Configuración de la Autenticación Basada en MAC en un Switch a través de la Interfaz de Línea de Comandos

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 mediante la interfaz de línea de comandos (CLI).

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 administrar tiene una dirección IP estática de 192.168.1.100 y el autenticador tiene una dirección IP estática de 192.168.1.101.

Dispositivos aplicables

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

Versión del software

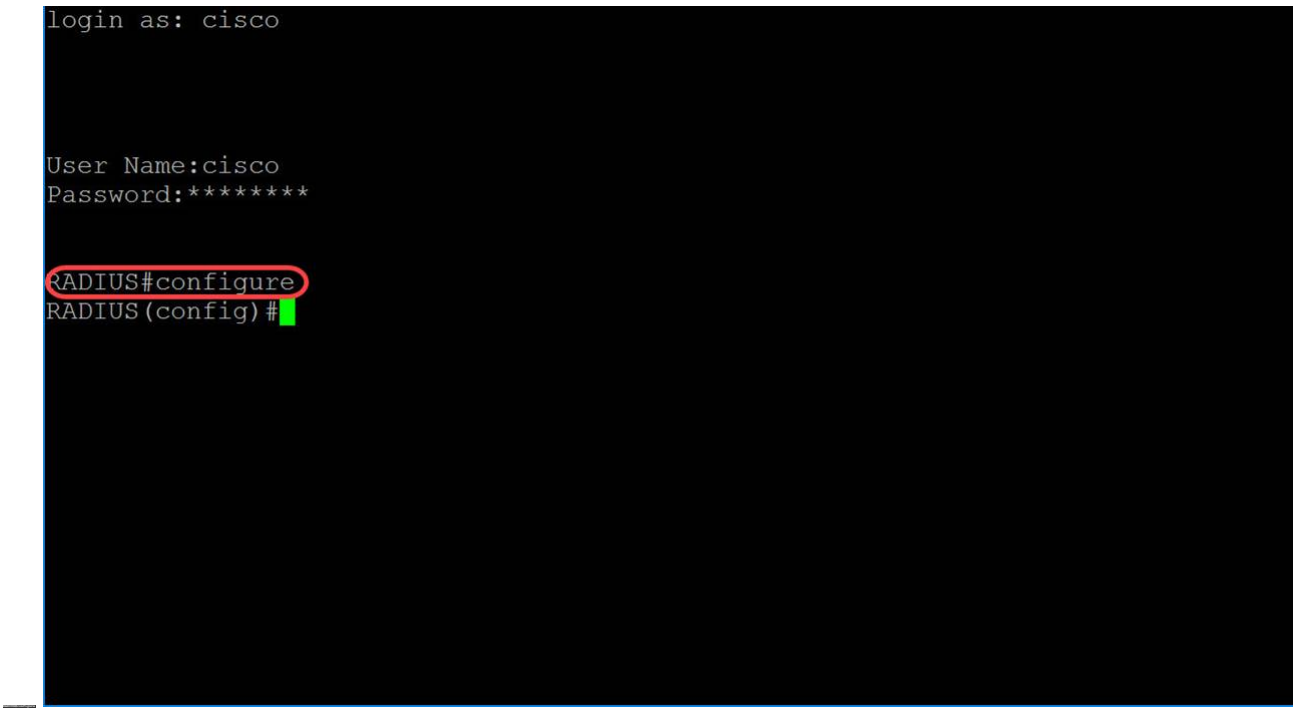
- 2.4.0.94

Configuración del servidor RADIUS en un switch

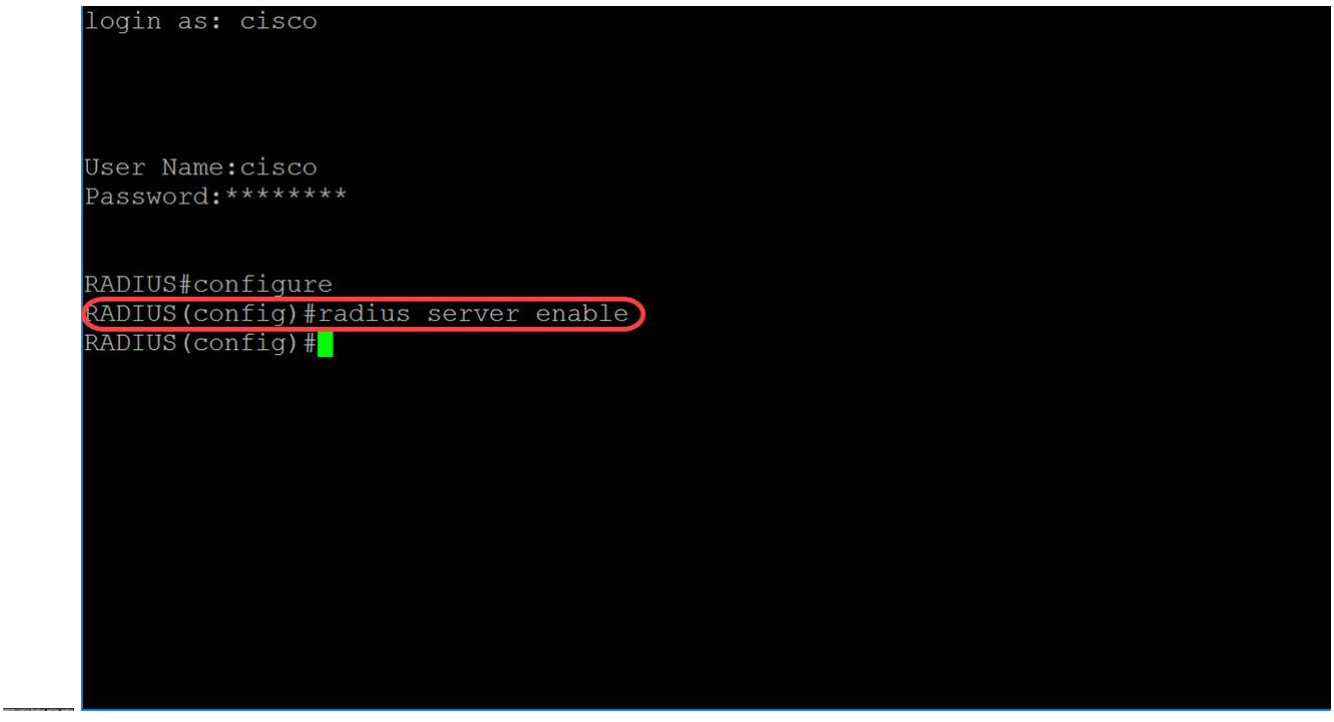
Paso 1. SSH al switch que será el servidor RADIUS. El nombre de usuario y la contraseña predeterminados son cisco/cisco. Si ha configurado un nuevo nombre de usuario o contraseña, introduzca las credenciales en su lugar.

Nota: Para obtener información sobre cómo acceder a un switch SMB a través de SSH o Telnet, haga clic en aquí.

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



Paso 3. Utilice el comando **radius server enable** para habilitar el servidor RADIUS.

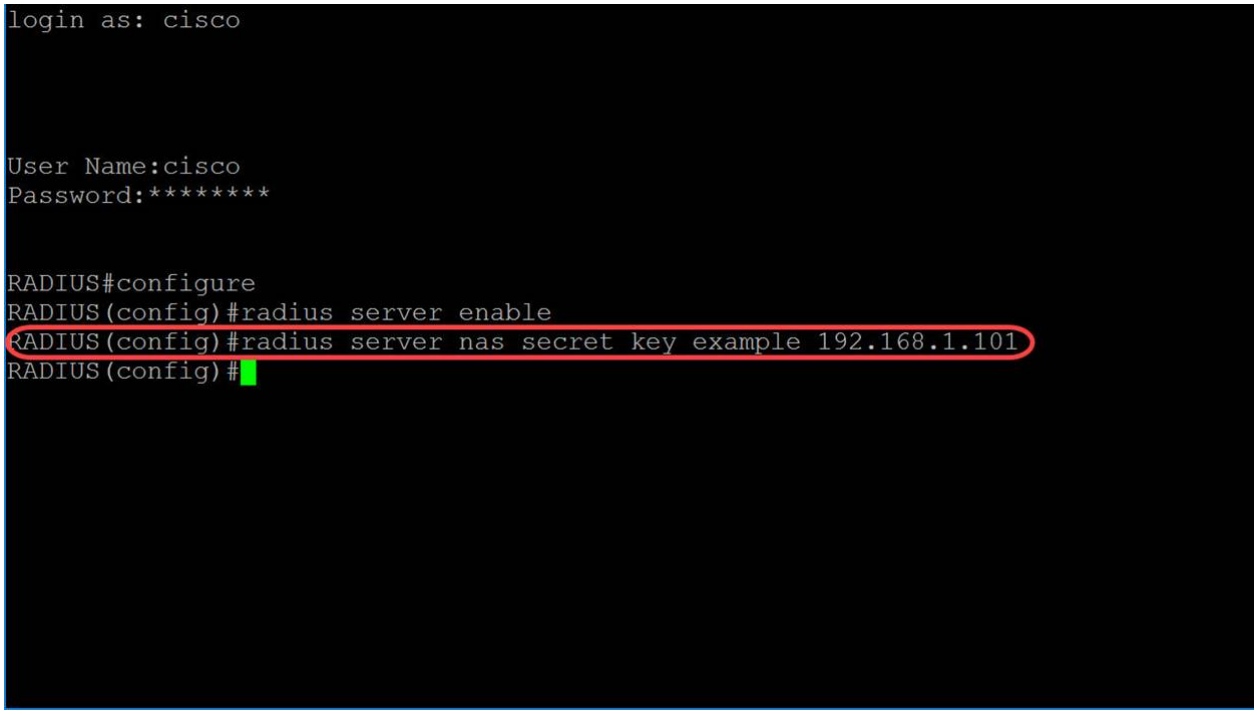


Paso 4. Para crear una clave secreta, utilice el comando **radius server nas secret key** en el

modo Global Configuration. Los parámetros se definen como:

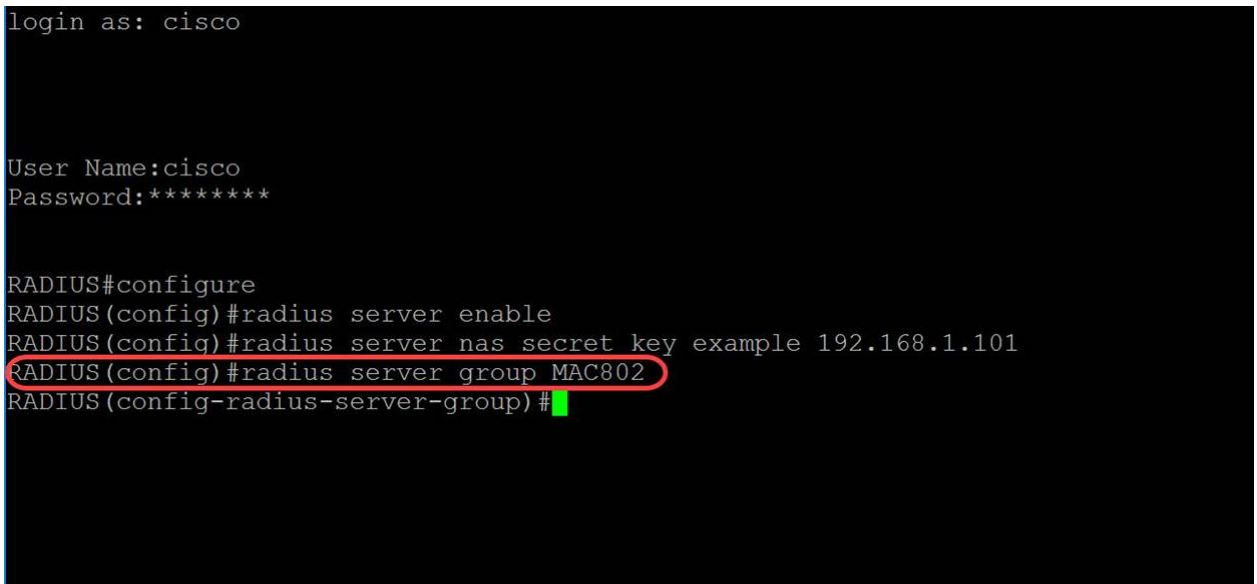
- key: especifica la clave de autenticación y cifrado para las comunicaciones entre el dispositivo y los usuarios del grupo dado. Este intervalo va de 0 a 128 caracteres.
- default: especifica la clave secreta predeterminada que se aplicará para comunicarse con NAS que no tienen una clave privada.
- ip-address: especifica la dirección IP del host del cliente RADIUS. La dirección IP puede ser una dirección IPv4, IPv6 o IPv6z.

En este ejemplo, usaremos el **ejemplo** como nuestra clave y **192.168.1.101** como la dirección IP de nuestro autenticador.



Paso 5. Para entrar en el modo de configuración de grupo de servidores RADIUS y crear un grupo si no existe, utilice el comando radius server group en el modo de configuración global.

En este artículo, usaremos **MAC802** como nuestro nombre de grupo.

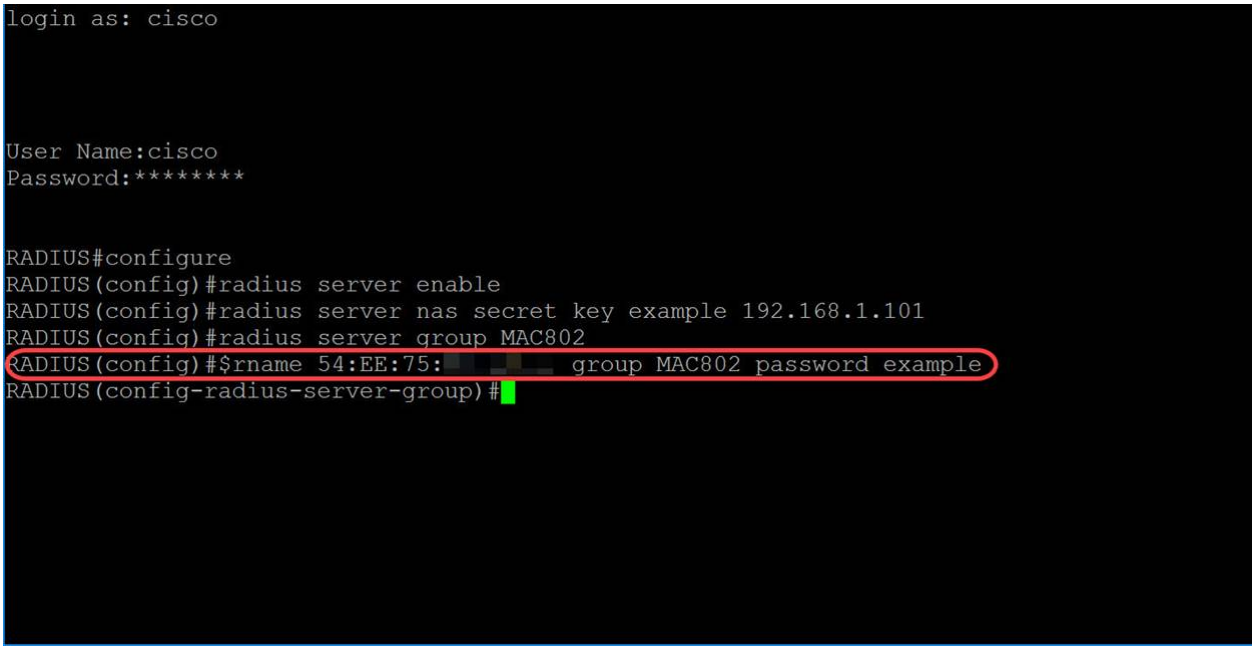


Paso 6. Para crear un usuario, utilice el comando **radius server user** en el modo Global Configuration. Los parámetros se definen como:

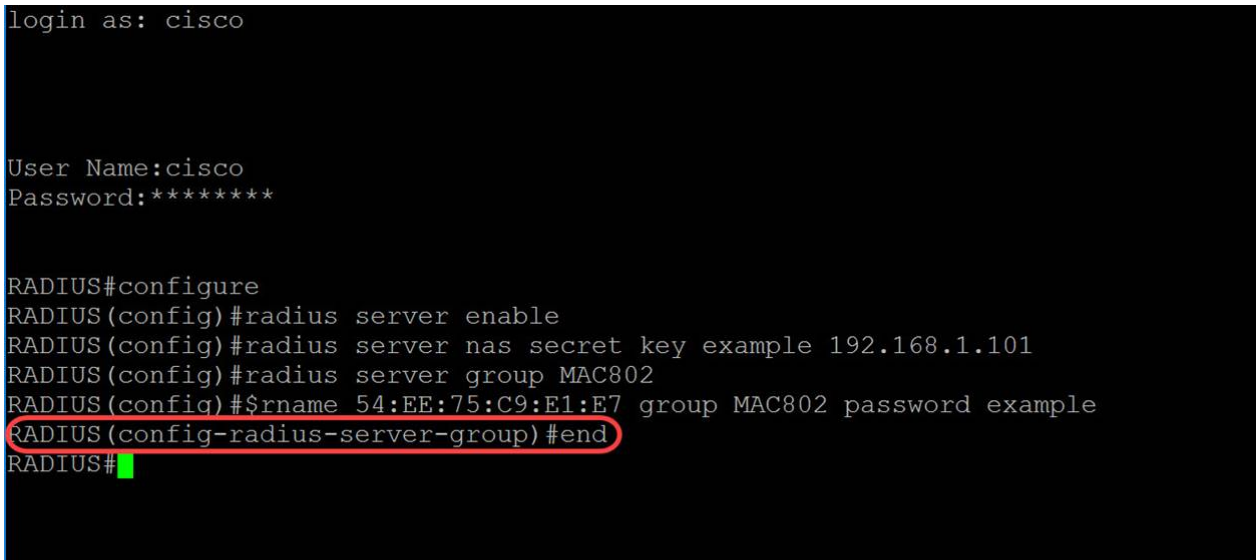
- user-name: especifica el nombre de usuario. La longitud es de 1 a 32 caracteres.
- group-name : especifica el nombre del grupo de usuarios. La longitud del nombre del grupo es de 1 a 32 caracteres.
- unencryption-password: especifica la contraseña de usuario. La longitud puede tener entre 1 y 64 caracteres.

Para este ejemplo, usaremos la dirección MAC de nuestro puerto Ethernet como nuestro nombre de usuario, **MAC802** como nuestro *nombre de grupo* y la **contraseña no cifrada** como ejemplo.

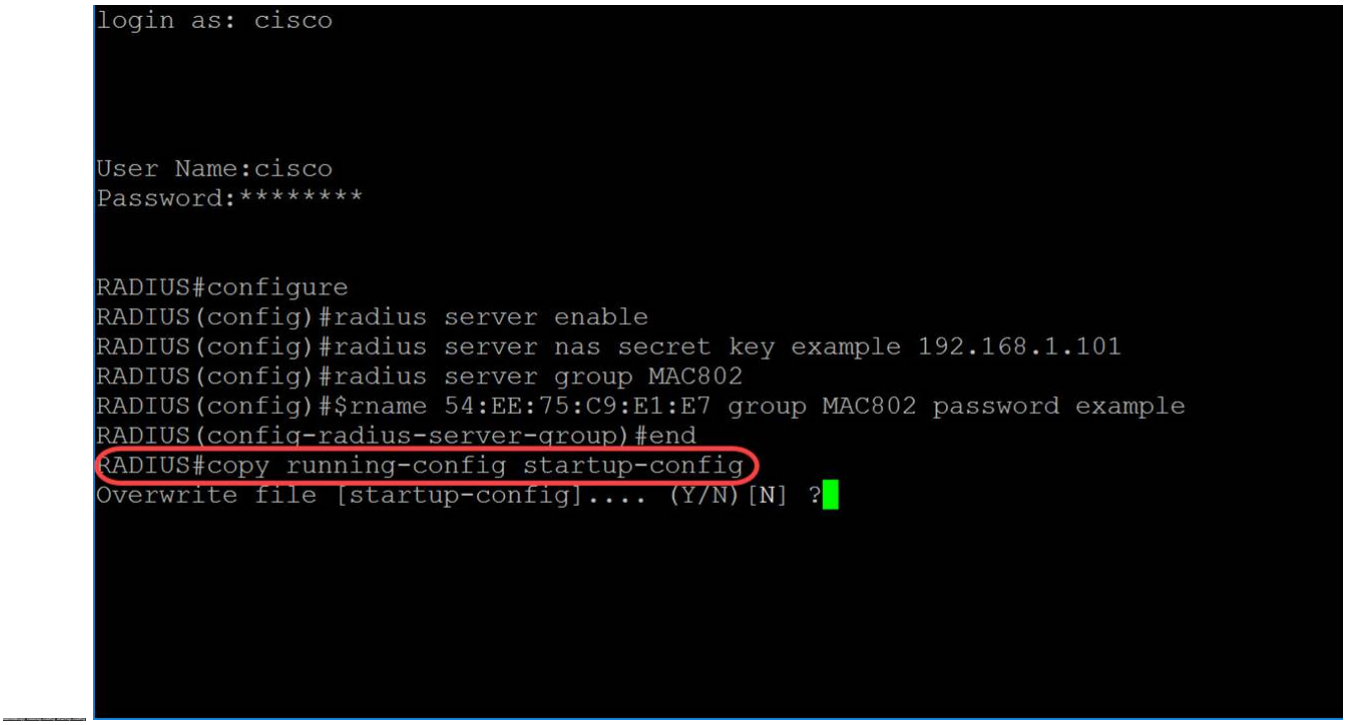
Nota: Algunos de los octetos de la dirección MAC se difuminan. El **ejemplo de** contraseña no es una contraseña segura. Utilice una contraseña más segura, ya que sólo se utilizó como ejemplo. Además, tenga en cuenta que el comando era demasiado largo en la imagen que ajustó automáticamente el comando.



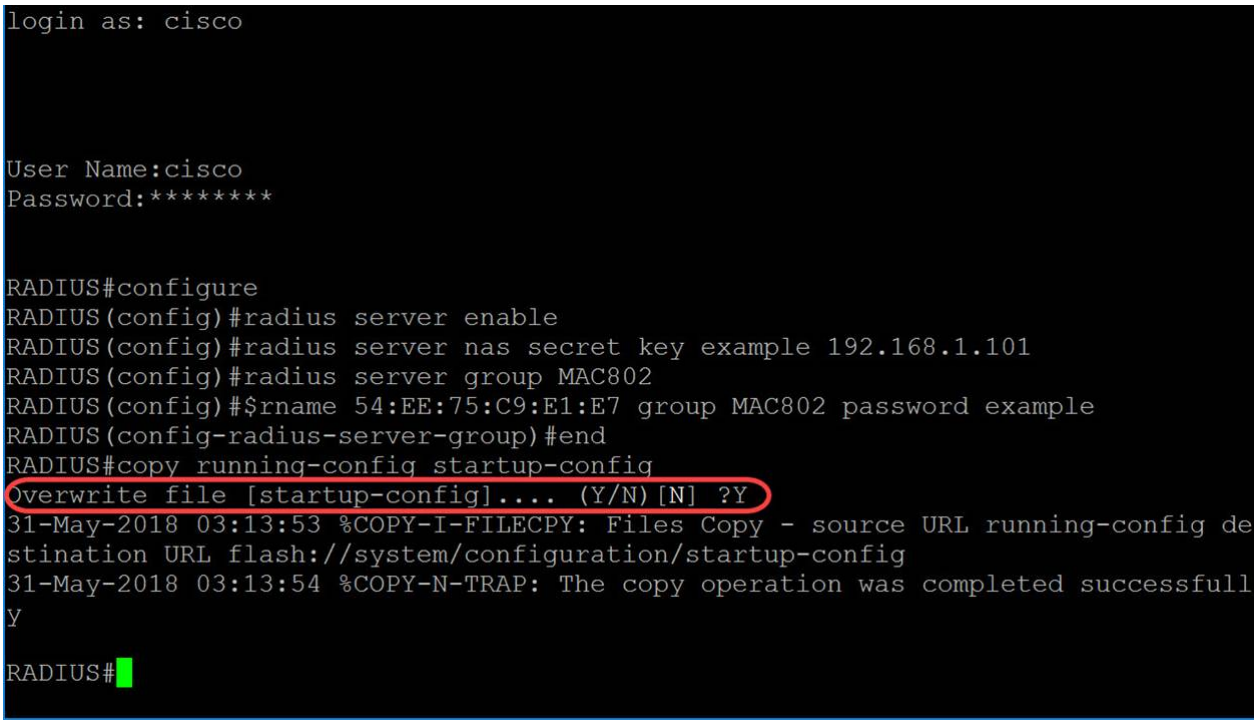
Paso 7. (Opcional) Para finalizar la sesión de configuración actual y volver al modo EXEC privilegiado, utilice el comando **end**.



Paso 8. (Opcional) Para copiar cualquier archivo de un origen a un destino, utilice el comando **copy** en el modo EXEC privilegiado. En este ejemplo, vamos a guardar nuestra configuración en ejecución en startup-config.



Paso 9. (Opcional) Aparecerá un mensaje preguntando si desea sobrescribir el archivo startup-config. Escriba **Y** para sí o **N** para no. Escribiremos **Y** para sobreescribir nuestro archivo startup-config.



Configuración del Switch Authenticator

Paso 1. SSH al switch que será el autenticador. El nombre de usuario y la contraseña predeterminados son cisco/cisco. Si ha configurado un nuevo nombre de usuario o contraseña, introduzca esas credenciales en su lugar.

Nota: Para obtener información sobre cómo acceder a un switch SMB a través de SSH o

Telnet, haga clic en aquí.

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#
```

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

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#configure
Authenticator(config)#
```

Paso 3. Para habilitar 802.1X globalmente, utilice el comando dot1x system-auth-control en el modo Configuración global.

```
login as: cisco



User Name:cisco
Password:*****

Authenticator#configure
Authenticator(config)#dot1x system-auth-control
Authenticator(config)#
```

Paso 4. Utilice el comando **radius-server host** Global Configuration mode para configurar un host de servidor RADIUS. Los parámetros se definen como:

- ip-address: especifica la dirección IP del host del servidor RADIUS. La dirección IP puede ser una dirección IPv4, IPv6 o IPv6z.

- hostname: especifica el nombre de host del servidor RADIUS. Sólo se admite la traducción a direcciones IPv4. La longitud es de 1 a 158 caracteres y la longitud máxima de etiqueta de cada parte del nombre de host es de 63 caracteres.

- auth-port *auth-port-number*: especifica el número de puerto para las solicitudes de autenticación. Si el número de puerto está configurado en 0, el host no se utiliza para la autenticación. El rango está entre 0-65535.

- Acc-port *acct-port-number*: número de puerto para las solicitudes de contabilización. El host no se utiliza para la contabilización si se establece en 0. Si no se especifica, el número de puerto predeterminado es 1813.

- timeout *timeout* : especifica el valor de tiempo de espera en segundos. Este rango oscila entre 1 y 30.

- retransmitir *reintentos* — Especifica el número de retransmisiones de reintento. El rango está entre 1 y 15.

- deadtime *deadtime*: especifica el tiempo en minutos durante el cual las solicitudes de transacción omiten un servidor RADIUS. Varía entre 0 y 2000.

- key *key-string*: Especifica la clave de autenticación y cifrado para todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con el cifrado utilizado en el demonio RADIUS. Para especificar una cadena vacía, introduzca "". La longitud puede tener entre 0 y 128 caracteres. Si se omite este parámetro, se utilizará la clave radius configurada globalmente.

- key *encryption-key-string*: Igual que key-string, pero la clave está en formato cifrado.

- priority *priority*: especifica el orden en que se utilizan los servidores, donde 0 tiene la prioridad más alta. El rango de prioridad está entre 0 y 65535.

- use {login|dot1.x|all}: especifica el tipo de uso del servidor RADIUS. Los valores posibles son:

    - login: Especifica que el servidor RADIUS se utiliza para la autenticación de parámetros de inicio de sesión de usuario.

    - dot1.x: especifica que el servidor RADIUS se utiliza para la autenticación de puertos 802.1x.

    - all: especifica que el servidor RADIUS se utiliza para la autenticación de inicio de sesión del usuario y la autenticación de puerto 802.1x.

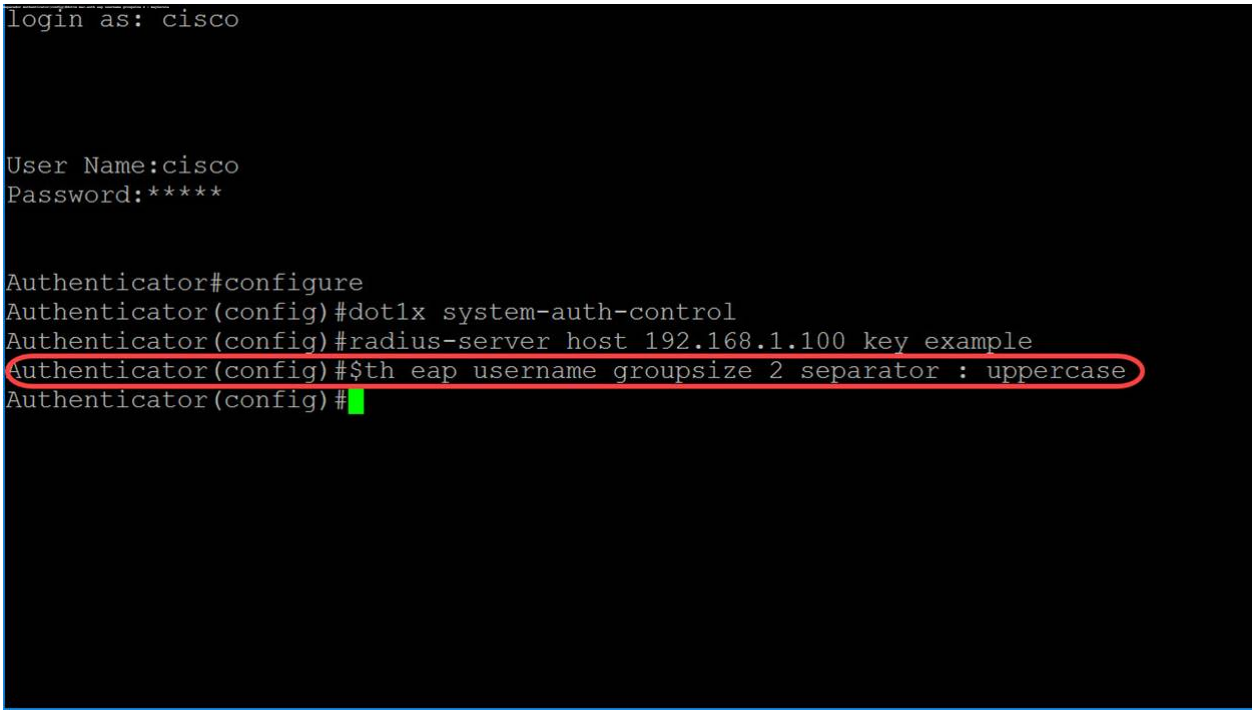
En este ejemplo, sólo se utilizan los parámetros de host y clave. Utilizaremos la dirección IP **192.168.1.100** como dirección IP del servidor RADIUS y la palabra **ejemplo** como cadena de clave.

Paso 5. En la autenticación basada en MAC, el nombre de usuario del solicitante se basa en la dirección MAC del dispositivo solicitante. A continuación se define el formato de este nombre de usuario basado en MAC, que se envía desde el switch al servidor RADIUS, como parte del proceso de autenticación. Los campos siguientes se definen como:

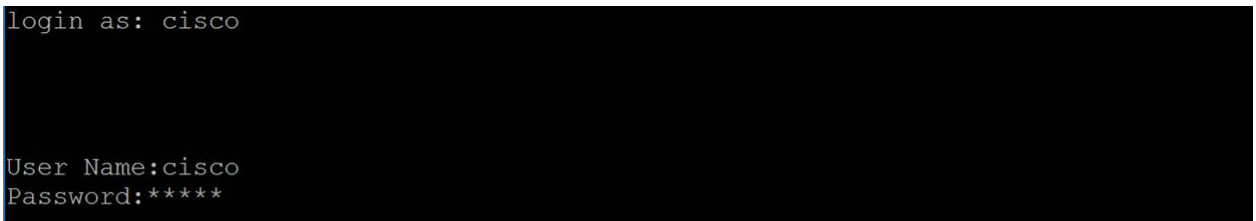
- tipo mac-auth: elija un tipo de autenticación MAC
    - eap: utilice RADIUS con encapsulación EAP para el tráfico entre el switch (cliente RADIUS) y el servidor RADIUS, que autentica un suplicante basado en MAC.
    - RADIUS: utilice RADIUS sin encapsulación EAP para el tráfico entre el switch (cliente RADIUS) y el servidor RADIUS, que autentica un suplicante basado en MAC.
- groupsize — Número de caracteres ASCII entre los delimitadores de la dirección MAC enviada como nombre de usuario. La opción es 1, 2, 4 o 12 caracteres ASCII entre delimitadores.
- separador: carácter utilizado como delimitador entre los grupos de caracteres definidos en la dirección MAC. Las opciones son guiones, puntos o puntos como delimitador.
- case — Enviar nombre de usuario en mayúsculas o minúsculas. Las opciones son minúsculas o mayúsculas.

dot1x mac-auth

En este ejemplo, usaremos **eap** como nuestro tipo de autenticación mac, un tamaño de grupo de **2**, el **colon** como nuestro separador, y enviaremos nuestro nombre de usuario en **mayúscula**.

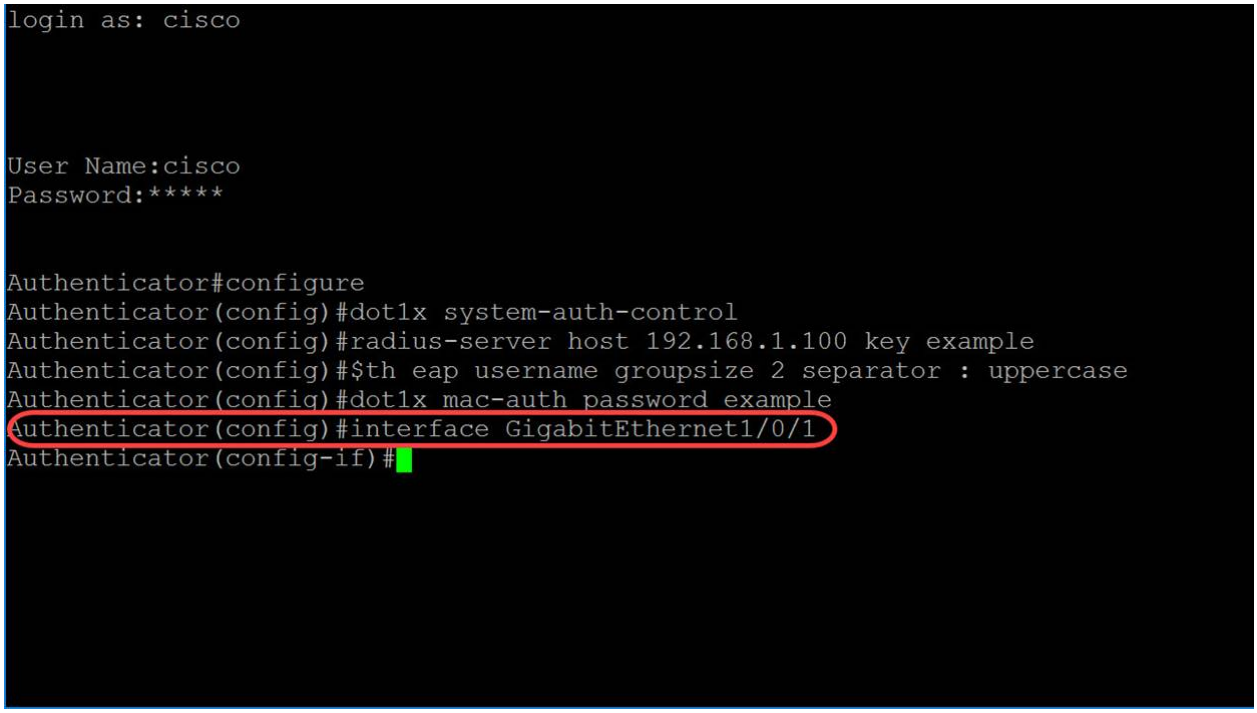


Paso 6. Utilice el siguiente comando para definir la contraseña que el switch utilizará para la autenticación basada en MAC en lugar de la dirección MAC del host. Usaremos la palabra **ejemplo** como contraseña.



Paso 7. Para ingresar al modo de configuración de interfaz para configurar una interfaz, utilice el comando **interface** Global Configuration mode. Configuraremos GigabitEthernet1/0/1 porque nuestro host final está conectado a él.

Nota: No configure el puerto que está conectado al servidor RADIUS.



Nota: Si desea configurar varios puertos al mismo tiempo, utilice el comando interface range.

Vea el siguiente ejemplo para configurar los puertos 1-4 usando el comando range:

Paso 8. Para permitir un host único (cliente) o varios hosts en un puerto autorizado IEEE802.1X, utilice el comando **dot1x host-mode** en el modo de configuración de la interfaz. Los parámetros se definen como:

- multi-host: habilita el modo de varios hosts
    - 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*.

- host único: habilita el 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*.

- multisesión: habilitar modo de sesiones múltiples

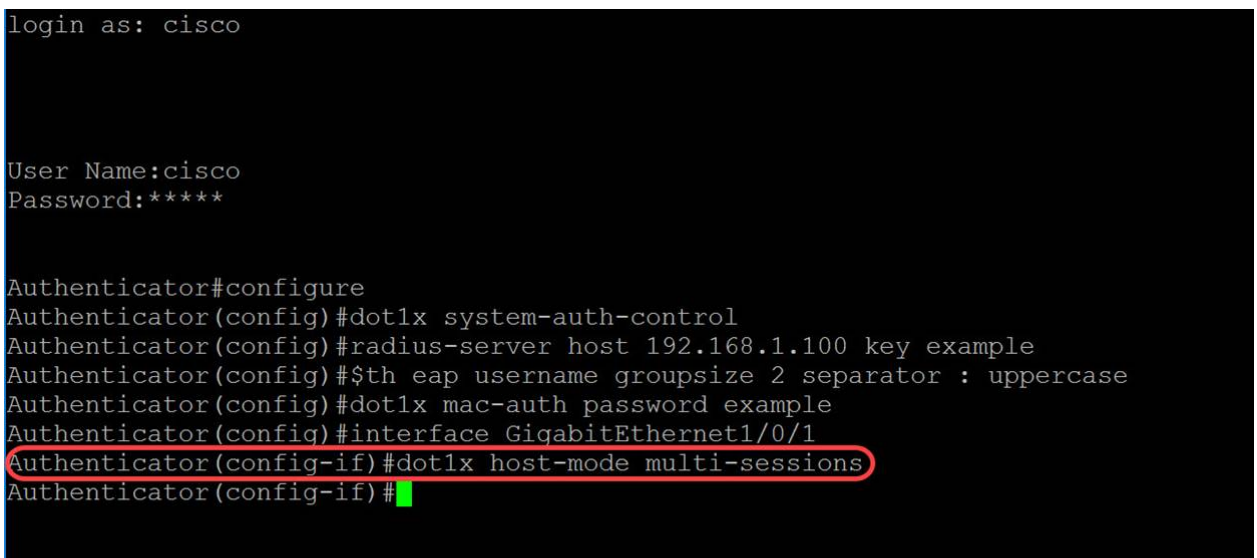
    - A diferencia de los modos de host único y host múltiple, un puerto en el modo de sesiones múltiples no tiene un estado de autenticación. Este estado se asigna a cada cliente conectado al puerto.

    - El tráfico etiquetado que pertenece a una VLAN no autenticada siempre se puentea independientemente de si el host está autorizado o no.

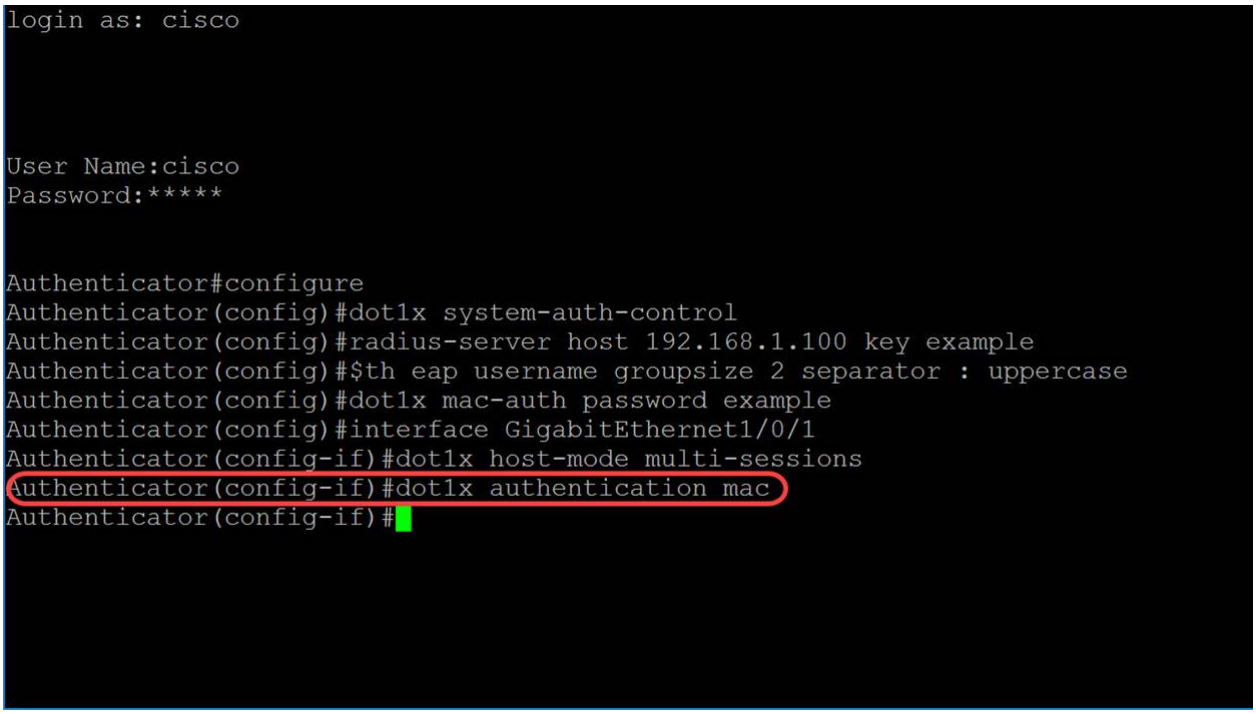
    - El tráfico etiquetado y no etiquetado de hosts no autorizados que no pertenecen a una VLAN no autenticada se reasigna a la VLAN de invitado si se define y se habilita en la VLAN, o se descarta si la VLAN de invitado no está habilitada en el puerto.

    - 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*.

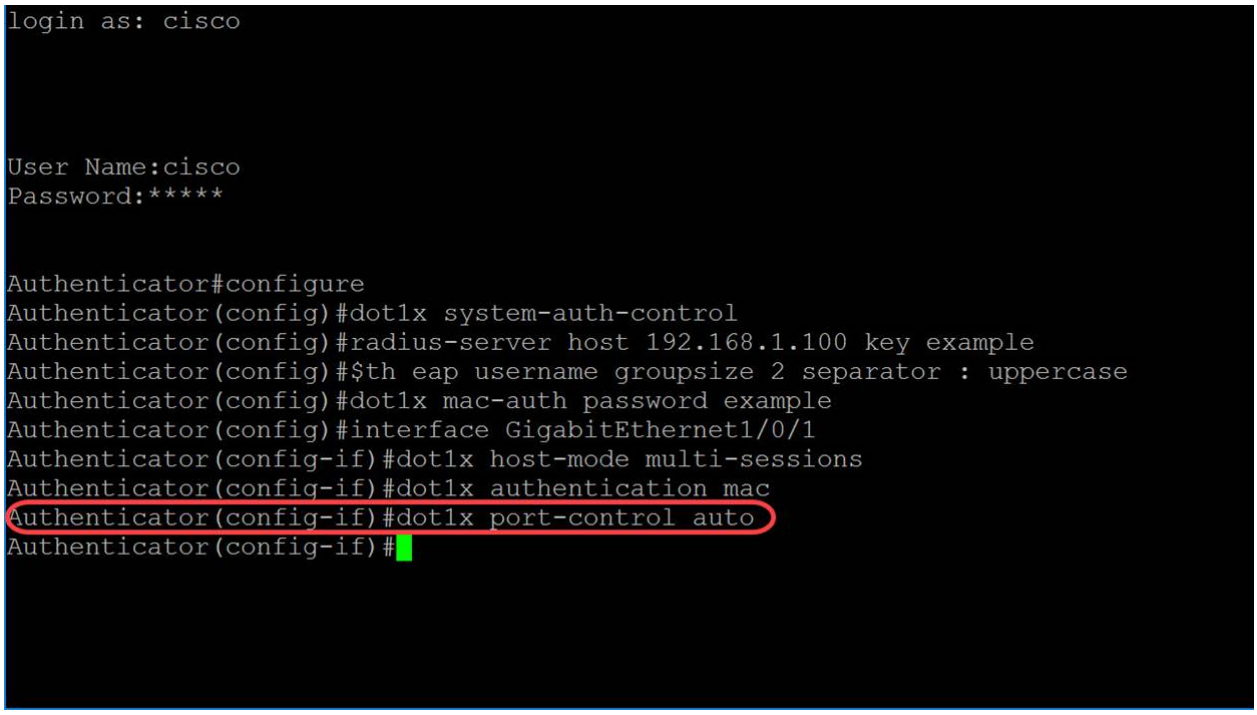
En este ejemplo, configuraremos el modo host para que sea multisesión.



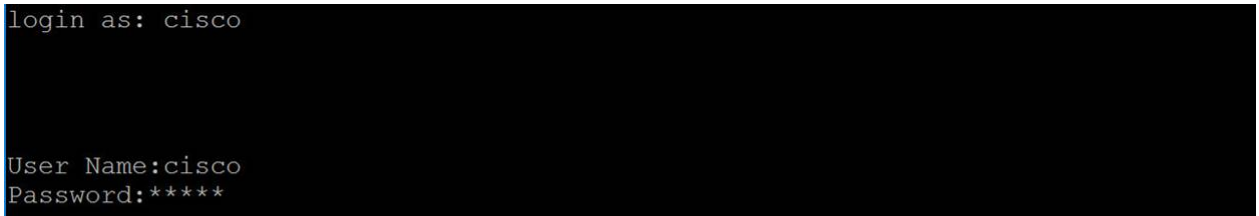
Paso 9. Para configurar el método de autenticación en un puerto, utilice el siguiente comando para habilitar la autenticación basada en MAC.



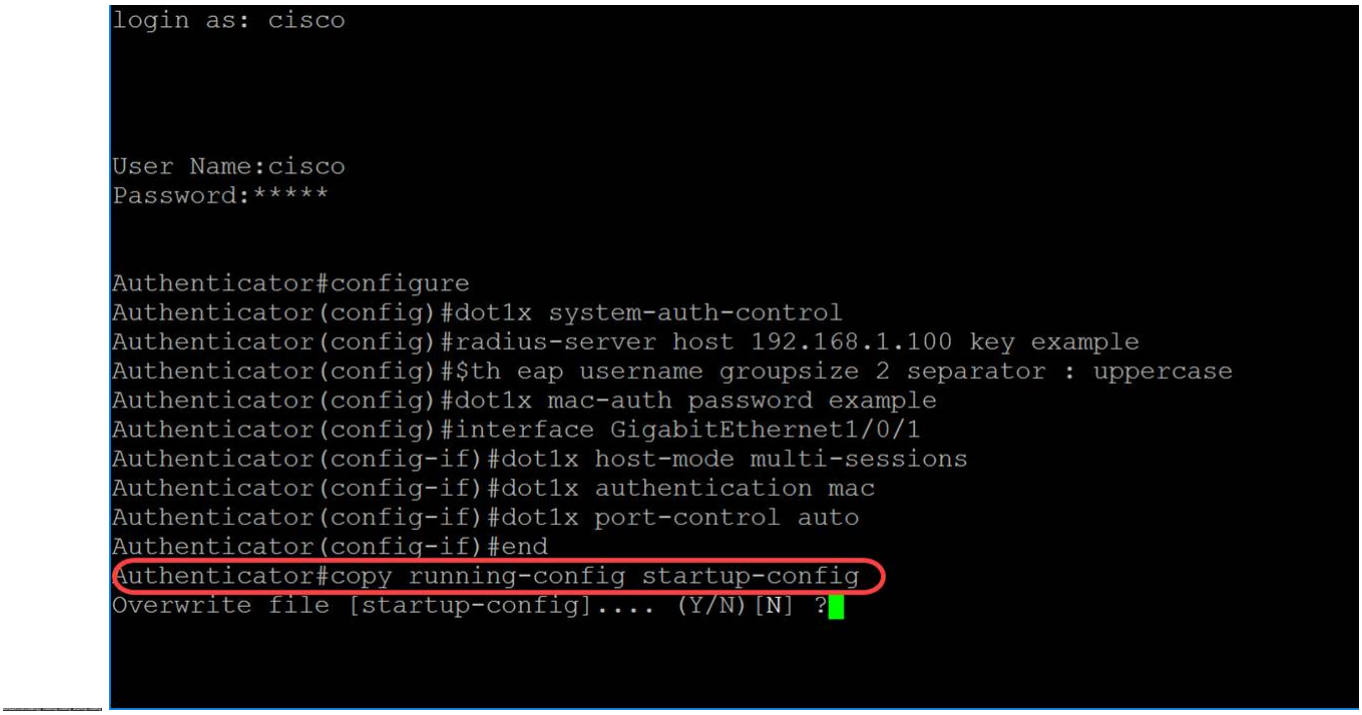
Paso 10. Para habilitar la autenticación y autorización basada en puerto en el dispositivo, utilice el comando **port-control** para configurar el valor de control de puerto. Seleccionaremos el estado de autorización de puerto administrativo como **automático**. Esto nos permitirá habilitar la autenticación 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.



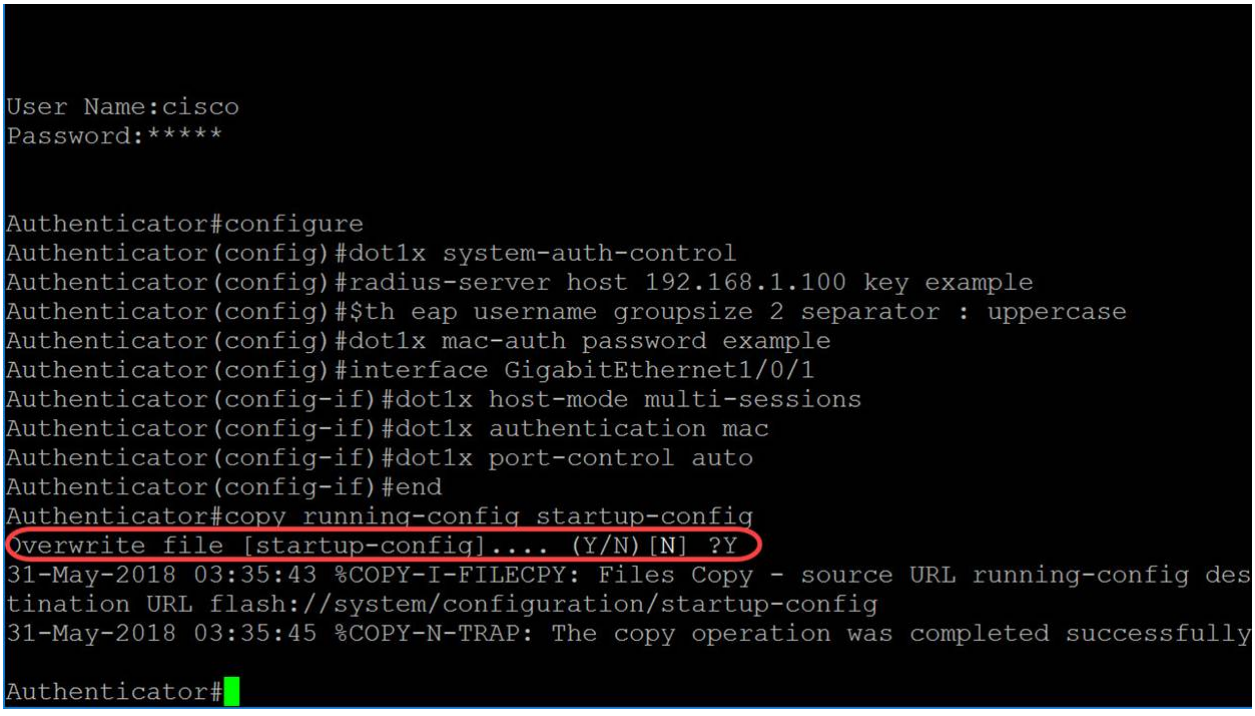
Paso 11. (Opcional) Para finalizar la sesión de configuración actual y volver al modo EXEC privilegiado, utilice el comando **end**.



Paso 12. (Opcional) Para copiar cualquier archivo de un origen a un destino, utilice el comando **copy** en el modo EXEC privilegiado. En este ejemplo, vamos a guardar nuestra configuración en ejecución en startup-config.



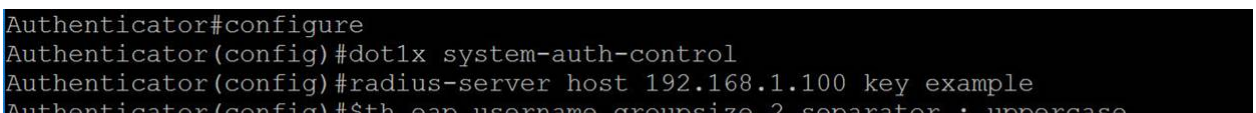
Paso 13. (Opcional) Aparecerá un mensaje y pregunte si desea sobrescribir el archivo startup-config. Escriba **Y** para sí o **N** para no. Escribiremos **Y** para sobreescribir nuestro archivo startup-config.



Conclusión

Ahora debería haber configurado la autenticación basada en MAC en su switch mediante la CLI. Siga estos pasos para verificar que la autenticación basada en MAC funcione.

Paso 1. Para mostrar usuarios autorizados 802.1X activos para el dispositivo, utilice el comando **show dot1x users** en el modo EXEC privilegiado.



Paso 2. Para mostrar las interfaces 802.1X o el estado de la interfaz especificado, utilice el comando **show dot1x** en el modo EXEC privilegiado.

```
Authenticator#show dot1x interface GigabitEthernet1/0/1

Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius
MAC-Based Authentication:
  Type: Eap
  Username Groupsize: 2
  Username Separator: :
  Username case: Uppercase
  Password: MD5 checksum 1a79a4d60de6718e8e5b326e338ae533
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled
Supplicant Global Configuration:
Supplicant Authentication success traps are disabled
Supplicant Authentication failure traps are disabled

gi1/0/1
 Authenticator is enabled
 Supplicant is disabled
 Authenticator Configuration:
 Host mode: multi-sessions
 Authentication methods: mac
 Port Administrated Status: auto
 Guest VLAN: disabled
 VLAN Radius Attribute: disabled
 Open access: disabled
 Server timeout: 30 sec
 Maximum Hosts: unlimited
 Maximum Login Attempts: 0
 Reauthentication is disabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 1
 Authentication fails: 0
 Number of Authorized Hosts: 1
```