Transfer Cisco IOS Images to Routers and Switches Securely

Contents

Introduction

This document describes how to copy the Cisco IOS® image file from the local Windows/Linux/macOS PC to Cisco routers and switches securely.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Secure Shell (SSH) reachability to the device with privilege level 15 access.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISR3945 CGR2010 router
- Windows 10 OS
- RedHat Linux OS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The process for how to copy the Cisco IOS image file from the local Windows/ Linux/ macOS PC to Cisco routers and switches securely without the need for any external server or software like Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or Secure Copy Protocol (SCP) is described in this document.

Problem

Sometimes in a secure environment, it is difficult to get to a TFTP/ FTP/ SFTP/ SCP server in order to copy the Cisco IOS image to routers and switches. There is a chance the firewall blocks the ports used by any of these previously mentioned protocols between source and destination devices.

Solution

With SCP enabled on the Cisco device, you can copy the file from a local PC to devices without any server or application. Get the Cisco IOS software image from the download portal, note the MD5 of the image, and validate it on the local PC.

Linux:

```
<#root>

[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
```

Windows users can use WinMD5 or a similar application, which can calculate the MD5 of the file. The macOS has a command line similar to Linux.

The MD5 of the Cisco IOS image must be the same to rule out any corruption at the time of the transfer. Validate if you have SSH access from the local PC to the device with privilege level 15 access and have admin rights to make configuration changes on the devices.

Here is the minimum configuration required on the device.

```
<#root>

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


!
! disable the above command after copy is completed


end


!--- optional

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

Copy the Cisco IOS images with the use of this command:

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

Windows 10:

<#root>

```
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

Linux:

<#root>

```
[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 517.1K

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

The macOS has a similar command:

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

Now, verify the MD5 of the file on the device.

<#root>

```
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
```

In all the places, MD5 must match to rule out any corruption of the file at the time of the transfer from Cisco.com to the PC and to other devices.

Related Information

- **Secure Shell Configuration Guide**
- **Cisco Technical Support & Downloads**