

Configurazione dell'autenticazione della porta 802.1X sugli Smart Switch Cisco serie Sx220

Obiettivo

L'obiettivo di questo articolo è quello di mostrare come configurare l'autenticazione delle porte sugli smart switch serie Sx220.

L'autenticazione porta 802.1X consente la configurazione dei parametri 802.1X per ciascuna porta del dispositivo. Una porta che richiede l'autenticazione viene chiamata supplicant. L'autenticatore è uno switch o un punto di accesso che funge da protezione di rete per i supplicant. L'autenticatore inoltra i messaggi di autenticazione al server RADIUS in modo che una porta possa essere autenticata e possa inviare e ricevere informazioni.

Dispositivi interessati

- Serie Sx220

Versione del software

- 1.1.0.14

Configura autenticazione porta

Passaggio 1. Accedere all'utility basata sul Web dello switch e selezionare Security > 802.1X > Port Authentication (Sicurezza > 802.1X > Autenticazione porta).

▶ IP Configuration

▼ Security

TACACS+

RADIUS

▶ Management Access Method

Password Strength

Management Access Authentication

TCP/UDP Services

Storm Control

Port Security

▼ 802.1X

Properties

Port Authentication

Host and Session Authentication

Authenticated Hosts

▶ Denial of Service

Passaggio 2. Fare clic sul pulsante di opzione relativo alla porta che si desidera configurare, quindi fare clic su Modifica.

| | | | | | | | |
|----------------------------------|----|------|-----|----------|----------|----------|---------|
| <input type="radio"/> | 3 | GE3 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input checked="" type="radio"/> | 4 | GE4 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 5 | GE5 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 6 | GE6 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 7 | GE7 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 8 | GE8 | N/A | Auto | Disabled | Enabled | Enabled |
| <input type="radio"/> | 9 | GE9 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 10 | GE10 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 11 | GE11 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 12 | GE12 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 13 | GE13 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 14 | GE14 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 15 | GE15 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 16 | GE16 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 17 | GE17 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 18 | GE18 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 19 | GE19 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 20 | GE20 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 21 | GE21 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 22 | GE22 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 23 | GE23 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 24 | GE24 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 25 | GE25 | N/A | Disabled | Disabled | Disabled | Enabled |
| <input type="radio"/> | 26 | GE26 | N/A | Disabled | Disabled | Disabled | Enabled |

Copy Settings... Edit...

Nota: nell'esempio, è stata scelta la porta GE4.

Passaggio 3. Viene visualizzata la finestra Modifica autenticazione porta. Dall'elenco a discesa Interface (Interfaccia), verificare che la porta specificata sia quella scelta nel passaggio 2. In caso contrario, fare clic sulla freccia dell'elenco a discesa e scegliere la porta destra.

Interface: Port GE4 ▼

Administrative Port Control: Disabled
 Force Unauthorized
 Auto
 Force Authorized

RADIUS VLAN Assignment: Disabled
 Reject
 Static

Guest VLAN: Enable

Passaggio 4. Scegliere un pulsante di opzione per il controllo della porta amministrativa. Questo determinerà lo stato di autorizzazione della porta. Le opzioni sono:

- Disabilitato: disabilita 802.1X. Si tratta dello stato predefinito.
- Force Unauthorized - Nega l'accesso all'interfaccia attivando lo stato non autorizzato sull'interfaccia stessa. Lo switch non fornisce servizi di autenticazione al client tramite l'interfaccia.
- Auto: attiva l'autenticazione e l'autorizzazione basate sulle porte sullo switch. L'interfaccia viene spostata tra uno stato autorizzato e uno non autorizzato in base allo scambio di autenticazione tra lo switch e il client.
- Force Authorized: autorizza l'interfaccia senza autenticazione.

Interface: Port GE4 ▼

Administrative Port Control: Disabled
 Force Unauthorized
 Auto
 Force Authorized

RADIUS VLAN Assignment: Disabled
 Reject
 Static

Guest VLAN: Enable

Nota: in questo esempio, viene scelto Auto.

Passaggio 5. (Facoltativo) Scegliere un pulsante di opzione per l'assegnazione della VLAN RADIUS. L'assegnazione della VLAN dinamica verrà abilitata sulla porta specificata. Le opzioni sono:

- Disabled: ignora i risultati dell'autorizzazione VLAN e mantiene la VLAN originale dell'host. Questa è l'azione predefinita.
- Rifiuta: se la porta specificata riceve un'informazione di autorizzazione VLAN, utilizzerà tale informazione. Tuttavia, in assenza di informazioni autorizzate sulla VLAN, l'host viene rifiutato e reso non autorizzato.
- Statica: se la porta specificata riceve un'informazione autorizzata dalla VLAN, utilizzerà tale informazione. Tuttavia, se non sono presenti informazioni autorizzate sulla VLAN, rimarrà la VLAN originale dell'host.

Nota: se sono presenti informazioni autorizzate VLAN provenienti da RADIUS, ma la VLAN non è stata creata amministrativamente su Device Under Test (DUT), la VLAN verrà creata automaticamente. Nell'esempio, viene scelto Static.

| | | |
|------------------------------|----------------------------------|--------------------|
| Interface: | Port | GE4 ▼ |
| Administrative Port Control: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Force Unauthorized |
| | <input checked="" type="radio"/> | Auto |
| | <input type="radio"/> | Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Reject |
| | <input checked="" type="radio"/> | Static |
| Guest VLAN: | <input type="checkbox"/> | Enable |

Suggerimento rapido: affinché la funzione di assegnazione dinamica della VLAN funzioni, lo switch richiede l'invio da parte del server RADIUS dei seguenti attributi VLAN:

- [64] Tipo di tunnel = VLAN (tipo 13)
- [65] Tunnel-Medium-Type = 802 (tipo 6)
- [81] Tunnel-Private-Group-Id = ID VLAN

Passaggio 6. (Facoltativo) Selezionare la casella di controllo Abilita per fare in modo che la VLAN guest utilizzi una VLAN guest per le porte non autorizzate.

| | |
|------------------------------|---|
| Interface: | Port <input type="text" value="GE4"/> |
| Administrative Port Control: | <input type="radio"/> Disabled <input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> Disabled <input type="radio"/> Reject <input checked="" type="radio"/> Static |
| Guest VLAN: | <input checked="" type="checkbox"/> Enable |

Passaggio 7. Selezionare la casella di controllo Attiva per la riautenticazione periodica. Verranno abilitati i tentativi di riautenticazione delle porte dopo il periodo di riautenticazione specificato.

| | |
|------------------------------|---|
| Interface: | Port <input type="text" value="GE4"/> |
| Administrative Port Control: | <input type="radio"/> Disabled <input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> Disabled <input type="radio"/> Reject <input checked="" type="radio"/> Static |
| Guest VLAN: | <input checked="" type="checkbox"/> Enable |
| Periodic Reauthentication: | <input checked="" type="checkbox"/> Enable |

Nota: questa funzione è attivata per default.

Passaggio 8. Immettere un valore nel campo Periodo di riautenticazione. Tempo di riautenticazione della porta espresso in secondi.

| | | |
|------------------------------|-------------------------------------|--------------------|
| Interface: | Port | GE4 ▼ |
| Administrative Port Control: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Force Unauthorized |
| | <input checked="" type="radio"/> | Auto |
| | <input type="radio"/> | Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Reject |
| | <input checked="" type="radio"/> | Static |
| Guest VLAN: | <input checked="" type="checkbox"/> | Enable |
| Periodic Reauthentication: | <input checked="" type="checkbox"/> | Enable |
| ⚙ Reauthentication Period: | <input type="text" value="3600"/> | |
| Reauthenticate Now: | <input type="checkbox"/> | |

Nota: nell'esempio viene utilizzato il valore predefinito 3600.

Passaggio 9. (Facoltativo) Selezionare la casella di controllo Riautentica ora per abilitare la riautenticazione immediata delle porte.

Nota: nel campo Stato autenticatore viene visualizzato lo stato corrente dell'autenticazione.

| | | |
|------------------------------|-------------------------------------|--------------------|
| Interface: | Port | GE4 ▼ |
| Administrative Port Control: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Force Unauthorized |
| | <input checked="" type="radio"/> | Auto |
| | <input type="radio"/> | Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> | Disabled |
| | <input type="radio"/> | Reject |
| | <input checked="" type="radio"/> | Static |
| Guest VLAN: | <input checked="" type="checkbox"/> | Enable |
| Periodic Reauthentication: | <input checked="" type="checkbox"/> | Enable |
| ⚙ Reauthentication Period: | <input type="text" value="3600"/> | |
| Reauthenticate Now: | <input checked="" type="checkbox"/> | |
| Authenticator State: | N/A | |

Nota: se la porta non è in stato Force Authorized o Force Unauthorized, si trova in modalità automatica e l'autenticatore visualizza lo stato dell'autenticazione in corso. Dopo l'autenticazione della porta, lo stato viene visualizzato come Autenticato.

Passaggio 10. Nel campo Max Hosts, immettere il numero massimo di host autenticati consentiti sulla porta specifica. Questo valore ha effetto solo sulla modalità multisessione.

| | | |
|------------------------------|--|--|
| Interface: | Port | GE4 ▼ |
| Administrative Port Control: | <input type="radio"/> Disabled | <input type="radio"/> Force Unauthorized |
| | <input checked="" type="radio"/> Auto | <input type="radio"/> Force Authorized |
| RADIUS VLAN Assignment: | <input type="radio"/> Disabled | <input type="radio"/> Reject |
| | <input checked="" type="radio"/> Static | |
| Guest VLAN: | <input checked="" type="checkbox"/> Enable | |
| Periodic Reauthentication: | <input checked="" type="checkbox"/> Enable | |
| ⚙️ Reauthentication Period: | <input type="text" value="3600"/> | |
| Reauthenticate Now: | <input checked="" type="checkbox"/> | |
| Authenticator State: | N/A | |
| ⚙️ Max Hosts: | <input type="text" value="256"/> | |

Nota: nell'esempio viene utilizzato il valore predefinito 256.

Passaggio 11. Nel campo Quiet Period (Periodo di inattività), immettere il numero di secondi durante i quali lo switch rimane in stato di inattività in seguito a uno scambio di autenticazione non riuscito. Quando lo switch è in modalità non interattiva, significa che non è in ascolto di nuove richieste di autenticazione da parte del client.

| | |
|-----------------------------|-------------------------------------|
| ⚙️ Reauthentication Period: | <input type="text" value="3600"/> |
| Reauthenticate Now: | <input checked="" type="checkbox"/> |
| Authenticator State: | N/A |
| ⚙️ Max Hosts: | <input type="text" value="256"/> |
| ⚙️ Quiet Period: | <input type="text" value="60"/> |

Nota: nell'esempio viene utilizzato il valore predefinito 60.

Passaggio 12. Nel campo Rinvio EAP, immettere il numero di secondi che lo switch attende per la risposta a una richiesta EAP (Extensible Authentication Protocol) o a un frame di identità dal supplicant (client) prima di inviare nuovamente la richiesta.

| | |
|-----------------------------|-------------------------------------|
| ⚙️ Reauthentication Period: | <input type="text" value="3600"/> |
| Reauthenticate Now: | <input checked="" type="checkbox"/> |
| Authenticator State: | N/A |
| ⚙️ Max Hosts: | <input type="text" value="256"/> |
| ⚙️ Quiet Period: | <input type="text" value="60"/> |
| ⚙️ Resending EAP: | <input type="text" value="30"/> |

Nota: nell'esempio viene utilizzato il valore predefinito 30.

Passaggio 13. Nel campo Numero massimo di richieste EAP, immettere il numero massimo di richieste EAP che possono essere inviate. Se non si riceve una risposta dopo il periodo definito (timeout del supplicant), il processo di autenticazione viene riavviato.

| | |
|----------------------------|-------------------------------------|
| ⚙ Reauthentication Period: | <input type="text" value="3600"/> |
| Reauthenticate Now: | <input checked="" type="checkbox"/> |
| Authenticator State: | N/A |
| ⚙ Max Hosts: | <input type="text" value="256"/> |
| ⚙ Quiet Period: | <input type="text" value="60"/> |
| ⚙ Resending EAP: | <input type="text" value="30"/> |
| ⚙ Max EAP Requests: | <input type="text" value="2"/> |

Nota: nell'esempio viene utilizzato il valore predefinito 2.

Passaggio 14. Nel campo Timeout supplicant, immettere il numero di secondi che devono trascorrere prima che le richieste EAP vengano inviate al supplicant.

| | |
|-----------------------|----------------------------------|
| ⚙ Max Hosts: | <input type="text" value="256"/> |
| ⚙ Quiet Period: | <input type="text" value="60"/> |
| ⚙ Resending EAP: | <input type="text" value="30"/> |
| ⚙ Max EAP Requests: | <input type="text" value="2"/> |
| ⚙ Supplicant Timeout: | <input type="text" value="30"/> |

Nota: nell'esempio viene utilizzato il valore predefinito 30.

Passaggio 15. Nel campo Server Timeout (Timeout server), immettere il numero di secondi che devono trascorrere prima che lo switch invii nuovamente una richiesta al server di autenticazione.

| | |
|-----------------------|----------------------------------|
| ⚙ Max Hosts: | <input type="text" value="256"/> |
| ⚙ Quiet Period: | <input type="text" value="60"/> |
| ⚙ Resending EAP: | <input type="text" value="30"/> |
| ⚙ Max EAP Requests: | <input type="text" value="2"/> |
| ⚙ Supplicant Timeout: | <input type="text" value="30"/> |
| ⚙ Server Timeout: | <input type="text" value="30"/> |

Nota: nell'esempio viene utilizzato il valore predefinito 30.

Passaggio 16. Fare clic su Apply (Applica).

A questo punto, la configurazione dell'autenticazione della porta sullo switch è riuscita.

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).