

# Copie imágenes de Cisco IOS en routers y switches de forma segura

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo copiar el archivo de imagen de Cisco IOS® desde el PC local con Windows/ Linux/ macOS a los routers y switches de Cisco de manera segura.

## Prerequisites

### Requirements

Cisco recomienda que conozca la disponibilidad de Secure Shell (SSH) para el dispositivo con el nivel de privilegio 15 de acceso.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco ISR3945 CGR2010
- SO Windows 10
- Sistema operativo RedHat Linux

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

En este documento se describe el proceso para copiar el archivo de imagen de Cisco IOS desde el PC Windows/ Linux/ macOS local a los routers y switches de Cisco de forma segura sin necesidad de ningún servidor o software externo como el Protocolo de transferencia de archivos

trivial (TFTP), el Protocolo de transferencia de archivos (FTP), el Protocolo de transferencia de archivos segura (SFTP) o el Protocolo de copia segura (SCP).

## Problema

A veces, en un entorno seguro, es difícil llegar a un servidor TFTP/ FTP/ SFTP/ SCP para copiar la imagen del IOS de Cisco en routers y switches. Existe la posibilidad de que el firewall bloquee los puertos utilizados por cualquiera de estos protocolos mencionados anteriormente entre los dispositivos de origen y destino.

## Solución

Con SCP activado en el dispositivo de Cisco, puede copiar el archivo desde un PC local a dispositivos sin ningún servidor o aplicación. Obtenga la imagen del software del IOS de Cisco del portal de descargas, observe el MD5 de la imagen y confírmela en el PC local.

Linux:

```
[root@root ios]# ls -lshr
total 183M
80M   -rw-r--r--. 1 root root 80M Mar 23 11:52 cgr2010-universalk9-mz.SPA.157-3.M6.bin
103M -rw-r--r--. 1 root root 103M Mar 24 09:35 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
[root@root ios]# md5sum c3900e-universalk9-mz.SPA.155-1.T2.bin
19c881db6ea7ad92dc71f35807a44b82 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

Los usuarios de Windows pueden utilizar WinMD5 o una aplicación similar, que puede calcular el MD5 del archivo. El macOS tiene una línea de comandos similar a Linux.

El MD5 de la imagen del IOS de Cisco debe ser el mismo para descartar cualquier corrupción en el momento de la transferencia. Valide si tiene acceso SSH desde el equipo local al dispositivo con nivel de privilegio 15 y derechos de administrador para realizar cambios de configuración en los dispositivos.

Esta es la configuración mínima requerida en el dispositivo.

```
hostname CGR2010
!
interface GigabitEthernet0/1
ip address x.x.x.x 255.255.255.0
no shut
!
ip route 0.0.0.0 0.0.0.0 x.x.x.x
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
ip domain name cisco.com
!
```

```
!--- key used in this example is 1024

!
crypto key generate rsa
!
username cisco privilege 15 secret 5 $1$jv8O$1VC3PmgNX9o.rsDD3DKeV1
!
line vty 0 4
transport input ssh
!
ip scp server enable
!
end
```

!--- optional

```
!
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2
!
```

Copie las imágenes de Cisco IOS con el uso de este comando:

```
scp ios_filename username@<ip_address_of_the_device>:ios_filename
```

**Windows 10:**

```
Microsoft Windows [Version 10.0.17134.1365]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\mmehtabu>cd /
C:\>cd ios
```

```
C:\ios>dir
Volume in drive C is OSDisk
Volume Serial Number is 0003-4095
```

Directory of C:\ios

```
04/10/2020 01:43 PM <DIR> .
03/24/2020 09:35 AM 107,892,232 c3900e-universalk9-mz.SPA.155-1.T2.bin
1 File(s) 107,892,232 bytes
2 Dir(s) 84,203,741,184 bytes free
```

```
C:\ios>scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-universalk9-
mz.SPA.155-1.T2.bin
```

```
Password:
c3900e-universalk9-mz.SPA.155-1.T2.bin 100%
103MB 61.8KB/s 28:26
```

**Linux:**

```
[root@root ios]# scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-
universalk9-mz.SPA.155-1.T2.bin
```

```
Password:
c3900e-universalk9-mz.SPA.155-1.T2.bin 100%
103MB 517.1KB/s 03:23
```

```
Connection to 10.106.37.44 closed by remote host.
```

El macOS tiene un comando similar:

```
scp c3900e-universalk9-mz.SPA.155-1.T2.bin cisco@10.106.37.44:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

Ahora, verifique el MD5 del archivo en el dispositivo.

```
login as: cisco
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
```

```
CISCO3945#dir
```

```
Directory of flash0:/
```

```
1 -rw- 106362996 Apr 10 2020 07:07:06 +00:00 c3900e-universalk9-mz.SPA.154-3.M3.bin
2 -rw- 107892232 Apr 10 2020 07:16:50 +00:00 c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
1024655360 bytes total (810369024 bytes free)
```

```
CISCO3945#verify flash0:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

```
Starting image verification
Hash Computation: 100% Done!
.. omitted for brevity ...
```

```
CCO Hash MD5 : 19C881DB6EA7AD92DC71F35807A44B82
```

```
Digital signature successfully verified in file flash0:c3900e-universalk9-mz.SPA.155-1.T2.bin
```

En todos los lugares, MD5 debe coincidir para descartar cualquier corrupción del archivo en el momento de la transferencia de Cisco.com al PC y a otros dispositivos.

## Información Relacionada

- [Guía de configuración de Secure Shell](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).