Exemplo de Configuração da Autenticação Multidomínio IEEE 802.1x em Switches de Configuração Fixa de Camada 3 do Cisco Catalyst

Contents

Introduction

A autenticação multidomínio permite que um telefone IP e um PC se autentiquem na mesma porta do switch enquanto os coloca em VLANs de voz e dados apropriadas. Este documento explica como configurar a MDA (Multi-Domain Authentication) IEEE 802.1x em switches de configuração fixa da camada 3 do Cisco Catalyst.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Como funciona o RADIUS?
- Guia de implantação do Catalyst Switching e ACS
- Guia do usuário do Cisco Secure Access Control Server 4.1
- Uma visão geral do telefone IP Cisco Unified

Componentes Utilizados

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

- Switch Cisco Catalyst 3560 Series que executa o Cisco IOS® Software Release 12.2(37)SE1**Observação:** o suporte à autenticação multidomínio está disponível somente no Cisco IOS Software Release 12.2(35)SE e posterior.
- 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.
- Cisco Unified IP Phone 7970G com firmware SCCP versão 8.2(1)
- Cisco Unified IP Phone 7961G com firmware SCCP versão 8.2(2)
- Servidor de cobertura de mídia (MCS) com Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

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.

Produtos Relacionados

Esta configuração também pode ser utilizada com o seguinte hardware:

- Switch Cisco Catalyst 3560-E Series
- Switch Cisco Catalyst 3750 Series
- Switch Cisco Catalyst 3750-E Series

Observação: o switch Cisco Catalyst 3550 Series não suporta a autenticação multidomínio 802.1x.

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.

O 802.1x é composto de três componentes principais. Cada uma é chamada de Entidade de Acesso à Porta (PAE - Port Access Entity).

- Requerente: dispositivo cliente que solicita acesso à rede, por exemplo, telefones IP e PCs conectados
- Autenticador—Dispositivo de rede que facilita as solicitações de autorização do requerente, por exemplo, Cisco Catalyst 3560
- Servidor de autenticação—Um servidor de usuário de discagem de autenticação remota (RADIUS - Remote Authentication Dial-in User Server), que fornece o serviço de autenticação, por exemplo, o Cisco Secure Access Control Server

Os telefones IP Cisco Unified também contêm um suplicante 802.1X. Este suplicante permite que os administradores de rede controlem a conectividade dos telefones IP às portas do switch LAN. A versão inicial do requerente do telefone IP 802.1X implementa a opção EAP-MD5 para autenticação 802.1X. Em uma configuração de vários domínios, o Telefone IP e o PC conectado devem solicitar acesso à rede independentemente pela especificação de um nome de usuário e senha. O dispositivo Authenticator pode exigir informações do RADIUS chamado de atributos. Os atributos especificam informações adicionais de autorização, como se o acesso a uma VLAN específica é permitido para um requerente. Esses atributos podem ser específicos do fornecedor. A Cisco usa o atributo RADIUS `cisco-av-pair` para informar ao Autenticador (Cisco Catalyst 3560) que um requerente (telefone IP) é permitido na VLAN de voz.

Configurar

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

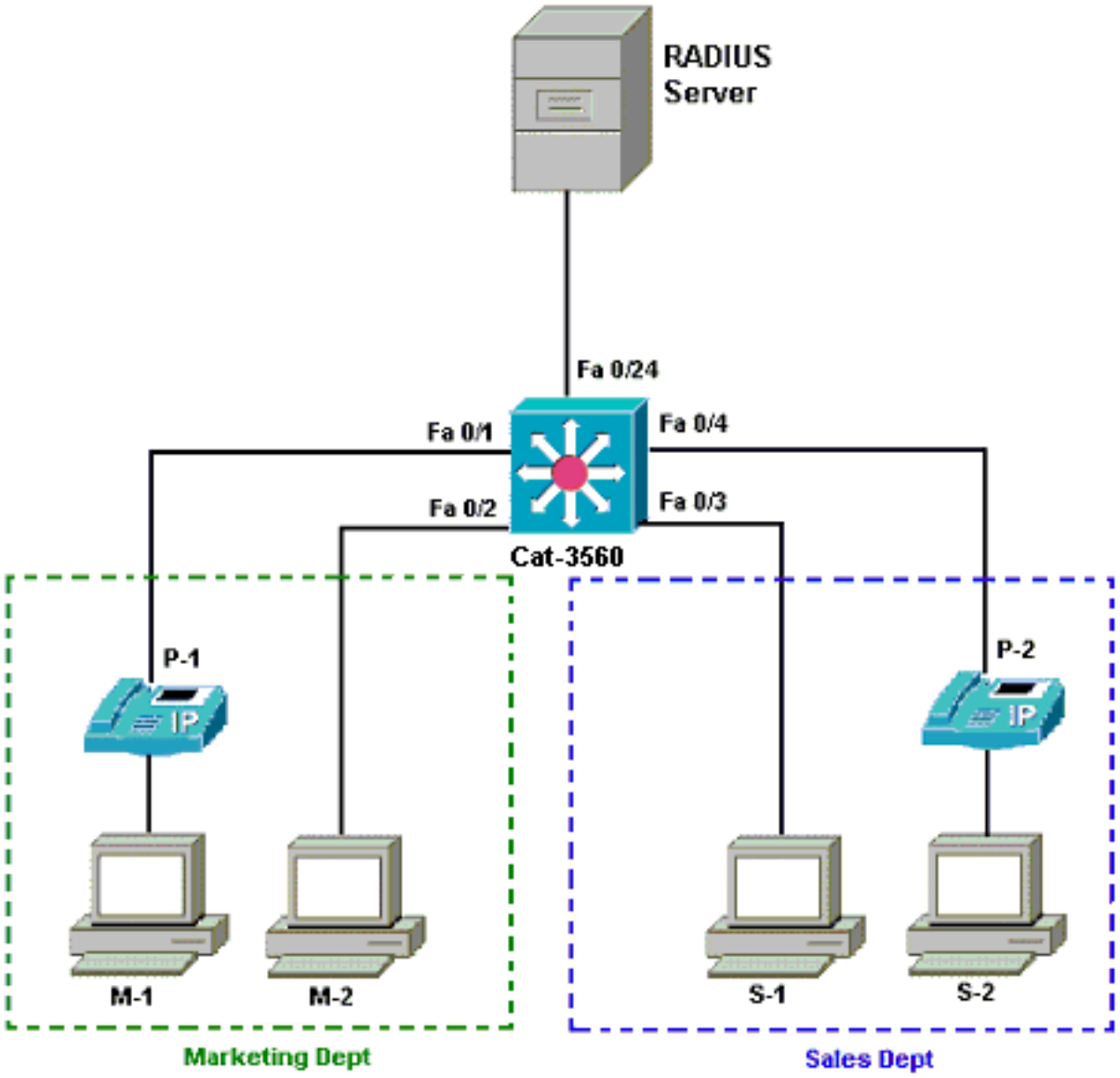
Essa configuração requer estes passos:

- Configure o Switch Catalyst para a autenticação multidomínio 802.1x.
- Configure o servidor RADIUS.
- Configure os clientes PC para usar a autenticação 802.1x.
- Configure os telefones IP para usar a autenticação 802.1x.

Observação: use a Command Lookup Tool (somente clientes registrados) para encontrar mais informações sobre os comandos usados neste documento.

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 Cisco ACS é instalado e configurado em um Servidor de cobertura de mídia (MCS) para autenticação e atribuição de VLAN. O MCS também é o servidor TFTP e o Cisco Unified Communications Manager (Cisco CallManager) para os telefones IP.
- 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 3560 também é configurado como um servidor DHCP. O suporte à autenticação 802.1x para o Dynamic Host Configuration Protocol (DHCP) permite que o servidor DHCP atribua os endereços IP às diferentes classes de usuários finais. Para fazer isso, ele adiciona a identidade do usuário autenticado ao processo de descoberta de DHCP. As portas FastEthernet 0/1 e 0/4 são as únicas portas configuradas para autenticação multidomínio 802.1x. As portas FastEthernet 0/2 e 0/3 estão no modo de host único 802.1x padrão. A porta FastEthernet 0/24 se conecta ao servidor RADIUS.**Observação:** se você usar um servidor DHCP externo, não se esqueça de adicionar o comando **ip helper-address** na interface SVI (vlan), em que o cliente reside, que aponta para o servidor DHCP.
- Clientes—Estes são dispositivos, por exemplo, telefones IP ou estações de trabalho, que

solicitam acesso à LAN e serviços de switch e respondem a solicitações do switch. Aqui, os clientes são configurados para obter o endereço IP de um servidor DHCP. Os dispositivos M-1, M-2, S-1 e S-2 são os clientes da estação de trabalho que solicitam acesso à rede. P-1 e P-2 são os clientes do telefone IP que solicitam acesso à rede. M-1, M-2 e P-1 são dispositivos clientes no departamento de marketing. S-1, S-2 e P-2 são dispositivos clientes no departamento de vendas. Os telefones IP P-1 e P-2 estão configurados para estarem na mesma VLAN de voz (VLAN 3). As estações de trabalho M-1 e M-2 estão configuradas para estarem na mesma VLAN de dados (VLAN 4) após uma autenticação bem-sucedida. As estações de trabalho S-1 e S-2 também são configuradas para estarem na mesma VLAN de dados (VLAN 5) após uma autenticação bem-sucedida.**Observação:** você pode usar a atribuição de VLAN dinâmica de um servidor RADIUS somente para os dispositivos de dados.

Configurar o Switch Catalyst para a autenticação multidomínio 802.1x

Este exemplo de configuração de switch inclui:

- Como ativar a autenticação multidomínio 802.1x nas portas do switch
- configuração relacionada ao servidor RADIUS
- Configuração do servidor DHCP para atribuição de endereço IP
- Roteamento entre VLANs para ter conectividade entre clientes após a autenticação

Consulte Utilização da Autenticação Multidomínio para obter mais informações sobre as diretrizes de configuração do MDA.

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

Observação: somente a configuração relevante é mostrada aqui.

Cat-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Sets the hostname for the switch. Cat-
3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- VLAN should already exist in the switch for a
successful authentication. Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for the RADIUS Server.
Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for IP Phone clients in
VLAN 3. Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
```

```
!--- This is the gateway address for PC clients in VLAN
4. Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
5. Cat-3560(config-if)#exit
Cat-3560(config)#ip routing
!--- Enables IP routing for interVLAN routing. Cat-
3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- This is a dedicated VLAN for the RADIUS server.
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- You must configure the voice VLAN for the IP phone
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
device fails authorization.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Enables IEEE 802.1x authentication on the port.
Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Allow both a host and a voice device to be !---
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- The guest VLAN and restricted VLAN features only
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
!--- Enables periodic re-authentication of the client.
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Set the number of seconds between re-authentication
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
!--- Specifies the number of authentication attempts to
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- By default a 802.1x authorized port allows only a
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- This pool assigns ip address for IP Phones. !---
Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
```

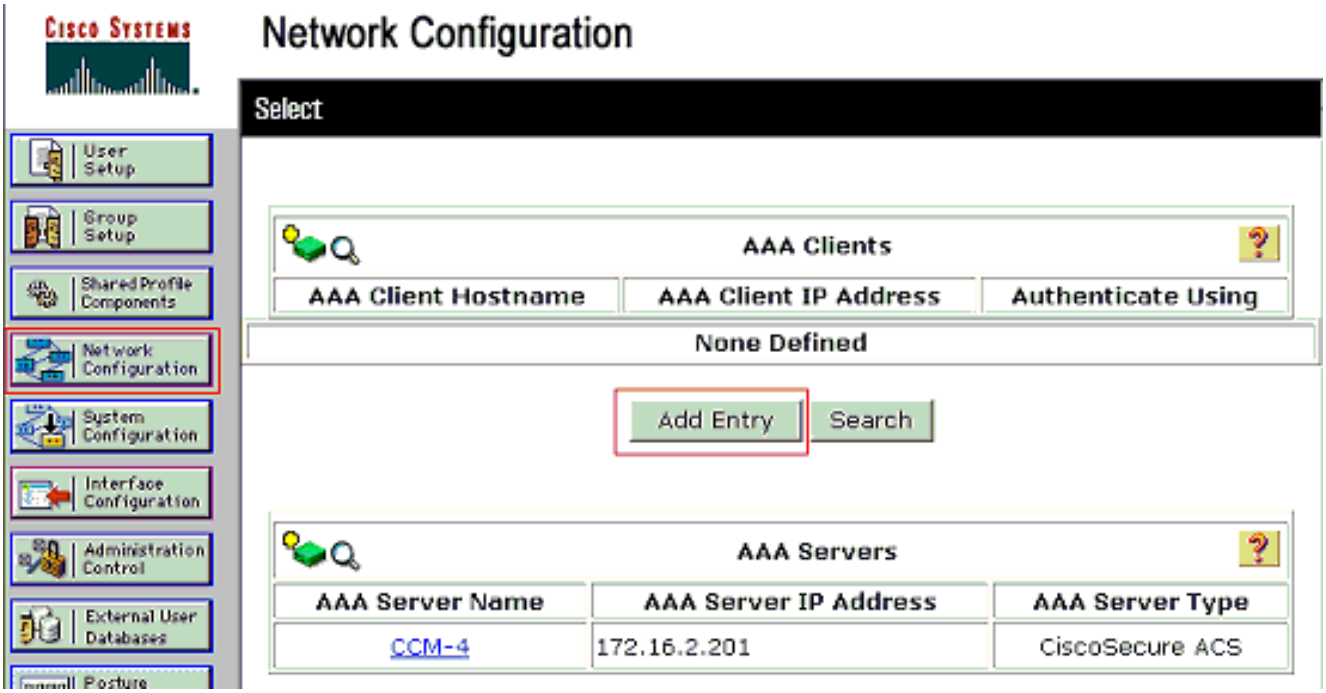
```
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing Dept. Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- This pool assigns ip address for PC clients in
Sales Dept. Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat-3560(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat-3560(config)#radius-server host
172.16.2.201 key CisCo123
!--- The key must match the key used on the RADIUS
server. Cat-3560(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat-3560(config)#interface
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
-----------------------
1    default                           active    Fa0/1,
Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21,
Fa0/22, Fa0/23, Gi0/1
                                                 Gi0/2
2    SERVER                            active    Fa0/24
3    VOICE                             active    Fa0/1,
Fa0/4
4    MARKETING                         active
5    SALES                             active
6    GUEST_and_AUTHFAIL                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

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

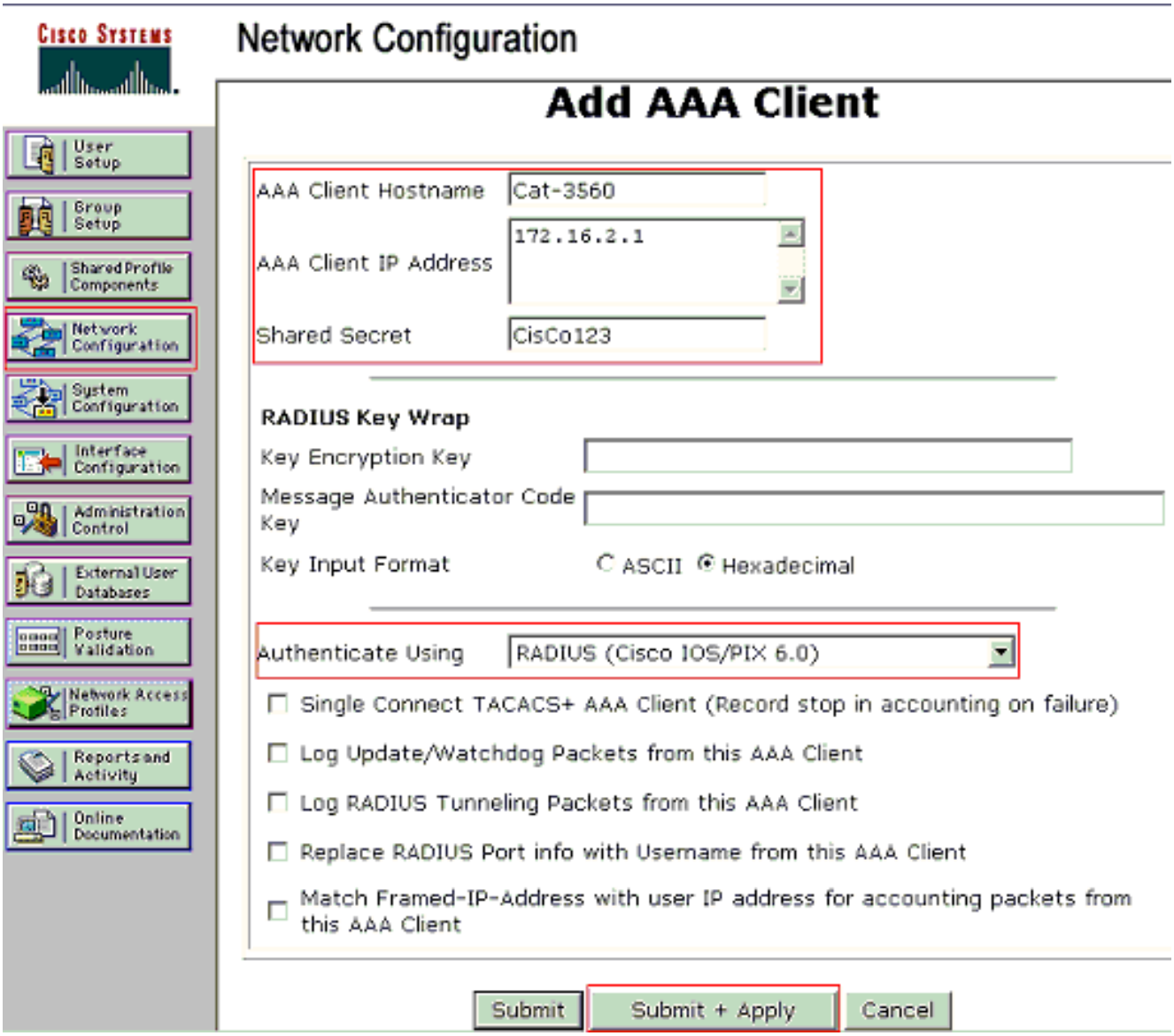
Configurar o servidor RADIUS

O servidor RADIUS é configurado com um endereço IP estático de 172.16.2.201/24. 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 (**Cat-3560**).Endereço IP do cliente AAA = Endereço IP da interface de gerenciamento do switch (**172.16.2.1**).Segredo compartilhado = chave RADIUS configurada no switch (**CisCo123**).**Observação:** para uma operação correta, a chave secreta compartilhada deve ser idêntica no cliente AAA e no ACS. As chaves diferenciam maiúsculas e minúsculas.Autentique usando = **RADIUS (Cisco IOS/PIX 6.0)**.**Observação:** o atributo de par Atributo-Valor (AV) da Cisco está disponível nesta opção.
4. Clique em **Enviar + Aplicar** para tornar essas alterações efetivas, como mostrado neste exemplo:



Configuração do grupo

Consulte esta tabela para configurar o servidor RADIUS para autenticação.

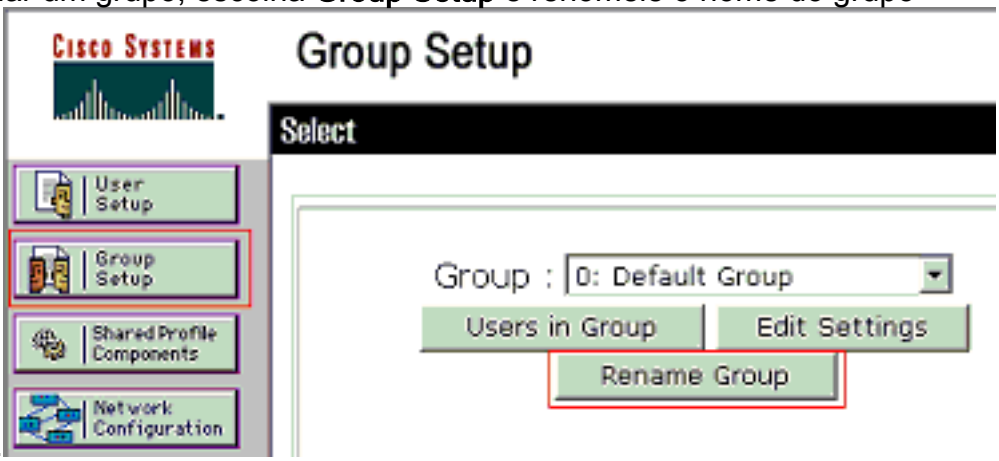
Dispositivo	Departamento	Grupo	Usuário	Senha	VLAN	Pool DHCP
M-1	Marketing	Marketing	mkt-manager	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	mkt-staff	MScisco	MARKETING	Marketing
S-2	Vendas	Vendas	gerente de vendas	SMcisco	VENDAS	Vendas
S-1	Vendas	Vendas	equipe de	Cisco	VENDAS	Vendas

			vendas			
P-1	Marketing	Telefones IP	CP-7970G-SEP001759E7492C	P1cisco	VOZ	Telefones IP
P-2	Vendas	Telefones IP	CP-7961G-SEP001A2F80381F	P2cisco	VOZ	Telefones IP

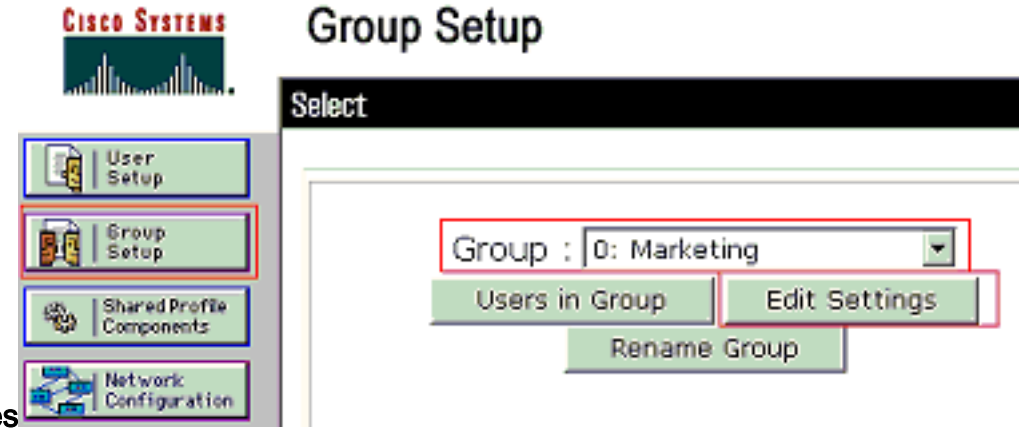
Crie grupos para clientes que se conectam às VLANs 3 (VOICE), 4 (MARKETING) e 5 (VENDAS). Aqui, grupos de **telefones IP**, **marketing** e **vendas** são criados para essa finalidade.

Observação: esta é a configuração dos grupos de **Marketing** e **Telefones IP**. Para a configuração do grupo **Sales**, faça as etapas para o grupo **Marketing**.

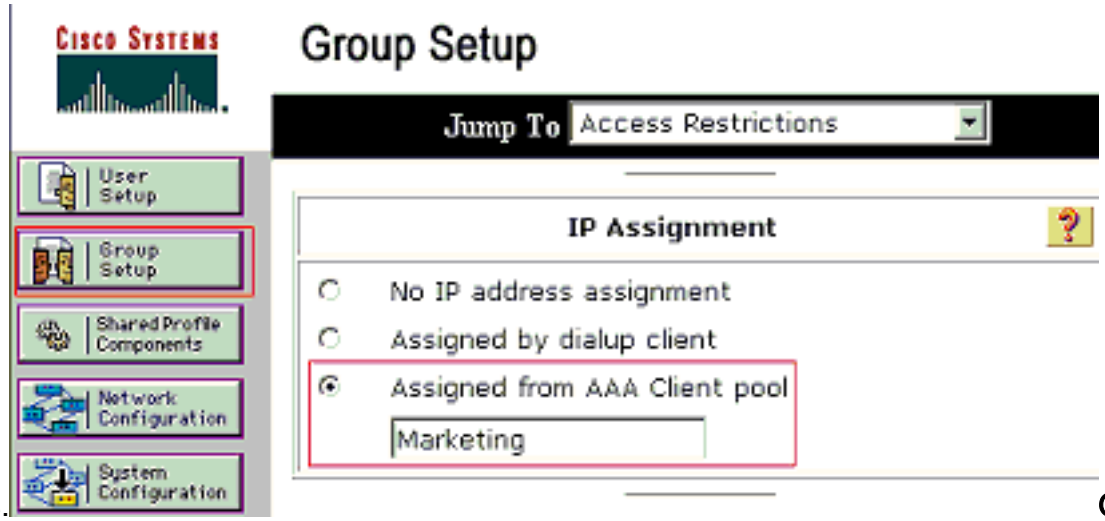
1. Para criar um grupo, escolha **Group Setup** e renomeie o nome do grupo padrão.



2. Para configurar um grupo, escolha o grupo na lista e clique em **Editar configurações**

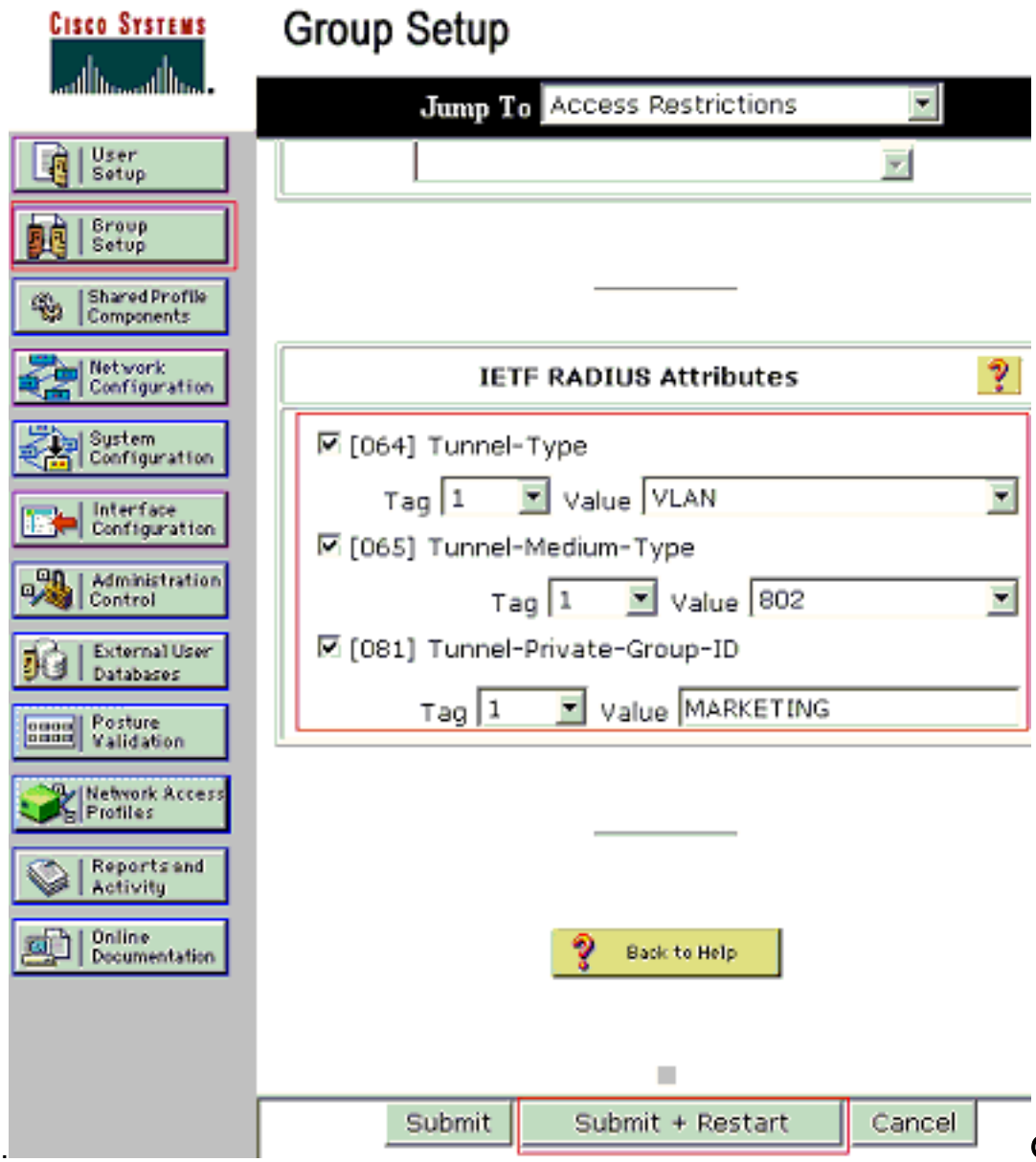


3. Defina a atribuição do endereço IP do cliente como **atribuído pelo pool de clientes AAA**. Insira o nome do pool de endereços IP configurado no switch para esse grupo de



clientes. **Observação:** escolha essa 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.**Observação:** para a configuração do grupo **Telefones IP**, ignore a próxima etapa, etapa 4, e vá para a etapa 5.

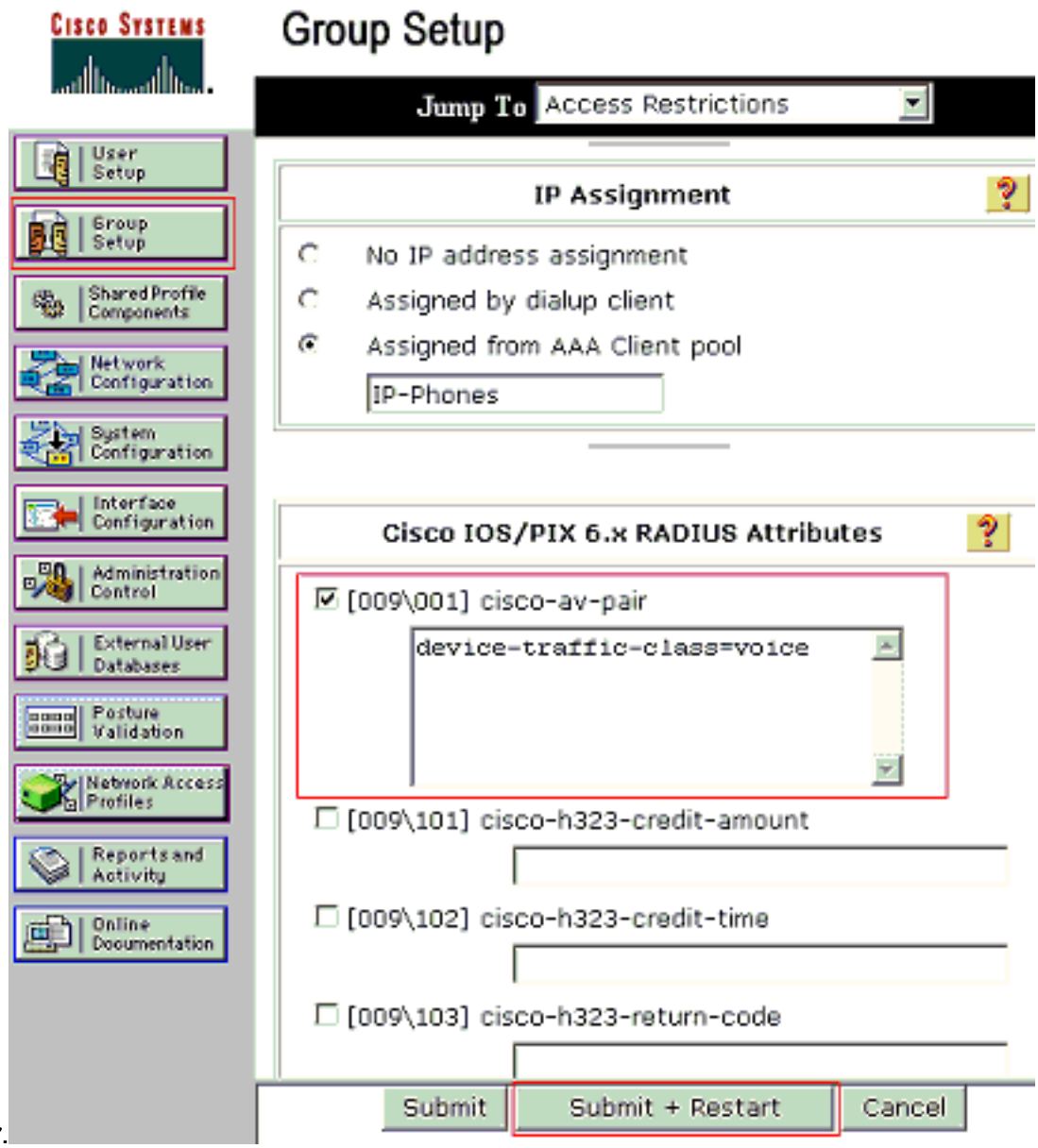
4. Defina os atributos da IETF (Internet Engineering Task Force) **64**, **65** e **81** e clique em **Submit + Restart**.Certifique-se de que as Marcas dos Valores estejam definidas como **1**, como mostrado neste exemplo. O Catalyst ignora qualquer marca diferente de 1. Para atribuir um usuário a uma 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:** consulte o RFC 2868: Atributos RADIUS para suporte ao protocolo de túnel para obter mais informações sobre esses atributos IETF.**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 será atribuído 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.**Observação:** a próxima etapa só se aplica ao grupo **Telefones IP**.

5. Configure o servidor RADIUS para enviar um atributo de par Cisco Attribute-Value (AV) para autorizar um dispositivo de voz. Sem isso, o switch trata o dispositivo de voz como um dispositivo de dados. Defina o atributo de par Atributo-Valor (AV) da Cisco com um valor de *device-traffic-class=voice* e clique em **Enviar +**

Reiniciar.

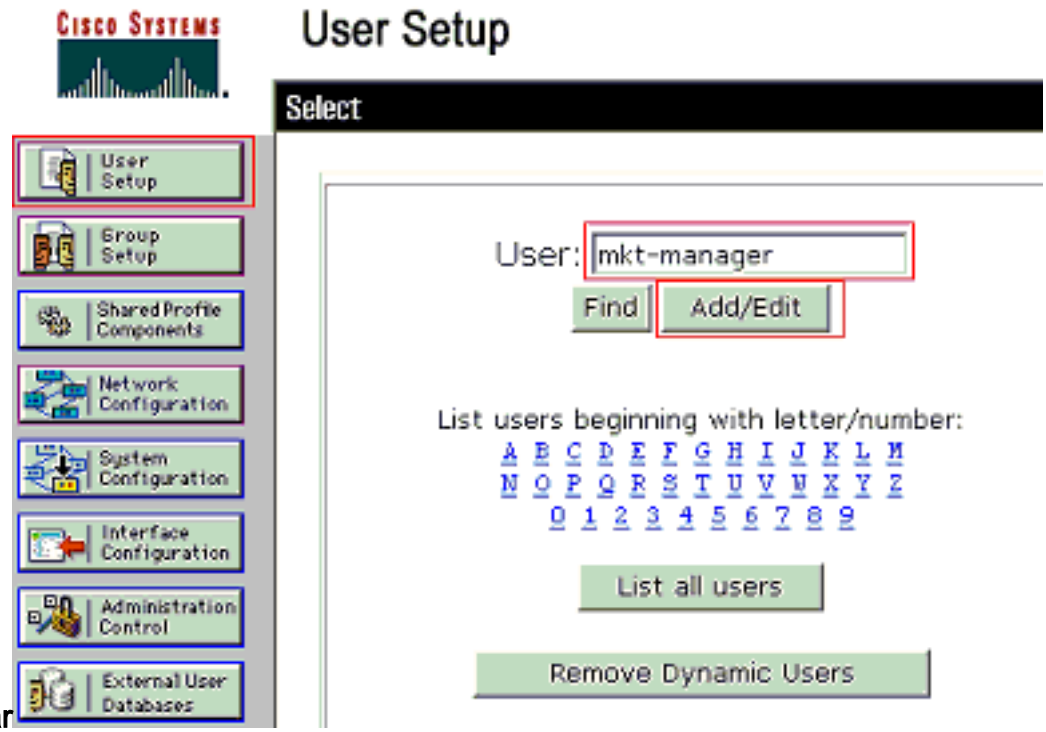


Configuração do usuário

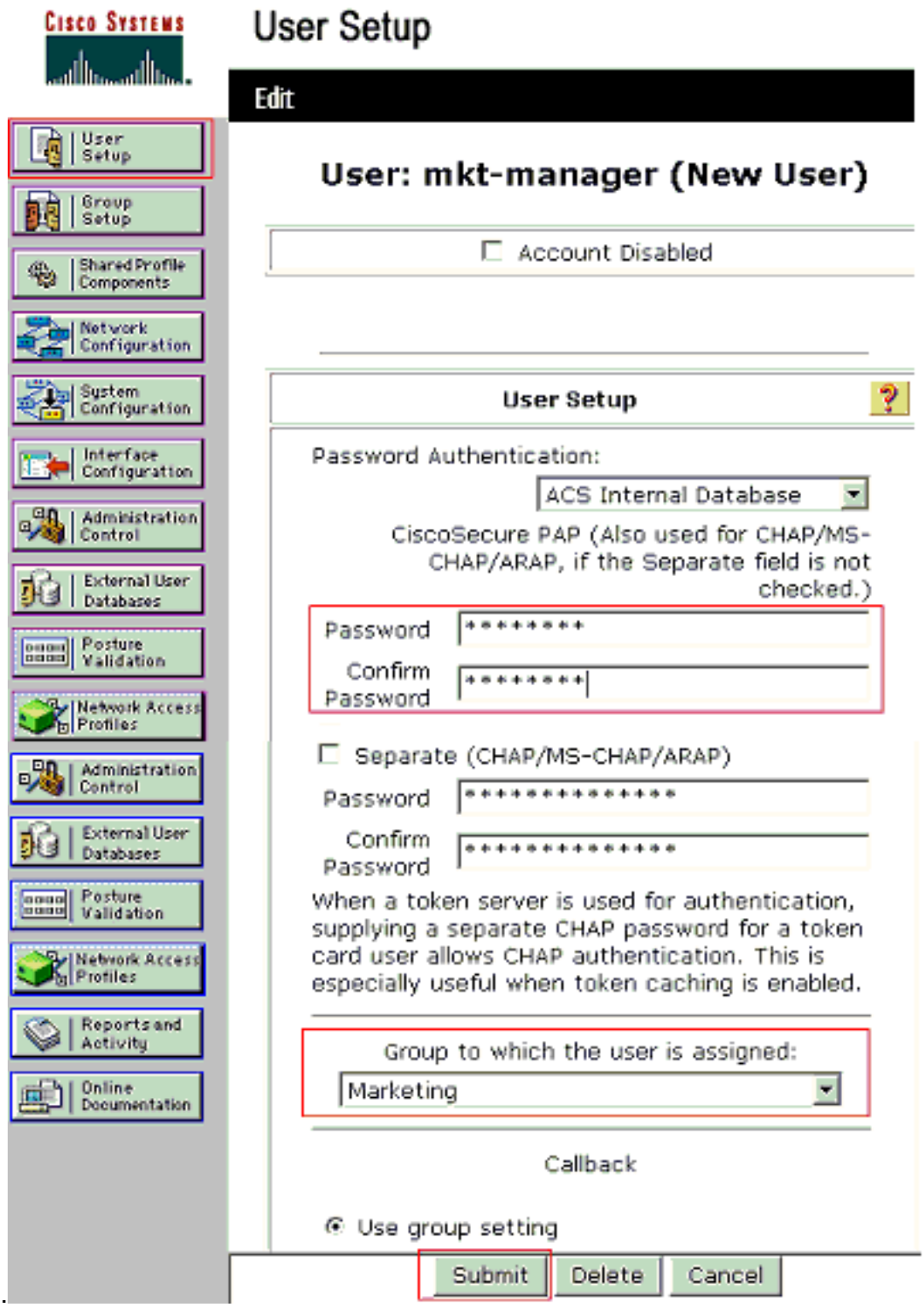
Conclua estes passos para adicionar e configurar um usuário.

1. Para adicionar e configurar usuários, escolha **User Setup**. Digite o nome de usuário e clique

em **Adicionar/Editar**

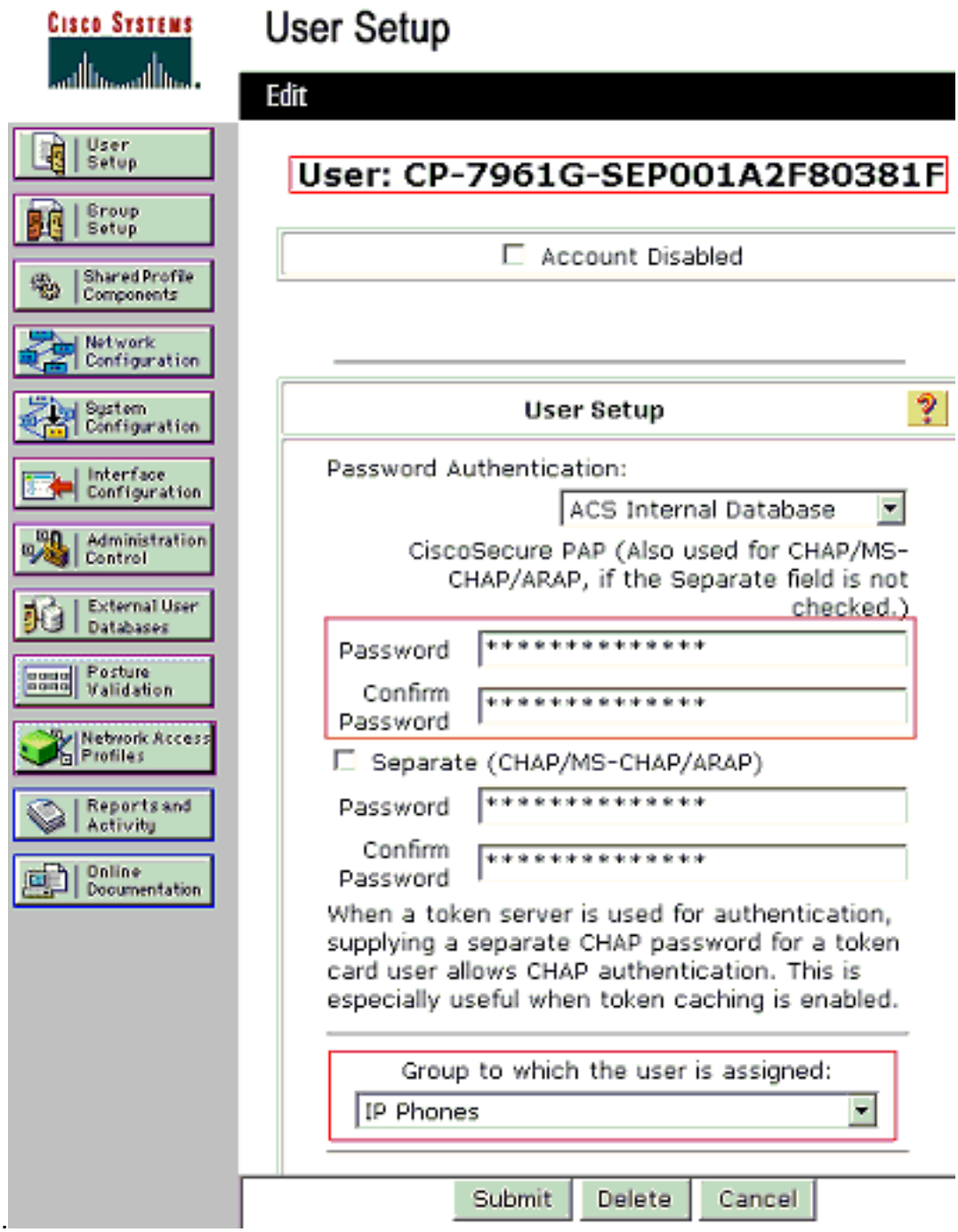


2. Defina o nome de usuário, a senha e o grupo do



usuário.

3. O telefone IP usa sua ID de dispositivo como nome de usuário e segredo compartilhado como senha para autenticação. Esses valores devem corresponder no servidor RADIUS. Para os telefones IP P-1 e P-2, crie nomes de usuário iguais à ID do dispositivo e à senha iguais ao segredo compartilhado configurado. Consulte a seção Configure the IP Phones to Use 802.1x Authentication para obter mais informações sobre o ID do dispositivo e o segredo compartilhado em um telefone



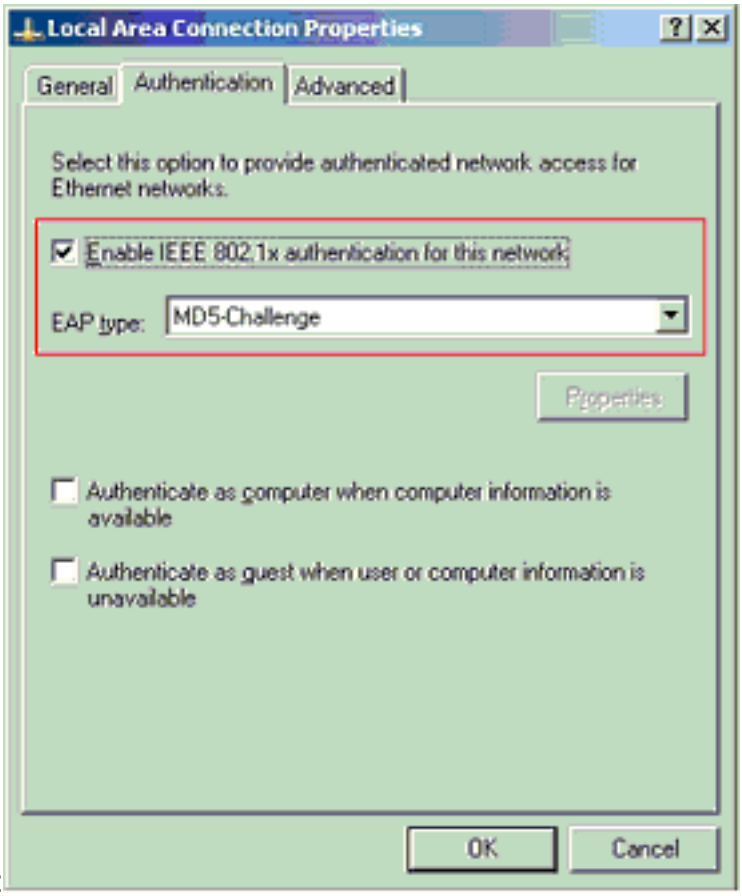
IP.

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):

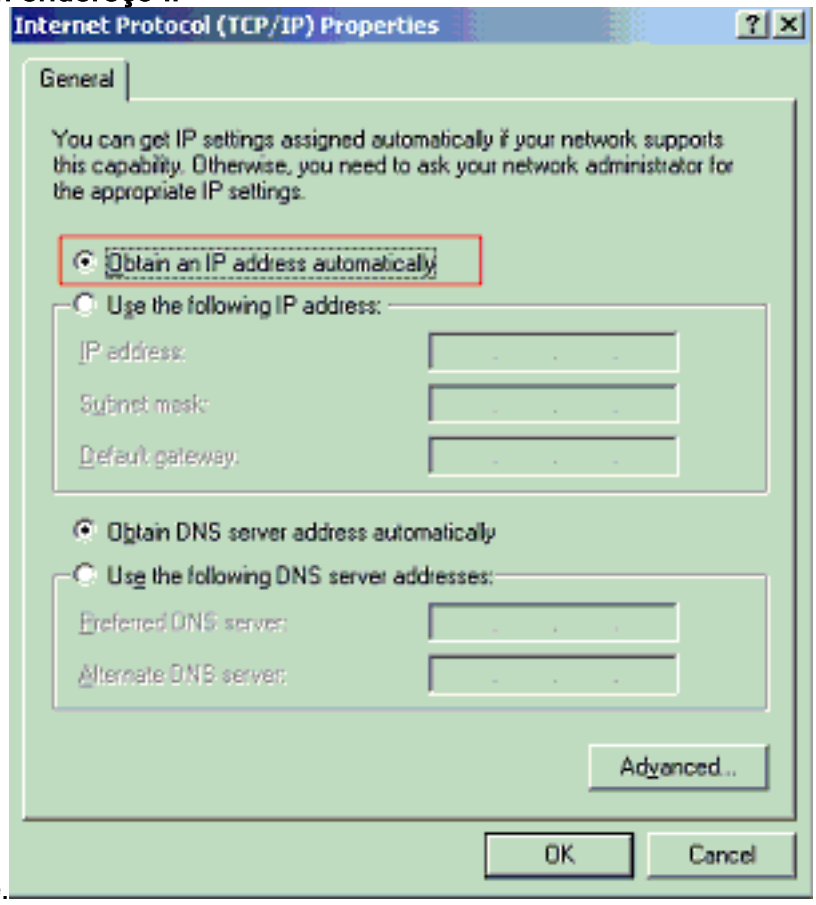
1. Escolha **Iniciar > Painel de controle > Conexões de rede**, clique com o botão direito do mouse em sua **Conexão local** e escolha **Propriedades**.
2. Marque **Mostrar ícone na área de notificação quando conectado** na guia Geral.
3. Na guia Authentication (Autenticação), marque Enable IEEE 802.1x 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**.



Configurar os telefones IP para usar a autenticação 802.1x

Conclua estes passos para configurar os telefones IP para autenticação 802.1x.

1. Pressione o botão **Settings** para acessar as configurações **de autenticação 802.1X** e escolha **Security Configuration > 802.1X Authentication > Device Authentication**.
2. Defina a opção **Device Authentication (Autenticação de dispositivo)** como **Enabled (Habilitado)**.
3. Pressione a tecla de software **Save.**
4. Escolha **Autenticação 802.1X > EAP-MD5 > Segredo compartilhado** para definir uma senha no telefone.
5. Digite o segredo compartilhado e pressione **Salvar**.**Observação:** a senha deve ter entre seis e 32 caracteres, que consistem em qualquer combinação de números ou letras. `Essa chave não está ativa aqui` é exibida uma mensagem e a senha não é salva se essa condição não for atendida.**Observação:** se você desativar a autenticação 802.1X ou executar uma redefinição de fábrica no telefone, o segredo compartilhado MD5 configurado anteriormente será excluído.**Observação:** as outras opções, ID do dispositivo e território não podem ser configuradas. A ID do dispositivo é usada como nome de usuário para autenticação 802.1x. Este é um derivado do número do modelo do telefone e do endereço MAC exclusivo exibidos neste formato: CP-<modelo>-SEP-<MAC>. Por exemplo, **CP-7970G-SEP001759E7492C**. Consulte Configurações de Autenticação do 802.1X para obter mais informações.

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

1. Pressione o botão **Settings** para acessar as configurações **de configuração de rede** e escolha **Network Configuration**.
2. Desbloquear opções **de configuração de rede** Para desbloquear, pressione ****#**.**Nota:** Não pressione ****#** para desbloquear as opções e pressione imediatamente ****#** novamente para bloquear as opções. O telefone interpreta esta sequência como ****#****, que redefine o telefone. Para bloquear as opções depois de desbloqueá-las, aguarde pelo menos 10 segundos antes de pressionar ****#** novamente.
3. Role até a opção DHCP ativado e pressione a tecla de função **Sim** para habilitar o DHCP.
4. Pressione a tecla de software **Save.**

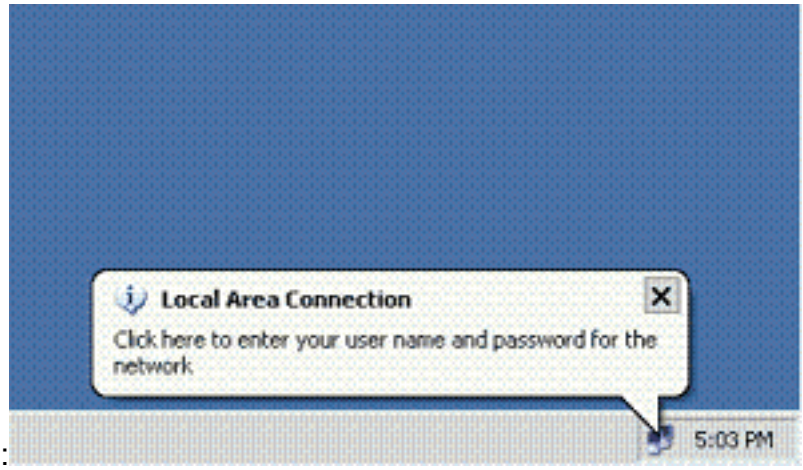
Verificar

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

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.**Observação:** o MDA não impõe a ordem de autenticação do dispositivo. Mas, para obter os melhores resultados, a Cisco recomenda que um dispositivo de voz seja autenticado antes de um dispositivo de dados em uma porta habilitada para MDA.

2. Digite o nome de usuário e a senha.
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**.**Observação:** se esse erro for exibido, verifique se o nome de usuário e a senha estão corretos: 

Telefones IP

O menu Status da autenticação 802.1X nos telefones IP permite monitorar o status da autenticação.

1. Pressione o botão **Settings** para acessar as Estatísticas em Tempo Real de Autenticação 802.1X e escolha **Security Configuration > 802.1X Authentication Status**.

2. O **Status da transação** deve ser **Autenticado**. Consulte Status em Tempo Real de Autenticação 802.1X para obter mais informações.**Observação:** o status da autenticação também pode ser verificado em **Configurações > Status > Mensagens de status**.

Switch de Camada 3

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.

```
Cat-3560#show dot1x all summary
Interface       PAE     Client          Status
---------------------------------------------------------
Fa0/1           AUTH    0016.3633.339c  AUTHORIZED
                        0017.59e7.492c  AUTHORIZED
Fa0/2           AUTH    0014.5e94.5f99  AUTHORIZED
Fa0/3           AUTH    0011.858D.9AF9  AUTHORIZED
Fa0/4           AUTH    0016.6F3C.A342  AUTHORIZED
                        001a.2f80.381f  AUTHORIZED


Cat-3560#show dot1x interface fastEthernet 0/1 details

Dot1x Info for FastEthernet0/1
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = AUTO
ControlDirection        = Both
HostMode                = MULTI_DOMAIN
ReAuthentication        = Enabled
QuietPeriod             = 10
ServerTimeout           = 30
SuppTimeout             = 30
ReAuthPeriod            = 60 (Locally configured)
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
RateLimitPeriod         = 0
Auth-Fail-Vlan          = 6
Auth-Fail-Max-attempts  = 2
Guest-Vlan              = 6

Dot1x Authenticator Client List
-------------------------------
Domain                  = DATA
Supplicant              = 0016.3633.339c
    Auth SM State       = AUTHENTICATED
    Auth BEND SM State  = IDLE
Port Status             = AUTHORIZED
ReAuthPeriod            = 60
ReAuthAction            = Reauthenticate
TimeToNextReauth        = 29
Authentication Method   = Dot1x
Authorized By           = Authentication Server
Vlan Policy             = 4

Domain                  = VOICE
Supplicant              = 0017.59e7.492c
    Auth SM State       = AUTHENTICATED
    Auth BEND SM State  = IDLE
Port Status             = AUTHORIZED
```

```
ReAuthPeriod              = 60
ReAuthAction              = Reauthenticate
TimeToNextReauth          = 15
Authentication Method     = Dot1x
Authorized By             = Authentication Server
```

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

```
Cat-3560#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
2    SERVER                           active    Fa0/24
3    VOICE                            active    Fa0/1, Fa0/4
4    MARKETING                        active    Fa0/1, Fa0/2
5    SALES                            active    Fa0/3, Fa0/4
6    GUEST_and_AUTHFAIL               active
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 após uma autenticação bem-sucedida.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.3.2       0100.1759.e749.2c       Aug 24 2007 06:35 AM    Automatic
172.16.3.3       0100.1a2f.8038.1f       Aug 24 2007 06:43 AM    Automatic
172.16.4.2       0100.1636.3333.9c       Aug 24 2007 06:50 AM    Automatic
172.16.4.3       0100.145e.945f.99       Aug 24 2007 08:17 AM    Automatic
172.16.5.2       0100.166F.3CA3.42       Aug 24 2007 08:23 AM    Automatic
172.16.5.3       0100.1185.8D9A.F9       Aug 24 2007 08:51 AM    Automatic
```

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

Troubleshoot

Falha na autenticação do telefone IP

O status do telefone IP exibe `Configurando IP` ou `Registrando` se a autenticação 802.1x falhar. Conclua estes passos para solucionar esses problemas:

- Confirme se o 802.1x está ativado no telefone IP.
- Verifique se a ID do dispositivo foi inserida no servidor de autenticação (RADIUS) como o nome de usuário.
- Confirme se o segredo compartilhado está configurado no telefone IP.
- Se o segredo compartilhado estiver configurado, verifique se você tem o mesmo segredo compartilhado inserido no servidor de autenticação.
- Verifique se você configurou corretamente os outros dispositivos necessários, por exemplo, o switch e o servidor de autenticação.

Informações Relacionadas

- Configurando a autenticação baseada em porta IEEE 802.1x
- Configurar o telefone IP para usar a autenticação 802.1x
- 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
- Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o Cisco IOS Software Configuration Example
- Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o exemplo de configuração de software CatOS
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems