

Configuración de la Autenticación Basada en MAC en un Switch

Objetivo

802.1X es una herramienta de administración para permitir la lista de dispositivos, lo que garantiza que no haya acceso no autorizado a la red. Este documento muestra cómo configurar la autenticación basada en MAC en un switch usando la interfaz gráfica de usuario (GUI). Para obtener información sobre cómo configurar la autenticación basada en MAC mediante la interfaz de línea de comandos (CLI), haga clic [aquí](#).

Nota: Esta guía es extensa en 9 secciones y 1 sección para verificar que un host ha sido autenticado. Tome café, té o agua y asegúrese de tener tiempo suficiente para revisar y ejecutar los pasos que se indican.

[Consulte el glosario para obtener información adicional.](#)

¿Cómo funciona RADIUS?

Hay tres componentes principales para la autenticación 802.1X, un suplicante (cliente), un autenticador (dispositivo de red como un switch) y un servidor de autenticación (RADIUS). El servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un servidor de acceso que utiliza el protocolo de autenticación, autorización y contabilidad (AAA) que ayuda a gestionar el acceso a la red. RADIUS utiliza un modelo cliente-servidor en el que se intercambia información de autenticación segura entre el servidor RADIUS y uno o más clientes RADIUS. Valida la identidad del cliente y notifica al switch si el cliente está autorizado o no para acceder a la LAN.

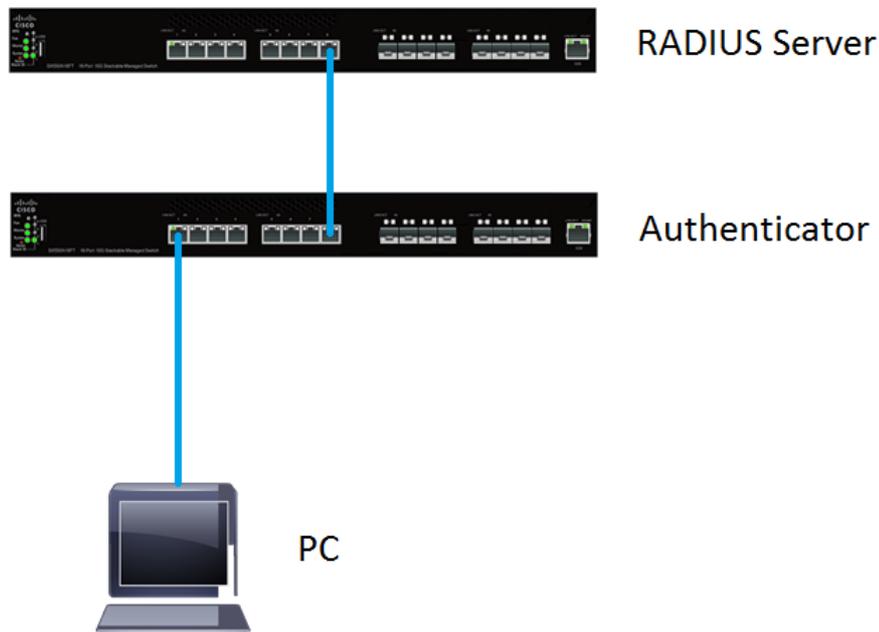
Un autenticador funciona entre el cliente y el servidor de autenticación. Primero, solicitará información de identidad al cliente. En respuesta, el autenticador verificaría la información con el servidor de autenticación. Por último, transmitiría una respuesta al cliente. En este artículo, el autenticador sería un switch que incluye el cliente RADIUS. El switch podría encapsular y desencapsular las tramas del protocolo de autenticación extensible (EAP) para interactuar con el servidor de autenticación.

¿Qué ocurre con la autenticación basada en MAC?

En la autenticación basada en MAC, cuando el solicitante no entiende cómo comunicarse con el autenticador o no puede hacerlo, utiliza la dirección MAC del host para autenticarse. Los suplicantes basados en MAC se autentican mediante RADIUS puro (sin utilizar EAP). El servidor RADIUS tiene una base de datos de host dedicada que contiene solamente las direcciones MAC permitidas. En lugar de tratar la solicitud de autenticación basada en MAC como una autenticación de protocolo de autenticación de contraseña (PAP), los servidores reconocen dicha solicitud mediante el atributo 6 [tipo de servicio] = 10. Compararán la dirección MAC en el atributo Calling-Station-Id con las direcciones MAC almacenadas en la base de datos host.

La versión 2.4 añade la capacidad de configurar el formato del nombre de usuario enviado para los suplicantes basados en MAC y ser definido ya sea el método de autenticación EAP o RADIUS puro. En esta versión, también puede configurar el formato del nombre de usuario así como una contraseña específica, diferente del nombre de usuario, para los suplicantes basados en MAC.

Topología:



Nota: En este artículo, utilizaremos el SG550X-24 tanto para el servidor RADIUS como para el autenticador. El servidor RADIUS tiene una dirección IP estática de 192.168.1.100 y el autenticador tiene una dirección IP estática de 192.168.1.101.

Los pasos de este documento se realizan bajo el modo **avanzado** de visualización. Para cambiar el modo a avanzado, vaya a la esquina superior derecha y seleccione **Avanzado** en la lista desplegable *Modo de visualización*.



Tabla de contenido

1. [Configuración global del servidor RADIUS](#)
2. [Teclas de servidor RADIUS](#)
3. [Grupos de servidores RADIUS](#)
4. [Usuarios del servidor RADIUS](#)
5. [Cliente RADIUS](#)
6. [Propiedades de autenticación 802.1X](#)
7. [Configuración de autenticación basada en MAC de autenticación 802.1X](#)
8. [Autenticación de host de autenticación 802.1X y autenticación de sesión](#)
9. [Autenticación del puerto de autenticación 802.1X](#)
10. [Conclusión](#)

Dispositivos aplicables

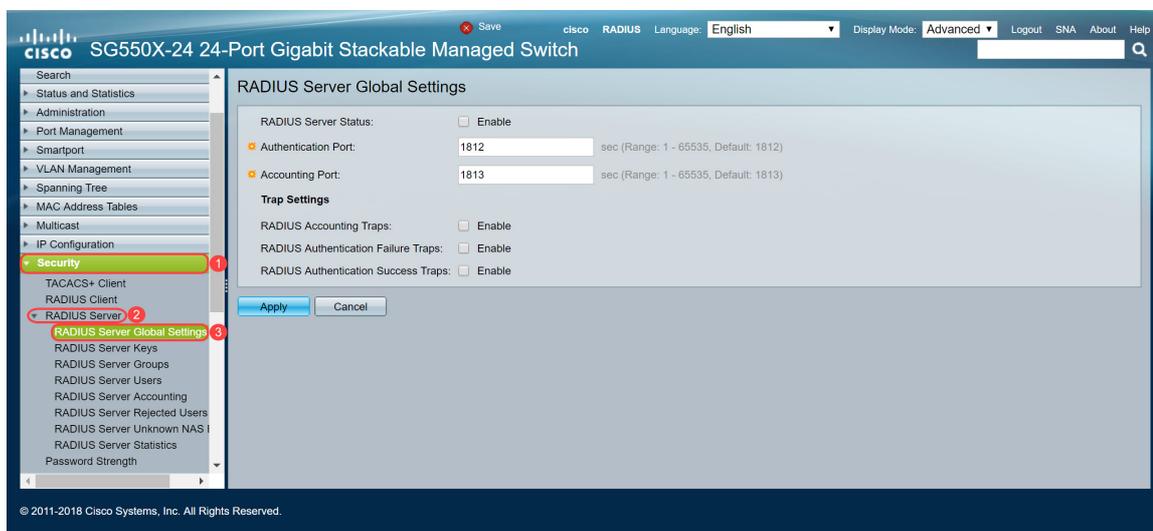
- Serie Sx350X
- Serie SG350XG
- Serie Sx550X
- Serie SG550XG

Versión del software

- 2.4.0.94

Configuración global del servidor RADIUS

Paso 1. Inicie sesión en la utilidad basada en web de su switch que se configurará como servidor RADIUS y navegue hasta **Seguridad > Servidor RADIUS > Configuración global del servidor RADIUS**.



Paso 2. Para habilitar el estado de la función del servidor RADIUS, marque la casilla de verificación **Enable** en el campo *RADIUS Server Status* .



Paso 3. Para generar trampas para los eventos de contabilización RADIUS, los inicios de sesión que fallaron o para los inicios de sesión que se realizaron correctamente, marque la casilla de verificación **Enable** para generar trampas. Las trampas son mensajes de eventos del sistema generados a través del protocolo simple de administración de red (SNMP). Se envía una trampa al administrador SNMP del switch cuando se produce una violación. La siguiente configuración de trampa es:

- Trampas de Contabilización RADIUS: verifique para generar trampas para los eventos de contabilización RADIUS.
- Trampas de Fallas de Autenticación RADIUS: verifique para generar trampas para los logins que fallaron.
- Trampas de autenticación exitosa de RADIUS: verifique para generar trampas para los logins que se han realizado correctamente.

RADIUS Server Global Settings

RADIUS Server Status: Enable

Authentication Port: sec (Range: 1 - 65535, Default: 1812)

Accounting Port: sec (Range: 1 - 65535, Default: 1813)

Trap Settings

RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Paso 4. Haga clic en **Aplicar** para guardar los parámetros.

Teclas de servidor RADIUS

Paso 1. Vaya a **Security > RADIUS Server > RADIUS Server Keys**. Se abre la página *RADIUS Server Key*.

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Paso 2. En la sección *Tabla de claves secretas*, haga clic en **Agregar...** para agregar una clave secreta.

RADIUS Server Keys

Default Key: Keep existing default key
 Encrypted
 Plaintext (0/128 characters used)

MD5 Digest:

Apply

Cancel

Secret Key Table

<input type="checkbox"/>	NAS Address	Secret Key's MD5
--------------------------	-------------	------------------

0 results found.

Add...

Edit...

Delete

Paso 3. Se abre la página *Agregar clave secreta*. En el campo *NAS Address*, ingrese la dirección del switch que contiene el cliente RADIUS. En este ejemplo, usaremos la dirección IP 192.168.1.101 como nuestro cliente RADIUS.

NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key: Use default key
 Encrypted
 Plaintext (0/128 characters used)

Apply

Close

Paso 4. Seleccione uno de los botones de opción que se utiliza como *clave secreta*. Las siguientes opciones son:

- Utilice la clave predeterminada: para los servidores especificados, el dispositivo intenta autenticar el cliente RADIUS mediante la cadena de clave predeterminada existente.
- Cifrado: para cifrar las comunicaciones mediante el algoritmo Message-Digest 5 (MD5), introduzca la clave de forma cifrada.
- Texto sin formato: introduzca la cadena de clave en el modo de texto sin formato.

En este ejemplo, seleccionaremos *texto sin formato* y usaremos la palabra **ejemplo** como nuestra *clave secreta*. Después de pulsar aplicar, la clave se mostrará en un formulario cifrado.

Nota: No recomendamos utilizar la palabra **ejemplo** como clave secreta. Utilice una clave más fiable. Se pueden utilizar hasta 128 caracteres. Si tu contraseña es demasiado compleja para recordarla, entonces es una buena contraseña, pero aún mejor si puedes convertir la contraseña en una frase de paso memorable con caracteres y números especiales reemplazando las vocales — "P@55w0rds@reH@rdT0Remember". Es mejor no usar ninguna palabra que se encuentre en un diccionario. Es mejor elegir una frase y cambiar algunas letras por caracteres y números especiales. Consulte esta publicación [del blog de Cisco](#) para obtener más detalles.

NAS Address: 192.168.1.101 (IPv4 or IPv6 Address)

Secret Key:
 Use default key
 Encrypted
 Plaintext
 (128 characters used)

Paso 5. Haga clic en **Aplicar** para guardar la configuración. La clave secreta se cifra ahora con MD5. MD5 es una función hash criptográfica que toma un trozo de datos y crea un resultado hexadecimal único que normalmente no se puede reproducir. MD5 utiliza un valor hash de 128 bits.

RADIUS Server Keys

Default Key:
 Keep existing default key
 Encrypted
 Plaintext
 (0/128 characters used)

MD5 Digest:

Secret Key Table

<input type="checkbox"/>	NAS Address	Secret Key's MD5
<input type="checkbox"/>	192.168.1.101	1a79a4d60de6718e8e5b326e338ae533

Grupos de servidores RADIUS

Paso 1. Vaya a **Security > RADIUS Server > RADIUS Server Groups**.

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Paso 2. Haga clic en **Add (Agregar)...** para agregar un nuevo grupo de servidores RADIUS.

RADIUS Server Groups

RADIUS Server Group table

<input type="checkbox"/>	Group Name	Privilege Level	Time Range		VLAN ID	VLAN Name
			Name	State		
0 results found.						
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>						

Paso 3. Se abre la página *Agregar grupo de servidores RADIUS*. Introduzca un nombre para el grupo. En este ejemplo, usaremos **MAC802** como nuestro nombre de grupo.

Group Name: (6/32 characters used)

Privilege Level: (Range: 1 - 15, Default: 1)

Time Range: Enable

Time Range Name:

VLAN: None

VLAN ID (Range: 1 - 4094)

VLAN Name (0/32 characters used)

Paso 4. Introduzca el nivel de privilegio de acceso a la administración del grupo en el campo *Nivel de privilegio*. El rango está entre 1 y 15, siendo 15 el más privilegiado y el valor predeterminado es 1. En este ejemplo, dejaremos el nivel de privilegio como 1.

Nota: No vamos a configurar *Time Range* ni *VLAN* en este artículo.

Group Name: (6/32 characters used)

Privilege Level: (Range: 1 - 15, Default: 1)

Time Range: Enable

Time Range Name:

VLAN: None

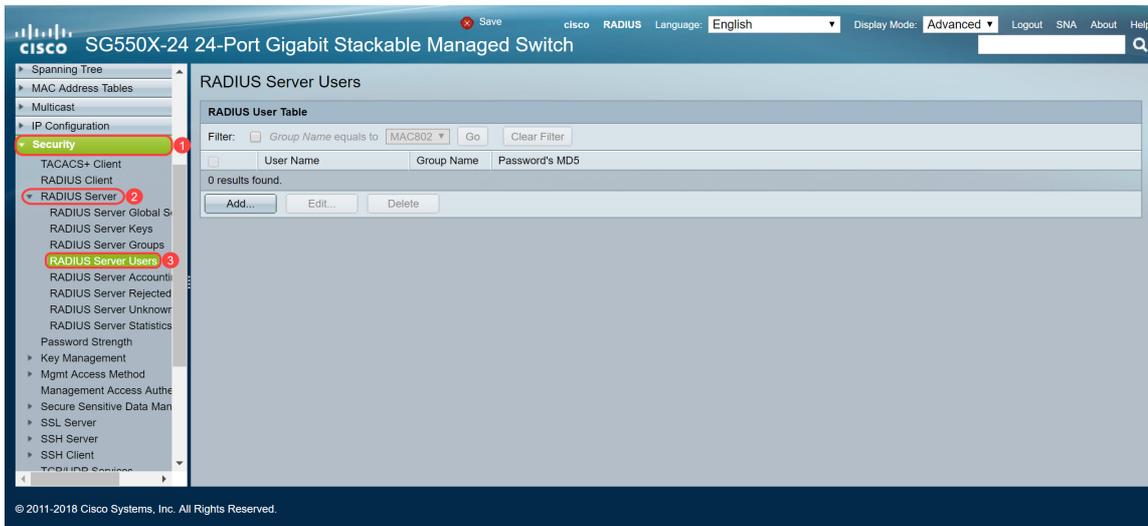
VLAN ID (Range: 1 - 4094)

VLAN Name (0/32 characters used)

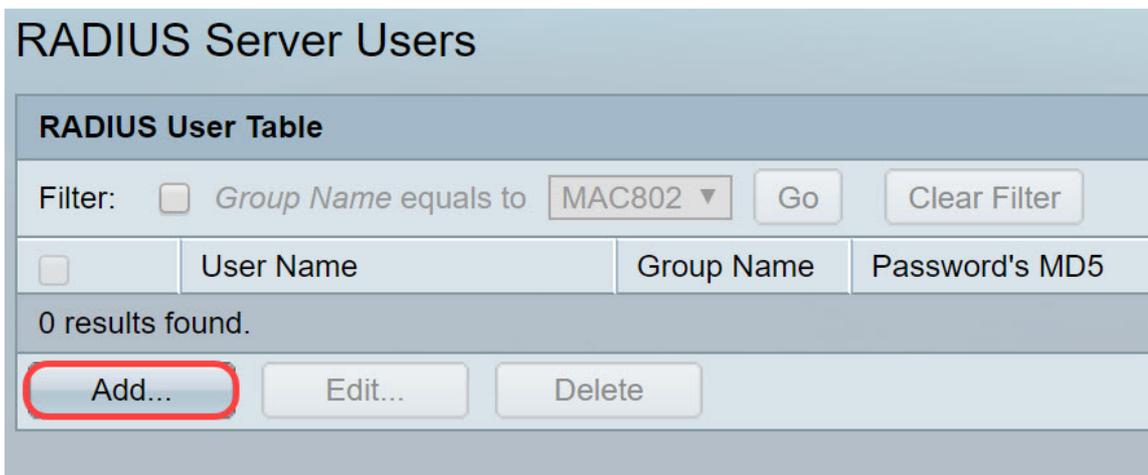
Paso 5. Haga clic en **Aplicar** para guardar los parámetros.

Usuarios del servidor RADIUS

Paso 1. Navegue hasta **Seguridad > Servidor RADIUS > Usuarios de Servidor RADIUS** para configurar usuarios para RADIUS.



Paso 2. Haga clic en Add (Agregar)... para agregar un nuevo usuario.



Paso 3. Se abre la página *Agregar usuario de servidor RADIUS*. En el campo *User Name*, ingrese la dirección MAC de un usuario. En este ejemplo, utilizaremos nuestra dirección MAC Ethernet en nuestro ordenador.

Nota: Se ha difuminado una parte de la dirección MAC.

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802 ▼

Password: Encrypted
 Plaintext (0/32 characters used)

Apply Close

Paso 4. Seleccione un grupo en la lista desplegable *Nombre de grupo*. Como se destaca en el [paso 3](#) de la sección [Grupo de servidores RADIUS](#), seleccionaremos **MAC802** como nuestro Nombre de grupo para este usuario.

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802 ▼

Password: Encrypted
 Plaintext (0/32 characters used)

Apply Close

Paso 5. Seleccione uno de los siguientes botones de opción:

- Cifrado: se utiliza una clave para cifrar las comunicaciones mediante MD5. Para utilizar el cifrado, introduzca la clave en el formulario cifrado.
- Texto sin formato: si no tiene una cadena de clave cifrada (de otro dispositivo), introduzca la cadena de clave en modo de texto sin formato. Se genera y se muestra la cadena de clave cifrada.

Seleccionaremos el *texto sin formato* como nuestra contraseña para este usuario y escribiremos **ejemplo** como nuestra contraseña de texto sin formato.

Nota: No se recomienda utilizar **ejemplo** como contraseña de texto sin formato. Se recomienda utilizar una contraseña más segura.

User Name: 54:EE:75: (17/32 characters used)

Group Name: MAC802

Password: Encrypted Plaintext example (/32 characters used)

Apply Close

Paso 6. Haga clic en **Aplicar** cuando haya terminado de configurar.

Ahora ha terminado de configurar el servidor RADIUS. En la siguiente sección, configuraremos el segundo switch para que sea un autenticador.

Cliente RADIUS

Paso 1. Inicie sesión en la utilidad basada en web de su switch que se configurará como el autenticador y navegue hasta **Security > RADIUS Client**.

SG550X-24 24-Port Gigabit Stackable Managed Switch

Language: English Display Mode: Advanced Logout SNA About Help

Getting Started Dashboard Configuration Wizards Search Status and Statistics Administration Port Management Smartport VLAN Management Spanning Tree MAC Address Tables Multicast IP Configuration

Security 1

TACACS+ Client RADIUS Client 2

RADIUS Server Password Strength Key Management Mgmt Access Method Management Access Authn Secure Sensitive Data Man

RADIUS Client

RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounting is disabled. TACACS+ Accounting is currently Disabled.

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based, Web Authentication) Management Access Both Port Based Access Control and Management Access None

Use Default Parameters

Retries: 3 (Range: 1 - 15, Default: 3)

Timeout for Reply: 3 sec (Range: 1 - 30, Default: 3)

Dead Time: 0 min (Range: 0 - 2000, Default: 0)

Key String: Encrypted Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

Apply Cancel

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Paso 2. Desplácese hacia abajo hasta la sección *Tabla RADIUS* y luego haga clic en **Agregar...** para agregar un servidor RADIUS.

Use Default Parameters

Retries: (Range: 1 - 15, Default: 3)

Timeout for Reply: sec (Range: 1 - 30, Default: 3)

Dead Time: min (Range: 0 - 2000, Default: 0)

Key String: Encrypted
 Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.									

An * indicates that the parameter is using the default global value.

Paso 3. (Opcional) Seleccione si desea especificar el servidor RADIUS por dirección IP o nombre en el campo *Definición de servidor*. En este ejemplo, mantendremos la selección predeterminada de **Por dirección IP.**

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name:

Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default
 User Defined sec (Range: 1 - 30, Default: 3)

Authentication Port: (Range: 0 - 65535, Default: 1812)

Accounting Port: (Range: 0 - 65535, Default: 1813)

Retries: Use Default
 User Defined (Range: 1 - 15, Default: 3)

Dead Time: Use Default
 User Defined min (Range: 0 - 2000, Default: 0)

Usage Type: Login
 802.1x
 All

Paso 4. (Opcional) Seleccione la versión de la dirección IP del servidor RADIUS en el campo *Versión IP*. Conservaremos la selección predeterminada de la **Versión 4 para este ejemplo.**

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name:

Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default
 User Defined sec (Range: 1 - 30, Default: 3)

Authentication Port: (Range: 0 - 65535, Default: 1812)

Accounting Port: (Range: 0 - 65535, Default: 1813)

Retries: Use Default
 User Defined (Range: 1 - 15, Default: 3)

Dead Time: Use Default
 User Defined min (Range: 0 - 2000, Default: 0)

Usage Type: Login
 802.1x
 All

Paso 5. Introduzca en el servidor RADIUS por dirección IP o nombre. Entraremos la dirección IP de **192.168.1.100 en el campo *Server IP Address/Name*.**

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.100

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Paso 6. Introduzca la prioridad del servidor. La prioridad determina el orden en que el dispositivo intenta ponerse en contacto con los servidores para autenticar a un usuario. El dispositivo comienza con el servidor RADIUS de mayor prioridad primero. El cero es la prioridad más alta.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.100

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Paso 7. Introduzca la cadena de clave utilizada para autenticar y cifrar la comunicación entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la clave configurada en el servidor RADIUS. Se puede ingresar en formato **cifrado** o **texto sin formato**. Si se selecciona **Usar valor predeterminado**, el dispositivo intenta autenticarse en el servidor RADIUS utilizando la cadena de clave predeterminada. Utilizaremos el **texto definido por el usuario (texto sin formato)** e introduciremos el **ejemplo** clave.

Nota: Dejaremos el resto de la configuración como predeterminada. Puede configurarlos si lo desea.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

Server IP Address/Name:

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted)
 User Defined (Plaintext) (7/128 characters used)

Timeout for Reply: Use Default User Defined sec (Range: 1 - 30, Default: 3)

Authentication Port: (Range: 0 - 65535, Default: 1812)

Accounting Port: (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Paso 8. Haga clic en **Aplicar** para guardar la configuración.

Propiedades de autenticación 802.1X

La página de propiedades se utiliza para habilitar globalmente la autenticación de puerto/dispositivo. Para que la autenticación funcione, debe activarse tanto de forma global como individual en cada puerto.

Paso 1. Vaya a **Seguridad > Autenticación 802.1X > Propiedades**.

The screenshot shows the Cisco configuration interface for an SG550X-24 switch. The left sidebar shows the navigation menu with 'Security' expanded and '802.1X Authentication' selected. The main area displays the 'Properties' page for 802.1X authentication. The 'Port-Based Authentication' checkbox is checked. The 'Authentication Method' is set to 'RADIUS'. The 'Guest VLAN' is set to '1'. The 'Guest VLAN Timeout' is set to 'Immediate'. The 'Trap Settings' section shows various traps are disabled.

Paso 2. Marque la casilla **Enable** para habilitar la autenticación basada en puerto.

Properties

Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✦ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
Trap Settings	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input type="checkbox"/> Enable
MAC Authentication Success Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

Paso 3. Seleccione los métodos de autenticación de usuario. Elegiremos RADIUS como nuestro método de autenticación. Las siguientes opciones son:

- RADIUS, Ninguno: realice primero la autenticación de puerto mediante el servidor RADIUS. Si no se recibe ninguna respuesta de RADIUS (por ejemplo, si el servidor está inactivo), no se realiza ninguna autenticación y se permite la sesión. Si el servidor está disponible pero las credenciales del usuario son incorrectas, se deniega el acceso y se finaliza la sesión.
- RADIUS: autentique al usuario en el servidor RADIUS. Si no se realiza ninguna autenticación, la sesión no está permitida.
- Ninguno: no autentique al usuario. Permita la sesión.

Properties

Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✦ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
Trap Settings	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input type="checkbox"/> Enable
MAC Authentication Success Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

Paso 4. (Opcional) Marque la casilla de verificación **Enable** para *Trampas de Fallas de Autenticación MAC* y *Trampas de Éxito de Autenticación MAC*. Esto generará una trampa si la autenticación MAC falla o se realiza correctamente. En este ejemplo, habilitaremos tanto *Trampas de Fallas de Autenticación MAC* como *Trampas de Éxito de Autenticación MAC*.

Properties

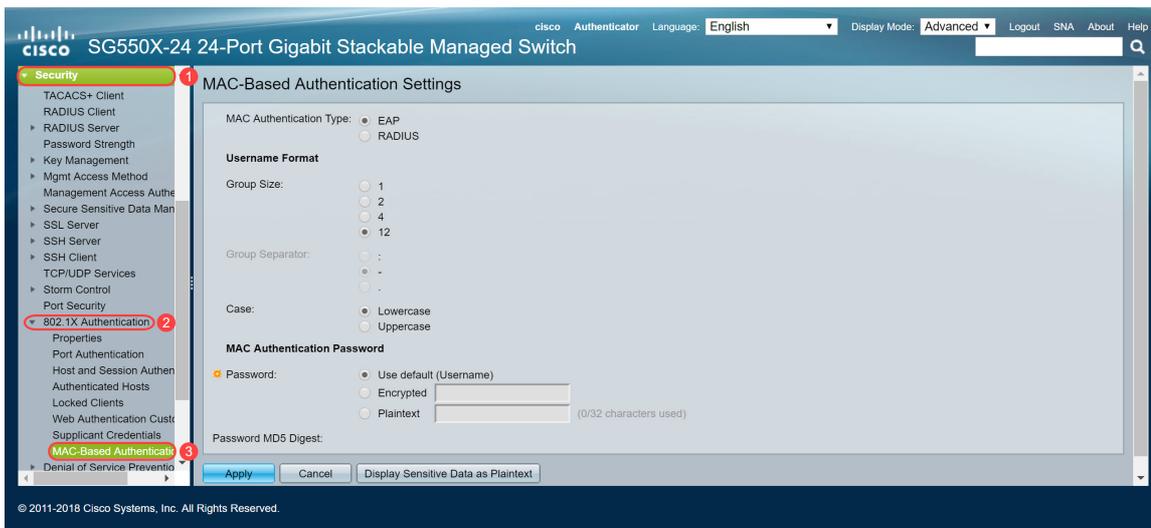
Port-Based Authentication:	<input checked="" type="checkbox"/> Enable
Authentication Method:	<input type="radio"/> RADIUS, None <input checked="" type="radio"/> RADIUS <input type="radio"/> None
Guest VLAN:	<input type="checkbox"/> Enable
Guest VLAN ID:	1 ▾
✦ Guest VLAN Timeout:	<input checked="" type="radio"/> Immediate <input type="radio"/> User Defined <input type="text"/> sec (Range: 30 - 180)
Trap Settings	
802.1x Authentication Failure Traps:	<input type="checkbox"/> Enable
802.1x Authentication Success Traps:	<input type="checkbox"/> Enable
MAC Authentication Failure Traps:	<input checked="" type="checkbox"/> Enable
MAC Authentication Success Traps:	<input checked="" type="checkbox"/> Enable
Supplicant Authentication Failure Traps:	<input type="checkbox"/> Enable
Supplicant Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Failure Traps:	<input type="checkbox"/> Enable
Web Authentication Success Traps:	<input type="checkbox"/> Enable
Web Authentication Quiet Traps:	<input type="checkbox"/> Enable

Paso 5. Haga clic en Apply (Aplicar).

Configuración de autenticación basada en MAC de autenticación 802.1X

Esta página permite configurar varios parámetros aplicables a la autenticación basada en MAC.

Paso 1. Vaya a **Seguridad > Autenticación 802.1X > Configuración de autenticación basada en MAC**.



Paso 2. En *Tipo de autenticación MAC*, seleccione una de las siguientes opciones:

- EAP: utilice RADIUS con encapsulación EAP para el tráfico entre el switch (cliente RADIUS) y el servidor RADIUS, que autentica un suplicante basado en MAC.
- RADIUS: utilice RADIUS sin encapsulación EAP para el tráfico entre el switch (cliente RADIUS) y el servidor RADIUS, que autentica un suplicante basado en MAC.

En este ejemplo, elegiremos RADIUS como nuestro tipo de autenticación MAC.

MAC-Based Authentication Settings

MAC Authentication Type: EAP
 RADIUS

Username Format

Group Size: 1
 2
 4
 12

Group Separator: :
 -
 .

Case: Lowercase
 Uppercase

MAC Authentication Password

✱ Password: Use default (Username)
 Encrypted
 Plaintext (0/32 characters used)

Password MD5 Digest:

Paso 3. En el *Formato de nombre de usuario*, seleccione el número de caracteres ASCII entre los delimitadores de la dirección MAC enviada como nombre de usuario. En este caso, elegiremos 2 como nuestro tamaño de grupo.

Nota: Asegúrese de que el formato del nombre de usuario sea el mismo que el que ingresó la dirección MAC en la sección [Usuarios del servidor Radius](#).

MAC-Based Authentication Settings

MAC Authentication Type: EAP
 RADIUS

Username Format

Group Size: 1
 2
 4
 12

Group Separator: :
 -
 .

Case: Lowercase
 Uppercase

MAC Authentication Password

 Password: Use default (Username)
 Encrypted
 Plaintext (0/32 characters used)

Password MD5 Digest:

Apply

Cancel

Display Sensitive Data as Plaintext

Paso 4. Seleccione el carácter utilizado como delimitador entre los grupos de caracteres definidos en la dirección MAC. En este ejemplo, seleccionaremos : como nuestro separador de grupo.

MAC-Based Authentication Settings

MAC Authentication Type: EAP
 RADIUS

Username Format

Group Size: 1
 2
 4
 12

Group Separator: :
 -
 .

Case: Lowercase
 Uppercase

MAC Authentication Password

✱ Password: Use default (Username)
 Encrypted
 Plaintext (0/32 characters used)

Password MD5 Digest:

Paso 5. En el campo *Case*, seleccione **Low-Case** o **Uppercase** para enviar el nombre de usuario en mayúsculas o minúsculas.

MAC-Based Authentication Settings

MAC Authentication Type: EAP
 RADIUS

Username Format

Group Size: 1
 2
 4
 12

Group Separator: :
 -
 .

Case: Lowercase
 Uppercase

MAC Authentication Password

✱ Password: Use default (Username)
 Encrypted
 Plaintext (0/32 characters used)

Password MD5 Digest:

Paso 6. La contraseña define cómo el switch utilizará para la autenticación a través del servidor RADIUS. Seleccione una de las siguientes opciones:

- Usar valor predeterminado (Nombre de usuario): seleccione esta opción para utilizar el nombre de usuario definido como la contraseña.
- Cifrado: defina una contraseña en formato cifrado.
- Texto sin formato: defina una contraseña en formato de texto sin formato.

MAC-Based Authentication Settings

MAC Authentication Type: EAP
 RADIUS

Username Format

Group Size: 1
 2
 4
 12

Group Separator: :
 -
 .

Case: Lowercase
 Uppercase

MAC Authentication Password

✱ Password: Use default (Username)
 Encrypted
 Plaintext (7/32 characters used)

Password MD5 Digest:

Nota: *Password Message-Digest Algorithm 5 (MD5) Digest muestra la contraseña MD5 Digest.* MD5 es una función hash criptográfica que toma un trozo de datos y crea un resultado hexadecimal único que normalmente no se puede reproducir. MD5 utiliza un valor hash de 128 bits.

Paso 7. Haga clic en **Aplicar** y la configuración se guardará en el archivo Configuración en ejecución.

Autenticación de host de autenticación 802.1X y autenticación de sesión

La página *Autenticación de host y sesión* habilita la definición del modo en el que 802.1X opera en el puerto y la acción que se debe realizar si se ha detectado una violación.

Paso 1. Vaya a **Seguridad > Autenticación 802.1X > Autenticación de host y sesión**.

SG550X-24 24-Port Gigabit Stackable Managed Switch

Host and Session Authentication

Host and Session Authentication Table

Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Host Authentication	Single Host			
			Action on Violation	Traps	Trap Frequency	Number of Violations
<input type="radio"/>	1	GE1	Multiple Host (802.1X)			
<input type="radio"/>	2	GE2	Multiple Host (802.1X)			
<input type="radio"/>	3	GE3	Multiple Host (802.1X)			
<input type="radio"/>	4	GE4	Multiple Host (802.1X)			
<input type="radio"/>	5	GE5	Multiple Host (802.1X)			
<input type="radio"/>	6	GE6	Multiple Host (802.1X)			
<input type="radio"/>	7	GE7	Multiple Host (802.1X)			
<input type="radio"/>	8	GE8	Multiple Host (802.1X)			
<input type="radio"/>	9	GE9	Multiple Host (802.1X)			
<input type="radio"/>	10	GE10	Multiple Host (802.1X)			
<input type="radio"/>	11	GE11	Multiple Host (802.1X)			
<input type="radio"/>	12	GE12	Multiple Host (802.1X)			
<input type="radio"/>	13	GE13	Multiple Host (802.1X)			
<input type="radio"/>	14	GE14	Multiple Host (802.1X)			
<input type="radio"/>	15	GE15	Multiple Host (802.1X)			

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Paso 2. Seleccione el puerto que desea configurar la autenticación de host. En este ejemplo, configuraremos GE1 cuando esté conectado a un host final.

Host and Session Authentication

Host and Session Authentication Table

Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Host Authentication	Single Host			
			Action on Violation	Traps	Trap Frequency	Number of Violations
<input checked="" type="radio"/>	1	GE1	Multiple Host (802.1X)			
<input type="radio"/>	2	GE2	Multiple Host (802.1X)			
<input type="radio"/>	3	GE3	Multiple Host (802.1X)			
<input type="radio"/>	4	GE4	Multiple Host (802.1X)			
<input type="radio"/>	5	GE5	Multiple Host (802.1X)			
<input type="radio"/>	6	GE6	Multiple Host (802.1X)			
<input type="radio"/>	7	GE7	Multiple Host (802.1X)			
<input type="radio"/>	8	GE8	Multiple Host (802.1X)			
<input type="radio"/>	9	GE9	Multiple Host (802.1X)			
<input type="radio"/>	10	GE10	Multiple Host (802.1X)			
<input type="radio"/>	11	GE11	Multiple Host (802.1X)			
<input type="radio"/>	12	GE12	Multiple Host (802.1X)			
<input type="radio"/>	13	GE13	Multiple Host (802.1X)			
<input type="radio"/>	14	GE14	Multiple Host (802.1X)			

Paso 3. Haga clic en **Editar...** para configurar el puerto.

<input type="radio"/>	10	GE10	Multiple Host (802.1X)
<input type="radio"/>	11	GE11	Multiple Host (802.1X)
<input type="radio"/>	12	GE12	Multiple Host (802.1X)
<input type="radio"/>	13	GE13	Multiple Host (802.1X)
<input type="radio"/>	14	GE14	Multiple Host (802.1X)
<input type="radio"/>	15	GE15	Multiple Host (802.1X)
<input type="radio"/>	16	GE16	Multiple Host (802.1X)
<input type="radio"/>	17	GE17	Multiple Host (802.1X)
<input type="radio"/>	18	GE18	Multiple Host (802.1X)
<input type="radio"/>	19	GE19	Multiple Host (802.1X)
<input type="radio"/>	20	GE20	Multiple Host (802.1X)
<input type="radio"/>	21	GE21	Multiple Host (802.1X)
<input type="radio"/>	22	GE22	Multiple Host (802.1X)
<input type="radio"/>	23	GE23	Multiple Host (802.1X)
<input type="radio"/>	24	GE24	Multiple Host (802.1X)
<input type="radio"/>	25	XG1	Multiple Host (802.1X)
<input type="radio"/>	26	XG2	Multiple Host (802.1X)
<input type="radio"/>	27	XG3	Multiple Host (802.1X)
<input type="radio"/>	28	XG4	Multiple Host (802.1X)

Copy Settings... Edit...

Paso 4. En el campo *Host Authentication*, seleccione una de las siguientes opciones:

1. Modo de host único

- Se autoriza un puerto si hay un cliente autorizado. Sólo se puede autorizar un host en un puerto.
- Cuando un puerto no está autorizado y la VLAN de invitado está habilitada, el tráfico sin etiquetas se reasigna a la VLAN de invitado. El tráfico etiquetado se descarta a menos que pertenezca a la VLAN de invitado o a una VLAN no autenticada. Si una VLAN de invitado no está habilitada en el puerto, sólo se puentea el tráfico etiquetado que pertenece a las VLAN no autenticadas.
- Cuando se autoriza un puerto, el tráfico no etiquetado y etiquetado del host autorizado se puentea en función de la configuración del puerto de pertenencia de VLAN estática. Se descarta el tráfico de otros hosts.
- Un usuario puede especificar que el tráfico sin etiquetas del host autorizado se remapeará a una VLAN que es asignada por un servidor RADIUS durante el proceso de autenticación. El tráfico etiquetado se descarta a menos que pertenezca a la VLAN asignada por RADIUS o a las VLAN no autenticadas. La asignación de VLAN RADIUS en un puerto se configura en la página *de autenticación de puerto*.

2. Modo de host múltiple

- Se autoriza un puerto si hay al menos un cliente autorizado.
- Cuando un puerto no está autorizado y se habilita una VLAN de invitado, el tráfico sin etiquetas se reasigna a la VLAN de invitado. El tráfico etiquetado se descarta a menos que

pertenezca a la VLAN de invitado o a una VLAN no autenticada. Si la VLAN de invitado no está habilitada en un puerto, sólo se puentea el tráfico etiquetado que pertenece a VLAN no autenticadas.

- Cuando se autoriza un puerto, se puentea el tráfico sin etiquetas y etiquetado de todos los hosts conectados al puerto, en función de la configuración del puerto de pertenencia de VLAN estática.
- Puede especificar que el tráfico sin etiquetas del puerto autorizado se remapeará a una VLAN que es asignada por un servidor RADIUS durante el proceso de autenticación. El tráfico etiquetado se descarta a menos que pertenezca a la VLAN asignada por RADIUS o a las VLAN no autenticadas. La asignación de VLAN RADIUS en un puerto se establece en la página *Autenticación de Puerto*.

3. Modo multisesión

- A diferencia de los modos de host único y host múltiple, un puerto en el modo de sesiones múltiples no tiene un estado de autenticación. Este estado se asigna a cada cliente conectado al puerto.
- El tráfico etiquetado que pertenece a una VLAN no autenticada siempre se puentea independientemente de si el host está autorizado o no.
- El tráfico etiquetado y no etiquetado de hosts no autorizados que no pertenecen a una VLAN no autenticada se reasigna a la VLAN de invitado si se define y se habilita en la VLAN, o se descarta si la VLAN de invitado no está habilitada en el puerto.
- Puede especificar que el tráfico sin etiquetas del puerto autorizado se remapeará a una VLAN que es asignada por un servidor RADIUS durante el proceso de autenticación. El tráfico etiquetado se descarta a menos que pertenezca a la VLAN asignada por RADIUS o a las VLAN no autenticadas. La asignación de VLAN RADIUS en un puerto se establece en la página *Autenticación de Puerto*.

Interface: Unit Port

Host Authentication:

- Single Host
- Multiple Host (802.1X)
- Multiple Sessions

Single Host Violation Settings

Action on Violation:

- Protect (Discard)
- Restrict (Forward)
- Shutdown

Traps:

- Enable

Trap Frequency: sec (Range: 1 - 1000000, Default: 10)

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

Nota: Usar *Copiar configuración...* para aplicar la misma configuración de GE1 a varios puertos. Deje el puerto que está conectado al servidor RADIUS como *host múltiple (802.1X)*.

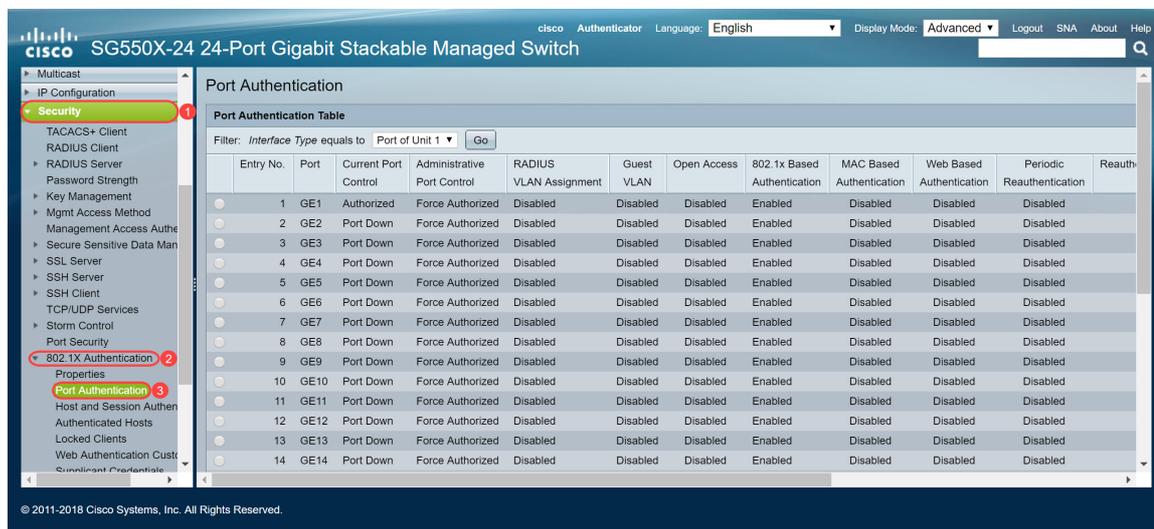
Autenticación del puerto de autenticación 802.1X

La página *Autenticación de Puerto* habilita la configuración de parámetros para cada puerto.

Debido a que algunos de los cambios de configuración sólo son posibles mientras el puerto está en estado Forzar Autorizado, como la autenticación de host, se recomienda cambiar el control de puerto a Forzar Autorizado antes de realizar cambios. Cuando se complete la configuración, devuelva el control de puerto a su estado anterior.

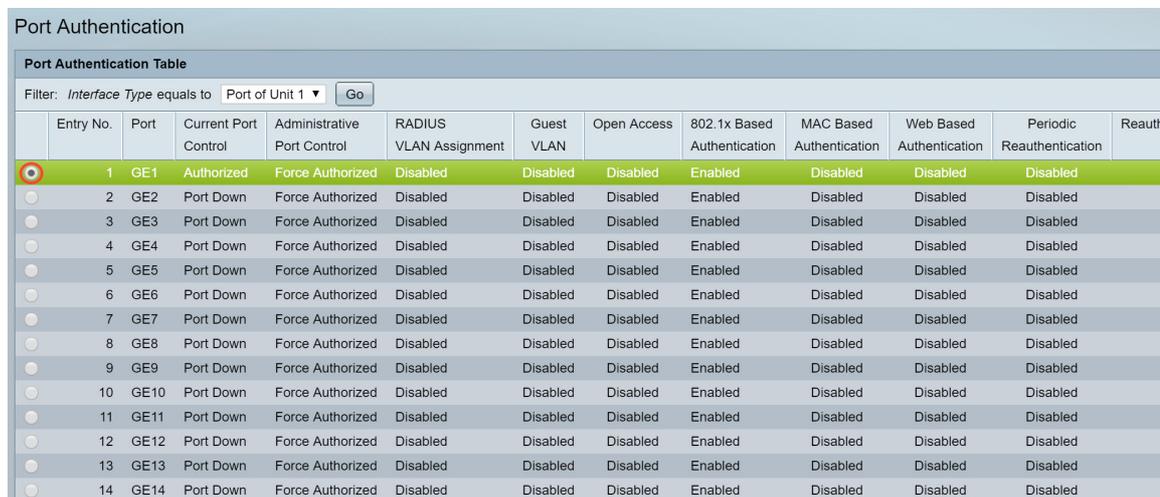
Nota: Sólo configuraremos los ajustes necesarios para la autenticación basada en MAC. El resto de la configuración se dejará como valor predeterminado.

Paso 1. Vaya a **Seguridad > Autenticación 802.1X > Autenticación de puerto.**



Paso 2. Seleccione el puerto que desea configurar la autorización de puerto.

Nota: No configure el puerto al que está conectado el switch. El switch es un dispositivo de confianza, por lo que deja ese puerto como *Autorizado Forzado*.



Paso 3. Desplácese hacia abajo y haga clic en **Editar...** para configurar el puerto.

11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
15	GE15	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
16	GE16	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
17	GE17	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
18	GE18	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
19	GE19	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
20	GE20	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
21	GE21	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
22	GE22	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
23	GE23	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
24	GE24	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
25	XG1	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
26	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
27	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

En la página *Editar autenticación de puerto*, el campo *Control de puerto actual* muestra el estado actual de autorización de puerto. Si el estado es *Authorized*, el puerto es autenticado o el *Administrative Port Control* es *Force Authorized*. A la inversa, si el estado es *Unauthorized*, el puerto no está autenticado o el *Administrative Port Control* es *Force Unauthorized*. Si el solicitante está habilitado en una interfaz, el control de puerto actual será *Supplicant*.

Paso 4. Seleccione el estado de autorización del puerto administrativo. Configure el puerto en **Auto**. Las opciones disponibles son:

- **Forced Unauthorized**: Niega el acceso a la interfaz al mover la interfaz al estado no autorizado. El dispositivo no proporciona servicios de autenticación al cliente a través de la interfaz.
- **Automático**: habilita la autenticación y autorización basadas en puertos en el dispositivo. La interfaz se mueve entre un estado autorizado o no autorizado en función del intercambio de autenticación entre el dispositivo y el cliente.
- **Forced Authorized** : autoriza la interfaz sin autenticación.

Nota: *Forced Authorized* es el valor predeterminado.

Paso 5. En el campo *Autenticación basada en 802.1X*, desmarque la **casilla Habilitar** ya que no vamos a utilizar 802.1X como nuestra autenticación. El valor predeterminado de *Autenticación basada en 802.1x* está habilitado.

Interface: Unit 1 Port GE1

Current Port Control: Authorized

Administrative Port Control: Force Unauthorized Auto Force Authorized

RADIUS VLAN Assignment: Disable Reject Static

Guest VLAN: Enable

Open Access: Enable

802.1x Based Authentication: Enable **Enable**

MAC Based Authentication: Enable **Enable**

Web Based Authentication: Enable

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec (Range: 300 - 4294967295, Default: 3600)

Reauthenticate Now:

Authenticator State: Force Authorized

Time Range: Enable

Time Range Name: Edit

Maximum WBA Login Attempts: Infinite User Defined (Range: 3 - 10)

Maximum WBA Silence Period: Infinite

Paso 6. Marque la casilla de verificación **Enable** para *MAC Based Authentication* ya que queremos habilitar la autenticación de puerto basada en la dirección MAC del solicitante. Sólo se pueden utilizar 8 autenticaciones basadas en MAC en el puerto.

Interface: Unit 1 Port GE1

Current Port Control: Authorized

Administrative Port Control: Force Unauthorized Auto Force Authorized

RADIUS VLAN Assignment: Disable Reject Static

Guest VLAN: Enable

Open Access: Enable

802.1x Based Authentication: Enable **Enable**

MAC Based Authentication: **Enable** Enable

Web Based Authentication: Enable

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec (Range: 300 - 4294967295, Default: 3600)

Reauthenticate Now:

Authenticator State: Force Authorized

Time Range: Enable

Time Range Name: Edit

Maximum WBA Login Attempts: Infinite User Defined (Range: 3 - 10)

Maximum WBA Silence Period: Infinite

Paso 7. Haga clic en **Aplicar** para guardar los cambios.

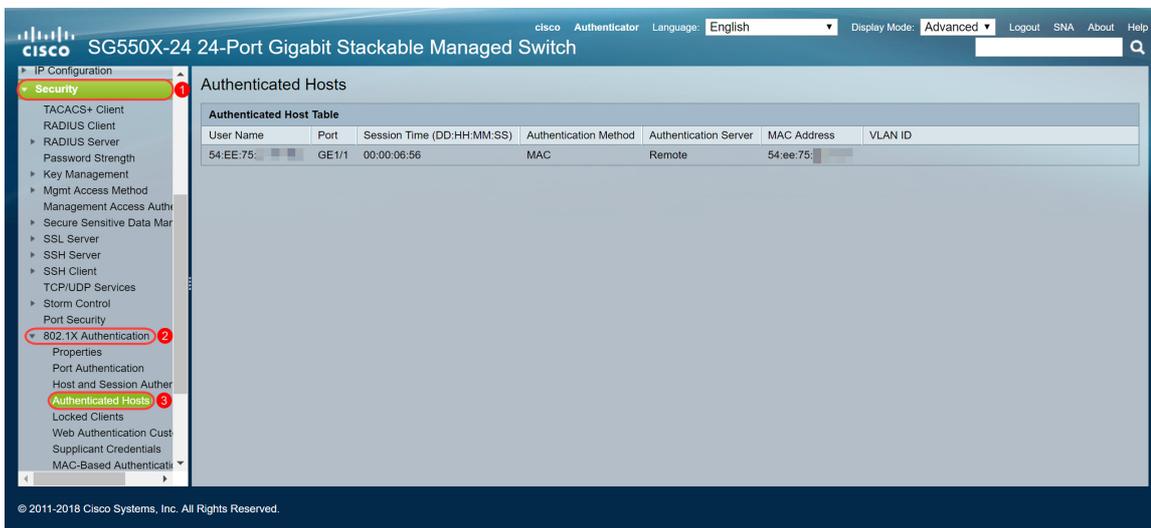
Si desea guardar la configuración, pulse el botón **Guardar** de la parte superior de la pantalla.



Conclusión

Ahora ha configurado correctamente la autenticación basada en MAC en su switch. Para verificar que la autenticación basada en MAC funciona, siga los pasos a continuación.

Paso 1. Navegue hasta **Seguridad > Autenticación 802.1X > Hosts autenticados** para ver detalles sobre los usuarios autenticados.

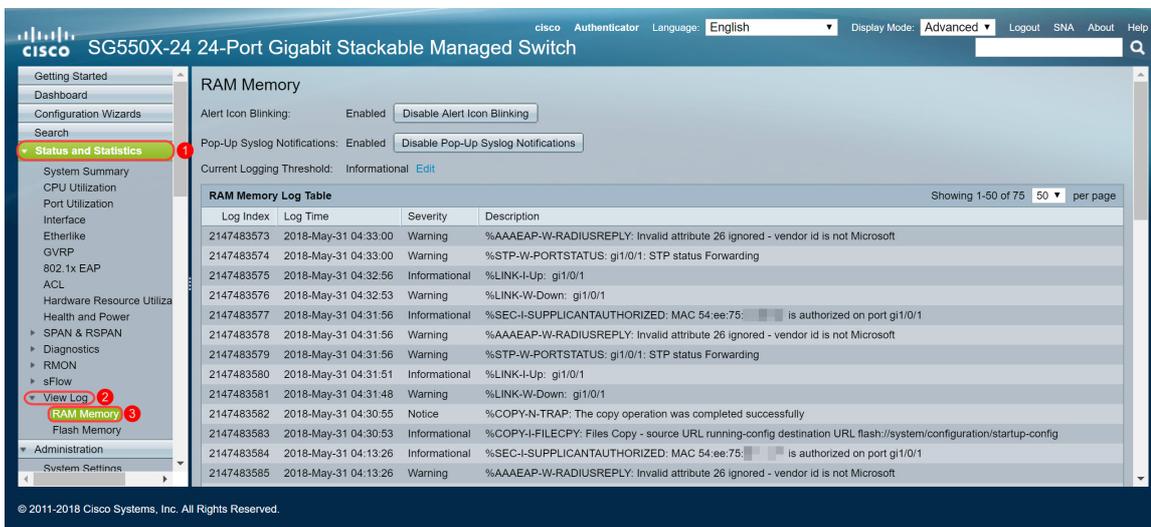


Paso 2. En este ejemplo, puede ver que nuestra dirección Ethernet MAC fue autenticada en la *Tabla de Host Autenticado*. Los campos siguientes se definen como:

- Nombre de usuario: nombres de solicitante que se autenticaron en cada puerto.
- Puerto: número del puerto.
- Tiempo de sesión (DD:HH:MM:SS): cantidad de tiempo durante el cual se autenticó al solicitante y se autorizó su acceso en el puerto.
- Método de autenticación: método por el que se autenticó la última sesión.
- Servidor autenticado: servidor RADIUS.
- Dirección MAC: muestra la dirección MAC del solicitante.
- ID de VLAN: VLAN del puerto.



Paso 3. (Opcional) Navegue hasta **Estado y estadísticas > Ver registro > Memoria RAM**. La página *Memoria RAM* mostrará todos los mensajes guardados en la memoria RAM (caché) en orden cronológico. Las entradas se almacenan en el registro de RAM según la configuración de la página *Configuración de registro*.



Paso 4. En la *Tabla de registro de memoria RAM*, debería ver un mensaje de registro informativo que indica que su dirección MAC está autorizada en el puerto gi1/0/1.

Nota: Parte de la dirección MAC se desdibuja.

2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1

Ver la versión de vídeo de este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)