Configuración de autenticación de puerto 802.1X en los switches gestionados de la serie 200/300 de Cisco

Objetivo

El objetivo de este documento es explicar la autenticación de puertos 801.1X en los switches gestionados serie 200/300. La autenticación de puerto 802.1X habilita la configuración de parámetros 802.1X para cada puerto. Un puerto que solicita autenticación se denomina suplicante. El autenticador es un switch o un punto de acceso que actúa como protector de red para los suplicantes. El autenticador reenvía los mensajes de autenticación al servidor RADIUS para que un puerto pueda ser autenticado y pueda enviar y recibir información.

Dispositivos aplicables

Switches gestionados · SF/SG serie 200 y SF/SG serie 300

Versión del software

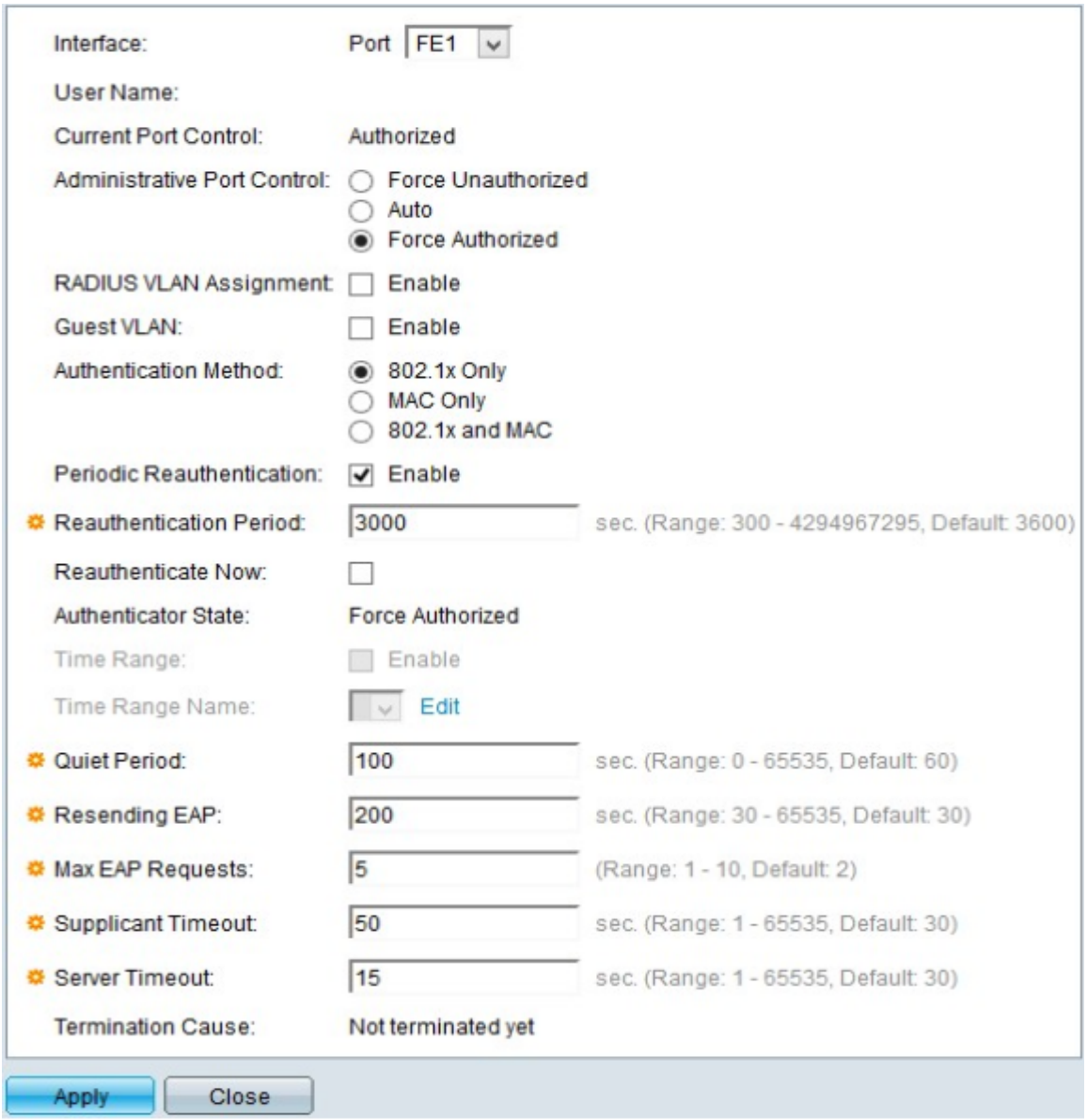
•1.3.0.62

Configuración de autenticación de puerto

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > 802.1x > Port Authentication**. Se abre la página *Autenticación de Puerto*:

Paso 2. Haga clic en el botón de opción correspondiente al puerto que desea editar.

Paso 3. Haga clic en **Editar**. Aparece la ventana *Edit Port Authentication*.



El campo Nombre de usuario muestra el nombre de usuario del puerto.

Nota: El campo Current Port Control (Control de puerto actual) muestra el estado del puerto actual. Si el puerto está en estado No autorizado significa que el puerto no está autenticado o que el Control de Puerto Administrativo está configurado como Forzar no autorizado. Por otra parte, si el puerto está en estado Autorizado, significa que el puerto está autenticado o que el Control de Puerto Administrativo está configurado como Forzar autorizado.

Paso 4. En el campo Administrative Port Control (Control de puerto administrativo), haga clic en uno de los botones de opción disponibles para determinar el estado de autorización de puerto:

·Forzar no autorizado: esta opción mueve la interfaz elegida al estado No autorizado. En este estado, el switch no proporciona autenticación al cliente conectado a la interfaz.

·Automático: esta opción habilita la autenticación y autorización en la interfaz elegida. En este estado, el switch proporciona autenticación 802.1X a los clientes conectados a la interfaz y decide, en base al intercambio de información de autenticación con el cliente, si el cliente se autentica o no, y mueve la interfaz a estado Autorizado o No Autorizado.

·Force Authorized : Esta opción establece la interfaz en Authorized sin autenticación de cliente.

Paso 5. (Opcional) En el campo VLAN de invitado, marque la casilla de verificación **Enable** para utilizar una VLAN de invitado para puertos no autorizados.

Paso 6. En el campo Authentication Method (Método de autenticación), haga clic en uno de los botones de opción disponibles para autenticar el puerto. Las opciones son:

Sólo 802.1X ·: sólo se realiza la autenticación 802.1X en el puerto.

·sólo MAC: sólo se realiza la autenticación basada en MAC en el puerto. Sólo se pueden realizar 8 autenticaciones basadas en MAC en un único puerto.

·802.1X y MAC: ambos métodos de autenticación se realizan en el puerto.

Paso 7. En el campo Reautenticación periódica, marque la casilla de verificación **Enable** para habilitar la autenticación periódica del puerto basada en el valor del Período de Reautenticación.

Paso 8. En el campo Periodo de Reautenticación, introduzca el tiempo en segundos para volver a autenticar el puerto.

Paso 9. Marque la casilla de verificación **Reautenticar ahora** para volver a autenticar inmediatamente el puerto.

Nota: El campo Estado del autenticador muestra el estado actual de la autenticación.

Paso 10. (Opcional) Si la autenticación basada en puerto está activada en el switch, los campos Rango de tiempo y Nombre de rango de tiempo están habilitados. En el campo Rango de tiempo, introduzca un tiempo (en segundos) en el que el puerto esté autorizado para su uso si la autorización 802.1X está habilitada. En la lista desplegable Nombre del rango de tiempo, elija el perfil que identifica el rango de tiempo.

Paso 11. En el campo Período silencioso, introduzca la hora en la que el switch permanece en estado completo después de un intercambio de autenticación fallido. Cuando el switch se encuentra en estado silencioso, significa que el switch no está escuchando nuevas solicitudes de autenticación del cliente.

Paso 12. En el campo EAP de reenvío (protocolo de autenticación extensible), introduzca la hora a la que el switch espera un mensaje de respuesta del solicitante antes de reenviar una solicitud.

Paso 13. En el campo Max EAP Requests (Máximo de solicitudes EAP), introduzca el número máximo de solicitudes EAP que se pueden enviar. EAP es un método de autenticación utilizado en 802.1X que proporciona intercambio de información de autenticación entre el switch y el cliente. En este caso, la solicitud EAP se envía al cliente para la autenticación. A continuación, el cliente debe responder y coincidir con la información de autenticación. Si el cliente no responde, se establece otra solicitud EAP en función del valor EAP de reenvío y se reinicia el proceso de autenticación.

Paso 14. En el campo Límite de tiempo del solicitante, introduzca el tiempo antes de que las solicitudes EAP se envíen al solicitante.

Paso 15. En el campo Server Timeout (Tiempo de espera del servidor), introduzca el tiempo que transcurre antes de que el switch envíe una solicitud de nuevo al servidor RADIUS.

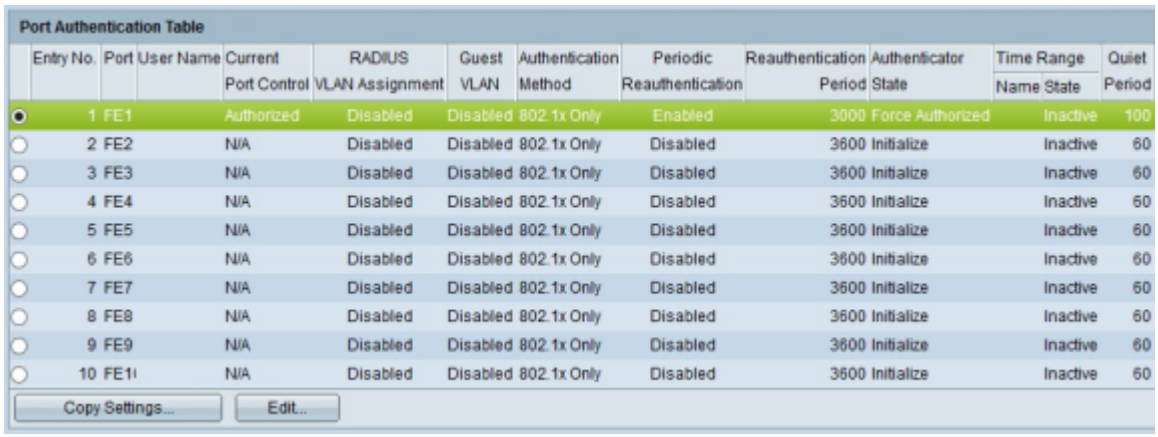
El campo Causa de terminación muestra los motivos de la falla de autenticación de puerto.

Paso 16. Haga clic en **Aplicar** para guardar la configuración.

Aplicación de una Configuración de Interfaz a Varias Interfaces

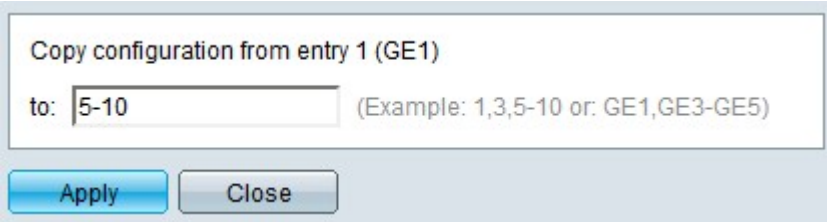
Esta sección explica cómo aplicar la configuración de autenticación 802.1X de un puerto a varios puertos.

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > 802.1x > Port Authentication**. Se abre la página *Autenticación de Puerto*:



Paso 2. Haga clic en el botón de opción de la interfaz que desea aplicar la configuración de autenticación a varias interfaces.

Paso 3. Haga clic en **Copiar configuración**. Aparecerá la ventana *Copiar configuración*.



Paso 4. En el campo **to**, ingrese el rango de interfaces que desea aplicar la configuración de la interfaz elegida en el Paso 2. Puede utilizar los números de interfaz o el nombre de las interfaces como entrada. Puede ingresar cada interfaz separada por una coma (por ejemplo: 1, 3, 5 o GE1, GE3, GE5) o puede introducir un intervalo de interfaces (por ejemplo: 1-5 o GE1-GE5).

Paso 5. Haga clic en **Aplicar** para guardar la configuración.

La siguiente imagen muestra los cambios después de la configuración.

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...