

Actualización/copia de seguridad del firmware e intercambio de imágenes en SG350XG y SG550XG

Objetivos

Este objetivo de este documento es explicar cómo actualizar, realizar copias de seguridad o intercambiar el firmware en los switches SG350XG y SG550XG.

El uso del firmware más reciente es una práctica recomendada tanto para la seguridad como para el rendimiento. Se puede guardar más de una versión de firmware en el switch y se puede intercambiar cuando se desee. También se puede realizar una copia de seguridad de las versiones del firmware. Esto puede ser útil para guardar copias de seguridad del firmware en caso de que se produzca una falla en el dispositivo.

Dispositivos aplicables

- SG350XG
- SG550XG

Versión del software

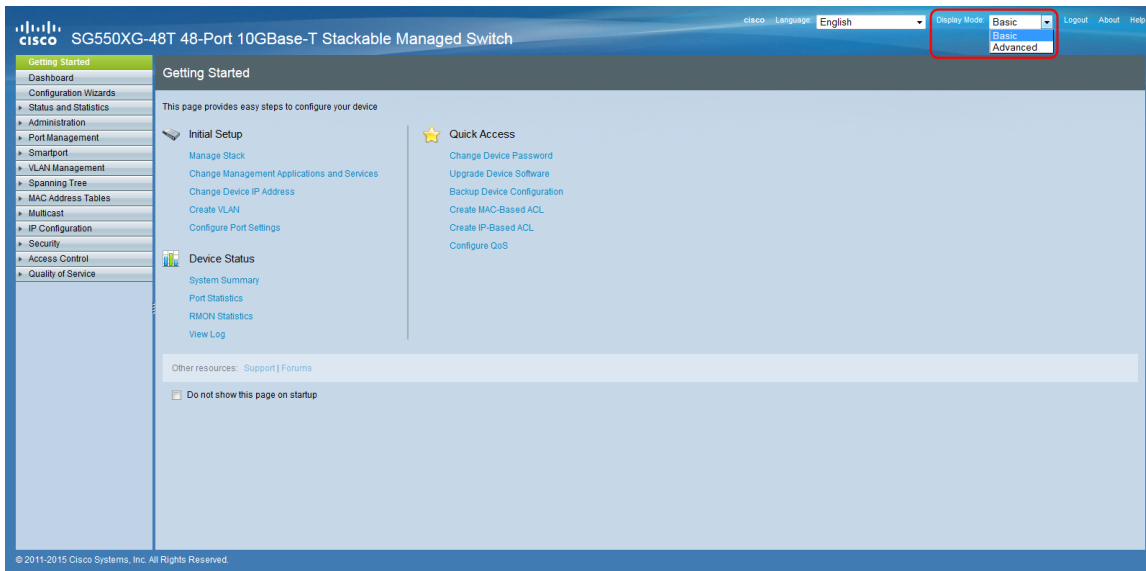
- v2.0.0.73

Tabla de pasos

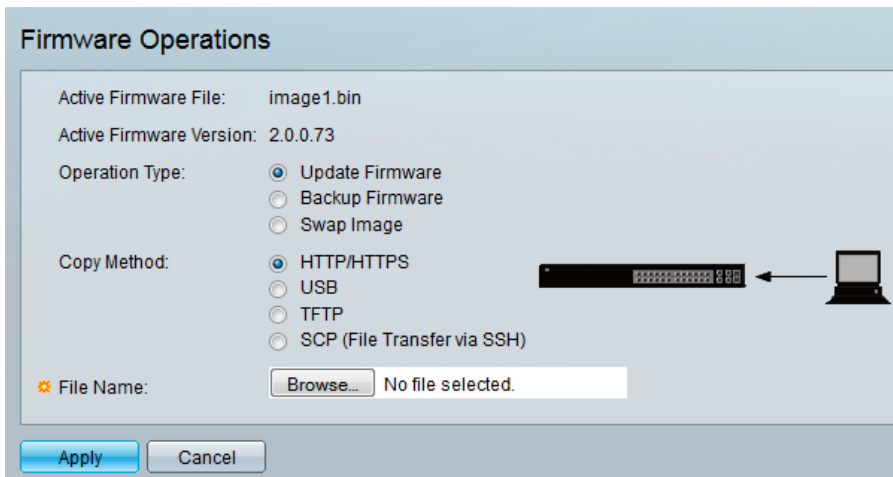
1. Inicio de sesión
2. [Actualización/Copia de seguridad del firmware](#)
 - [Método: HTTP/HTTPS](#)
 - [Método: USB](#)
 - [Método: TFTP](#)
 - [Método: SCP](#)
3. [Cambiar imagen](#)

Inicio de sesión

Nota: Las siguientes capturas de pantalla pertenecen a la pantalla avanzada. Esto se puede cambiar haciendo clic en la lista desplegable *Modo de visualización* situada en la parte superior derecha de la pantalla

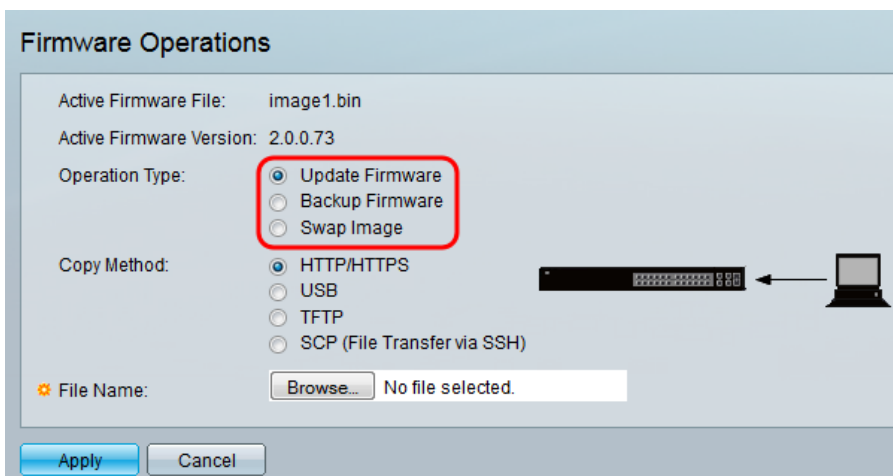


Paso 1. Inicie sesión en la utilidad de configuración web y **elija Administration > File Management > Firmware Operations**. Se abre la página *Operaciones de Firmware*.



Nota: Puede ver el archivo de firmware y la versión actuales en el campo *Archivo de firmware activo* y en el campo *Versión de firmware activo*.

Paso 2. Haga clic en el botón de opción deseado en el área *Tipo de operación*.



Las opciones se describen de la siguiente manera:

- [Actualizar firmware](#): actualiza el firmware del dispositivo.

- [Firmware de copia de seguridad](#): crea una copia de seguridad del firmware del dispositivo.
- [Cambiar imagen](#): cambia el firmware del dispositivo por uno almacenado en la memoria flash del dispositivo.

Actualización/Copia de seguridad del firmware

Paso 1. Haga clic en el botón de opción de la sección *Copiar método* para obtener el método deseado para transferir el archivo.

The screenshot shows a 'Firmware Operations' dialog box. It contains the following fields and options:

- Active Firmware File: image1.bin
- Active Firmware Version: 2.0.0.73
- Operation Type:
 - Update Firmware
 - Backup Firmware
 - Swap Image
- Copy Method:
 - HTTP/HTTPS (highlighted with a red box)
 - USB
 - TFTP
 - SCP (File Transfer via SSH)
- File Name: [Browse...] No file selected.

At the bottom, there are 'Apply' and 'Cancel' buttons. To the right of the dialog, there is a small diagram showing a laptop connected to a switch via a cable.

Las opciones se describen de la siguiente manera:

- [HTTP/HTTPS](#): utiliza las instalaciones proporcionadas por el explorador.
- [USB](#) - Utiliza el puerto USB de los switches.
- [TFTP](#) - El protocolo trivial de transferencia de archivos (TFTP) es un protocolo simple de transferencia de archivos que permite a un cliente obtener o poner un archivo en un host remoto.
- [SCP](#) (Transferencia de archivos a través de SSH) - El protocolo de copia segura (SCP) admite transferencias de archivos entre hosts en una red. Utiliza Secure Shell (SSH) para la transferencia de datos y utiliza los mismos mecanismos de autenticación, garantizando así la autenticidad y confidencialidad de los datos en tránsito.

HTTP/HTTPS

Paso 1. Haga clic en el botón **Browse** en el campo *File Name* para seleccionar el archivo de imagen que desea actualizar. Este paso no es relevante para la copia de seguridad mediante HTTP/HTTPS.

Copy Method: HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

File Name:

Paso 2. Haga clic en Apply (Aplicar).

Copy Method: HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

File Name:

Paso 3. Vaya a **Administración > Reinicio**. Se abrirá la página *Reboot*.

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Paso 4. Haga clic en **Reiniciar**. Aparecerá una ventana de confirmación.

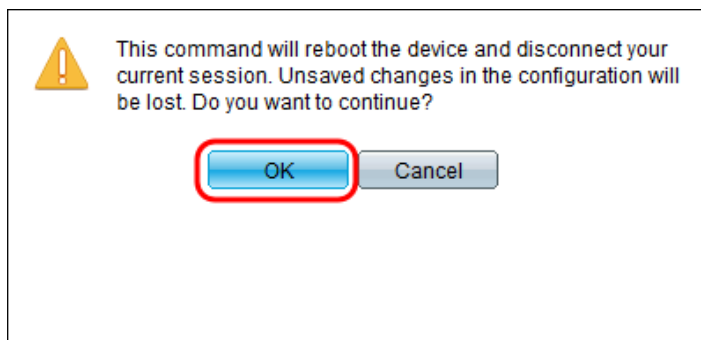
Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

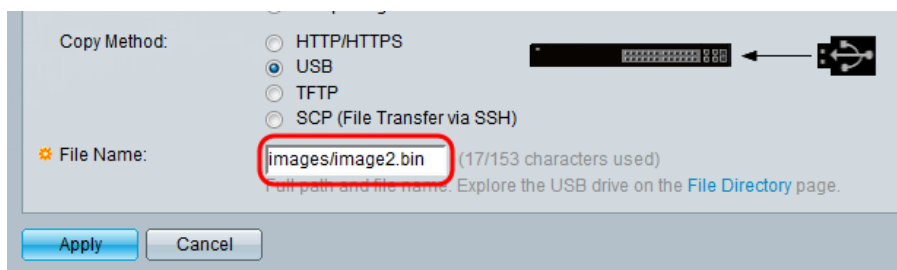
Paso 5. Click OK.



Nota: El dispositivo se reiniciará ahora, lo que desconectará la sesión actual. Una vez que se complete el reinicio, se conectará una nueva sesión.

USB

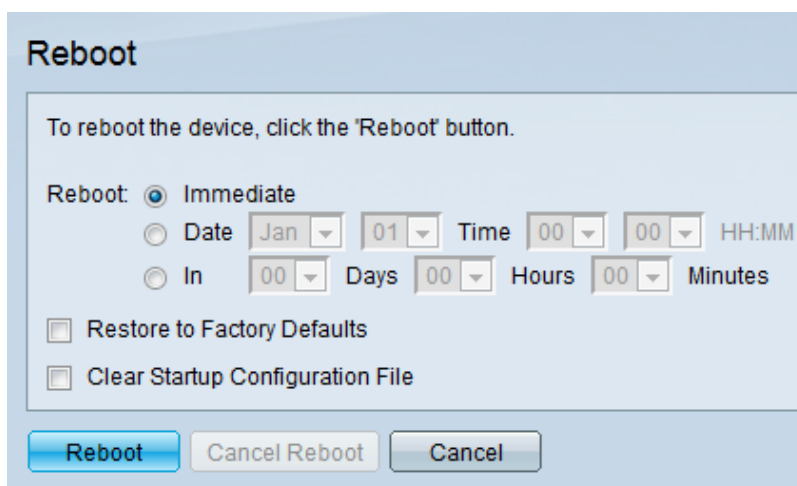
Paso 1. Introduzca la ruta del archivo de imagen ubicado en el USB en el campo *Nombre de archivo*.



Paso 2. Haga clic en Apply (Aplicar).



Paso 3. En la utilidad de configuración web y **elija Administration > Reboot**. Se abrirá la página *Reboot*.



Paso 4. Haga clic en **Reiniciar**.

Reboot


To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Reboot Cancel Reboot Cancel

Paso 5. Aparecerá una ventana de confirmación. Click OK.

 This command will reboot the device and disconnect your current session. Unsaved changes in the configuration will be lost. Do you want to continue?

OK Cancel

Nota: El dispositivo se reiniciará ahora, lo que desconectará la sesión actual. Una vez que se complete el reinicio, se conectará una nueva sesión.

TFTP

Paso 1. Seleccione el botón de opción correspondiente para definir el servidor TFTP. El servidor se puede definir bien **Por dirección IP** o bien **Por nombre**. Si ha seleccionado **Por nombre**, vaya directamente al [Paso 5](#).

Copy Method: Swap image
 HTTP/HTTPS
 USB
 TFTP
 SCP (File Transfer via SSH)

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:

Source File Name: (0/160 characters used)

Apply Cancel

Paso 2. (Opcional) Seleccione la versión de la dirección IP del servidor. Si **se selecciona la versión 4**, vaya directamente al [paso 5](#).

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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:

Source File Name: (0/160 characters used)

Apply Cancel

Las opciones se describen de la siguiente manera:

- IPv4: dirección de 32 bits (cuatro bytes).
- IPv6: sucesor de IPv4, consta de una dirección de 128 bits (8 bytes).

Paso 3. (Opcional) Seleccione el tipo de dirección IPv6. Puede seleccionar **Link Local** o **Global** para su tipo de dirección. Si se ha seleccionado **Global**, vaya directamente al [Paso 5](#).

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:

Source File Name: (0/160 characters used)

Apply Cancel

Paso 4. (Opcional) Seleccione la VLAN deseada en la lista desplegable *Link Local Interface*.

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:

Source File Name: (0/160 characters used)

Apply Cancel

Paso 5. Ingrese el nombre o la dirección IP del servidor en el campo *Server IP Address/Name*.

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: (0/160 characters used)

Apply Cancel

Nota: El siguiente campo depende de la opción seleccionada en el [Paso 1](#).

Paso 6. Ingrese el nombre de archivo en el campo *Source/Destination File Name*.

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: image2.bin (10/160 characters used)

Apply Cancel

Nota: El siguiente campo se titula *Nombre de archivo de destino* para copia de seguridad por TFTP.

Paso 7. Haga clic en Apply (Aplicar).

Copy Method: HTTP/HTTPS USB TFTP SCP (File Transfer via SSH)

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: 192.0.2.1

Source File Name: image2.bin (10/160 characters used)

Apply Cancel

SCP (transferencia de archivos a través de SSH)

Paso 1. Para habilitar la autenticación del servidor SSH (que está desactivada de forma predeterminada), haga clic en **Editar** mediante *autenticación del servidor SSH remoto*. Esto lo lleva a la *página Client SSH UserAuthentication* para configurar el usuario SSH.

Nota: Para obtener más información sobre las Credenciales del Sistema del Cliente SSH, consulte el artículo Autenticación del Usuario SSH.

Paso 2. Seleccione la autenticación SSH deseada en el campo *SSH Client Authentication*.

Las opciones disponibles se definen de la siguiente manera:

- Utilice Credenciales del Sistema del Cliente SSH - Establece las credenciales permanentes del usuario SSH. Haga clic
 - **Credenciales del sistema** para ir a la *página SSH User Authentication* donde el usuario/la contraseña se puede establecer una vez para todo uso futuro
 - Usar credenciales de cliente SSH una vez: establece credenciales de usuario SSH únicas.
- Nota:** Para obtener más información sobre las Credenciales del Sistema del Cliente SSH, consulte el artículo Autenticación del Usuario SSH.

Paso 3. (Opcional) Introduzca el *nombre de usuario* y la *contraseña* deseados en sus campos respectivos.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

✦ Source File Name: (0/160 characters used)

Paso 4. Seleccione el botón de opción correspondiente para definir el servidor SCP. El servidor se puede definir bien **Por dirección IP** o bien **Por nombre**. Si ha seleccionado **Por nombre**, vaya al [Paso 8](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

✦ Source File Name: (0/160 characters used)

Paso 5. (Opcional) Seleccione la versión de la dirección IP del servidor. Si **se selecciona la versión 4**, vaya directamente al [paso 8](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

✦ Source File Name: (0/160 characters used)

Las opciones se describen de la siguiente manera:

- IPv4: dirección de 32 bits (cuatro bytes).
- IPv6: sucesor de IPv4, consta de una dirección de 128 bits (8 bytes).

Paso 6. (Opcional) Seleccione el tipo de dirección IPv6. Puede seleccionar **Link Local** o

Global para su tipo de dirección. Si se ha seleccionado **Global**, vaya directamente al [Paso 8](#).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Paso 7. (Opcional) Seleccione la VLAN deseada en la lista desplegable *Link Local Interface*

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Paso 8. Ingrese el nombre o la dirección IP del servidor en el campo *Server IP Address/Name*.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (0/160 characters used)

[Apply](#) [Cancel](#)

Paso 9. Introduzca el nombre del archivo en el *Fuente/Destination Nombre del archivo* campo.

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (10/160 characters used)

Nota: El campo se titula *Nombre de archivo de destino* para copia de seguridad por SCP.

Paso 10. Haga clic en Apply (Aplicar).

Remote SSH Server Authentication: Disabled [Edit](#)

SSH Client Authentication: Use SSH Client [System Credentials](#)
 Use SSH Client One-Time Credentials:

Username:

Password:

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:

Source File Name: (10/160 characters used)

Cambiar imagen

Paso 1. Seleccione el archivo de firmware que desea que esté activo después del reinicio en la lista desplegable *Imagen activa después del reinicio*.

Firmware Operations

Active Firmware File: image1.bin

Active Firmware Version: 2.0.0.73

Operation Type: Update Firmware
 Backup Firmware
 Swap Image

Active Image After Reboot:

Paso 2. Haga clic en Apply (Aplicar).

Firmware Operations

Active Firmware File:	image1.bin
Active Firmware Version:	2.0.0.73
Operation Type:	<input type="radio"/> Update Firmware <input type="radio"/> Backup Firmware <input checked="" type="radio"/> Swap Image
Active Image After Reboot:	image1.bin
Active Image Version Number After Reboot:	2.0.0.73

Paso 3. En la utilidad de configuración web y elija **Administration > Reboot**. Se abrirá la página *Reboot*.

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Paso 4. Haga clic en **Reiniciar**. Aparecerá una ventana de confirmación.

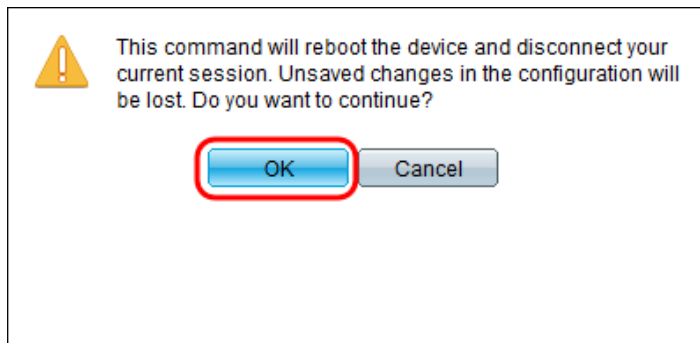
Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Time HH:MM
 In Days Hours Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Paso 5. Click OK.



Nota: El dispositivo se reiniciará ahora, lo que desconectará la sesión actual. Una vez que se complete el reinicio, se conectará una nueva sesión.

Ver un vídeo relacionado con este artículo...

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