes do Microsoft Windows XP.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

O padrão do IEEE 802.1X define um servidor cliente - controle de acesso e o protocolo de autenticação baseados que restringe dispositivos desautorizados da conexão a um LAN através das portas publicamente acessíveis. o 802.1x controla o acesso de rede criando dois pontos de acesso virtual distintos em cada porta. Um Access point é uma porta descontrolada; a outro é uma porta controlada. Todo o tráfego através da porta única está disponível a ambos os Access point. o 802.1x autentica cada dispositivo de usuário que é conectado a uma porta de switch e atribui a porta a um VLAN antes que faça disponível todos os serviços que estiverem oferecidos pelo interruptor ou pelo LAN. Até que o dispositivo esteja autenticado, o controle de acesso do 802.1x permite somente o protocolo extensible authentication sobre o tráfego LAN (EAPOL) através da porta a que o dispositivo é conectado. Depois que a autenticação é bem sucedida, o tráfego normal pode passar através da porta.

Nota: Se o interruptor recebe pacotes EAPOL da porta que não está configurada para a autenticação do 802.1x ou se o interruptor não apoia a autenticação do 802.1x, a seguir os pacotes EAPOL estão deixados cair e não enviados a nenhuns dispositivos ascendentes.

Configurar

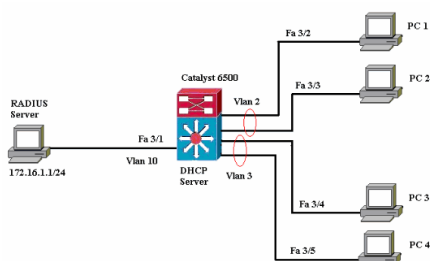
Nesta seção, você é apresentado com a informação para configurar a característica do 802.1x descrita neste documento.

Essa configuração requer estes passos:

- [Configurar o Catalyst Switch para a autenticação do 802.1x.](#)
- [Configurar o servidor Radius.](#)
- [Configurar os clientes PC para usar a autenticação do 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 interruptor mesmo se o cliente está autorizado alcançar o LAN e comutar serviços. Aqui, o servidor Radius é configurado para a autenticação e a atribuição de VLAN.
- Interruptor? Controla o acesso físico ao baseado na rede no status de autenticação do cliente. O interruptor atua como um intermediário (proxy) entre o cliente e o servidor Radius. Pede a informação de identidade do cliente, verifica essa informação com o servidor Radius, e retransmite uma resposta ao cliente. Aqui, o Catalyst 6500 Switch é configurado igualmente como um servidor DHCP. O apoio da autenticação do 802.1x para o protocolo de configuração dinâmica host (DHCP) permite que o servidor DHCP atribua os endereços IP de Um ou Mais Servidores Cisco ICM NT às classes diferentes de utilizadores finais adicionando a identidade do usuário autenticado no processo de descoberta DHCP.
- Clientes? Os dispositivos (estações de trabalho) esses pedem o acesso aos serviços LAN e de interruptor e respondem aos pedidos do interruptor. Aqui, os PC 1 4 são os clientes que pedem um acesso de rede autenticado. Os PC 1 e 2 usam as mesmas credenciais de logon que estão no VLAN2. Similarmente, os PC 3 e 4 usam umas credenciais de logon para clientes VLAN 3. PC são configurados para alcançar o endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP.

[Configurar o Catalyst Switch para a autenticação do 802.1x](#)

Esta configuração de switch da amostra inclui:

- Como permitir a autenticação do 802.1x em portas fastethernet.
- Como conectar um servidor Radius ao VLAN10 atrás da porta fastethernet 3/1.
- Uma configuração do servidor de DHCP para duas associações IP, uma para clientes no VLAN2 e a outro para clientes no VLAN3.
- Roteamento Inter-Vlan para ter a Conectividade entre clientes após a autenticação.

Refira [diretrizes com base na porta e limitações da autenticação do 802.1x](#) para as diretrizes em como configurar a autenticação do 802.1x.

Nota: Certifique-se de que o servidor Radius conecta sempre atrás de uma porta autorizada.

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, Fa3/482 VLAN2
active3 VLAN3 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.

```

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

[Configurar o servidor Radius](#)

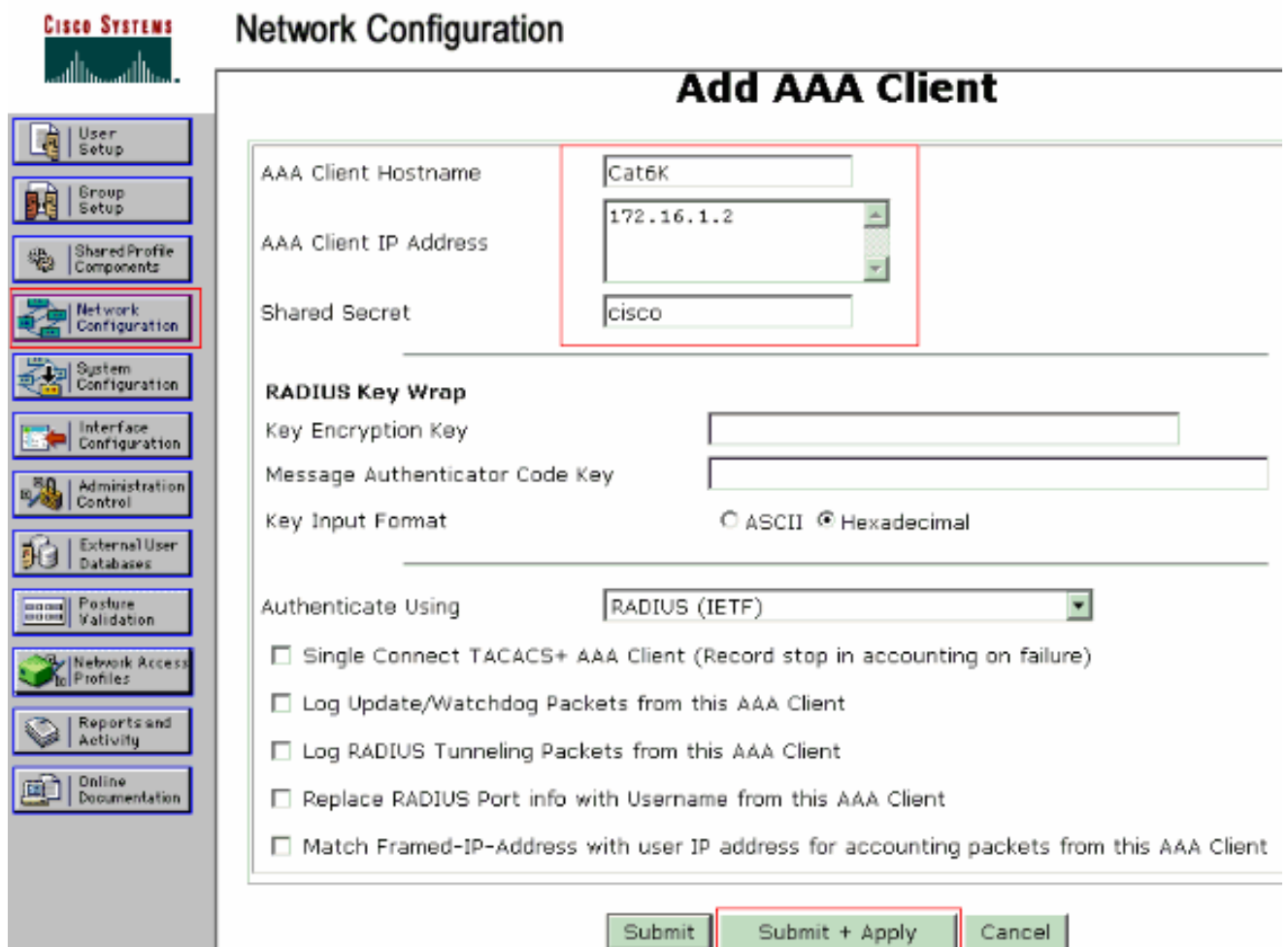
O servidor Radius é configurado com um endereço IP estático de 172.16.1.1/24. Termine estas

etapas a fim configurar o servidor Radius para um cliente de AAA:

1. Clique a **configuração de rede** na janela Administração ACS a fim configurar um cliente de AAA.
2. O clique **adiciona a entrada** sob a seção dos clientes de AAA.



3. Configurar o nome de host do cliente AAA, o endereço IP de Um ou Mais Servidores Cisco ICM NT, a chave secreta compartilhada e o tipo de autenticação como: Hostname do nome de host do cliente AAA = do interruptor (**Cat6K**). Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA = endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do interruptor (**172.16.1.2**). Segredo compartilhado = chave do RAO configurada no interruptor (**Cisco**). Autentique usando-se = o **RAIO IETF**. Nota: Para a operação correta, a chave secreta compartilhada deve ser idêntica no cliente de AAA e no ACS. As chaves são diferenciando maiúsculas e minúsculas.
4. O clique **submete-se + aplica-se** para fazer estas mudanças eficazes, porque este exemplo mostra:

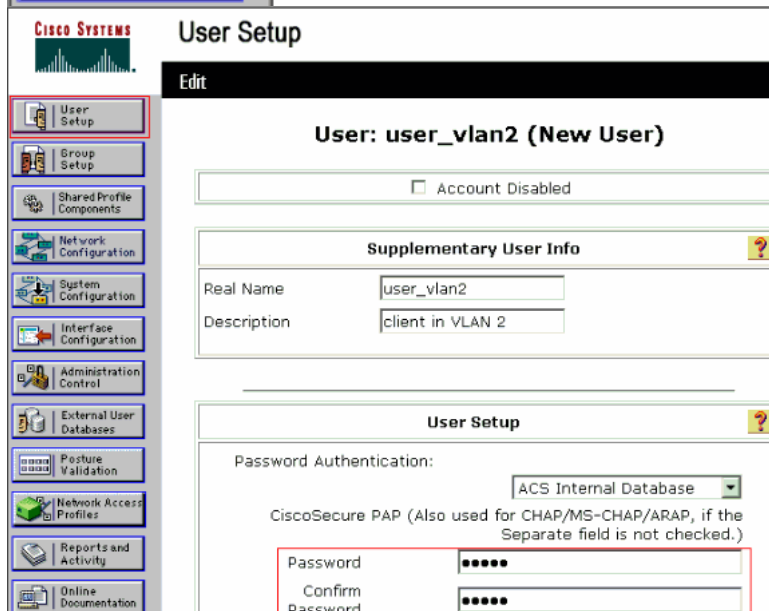
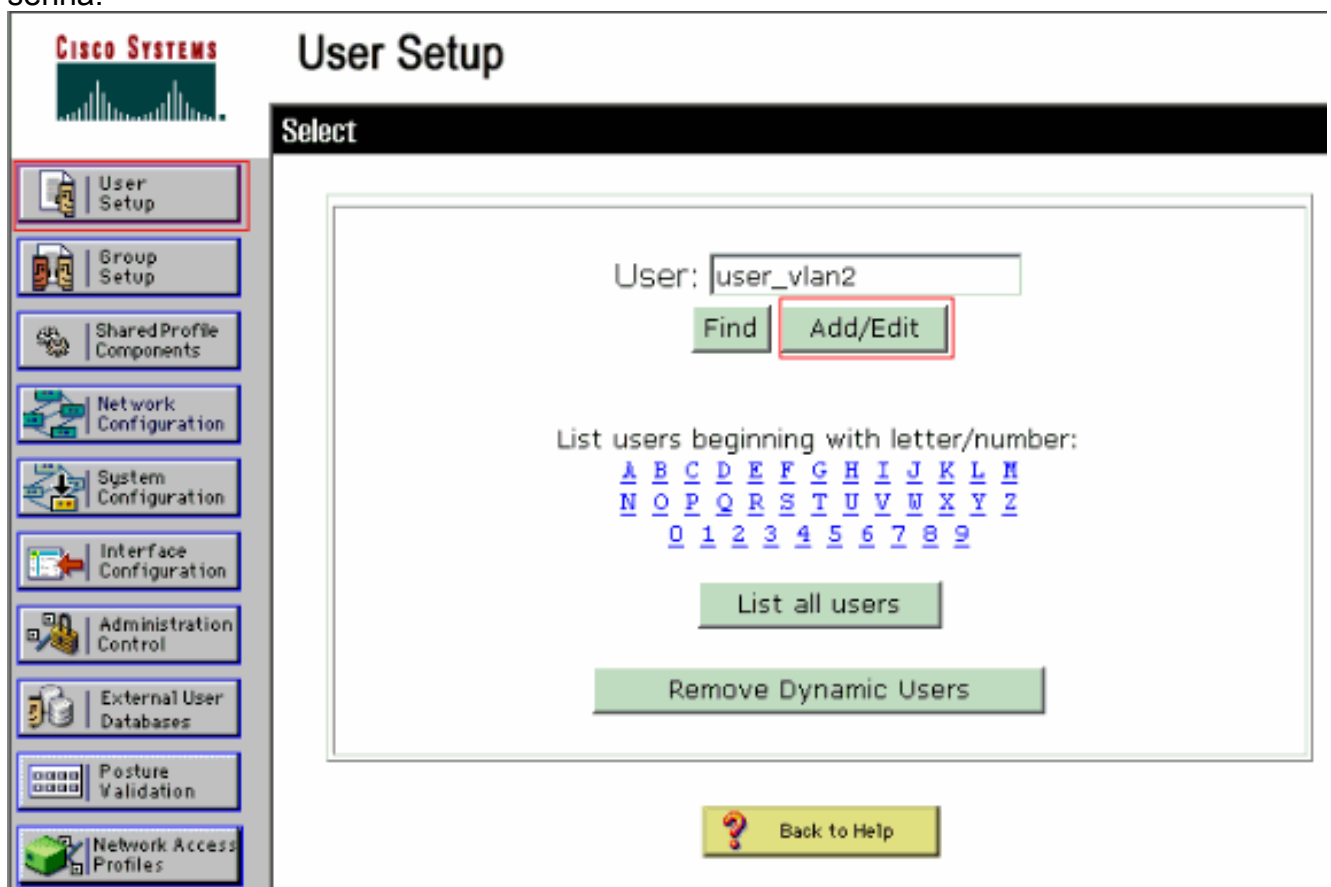


Termine estas etapas a fim configurar o servidor Radius para a autenticação, o VLAN e a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT.

Dois nomes de usuário têm que ser criados separadamente para os clientes que conectam ao VLAN2 assim como para o VLAN3. Aqui, um usuário **user_vlan2** para os clientes que conectam a VLAN2 e a um outro usuário **user_vlan3** para os clientes que conectam ao VLAN3 é criado por esse motivo.

Nota: Aqui, a configuração do usuário é mostrada para os clientes que conectam ao VLAN2 somente. Para os usuários que conectam ao VLAN3, siga o mesmo procedimento.

1. A fim adicionar e configurar usuários, **instalação de usuário** do clique e definir o nome de usuário e a senha.



- Defina a atribuição de endereço IP cliente como **atribuída pelo pool do cliente de AAA**. Dê entrada com o nome do pool do endereço IP de Um ou Mais Servidores Cisco ICM NT configurado no interruptor para os clientes VLAN2.

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

Nota: Selecione esta opção e datilografe o nome do IP pool do cliente de AAA na caixa, simplesmente se este usuário deve ter o endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído por um pool do endereço IP de Um ou Mais Servidores Cisco ICM NT configurado no cliente de AAA.

- Defina os atributos **64** e **65** do Internet Engineering Task Force (IETF). Certifique-se de que as etiquetas dos valores estão ajustadas a **1**, porque este exemplo mostra. O catalizador ignora toda a etiqueta a não ser 1. a fim atribuir um usuário a um VLAN específico, você deve igualmente definir o atributo **81** com um *nome* ou um número de VLAN VLAN que corresponda. **Nota:** Se você usa o *nome* VLAN, deve ser exatamente mesmo que esse

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

configurado no interruptor.

Nota: Para obter mais informações

sobre destes atributos IETF, refira o [RFC 2868: Atributos do RADIUS para suporte de protocolo de túnel.](#) **Nota:** Na configuração inicial do servidor ACS, os atributos de raio de IETF podem não indicam na **instalação de usuário**. A fim permitir atributos IETF em telas da configuração do usuário, escolha a **configuração da interface > o RAIO (IETF)**. Em seguida, verifique os atributos 64, 65 e 81 nas colunas User e Group.**Nota:** Se você não define o atributo 81 IETF e a porta é uma porta de switch no modo de acesso, o cliente tem a atribuição ao acesso VLAN da porta. Se você definiu o atributo 81 para a atribuição do VLAN dinâmico e a porta é uma porta de switch no modo de acesso, você precisa de emitir o **raio do grupo padrão** do comando `aaa authorization network` no interruptor. Este comando atribui a porta à VLAN que o servidor de RADIUS fornece. Se não, o 802.1x move a porta para o estado `AUTORIZADO` após a autenticação do usuário; mas a porta está ainda no VLAN padrão da porta, e a Conectividade pode falhar. Se você definiu o atributo 81, mas você configurou a porta como uma porta roteada, a recusa do acesso ocorre. Esta mensagem de erro é

```

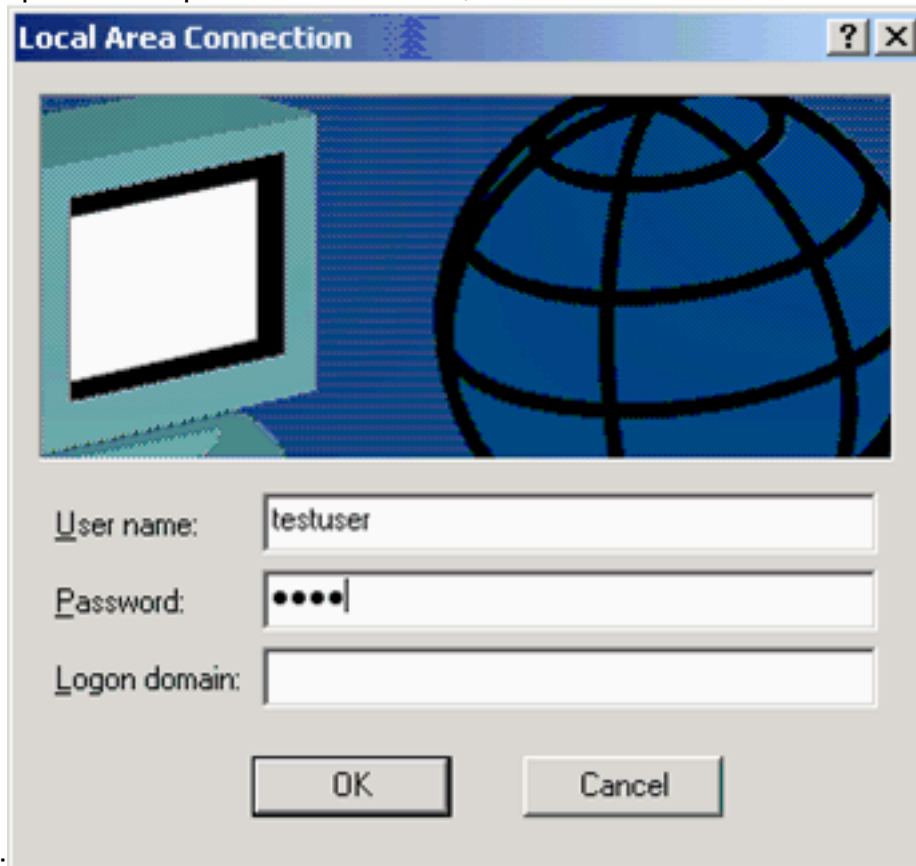
exibida:Router#configure terminalEnter configuration commands, one per line. End with
CNTL/Z.Router(config)#hostname Cat6K!-- Sets the hostname for the switch.Cat6K(config)#vlan
2Cat6K(config-vlan)#name VLAN2Cat6K(config-vlan)#vlan 3Cat6K(config-vlan)#name VLAN3!-- VLAN
should be existing in the switch 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, Fa3/482 VLAN2 active3 VLAN3
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.

```


Configurar os clientes PC para usar a autenticação do 802.1x

Este exemplo é específico ao Extensible Authentication Protocol (EAP) do Microsoft Windows XP sobre o cliente LAN (EAPOL):

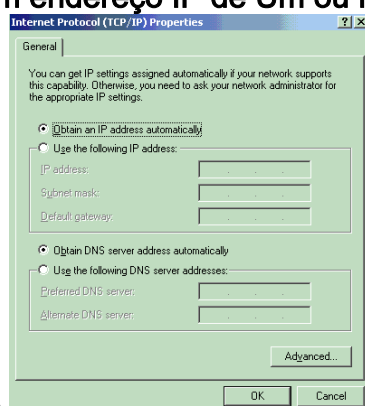
1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**, a seguir clicar com o botão direito em sua **conexão de área local** e escolha **propriedades**.
2. Verifique o ícone da mostra na área de notificação quando conectado sob o tab geral.
3. Na guia Authentication (Autenticação), marque **Enable 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:

Termine estas etapas para configurar os clientes para obter o endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP.

1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**, a seguir clicar com o botão direito em sua **conexão de área local** e escolha **propriedades**.
2. Sob o tab geral, clique o **protocolo de internet (TCP/IP)** e então as **propriedades**.
3. Escolha **obtem um endereço IP de Um ou Mais Servidores Cisco ICM NT**



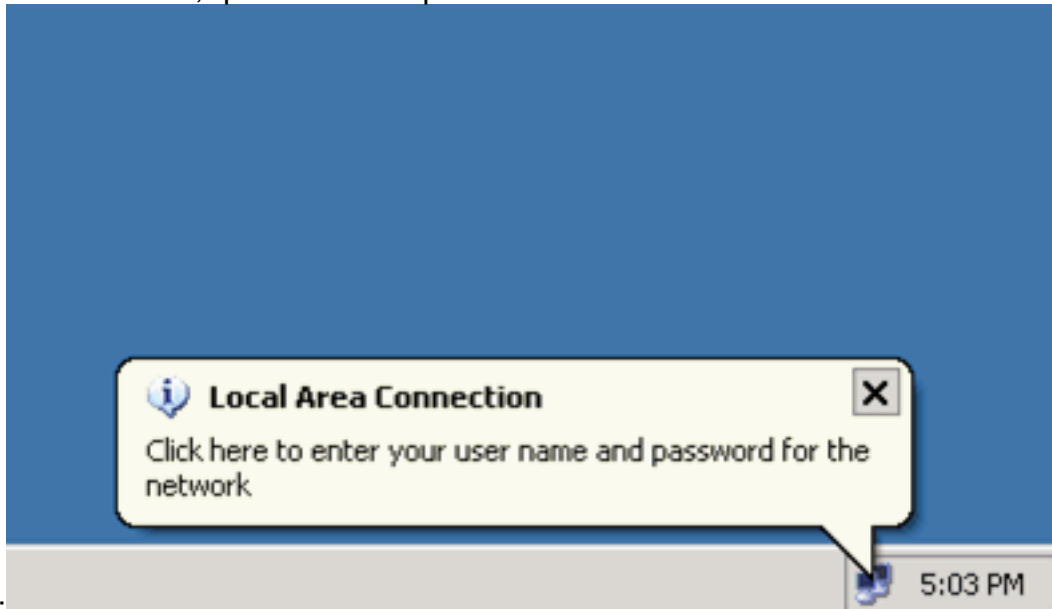
automaticamente.

Verificar

Cientes PC

Se você tem completado corretamente a configuração, os clientes PC indicam uma alerta do pop-up para incorporar um nome de usuário e uma senha.

1. Clique sobre a alerta, que este exemplo

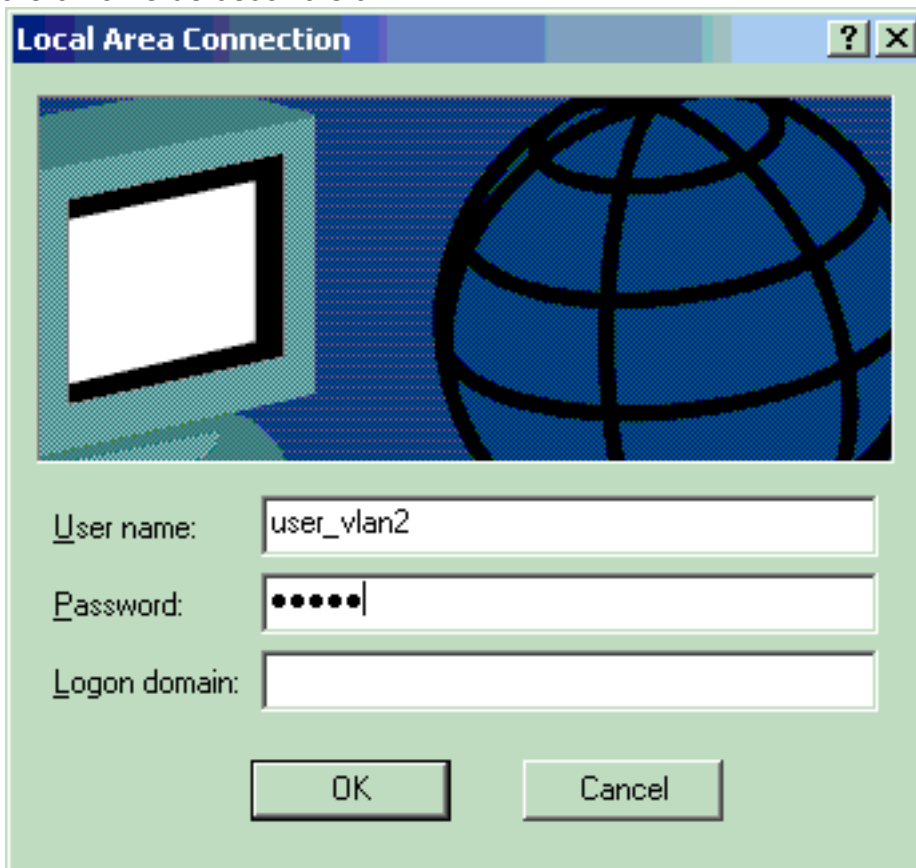


mostra:

s do indicador de um nome de usuário e da entrada de senha.

Indicadore

2. Incorpore o nome de usuário e a



senha.

Nota: No PC1 e em

2, incorpore credenciais do usuário VLAN2 e no PC3 e em 4 incorpore credenciais do usuário VLAN3.

3. Se nenhuma Mensagem de Erro aparece, verifique a Conectividade com os métodos comuns, tais como o acesso direto dos recursos de rede e com sibilos. Esta saída é do PC1, e mostra um ping bem-sucedido a 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

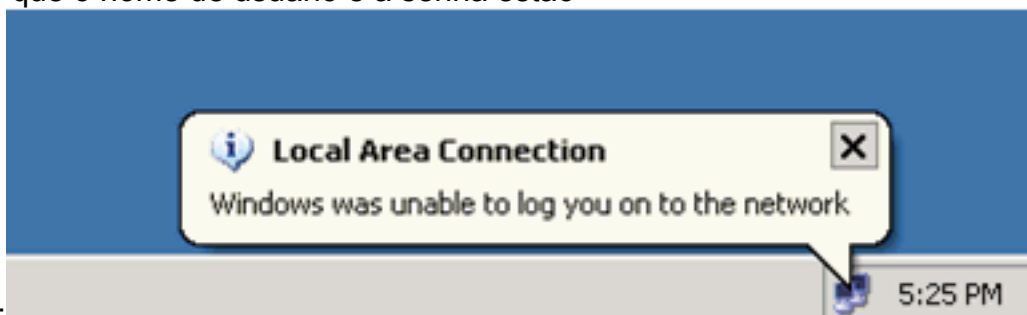
Pinging 172.16.3.2 with 32 bytes of data:

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: C:\Documents and Settings\Administrator> Se este erro aparece, verifique que o nome de usuário e a senha estão



corretos:

Catalyst 6500

Se a senha e o nome de usuário parecem estar corretos, verifique o estado de porta do 802.1x no interruptor.

1. Procure um status de porta que indique 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 =
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 3/1`Default 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

Verifique o status de 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, Fa3/482 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. Verifique o estado obrigatório DHCP do 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 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
- [A Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Recolha a saída destes comandos debug a fim pesquisar defeitos:

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

- debugar eventos do dot1x? Permite a eliminação de erros das indicações da cópia guardadas pela bandeira de eventos do dot1x. `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#

```

- **debugar o raio?** Indica a informação associada com o RAIIO.



```

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 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
FFFFFFFE00:13:36: 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 FFFFFFFF00:19:58: 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#
```

[Informações Relacionadas](#)

- [Autenticação do IEEE 802.1X com o Catalyst 6500/6000 que executa o exemplo de configuração do CatOS Software](#)
- [Diretrizes para o desenvolvimento do Cisco Secure ACS para server de Windows Nt/2000 em um ambiente do interruptor do Cisco catalyst](#)
- [RFC 2868: Atributos de RADIUS para suporte a protocolo de túnel](#) 
- [Configurando a autenticação com base na porta do IEEE 802.1X](#)
- [Suporte a Produtos de LAN](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)