Upgrade Catalyst 9600 Switches

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Recommended Releases

Software Download

Essential Criteria for Upgrade

Rommon Upgrade OR Bootloader Upgrade

Upgrade Methods

- Install Mode
- Bundle Mode
- In Service Software Upgrade (ISSU)
  - Pre-requisites for ISSU
  - Steps to Upgrade
  - ISSU Validation Steps
  - Steps to Recover from ISSU Failure
  - Abort ISSU
  - Clean ISSU State

Introduction

This document describes the methods for upgrading Catalyst 9600 switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on C9600.

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

This document covers upgrade procedures for Catalyst 9600 switches that use either BUNDLE or INSTALL modes. ISSU is supported for C9600 High Availability Setup.

Recommended Releases

For the recommended software versions based on the downloads page, see Recommended Releases for Catalyst 9200/9300/9400/9500/9600 Platforms.

Software Download

Download the software at Software Download.

Essential Criteria for Upgrade

- A maintenance window of 2-3 hours can be sufficient for upgrading to the target version or rolling back to the previous version if any issues arise.
- Ensure you have a 4GB or 8GB USB drive with the .bin files of both the current and target Cisco IOS® versions. The USB drive can be formatted in FAT32 to copy the Cisco IOS image.
- Verify that TFTP is set up with both the current and target Cisco IOS versions and is reachable to download these versions to the switch if needed.
- Confirm that console access to the device is available in case any issues occur.
- Ensure there is at least 1GB to 1.5GB of available space in the flash memory for the expansion of the new image. If there is insufficient space, remove old installation files.

Rommon Upgrade OR Bootloader Upgrade

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades can be required to resolve firmware defects or to support new features, but there cannot be new versions with every release.

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader can be automatically upgraded, based on the hardware version of the switch. If the bootloader is automatically upgraded, it can take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated bootloader supports all previous releases.

To know the ROMMON or bootloader version that applies to every major and maintenance release, see:

ROMMON versions for 17.x.x:

ROMMON versions for 16.x.x:

Upgrade the ROMMON before or after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to:

- Upgrading the ROMMON in the primary SPI flash device

  This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. Enter the upgrade rom-monitor capsule golden switch command in privileged EXEC mode.

Note: In the case of a Cisco StackWise Virtual setup, upgrade the active and standby supervisor modules.

- In case of a High Availability set-up, upgrade the active and standby supervisor modules.

After the ROMMON is upgraded, it can take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

Upgrade Methods

This document covers upgrade procedures for the Catalyst 9600 switch that uses either BUNDLE or INSTALL modes.

Install Mode

An install mode upgrade on a Cisco Catalyst 9600 switch is a method of upgrading the switch's software that involves using individual software packages rather than a single monolithic image file.

Perform these steps for an upgrade in Install mode:

1. Cleanup: remove any inactive installations:

```
Switch#install remove inactive
```

2. Copy the new image

Transfer the new .bin image file to the active supervisor's flash storage using one of these methods:

via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> flash:
```

via USB:

```
Switch# copy usbflash0:<file_name> flash:
```

Confirm the available file systems:

```
Switch#show file systems
```

3. Verification

After transferring the Cisco IOS to the active supervisor's flash, check if the image is correctly copied:

```
Switch#dir flash:
```

(Optional) To verify the MD5 checksum:

```
Switch#verify /md5 flash:<file_name>
```

En sure this checksum matches the one provided on the Software Download page.

4. Set the Boot Variable

Set the **boot variable** to point to the packages.conf file with these commands:

```
Switch#config terminal

Switch(config)#no boot system

Switch(config)#boot system flash:packages.conf

Switch(config)#end
```

5. Autoboot Configuration

Configure the switch to autoboot by executing:

```
Switch#config terminal

Switch(config)#no boot manual

Switch(config)#end
```

6. Save configuration

Save your current configuration with:

```
Switch#write memory
```

Confirm the boot settings:

```
Switch#show boot
```

7. Install the image:

```
Switch#install add file flash:<file_name> activate commit
```

When prompted with **This operation requires a reload of the system. Do you want to proceed? [y/n]**, respond with **y** to proceed.

8. Verification of successful upgrade

```
Switch#show version

Switch#show redundancy
```



Note: Replace with the actual name of your Cisco IOS image file throughout the steps.

Bundle Mode

A bundle mode upgrade on a Cisco Catalyst 9600 switch refers to a method of upgrading the switch's software where the entire software image is bundled into a single file. This file includes all the necessary components such as the operating system, device drivers, and other essential software required for the switch to operate. The upgrade involves a single software image file, typically with a .bin extension. This contrasts with other methods, such as install mode, which can involve multiple files and packages.

Perform these steps for an upgrade in Bundle mode:

1. Transfer the **new image** (.bin file) to the flash memory of each supervisor module installed (in case of dual sup or SVL) in the switch using one of these methods

Via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> bootflash:

Switch#copy tftp://Location/directory/<file_name> stby-bootflash:
```

Via USB:

```
Switch#copy usbflash0:<file_name> bootflash:

Switch#copy usbflash0:<file_name> stby-bootflash:
```

2. Confirm the available file systems by using the command

```
Switch#show file systems
```

3. After copying the Cisco IOS to all member switches, verify that the image has been correctly copied with

```
Switch#dir bootflash:

Switch#dir stby-bootflash:
```

4. (Optional) Verify the MD5 checksum with the command:

```
Switch#verify /md5 bootflash:<file_name>
Switch#verify /md5 stby-bootflash:<file_name>
```

Ensure the output matches the MD5 checksum value provided on the Software Download page.

5. Configure the boot variable to point to the new image file with these commands

```
Switch#config terminal
Switch(config)#no boot system
Switch(config)#boot system bootflash:<file_name>
Switch(config)#end
```

6. Save the **configuration**.

```
Switch#write memory
```

7. Verify the boot settings using

```
Switch#show boot
```

8. Reload the switch to apply the new Cisco IOS

```
Switch#reload
```

9. Verification of successful upgrade.

```
Switch#show version
Switch#show redundancy
```

Note: Replace with the actual name of your Cisco IOS image file throughout the steps.

In Service Software Upgrade (ISSU)

In-Service Software Upgrade is a process that upgrades an image to another image on a device while the network continues to forward packets. ISSU helps network administrators avoid a network outage when they perform a software upgrade. The images are upgraded in install mode, wherein, each package is upgraded individually.

ISSU upgrade is supported on 9600 Stackwise-Virtual and also on 9600 stand-alone chassis with dual supervisors. ISSU downgrades are not supported.

- For Catalyst 9600 in dual supervisor module configuration and with StackWise Virtual, ISSU support starts from Cisco IOS XE Gibraltar 16.12.1.
- For Catalyst 9600X with StackWise Virtual, ISSU support starts from Cisco IOS XE Cupertino 17.12.1.
- For Catalyst 9600X in dual supervisor module configuration, ISSU support starts from Cisco IOS XE Cupertino 17.9.1.

Ensure the current SW version and Target SW version is suitable for ISSU upgrade at Compatibility Matrix.

- For ISSU upgrade from 17.3.1, 17.3.2, 17.3.3, or 17.3.4 to 17.6.x in standalone chassis with quad supervisor or high availability setup, you must perform an ISSU upgrade to 17.3.5 and then perform ISSU upgrade to the final target release version. ISSU upgrade to 17.9.1 can fail. See Cisco bug ID CSCwc54402 for more details.
- ISSU upgrade from 17.6.4 to 17.9.3 can fail. See Ciscobug ID CSCwc54402 for more details.

Pre-requisites for ISSU

1. Check the Current Code Version.

```
C9600#show version | include IOS XE
```

2. Check the Boot Mode.

ISSU is supported only if both the switches in StackWise Virtual are booted in **Install** mode.

```
C9600#show ver | include INSTALL
```

3. Check if There is Sufficient Available Memory on Flash.

```
C9600#dir flash: | include free
11353194496 bytes total (8565174272 bytes free)
```

```
C9600#dir stby-flash: | include free
11353980928 bytes total (8566865920 bytes free)
```

4. Check if Switches are in SSO Mode.

```
C9600#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 4 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso <----------
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE <----------
       Uptime in current state = 30 minutes
                 Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), V
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 05-Nov-18 19:32 by mcpre
                         BOOT = flash:packages.conf;
                  CONFIG_FILE =
        Configuration register = 0x102

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT <----------
       Uptime in current state = 26 minutes
                 Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), V
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 05-Nov-18 19:32 by mcpre
                         BOOT = flash:packages.conf;
                  CONFIG_FILE =
        Configuration register = 0x102
```

5. Check if Auto-Boot is enabled.

```
C9600#show boot system
--------------------------
Switch 1
--------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;
```

```
Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no    <----- Manual Boot should be set to "no"
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
--------------------------
Switch 2
--------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
Boot Mode = DEVICE
iPXE Timeout = 0
```

If Auto-Boot is not enabled, change as shown:

<#root>

C9600(config)#no boot manual

6. Check the Current ISSU and Install states.

```
C9600#show issu state detail
--- Starting local lock acquisition on switch 1 ---
Finished local lock acquisition on switch 1

No ISSU operation is in progress <----- If see anything else, abort ISSU before proceeding.
Check on how to manually abort ISSU.
```

```
C9600#show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    16.9.2.0.2433      <----- State should be Activated & Committed for current version alone.
 If not clear install state before proceeding. Check on how to clear install state.

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Steps to Upgrade

Perform these steps to perform an In-Service Software Upgrade (ISSU) upgrade.

1. Cleanup – Remove any **inactive installations**:

```
Switch#install remove inactive
```

2. Copy the new image – Transfer the **new .bin image file** to the active supervisor's flash storage using one of these methods:

Via TFTP:

```
Switch#copy tftp://Location/directory/<file_name> flash:
```

Via USB:

```
Switch#copy usbflash0:<file_name> flash:
```

Confirm the available file systems with: **show file systems**

3. Verification – After transferring the Cisco IOS to the active supervisor's flash, check if the image is correctly copied with:

```
Switch#dir flash:
```

(Optional) To verify the MD5 checksum:

```
Switch#verify /md5 flash:<File_name>
```

Make sure this checksum matches the one provided on the Software Download page.

4. Set the **boot variable** to point to the packages.conf file:

```
Switch#config terminal
 Switch(config)#no boot system
 Switch(config)#boot system flash:packages.conf
 Switch(config)#end
```

5. Configure the **switch** to autoboot:

```
Switch#config terminal

Switch(config)#no boot manual

Switch(config)#end
```

6. Save your **current configuration** with:

```
Switch#write memory
```

Confirm the boot settings with the command:

```
Switch#show boot
```

7. Install the image:

```
Switch#install add file flash:<file_name> activate issu commit
```

Once you run the command noted here, the process starts and reloads sup automatically. Do not run the command until you are ready for sups to start to reboot. Unlike the normal upgrade process, it does not ask for confirmation from you before the reload happens.

Once you run this command, the ISSU process extracts the files, reloads the standby sup, waits for it to get back to SSO then failover reloads the active.



Note: Replace with the actual name of your Cisco IOS image file throughout the steps.

ISSU Validation Steps

Once ISSU is completed:

- Check if both switches run on the new software.
- Check **show issu state detail** output to be clean and not showing any ISSU in progress.
- Check **show install issu history** output to ensure successful ISSU operation (Command available only

with 16.10.1 release and later).

Steps to Recover from ISSU Failure

- If ISSU fails, it is expected that auto-abort can recover the system back to its initial state (older image). However, if this fails as well, manual recovery of the chassis is expected.
- During manual recovery, check if both active and standby run the older image (if not, recover the individual chassis).
- After you ensure both chassis, run the old image, run **install remove inactive** to remove any unused image packages.
- Once both chassis run the old software, manually clean all the internal states of ISSU operation. (Refer here on how to clean the internal ISSU states).

Abort ISSU

In the 3-Step Work Flow, during the activate ISSU process, the system can auto-abort to an older image if the abort-timer expires. Manual abort is required if the standby does not reach SSO during abort. Also, if for any reason you wish to abort the ISSU in between, manual abort is required.

```
C9600#install abort issu
```

Clean ISSU State

If ISSU upgrade/downgrade/abort/auto-abort is not successful, manual clean-up of ISSU internal states is required.

Enable the service internally before running this command:

```
C9600(config)#service internal
C9600(config)#end
C9600#clear install state
clear_install_state: START Tue Nov 13 17:05:47 UTC 2018
--- Starting clear_install_state ---
Performing clear_install_state on all members
  [1] clear_install_state package(s) on chassis 1
  [1] Finished clear_install_state on chassis 1
Checking status of clear_install_state on [1]
clear_install_state: Passed on [1]
Finished clear_install_state

C9600#show issu state detail
--- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1

No ISSU operation is in progress
```