Configurazione delle proprietà globali 802.1x su uno switch dalla CLI

Introduzione

IEEE 802.1x è uno standard che facilita il controllo dell'accesso tra un client e un server. Prima che i servizi possano essere forniti a un client da una rete LAN o da uno switch, il client connesso alla porta dello switch deve essere autenticato dal server di autenticazione che esegue RADIUS (Remote Authentication Dial-In User Service).

L'autenticazione 802.1x impedisce ai client non autorizzati di connettersi a una rete LAN tramite porte accessibili pubblicamente. L'autenticazione 802.1x è un modello client-server. In questo modello, i dispositivi di rete hanno i seguenti ruoli specifici:

- Client o supplicant: un client o un supplicant è un dispositivo di rete che richiede l'accesso alla LAN. Il client è connesso a un autenticatore.
- Autenticatore: un autenticatore è un dispositivo di rete che fornisce servizi di rete e al quale sono collegate le porte supplicant. Sono supportati i seguenti metodi di autenticazione:

  - Basato su 802.1x: supportato in tutte le modalità di autenticazione. Nell'autenticazione basata su 802.1x, l'autenticatore estrae i messaggi EAP (Extensible Authentication Protocol) dai messaggi 802.1x o dai pacchetti EAPoL (EAP over LAN) e li passa al server di autenticazione, utilizzando il protocollo RADIUS.

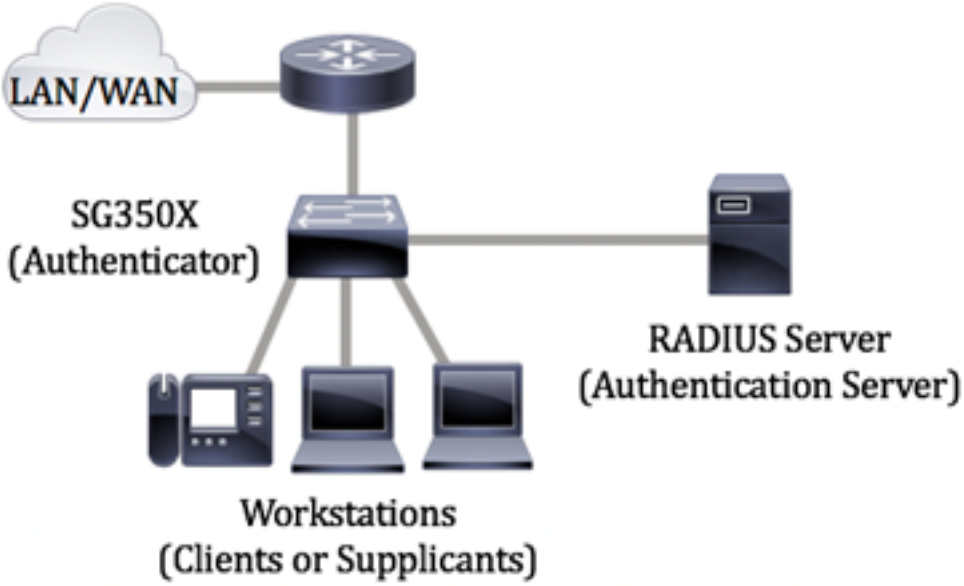
  - Basato su MAC: supportato in tutte le modalità di autenticazione. Con il Media Access Control (MAC), l'autenticatore esegue la parte client EAP del software per conto dei client che richiedono l'accesso alla rete.

  - Basato su Web: supportato solo in modalità multisessione. Con l'autenticazione basata sul Web, l'autenticatore stesso esegue la parte client EAP del software per conto dei client che richiedono l'accesso alla rete.

- Server di autenticazione: un server di autenticazione esegue l'autenticazione effettiva del client. Il server di autenticazione per il dispositivo è un server di autenticazione RADIUS con estensioni EAP.

  Nota: Un dispositivo di rete può essere un client o un supplicant, un autenticatore o entrambi per porta.

  L'immagine seguente mostra una rete che ha configurato i dispositivi in base ai ruoli specifici. Nell'esempio viene usato uno switch SG350X.



Linee guida in configurazione di 802.1x:

1. Configurare il server RADIUS. per informazioni su come configurare le impostazioni del server RADIUS sullo switch, fare clic qui.
2. Configurare le VLAN (Virtual Local Area Network). Per creare le VLAN con l'utility basata sul Web dello switch, fare clic qui. Per le istruzioni basate sulla CLI, fare clic qui.
3. Configurare le impostazioni della porta sulla VLAN sullo switch. Per eseguire la configurazione utilizzando l'utility basata sul Web, fare clic qui. Per utilizzare la CLI, fare clic qui.
4. Configurare le proprietà globali 802.1x sullo switch. Per istruzioni su come configurare le proprietà globali 802.1x con l'utility basata sul Web dello switch, fare clic qui.
5. (Facoltativo) Configurare l'intervallo di tempo sullo switch. per informazioni su come configurare le impostazioni dell'intervallo di tempo sullo switch, fare clic qui.
6. Configurare l'autenticazione della porta 802.1x. Per usare l'utility basata sul Web dello switch, fare clic qui.

Obiettivo

In questo documento viene spiegato come configurare le proprietà globali 802.1x dall'interfaccia della riga di comando (CLI) dello switch, incluse le proprietà Authentication e Guest VLAN. La VLAN guest consente di accedere a servizi che non richiedono l'autenticazione e l'autorizzazione delle porte o dei dispositivi in abbonamento tramite l'autenticazione 802.1x, basata su MAC o basata sul Web.

Dispositivi interessati

- Serie Sx300
- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

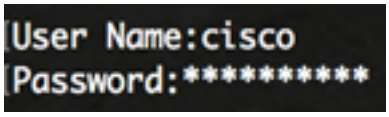
Versione del software

- 1.4.7.06 — Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Configurazione delle proprietà 802.1x su uno switch dalla CLI

Configura impostazioni 802.1x

Passaggio 1. Accedere alla console dello switch. Il nome utente e la password predefiniti sono cisco/cisco. Se sono stati configurati un nuovo nome utente o password, immettere queste credenziali.



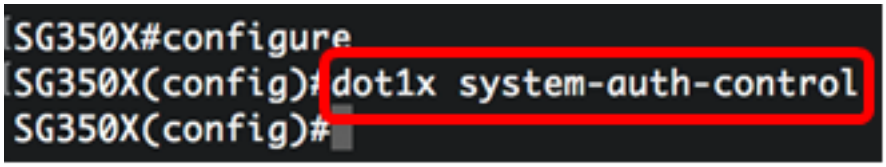
Nota: i comandi possono variare a seconda del modello di switch in uso. Nell'esempio, è possibile accedere allo switch SG350X in modalità Telnet.

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

```
SG350x#configure
```

Passaggio 3. Per abilitare l'autenticazione 802.1x a livello globale sullo switch, usare il comando **dot1x system-auth-control** in modalità di configurazione globale.

```
SG350x(config)#dotx1 system-auth-control
```



Passaggio 4. (Facoltativo) Per disabilitare l'autenticazione 802.1x a livello globale sullo switch, immettere quanto segue:

```
SG350x(config)#no dotx1 system-auth-control
```

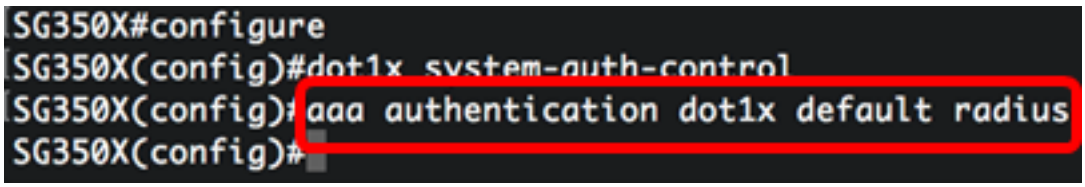
Nota: Se questa opzione è disabilitata, le autenticazioni 802.1X, basate su MAC e basate sul Web sono disabilitate.

Passaggio 5. Per specificare i server da utilizzare per l'autenticazione quando è abilitata l'autenticazione 802.1x, immettere quanto segue:

```
SG350x(config)#aaa authentication dot1x default [radius none | raggio | none]
```

Le opzioni sono:

- radius none: esegue l'autenticazione della porta innanzitutto con l'aiuto del server RADIUS. Se il server non risponde, ad esempio quando è inattivo, non viene eseguita alcuna autenticazione e la sessione è consentita. Se il server è disponibile e le credenziali utente non sono corrette, l'accesso viene negato e la sessione viene terminata.
- radius: esegue l'autenticazione della porta in base al server RADIUS. Se non viene eseguita alcuna autenticazione, la sessione viene terminata. Questa è l'autenticazione predefinita.
- none: non autentica l'utente e consente la sessione.



Nota: In questo esempio, il server di autenticazione 802.1x predefinito è RADIUS.

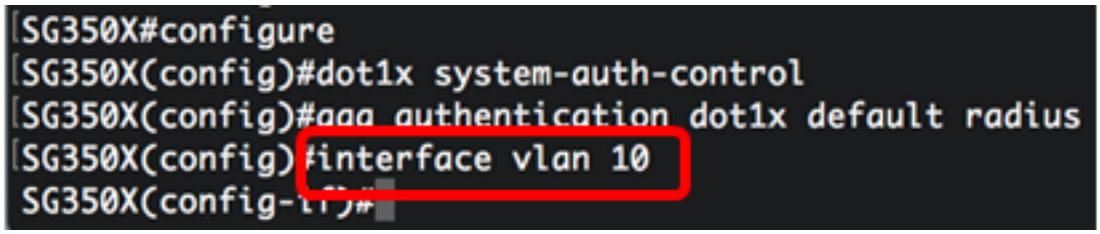
Passaggio 6. (Facoltativo) Per ripristinare l'autenticazione predefinita, immettere quanto segue:

```
SG350X(config)#no aaa authentication dot1x default
```

Passaggio 7. In modalità di configurazione globale, accedere al contesto di configurazione dell'interfaccia VLAN immettendo quanto segue:

```
SG350X(config)#interface vlan [vlan-id]
```

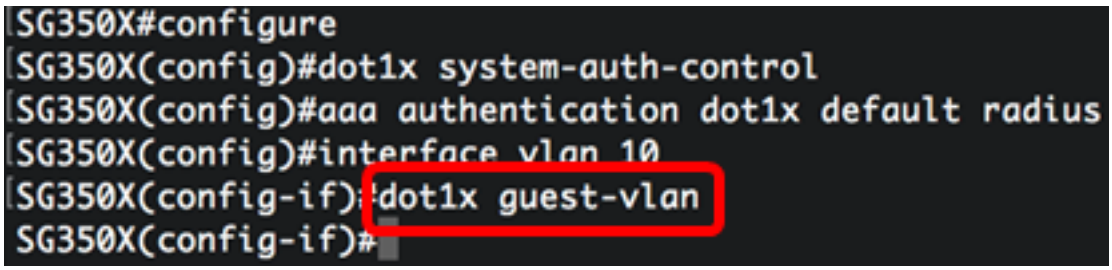
- vlan-id: per specificare un ID VLAN da configurare.



Passaggio 8. Per abilitare l'uso di una VLAN guest per le porte non autorizzate, immettere quanto segue:

```
SG350X (config-if)#dot1x guest-vlan
```

Nota: Se è abilitata una VLAN guest, tutte le porte non autorizzate si uniscono automaticamente alla VLAN scelta nella VLAN guest. Se una porta viene successivamente autorizzata, viene rimossa dalla VLAN guest.



Passaggio 9. Per uscire dal contesto di configurazione interfaccia, immettere quanto segue:

```
SG350X (Config-if) #exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#
```

Passaggio 10. Per impostare il ritardo tra l'abilitazione di 802.1X (o porta attiva) e l'aggiunta di una porta alla VLAN guest, immettere quanto segue:

```
SG350X(config)#dot1x timeout guest-vlan [timeout]
```

- timeout: per specificare il ritardo in secondi tra l'abilitazione di 802.1X (o porta attiva) e l'aggiunta della porta alla VLAN guest. L'intervallo va da 30 a 180 secondi.

Nota: Dopo il collegamento, se il software non rileva un supplicant 802.1x o l'autenticazione della porta non è riuscita, la porta viene aggiunta alla VLAN guest solo dopo la scadenza del periodo di timeout della VLAN guest. Se la porta viene modificata da Autorizzata a Non autorizzata, viene aggiunta alla VLAN guest solo dopo la scadenza del periodo di timeout della VLAN guest. L'autenticazione VLAN può essere abilitata o disabilitata dall'autenticazione VLAN.

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#
```

Nota: Nell'esempio, il timeout della VLAN guest usato è 60 secondi.

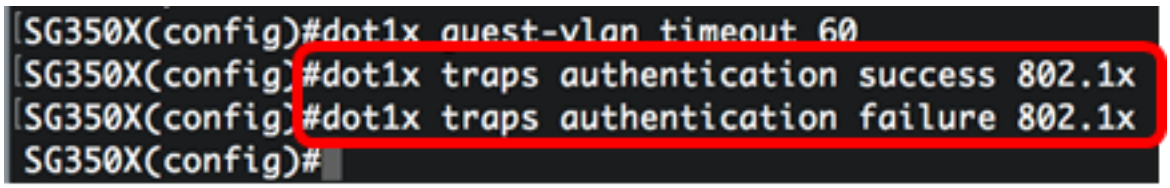
Passaggio 11. Per abilitare le trap, selezionare una o più delle opzioni seguenti:

```
SG350X(config)# dot1x traps authentication [errore | operazione riuscita | quiet] [802.1x | mac | Web]
```

Le opzioni sono:

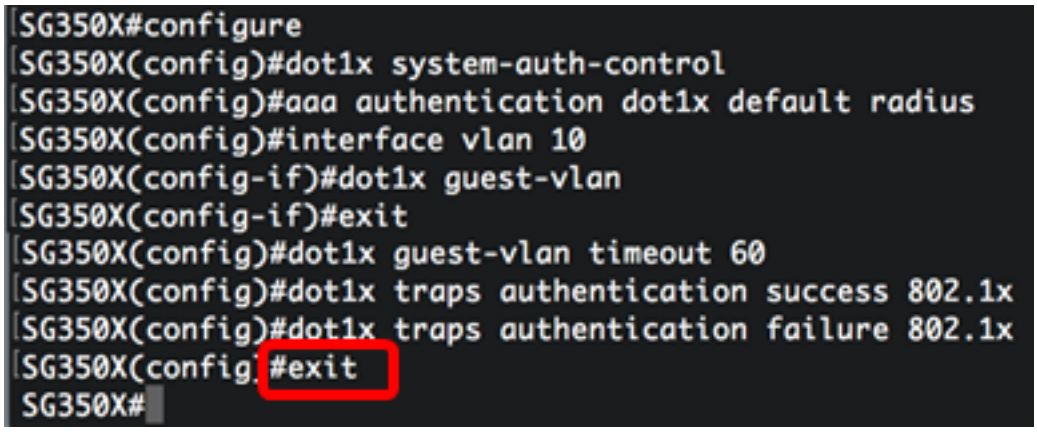
- Trap errori autenticazione 802.1x: invio di trap se l'autenticazione 802.1x non riesce.
- Trap per l'autenticazione 802.1x: invio di trap se l'autenticazione 802.1x ha esito positivo.
- trap errore autenticazione mac: invio di trap se l'autenticazione MAC non riesce.
- trapping per autenticazione mac riuscita: invio di trap se l'autenticazione MAC ha esito positivo.
- intercettazioni degli errori di autenticazione Web: invio di trap in caso di errore dell'autenticazione Web.
- intercettazioni di riuscita dell'autenticazione Web: invio di trap in caso di esito positivo dell'autenticazione Web.
- Trap silenziose per l'autenticazione Web: invio di trap se inizia un periodo di silenzio.

Nota: nell'esempio vengono immesse le trap per errori e operazioni riuscite dell'autenticazione 802.1x.



Passaggio 12. Per uscire dal contesto di configurazione interfaccia, immettere quanto segue:

```
SG350X(config)#exit
```



Passaggio 13. (Facoltativo) Per visualizzare le proprietà globali 802.1x configurate sullo switch, immettere quanto segue:

```
SG350X#show dot1x
```

A questo punto, è necessario configurare correttamente le proprietà 802.1x sullo switch.

Configurazione dell'autenticazione VLAN

Quando lo standard 802.1x è abilitato, le porte o i dispositivi non autorizzati non sono autorizzati ad accedere alla VLAN a meno che non facciano parte della VLAN guest o non siano autenticati. Le porte devono essere aggiunte manualmente alle VLAN.

Per disabilitare l'autenticazione su una VLAN, attenersi alla seguente procedura:

Passaggio 1. In modalità di esecuzione privilegiata dello switch, accedere alla modalità di configurazione globale immettendo quanto segue:

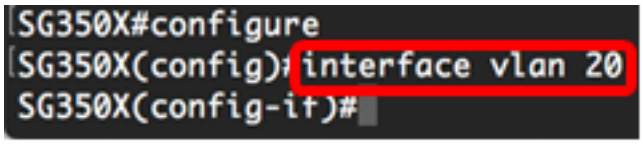
```
SG350X#configure
```

Passaggio 2. In modalità di configurazione globale, accedere al contesto di configurazione

dell'interfaccia VLAN immettendo quanto segue:

```
KSG350x(config)# interface vlan [vlan-id]
```

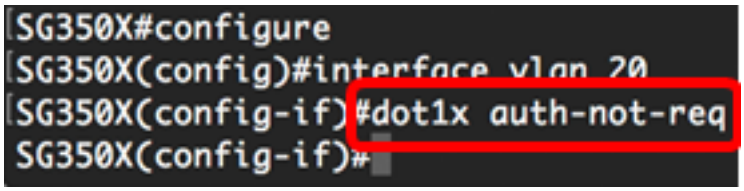
- vlan-id: per specificare un ID VLAN da configurare.



Nota: nell'esempio viene scelta la VLAN 20.

Passaggio 3. Per disabilitare l'autenticazione 802.1x sulla VLAN, immettere quanto segue:

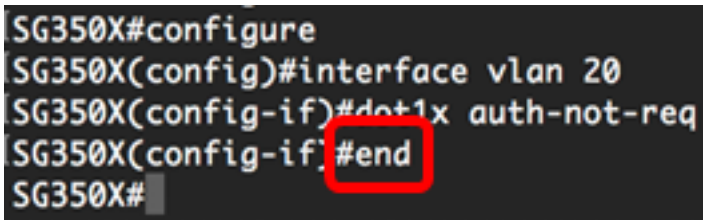
SG350X (config-if)#dot1x auth-not-req



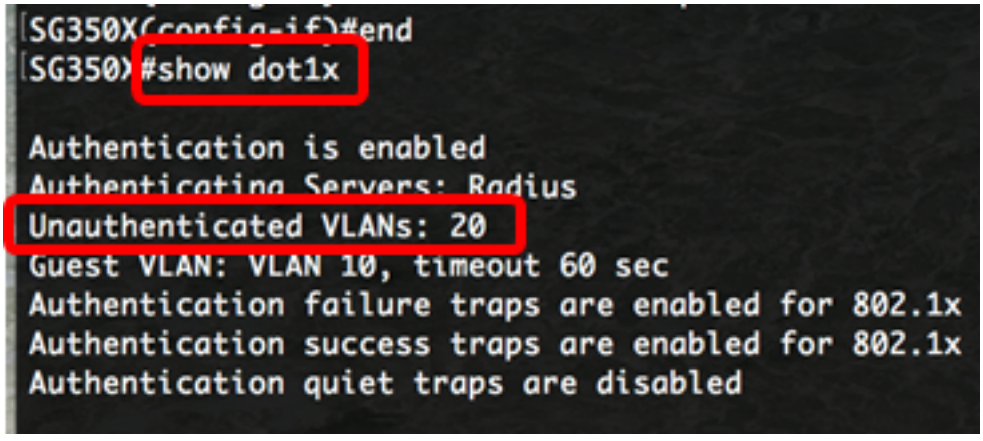
Passaggio 4. (Facoltativo) Per abilitare l'autenticazione 802.1x sulla VLAN, immettere quanto segue:

SG350X (config-if)#no dot1x auth-not-req

Passaggio 5. Per uscire dal contesto di configurazione interfaccia, immettere quanto segue:



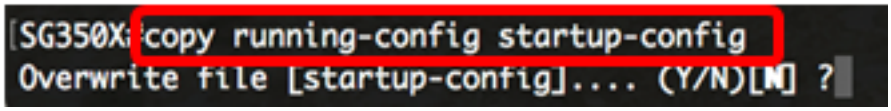
Passaggio 6. (Facoltativo) Per visualizzare le impostazioni di autenticazione globale 802.1x sullo switch, immettere quanto segue:



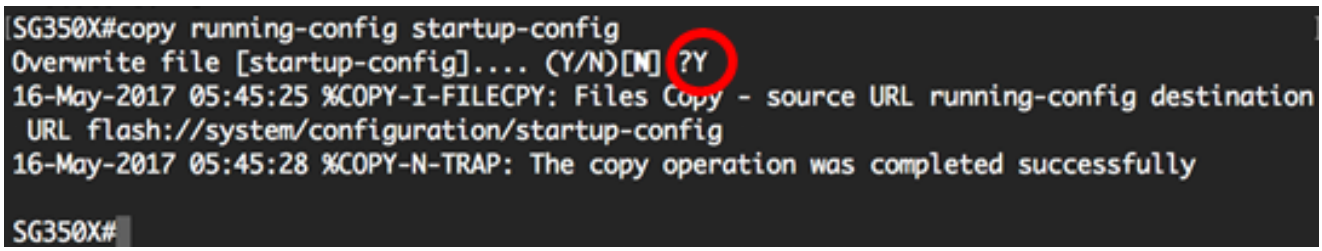
Nota: Nell'esempio, la VLAN 20 è mostrata come VLAN non autenticata.

Passaggio 7. (Facoltativo) In modalità di esecuzione privilegiata dello switch, salvare le impostazioni configurate nel file della configurazione di avvio, immettendo quanto segue:

```
SG350X#copy running-config startup-config
```



Passaggio 8. (Facoltativo) Premere **Y** per Sì o **N** per No sulla tastiera quando compare il prompt Overwrite file [startup-config]… (Sovrascrivi file [startup-config]).



A questo punto, le impostazioni di autenticazione 802.1x sulle VLAN dello switch sono state configurate correttamente.

Importante: per continuare a configurare le impostazioni di autenticazione della porta 802.1x sullo switch, attenersi alle linee guida menzionate sopra.