Esempio di autenticazione IEEE 802.1x con Catalyst 6500/6000 con software CatOS

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazione dello switch Catalyst per l'autenticazione 802.1x Configurazione del server RADIUS Configurazione dei client PC per l'utilizzo dell'autenticazione 802.1x Verifica **Client PC** Catalyst 6500 Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento spiega come configurare IEEE 802.1x su uno switch Catalyst 6500/6000 in modalità ibrida (CatOS sul Supervisor Engine e software Cisco IOS® sull'MSFC) e su un server RADIUS (Remote Authentication Dial-In User Service) per l'autenticazione e l'assegnazione della VLAN.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- Guida all'installazione di Cisco Secure ACS per Windows 4.1
- Guida per l'utente di Cisco Secure Access Control Server 4.1
- <u>Come funziona RADIUS?</u>
- Guida allo switching Catalyst e alla distribuzione di ACS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 6500 con software CatOS versione 8.5(6) sul Supervisor Engine e software Cisco IOS versione 12.2(18)SXF sull'MSFCNota: per supportare l'autenticazione basata sulla porta 802.1x, è necessario disporre di CatOS versione 6.2 o successive.Nota: prima della versione software 7.2(2), una volta autenticato l'host 802.1x, questo viene aggiunto a una VLAN configurata con NVRAM. Con la versione software 7.2(2) e successive, dopo l'autenticazione, un host 802.1x può ricevere l'assegnazione della VLAN dal server RADIUS.
- In questo esempio viene utilizzato Cisco Secure Access Control Server (ACS) 4.1 come server RADIUS.Nota: prima di abilitare 802.1x sullo switch, è necessario specificare un server RADIUS.
- Client PC che supportano l'autenticazione 802.1x.**Nota:** in questo esempio vengono utilizzati client Microsoft Windows XP.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Premesse

Lo standard IEEE 802.1x definisce un protocollo di autenticazione e controllo degli accessi basato su client-server che impedisce ai dispositivi non autorizzati di connettersi a una rete LAN tramite porte accessibili pubblicamente. 802.1x controlla l'accesso alla rete creando due punti di accesso virtuali distinti a ciascuna porta. Un punto di accesso è una porta non controllata; l'altra è una porta controllata. Tutto il traffico che attraversa la singola porta è disponibile per entrambi i punti di accesso. La licenza 802.1x autentica ciascun dispositivo utente collegato a una porta dello switch e assegna la porta a una VLAN prima di rendere disponibili i servizi offerti dallo switch o dalla LAN. Finché il dispositivo non viene autenticato, il controllo degli accessi 802.1x consente solo il traffico EAP (Extensible Authentication Protocol) over LAN (EAPOL) attraverso la porta a cui è connesso il dispositivo. Dopo l'autenticazione, il traffico normale può passare attraverso la porta.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare la funzionalità 802.1x descritta in questo documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Questa configurazione richiede i seguenti passaggi:

- <u>Configurazione dello switch Catalyst per l'autenticazione 802.1x</u>
- <u>Configurazione del server RADIUS</u>

<u>Configurazione dei client PC per l'utilizzo dell'autenticazione 802.1x</u>

Esempio di rete

Nel documento viene usata questa impostazione di rete:



- Server RADIUS: esegue l'autenticazione effettiva del client. Il server RADIUS convalida l'identità del client e notifica allo switch se il client è autorizzato o meno ad accedere ai servizi LAN e dello switch. In questo caso, il server RADIUS è configurato per l'autenticazione e l'assegnazione della VLAN.
- Switch Controlla l'accesso fisico alla rete in base allo stato di autenticazione del client. Lo switch funge da intermediario (proxy) tra il client e il server RADIUS, richiedendo informazioni di identità dal client, verificandole con il server RADIUS e inoltrando una risposta al client. In questo caso, lo switch Catalyst 6500 è configurato anche come server DHCP. Il supporto dell'autenticazione 802.1x per il protocollo DHCP (Dynamic Host Configuration Protocol) consente al server DHCP di assegnare gli indirizzi IP alle diverse classi di utenti finali aggiungendo l'identità dell'utente autenticato nel processo di rilevamento DHCP.
- Client: dispositivi (workstation) che richiedono l'accesso ai servizi LAN e switch e rispondono alle richieste dello switch. Qui, i PC da 1 a 4 sono i client che richiedono un accesso di rete autenticato. I PC 1 e 2 utilizzeranno le stesse credenziali di accesso della VLAN 2. Analogamente, i PC 3 e 4 useranno le credenziali di accesso della VLAN 3. I client PC sono configurati per ottenere l'indirizzo IP da un server DHCP.Nota: in questa configurazione, a qualsiasi client che non supera l'autenticazione o a qualsiasi client non compatibile con 802.1x che si connette allo switch viene negato l'accesso alla rete spostandolo su una VLAN non utilizzata (VLAN 4 o 5) con le funzionalità di autenticazione errata e VLAN guest.

Configurazione dello switch Catalyst per l'autenticazione 802.1x

La configurazione di esempio dello switch include:

- Abilitare l'autenticazione 802.1x e le funzionalità associate sulle porte Fast Ethernet.
- Collegare il server RADIUS alla VLAN 10 dietro la porta Fast Ethernet 3/1.
- Configurazione del server DHCP per due pool IP, uno per i client della VLAN 2 e l'altro per i client della VLAN 3.
- Dopo l'autenticazione, il routing tra VLAN deve avere la connettività tra i client.

Per le linee guida su come configurare l'autenticazione 802.1x, consultare il documento <u>Guide alla</u> configurazione dell'autenticazione.

Nota: verificare che il server RADIUS si connetta sempre dietro una porta autorizzata.

```
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
- ----- 1 default
active 6 2/1-2
3/2-48
2
   VLAN2
                                   active 83
3
   VLAN3
                                   active 84
4
  AUTHFAIL_VLAN
                                  active 85
5
  GUEST VLAN
                                  active 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
quiet-period
                       60 seconds
re-authperiod
                       3600 seconds
                        30 seconds
server-timeout
shutdown-timeout
                        300 seconds
supp-timeout
                        30 seconds
tx-period
                        30 seconds
!--- Verifies dot1x status before authentication. Cat6K>
(enable)
```

Configurazione del server RADIUS

Il server RADIUS è configurato con un indirizzo IP statico di 172.16.1.1/24. Per configurare il server RADIUS per un client AAA, attenersi alla seguente procedura:

- 1. Per configurare un client AAA, fare clic su **Configurazione di rete** nella finestra di amministrazione di ACS.
- 2. Fare clic su Add Entry (Aggiungi voce) nella sezione AAA Client (Client

AAA).			
CISCO SYSTEMS	Network Configuration		
- attilling attilling -	Select		
User Setup			
Greup Setup	% Q	AAA Clients	?
Shared Profile Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using
Network Configuration		None Defined	
System Configuration		Add Entry Search	

- 3. Configurare il nome host del client AAA, l'indirizzo IP, la chiave segreta condivisa e il tipo di autenticazione come:Nome host client AAA = Nome host switch (Cat6K).Indirizzo IP client AAA = Indirizzo IP dell'interfaccia di gestione (sc0)dello switch (172.16.1.2).Shared Secret = Chiave Radius configurata sullo switch (cisco).Autentica utilizzando = RADIUS IETF.Nota: per un corretto funzionamento, la chiave privata condivisa deve essere identica sul client AAA e su ACS. Le chiavi distinguono tra maiuscole e minuscole.
- 4. Fare clic su **Invia + Applica** per rendere effettive le modifiche, come illustrato nell'esempio seguente:

Cisco Systems	Network Configuration Add AAA Client			
- aillin aillin -				
User Setup Exetup Setup Shared Profile Components	AAA Client Hostname Cat6K AAA Client IP Address I72.16.1.2			
Net work Configuration	Shared Secret cisco			
System Configuration	RADIUS Key Wrap			
Configuration	Key Encryption Key			
Administration Control	Message Authenticator Code Key			
External User Databases	Key Input Format C ASCII Hexadecimal			
Posture Validation	Authenticate Using RADIUS (IETF)			
Network Access	□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)			
Reports and	Log Update/Watchdog Packets from this AAA Client			
Activity	Log RADIUS Tunneling Packets from this AAA Client			
Documentation	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			

Per configurare il server RADIUS per l'autenticazione, la VLAN e l'assegnazione degli indirizzi IP, completare la procedura seguente:

Due nomi utente devono essere creati separatamente per i client che si connettono alla VLAN 2 e per la VLAN 3. A questo scopo, vengono creati un utente **user_vlan2** per i client che si connettono alla VLAN 2 e un altro utente **user_vlan3** per i client che si connettono alla VLAN 3.

Nota: qui viene mostrata la configurazione utente per i client che si connettono solo alla VLAN 2. Per gli utenti che si connettono alla VLAN 3, completare la stessa procedura.

1. Per aggiungere e configurare gli utenti, fare clic su **User Setup** (Impostazione utente) e definire il nome utente e la password.

Cisco Systems	User Setup	
- مىناالالىسىنالاللىب. -	Select	
User Setup		
Broup 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
Databases		Remove Dynamic Users
Posture Validation		
Network Access Profiles		Pack to Help

CISCO SYSTEMS	User Setup
Illin	Edit
User Setup	User: user_vlan2 (New User)
Setup	
Shared Profile Components	Account Disabled
Network Configuration	Supplementary User Info ?
System Configuration	Real Name user_vlan2
Interface Configuration	Description client in VLAN 2
Administration Control	<u></u>
Di External User Databases	User Setup ?
Posture Validation	Password Authentication:
	ACS Internal Database
Profiles	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Reports and Activity	Password •••••
Online Documentation	Confirm Password

 Definire l'assegnazione dell'indirizzo IP del client come assegnato dal pool di client AAA. Immettere il nome del pool di indirizzi IP configurato sullo switch per i client 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	Ose group setting
	O No callback allowed
Control	Callback using this number
= External User	C Dialup client specifies callback number
와데 Databases	C Use Windows Database callback settings
Posture Validation	
Network Access Profiles	Client IP Address Assignment
CA Reports and	C Use group settings
Activity	C No IP address assignment
0nline	O Assigned by dialup client
	C Assign static IP address
	Assigned by AAA client pool vlan2_clients

Nota: selezionare questa opzione e digitare il nome del pool IP del client AAA nella casella, solo se l'indirizzo IP deve essere assegnato da un pool di indirizzi IP configurato sul client AAA.

3. Definire gli attributi 64 e 65 della Internet Engineering Task Force (IETF). Assicurarsi che le etichette dei valori siano impostate su 1, come illustrato nell'esempio. Catalyst ignora i tag diversi da 1. Per assegnare un utente a una VLAN specifica, è necessario definire anche l'attributo 81 con un *nome di* VLAN corrispondente. Nota: il *nome* della VLAN deve essere esattamente uguale a quello configurato nello switch. Nota: l'assegnazione della VLAN basata sul *numero* VLAN non è supportata con CatOS.



Per ulteriori informazioni, fare riferimento alla <u>RFC 2868: per</u> ulteriori informazioni sugli attributi IETF, <u>consultare</u> la sezione <u>Attributi RADIUS per</u> il <u>supporto</u> del <u>protocollo</u> <u>tunnel</u>.**Nota:** nella configurazione iniziale del server ACS, gli attributi RADIUS IETF potrebbero non essere visualizzati in **Impostazione utente**. Per abilitare gli attributi IETF nella schermata di configurazione utente, scegliere **Configurazione interfaccia > RADIUS (IETF)**. Verificare quindi gli attributi **64**, **65** e **81** nelle colonne Utente e Gruppo.

Configurazione dei client PC per l'utilizzo dell'autenticazione 802.1x

Questo esempio è specifico del client Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL). Attenersi alla seguente procedura:

- 1. Scegliere Start > Pannello di controllo > Connessioni di rete, fare clic con il pulsante destro del mouse su Connessione alla rete locale e scegliere Proprietà.
- 2. Selezionare Mostra icona nell'area di notifica quando si è connessi nella scheda Generale.
- 3. Nella scheda Autenticazione selezionare Attiva autenticazione IEEE 802.1x per la rete.
- 4. Impostare il tipo EAP su MD5-Challenge, come mostrato

	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 computer when computer information is available
	Authenticate as guest when user or computer information is unavailable
	OK Cancel
nell'esempio:	

Per configurare i client in modo da ottenere un indirizzo IP da un server DHCP, completare la procedura seguente:

- 1. Scegliere Start > Pannello di controllo > Connessioni di rete, fare clic con il pulsante destro del mouse su Connessione alla rete locale e scegliere Proprietà.
- 2. Nella scheda Generale fare clic su Protocollo Internet (TCP/IP) e quindi su Proprietà.
- 3. Scegliere Ottieni automaticamente un indirizzo

Internet Protocol (TCP/IP) Proper	ties ?
You can get IP settings assigned au this capability. Otherwise, you need t the appropriate IP settings.	tomatically if your network supports to ask your network administrator for
Obtain an IP address automatic	cally
$\square \bigcirc \bigcirc$ Use the following IP address: -	
[P address:	· · · · ·
S <u>u</u> bnet mask:	
Default gateway:	
 Uptain UNS server address au Use the following DNS server : 	tomatically
Preferred DNS server.	
Alternate DNS server:	
	Ad <u>v</u> anced
	OK Cancel

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

<u>Client PC</u>

Se la configurazione è stata completata correttamente, i client del PC visualizzeranno una richiesta di immissione di nome utente e password.

1. Fare clic sul prompt, illustrato



Vien

nell'esempio:

e visualizzata una finestra per l'immissione del nome utente e della password.

2. Immettere	e il nome utente e la	
	Local Area Connection	
	User_vlan2	
	Password:	
	Logon domain:	
	OK Cancel	
password.	Not	a: in PC 1 e

2, immettere le credenziali utente della VLAN 2. In PC 3 e 4, immettere le credenziali utente della VLAN 3.

3. Se non viene visualizzato alcun messaggio di errore, verificare la connettività con i metodi tradizionali, ad esempio tramite l'accesso alle risorse di rete e con il comando **ping**. Questo è l'output restituito dal PC 1, da cui si ottiene un **ping** riuscito al 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 viene visualizzato questo errore, verificare che il nome utente e la password siano



Catalyst 6500

172.16.3.2

172.16.3.3

Se la password e il nome utente sembrano corretti, verificare lo stato della porta 802.1x sullo switch.

```
1. Cercare uno stato della porta che indichi autorizzato.
  Cat6K> (enable) show port dot1x 3/1-5
                  BEnd-State Port-Control
  Port Auth-State
                                             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
                                               authorized
                              auto
                      idle
  3/4 authenticated
                              auto
                                               authorized
  3/5 authenticated
                      idle
                               auto
                                                authorized
  Port Port-Mode Re-authentication Shutdown-timeout
  3/1 SingleAuth disabled
                                  disabled
  3/2 SingleAuth disabled
                                  disabled
  3/3 SingleAuth disabled
3/4 SingleAuth disabled
                                  disabled
                                  disabled
  3/5 SingleAuth disabled
                                   disabled
  Verificare lo stato della VLAN dopo aver completato l'autenticazione.
  Cat6K> (enable) show vlan
  VLAN Name
                                Status IfIndex Mod/Ports, Vlans
  _____ _____
                                 active 6
  1
    default
                                              2/1-2
                                               3/6-48
                                 active 83
  2
     VLAN2
                                               3/2-3
                                       84
    VLAN3
  3
                                               3/4-5
                                active
    AUTHFAIL_VLAN
  4
                                active 85
  5
    GUEST_VLAN
                                active 86
  10 RADIUS_SERVER
                                active 87
                                               3/1
 1002 fddi-default
                                active
                                        78
  1003 token-ring-default
                                active
                                        81
  1004 fddinet-default
                                active
                                         79
  1005 trnet-default
                                active
                                         80
  !--- Output suppressed.
2. Verificare lo stato del binding DHCP dal modulo di routing (MSFC) dopo l'autenticazione.
```

```
Router#show ip dhcp bindingIP addressHardware addressLease expirationType172.16.2.20100.1636.3333.9cFeb 14 2007 03:00 AMAutomatic172.16.2.30100.166F.3CA3.42Feb 14 2007 03:03 AMAutomatic
```

Feb 14 2007 03:05 AM

Feb 14 2007 03:07 AM

Automatic

Automatic

0100.145e.945f.99

0100.1185.8D9A.F9

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Esempio di autenticazione IEEE 802.1x con Catalyst 6500/6000 con software Cisco IOS
- Guida allo switching Catalyst e alla distribuzione di ACS
- <u>RFC 2868: Attributi RADIUS per il supporto del protocollo tunnel</u>
- <u>Configurazione dell'autenticazione 802.1x</u>
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico Cisco Systems