Índice

Introdução

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

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 RAIO 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 a CatOS Software release 8.5(6) no Supervisor Engine e o Cisco IOS Software Release 12.2(18)SXF no MSFC**Nota:** Você precisa a liberação 6.2 de CatOS ou mais atrasado de apoiar a autenticação com base na porta do 802.1x.**Nota:** Antes que o Software Release 7.2(2), uma vez que o host do 802.1x está autenticado, ele se juntar a um VLAN NVRAM-configurado. Com liberações do Software Release 7.2(2) e Mais Recente, após a autenticação, um host do 802.1x pode receber sua atribuição de VLAN do servidor Radius.
- 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 de permitir 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 de fazer disponível algum serviços que for oferecido pelo interruptor ou pelo LAN. Até que o dispositivo esteja autenticado, o controle de acesso do 802.1x permite somente o Extensible Authentication Protocol (EAP) 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.

Configurar

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

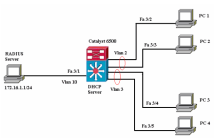
Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

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, pedindo a informação de identidade do cliente, verificando essa informação com o servidor Radius, e retransmitindo 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) esse acesso do pedido 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 usarão as mesmas credenciais de logon para estar no VLAN2. Similarmente, os PC 3 e 4 usarão 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.**Nota:** Nesta configuração, todo o cliente que falhar a autenticação ou qualquer cliente capaz non-802.1x que conecta ao interruptor são negados o acesso de rede movendo os para um VLAN não utilizado (VLAN 4 ou 5) que usa as características da falha de autenticação e do convidado VLAN.

Configurar o Catalyst Switch para a autenticação do 802.1x

Esta configuração de switch da amostra inclui:

- Permita a autenticação do 802.1x e características associadas em portas fastethernet.
- Conecte o servidor Radius ao VLAN10 atrás da porta fastethernet 3/1.
- Configuração do servidor de DHCP para duas associações IP, uma para clientes no VLAN2 e outro para clientes no VLAN3.
- Roteamento Inter-Vlan para ter a Conectividade entre clientes após a autenticação.

Refira diretrizes da configuração de autenticação 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

```
Console (enable) set system name Cat6K System name set.!---
Sets the hostname for the switch.Cat6K> (enable) set
localuser user admin password ciscoAdded local user
admin.Cat6K> (enable) set localuser authentication
enableLocalUser authentication enabled!--- Uses local user
authentication to access the switch.Cat6K> (enable) set vtp
domain ciscoVTP domain cisco modified!--- Domain name must be
configured for VLAN configuration.Cat6K> (enable) set vlan 2
name VLAN2VTP advertisements transmitting temporarily
stopped,and will resume after the command finishes.Vlan 2
configuration successful!--- VLAN should be existing in the
switch !--- for a successsful authentication.Cat6K> (enable)
set vlan 3 name VLAN3VTP advertisements transmitting
temporarily stopped,and will resume after the command
```

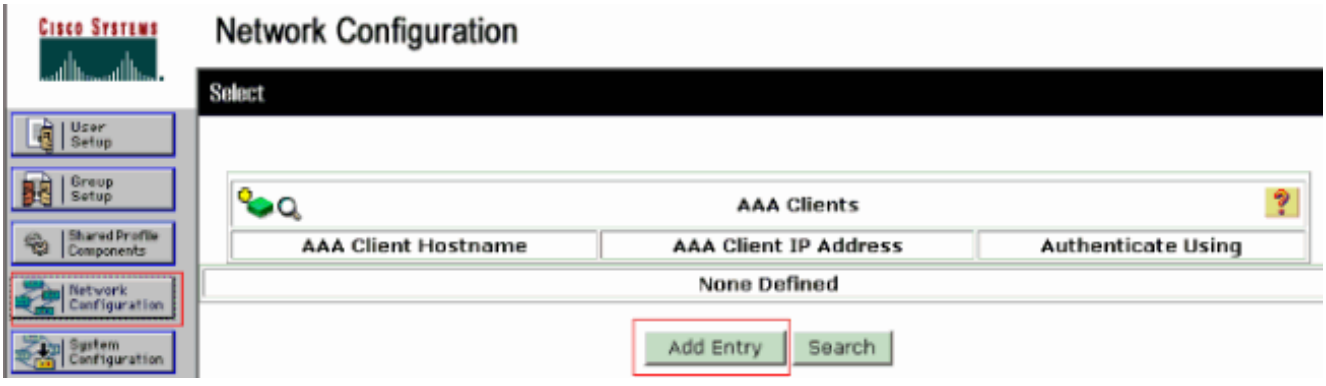
finishes.Vlan 3 configuration successful*!--- VLAN names will be used in RADIUS server for VLAN assignment.*Cat6K> (enable) **set vlan 4 name AUTHFAIL_VLAN**VTP advertisements transmitting temporarily stopped,and will resume after the command finishes.Vlan 4 configuration successful*!--- A VLAN for non-802.1x capable hosts.*Cat6K> (enable) **set vlan 5 name GUEST_VLAN**VTP advertisements transmitting temporarily stopped,and will resume after the command finishes.Vlan 4 configuration successful*!--- A VLAN for failed authentication hosts.*Cat6K> (enable) **set vlan 10 name RADIUS_SERVER**VTP advertisements transmitting temporarily stopped,and will resume after the command finishes.Vlan 10 configuration successful*!--- This is a dedicated VLAN for the RADIUS Server.*Cat6K> (enable) **set interface sc0 10 172.16.1.2 255.255.255.0**Interface sc0 vlan set, IP address and netmask set.*!---* **Note:** 802.1x authentication always uses the !--- sc0 interface as the identifier for the authenticator !--- when communicating with the RADIUS server.Cat6K> (enable) **set vlan 10 3/1**VLAN 10 modified.VLAN 1 modified.VLAN Mod/Ports---- ---------------------10   3/1*!--- Assigns port connecting to RADIUS server to VLAN 10.*Cat6K> (enable) **set radius server 172.16.1.1 primary**172.16.1.1 with auth-port 1812 acct-port 1813 added to radius server table as primary server.*!--- Sets the IP address of the RADIUS server.*Cat6K> (enable) **set radius key cisco**Radius key set to cisco*!--- The key must match the key used on the RADIUS server.*Cat6K> (enable) **set dot1x system-auth-control enable**dot1x system-auth-control enabled.Configured RADIUS servers will be used for dot1x authentication.*!--- Globally enables 802.1x. !--- You must specify at least one RADIUS server before !--- you can enable 802.1x authentication on the switch.*Cat6K> (enable) **set port dot1x 3/2-48 port-control auto**Port 3/2-48 dot1x port-control is set to auto.Trunking disabled for port 3/2-48 due to Dot1x feature.Spantree port fast start option enabled for port 3/2-48.*!--- Enables 802.1x on all FastEthernet ports. !--- This disables trunking and enables portfast automatically.*Cat6K> (enable) **set port dot1x 3/2-48 auth-fail-vlan 4**Port 3/2-48 Auth Fail Vlan is set to 4*!--- Ports will be put in VLAN 4 after three !--- failed authentication attempts.*Cat6K> (enable) **set port dot1x 3/2-48 guest-vlan 5**Ports 3/2-48 Guest Vlan is set to 5*!--- Any non-802.1x capable host connecting or 802.1x !--- capable host failing to respond to the username and password !--- authentication requests from the Authenticator is placed in the !--- guest VLAN after 60 seconds. !---* **Note:** An authentication failure VLAN is independent !--- of the guest VLAN. However, the guest VLAN can be the same !--- VLAN as the authentication failure VLAN. If you do not want to !--- differentiate between the non-802.1x capable hosts and the !--- authentication failed hosts, you can configure both hosts to !--- the same VLAN (either a guest VLAN or an authentication failure VLAN). !--- For more information, refer to !--- Understanding How 802.1x Authentication for the Guest VLAN Works.Cat6K> (enable) **switch console**Trying Router-16...Connected to Router-16.Type ^C^C^C to switch back...*!--- Transfers control to the routing module (MSFC).*Router>**enable**Router#**conf t**Enter configuration commands, one per line. End with CNTL/Z.Router(config)#**interface vlan 10**Router(config-if)#**ip address 172.16.1.3 255.255.255.0***!--- This is used as the gateway address in RADIUS server.*Router(config-if)#**no shut**Router(config-if)#**interface vlan 2**Router(config-if)#**ip address 172.16.2.1 255.255.255.0**Router(config-if)#**no shut***!--- This is the gateway address for clients in VLAN*

```
2.Router(config-if)#interface vlan 3Router(config-if)#ip
address 172.16.3.1 255.255.255.0Router(config-if)#no shut!---
This is the gateway address for clients in VLAN
3.Router(config-if)#exitRouter(config)#ip dhcp pool
vlan2_clientsRouter(dhcp-config)#network 172.16.2.0
255.255.255.0Router(dhcp-config)#default-router 172.16.2.1!--
- This pool assigns ip address for clients in VLAN
2.Router(dhcp-config)#ip dhcp pool vlan3_clientsRouter(dhcp-
config)#network 172.16.3.0 255.255.255.0Router(dhcp-
config)#default-router 172.16.3.1!--- This pool assigns ip
address for clients in VLAN 3.Router(dhcp-
config)#exitRouter(config)#ip dhcp excluded-address
172.16.2.1Router(config)#ip dhcp excluded-address
172.16.3.1!--- In order to go back to the Switching module,
!--- enter Ctrl-C three times.Router#Router#^CCat6K>
(enable)Cat6K> (enable) show vlanVLAN Name Status IfIndex
Mod/Ports, Vlans---- ------------------ --------- ------- ---
--------------------1    default
active    6       2/1-2
3/2-48               2    VLAN2
active    833    VLAN3                              active
844    AUTHFAIL_VLAN                    active    85      5
GUEST_VLAN                        active    8610
RADIUS_SERVER                     active    87      3/11002
fddi-default                      active    781003 token-ring-
default               active    811004 fddinet-default
active    791005 trnet-default                    active
80!--- Output suppressed. !--- All active ports will be in
VLAN 1 (except 3/1) before authentication.Cat6K> (enable)
show dot1xPAE Capability             Authenticator
OnlyProtocol Version           1system-auth-control
enabledmax-req                    2quiet-period
60 secondsre-authperiod              3600 secondsserver-
timeout             30 secondsshutdown-timeout           300
secondssupp-timeout               30 secondstx-period
30 seconds!--- Verifies dot1x status before
authentication.Cat6K> (enable)
```

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:

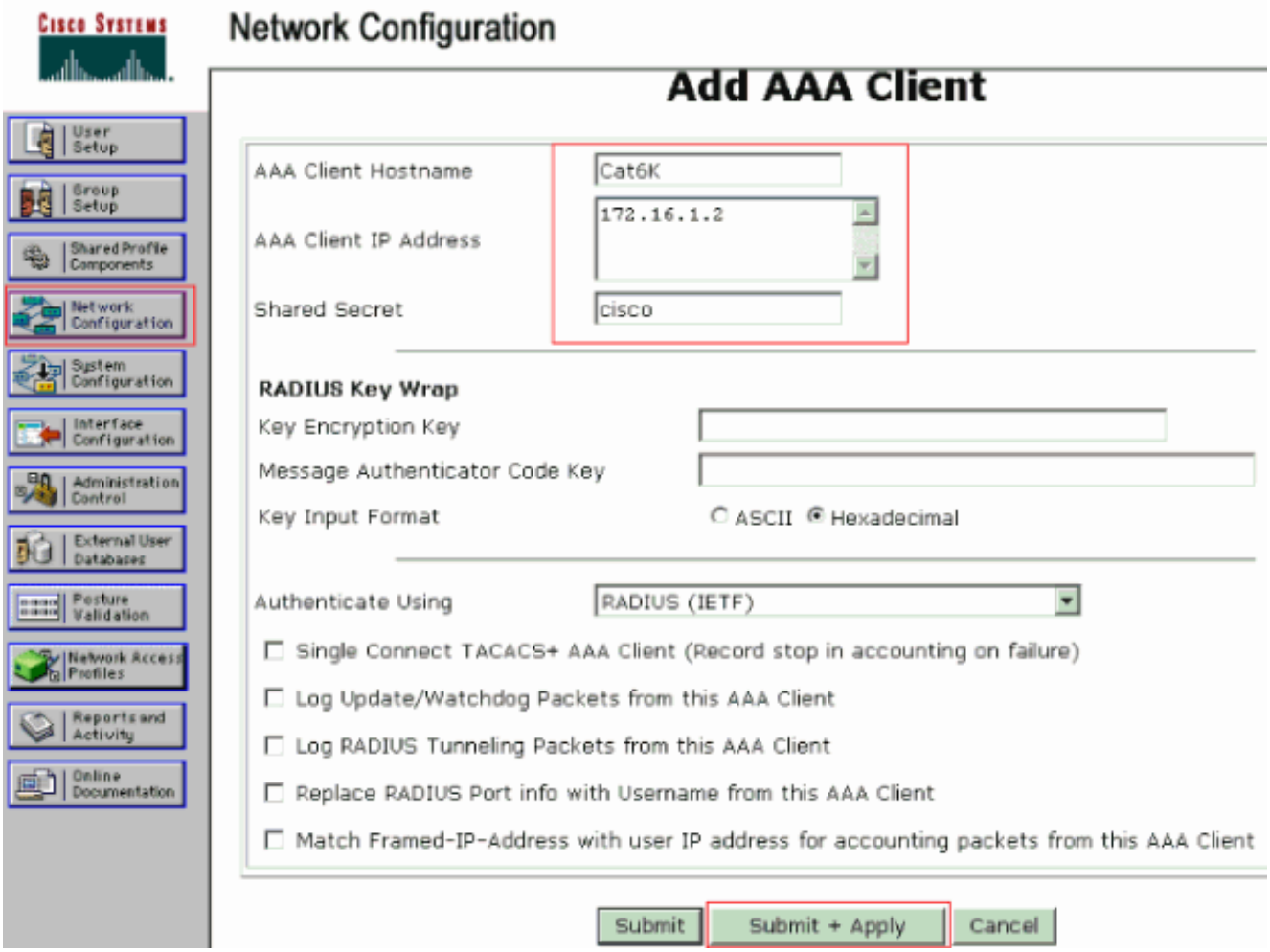
1. A fim configurar um cliente de AAA, clique a **configuração de rede na** janela Administração ACS.
2. O clique **adiciona a entrada** sob a seção dos clientes de AAA.



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 do 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 = interface de gerenciamento (endereço sc0)IP do interruptor (**172.16.1.2**).Segredo compartilhado = chave do raio 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.

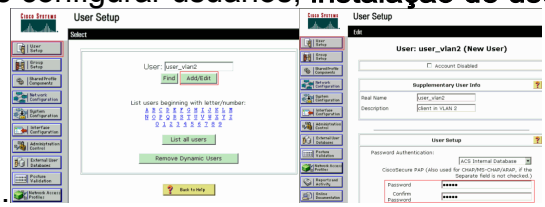
4. O clique **submete-se + aplica-se** para fazer estas mudanças eficazes, porque este exemplo mostra:



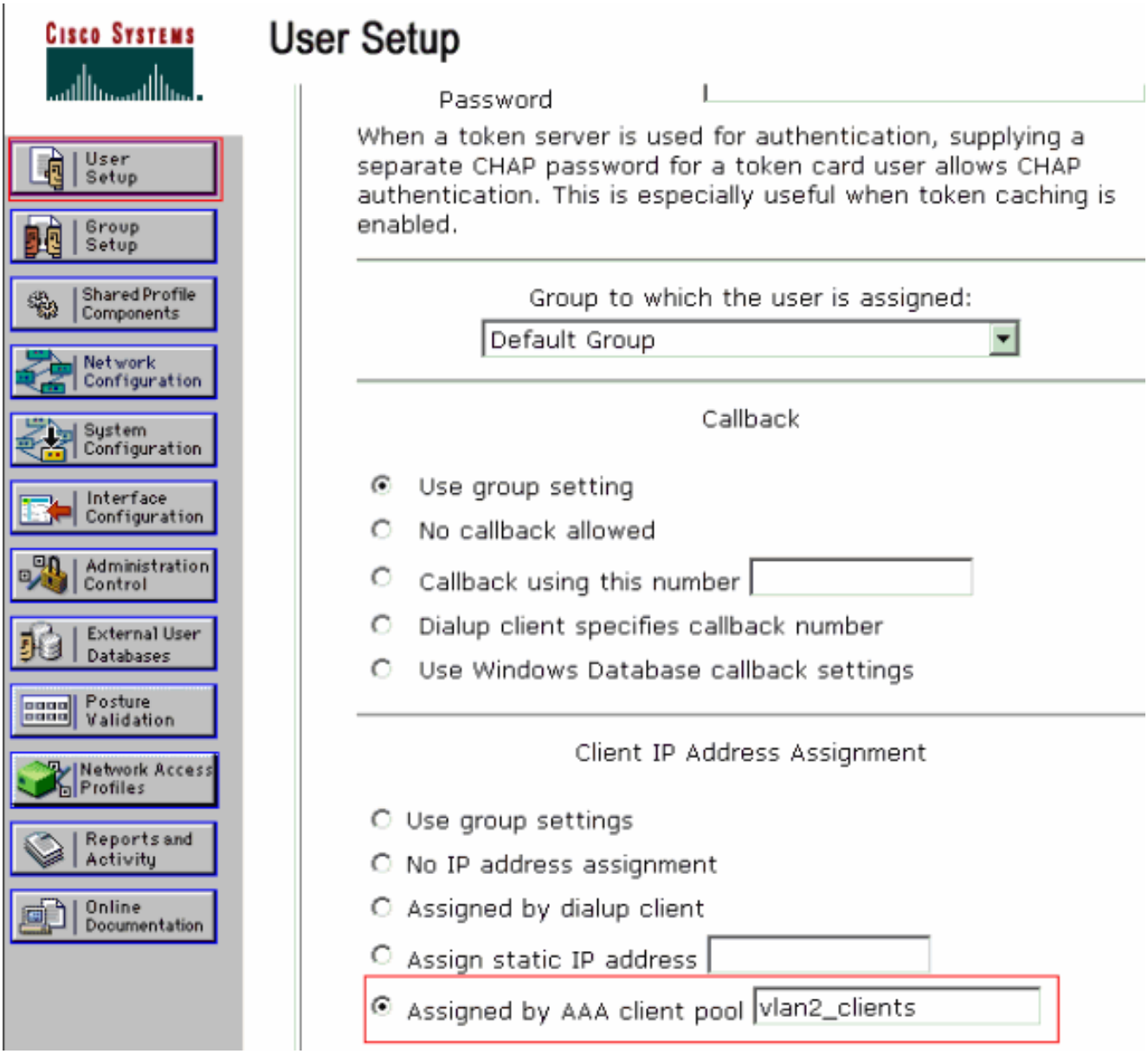
Termine estas etapas a fim configurar o servidor Radius para a autenticação, o VLAN e a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT:

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 ao VLAN2 e um outro usuário **user_vlan3** para os clientes que conectam ao VLAN3 são criados 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, termine o mesmo procedimento.

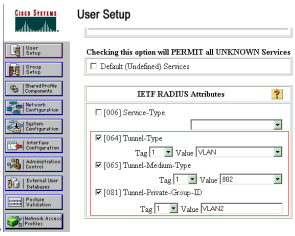
1. A fim adicionar e configurar usuários, **instalação de usuário do** clique e definir o nome de usuário e senha. 

2. 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.



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.

3. 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* VLAN que corresponda.**Nota:** *O nome* VLAN deve ser exatamente mesmo que esse configurado no interruptor.**Nota:** A atribuição de VLAN baseada no número de VLAN não é apoiada com



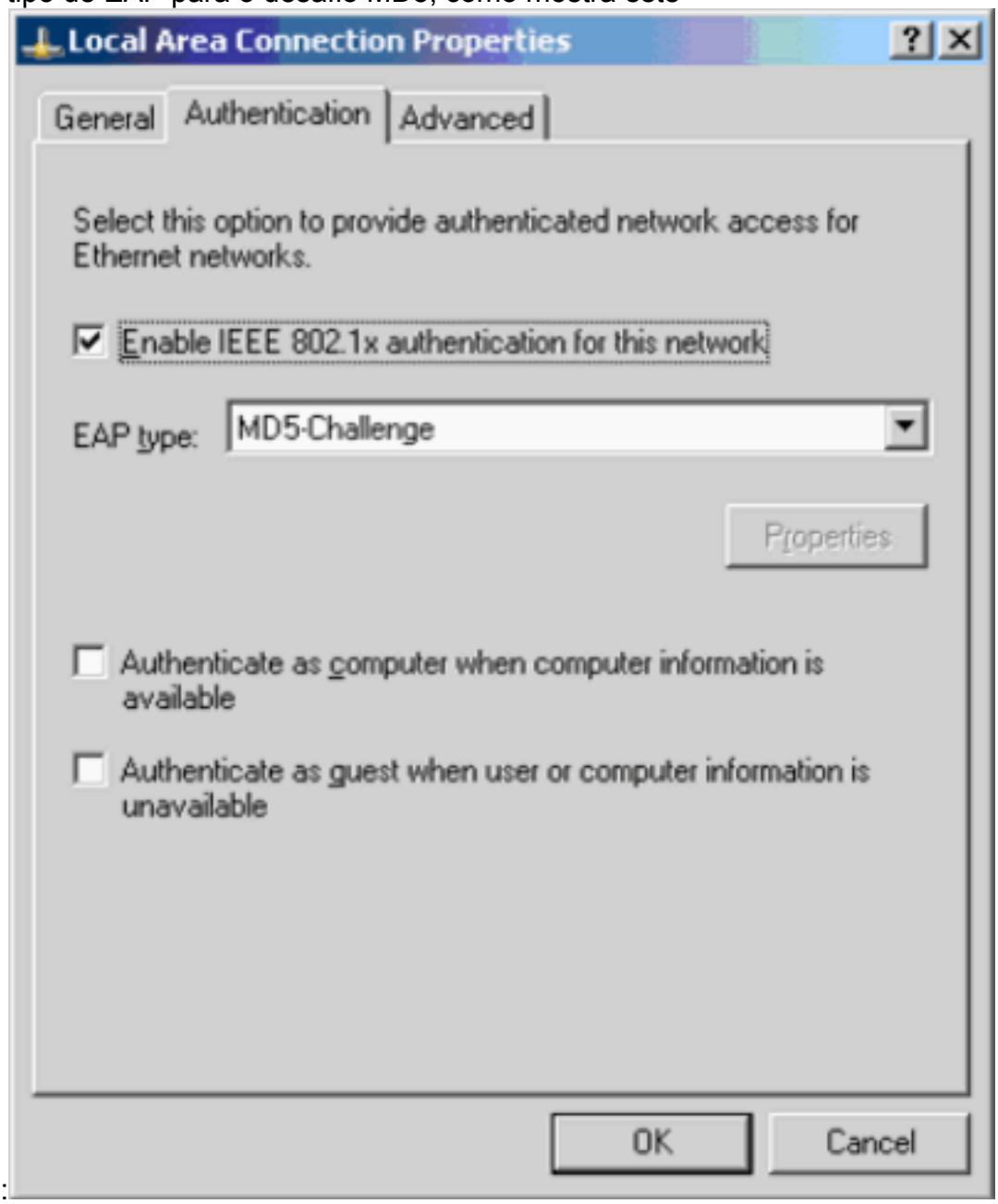
CatOS. Refira o [RFC 2868: Atributos RADIUS para o apoio do protocolo

de túnel para obter mais informações sobre destes atributos IETF.**Nota:** Na configuração inicial do servidor ACS, os atributos de raio de IETF podem não indicam na **instalação de usuário**. Escolha a **configuração da interface > o RAIO (IETF)** a fim permitir atributos IETF na tela da configuração do usuário. Em seguida, verifique os atributos 64, 65 e 81 nas colunas User e Group.

Configurar os clientes PC para usar a autenticação do 802.1x

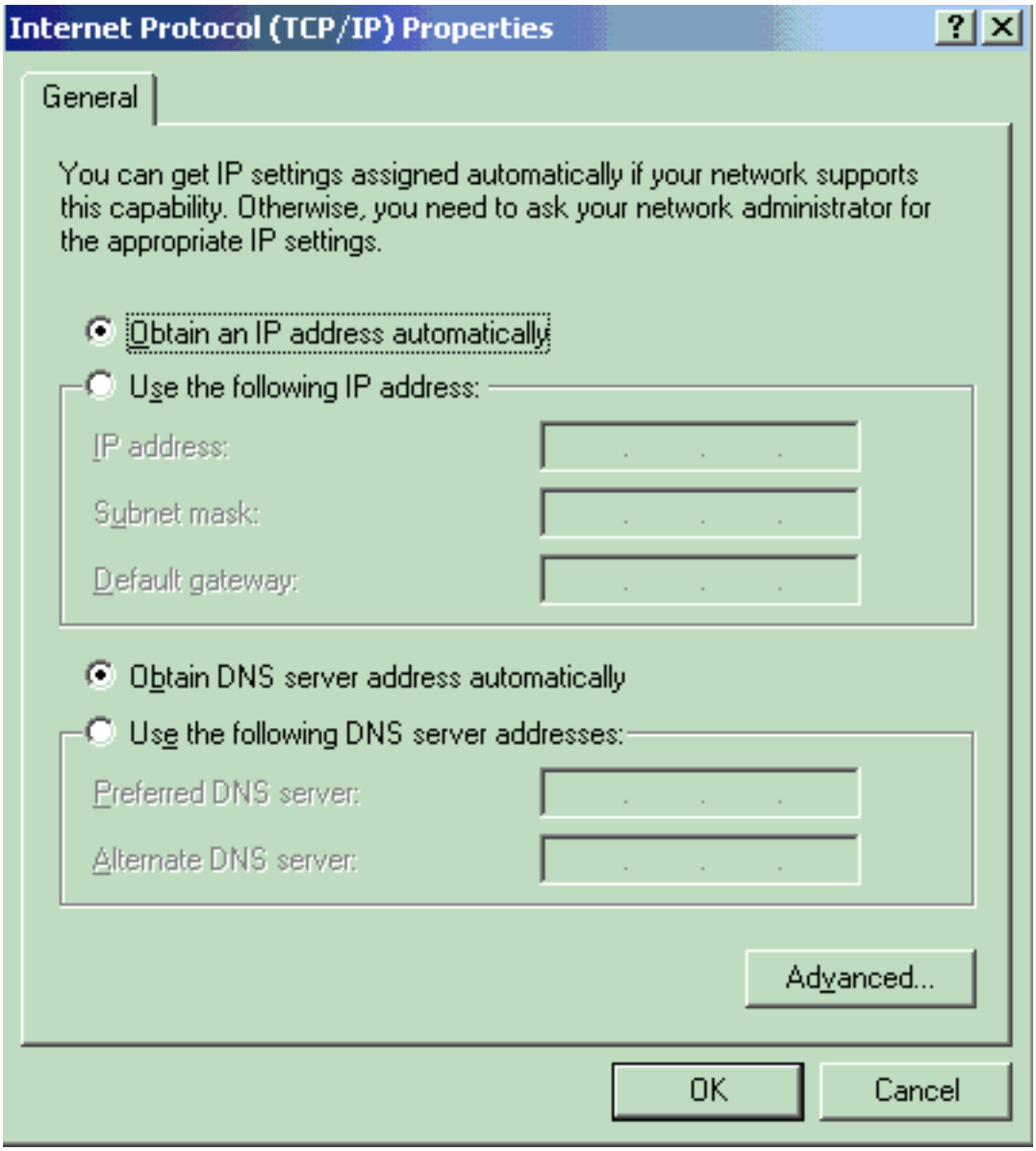
Este exemplo é específico ao Extensible Authentication Protocol (EAP) do Microsoft Windows XP sobre o cliente LAN (EAPOL). Conclua estes passos:

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 a fim configurar os clientes para obter um 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 **obtêm um endereço IP de Um ou Mais Servidores Cisco ICM NT automaticamente**.



Verificar

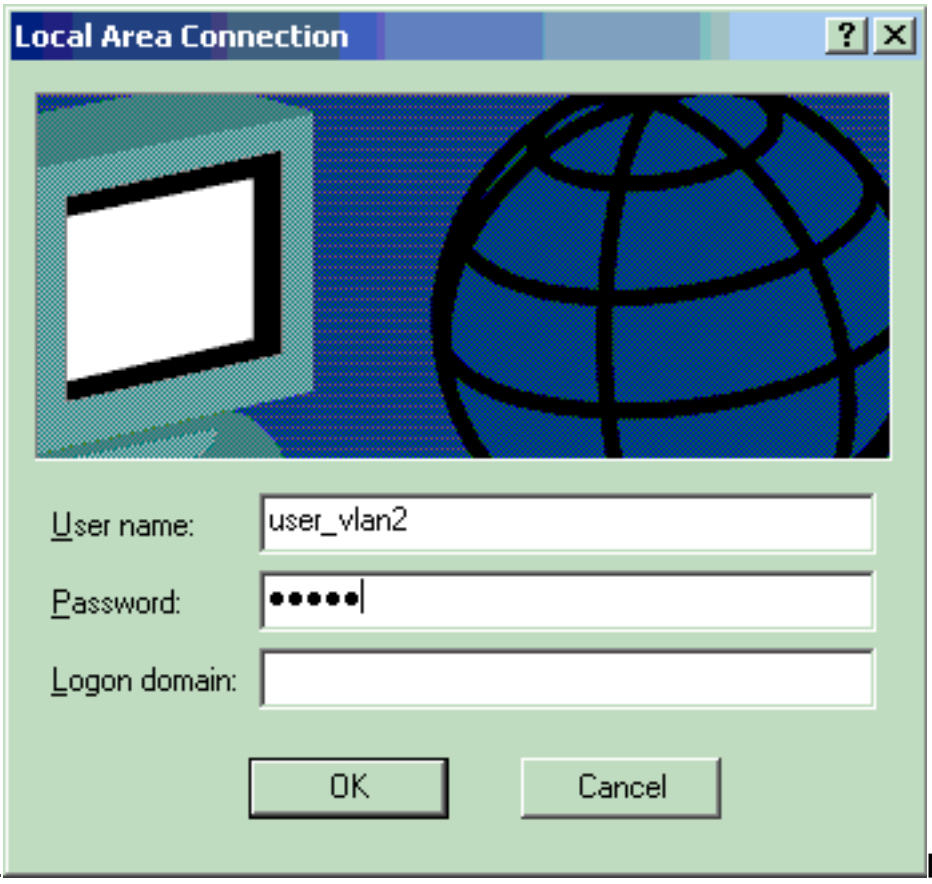
Use esta seção para confirmar se a sua configuração funciona corretamente.

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.

Clientes PC

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

1. Clique sobre a alerta, que este exemplo mostra:Indicadores de uma janela de entrada do nome de usuário e senha.
2. Incorpore o nome de usuário e



senha.**Nota:** No PC1 e em 2, incorpore credenciais do usuário VLAN2. No PC3 e em 4, incorpore credenciais do usuário VLAN3.
3. Se nenhum Mensagem de Erro aparece, verifique a Conectividade com os métodos comuns, tais como o acesso direto dos recursos de rede e com o **comando ping**. Esta é uma saída do

PC1, que mostra um ping bem-sucedido a PC 4:Se

este erro aparece, verifique que o nome de usuário e senha está correto:

Catalyst 6500

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

1. Procure um status de porta que indique autorizado.
```
Cat6K> (enable) show port dot1x 3/1-5
Port Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- --------- ------------------- -------------
3/1  force-authorized    idle       force-authorized    authorized
!--- This is the port to which RADIUS server is connected.
3/2  authenticated       idle       auto                authorized
3/3  authenticated       idle       auto                authorized
3/4  authenticated       idle       auto                authorized
3/5  authenticated       idle       auto                authorized

Port  Port-Mode     Re-authentication    Shutdown-timeout
----- ------------- ------------------   ----------------
3/1   SingleAuth    disabled             disabled
3/2   SingleAuth    disabled             disabled
3/3   SingleAuth    disabled             disabled
3/4   SingleAuth    disabled             disabled
3/5   SingleAuth    disabled             disabled
```
Verifique o status de vlan após a autenticação bem sucedida.
```
Cat6K> (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ---------------
1    default                          active    6       2/1-2
                                                        3/6-48
2    VLAN2                            active    83      3/2-33
3    VLAN3                            active    84      3/4-5
4    AUTHFAIL_VLAN                    active    85      5
5    GUEST_VLAN                       active    8610
6    RADIUS_SERVER                    active    87      3/11
1002 fddi-default                     active    781003
token-ring-default                    active    811004
fddinet-default                       active    791005
trnet-default                         active    80
!--- Output suppressed.
```
2. Verifique o estado obrigatório DHCP do módulo de roteamento (MSFC) 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       Feb 14 2007 03:00 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Feb 14 2007 03:03 AM    Automatic
172.16.3.2       0100.145e.945f.99       Feb 14 2007 03:05 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Feb 14 2007 03:07 AM    Automatic
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Autenticação do IEEE 802.1X com o Catalyst 6500/6000 que executa o exemplo de configuração do Cisco IOS Software
- Interruptor do catalizador e guia de distribuição ACS
- RFC 2868: Atributos de RADIUS para suporte a protocolo de túnel
- Configurando a autenticação do 802.1x
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems