

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

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 esecuzione in modalità nativa (un'unica immagine software Cisco IOS® per Supervisor Engine e MSFC) e 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](#)
- [Come funziona RADIUS?](#)
- [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 Cisco IOS versione 12.2(18)SXF su Supervisor Engine **Nota:** per il supporto dell'autenticazione basata sulla porta 802.1x, è necessario il software Cisco IOS versione 12.1(13)E o successive.
- 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

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

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 EAPOL (Extensible Authentication Protocol over LAN) attraverso la porta a cui è connesso il dispositivo. Dopo l'autenticazione, il traffico normale può passare attraverso la porta.

Nota: se lo switch riceve pacchetti EAPOL dalla porta che non è configurata per l'autenticazione 802.1x o se lo switch non supporta l'autenticazione 802.1x, i pacchetti EAPOL vengono scartati e non vengono inoltrati ad alcun dispositivo upstream.

Configurazione

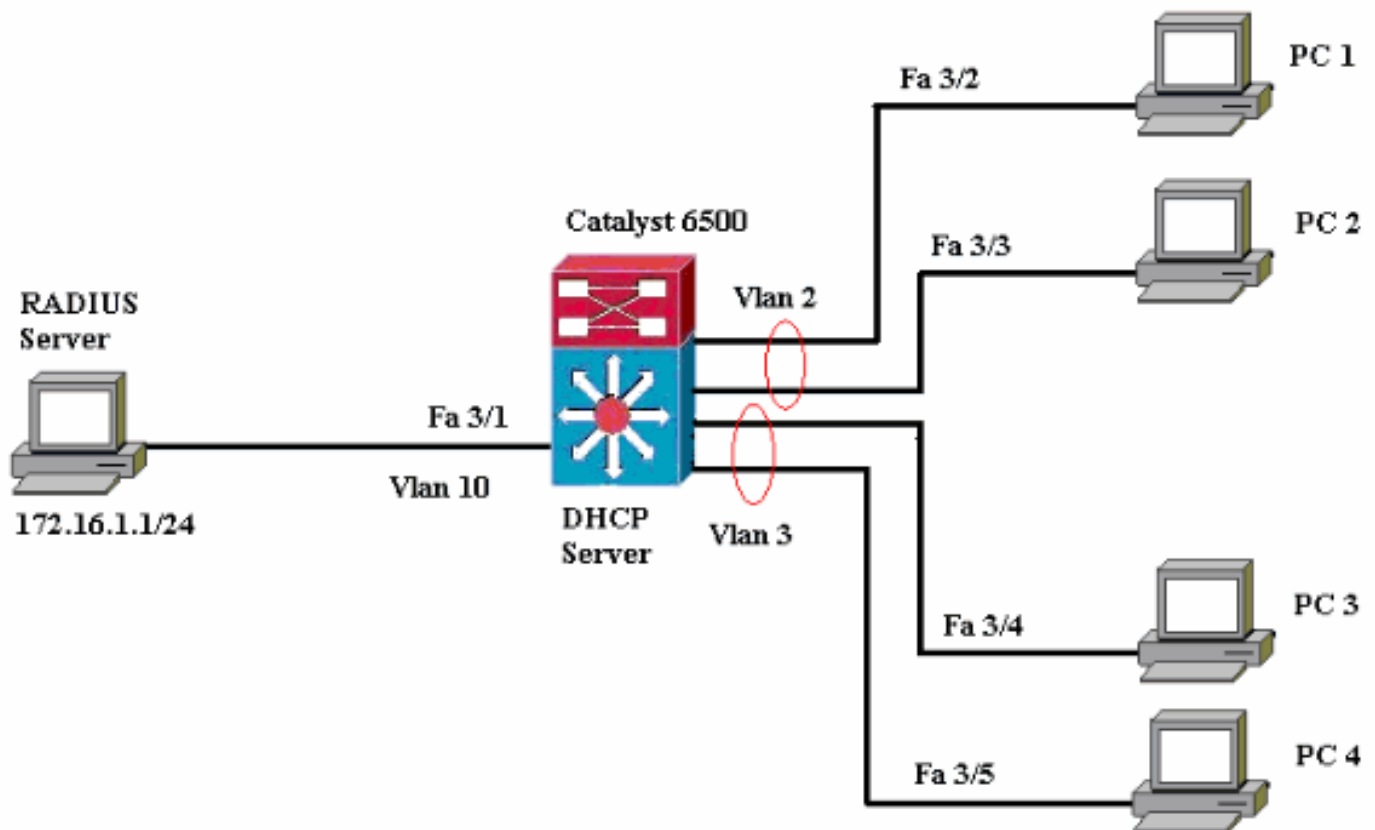
In questa sezione vengono presentate le informazioni necessarie per configurare la funzionalità 802.1x descritta in questo documento.

Questa configurazione richiede i seguenti passaggi:

- [Configurare lo switch Catalyst per l'autenticazione 802.1x](#).
- [Configurare il server RADIUS](#).
- [Configurare i client PC per l'utilizzo dell'autenticazione 802.1x](#).

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. Richiede informazioni sull'identità al client, verifica tali informazioni con il server RADIUS e invia 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 usano le stesse credenziali di accesso della VLAN 2. Analogamente, i PC 3 e 4 usano le credenziali di accesso della VLAN 3. I client PC sono configurati per ottenere l'indirizzo IP da un server DHCP.

Configurazione dello switch Catalyst per l'autenticazione 802.1x

La configurazione di esempio dello switch include:

- Come abilitare l'autenticazione 802.1x sulle porte Fast Ethernet.
- Come connettere un server RADIUS alla VLAN 10 dietro la porta Fast Ethernet 3/1.

- Una 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 [Linee guida e restrizioni](#) per l'autenticazione basata sulla porta 802.1x.

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

Catalyst 6500

```

Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname Cat6K
!--- Sets the hostname for the switch.
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
!--- This is a dedicated VLAN for the RADIUS server.
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut
!--- Assigns the port connected to the RADIUS server to
VLAN 10. !--- Note:- All the active access ports are in
VLAN 1 by default.

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat6K(config)#interface
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
!--- Enables 802.1x on all the FastEthernet interfaces.
Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model
!--- Enables AAA. Cat6K(config)#aaa authentication dot1x
default group radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat6K(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat6K(config)#radius-server host
172.16.1.1
!--- Sets the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco
!--- The key must match the key used on the RADIUS
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2

```

```

Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.2.1
!--- This pool assigns ip address for clients in VLAN 2.
Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

```

VLAN Name	Status	Ports

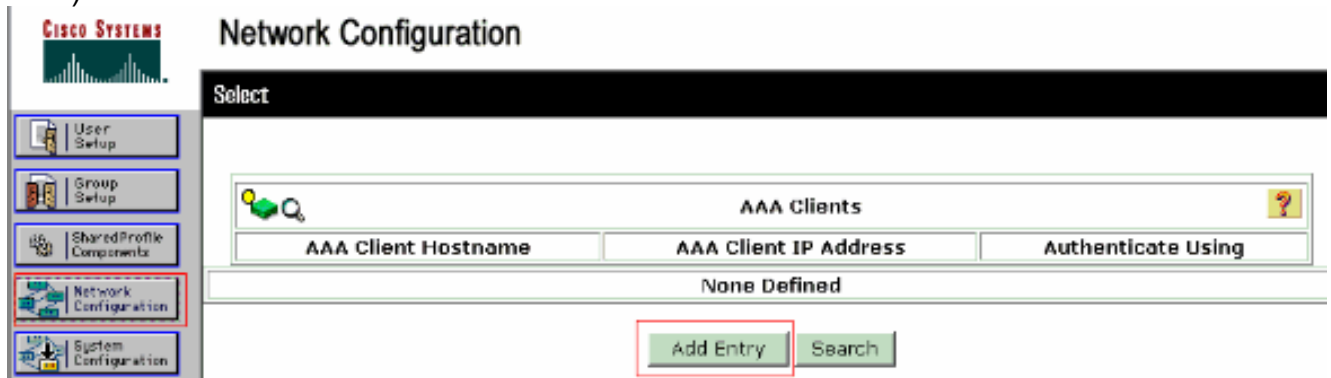
1 default	active	Fa3/2,
Fa3/3, Fa3/4, Fa3/5		Fa3/6,
Fa3/7, Fa3/8, Fa3/9		Fa3/10,
Fa3/11, Fa3/12, Fa3/13		Fa3/14,
Fa3/15, Fa3/16, Fa3/17		Fa3/18,
Fa3/19, Fa3/20, Fa3/21		Fa3/22,
Fa3/23, Fa3/24, Fa3/25		Fa3/26,
Fa3/27, Fa3/28, Fa3/29		Fa3/30,
Fa3/31, Fa3/32, Fa3/33		Fa3/34,
Fa3/35, Fa3/36, Fa3/37		Fa3/38,
Fa3/39, Fa3/40, Fa3/41		Fa3/42,
Fa3/43, Fa3/44, Fa3/45		Fa3/46,
Fa3/47, Fa3/48		
2 VLAN2	active	
3 VLAN3	active	
10 RADIUS_SERVER	active	Fa3/1
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	
<i>!--- Output suppressed. !--- All active ports are in VLAN 1 (except 3/1) before authentication.</i>		

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

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:

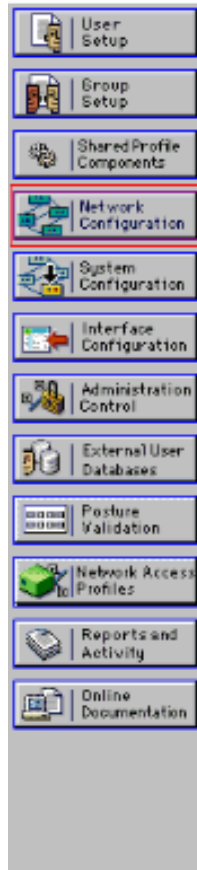
1. Per configurare un client AAA, fare clic su **Configurazione di rete** nella finestra di amministrazione di ACS.
2. Fare clic su **Add Entry** (Aggiungi voce) nella sezione AAA Client (Client AAA).



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 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:



Network Configuration



Add AAA Client

AAA Client Hostname	<input type="text" value="Cat6K"/>
AAA Client IP Address	<input type="text" value="172.16.1.2"/>
Shared Secret	<input type="text" value="cisco"/>
RADIUS Key Wrap	
Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal
Authenticate Using	<input type="text" value="RADIUS (IETF)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	
<input type="button" value="Submit"/> <input type="button" value="Submit + Apply"/> <input type="button" value="Cancel"/>	

Completare la procedura descritta di seguito per configurare il server RADIUS per l'autenticazione, la VLAN e l'assegnazione dell'indirizzo IP.

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, seguire 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**

Select

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

CISCO SYSTEMS **User Setup**

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info

Real Name
 Description

User Setup


Password Authentication:

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

Password
 Confirm Password

2. 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.



User Setup

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:

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

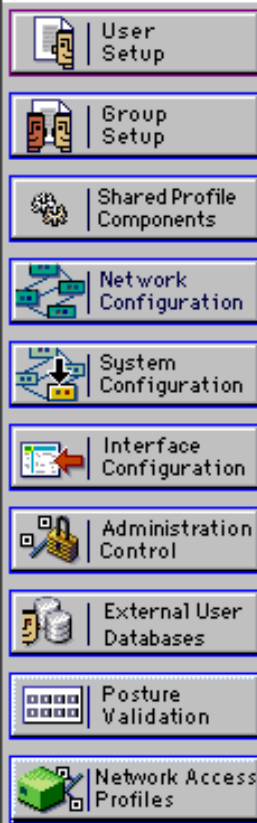
- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

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** di 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* o un *numero di VLAN* corrispondente. **Nota:** se si usa il *nome* VLAN, deve essere esattamente lo stesso di quello configurato nello switch.



User Setup



Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes

[006] Service-Type

[064] Tunnel-Type

Tag Value

[065] Tunnel-Medium-Type

Tag Value

[081] Tunnel-Private-Group-ID

Tag Value

Nota: Per ulteriori informazioni su questi attributi IETF, fare riferimento alla [RFC 2868: Attributi RADIUS per il supporto del protocollo tunnel](#). **Nota:** nella configurazione iniziale del server ACS, gli attributi RADIUS IETF potrebbero non essere visualizzati in **Impostazione utente**. Per abilitare gli attributi IETF nelle schermate di configurazione utente, scegliere **Configurazione interfaccia > RADIUS (IETF)**. Verificare quindi gli attributi **64**, **65** e **81** nelle colonne Utente e Gruppo. **Nota:** se non si definisce l'attributo IETF **81** e la porta è una porta dello switch in modalità di accesso, il client ha assegnato la VLAN di accesso della porta. Se è stato definito l'attributo **81** per l'assegnazione dinamica della VLAN e la porta è una porta dello switch in modalità di accesso, è necessario usare il comando **aaa authorization network default group radius (raggio del gruppo predefinito)** sullo switch). Con questo comando la porta viene assegnata alla VLAN fornita dal server RADIUS. In caso contrario, 802.1x sposta la porta allo stato **AUTORIZZATO** dopo l'autenticazione dell'utente; tuttavia, la porta si trova ancora nella VLAN predefinita e la connettività potrebbe non riuscire. Se è stato definito l'attributo **81**, ma la porta è stata configurata come porta instradata, si verifica un rifiuto di accesso. Questo messaggio di errore visualizza:

```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
```

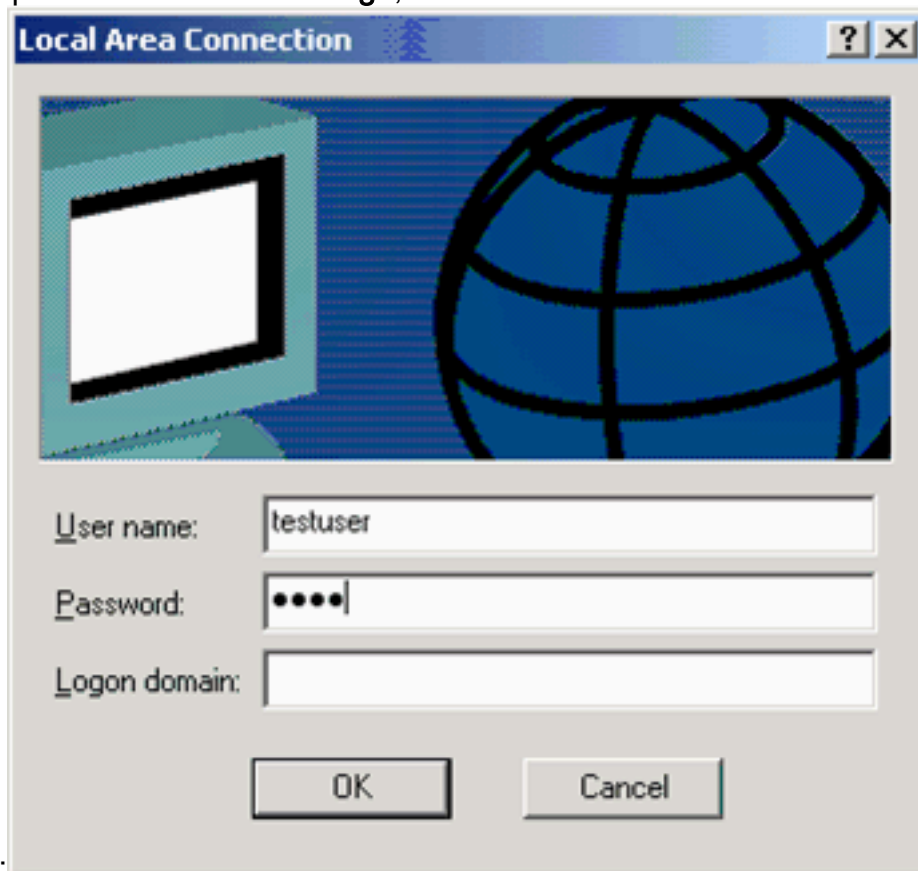
```
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose  
VLAN cannot be assigned.
```

[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):

1. Scegliere **Start > Pannello di controllo > Connessioni di rete**, fare clic con il pulsante destro

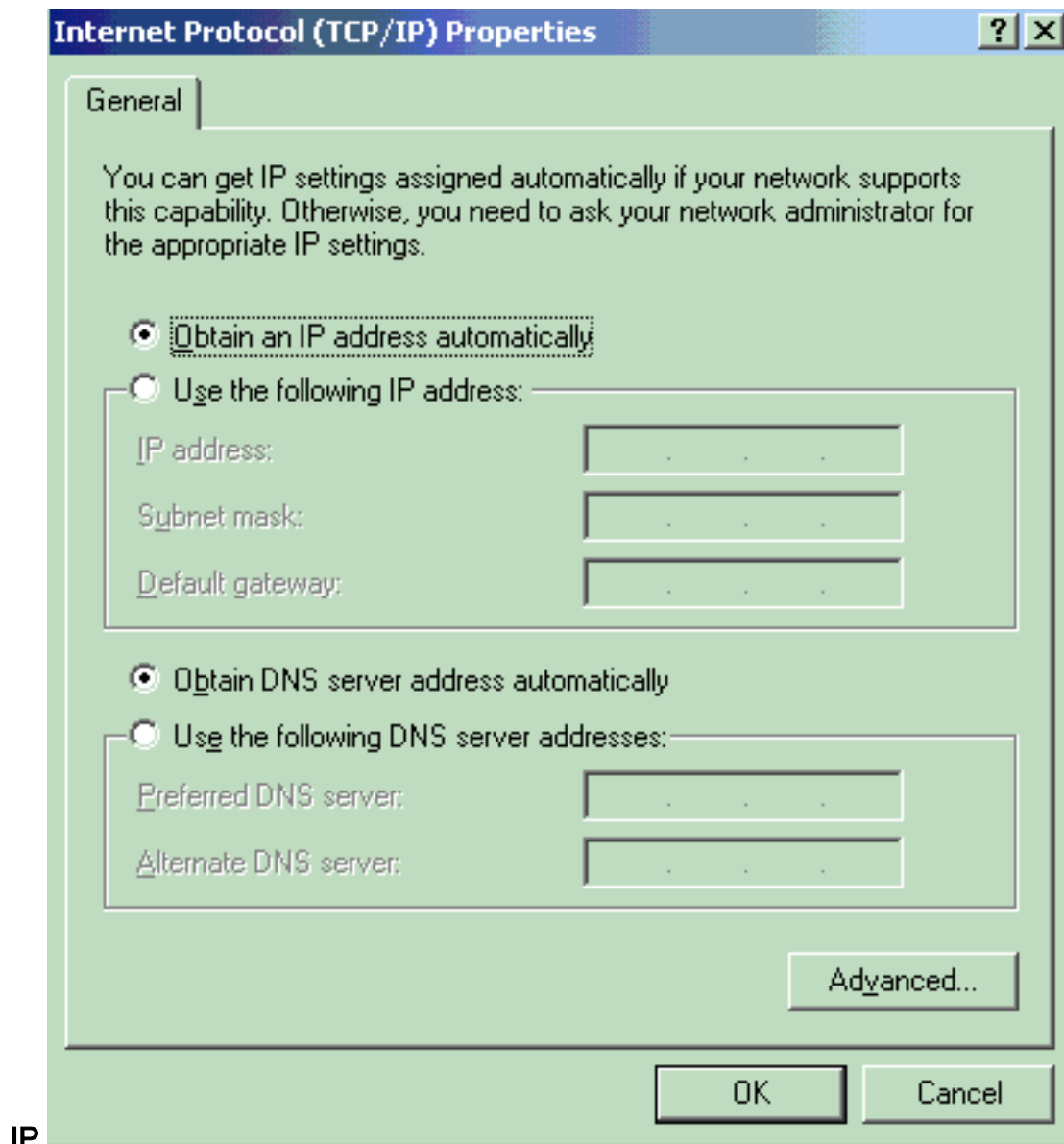
- del mouse su **Connessione alla rete locale** e scegliere **Proprietà**.
- Selezionare **Mostra icona nell'area di notifica quando si è connessi** nella scheda Generale.
- Nella scheda Autenticazione selezionare **Attiva autenticazione IEEE 802.1x per la rete**.
- Impostare il tipo EAP su **MD5-Challenge**, come mostrato



nell'esempio:

Completare la procedura seguente per configurare i client in modo che ottengano l'indirizzo IP da un server DHCP.

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



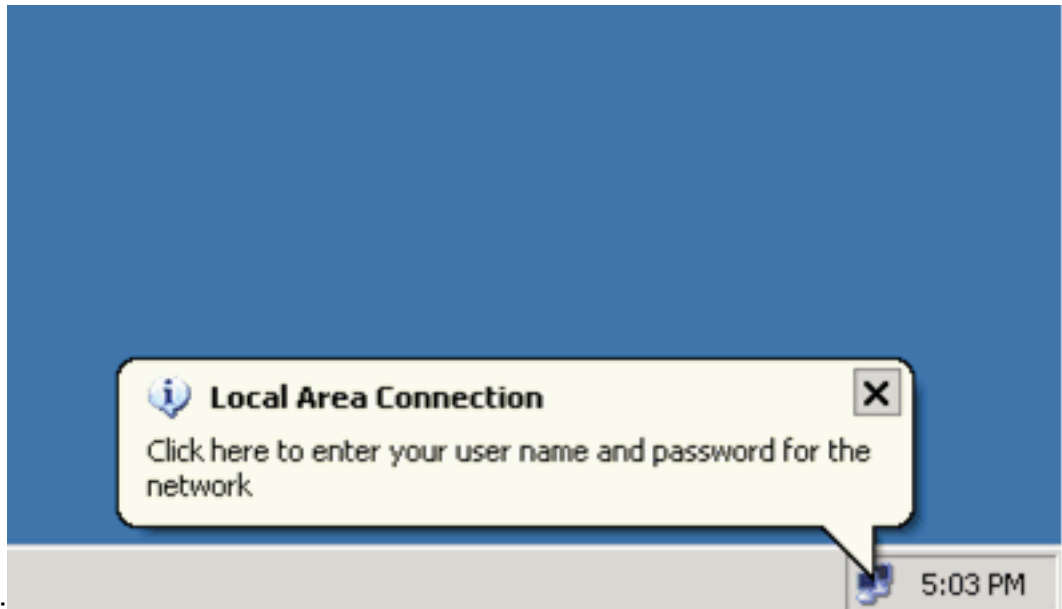
IP.

[Verifica](#)

[Client PC](#)

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

1. Fare clic sul prompt, illustrato

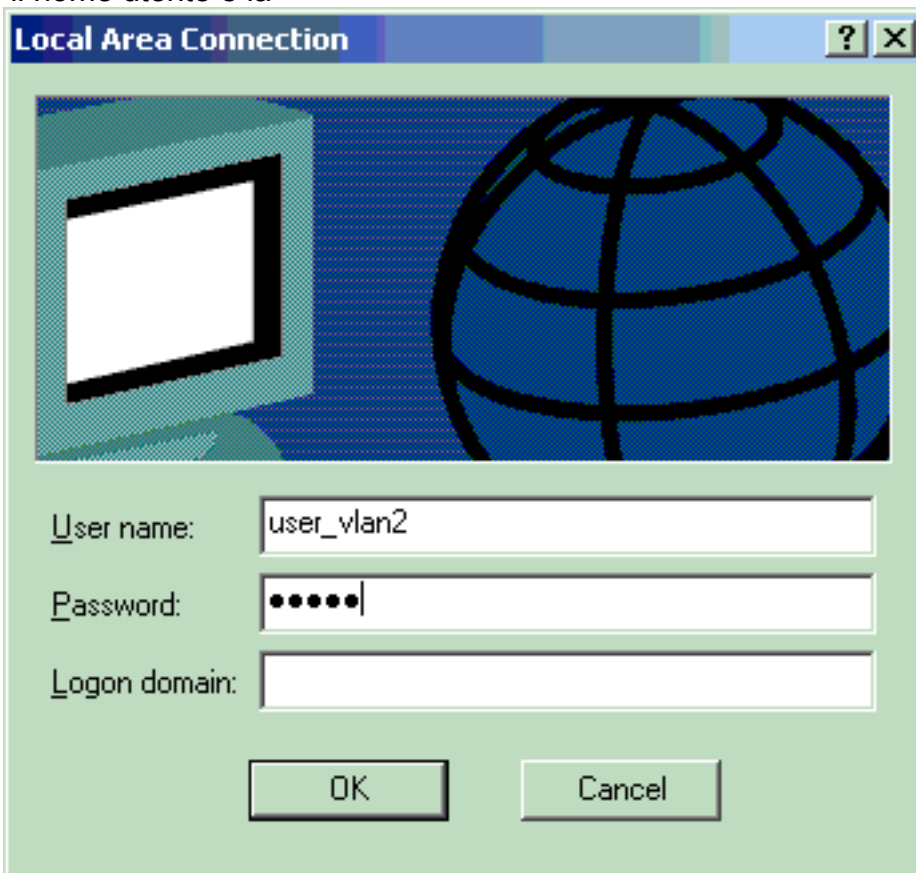


nell'esempio:

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

Vien

2. Immettere il nome utente e la



password.

Nota: nei PC 1 e

2, immettere le credenziali utente della VLAN 2 e nei 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 **ping**. Questo output viene dal PC 1 e visualizza il risultato positivo del **ping** 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 . :
    IP Address . . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    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
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
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 = 0ms, Maximum = 0ms, Average = 0ms

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
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
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 = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2

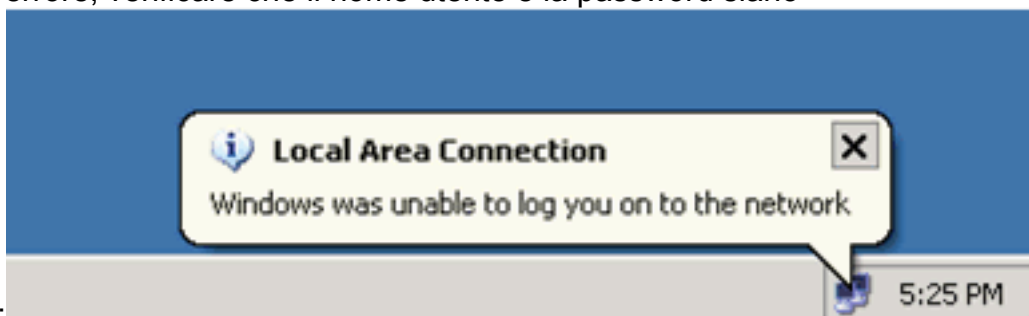
Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
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 = 0ms, Maximum = 0ms, Average = 0ms

4: C:\Documents and Settings\Administrator>
```

Se viene visualizzato questo errore, verificare che il nome utente e la password siano



corretti:

Catalyst 6500

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#show dot1x
```

```
Sysauthcontrol           = Enabled
Dot1x Protocol Version   = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Cat6K#show dot1x interface fastEthernet 3/2
```

```
AuthSM State             = AUTHENTICATED
BendSM State             = IDLE
PortStatus              = AUTHORIZED
MaxReq                   = 2
MultiHosts               = Enabled
Port Control             = Auto
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod            = 3600 Seconds
ServerTimeout           = 30 Seconds
SuppTimeout             = 30 Seconds
TxPeriod                 = 30 Seconds
```

```
Cat6K#show dot1x interface fastEthernet 3/4
```

```
AuthSM State             = AUTHENTICATED
BendSM State             = IDLE
PortStatus              = AUTHORIZED
MaxReq                   = 2
MultiHosts               = Enabled
Port Control             = Auto
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod            = 3600 Seconds
ServerTimeout           = 30 Seconds
SuppTimeout             = 30 Seconds
TxPeriod                 = 30 Seconds
```

```
Cat6K#show dot1x interface fastEthernet 3/1
```

```
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State             = FORCE AUTHORIZED
BendSM State             = IDLE
PortStatus              = AUTHORIZED
MaxReq                   = 2
MultiHosts               = Disabled
PortControl             = Force Authorized
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod            = 3600 Seconds
ServerTimeout           = 30 Seconds
SuppTimeout             = 30 Seconds
TxPeriod                 = 30 Seconds
```

Verificare lo stato della VLAN dopo aver completato l'autenticazione.

```
Cat6K#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25,

```

Fa3/26, Fa3/27, Fa3/28, Fa3/29,
Fa3/30, Fa3/31, Fa3/32, Fa3/33,
Fa3/34, Fa3/35, Fa3/36, Fa3/37,
Fa3/38, Fa3/39, Fa3/40, Fa3/41,
Fa3/42, Fa3/43, Fa3/44, Fa3/45,
Fa3/46, Fa3/47, Fa3/48
2    VLAN2          active    Fa3/2, Fa3/3
3    VLAN3          active    Fa3/4, Fa3/5
10   RADIUS_SERVER active    Fa3/1
1002 fddi-default    act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
!--- Output suppressed.

```

2. Verificare lo stato del binding DHCP da dopo l'autenticazione.

```

Router#show ip dhcp binding
IP address      Hardware address   Lease expiration   Type
172.16.2.2      0100.1636.3333.9c  Mar 04 2007 06:35 AM Automatic
172.16.2.3      0100.166F.3CA3.42  Mar 04 2007 06:43 AM Automatic
172.16.3.2      0100.145e.945f.99  Mar 04 2007 06:50 AM Automatic
172.16.3.3      0100.1185.8D9A.F9  Mar 04 2007 06:57 AM Automatic

```

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Raccogli l'output di questi comandi di **debug** per risolvere i problemi:

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug dot1x events:** abilita il debug delle istruzioni di stampa protette dal flag eventi dot1x.

```

Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
this id 13
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS

```



```

00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
    id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
    will pick up any pending requests from the queue
Cat6K#
Cat6K#
!--- Debug output for PC 3 connected to Fa3/4. 00:19:58: dot1x-ev:Got a Request from SP to
send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0
00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 00:19:58: dot1x-
ev:The Interface on which we got this AAA
    Request is FastEthernet3/4
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
    for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
    for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
    will pick up any pending requests from the queue
Cat6K#

```

- **debug radius - Visualizza le informazioni associate a RADIUS.**

```

Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-
login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit
FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6
AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36:
Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18
CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79
00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18
172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80
18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104
00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8

```

```
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36:
Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18
11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# !--- Debug
output for PC 3 connected to Fa3/4. 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11
172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute
61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58:
Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from
id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58:
Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

Informazioni correlate

- [Esempio di autenticazione IEEE 802.1x con Catalyst 6500/6000 con software CatOS](#)
- [Linee guida per la distribuzione di Cisco Secure ACS per server Windows NT/2000 in un ambiente switch Cisco Catalyst](#)
- [RFC 2868: Attributi RADIUS per il supporto del protocollo tunnel](#)
- [Configurazione dell'autenticazione basata sulla porta IEEE 802.1X](#)
- [Supporto dei prodotti LAN](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)