

Esempio di autenticazione cablata 802.1x su uno switch Catalyst serie 3550 e su una configurazione ACS versione 4.2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di configurazione dello switch](#)

[Configurazione ACS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene illustrato un esempio di configurazione di base di IEEE 802.1x con Cisco Access Control Server (ACS) versione 4.2 e il protocollo RADIUS (Remote Access Dial In User Service) per l'autenticazione cablata.

Prerequisiti

Requisiti

Cisco consiglia di:

- Confermare la raggiungibilità IP tra ACS e lo switch.
- Verificare che le porte UDP (User Datagram Protocol) 1645 e 1646 siano aperte tra ACS e lo switch.

Componenti usati

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

- Switch Cisco Catalyst serie 3550

- Cisco Secure ACS versione 4.2

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.

Configurazione

Esempio di configurazione dello switch

1. Per definire il server RADIUS e la chiave già condivisa, immettere questo comando:

```
Switch(config)# radius-server host 192.168.1.3 key cisco123
```

2. Per abilitare la funzionalità 802.1x, immettere questo comando:

```
Switch(config)# dot1x system-auth-control
```

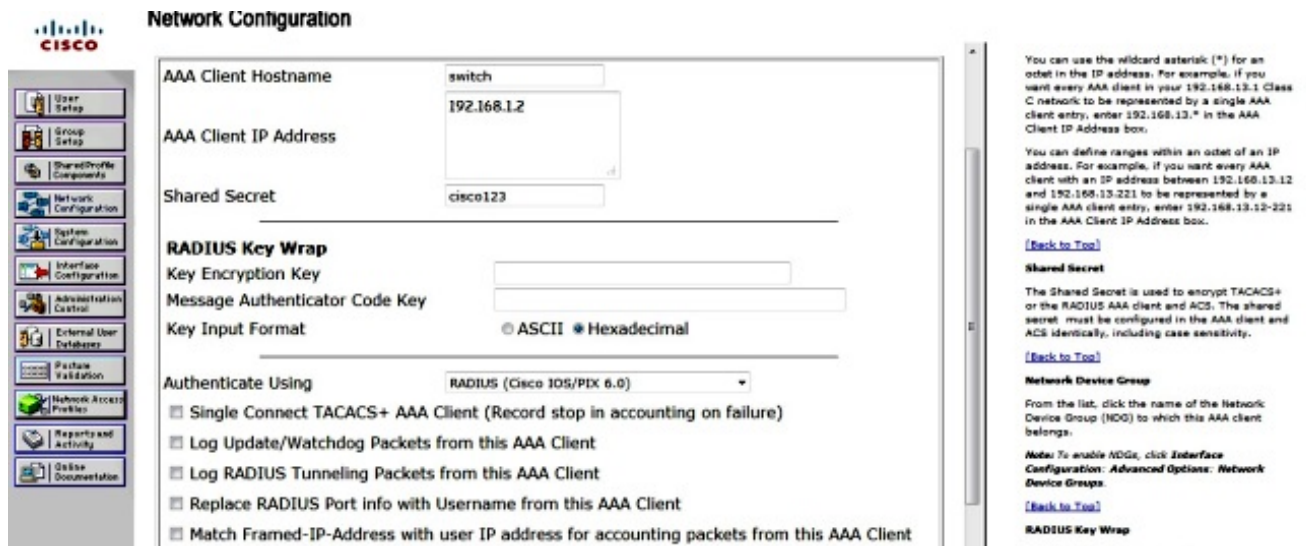
3. Per abilitare l'autenticazione, l'autorizzazione e l'accounting AAA (Authentication, Authorization, and Accounting) e RADIUS a livello globale, immettere i seguenti comandi:
Nota: questa operazione è necessaria se è necessario passare attributi dal server RADIUS. In caso contrario, è possibile ignorarla.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

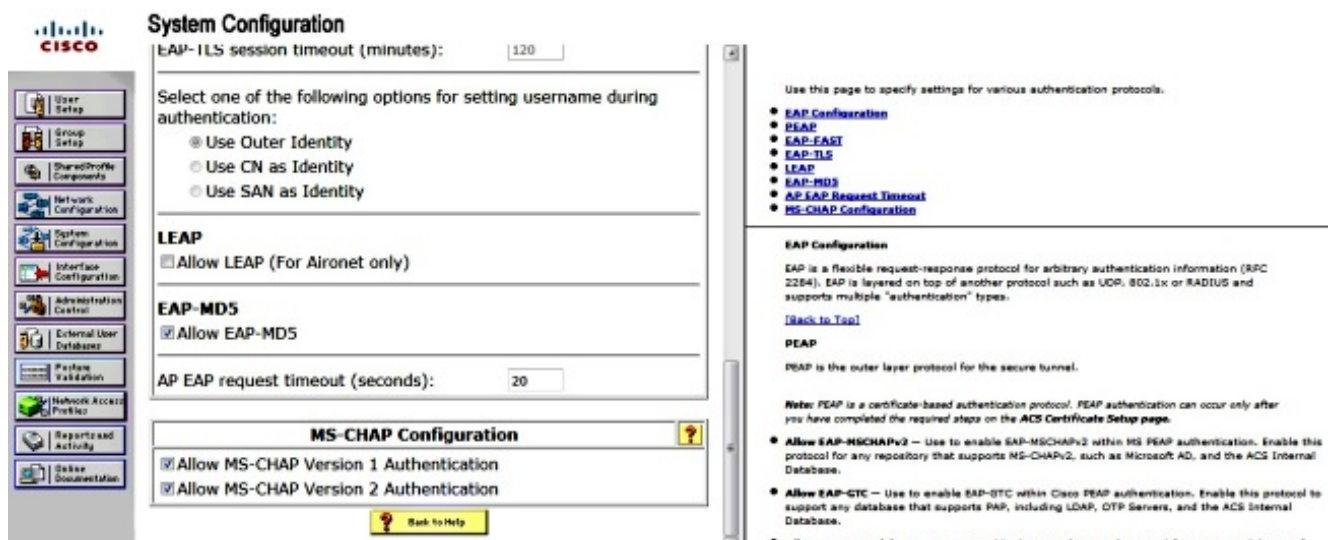
```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

Configurazione ACS

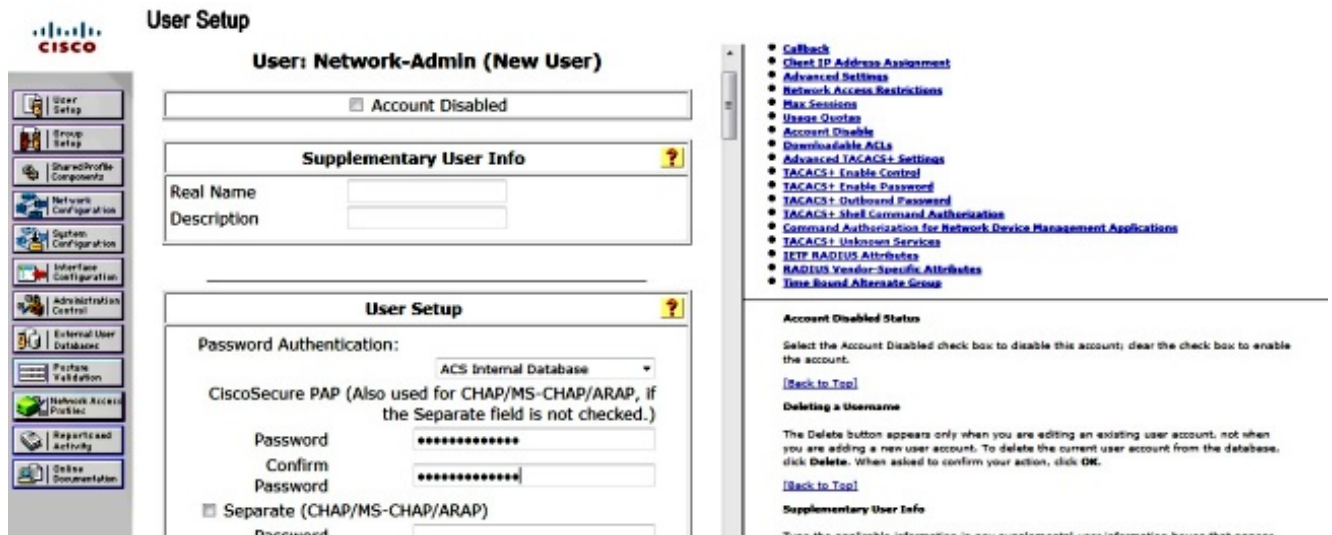
1. Per aggiungere lo switch come client AAA in ACS, selezionare **Configurazione di rete > Aggiungi voce client AAA**, quindi immettere le seguenti informazioni:
Indirizzo IP: <IP> Segreto condiviso: <chiave> Autenticazione tramite: Radius (Cisco IOS®/PIX 6.0)



2. Per configurare l'impostazione dell'autenticazione, passare a **Configurazione di sistema > Impostazione autenticazione globale** e verificare che la casella di controllo **Consenti autenticazione MS-CHAP versione 2** sia selezionata:



3. Per configurare un utente, scegliere **Configurazione utente** dal menu e attenersi alla seguente procedura:
 Immettere le informazioni **utente**: Network-Admin <nomeutente>. Fare clic su **Aggiungi/Modifica**. Immettere il **nome reale**: Network-Admin <nome descrittivo>. Aggiungere una **descrizione**: <scelta>. Selezionare **Autenticazione password**: Database interno ACS. Inserire la **password**: <password>. Confermare la **password**: <password>. Fare clic su **Invia**.



Verifica

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

Per verificare che la configurazione funzioni correttamente, immettere questi comandi:

- mostra punto1x
- mostra riepilogo dot1x
- interfaccia show dot1x
- show authentication sessions interface <interface>
- show authentication interface <interface>

```
Switch(config)# show dot1x
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

```
Switch(config)# show dot1x summary
```

```
Interface PAE Client Status
```

```
Fa0/4 AUTH
```

```
Switch(config)# show dot1x interface fa0/4 detail
```

```
Dot1x Info for FastEthernet0/4
```

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

Risoluzione dei problemi

In questa sezione vengono forniti i comandi di debug che è possibile utilizzare per risolvere i problemi relativi alla configurazione.

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

- debug dot1x all
- debug authentication all
- debug radius (fornisce le informazioni sul raggio a livello di debug)
- debug autenticazione aaa (debug per l'autenticazione)
- autorizzazione debug aaa (debug per autorizzazione)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).