Configurazione dell'autenticazione basata sull'indirizzo MAC su uno switch dall'interfaccia della riga di comando

Obiettivo

802.1X è uno strumento di amministrazione che consente di elencare i dispositivi e garantisce che non vi siano accessi non autorizzati alla rete. In questo documento viene spiegato come configurare l'autenticazione basata sull'indirizzo MAC su uno switch con l'interfaccia della riga di comando (CLI).

Per ulteriori informazioni, consultare il glossario.

Come funziona RADIUS?

Esistono tre componenti principali per l'autenticazione 802.1X, un supplicant (client), un autenticatore (dispositivo di rete come uno switch) e un server di autenticazione (RADIUS). Il servizio RADIUS (Remote Authentication Dial-In User Service) è un server di accesso che utilizza il protocollo di autenticazione, autorizzazione e accounting (AAA) e che consente la gestione di un indirizzo IP statico di 192.168.1.100. L'indirizzo IP statico dell'autenticatore è 192.168.1.101.

Dispositivi interessati

- Serie Sx350X
- Serie SG350XG
- Serie Sx550X
- Serie SG550XG

Versione del software

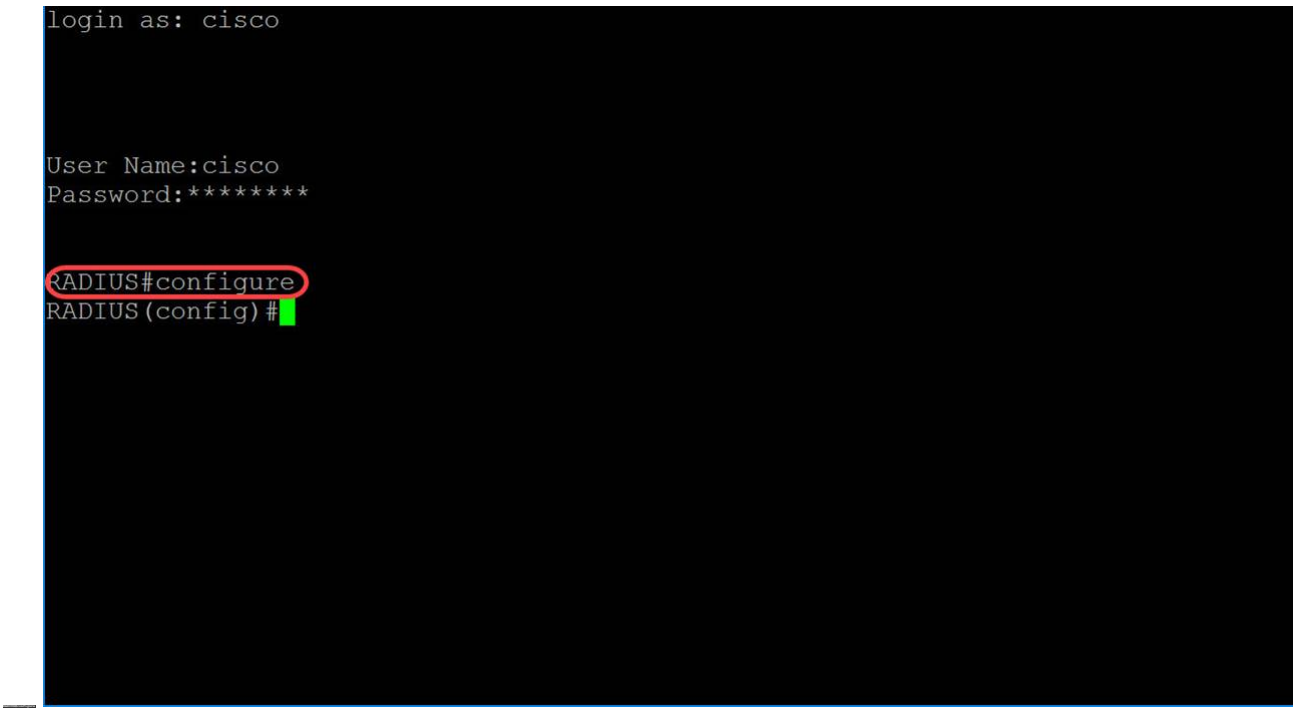
- 2.4.0.94

Configurazione del server RADIUS su uno switch

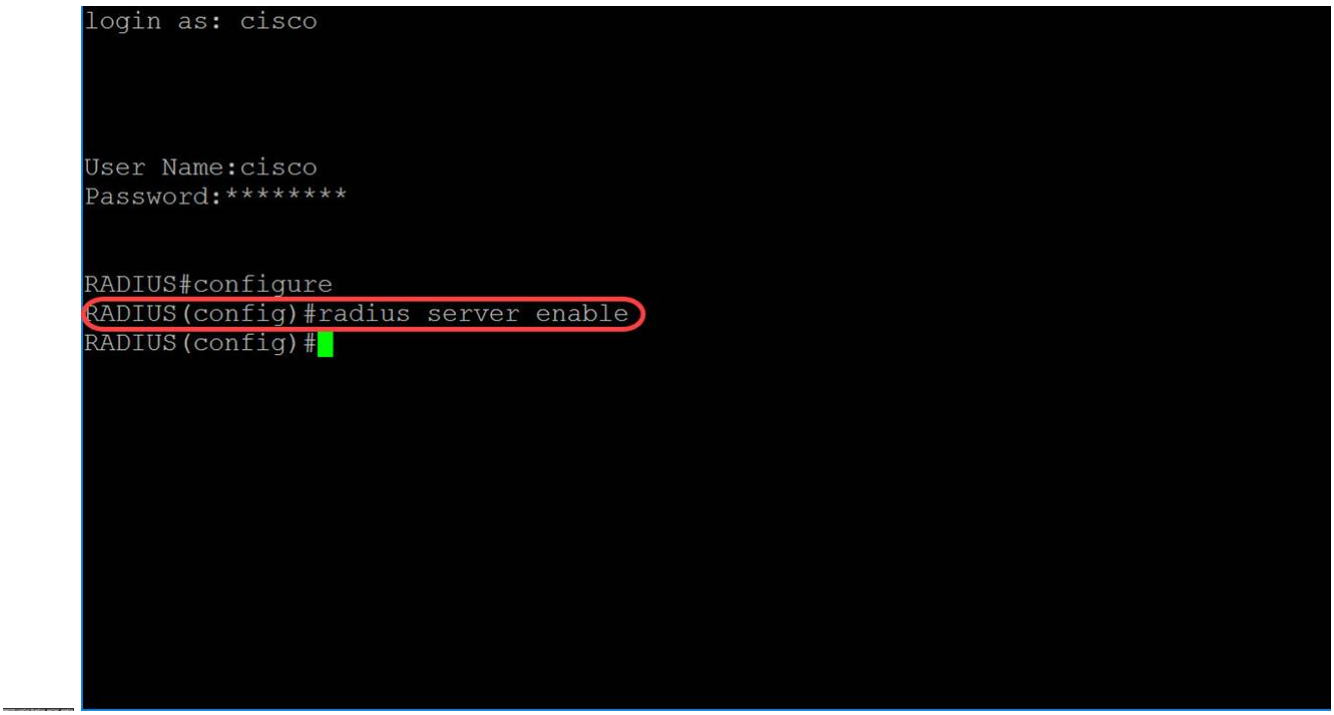
Passaggio 1. Collegare SSH allo switch che diventerà il server RADIUS. Il nome utente e la password predefiniti sono cisco/cisco. Se sono stati configurati un nuovo nome utente o password, immettere queste credenziali.

Nota: Per informazioni su come accedere a uno switch per PMI tramite SSH o Telnet, fare clic su qui.

Passaggio 2. In modalità di esecuzione privilegiata dello switch, accedere alla modalità di configurazione globale immettendo quanto segue:



Passaggio 3. Utilizzare il comando **radius server enable** per abilitare il server RADIUS.

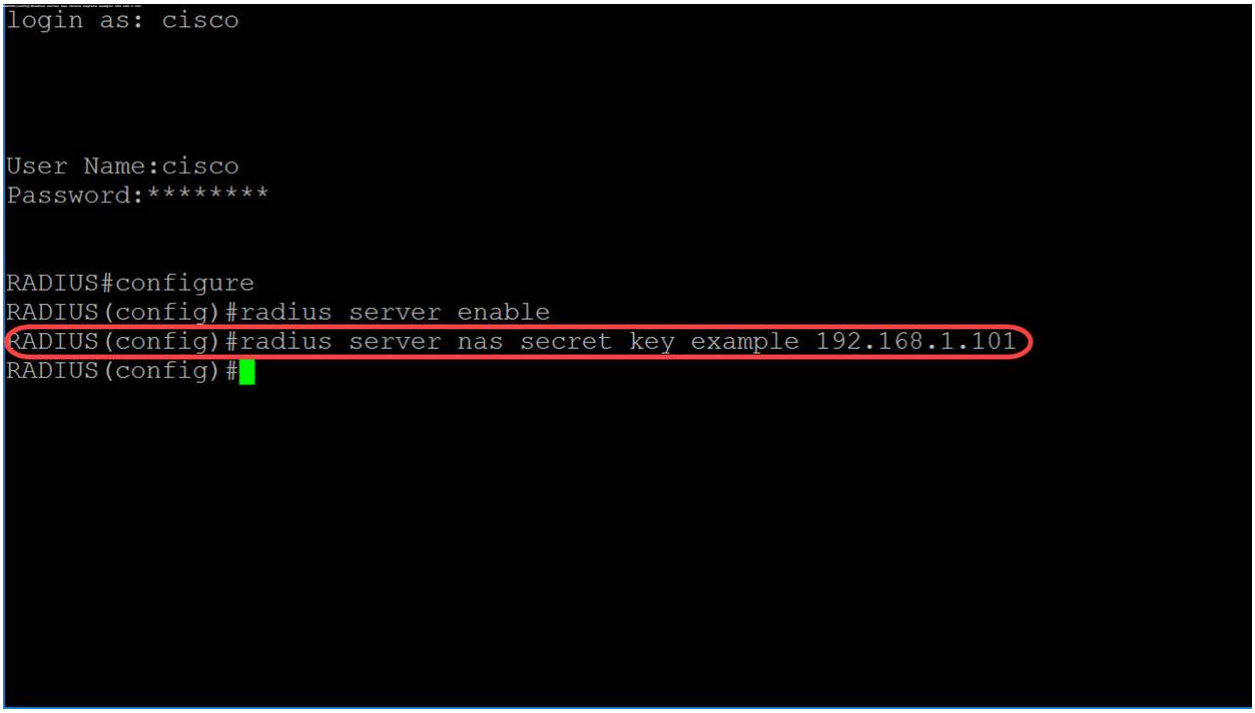


Passaggio 4. Per creare una chiave segreta, utilizzare il comando **radius server nas secret**

key in modalità di configurazione globale. I parametri sono definiti come segue:

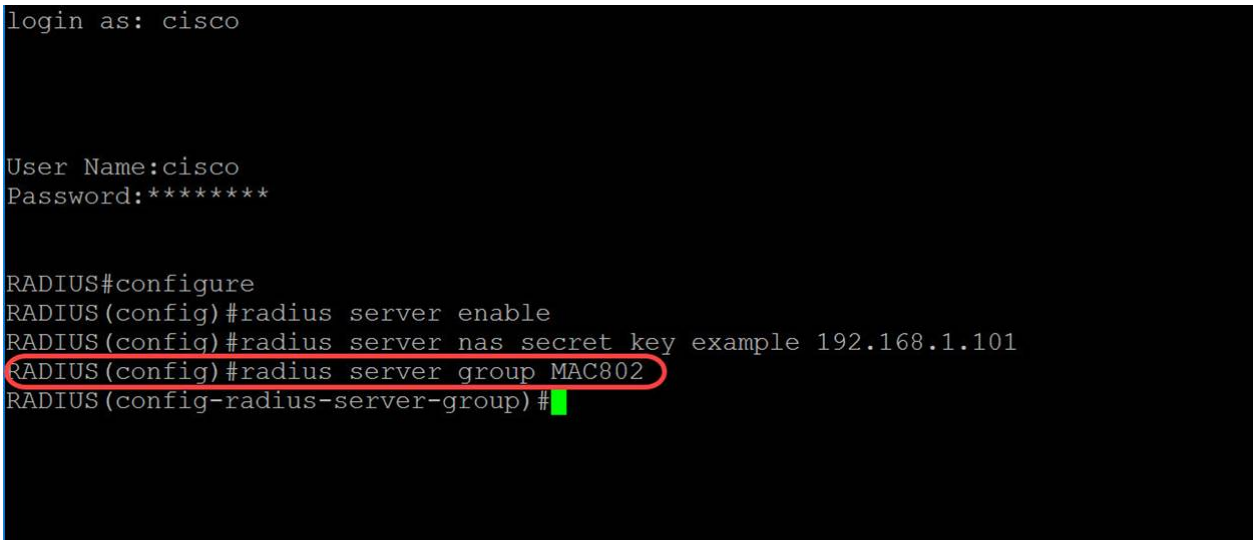
- chiave — specifica la chiave di autenticazione e crittografia per le comunicazioni tra il dispositivo e gli utenti del gruppo specificato. L'intervallo è compreso tra 0 e 128 caratteri.
- default - Specifica la chiave segreta predefinita che verrà applicata per comunicare con NAS che non dispongono di una chiave privata.
- ip-address: specifica l'indirizzo IP dell'host del client RADIUS. L'indirizzo IP può essere un indirizzo IPv4, IPv6 o IPv6z.

In questo esempio, verrà utilizzato **example** come chiave e **192.168.1.101** come indirizzo IP dell'autenticatore.



Passaggio 5. Per accedere alla modalità di configurazione del gruppo di server RADIUS e creare un gruppo se non esiste, utilizzare il comando radius server group in modalità di configurazione globale.

In questo articolo, utilizzeremo **MAC802** come nome del nostro gruppo.

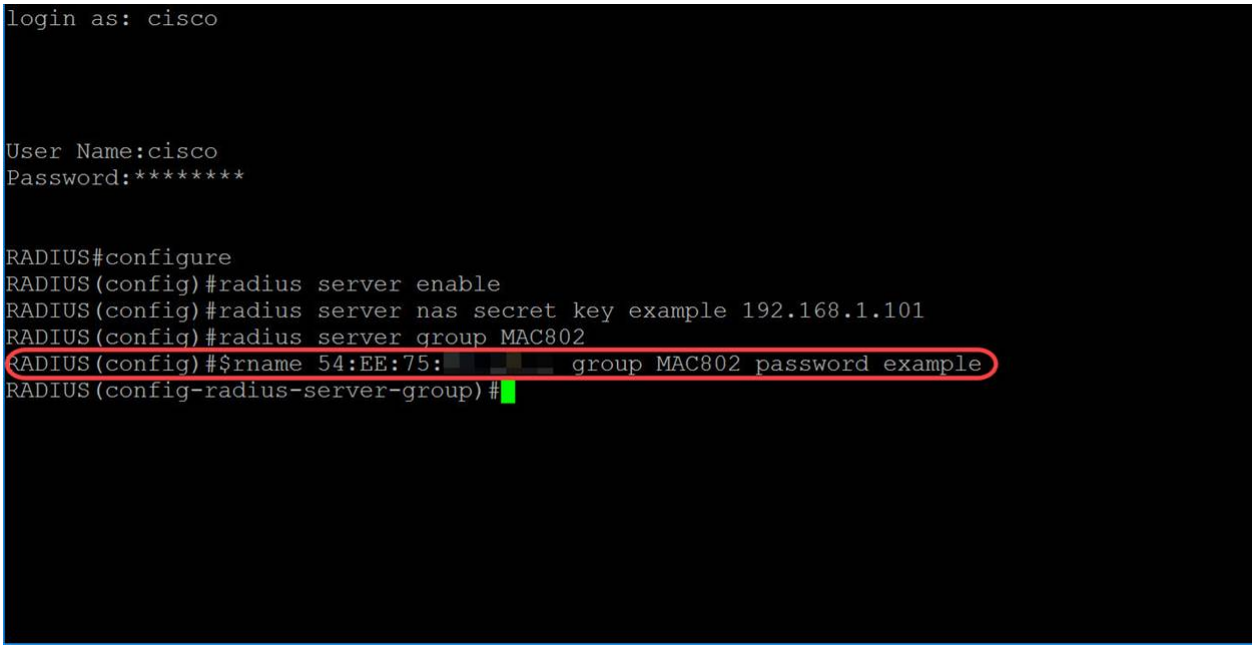


Passaggio 6. Per creare un utente, utilizzare il comando **radius server user** in modalità di configurazione globale. I parametri sono definiti come segue:

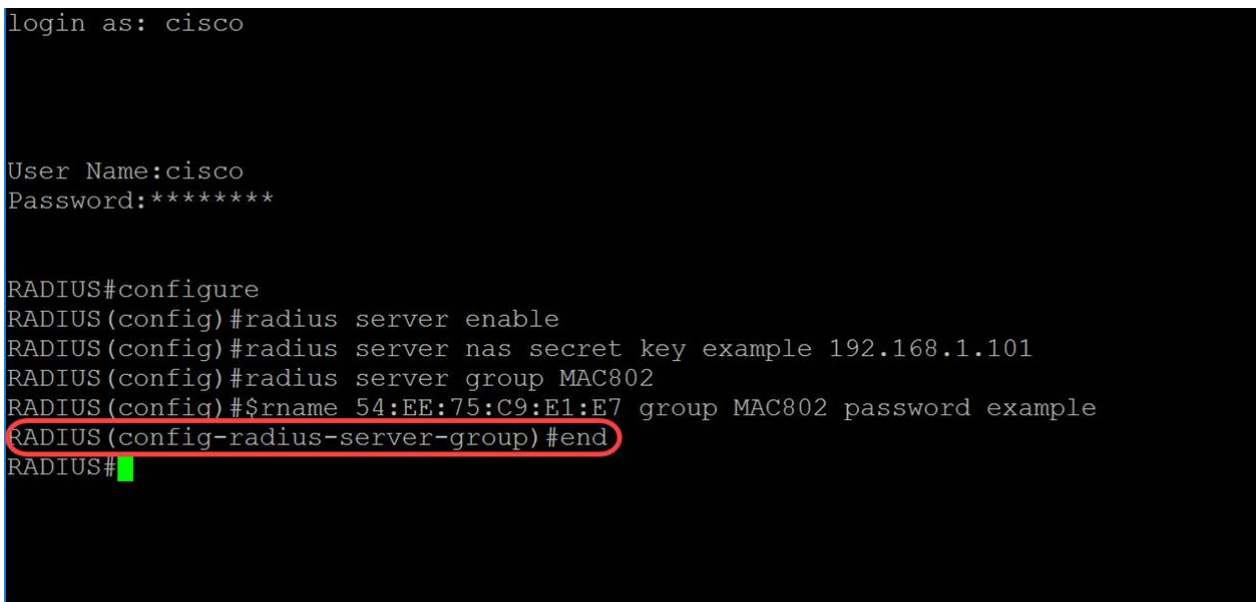
- user-name: specifica il nome utente. La lunghezza è compresa tra 1 e 32 caratteri.
- group-name - Specifica il nome del gruppo di utenti. La lunghezza del nome del gruppo è compresa tra 1 e 32 caratteri.
- unencrypted-password — specifica la password dell'utente. La lunghezza può essere compresa tra 1 e 64 caratteri.

Nell'esempio, verrà utilizzato l'indirizzo MAC della porta Ethernet come nome utente, **MAC802** come *nome gruppo* e *password non crittografata* come **esempio**.

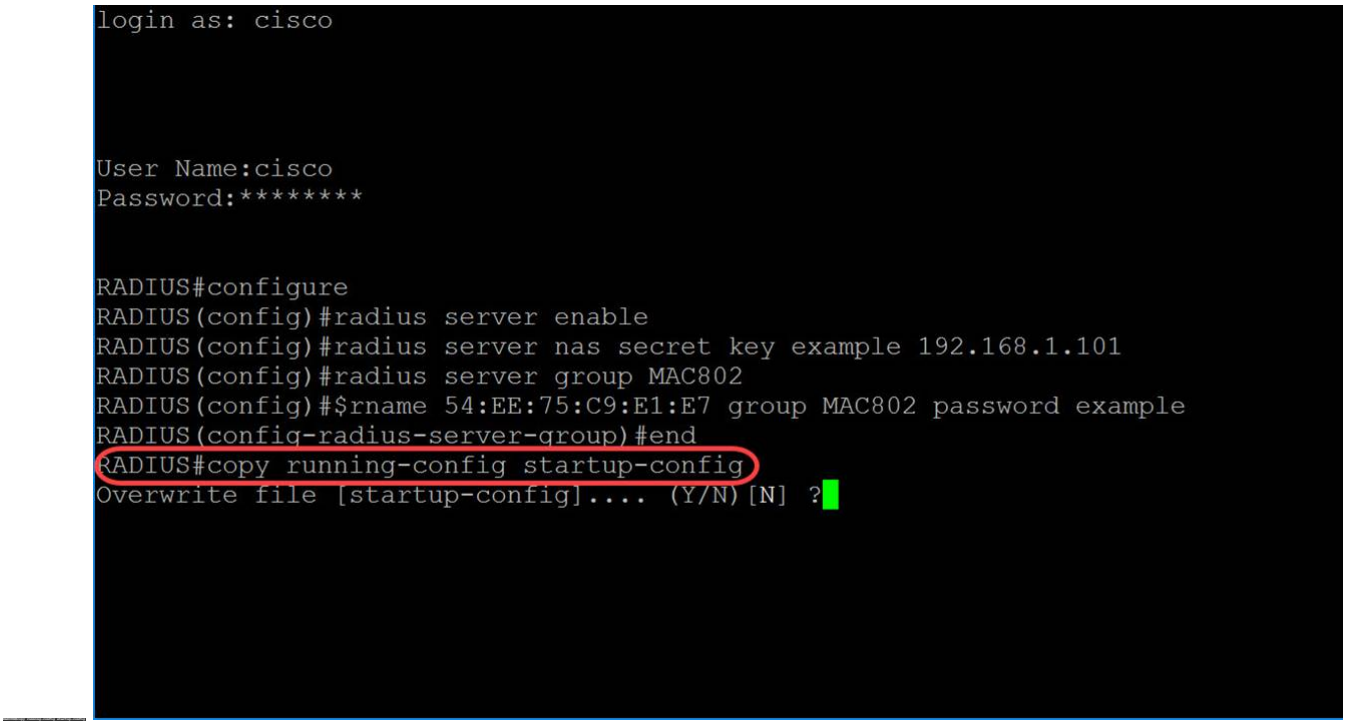
Nota: Alcuni ottetti dell'indirizzo MAC risultano sfocati. L'**esempio di** password non è una password complessa. Utilizza una password più complessa in quanto utilizzata solo come esempio. Si noti inoltre che il comando era troppo lungo nell'immagine per essere mandato a capo automaticamente.



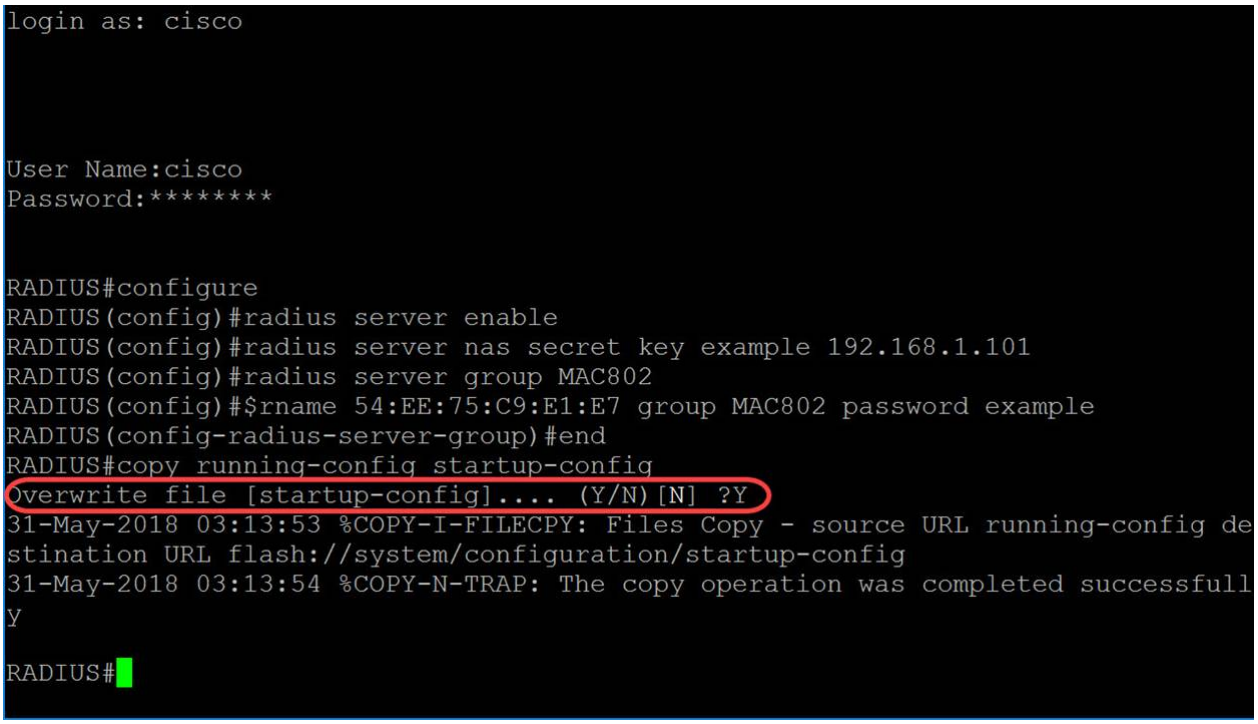
Passaggio 7. (Facoltativo) Per terminare la sessione di configurazione corrente e tornare in modalità di esecuzione privilegiata, utilizzare il comando **end**.



Passaggio 8. (Facoltativo) Per copiare un file da un'origine a una destinazione, utilizzare il comando **copy** in modalità di esecuzione privilegiata. Nell'esempio, la configurazione in esecuzione viene salvata nella configurazione di avvio.



Passaggio 9. (Facoltativo) Viene visualizzato un messaggio in cui viene chiesto se si desidera sovrascrivere il file della configurazione di avvio. Digitare **Y** per yes o **N** per no. Verrà digitato **Y** per sovrascrivere il file di configurazione di avvio.



Configurazione dello switch di autenticazione

Passaggio 1. SSH sullo switch che fungerà da autenticatore. Il nome utente e la password predefiniti sono cisco/cisco. Se il nome utente o la password sono stati modificati, immettere le nuove credenziali.

Nota: Per informazioni su come accedere a uno switch per PMI tramite SSH o Telnet, fare

clic su qui.

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#
```

Passaggio 2. In modalità di esecuzione privilegiata dello switch, accedere alla modalità di configurazione globale immettendo quanto segue:

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#configure
Authenticator(config)#
```

Passaggio 3. Per abilitare 802.1X a livello globale, usare il comando dot1x system-auth-control in modalità di configurazione globale.

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#configure
Authenticator(config)#dot1x system-auth-control
Authenticator(config)#
```

Passaggio 4. Utilizzare il comando **radius-server host** Global Configuration mode per configurare un host server RADIUS. I parametri sono definiti come segue:

- ip-address: specifica l'indirizzo IP dell'host del server RADIUS. L'indirizzo IP può essere un indirizzo IPv4, IPv6 o IPv6z.

- hostname — specifica il nome host del server RADIUS. È supportata solo la conversione in indirizzi IPv4. La lunghezza è compresa tra 1 e 158 caratteri e la lunghezza massima dell'etichetta di ciascuna parte del nome host è 63 caratteri.

- auth-port *auth-port-number* - Specifica il numero di porta per le richieste di autenticazione. Se il numero di porta è impostato su 0, l'host non viene utilizzato per l'autenticazione. L'intervallo è compreso tra 0 e 65535.

- Acc-port *acct-port-number* — Numero di porta per le richieste di accounting. L'host non viene utilizzato per l'accounting se impostato su 0. Se non specificato, il numero di porta predefinito è 1813.

- timeout *timeout*: per specificare il valore di timeout in secondi. Questo va da 1 a 30.

- retransmission *retries*: specifica il numero di retry di trasmissione. L'intervallo è compreso tra 1 e 15.

- deadtime *deadtime*: specifica il periodo di tempo in minuti durante il quale un server RADIUS viene ignorato dalle richieste di transazione. Varia da 0 a 2000.

- key *key-string*: specifica la chiave di autenticazione e crittografia per tutte le comunicazioni RADIUS tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere alla crittografia utilizzata nel daemon RADIUS. Per specificare una stringa vuota, immettere "". La lunghezza può essere compresa tra 0 e 128 caratteri. Se questo parametro viene omesso, verrà utilizzata la chiave radius configurata globalmente.

- key *encrypted-key-string*: uguale a key-string, ma la chiave è in formato crittografato.

- priority *priority*: specifica l'ordine di utilizzo dei server, dove 0 ha la priorità più alta. L'intervallo di priorità è compreso tra 0 e 65535.

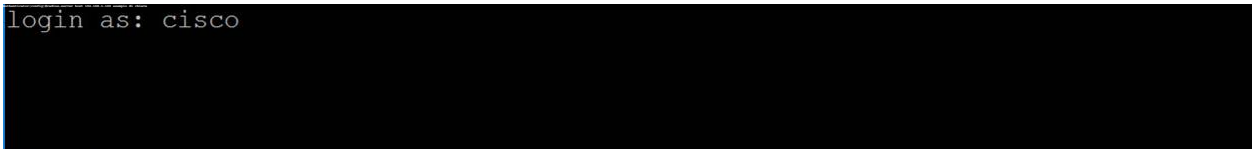
- Sintassi {login|dot1.x|all}: specifica il tipo di utilizzo del server RADIUS. I valori possibili sono:

    - login - Specifica che il server RADIUS viene utilizzato per l'autenticazione dei parametri di login utente.

    - dot1.x: specifica che il server RADIUS viene utilizzato per l'autenticazione della porta 802.1x.

    - all: specifica che il server RADIUS viene utilizzato per l'autenticazione dell'accesso utente e per l'autenticazione della porta 802.1x.

Nell'esempio vengono utilizzati solo i parametri host e key. L'indirizzo IP **192.168.1.100** verrà utilizzato come indirizzo IP del server RADIUS e la parola **example** come stringa di chiave.

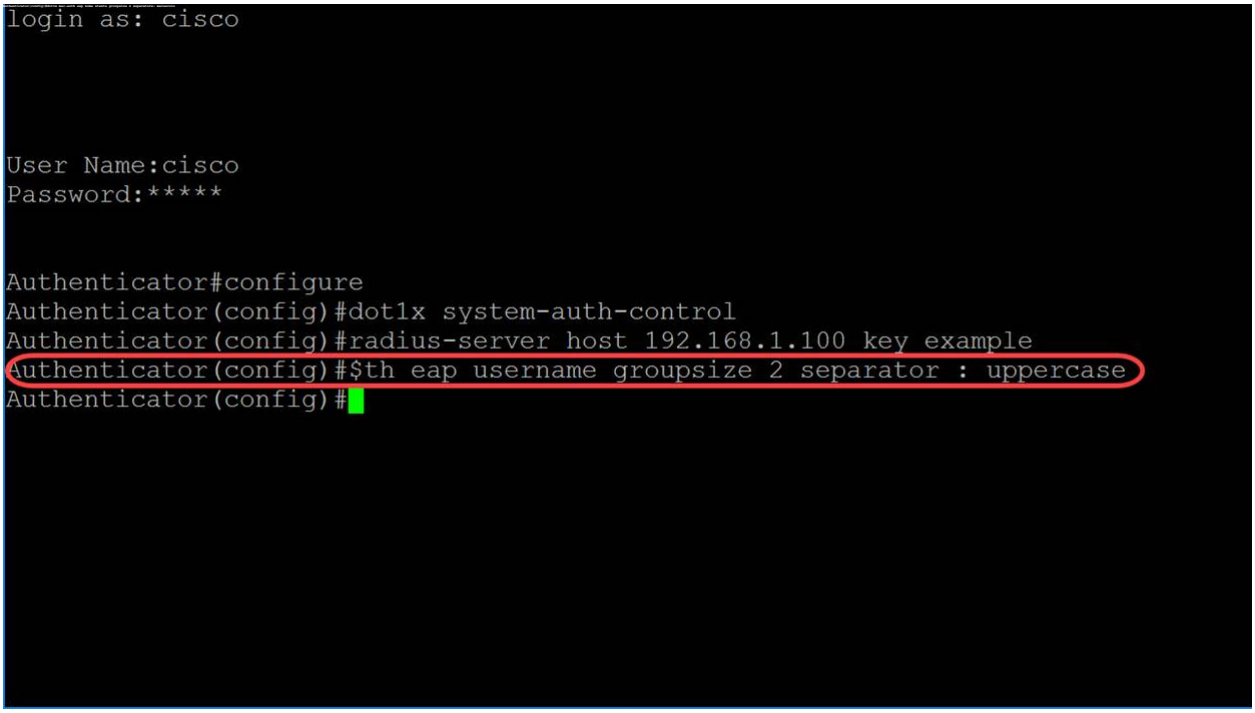


Passaggio 5. Nell'autenticazione basata su MAC, il nome utente del supplicant si basa sull'indirizzo MAC del dispositivo supplicant. Di seguito viene descritto il formato del nome utente basato su MAC, inviato dallo switch al server RADIUS, come parte del processo di autenticazione. I campi seguenti sono definiti come:

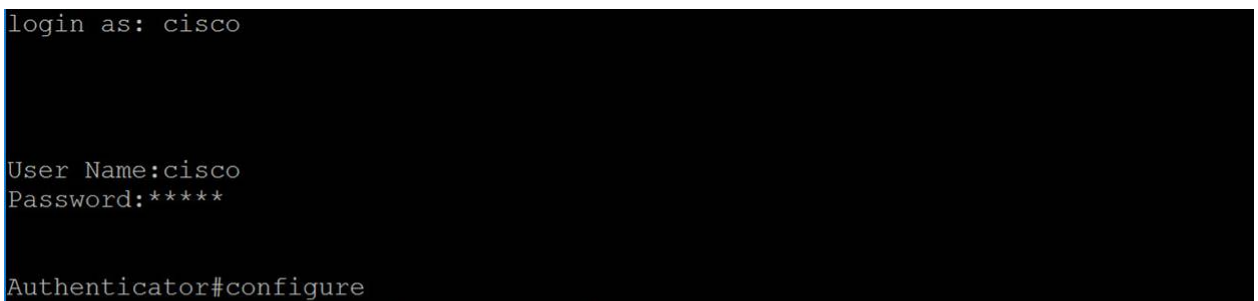
- tipo mac-auth: scegliere un tipo di autenticazione MAC
    - eap: utilizzare RADIUS con incapsulamento EAP per il traffico tra lo switch (client RADIUS) e il server RADIUS, che autentica un supplicant basato su MAC.
    - radius: utilizzare RADIUS senza incapsulamento EAP per il traffico tra lo switch (client RADIUS) e il server RADIUS, che autentica un supplicant basato su MAC.
- groupsize: numero di caratteri ASCII tra delimitatori dell'indirizzo MAC inviato come nome utente. Le opzioni disponibili sono 1, 2, 4 o 12 caratteri ASCII tra i delimitatori.
- separatore — carattere utilizzato come delimitatore tra i gruppi definiti di caratteri nell'indirizzo MAC. Le opzioni disponibili sono trattino, due punti o punto come delimitatore.
- case: invia il nome utente in lettere minuscole o maiuscole. Le opzioni sono minuscole o maiuscole.

dot1x mac-auth

In questo esempio verrà utilizzato **eap** come tipo di autenticazione mac, con dimensione di gruppo pari a **2**, i **due punti** come separatore e il nome utente in **lettere maiuscole**.

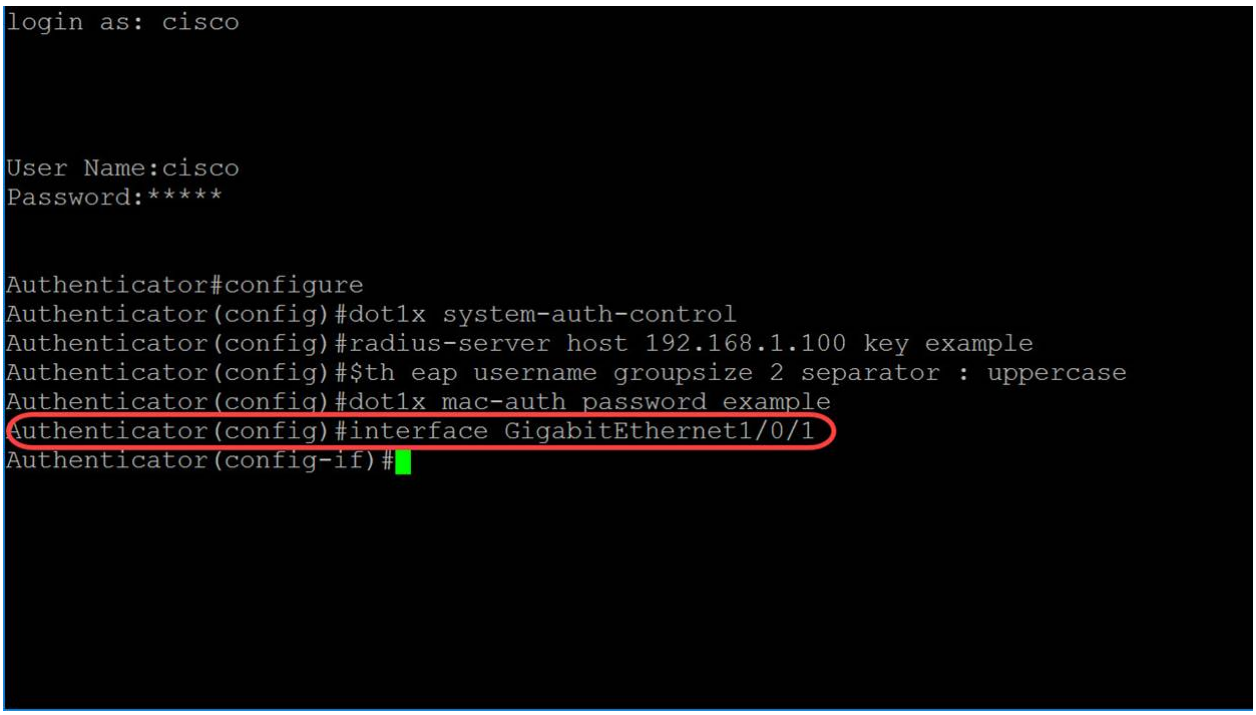


Passaggio 6. Utilizzare il comando seguente per definire la password che lo switch utilizzerà per l'autenticazione basata su MAC anziché l'indirizzo MAC dell'host. Utilizzeremo la parola **esempio** come password.



Passaggio 7. Per accedere alla modalità di configurazione interfaccia e configurare un'interfaccia, usare il comando **interface** Global Configuration mode. Verrà eseguita la configurazione di Gigabit Ethernet1/0/1 perché l'host finale è collegato.

Nota: Non configurare la porta connessa al server RADIUS.



Nota: Per configurare più porte contemporaneamente, utilizzare il comando interface range.

Vedere l'esempio seguente per configurare le porte da 1 a 4 con il comando range:

Passaggio 8. Per consentire un singolo host (client) o più host su una porta autorizzata IEEE802.1X, usare il comando **dot1x host-mode** in modalità di configurazione interfaccia. I parametri sono definiti come segue:

- multi-host — Abilita la modalità multi-host
    - Una porta è autorizzata se esiste almeno un client autorizzato.
    - Quando una porta non è autorizzata e una VLAN guest è abilitata, il traffico senza tag viene mappato nuovamente sulla VLAN guest. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN guest o a una VLAN non autenticata. Se la VLAN guest non è abilitata su una porta, viene eseguito il bridging solo del traffico con tag appartenente alle VLAN non autenticate.
    - Quando una porta è autorizzata, il traffico senza tag e con tag da tutti gli host connessi alla porta viene sottoposto a bridging in base alla configurazione della porta di appartenenza della VLAN statica.
    - È possibile specificare che il traffico senza tag proveniente dalla porta autorizzata venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o a VLAN non autenticate. L'assegnazione di VLAN Radius su una porta è impostata nella pagina *Port Authentication* (Autenticazione porta).

- host singolo: attivazione della modalità host singolo

    - Una porta è autorizzata se esiste un client autorizzato. Su una porta è possibile autorizzare un solo host.

    - Quando una porta non è autorizzata e la VLAN guest è abilitata, il traffico senza tag viene mappato nuovamente sulla VLAN guest. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN guest o a una VLAN non autenticata. Se una VLAN guest non è abilitata sulla porta, viene eseguito il bridging solo del traffico con tag appartenente alle VLAN non autenticate.

    - Quando una porta è autorizzata, il traffico non contrassegnato e contrassegnato proveniente dall'host autorizzato viene bloccato in base alla configurazione della porta di appartenenza della VLAN statica. Il traffico proveniente da altri host viene scartato.

    - Un utente può specificare che il traffico senza tag proveniente dall'host autorizzato venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico contrassegnato viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o alle VLAN non autenticate. L'assegnazione di VLAN Radius su una porta è impostata nella pagina *Port Authentication* (Autenticazione porta).

- multisessione - Abilita modalità sessioni multiple

    - A differenza delle modalità host singolo e host multiplo, le porte in modalità multisessione non hanno uno stato di autenticazione. Questo stato viene assegnato a ciascun client connesso alla porta.

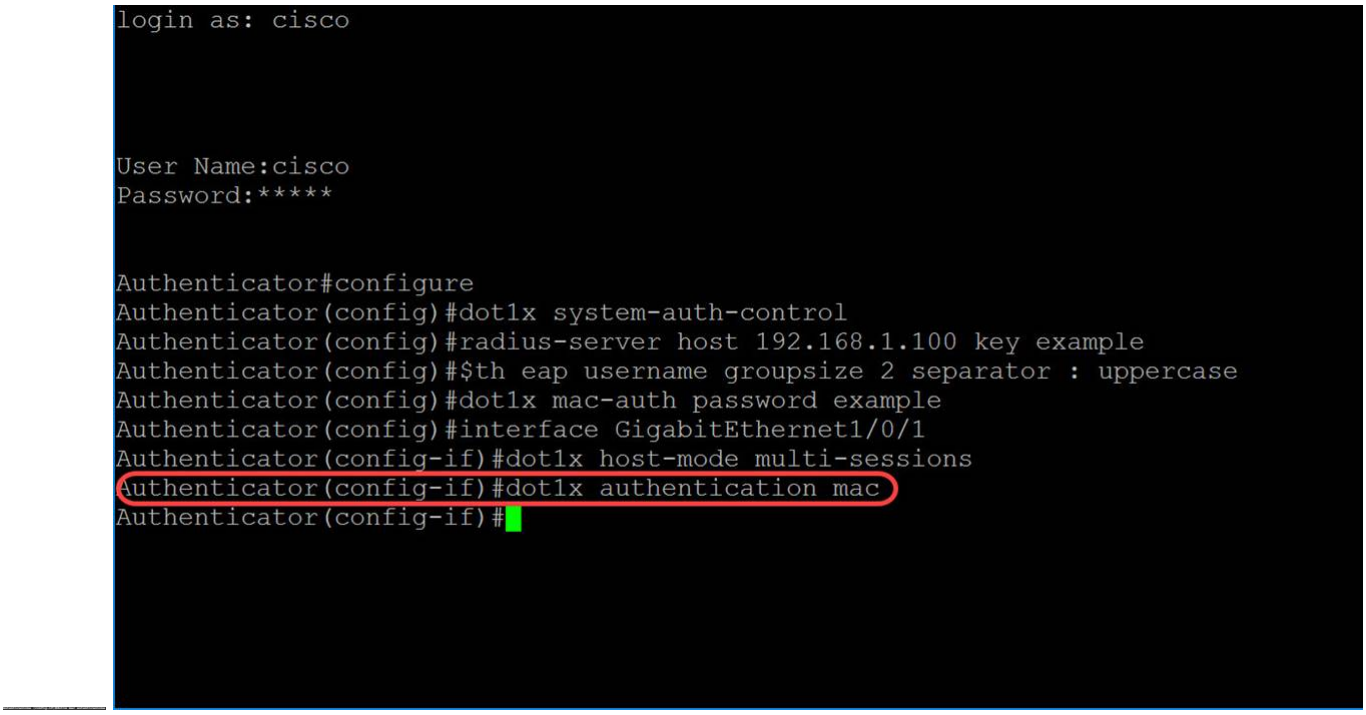
    - Il traffico contrassegnato appartenente a una VLAN non autenticata viene sempre indirizzato, indipendentemente dal fatto che l'host sia autorizzato o meno.

    - Il traffico contrassegnato e non contrassegnato proveniente da host non autorizzati che non appartengono a una VLAN non autenticata viene mappato nuovamente alla VLAN guest se è definita e abilitata sulla VLAN, oppure viene scartato se la VLAN guest non è abilitata sulla porta.

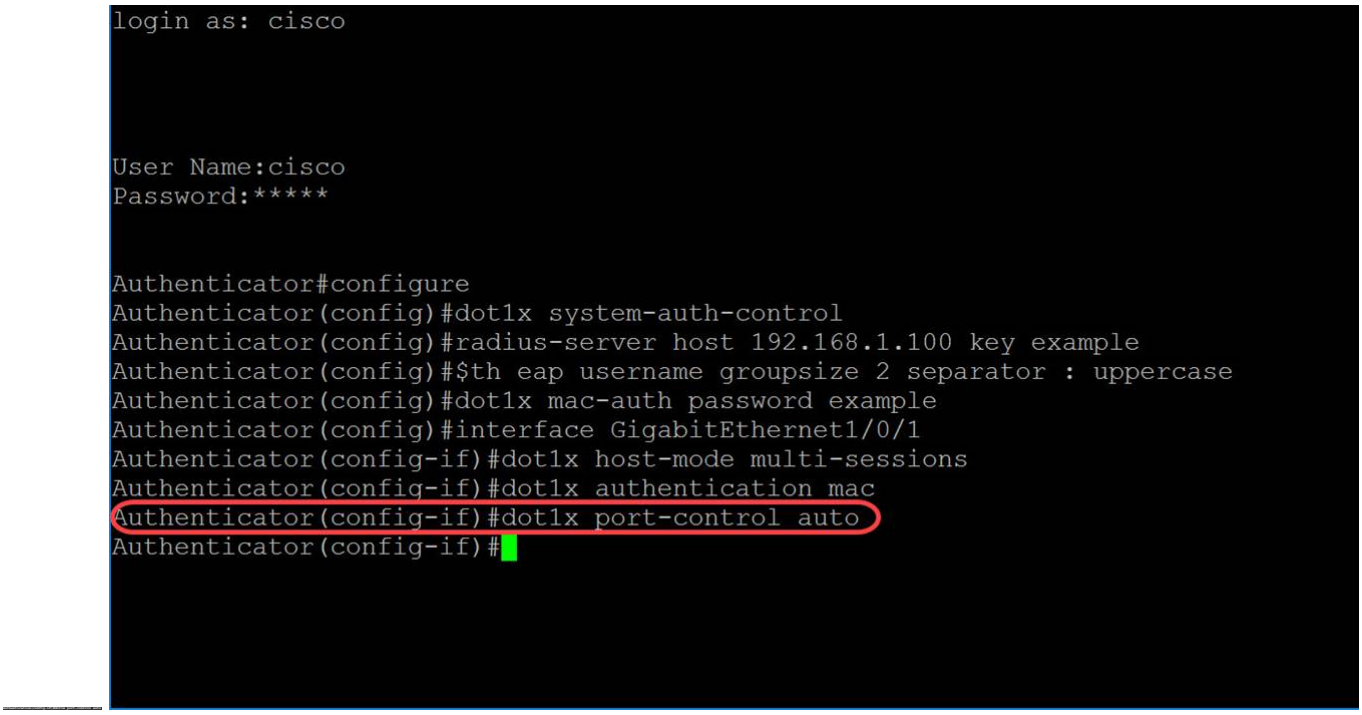
    - È possibile specificare che il traffico senza tag proveniente dalla porta autorizzata venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o a VLAN non autenticate. L'assegnazione di VLAN Radius a una porta è impostata nella pagina *Port Authentication*.

In questo esempio, la modalità host verrà configurata come multisessione.

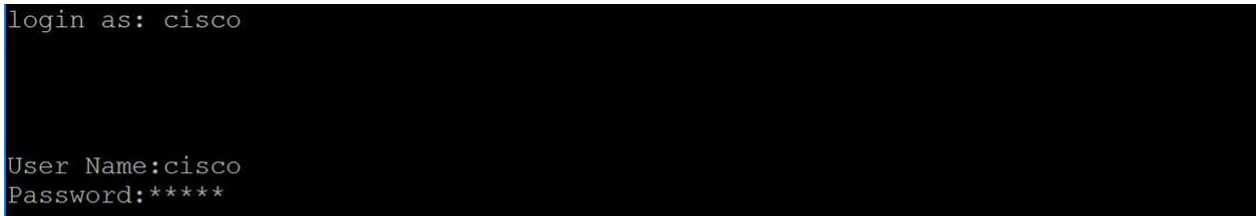
Passaggio 9. Per configurare il metodo di autenticazione su una porta, utilizzare il comando seguente per abilitare l'autenticazione basata su MAC.



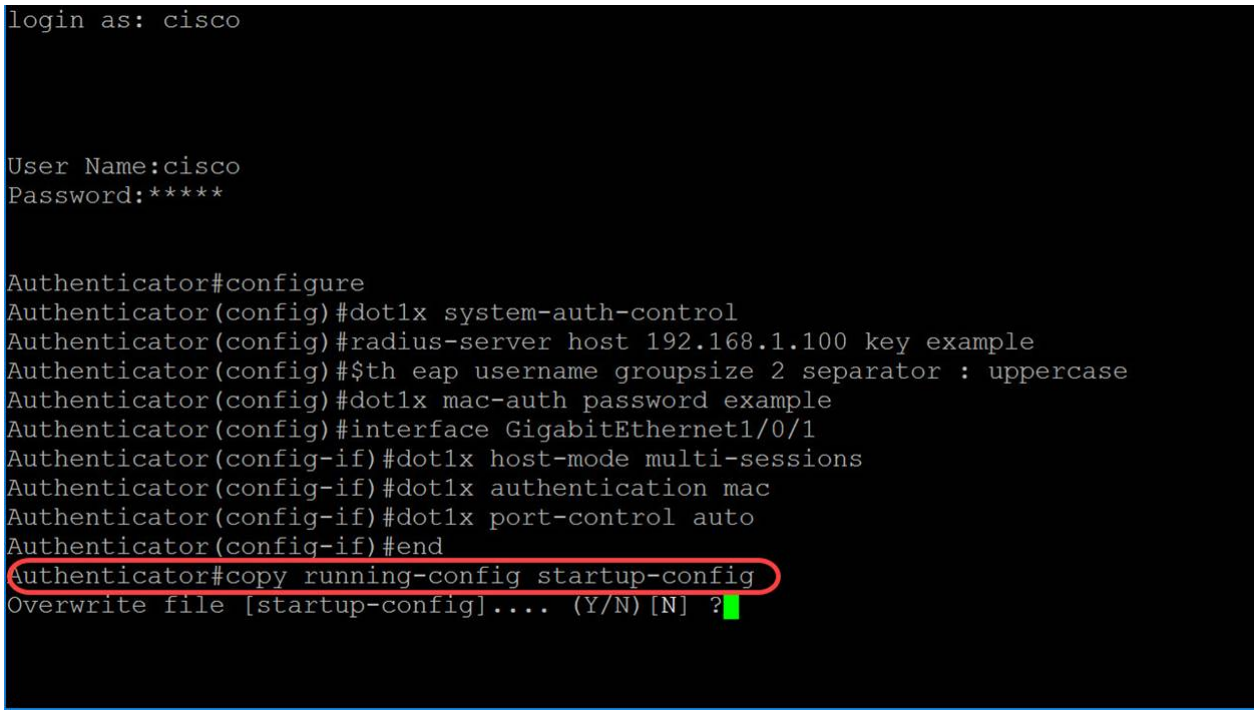
Passaggio 10. Per abilitare l'autenticazione e l'autorizzazione basate sulle porte sul dispositivo, usare il comando **port-control** per configurare il valore di controllo della porta. Lo stato di autorizzazione della porta amministrativa verrà selezionato come **auto**. In questo modo sarà possibile abilitare l'autenticazione e l'autorizzazione basate sulle porte sul dispositivo. L'interfaccia si sposta tra uno stato autorizzato e uno non autorizzato in base allo scambio di autenticazione tra il dispositivo e il client.



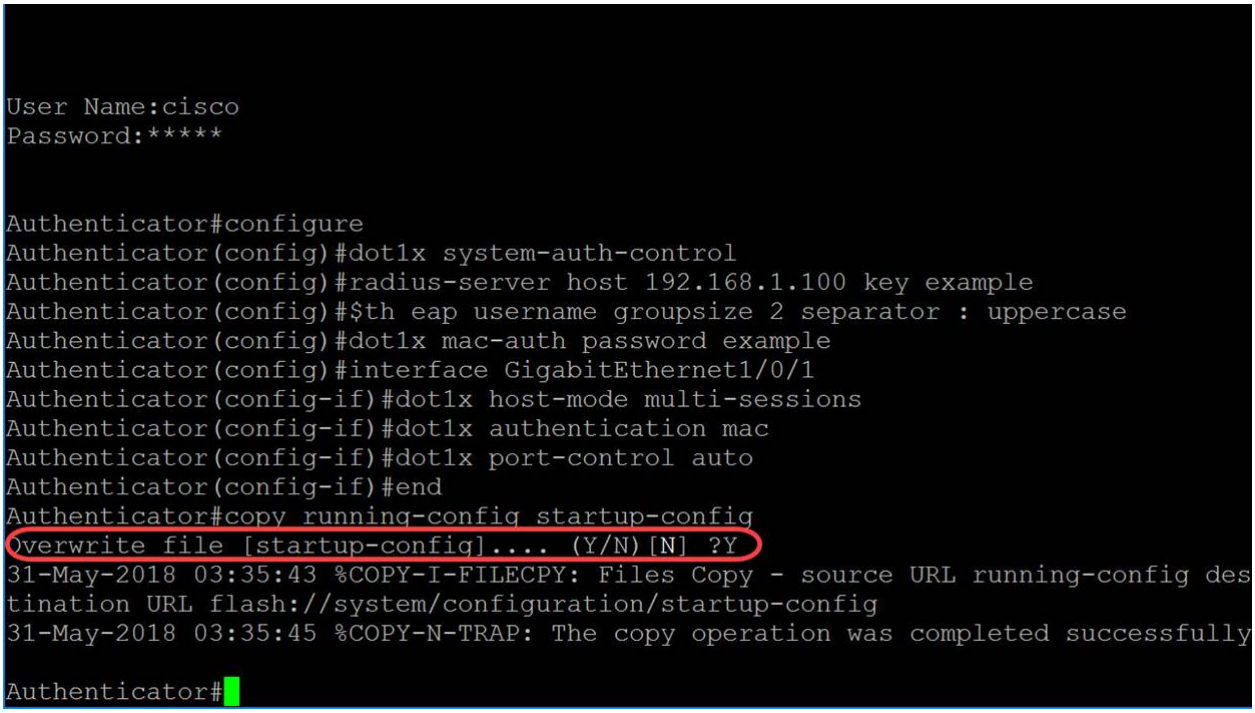
Passaggio 11. (Facoltativo) Per terminare la sessione di configurazione corrente e tornare in modalità di esecuzione privilegiata, utilizzare il comando **end**.



Passaggio 12. (Facoltativo) Per copiare un file da un'origine a una destinazione, utilizzare il comando **copy** in modalità di esecuzione privilegiata. Nell'esempio, la configurazione in esecuzione viene salvata nella configurazione di avvio.



Passaggio 13. (Facoltativo) Viene visualizzato un messaggio in cui si chiede se si desidera sovrascrivere il file della configurazione di avvio. Digitare **Y** per yes o **N** per no. Verrà digitato **Y** per sovrascrivere il file di configurazione di avvio.



Conclusioni

A questo punto, è necessario configurare l'autenticazione basata sull'indirizzo MAC sullo switch con la CLI. Per verificare che l'autenticazione basata su MAC funzioni correttamente, procedere come segue.

Passaggio 1. Per visualizzare gli utenti autorizzati 802.1X attivi per il dispositivo, usare il

comando **show dot1x users** in modalità di esecuzione privilegiata.

```
Authenticator#configure
Authenticator(config)#dot1x system-auth-control
Authenticator(config)#radius-server host 192.168.1.100 key example
Authenticator(config)#$th eap username groupsize 2 separator : uppercase
Authenticator(config)#dot1x mac-auth password example
Authenticator(config)#interface GigabitEthernet1/0/1
Authenticator(config-if)#dot1x host-mode multi-sessions
Authenticator(config-if)#dot1x authentication mac
Authenticator(config-if)#dot1x port-control auto
Authenticator(config-if)#end
Authenticator#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
31-May-2018 03:35:43 %COPY-I-FILECPY: Files Copy - source URL running-config des
tination URL flash://system/configuration/startup-config
31-May-2018 03:35:45 %COPY-N-TRAP: The copy operation was completed successfully

Authenticator#show dot1x users

                          MAC               Auth    Auth    Session        VLAN
Port     Username         Address           Method  Server  Time
-------- ---------------- ----------------- ------  ------  -------------- ----
gi1/0/1  54:EE:75:[illegible] 54:ee:75:[illegible] MAC     Remote  00:01:45

Authenticator#
```

Passaggio 2. Per visualizzare le interfacce 802.1X o lo stato dell'interfaccia specificato, usare il comando **show dot1x** in modalità di esecuzione privilegiata.

```
Authenticator#show dot1x interface GigabitEthernet1/0/1

Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius
MAC-Based Authentication:
  Type: Eap
  Username Groupsize: 2
  Username Separator: :
  Username case: Uppercase
  Password: MD5 checksum 1a79a4d60de6718e8e5b326e338ae533
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled
Supplicant Global Configuration:
Supplicant Authentication success traps are disabled
Supplicant Authentication failure traps are disabled

gi1/0/1
 Authenticator is enabled
 Supplicant is disabled
 Authenticator Configuration:
 Host mode: multi-sessions
 Authentication methods: mac
 Port Administrated Status: auto
 Guest VLAN: disabled
 VLAN Radius Attribute: disabled
 Open access: disabled
 Server timeout: 30 sec
 Maximum Hosts: unlimited
 Maximum Login Attempts: 0
 Reauthentication is disabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 1
 Authentication fails: 0
 Number of Authorized Hosts: 1
```