

Autenticação do Multi-domínio do IEEE 802.1X no exemplo de configuração dos switch de configuração fixa da camada 3 do Cisco catalyst

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

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

[Configurar o servidor Radius](#)

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

[Configurar os Telefones IP para usar a autenticação do 802.1x](#)

[Verificar](#)

[Clientes PC](#)

[Telefones IP](#)

[Switch de camada 3](#)

[Troubleshooting](#)

[A autenticação do telefone IP falha](#)

[Informações Relacionadas](#)

Introdução

A autenticação do Multi-domínio permite que um telefone IP e um PC autentiquem na mesma porta de switch quando os colocar na Voz e em VLAN de dados apropriados. Este documento explica como configurar a autenticação do Multi-domínio do IEEE 802.1X (MDA) em switch de configuração fixa da camada 3 do Cisco catalyst.

Pré-requisitos

Requisitos

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

- [Como o RAO trabalha?](#)
- [Interruptor do catalizador e guia de distribuição ACS](#)
- [Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1](#)
- [Uma vista geral de Cisco unificou o telefone IP](#)

[Componentes Utilizados](#)

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

- Cisco Catalyst 3560 Series Switch que executa a liberação 12.2(37)SE1 do Cisco IOS® Software **Nota:** O apoio da autenticação do Multi-domínio está disponível somente do Cisco IOS Software Release 12.2(35)SE e Mais Recente.
- 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.
- Telefone IP Cisco Unified 7970G com versão 8.2(1) do firmware SCCP
- Telefone IP Cisco Unified 7961G com versão 8.2(2) do firmware SCCP
- Server de Convergence dos media (MCS) com o gerente das comunicações unificadas de Cisco (CallManager da Cisco) 4.1(3)sr2

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.

[Produtos Relacionados](#)

Esta configuração também pode ser utilizada com o seguinte hardware:

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

Nota: O Cisco Catalyst 3550 Series Switch não apoia a autenticação do Multi-domínio do 802.1x.

[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 controle de acesso e um protocolo de autenticação baseados servidor cliente que restrinja dispositivos desautorizados da conexão a um LAN através das portas publicamente acessíveis. o 802.1x controla o acesso de rede pela criação de 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 conectada 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.

o 802.1x é compreendido de três componentes principais. Cada um é referido como uma entidade do acesso da porta (PAE).

- Suplicante — Dispositivo do cliente que pede o acesso de rede, por exemplo, os Telefones IP e PC anexados
- Autenticador — Dispositivo de rede que facilita os pedidos de autorização do suplicante, por exemplo, o Cisco catalyst 3560
- Authentication Server — Um Remote Authentication Dial-In User Server (RAIO), que proporciona o serviço de autenticação, por exemplo, Serviço de controle de acesso Cisco Secure

Os Telefones IP unificados Cisco igualmente contêm um suplicante do 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 suplicante do 802.1X do telefone IP executa a opção do EAP-MD5 para a autenticação do 802.1X. Em uma configuração do multi-domínio, o telefone IP e o PC anexado devem independentemente pedir o acesso à rede pela especificação de um nome de usuário e senha. O dispositivo do autenticador pode exigir a informação do RAIO chamado atributos. Os atributos especificam a informação de autorização adicional como se o acesso a um VLAN particular está permitido um suplicante. Estes atributos podem ser específico do vendedor. Cisco usa o `Cisco-av-pair` do atributo RADIUS a fim dizer o autenticador (Cisco catalyst 3560) que um suplicante (telefone IP) é permitido na Voz VLAN.

Configurar

Nesta seção, você é apresentado com a informação para configurar a característica de autenticação do multi-domínio do 802.1x descrita neste documento.

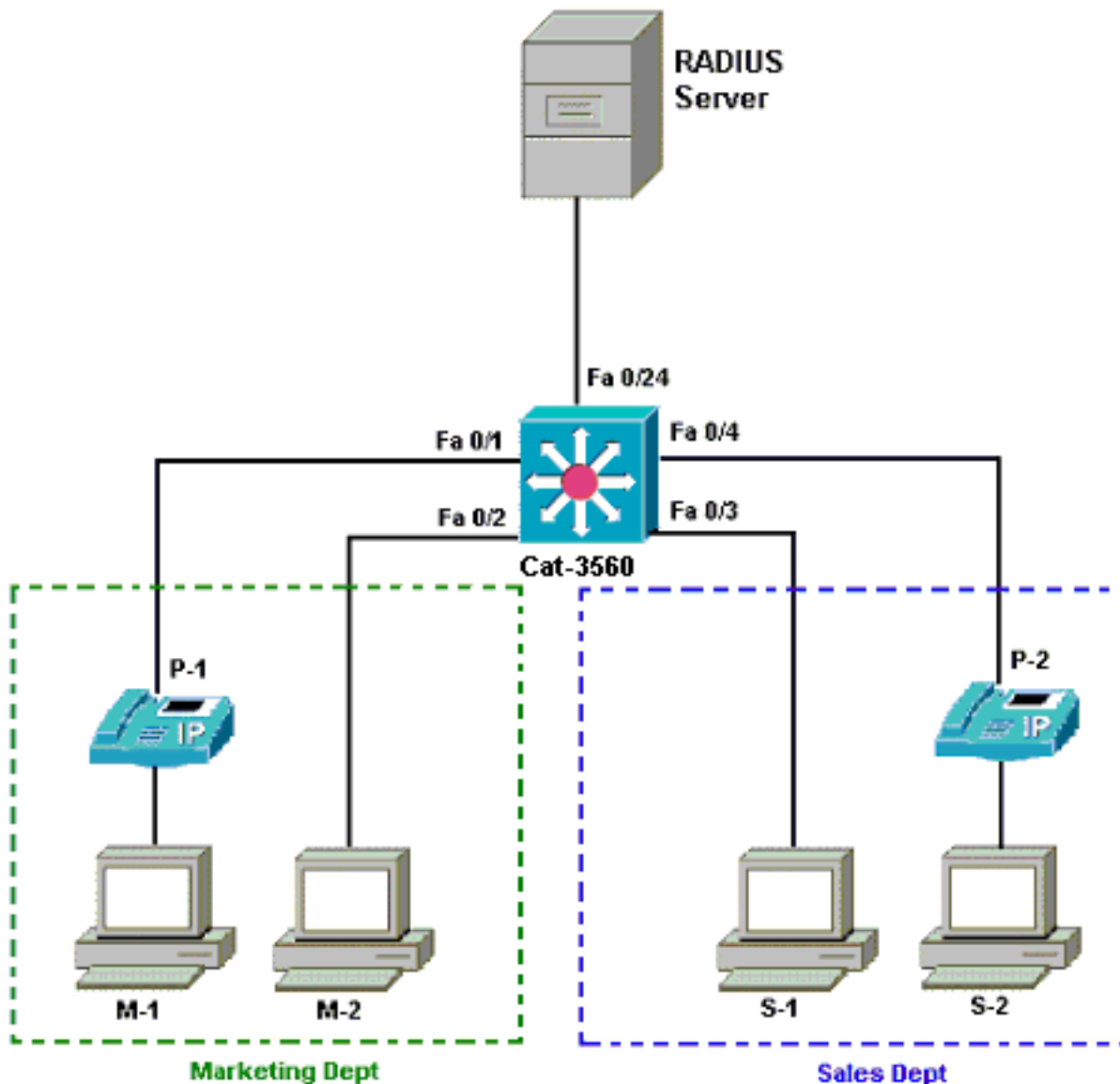
Essa configuração requer estes passos:

- [Configurar o Catalyst Switch para a autenticação do Multi-domínio do 802.1x.](#)
- [Configurar o servidor Radius.](#)
- [Configurar os clientes PC para usar a autenticação do 802.1x.](#)
- [Configurar os Telefones IP para usar a autenticação do 802.1x.](#)

Nota: Use a [ferramenta de consulta de comandos \(clientes registrados somente\)](#) a fim encontrar mais informação nos comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



- Servidor Radius — Isto 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, Cisco ACS é instalado e configurado em um server de Covergence dos media (MCS) para a autenticação e a atribuição de VLAN. O MCS é igualmente o servidor TFTP e o gerente das comunicações unificadas de Cisco (CallManager da Cisco) para os Telefones IP.
- Interruptor — Isto 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 3560 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. A fim fazer isto, adiciona a identidade do usuário autenticado no processo de descoberta DHCP. O FastEthernet0/1 e 0/4 das portas são as únicas portas configuradas para a autenticação do multi-domínio do 802.1x. Os FastEthernet 0/2 e 0/3 das portas reagem do modo do host único do 802.1x do padrão. O FastEthernet0/24 da porta conecta ao servidor Radius.**Nota:** Se você usa um servidor de DHCP externo, não esqueça adicionar o **comando ip helper-address** na relação (vlan) SVI, em que o cliente reside, que aponta ao servidor DHCP.

- Clientes — Estes são dispositivos, por exemplo, Telefones IP ou estações de trabalho, esse acesso do pedido aos serviços LAN e de interruptor e respondem aos pedidos do interruptor. Aqui, os clientes são configurados a fim alcançar o endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP. Os dispositivos M-1, M-2, S-1 e S-2 são os clientes da estação de trabalho que pedem o acesso à rede. P-1 e P-2 são os clientes do telefone IP que pedem o acesso à rede. O M-1, os M-2 e P-1 são dispositivos do cliente no departamento do mercado. O S-1, S-2 e P-2 são dispositivos do cliente no departamento de vendas. Os Telefones IP P-1 e P-2 são configurados para estar na mesma Voz VLAN (VLAN3). As estações de trabalho M-1 e M-2 são configuradas para estar no mesmo VLAN de dados (VLAN 4) após uma autenticação bem sucedida. As estações de trabalho S-1 e S-2 são configuradas igualmente para estar no mesmo VLAN de dados (VLAN 5) após uma autenticação bem sucedida. **Nota:** Você pode usar a atribuição do VLAN dinâmico de um servidor Radius somente para os dispositivos de dados.

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

Esta configuração de switch da amostra inclui:

- Como permitir a autenticação do multi-domínio do 802.1x nas portas de switch
- Configuração relacionada do servidor Radius
- Configuração do servidor de DHCP para a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT
- Roteamento Inter-Vlan para ter a Conectividade entre clientes após a autenticação

Refira a [utilização da autenticação de Multidomain](#) para obter mais informações sobre as diretrizes em como configurar MDA.

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

Nota: 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 CisCol23 !--- 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. 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.

The screenshot shows the Cisco ACS Network Configuration interface. The left sidebar has 'Network Configuration' highlighted. The main area displays 'AAA Clients' with a table that is currently empty (None Defined). Below the table is an 'Add Entry' button highlighted with a red box. The 'AAA Servers' section below shows a table with one entry: CCM-4, 172.16.2.201, CiscoSecure ACS.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

AAA Server Name	AAA Server IP Address	AAA Server Type
CCM-4	172.16.2.201	CiscoSecure ACS

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 (**Cat-3560**). 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 (**172.16.2.1**). Segredo compartilhado = chave do

RAIO configurada no interruptor (**cisco123**).**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. Autentique usando-se = **RAIO (Cisco IOS/PIX 6.0)**.**Nota:** O atributo dos pares do valor de atributo de Cisco (AV) está disponível sob esta opção.

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

CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit **Submit + Apply** Cancel

Instalação de grupo

Refira esta tabela a fim configurar o servidor Radius para a autenticação.

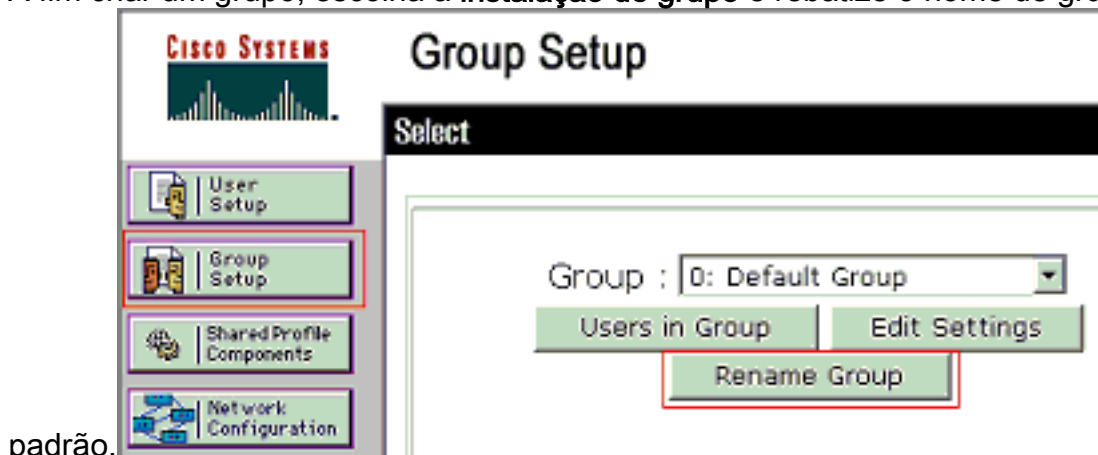
Dispositivo	Departamento	Grupo	Usuário	Senha	VLAN	Conjunto de DHCP
M-1	Mercado	Mercado	mkt-gerente	MMcisco	MERCADO	Mercado
M-2	Mercado	Mercado	mkt-pessoa	MScisco	MERCADO	Mercado

S-2	Vendas	Vendas	vendagerente	SMcisco	VENDAS	Vendas
S-1	Vendas	Vendas	equipe de vendas	SScisco	VENDAS	Vendas
P-1	Mercado	Telefones IP	CP-7970G-SEP001759E7492C	P1cisco	VOZ	Telefones IP
P-2	Vendas	Telefones IP	CP-7961G-SEP001A2F80381F	P2cisco	VOZ	Telefones IP

Crie grupos para os clientes que conectam a VLAN 3 (VOZ), 4 (MERCADO) e 5 (VENDAS). Aqui, os **Telefones IP dos grupos**, o **mercado** e as **vendas** são criados por esse motivo.

Nota: Esta é a configuração dos grupos do **mercado** e dos **Telefones IP**. Para **vendas** configuração de grupo, termine as etapas para o **grupo de marketing**.

1. A fim criar um grupo, escolha a **instalação de grupo** e rebatize o nome de grupo

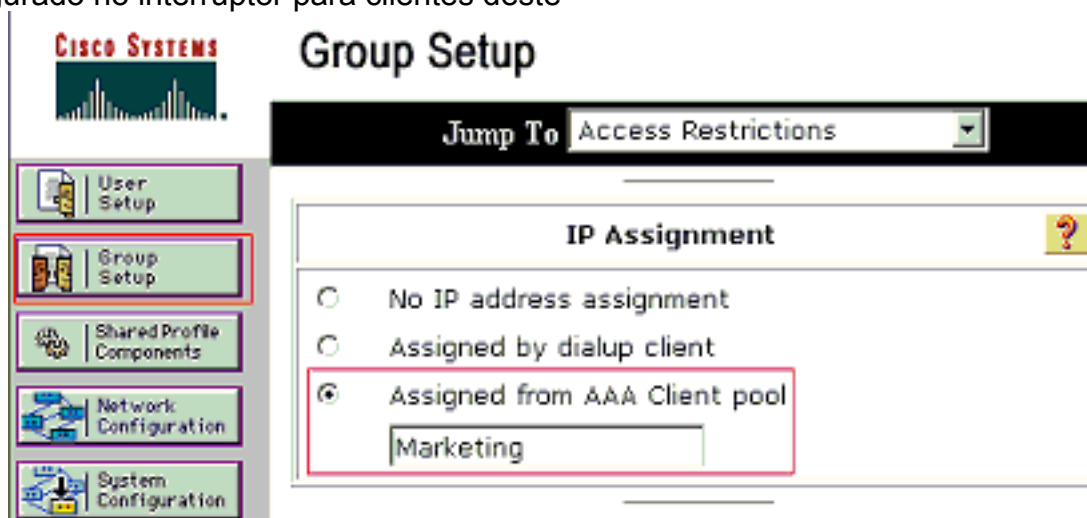


2. A fim configurar um grupo, para escolher o grupo da lista e do clique **edite**



ajustes

- 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 clientes deste



grupo.

Nota: Esc

olha 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. **Nota:** Para a configuração de grupo dos **Telefones IP** apenas, salte a próxima etapa, etapa 4, e vá pisar 5.

- Defina os atributos **64**, **65** e **81** do Internet Engineering Task Force (IETF) e clique-os então **Submit + Restart**. 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 configurado no

interruptor.

Nota:

Refira o [RFC 2868: Atributos RADIUS para o apoio do protocolo de túnel](#) para obter mais informações sobre estes atributos IETF. **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 RAO (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 está atribuído 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 **comando radius do grupo padrão da rede de autorização AAA** 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. **Nota:** A próxima etapa é somente aplicável ao grupo dos **Telefones IP**.

5. Configurar o servidor Radius para enviar um atributo dos pares do valor de atributo de Cisco (AV) para autorizar um dispositivo da Voz. Sem isto, o interruptor trata o dispositivo da Voz como um dispositivo de dados. Defina o atributo dos pares do valor de atributo de Cisco (AV) com um valor do `device-traffic-class=voice` e clique-o **Submit +**

CISCO SYSTEMS

Group Setup

Jump To: Access Restrictions

IP Assignment

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

IP-Phones

Cisco IOS/PIX 6.x RADIUS Attributes

[009\001] cisco-av-pair

device-traffic-class=voice

[009\101] cisco-h323-credit-amount

[009\102] cisco-h323-credit-time

[009\103] cisco-h323-return-code

Submit Submit + Restart Cancel

Restart.

[Instalação de usuário](#)

Termine estas etapas a fim adicionar e configurar um usuário.

1. A fim adicionar e configurar usuários, escolha a **instalação de usuário**. Incorpore o username e o clique



User Setup

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

adicionam/editam

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

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User: mkt-manager (New User)

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

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

Password *****
 Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****
 Confirm 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:

Marketing

Callback

Use group setting

Submit

Delete

Cancel

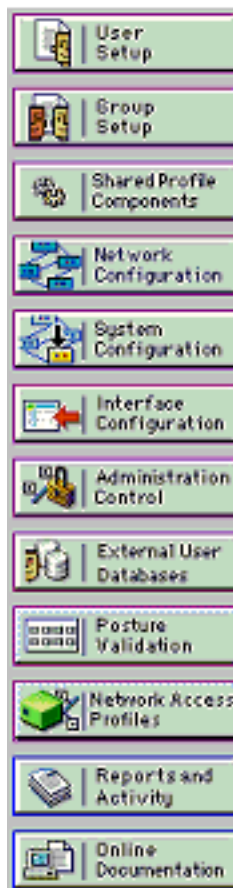
usuário.

3. O telefone IP usa seu identificador de dispositivo como o username e o segredo compartilhado como a senha de autenticação. Estes valores devem combinar no servidor Radius. Para os Telefones IP P-1 e P-2 crie nomes de usuário mesmos que seus identificador de dispositivo e senha mesmos que o segredo compartilhado configurado. Veja [configurar os Telefones IP para usar a seção da autenticação do 802.1x](#) para obter mais informações sobre do identificador de dispositivo e o segredo compartilhado em um telefone



User Setup

Edit



User: CP-7961G-SEP001A2F80381F

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

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

Password *****

Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****

Confirm 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:

IP Phones

Submit

Delete

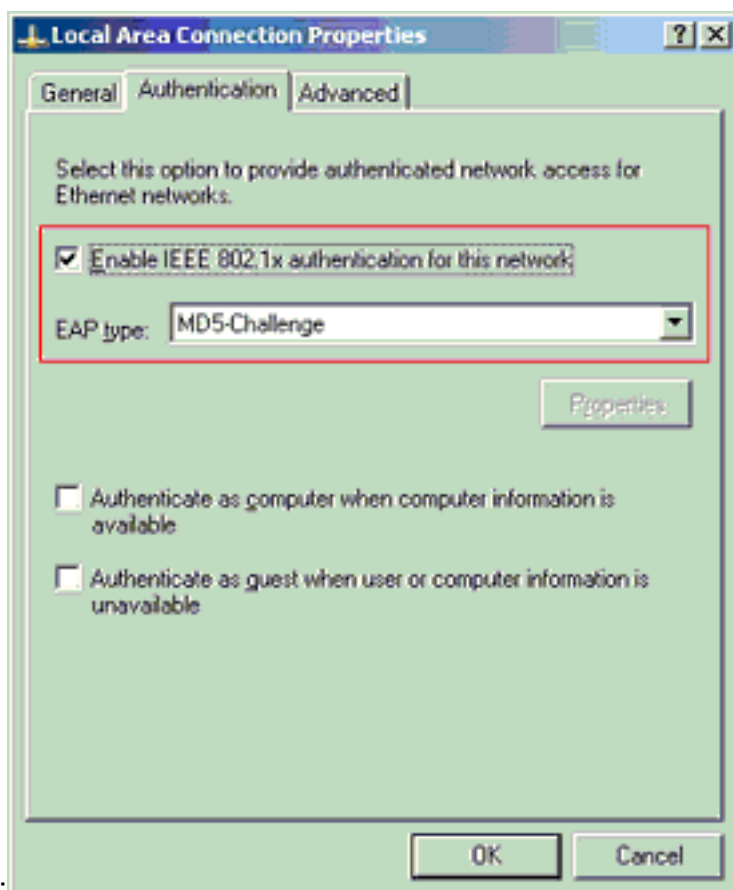
Cancel

IP.

[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):

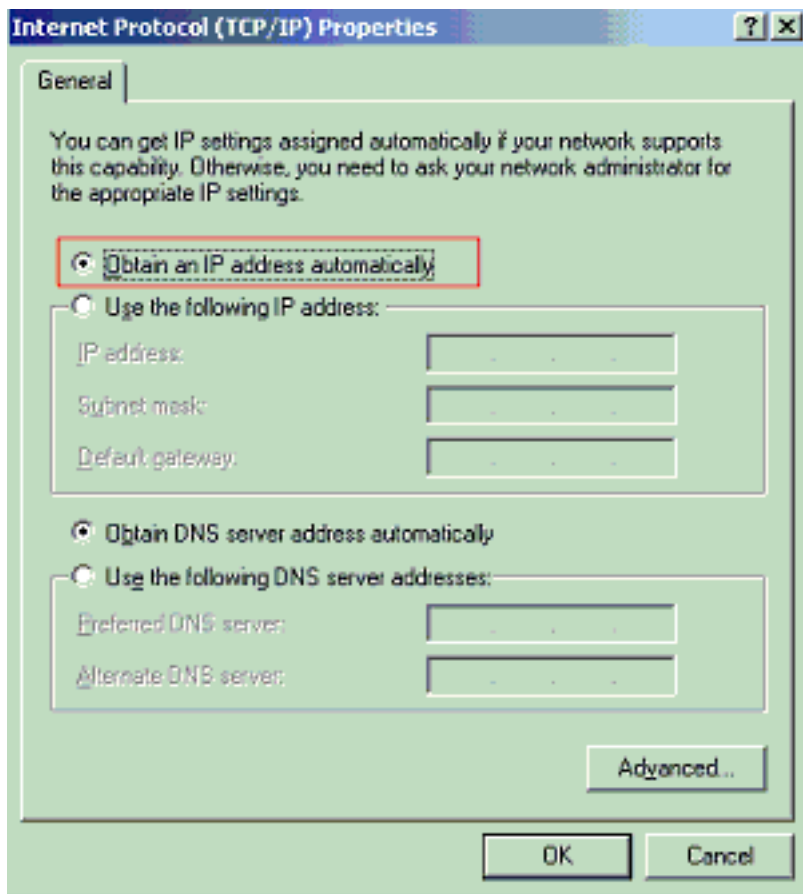
1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**, a seguir clicar com o botão direito em sua **conexão de área local** e escolha **propriedades**.
2. Verifique o **ícone da mostra na área de notificação quando conectado** sob o tab geral.
3. Na guia **Authentication (Autenticação)**,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

[Configurar os Telefones IP para usar a autenticação do 802.1x](#)

Termine estas etapas a fim configurar os Telefones IP para a autenticação do 802.1x.

1. Pressione o **botão Settings Button** a fim alcançar os ajustes da **autenticação do 802.1X** e escolher a **configuração de segurança > a autenticação do 802.1X > a autenticação do dispositivo**.
2. Ajuste a **opção de autenticação do dispositivo ao permitido**.
3. Pressione a tecla de software **Save**.
4. Escolha a **autenticação > o EAP-MD5 do 802.1X > segredo compartilhado** a fim ajustar uma senha no telefone.
5. Incorpore o segredo compartilhado e pressione a **salvaguarda**. **Nota:** A senha deve estar entre seis e 32 caracteres, que consistem em toda a combinação de números ou de letras. Que a chave não é aqui mensagem ativa está mostrado e a senha não salvar se esta circunstância não é satisfeita. **Nota:** Se você desabilita a autenticação do 802.1X ou executa uma fábrica restaurada no telefone, o segredo compartilhado MD5 previamente configurado está suprimido. **Nota:** As outras opções, o identificador de dispositivo e o reino não podem ser configurados. O identificador de dispositivo é usado como o username para a autenticação do 802.1x. Este é um derivado do número de modelo e do MAC address original do telefone indicados neste formato: CP-<model>-SEP-<MAC>. Por exemplo, CP-7970G-SEP001759E7492C. Refira [ajustes da autenticação do 802.1X](#) para mais informação.

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

1. Pressione o **botão Settings Button** a fim alcançar os ajustes da **configuração de rede e**

escolher a **configuração de rede**.

2. Destrave opções de **configuração de rede**. A fim destravar, para pressionar **** #**. **Nota:** Não pressione **** #** a fim destravar opções e as pressionar então imediatamente **** #** outra vez opções de fechamento. O telefone interpreta esta sequência como **** # ****, que restaura o telefone. Opções de fechamento depois que você os destrava, segundos 10 da espera pelo menos antes que você pressionar **** #** outra vez.
3. O rolo à opção permitida DHCP e pressiona a chave macia do **Yes** a fim permitir o DHCP.
4. Pressione a tecla de software **Save**.

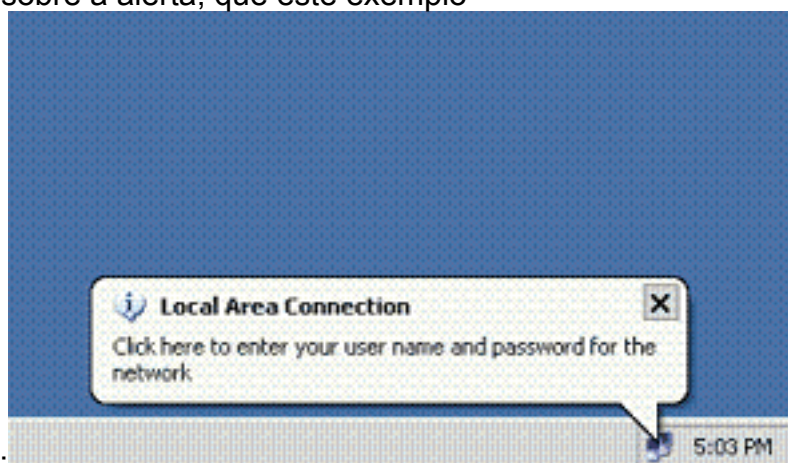
Verificar

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

Clientes PC

Se você 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

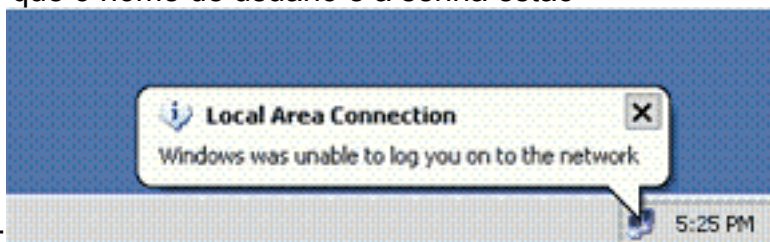


mostra:

Indicadores do indicador de um nome de usuário e da entrada de senha. **Nota:** MDA não reforça a ordem de autenticação do dispositivo. Mas, para os melhores resultados, Cisco recomenda que um dispositivo da Voz está autenticado antes de um dispositivo de dados em uma porta habilitada MDA.



2. Incorpore o nome de usuário e a senha.
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 **sibilo**.**Nota:** Se este erro aparece, verifique que o nome de usuário e a senha estão



corretos:

Telefones IP

o menu do status de autenticação do 802.1X nos Telefones IP reserva monitorar o status de autenticação.

1. Pressione o **botão Settings Button** a fim alcançar o Stats do tempo real da autenticação do 802.1X e escolher o **status de autenticação da configuração de segurança > do 802.1X**.
2. **O estado de transação deve ser autenticado**. Refira o [estado do tempo real da autenticação do 802.1X](#) para mais informação.**Nota:** O status de autenticação pode igualmente ser verificado dos **ajustes > do estado > dos mensagens de status**.

Switch de camada 3

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**.
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 de 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 estado obrigatório 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](#) ([apenas para clientes registrados](#)) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

## Troubleshooting

### A autenticação do telefone IP falha

Exibições de status do telefone IP que configuram o IP ou que registram-se se a autenticação do 802.1x falha. Termine estas etapas a fim pesquisar defeitos isto emite:

- Confirme que o 802.1x está permitido no telefone IP.
- Verifique que você tem o identificador de dispositivo entrado no server da autenticação (RAIO) como o username.
- Confirme que o segredo compartilhado está configurado no telefone IP.
- Se o segredo compartilhado é configurado, verifique que você tem o mesmo segredo compartilhado incorporado no Authentication Server.
- Verifique que você configurou corretamente os outros dispositivos exigidos, por exemplo, o interruptor e o Authentication Server.

## Informações Relacionadas

- [Configurando a autenticação com base na porta do IEEE 802.1X](#)
- [Configurar o telefone IP para usar a autenticação do 802.1x](#)
- [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](#)
- [Autenticação do IEEE 802.1X com o Catalyst 6500/6000 que executa o exemplo de configuração do Cisco IOS Software](#)
- [Autenticação do IEEE 802.1X com o Catalyst 6500/6000 que executa o exemplo de](#)



## configuração do Cactos Software

- [Páginas de Suporte de Produtos de LAN](#)
- [Página de suporte da switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)