Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o exemplo de configuração de software CatOS

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Informações de Apoio Configurar Diagrama de Rede Configurar o Switch Catalyst para autenticação 802.1x Configurar o servidor RADIUS Configurar os PC Clients para Usar a Autenticação 802.1x Verificar **Clientes PC** Catalyst 6500 Troubleshoot Informações Relacionadas

Introduction

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

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

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

Componentes Utilizados

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

- Catalyst 6500 que executa CatOS Software Release 8.5(6) no Supervisor Engine e Cisco IOS Software Release 12.2(18)SXF no MSFCObservação: você precisa do CatOS versão 6.2 ou posterior para suportar a autenticação baseada em porta 802.1x.Observação: antes do software versão 7.2(2), quando o host 802.1x é autenticado, ele ingressa em uma VLAN configurada na NVRAM. Com o software versão 7.2(2) e versões posteriores, após a autenticação, um host 802.1x pode receber sua atribuição de VLAN do servidor RADIUS.
- 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 ativar 802.1x no switch.
- Clientes PC que suportam autenticação 802.1x. Observação: este exemplo usa clientes Microsoft Windows XP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

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 EAP (Extensible Authentication Protocol) sobre LAN (EAPOL) através da porta à qual o dispositivo está conectado. Após a autenticação ser bem-sucedida, o tráfego normal pode passar pela porta.

Configurar

Nesta seção, você recebe as informações para configurar o recurso 802.1x descrito 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:

<u>Configurar o Switch Catalyst para autenticação 802.1x</u>

- <u>Configurar o servidor RADIUS</u>
- <u>Configurar os PC Clients para Usar a Autenticação 802.1x</u>

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



- Servidor RADIUS—Executa a autenticação real do cliente. O servidor RADIUS valida a identidade do cliente e notifica o switch se o cliente está autorizado a acessar os serviços de LAN e switch. Aqui, o servidor RADIUS está configurado para autenticação e atribuição de VLAN.
- Switch—Controla o acesso físico à rede com base no status de autenticação do cliente. O switch atua como um intermediário (proxy) entre o cliente e o servidor RADIUS, solicitando informações de identidade do cliente, verificando essas informações com o servidor RADIUS e transmitindo uma resposta ao cliente. Aqui, o switch Catalyst 6500 também é configurado como um servidor DHCP. O suporte à autenticação 802.1x para o DHCP (Dynamic Host Configuration Protocol) permite que o servidor DHCP atribua os endereços IP às diferentes classes de usuários finais adicionando a identidade de usuário autenticado ao processo de descoberta de DHCP.
- Clientes—Os dispositivos (estações de trabalho) que solicitam acesso à LAN e aos serviços de switch e respondem às solicitações do switch. Aqui, os PCs 1 a 4 são os clientes que solicitam um acesso autenticado à rede. Os PCs 1 e 2 usarão a mesma credencial de logon para estarem na VLAN 2. Da mesma forma, os PCs 3 e 4 usarão uma credencial de login para a VLAN 3. Os clientes PC são configurados para obter o endereço IP de um servidor DHCP. Observação: nesta configuração, qualquer cliente que falha na autenticação ou qualquer cliente com capacidade não 802.1x que se conecta ao switch tem o acesso negado à rede movendo-o para uma VLAN não utilizada (VLAN 4 ou 5) usando a falha de

autenticação e os recursos da VLAN de convidado.

Configurar o Switch Catalyst para autenticação 802.1x

Este exemplo de configuração de switch inclui:

- Ative a autenticação 802.1x e os recursos associados nas portas FastEthernet.
- Conecte o servidor RADIUS à VLAN 10 atrás da porta FastEthernet 3/1.
- Configuração do servidor DHCP para dois pools IP, um para clientes na VLAN 2 e outro para clientes na VLAN 3.
- Roteamento entre VLANs para ter conectividade entre clientes após a autenticação.

Consulte <u>Authentication Configuration Guidelines</u> para obter as diretrizes sobre como configurar a autenticação 802.1x.

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

Catalyst 6500 Console (enable) set system name Cat6K System name set. *!--- Sets the hostname for the switch.* Cat6K> (enable) set localuser user admin password cisco Added local user admin. Cat6K> (enable) set localuser authentication enable LocalUser authentication enabled !--- Uses local user authentication to access the switch. Cat6K> (enable) set vtp domain cisco VTP domain cisco modified !--- Domain name must be configured for VLAN configuration. Cat6K> (enable) set vlan 2 name VLAN2 VTP 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 VLAN3 VTP 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 3 Router(config-if)#ip address 172.16.3.1 255.255.255.0 Router(config-if)#no shut !--- This is the gateway address for clients in VLAN 3. Router(config-if)#exit Router(config) #ip dhcp pool vlan2_clients Router(dhcp-config)#network 172.16.2.0 255.255.255.0 Router(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_clients Router(dhcp-config)#network 172.16.3.0 255.255.255.0 Router(dhcp-config)#default-router 172.16.3.1 !--- This pool assigns ip address for clients in VLAN 3. Router(dhcp-config)#exit Router(config)#ip dhcp excluded-address 172.16.2.1 Router(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#^C Cat6K> (enable) Cat6K> (enable) show vlan VLAN Name Status IfIndex Mod/Ports, Vlans ---- -------- ----- 1 default 2/1-2 active 6 3/2-48 2 VLAN2 active 83 active 84 3 VLAN3 85 4 AUTHFAIL_VLAN active active 5 GUEST_VLAN 86 10 RADIUS_SERVER active 87 3/1 1002 fddi-default active 78 1003 token-ring-default active 81 79 1004 fddinet-default active 1005 trnet-default active 80 !--- Output suppressed. !--- All active ports will be in VLAN 1 (except 3/1) before authentication. Cat6K> (enable) **show dot1x** PAE Capability Authenticator Only Protocol Version 1 system-auth-control enabled max-req 2 60 seconds quiet-period re-authperiod 3600 seconds 30 seconds server-timeout shutdown-timeout 300 seconds supp-timeout 30 seconds 30 seconds tx-period !--- 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. Conclua estes passos para configurar o servidor RADIUS para um cliente AAA:

1. Para configurar um cliente AAA, clique em Network Configuration na janela de administração

do ACS.

2. Clique em **Add Entry** na seção AAA clients.

CISCO SYSTEMS	Network Configuration		
and I travent I they -	Select		
User Setup			
Greup Setup	% Q	AAA Clients	?
Shared Profile Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using
2 Network	None Defined		
System Configuration		Add Entry Search	

- 3. Configure o nome de host do cliente AAA, o endereço IP, a chave secreta compartilhada e o tipo de autenticação como:Nome de host do cliente AAA = Nome de host do switch (Cat6K).Endereço IP do cliente AAA = Endereço IP da interface de gerenciamento (sc0)do switch (172.16.1.2).Segredo compartilhado = Chave Radius configurada no switch (cisco).Autentique Usando = RADIUS IETF.Observação: para uma operação correta, a chave secreta compartilhada deve ser idêntica no cliente AAA e no ACS. As chaves diferenciam maiúsculas e minúsculas.
- 4. Clique em **Enviar + Aplicar** para tornar essas alterações efetivas, como mostrado neste exemplo:

Cisco Systems	Network Configuration
	Add AAA Client
User Setup Setup Shared Profile Components Network Configuration	AAA Client Hostname Cat6K AAA Client IP Address I72.16.1.2 Shared Secret Cisco
Sustem Configuration Interface Configuration Signature Control	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII
Pesture Validation Validation Network Access Profiles Reports and Activity Online Documentation	Authenticate Using RADIUS (IETF) 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

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

Dois nomes de usuário devem ser criados separadamente para clientes que se conectam à VLAN

2 e à VLAN 3. Aqui, um usuário **user_vlan2** para clientes que se conectam à VLAN 2 e outro usuário **user_vlan3** para clientes que se conectam à VLAN 3 são criados para essa finalidade.

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

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

CISCO SYSTEMS	User Setup	
Illin	Select	
User Setup		
Group Setup		User: user_vlan2
Shared Profile Components		Find Add/Edit
Network Configuration		List users beginning with letter/number:
System Configuration		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
Configuration		0123456789
Administration Control		List all users
External User Databases		Remove Dynamic Users
Posture Validation		
Network Access Profiles		Sack to Help

CISCO SYSTEMS	User Setup		
	Edit		
User Setup	User: user_vlan2 (New User)		
Setup	Account Disabled		
Components			
Network Configuration	Supplementary User Info 💡		
System Configuration	Real Name user_vlan2		
Interface Configuration	Description Client in VLAN 2		
Administration Control			
Di External User Databases	User Setup 🦻		
Posture Validation	Password Authentication:		
100 al Mahurak Basaca	ACS Internal Database		
Profiles	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)		
Activity	Password •••••		
Online Documentation	Confirm Password		

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

CISCO SYSTEMS	User Setup
	Password I
User Setup	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.
Shared Profile Components	Group to which the user is assigned:
Network	Default Group
System Configuration	Callback
Interface Configuration	 Use group setting No callback allowed
Administration Control	C Callback using this number
1 External User	O Dialup client specifies callback number
91 Databases	O Use Windows Database callback settings
Posture Validation	
Network Access	Client IP Address Assignment
	○ Use group settings
Activity	O No IP address assignment
0nline Documentation	O Assigned by dialup client
	O Assign static IP address
	Assigned by AAA client pool vlan2_clients

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

3. Defina os atributos 64 e 65 da IETF (Internet Engineering Task Force).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 que corresponda.**Observação:** o *nome* da VLAN deve ser exatamente o mesmo que o configurado no switch.**Observação:** a atribuição de VLAN com base no *número* de VLAN não é suportada com CatOS.



Consulte o <u>RFC 2868: Atributos RADIUS para suporte ao protocolo de túnel</u> 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**. Escolha **Interface configuration > RADIUS (IETF)** para habilitar os atributos IETF na tela de configuração do usuário. Em seguida, verifique os atributos 64, 65 e 81 nas colunas User e Group.

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). Conclua estes passos:

- 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

Local Area Connection Properties
General Authentication Advanced
Select this option to provide authenticated network access for Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type: MD5-Challenge
Properties
Authenticate as <u>c</u> omputer when computer information is available
Authenticate as guest when user or computer information is unavailable
exemplo:

Conclua estes passos para configurar os clientes para obter um 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.

nternet Protocol (TCP/IP) Prop	perties ? 🗙
General	
You can get IP settings assigned this capability. Otherwise, you ne the appropriate IP settings.	automatically if your network supports ed to ask your network administrator for
Obtain an IP address autor	natically
C Use the following IP addres	s:
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address	automaticallu
O Use the following DNS server	ver addresses:
Preferred DNS server:	· · · ·
Alternate DNS server:	· · · ·
	Ad <u>v</u> anced
	OK Cancel

Verificar

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

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

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:

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

2. Digite o nome de usuário e a

- 3.00			
	Local Area Conn	ection ? ×	
	<u>U</u> ser name:	user_vlan2	
	<u>P</u> assword:	•••••	
	Logon domain:		
		OK Cancel	
senha.			Observação: nos

PCs 1 e 2, insira as credenciais de usuário da VLAN 2. Nos PCs 3 e 4, insira as credenciais de usuário da VLAN 3.

3. Se nenhuma mensagem de erro for exibida, verifique a conectividade com os métodos comuns, como por meio do acesso aos recursos de rede e com o comando **ping**. Esta é uma saída do PC 1, que mostra um **ping** bem-sucedido para o PC

C:\WINDOWS\system32\cmd.exe C:\Documents and Settings\Administrator>ipconfig Windows IP Configuration Ethernet adapter Wireless Network Connection: Media State : Media disconnected Ethernet adapter Local Area Connection: Connection-specific DNS Suffix Default Gateway : 172.16.2.1 C:\Documents and Settings\Administrator>ping 172.16.2.1 Pinging 172.16.2.1 with 32 bytes of data: Reply from 172.16.2.1: bytes=32 time<1ms TTL=255 Ping statistics for 172.16.2.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms C:\Documents and Settings\Administrator>ping 172.16.1.1 Pinging 172.16.1.1 with 32 bytes of data: Reply from 172.16.1.1: bytes=32 time<1ms TTL=127 Ping statistics for 172.16.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms C:\Documents and Settings\Administrator>ping 172.16.3.2 Pinging 172.16.3.2 with 32 bytes of data: Reply from 172.16.3.2: bytes=32 time<1ms TTL=127 Ping statistics for 172.16.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms 4 C:\Documents and Settings\Administrator>_

e esse erro for exibido, verifique se o nome de usuário e a senha estão

S



Catalyst 6500

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

```
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
                authorized
 auto
  3/3 authenticated idle
                              auto
                                               authorized
                     idle
  3/4 authenticated
                              auto
                                               authorized
  3/5 authenticated
                      idle
                              auto
                                               authorized
 Port Port-Mode Re-authentication Shutdown-timeout
  disabled
  3/1 SingleAuth disabled
  3/2 SingleAuth disabled
  3/2 SingleAuth disabled
3/4 SingleAuth disabled
3/4 SingleAuth disabled
3/4 SingleAuth disabled
                                 disabled
                                 disabled
disabled
  3/5 SingleAuth disabled
                                   disabled
 Verifique o status da VLAN após a autenticação bem-sucedida.
 Cat6K> (enable) show vlan
 VLAN Name
                                Status IfIndex Mod/Ports, Vlans
 _____ _____
                                active 6
 1
    default
                                              2/1-2
                                              3/6-48
                                active 83
                                              3/2-3
 2
    VLAN2
    VLAN3
 3
                                active 84
                                               3/4-5
 4
   AUTHFAIL_VLAN
                                active 85
 5
   GUEST_VLAN
                                active 86
                                              3/1
 10 RADIUS_SERVER
                                active 87
 1002 fddi-default
                                active 78
 1003 token-ring-default
                                       81
                                active
 1004 fddinet-default
                                active
                                        79
 1005 trnet-default
                                active
                                        80
  !--- Output suppressed.
```

Verifique o status da associação DHCP do módulo de roteamento (MSFC) após a autenticação bem-sucedida.

Router#show ip dhcp binding

IP address	Hardware address	Lease expiration	Туре
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

Troubleshoot

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

Informações Relacionadas

- <u>Autenticação IEEE 802.1x com Catalyst 6500/6000 executando o Cisco IOS Software</u> <u>Configuration Example</u>
- Guia de implantação do Catalyst Switching e ACS
- <u>RFC 2868: Atributos de RADIUS para suporte a protocolo de túnel</u>
- <u>Configurando a autenticação 802.1x</u>
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- <u>Suporte Técnico e Documentação Cisco Systems</u>