Configurazione dell'autenticazione della porta 802.1X sugli switch gestiti Cisco serie 200/300

Obiettivo

L'obiettivo di questo documento è spiegare l'autenticazione della porta 801.1X sugli switch gestiti serie 200/300. L'autenticazione porta 802.1X consente la configurazione dei parametri 802.1X per ciascuna porta. 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

·SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

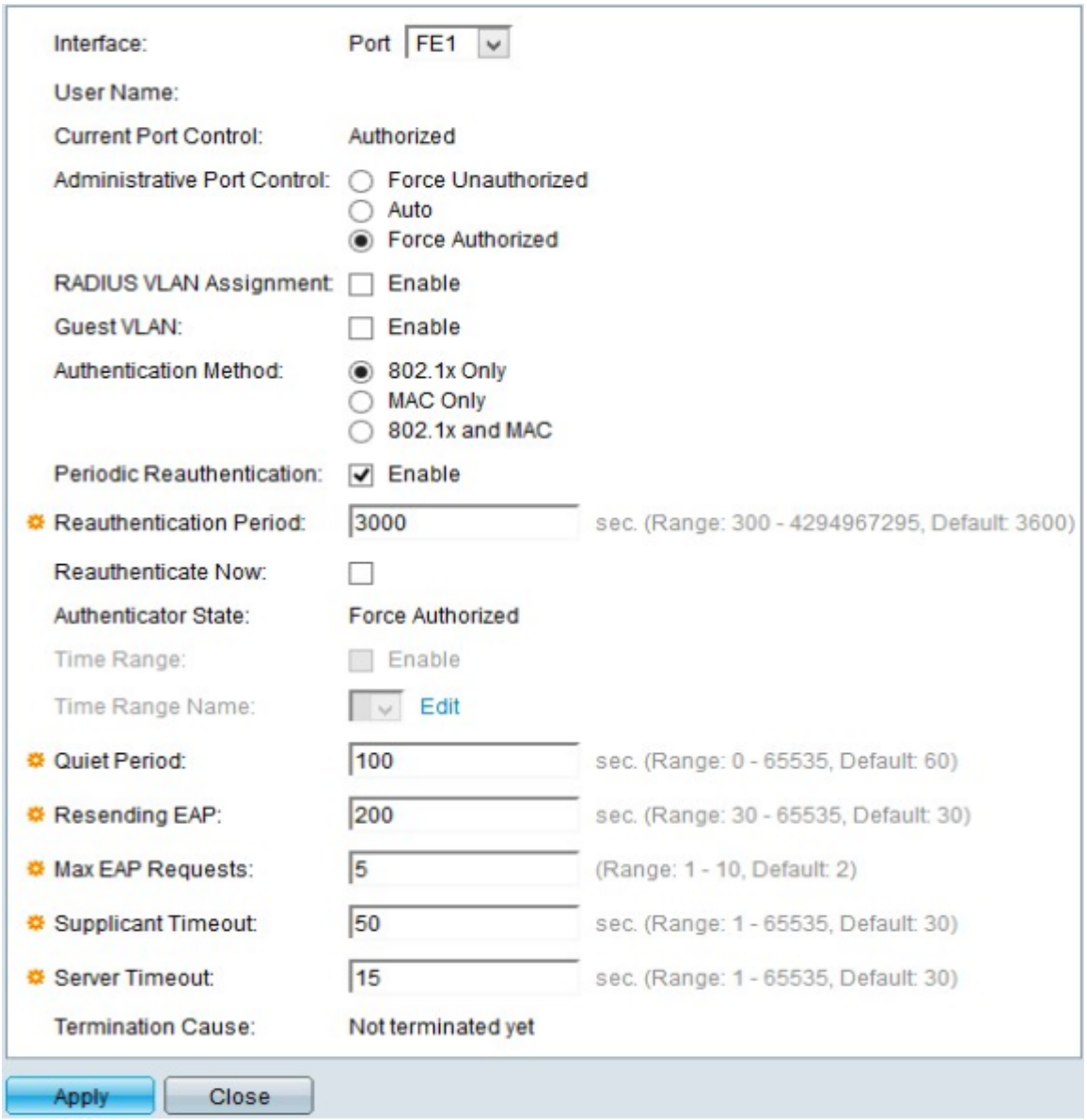
•1.3.0.62

Port Authentication Configuration

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > 802.1x > Autenticazione porta**. Viene visualizzata la pagina *Port Authentication* (Autenticazione porta):

Passaggio 2. Fare clic sul pulsante di opzione corrispondente alla porta che si desidera modificare.

Passaggio 3. Fare clic su **Modifica**. Viene visualizzata la finestra *Modifica autenticazione porta*.



Nel campo Nome utente viene visualizzato il nome utente della porta.

Nota: nel campo Controllo porta corrente viene visualizzato lo stato della porta corrente. Se la porta è in stato Non autorizzato, significa che la porta non è autenticata o che l'opzione Controllo porta amministrativa è impostata su Forza non autorizzato. D'altro canto, se la porta è in stato Autorizzato, significa che la porta è autenticata o che l'opzione Controllo porta amministrativa è impostata su Forza autorizzazione.

Passaggio 4. Nel campo Controllo porta amministrativa, fare clic su uno dei pulsanti di opzione disponibili per determinare lo stato di autorizzazione della porta:

·Force Unauthorized (Imponi non autorizzati) - Questa opzione imposta lo stato non autorizzato dell'interfaccia selezionata. In questo stato, lo switch non fornisce l'autenticazione al client connesso all'interfaccia.

·Auto: questa opzione abilita l'autenticazione e l'autorizzazione sull'interfaccia scelta. In questo stato, lo switch fornisce l'autenticazione 802.1X ai client connessi all'interfaccia e decide, in base alle informazioni di autenticazione scambiate con il client, se il client è autenticato o meno e sposta l'interfaccia allo stato Autorizzato o Non autorizzato.

·Force Authorized: questa opzione imposta l'interfaccia su Authorized senza autenticazione client.

Passaggio 5. (Facoltativo) Nel campo VLAN guest, selezionare la casella di controllo **Abilita** per usare una VLAN guest per le porte non autorizzate.

Passaggio 6. Nel campo Metodo di autenticazione fare clic su uno dei pulsanti di opzione disponibili per autenticare la porta. Le opzioni sono:

·Solo 802.1X: sulla porta viene eseguita solo l'autenticazione 802.1X.

·Solo MAC: solo l'autenticazione basata su MAC viene eseguita sulla porta. Su una singola porta è possibile eseguire solo 8 autenticazioni basate su MAC.

·802.1X e MAC: entrambi i metodi di autenticazione vengono eseguiti sulla porta.

Passaggio 7. Nel campo Riautenticazione periodica selezionare la casella di controllo **Abilita** per abilitare l'autenticazione periodica della porta in base al valore Periodo di riautenticazione.

Passaggio 8. Nel campo Periodo di riautenticazione immettere il tempo in secondi per la riautenticazione della porta.

Passaggio 9. Selezionare la casella di controllo **Riautentica ora** per riautenticare immediatamente la porta.

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

Passaggio 10. (Facoltativo) Se l'autenticazione basata sulla porta è abilitata sullo switch, i campi Intervallo di tempo e Nome intervallo di tempo sono abilitati. Nel campo Intervallo di tempo, immettere un'ora (in secondi) in cui la porta è autorizzata per l'uso se è abilitata l'autorizzazione 802.1X. Nell'elenco a discesa Nome intervallo di tempo, scegliere il profilo che identifica l'intervallo di tempo.

Passaggio 11. Nel campo Quiet Period (Periodo di attesa), immettere il periodo di tempo durante il quale lo switch rimane nello stato integro dopo 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.

Passaggio 12. Nel campo Resending EAP (Extensible Authentication Protocol), immettere l'ora in cui lo switch attende un messaggio di risposta dal supplicant prima di inviare nuovamente una richiesta.

Passaggio 13. Nel campo Numero massimo di richieste EAP immettere il numero massimo di richieste EAP che è possibile inviare. EAP è un metodo di autenticazione utilizzato in 802.1X che fornisce lo scambio di informazioni di autenticazione tra lo switch e il client. In questo caso, la richiesta EAP viene inviata al client per l'autenticazione. Il client deve quindi rispondere e corrispondere alle informazioni di autenticazione. Se il client non risponde, viene impostata un'altra richiesta EAP in base al valore EAP di rinvio e il processo di autenticazione viene riavviato.

Passaggio 14. Nel campo Timeout supplicant, immettere l'intervallo di tempo che deve trascorrere prima che le richieste EAP vengano inviate al supplicant.

Passaggio 15. Nel campo Timeout server immettere il tempo che deve trascorrere prima che lo switch invii nuovamente una richiesta al server RADIUS.

Nel campo Causa terminazione vengono visualizzati i motivi dell'errore di autenticazione

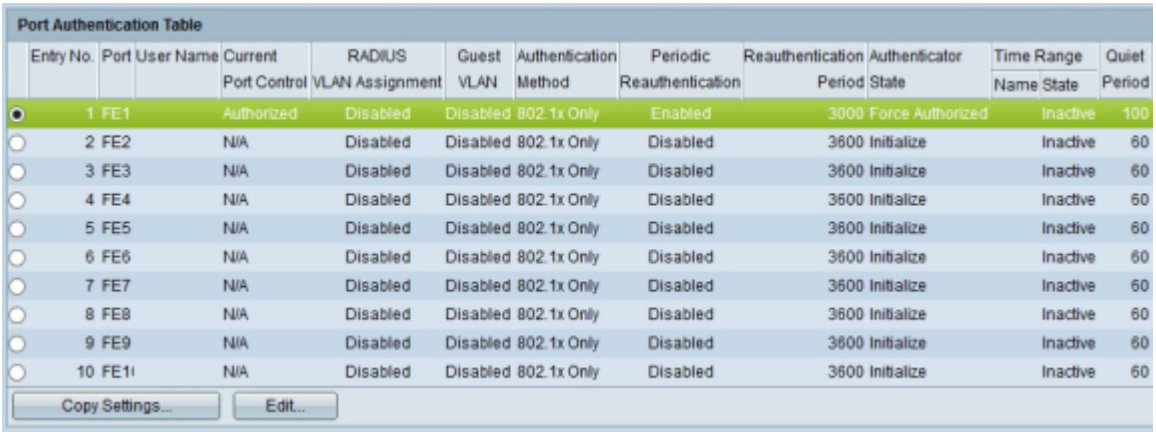
della porta.

Passaggio 16. Fare clic su **Apply** (Applica) per salvare la configurazione.

Applicazione di una configurazione interfaccia a più interfacce

Questa sezione spiega come applicare la configurazione dell'autenticazione 802.1X di una porta a più porte.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > 802.1x > Autenticazione porta**. Viene visualizzata la pagina *Port Authentication* (Autenticazione porta):



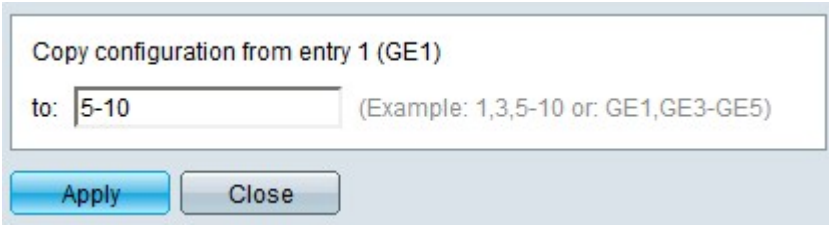
Port Authentication Table

	Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Time Range State	Quiet Period
◉	1	FE1		Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized		Inactive	100
○	2	FE2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	3	FE3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	4	FE4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	5	FE5		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	6	FE6		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	7	FE7		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	8	FE8		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	9	FE9		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	10	FE1		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60

Copy Settings... Edit...

Passaggio 2. Fare clic sul pulsante di opzione dell'interfaccia a cui si desidera applicare la configurazione di autenticazione a più interfacce.

Passaggio 3. Fare clic su **Copia impostazioni**. Viene visualizzata la finestra *Copia impostazioni*.



Passaggio 4. Nel campo **a**, immettere l'intervallo di interfacce a cui applicare la configurazione dell'interfaccia scelta nel passaggio 2. È possibile utilizzare i numeri di interfaccia o il nome delle interfacce come input. È possibile immettere le interfacce separate da una virgola, ad esempio 1, 3, 5 o GE1, GE3, GE5, oppure immettere un intervallo di interfacce, ad esempio 1-5 o GE1-GE5.

Passaggio 5. Fare clic su **Apply** (Applica) per salvare la configurazione.

L'immagine seguente mostra le modifiche apportate dopo la configurazione.

Port Authentication

Port Authentication Table

Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Time Range State	Quiet Period
1	FE1		Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized		Inactive	100
2	FE2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
3	FE3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
4	FE4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
5	FE5		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
6	FE6		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
7	FE7		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
8	FE8		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
9	FE9		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
10	FE1		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100

Copy Settings... Edit...

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).