Configure las propiedades globales de 802.1x en un switch a través de la CLI

Introducción

IEEE 802.1x es un estándar que facilita el control de acceso entre un cliente y un servidor. Antes de que una red de acceso local (LAN) o un switch puedan proporcionar servicios a un cliente, el servidor de autenticación que ejecuta el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) debe autenticar al cliente conectado al puerto del switch.

La autenticación 802.1x impide que los clientes no autorizados se conecten a una LAN a través de puertos de acceso público. La autenticación 802.1x es un modelo cliente-servidor. En este modelo, los dispositivos de red tienen las siguientes funciones específicas:

- Cliente o suplicante: un cliente o suplicante es un dispositivo de red que solicita acceso a la LAN. El cliente está conectado a un autenticador.
- Authenticator: un autenticador es un dispositivo de red que proporciona servicios de red y a los que se conectan los puertos de suplicante. Se admiten los siguientes métodos de autenticación:

  - Basado en 802.1x: soportado en todos los modos de autenticación. En la autenticación basada en 802.1x, el autenticador extrae los mensajes del protocolo de autenticación extensible (EAP) de los mensajes 802.1x o de los paquetes EAP sobre LAN (EAPoL) y los pasa al servidor de autenticación mediante el protocolo RADIUS.

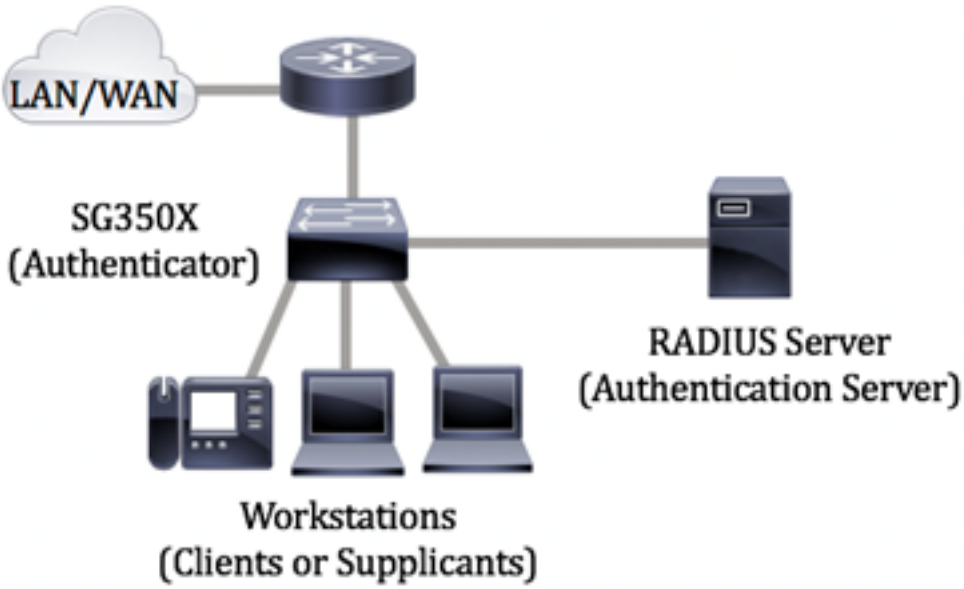
  - basado en MAC: compatible en todos los modos de autenticación. Con el control de acceso a medios (MAC) basado, el autenticador ejecuta la parte de cliente EAP del software en nombre de los clientes que buscan acceso a la red.

  - Basado en Web: soportado sólo en modos de sesiones múltiples. Con la autenticación basada en web, el autenticador ejecuta la parte de cliente EAP del software en nombre de los clientes que buscan acceso a la red.

- Servidor de autenticación: un servidor de autenticación realiza la autenticación real del cliente. El servidor de autenticación para el dispositivo es un servidor de autenticación RADIUS con extensiones EAP.

  Nota: Un dispositivo de red puede ser un cliente o suplicante, autenticador o ambos por puerto.

  La siguiente imagen muestra una red que ha configurado los dispositivos según las funciones específicas. En este ejemplo, se utiliza un switch SG350X.



Pautas in configuración de 802.1x:

1. Configure el servidor RADIUS. Para saber cómo configurar los parámetros del servidor RADIUS en su switch, haga clic aquí.
2. Configuración de redes de área local virtuales (VLAN). Para crear VLAN utilizando la utilidad basada en web de su switch, haga clic aquí. Para obtener instrucciones basadas en CLI, haga clic aquí.
3. Configure los parámetros de puerto a VLAN en su switch. Para configurar mediante la utilidad basada en web, haga clic aquí. Para utilizar la CLI, haga clic aquí.
4. Configure las propiedades globales 802.1x en el switch. Para obtener instrucciones sobre cómo configurar las propiedades 802.1x globales a través de la utilidad basada en web del switch, haga clic aquí.
5. (Opcional) Configure el rango de tiempo en el switch. Para aprender a configurar los parámetros de rango de tiempo en su switch, haga clic aquí.
6. Configure la autenticación de puerto 802.1x. Para utilizar la utilidad basada en web del switch, haga clic aquí.

Objetivo

En este artículo se proporcionan instrucciones sobre cómo configurar las propiedades globales de 802.1x a través de la interfaz de línea de comandos (CLI) del switch, que incluye propiedades de autenticación y VLAN de invitado. La VLAN de invitado proporciona acceso a servicios que no requieren que los dispositivos o puertos de suscripción sean autenticados y autorizados a través de autenticación 802.1x, basada en MAC o basada en web.

Dispositivos aplicables

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

- Serie Sx550X

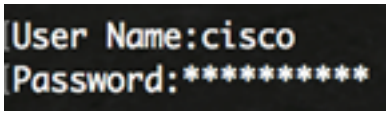
Versión del software

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

Configure las propiedades 802.1x en un switch a través de la CLI

Configuración de los parámetros 802.1x

Paso 1. Inicie sesión en la consola del switch. El nombre de usuario y la contraseña predeterminados son cisco/cisco. Si ha configurado un nuevo nombre de usuario o contraseña, introduzca las credenciales en su lugar.



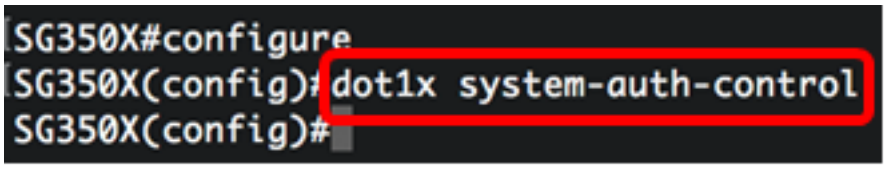
Nota: Los comandos pueden variar dependiendo del modelo exacto de su switch. En este ejemplo, se accede al switch SG350X a través de Telnet.

Paso 2. Desde el modo EXEC privilegiado del switch, ingrese el modo de configuración global ingresando lo siguiente:

```
SG350x#configure
```

Paso 3. Para habilitar globalmente la autenticación 802.1x en el switch, utilice el comando **dot1x system-auth-control** en el modo Global Configuration.

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



Paso 4. (Opcional) Para inhabilitar globalmente la autenticación 802.1x en el switch, introduzca lo siguiente:

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

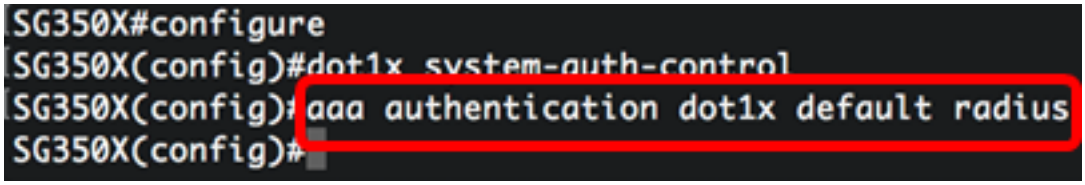
Nota: Si esto está desactivado, se desactivan las autenticaciones basadas en Web y en MAC 802.1X.

Paso 5. Para especificar qué servidores se utilizan para la autenticación cuando se habilita la autenticación 802.1x, introduzca lo siguiente:

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

Las opciones son:

- radius none: realiza primero la autenticación de puerto con la ayuda del servidor RADIUS. Si no hay respuesta del servidor como cuando el servidor está inactivo, no se realiza ninguna autenticación y se permite la sesión. Si el servidor está disponible y las credenciales del usuario son incorrectas, se deniega el acceso y la sesión finaliza.
- RADIUS: realiza la autenticación de puerto basada en el servidor RADIUS. Si no se realiza ninguna autenticación, la sesión finaliza. Ésta es la autenticación predeterminada.
- none: no autentica al usuario y permite la sesión.



Nota: En este ejemplo, el servidor de autenticación 802.1x predeterminado es RADIUS.

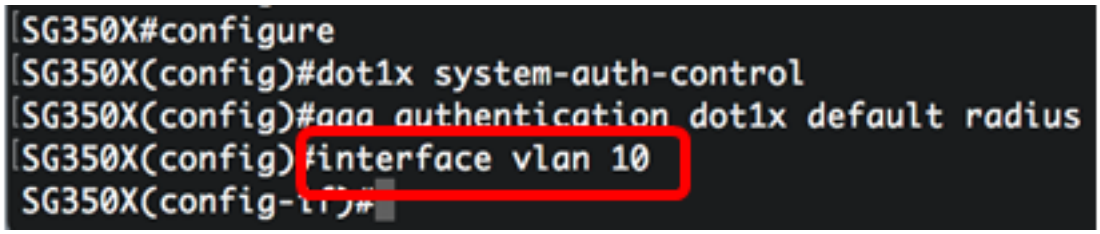
Paso 6. (Opcional) Para restaurar la autenticación predeterminada, introduzca lo siguiente:

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

Paso 7. En el modo Global Configuration, ingrese el contexto VLAN Interface Configuration ingresando lo siguiente:

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

- vlan-id: especifica un ID de VLAN que se debe configurar.



Paso 8. Para habilitar el uso de una VLAN de invitado para puertos no autorizados, introduzca lo siguiente:

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

Nota: Si se habilita una VLAN de invitado, todos los puertos no autorizados se unen automáticamente a la VLAN elegida en la VLAN de invitado. Si un puerto se autoriza posteriormente, se elimina de la VLAN de invitado.

Paso 9. Para salir del contexto de configuración de la interfaz, introduzca lo siguiente:

```
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)#
```

Paso 10. Para establecer el retardo de tiempo entre habilitar 802.1X (o puerto activo) y agregar un puerto a la VLAN de invitado, introduzca lo siguiente:

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

- timeout: especifica la demora en segundos entre habilitar 802.1X (o puerto activo) y agregar el puerto a la VLAN de invitado. El intervalo es de 30 a 180 segundos.

Nota: Después del link, si el software no detecta un suplicante 802.1x o si la autenticación de puerto falló, entonces el puerto se agrega a la VLAN de invitado solamente después de que venza el período de tiempo de espera de VLAN de invitado. Si el puerto cambia de Autorizado a No Autorizado, el puerto se agrega a la VLAN de invitado solamente después de que venza el período de tiempo de espera de la VLAN de invitado. Puede habilitar o inhabilitar la autenticación VLAN desde la autenticación VLAN.

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

Nota: En este ejemplo, el tiempo de espera de VLAN de invitado utilizado es de 60 segundos.

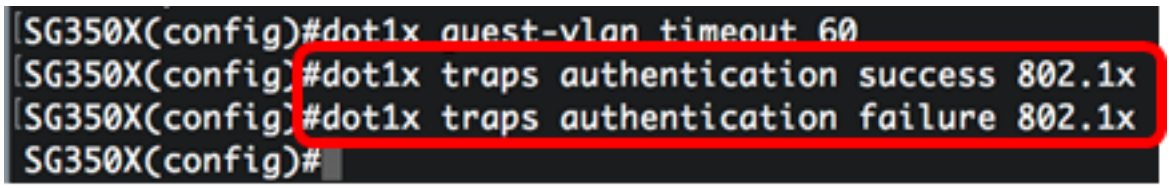
Paso 11. Para habilitar las trampas, verifique una o más de las siguientes opciones:

```
SG350X(config)# dot1x traps authentication [fallo | éxito | silenciosa] [802.1x | mac | web]
```

Las opciones son:

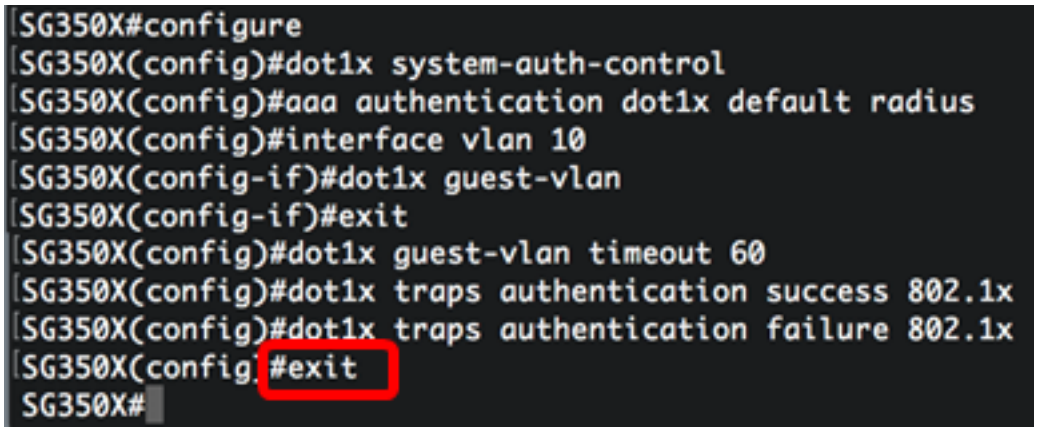
- Trampas de falla de autenticación 802.1x: envíe trampas si falla la autenticación 802.1x.
- trampas de éxito de autenticación 802.1x: envíe trampas si la autenticación 802.1x se realiza correctamente.
- trampas de falla de autenticación mac: envíe trampas si falla la autenticación MAC.
- trampas de éxito de autenticación mac: envíe trampas si la autenticación MAC se realiza correctamente.
- trampas de falla de autenticación web: envíe trampas si falla la autenticación web.
- trampas de éxito de autenticación web: envíe trampas si la autenticación web se realiza correctamente.
- trampas silenciosas de autenticación web: envíe trampas si comienza un período silencioso.

Nota: En este ejemplo, se ingresan trampas de error de autenticación 802.1x y de éxito.



Paso 12. Para salir del contexto de configuración de la interfaz, introduzca lo siguiente:

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



Paso 13. (Opcional) Para mostrar las propiedades 802.1x globales configuradas en el switch, introduzca lo siguiente:

```
SG350X#show dot1x
```

Ahora debería haber configurado correctamente las propiedades 802.1x en su switch.

Configuración de la Autenticación VLAN

Cuando se habilita 802.1x, los puertos o dispositivos no autorizados no pueden acceder a la VLAN a menos que formen parte de la VLAN de invitado o de una VLAN no autenticada. Los puertos deben agregarse manualmente a las VLAN.

Para inhabilitar la autenticación en una VLAN, siga estos pasos:

Paso 1. Desde el modo EXEC privilegiado del switch, ingrese el modo de configuración global ingresando lo siguiente:

```
SG350X#configure
```

Paso 2. En el modo Global Configuration, ingrese el contexto VLAN Interface Configuration

ingresando lo siguiente:

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

- vlan-id: especifica un ID de VLAN que se debe configurar.

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#
```

Nota: En este ejemplo, se elige VLAN 20.

Paso 3. Para inhabilitar la autenticación 802.1x en la VLAN, introduzca lo siguiente:

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

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#
```

Paso 4. (Opcional) Para habilitar la autenticación 802.1x en la VLAN, introduzca lo siguiente:

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

Paso 5. Para salir del contexto de configuración de la interfaz, introduzca lo siguiente:

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#end
SG350X#
```

Paso 6. (Opcional) Para mostrar los parámetros de autenticación global 802.1x en el switch, introduzca lo siguiente:

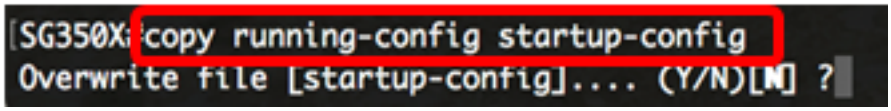
```
SG350X(config-if)#end
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

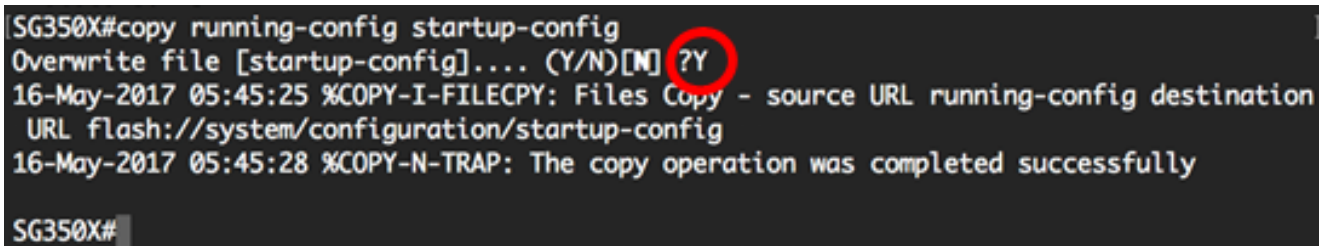
Nota: En este ejemplo, VLAN 20 se muestra como una VLAN no autenticada.

Paso 7. (Opcional) En el modo EXEC privilegiado del switch, guarde los parámetros configurados en el archivo de configuración de inicio, introduciendo lo siguiente:

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



Paso 8. (Opcional) Presione **Y** para Sí o **N** para No en su teclado una vez que aparezca el mensaje Sobrescribir archivo [startup-config]...



Ahora debería haber configurado correctamente los parámetros de autenticación 802.1x en las VLAN del switch.

Importante: Para continuar con la configuración de la autenticación de puerto 802.1x en su switch, siga las pautas anteriores.