configuración de autenticación del puerto del 802.1x en el Switches manejado 200/300 Series de Cisco

Objetivo

El objetivo de este documento es explicar la autenticación del puerto 801.1X en el Switches manejado las 200/300 Series. la autenticación del puerto del 802.1x habilita la configuración de los parámetros del 802.1x para cada puerto. Un puerto que pide la autenticación se llama el supplicant. El authenticator es un Switch o un Punto de acceso que actúa como guardia de la red a los suplicantes. Del authenticator los mensajes de autenticación adelante al servidor de RADIUS para poder autenticar y pueda enviar y recibir un puerto la información.

Dispositivos aplicables

- Switches manejado 300 Series SF/SG 200 y SF/SG

Versión del software

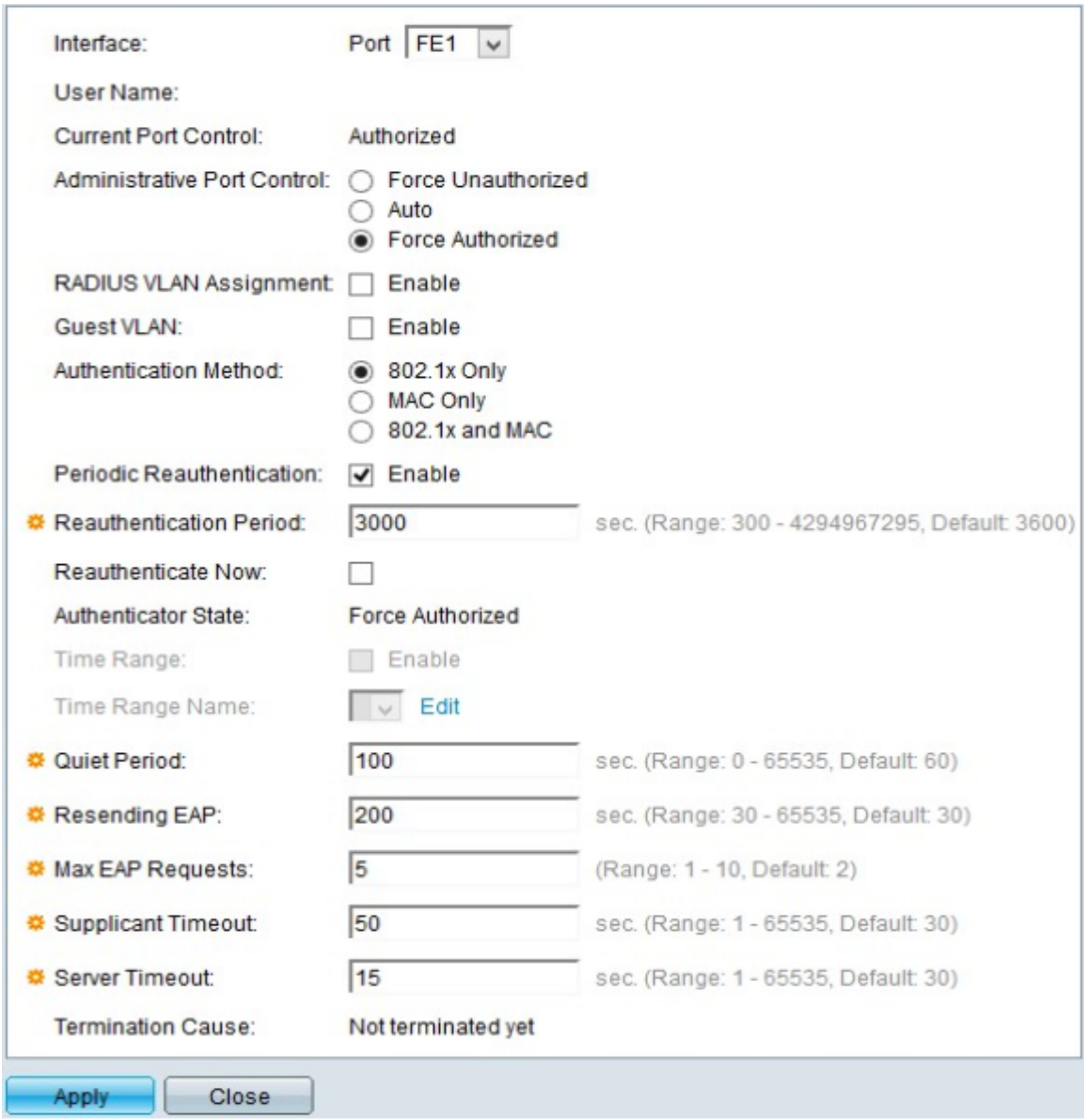
- 1.3.0.62

Configuración de autenticación del puerto

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > el 802.1x > la autenticación del puerto**. La página de la *autenticación del puerto* se abre:

Paso 2. Haga clic el botón de radio que corresponde al puerto que usted quisiera editar.

Paso 3. El tecleo **edita**. *El puerto del editar ventana Authentication (Autenticación)* aparece.



El campo de Nombre de usuario visualiza el Nombre de usuario del puerto.

Note: El Campo de control actual del puerto visualiza al estado de puerto actual. Si el puerto está en el estado desautorizado significa que el puerto o no está autenticado o el control administrativo del puerto está fijado para forzar desautorizado. Por otra parte, si el puerto está en el estado autorizado, significa que el puerto o está autenticado o el control administrativo del puerto está fijado para forzar autorizado.

Paso 4. En el Campo de control administrativo del puerto, haga clic uno de los botones de radio disponibles para determinar el estado de la autorización de puerto:

- Fuerza desautorizada — Esta opción mueve la interfaz elegida al estado desautorizado. En este estado, el Switch no proporciona la autenticación al cliente conectado con la interfaz.

- Auto — Esta opción habilita la autenticación y autorización en la interfaz elegida. En este estado, el Switch proporciona la autenticación del 802.1x a los clientes conectados con la interfaz y decide, sobre la base del intercambio de la información de autenticación con el cliente, si autentican al cliente o no, y mueve la interfaz al estado autorizado o desautorizado.

- Fuerza autorizada — Esta opción fijó la interfaz a autorizado sin la autenticación de

cliente.

El paso 5. (opcional) en el campo del VLA N del invitado, marca la casilla de verificación del permiso para utilizar un VLA N del invitado para los puertos desautorizados.

Paso 6. En el campo del método de autentificación, haga clic uno de los botones de radio disponibles para autenticar el puerto. Las opciones son:

- 802.1x solamente — Solamente la autenticación del 802.1x se realiza en el puerto.
- MAC solamente — Solamente la autenticación MAC basada se realiza en el puerto. Solamente 8 autenticaciones MAC basadas se pueden realizar en un puerto único.
- 802.1x y MAC — Ambos métodos de autentificación se realizan en el puerto.

Paso 7. En el campo periódico del Reauthentication, marque la casilla de verificación del permiso para habilitar la autenticación periódica del puerto basado en el valor del período del Reauthentication.

Paso 8. En el campo del período del Reauthentication, ingrese la época en los segundos de reauthenticate el puerto.

Paso 9. Ahora marque la casilla de verificación del Reauthenticate para reauthenticate inmediatamente el puerto.

Note: El campo de estado del authenticator visualiza al estado actual de autenticación.

El paso 10. (opcional) si la autenticación basada puerto se habilita en el Switch, después el rango de tiempo y los campos de nombre del rango de tiempo se habilita. En el campo del rango de tiempo, ingrese una época (en los segundos) donde el puerto se autoriza para el uso si se habilita la autorización del 802.1x. En la lista desplegable del nombre del rango de tiempo, elija el perfil que identifica el rango de tiempo.

Paso 11. En el campo del período tranquilo, ingrese el tiempo que sigue habiendo el Switch en muy el estado después de que un intercambio de la autenticación fallida. Cuando el Switch está en el estado reservado, significa que el Switch no está estando atentos los nuevos pedidos de autenticación del cliente.

Paso 12. En el campo de reenvío EAP (protocolo extensible authentication), ingrese el tiempo que el Switch espera un mensaje de respuesta del supplicant antes de volver a enviar una petición.

Paso 13. En el EAP máximo las peticiones colocan, ingresan el número máximo de peticiones EAP que puedan ser enviadas. El EAP es un método de autentificación usado en el 802.1x que proporciona el intercambio de la información de autenticación entre el Switch y el cliente. En este caso, la petición EAP se envía al cliente para la autenticación. El cliente después tiene que responder y hacer juego la información de autenticación. Si no responde el cliente, después otra petición EAP es determinada basada en el valor de reenvío EAP y se recomienza el proceso de autenticación.

Paso 14. En el campo del descanso del supplicant, ingrese el tiempo antes de que las peticiones EAP se vuelvan a enviar al supplicant.

Paso 15. En el campo del tiempo de espera del servidor, ingrese el tiempo que los pasajes antes de que el Switch envíe una petición otra vez al servidor de RADIUS.

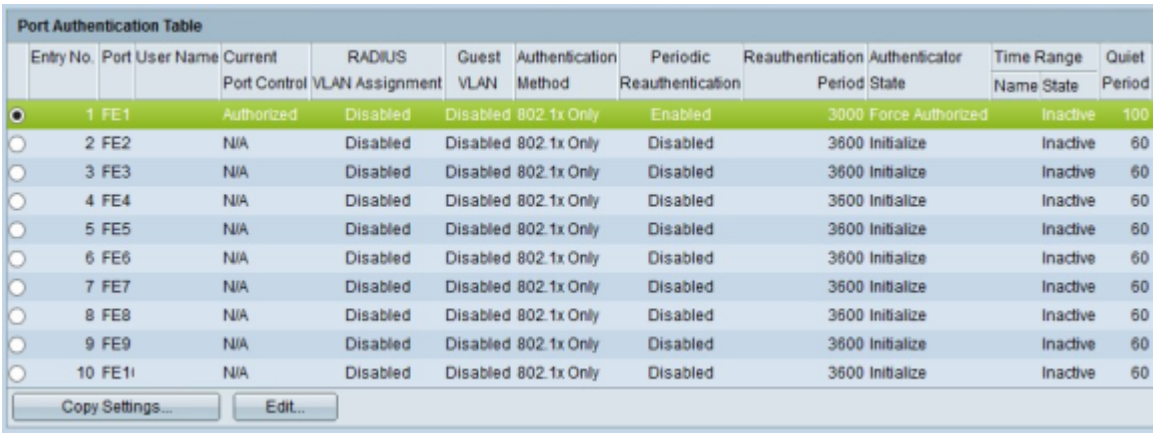
El campo de la causa de la terminación visualiza las razones de la falla de autenticación del puerto.

Paso 16. El tecleo **se aplica** para salvar su configuración.

Aplique una configuración de la interfaz a las interfaces múltiples

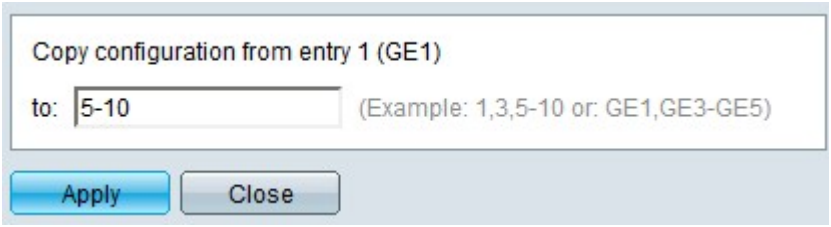
Esta sección explica cómo aplicar la configuración de autenticación del 802.1x de un puerto a los puertos múltiples.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > el 802.1x > la autenticación del puerto**. La página de la *autenticación del puerto* se abre:



Paso 2. Haga clic el botón de radio de la interfaz que usted quiere aplicar la configuración de autenticación a las interfaces múltiples.

Paso 3. **Configuraciones de la copia del** tecleo. *La ventana de configuración de la copia* aparece.



Paso 4. En a colocar, ingrese el rango de las interfaces que usted quiere para aplicar la configuración de la interfaz elegida en el paso 2. Usted puede utilizar los Números de interfaz o el nombre de las interfaces como entrada. Usted puede ingresar cada interfaz separada por una coma (por ejemplo: 1, 3, 5 o GE1, el GE3, GE5) o usted puede ingresar un rango de las interfaces (por ejemplo: 1-5 o GE1-GE5).

Paso 5. El tecleo **se aplica** para salvar su configuración.

La imagen abajo representa 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...