

Installing and Upgrading Software

- Software Packaging on the Router, on page 1
- Provisioning Files, on page 3
- File Systems on the Router, on page 3
- System Requirements, on page 4
- ISSU Support Matrix, on page 5
- Autogenerated Files and Directories, on page 9
- General Prerequisites for Software Upgrade, on page 9
- General Restrictions for Software Upgrade, on page 10
- Upgrading the ROMMON on the RSP Module, on page 10
- Upgrading the ROMMON on Cisco NCS 4201 and NCS 4202 Routers, on page 13
- Upgrading Firmware of the Power Supply Monitoring Device, on page 16
- Loading the New Image and Preparing for Upgrade, on page 18
- Upgrading the Cisco NCS4200 Series Chassis, on page 20
- Secure eUSB Configuration, on page 29
- Software Upgrade Process Using Install Commands, on page 30
- Additional References, on page 33

Software Packaging on the Router

Software Package Modes

The router can be booted using any of the following:

- Consolidated—A single software image containing a full collection of software packages. This mode provides a simplified installation and can be stored in the bootflash, a TFTP server, or a network server.
- Sub-package—One or more sub-images that are extracted from the consolidated image. This mode provides optimized memory usage and requires that you store files in the bootflash directory.

Upgrade IOS Image in Sub-packages Mode

To upgrade IOS image in sub-packages mode for the Cisco NCS 4202 routers:

```
request platform software package expand file source-URL [to destination-URL] [force]
[verbose] [wipe]
```

```
configure terminal
config-register 0x2
boot system flash [flash-fs:] [partition-number:] [filename]
exit
copy running-configuration startup-configuration
reload
```

Description of Commands

Command	Description
config-register 0x2	Use the command to boot the router using a specified image in NVRAM.
request platform software package expand file *source-URL* [**to** *destination-URL*] [**force**] [**verbose**] [**wipe**]	Use the command to expand the consolidated image file on the router.
boot system flash [*flash-fs:*] [*partition-number:*] [*filename*]	Use the command to set the router to boot using the packages.conf file.

Configuration Example for Upgrading IOS Image in Sub-packages Mode

The following example shows the upgrade of IOS image in sub-packages mode:

```
Router#request platform software package expand file
bootflash:ncs4202-universalk9_npe.17.03.01.SPA.bin
Verifying parameters
Expanding superpackage bootflash:ncs4202-universalk9_npe.17.03.01.SPA.bin
Validating package type
*Jul 16 14:41:05.881 IST: %INSTALL-5-OPERATION_START_INFO: R0/0: packtool:Started expand
package bootflash:ncs4202-universalk9_npe.17.03.01.SPA.bin

Copying package files
WARNING: packages.conf will replace the identical file that already exists in bootflash:
SUCCESS: Finished expanding all-in-one software package.
Router#
*Jul 16 14:45:30.606 IST: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: packtool:Completed
expand package bootflash:ncs4202-universalk9_npe.17.03.01.SPA.bin

Router#config t
Router(config)#config-reg 0x2
Router(config)#no boot sys
Router(config)#boot system bootflash:packages.conf
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Router#reload
```

Understanding Software Packages

Table 1: Individual Sub-Packages

Sub-Package	Purpose
RPBase	Route Switch Processor (RSP) operating system
RPControl	Control plane processes between IOS process and the rest of the platform.
RPAccess	Handles security features including Secure Socket Layer (SSL) and Secure Shell (SSH)
RPIOS	Cisco IOS kernel, which is where IOS features are stored and run. **Note** Each consolidated image has a unique RPIOS package.
SIPSPA Base	Controls interface module daemons.

Provisioning Files

Provisioning files manage the boot process when the router is configured to boot in sub-packages. The provisioning file manages the bootup of each individual sub-package. Provisioning files are extracted automatically when individual sub-package files are extracted from a consolidated package. Provisioning files are not necessary for running the router using the complete consolidated package.

File Systems on the Router

Table 2: File Systems

File System	Description
bootflash:	The boot flash memory file system on the active RSP.
cns:	The Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
stby-bootflash:	The boot flash memory file system on the standby RSP.
stby-harddisk:	The hard disk file system on the standby RSP.
stby-usb0:	The Universal Serial Bus (USB) flash drive file systems on the standby RSP. **Note** stby-usb1: is an internal port.
system:	The system memory file system, which includes the running configuration.
tar:	The archive file system.

File System	Description
tmpsys:	The temporary system files file system.
usb0:	The Universal Serial Bus (USB) flash drive file systems on the active RSP. **Note** usb1: is an internal port.

If you see a file system not listed in the above table, enter the **?** help option or see the **copy** command reference for additional information on that file system.

System Requirements

RP Memory Recommendations

Table 3: Memory Recommendations for the NCS 4200 RSP3 Module - Consolidated Package Image

Platform	Image Name	Software Image	Individual Sub-package Contents	DRAM Memory
NCS 4200 RSP3 Module	Cisco NCS 4200 Series RSP3 UNIVERSAL W/O CRYPTO	ncs4200rsp3-universal.*version* .bin	ncs4200rsp3-rpbase.*version* .pkg	8 GB (RSP3-400)
			ncs4200rsp3-rpcontrol.*version* .pkg	
			ncs4200rsp3-rpaccess.*version* .pkg	
			ncs4200rsp3-rpios-universal.*version*. pkg	
			ncs4200rsp3-espbase.*version.pkg*	
			ncs4200rsp3-sipbase.*version* .pkg	
			ncs4200rsp3-sipspa.*version* .pkg	
			ncs4200rsp3-packages-universal. version.conf	
			packages.conf	

Platform	Image Name	Software Image	Individual Sub-package Contents	DRAM Memory
NCS 4200 RSP3 Module	Cisco NCS 4200 Series RSP3 UNIVERSAL NPE	ncs4200rsp3-universalk9_npe.*version* .bin	ncs4200-hw-programmables.*version* . pkg	8 GB (RSP3-400)
			ncs4200rsp3-espbase.*version* .pkg	
			ncs4200rsp3-packages-universalk9.*version* .pkg	
			ncs4200rsp3-rpacess.*version* .pkg	
			ncs4200rsp3-rpbase.*version* .pkg	
			ncs4200rsp3-rpcontrol.*version* .pkg	
			ncs4200rsp3-rpios-universalk9_npe.*version* .pkg	
			ncs4200rsp3-sipbase.*version*.pkg	
			ncs4200rsp3-sipspa.*version*.pkg	
			packages.conf	

Determining the Software Version

You can use the **show version installed** command to list the installed sub-packages on the router.

ISSU Support Matrix

Legend:

NA: Not Applicable

NS: Not Supported

Table 4: ISSU Support Matrix

	Supported ISSU Upgrade Or Downgrade Version													
Base IOS Version	16.6.1	16.6.X (X = 2 to 6)	16.6.X (X = 7 and later)	16.9.X (X=1,2)	16.9.X (X= 3 and later)	16.11.X (X = 1 and later)	16.12.X (X= 1 and later)	17.3.1[5]	17.5.1	17.6.1	17.7.1	17.8.1	17.9.X (X=2 to 6)	17.12.X (X=2 to 5)
16.6.1	NA	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS
16.6.X (X=2 to 6)	NS	Yes	Yes	Yes[1]	Yes	Yes[11]	Yes	Yes	Yes 3 1	Yes 3 1	Yes 3 1	Yes 3 1	Yes 3 1	Yes 3 1

	Supported ISSU Upgrade Or Downgrade Version													
16.6.X (X=7 and later)	NS	Yes	Yes	Yes[1]	Yes	Yes[3]	Yes	Yes[3]	Yes	Yes	Yes	Yes	Yes	Yes
16.9.X (X = 1-2)	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]	Yes 3	Yes 3	Yes 3	Yes 3	Yes 3	Yes 3
16.9.X (X = 3 and later)	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16.11.X (X = 1 and later)	NS	Yes	Yes	Yes	Yes	NA	Yes	Yes[32]	Yes 3 4	Yes 3 4	Yes 3 4	Yes 3 4	Yes 3 4	Yes 3 4
16.12.1	NS	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
17.3.X (X = 2 to 8)[3]	NS	NS	NS	NS	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes
17.5.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes
17.6.X (X = 2 to 8)[4]	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes
17.7.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes
17.8.1	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	Yes
17.9.X (X=2 to 6)	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes
17.12X (X=2 to 5)	NS	NS	NS	NS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA

1 Step ISSU (upgrade) to 17.1.1 with any of these images as intermediate image (16.9.3 and higher)
2 Step ISSU (upgrade) to 17.x.x with any of these images as intermediate image (16.12.3)
3 The 17.3.1 image auto ROMMON upgrade enables the RSP for an additional reset during software upgrade if the RSP does not have the latest ROMMON version.
4 The 17.6.1 image auto ROMMON upgrade enables the RSP for an additional reset during software upgrade if the RSP does not have the latest ROMMON version.

Note

- All phase 1 interface modules undergo FPGA upgrade during the ISSU to Cisco IOS XE 17.4.1 from any earlier releases. This impacts the traffic for that IM until the FPGA is upgraded and the IM comes up after reload.
- All phase 1 and phase 2 interface modules undergo FPGA upgrade during ISSU to Cisco IOS XE 17.8.1 from any earlier releases in RSP2 and RSP3. This impacts the traffic for that interface module until the FPGA is upgraded and the interface module comes up after reload.
- For the phase 1 interface module nodes which are ISSU upgraded from Cisco IOS XE 17.4.1 or later release to Cisco IOS XE 17.8.1, the traffic is not impacted.

  Refer the following table for supported IMs:

Table 5: NCS 4200 Supported Ethernet Interface Module

Phase 1 IM	Phase 2 IM	Phase 3 IM
NCS4200-1T8LR	NCS4200-1T8LR-PS	NCS4200-8T-PS
		NCS4200-2Q-P
		NCS4200-2H-PQ

Restrictions

- The ISSU upgrade operation requires that the ROMmon version be 15.6(33r)S or higher for all releases starting from release Cisco IOS XE 16.11.x. For Cisco IOS XE Releases 16.6.x to 16.9.x, the minimum ROMmon version must be 15.6(20r)S.
- You must enable the **port-channel max-memlink-per-pc 8** command when downgrading from Cisco IOS XE Release 16.11.x else, ISSU will fail.
- For Cisco IOS XE Releases from 17.12.x, for ISSU upgrade, there's an increase in the ISSU upgrade duration when CEM scale on the IM is enabled for 5000 or more services.
- Executing service-related commands, including show commands, during an ISSU upgrade or IM reload may lead to unpredictable outcomes. We recommend to wait until the upgrade or reload process has fully completed before running these commands.

Setting the Interface Module Delay for ISSU

Interface module delay refers to the duration that the system waits before enabling the new software on the upgraded interface modules. This delay is to ensure that all the interface modules have successfully synchronized with the new software before they are functioning.

The delay duration can vary depending on several factors, including the specific network device, the number of interface modules, and the complexity of the software upgrade being performed.

To set an optimum delay duration for the ISSU process, refer to the following table:

Interface Module	CEM FPD upgrade		FPD Upgrade (Seconds)	CEM & FPD Upgrade	
	CEM Scale	Upgrade Time (Seconds)		CEM Scale	Upgrade Time (Seconds)
NCS4200-48T1E1-CE	256	120	NA	256	240
	512	180		512	300
NCS4200-48T3E3-CE	672	180	NA	672	300
	1344	360		1344	480
NCS4200-3GMS	672	300	NA	672	420
	1344	360		1344	480
NCS4200-1T8S-20CS	100	480	NA	100	660
	500	540		500	720
	1344	660		1344	840
	2500	840		2500	1020
	5000	1200		5000	1380
NCS4200-1T8S-10CS	100	420	NA	100	660
	500	420		500	720
	1344	540		1344	780
	2500	660		2500	900
	5000	900		5000	1140

For example, consider a router with four interface modules:

- NCS4200-48T1E1-CE with 512 CEM FPD upgrade
- NCS4200-48T3E3-CE with 672 CEM FPD upgrade
- NCS4200-3GMS with 1344 CEM FPD upgrade
- NCS4200-1T8S-20CS with 5000 CEM FPD upgrade

Compare the delay durations of the four interface modules and select the one with the longest duration. For example, the NCS4200-1T8S-20CS delay duration is 1200 seconds, which is the longest compared to the delay durations of the other three interface modules.

Based on this information, set the delay duration to 1200 seconds for the ISSU upgrade for this router.



Note For more information on FPGA versions, refer to the respective version release notes.

Autogenerated Files and Directories

Caution Any autogenerated file in the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by customer support; altering these files can have unpredictable consequences for system performance.

Table 6: Autogenerated Files

File or Directory	Description
crashinfo files	A crashinfo file may appear in the bootflash: file system. Crashinfo files are useful for tuning and troubleshooting, but are not related to router operations: you can erase them without impacting the router's performance.
core files	The bootflash/core directory is the storage area for .core files. **Warning** Do not erase or move the core directory.
lost+found directory	This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.
tracelogs files	The storage area for trace files is bootflash/tracelogs. Trace files are useful for troubleshooting; you can access trace files using diagnostic mode to gather information related to the IOS failure. **Warning** Do not erase or move the tracelog directory.

General Prerequisites for Software Upgrade

- The system must be booted in sub-package mode (with packages.conf).
- The packages.conf (base image packages) and the upgrade image should exist in the same location in the bootflash.

Bootflash Space Requirements

The software upgrade process requires a minimum of 2X image size available space in bootflash memory.

General Restrictions for Software Upgrade

- Cisco IOS XE software compatibility is supported only between identical image types. Cross-image-type upgrades or installations (such as from an Universal image to an *Universalk9_npeimage)* are *not* supported in the upgrade process.
- Running two different image types simultaneously is *not* supported.
- Software upgrades from one package mode to another are *not* supported.
- For software upgrade from IOS XE Release 16.x.x to IOS XE Release 16.z.z images, use the interface module delay as 1500, if the node has TDM IMs.

Upgrading the ROMMON on the RSP Module

Table 7: Feature History

Feature Name	Release Information	Description
Secondary ROMMON Partition Auto Upgrade	Cisco IOS XE Bengaluru 17.4.1	This feature supports secondary ROMMON partition auto upgrade after a successful primary ROMMON partition is complete for NCS 4216 routers.
Secondary ROMMON Version Auto Upgrade	Cisco IOS XE Bengaluru 17.5.1	After primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router. This is applicable to NCS 4201/4202 routers.

Starting with Cisco IOS XE Bengaluru release, 17.6.1, the 15.6(49r)S ROMMON version filters the restricted ROMMON variables during the bootup.

Starting with Cisco IOS XE Bengaluru release, 17.5.1, secondary ROMMON partition is also auto upgraded after a successful primary ROMMON partition upgrade is complete. You can reload the router at the next planned reload to complete the secondary ROMMON upgrade.

Note If the secondary ROMMON version is lesser than that of the primary ROMMON version, the secondary ROMMON gets auto upgraded.

For Cisco IOS XE Amsterdam Release 17.3.x, Cisco IOS XE Bengaluru Release 17.4.x, and earlier, the secondary ROMMON partition is not auto upgraded. You must manually upgrade it using the **upgrade rom-mon filename** command.

Starting with ROMMON release version 15.6(43r)S, ROMMON version is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.

Secure ROMMON is supported from Cisco IOS XE Amsterdam Release 17.3.1 onwards. However, it is compatible with all the releases.

Any future secure ROMMON upgrade or downgrade is only possible from Cisco IOS XE Amsterdam Release 17.3.1 onwards.

Any non-secure FPGA bundled releases moving to Cisco IOS XE Bengaluru Release 17.3.x or future releases can result in an FPGA upgrade and a ROMMON upgrade. If FPGA upgrade happens parallely with the ROMMON upgrade, you can only expect a single reload. If FPGA upgrade gets delayed and happens post ROMMON upgrade, two reloads are expected to complete both the upgrade processes. This is followed by a successful bootup of the target release image.

The router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.



Note For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, Cisco IOS XE Amsterdam 17.1.x, and Cisco IOS XE Amsterdam 17.3.1, a minimum diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots.



Note Routers running a ROMMON version that is lower than version 15.6(33r)S is auto upgraded to version 15.6(33r)S during a router restart. However, if a Cisco IOS XE release with ROMMON image is bundled with a version lower than the running ROMMON version, then the ROMMON is not auto downgraded.



Note Before installing the Cisco IOS XE Amsterdam 17.3.1, you *must* upgrade the ROMMON to version 15_6_43r_s or higher to avoid bootup failure. This is applicable to NCS 4202 routers.



Note Starting with Cisco IOS XE Amsterdam 17.3.1, While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade.



Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Procedure

Step 1 Check the RSP bootup ROMMON region (ROM0 or ROM1). The example, shows the RSP boots up from ROM0 region.

Example:

```
System Bootstrap, Version 15.6(4r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2015 by cisco Systems, Inc.
Compiled Thu 29-Oct-15 23:24 by ccai
Current image running: Boot ROM0
```

Step 2 Copy the ROMMON image to the bootflash on the active and standby RSP.

Example:

```
copy bootflash:ncs4200-rommon.15.6(4r)S.pkg
```

Step 3 Use the **upgrade rom-monitor filename** *bootflash:ncs4200-rommon.15.6(4r)S.pkg* **R0** command to upgrade the version.

Note
R0 represents RSP in slot0 of the chassis. Step 3 upgrades the ROMMON region of the RSP that is not used (ROM1 region) as ROM 0 region is used (in this procedure) in Step 1 to boot up the RSP.

Step 4 Upgrade the ROMMON on the Standby RSP (for High Availability) using **upgrade rom-monitor filename** *bootflash:ncs4200rommon.15.6(4r)S.pkg* **R1** command.

Note
R1 represents the RSP in slot1 of the chassis. Step 4 upgrades the ROMMON region of the RSP that is not used (ROM 0 region).

Step 5 Reload the router.

Example:

```
System Bootstrap, Version 15.6(4r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2015 by cisco Systems, Inc.
Compiled Thu 29-Oct-15 23:24 by ccai
Current image running: Boot ROM0
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Rommon upgrade requested
Flash upgrade reset 1 in progress
.......
System Bootstrap, Version 12.2(20120514:121217) [npenumar-pegasus_rommon_02 183], DEVELOPMENT
 SOFTWARE
Copyright (c) 1994-2008 by cisco Systems, Inc.
Compiled Fri 15-Jun-12 11:45 by ccai
Current image running: *Upgrade in progress* Boot ROM1
Last reset cause: BootRomUpgrade
UEA platform with 2097152 Kbytes of main memory
```

Step 6 Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

Example:

```
System Bootstrap, Version 15.6(4r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2015 by cisco Systems, Inc.
Compiled Thu 29-Oct-15 23:24 by ccai
Current image running: Boot ROM1
```

Step 7 Repeat Step 3 to Step 6 to update the other region on the RSP (ROM0) region in this procedure.

Note
We recommend that both region ROM0 andROM1 are upgraded.

Upgrading the ROMMON on Cisco NCS 4201 and NCS 4202 Routers

Table 8: Feature History

Feature Name	Release Information	Description
Secondary ROMMON Version Auto Upgrade	Cisco IOS XE Bengaluru 17.5.1	After primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router.

Starting with Cisco IOS XE Bengaluru release 17.5.1, after primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router.

Note If the secondary ROMMON version is lesser than that of the primary ROMMON version, the secondary ROMMON gets auto upgraded.

The router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

1. Check the booted ROMMON region (ROM0 or ROM1). The example, shows the device booting up from ROM0 region.

   Example:

   ```
   System Bootstrap, Version 15.6(32r)S, RELEASE SOFTWARE (fc1)
   Technical Support: http://www.cisco.com/techsupport
   ```

```
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Thu 30-Aug-18 06:23 by pallavik
*Upgrade in progress* Boot ROM1
Last reset cause: BootRomUpgrade
link status 0
link status 0
UEA platform with 3670016 Kbytes of main memory
```

2. Copy the ROMMON pkg file **asr920_15_6_43r_s_rommon.pkg** to the bootflash.
3. Use the **upgrade rom-monitor filename asr920_15_6_43r_s_rommon.pkg all** command to upgrade the version.
4. Reload the router and ensure device is booted from upgrade region ROM0.

   Example:

```
System Bootstrap, Version 15.6(32r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Thu 30-Aug-18 06:23 by pallavik
Boot ROM1
Last reset cause: RSP-Board
Rommon upgrade requested
Flash upgrade reset 1 in progress
.......
System Bootstrap, Version 15.6(43r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2020 by cisco Systems, Inc.
Compiled Tue 19-May-20 22:55 by pallavik
*Upgrade in progress* Boot ROM0
Last reset cause: BootRomUpgrade
link status 0
link status 0
UEA platform with 3670016 Kbytes of main memory

We're coming up from a flash upgrade reset cookie
rommon 1 >
```

5. Repeat steps 3 and 4 to update the other region router (ROM1) region in this procedure.



Note We recommend you to upgrade that both ROM0 and ROM1 regions.

Starting with Cisco IOS XE Amsterdam 17.3.1 and higher, secondary partition upgrade is performed only after loading version 17.3.1 or higher.

Verifying ROMMON Upgrade on the Cisco NCS 4202

Use the **show platform** command to verify the ROMMON upgrade.

```
Router#show platform
Chassis type: NCS4202-SA

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      12xGE-4x10GE-FIXED  ok                    00:40:35
 0/1      NCS4200-3GMS        ok                    00:40:35
R0        NCS4202-SA          ok, active            00:47:43
F0                            ok, active            00:47:43
```

```
P0         ASR920-PSU0          ok                    00:45:37
P1         ASR920-PSU1          N/A                   never
P2         ASR920-FAN           ok                    00:45:36

Slot       CPLD Version         Firmware Version
---------  -------------------  ------------------------------------
R0         2008241E             15.6(54r)S
F0         2008241E             15.6(54r)S

Router#
```

Auto Upgrade

Table 9: Feature History

Feature Name	Release Information	Description
Secondary ROMMON Version Auto Upgrade	Cisco IOS XE Bengaluru 17.5.1	After primary ROMMON version is auto upgraded, secondary ROMMON version auto upgrade process takes place. The secondary ROMMON upgrade is only completed during the next planned manual reload of the router.

- The ROMMON image upgrade from Cisco IOS XE Release 3.x to Cisco IOS XE Everest Release 16.5.1 is *not* mandatory. We recommend a ROMMON upgrade for effective utilization of the new features delivered in Cisco IOS XE Everest 16.5.1 and later releases.
- We recommend you to reload the router two times for successful ROMMON and software image upgrade.
- You cannot expand the Cisco IOS XE Release 16.x image into the Cisco IOS XE Release 3.x images. The bin. file may be used to reload the image.
- Before installing the Cisco IOS XE Amsterdam Release 17.3.1, you *must* upgrade the ROMMON to version 15_6_43r_s or higher to avoid bootup failure. Booting in sub package mode takes care of auto upgrade to ROMMON version 15_6_43r_s on bootup. This workaround is not applicable to devices installed with ROMMON version 15.6(9r)S.
- For Cisco IOS XE Amsterdam Release 17.3.x, a minimum diskspace of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a diskspace lesser than 2 MB, ROMMON auto upgrade fails and the router reboots.
- For Cisco IOS XE Amsterdam Release 17.3.x, Cisco IOS XE Bengaluru Release 17.4.x, and earlier, the secondary ROMMON partition is *not* auto upgraded. You must manually upgrade it using the **upgrade rom-mon filename** command.
- Secure ROMMON is supported from Cisco IOS XE Amsterdam Release 17.3.1 onwards. However, it is compatible with all the releases.
- Any future secure ROMMON upgrade or downgrade is only possible from Cisco IOS XE Amsterdam Release 17.3.1 onwards.
- Starting with Cisco IOS XE Bengaluru Release 17.4.1, Cisco NCS 4201 and Cisco NCS 4202 routers are auto upgraded to ROMMON version 15_6_44r_s.

- Starting with ROMMON release version 15.6(43r)S, ROMMON version is secure. Once the ROMMON version is upgraded, it cannot be downgraded to a non-secure ROMMON version.
- Starting with Cisco IOS XE Bengaluru Release 17.5.1, secondary ROMMON partition is also auto upgraded after a successful primary ROMMON partition upgrade is complete. You can reload the router at the next planned reload to complete the secondary ROMMON upgrade.



Note If the secondary ROMMON version is lesser than that of the primary ROMMON version, the secondary ROMMON gets auto upgraded.

- Any non-secure FPGA bundled releases moving to Cisco IOS XE Bengaluru Release 17.3.x or future releases can result in an FPGA upgrade and a ROMMON upgrade. If FPGA upgrade happens parallely with the ROMMON upgrade, you can only expect a single reload. If FPGA upgrade gets delayed and happens post ROMMON upgrade, two reloads are expected to complete both the upgrade processes. This is followed by a successful bootup of the target release image.

  However, starting with Cisco IOS XE Bengaluru Release 17.5.1, for Cisco NCS 4201 and Cisco NCS 4202 routers, ROMMON and FPGA upgrade are synchronized to happen in a single reload.

Upgrading Firmware of the Power Supply Monitoring Device

Table 10: Feature History

Feature Name	Release Information	Feature Description
Upgrading Power Supply Monitoring Firmware	Cisco IOS XE Bengaluru 17.6.1	This feature allows you to manually upgrade the firmware of the power supply monitoring device in a router. The firmware upgrade reduces unplanned hardware-related downtime caused by input voltage transients during a power outage.

Starting with Cisco IOS XE Bengaluru 17.6.1, you can manually upgrade the firmware of the power supply monitoring device in a router. The firmware upgrade reduces unplanned hardware-related downtime caused by input voltage transients during a power outage.

Supported Platforms

Table 11: Feature History

Feature Name	Release Information	Description
Support for Firmware Upgrade	Cisco IOS XE Cupertino 17.9.1	This release introduces the firmware upgrade support for ASR 920-10SZ-PD and Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, and Cisco ASR-920-24TZ-M routers.

Starting with Cisco IOS XE Cupertino Release 17.9.1, firmware upgrade is supported on the following routers:

- ASR 920-10SZ-PD
- ASR-920-24SZ-IM
- ASR-920-24SZ-M
- ASR-920-24TZ-M

The firmware upgrade reduces unplanned hardware-related downtime caused by input voltage transients during a power outage.

- NCS4202-SA using A920-PWR400-D power supply

Restrictions for Upgrading the Firmware

- Automatic firmware upgrade is not supported, you must upgrade it manually.
- For the upgrade to take effect, the router reboots automatically, which results in a service interruption for a few minutes.

Caution Ensure that there's a stable power supply during the firmware upgrade. This mitigates any unplanned hardware-related downtime in a router.

Upgrading the Firmware Manually

To upgrade the firmware, you should perform the following steps:

Procedure

Step 1 Execute the **show upgrade hw-programmable** command to display the current firmware version.

Example:

```
Router#show upgrade hw-programmable adm 0 firmware-version
Hw-programmable ADM Firmware Versions

version[0]                version[1]                version[2]
------------------------------------------------------------------------------
0                         1                         0
```

Step 2 Execute the **upgrade hw-programmable** command to upgrade the firmware.

Example:

```
Router#upgrade hw-programmable adm 0
*Jan 27 06:47:45.760: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 f/w upgrade,
*Jan 27 06:47:45.764: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 CONF EEPROM erase,
*Jan 27 06:47:46.312: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 CONF EEPROM program,
*Jan 27 06:47:47.089: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 CONF EEPROM verify,
*Jan 27 06:47:47.546: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 CONF EEPROM verify done,
*Jan 27 06:47:47.547: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 SE EEPROM erase,
*Jan 27 06:47:48.222: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 SE EEPROM program,
*Jan 27 06:47:49.213: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 SE EEPROM verify,
*Jan 27 06:47:49.714: %IOSXE-3-PLATFORM: F0: cmand: ADM1066 SE EEPROM verify done,
*Jan 27 06:47:49.714: %IOSXE-3-PLATFORM: F0: cmand: ADM Upgrade Completed System Going for
 Power Cycle
Router#
System Bootstrap, Version 15.6(43r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2020 by cisco Systems, Inc.
Compiled Mon 18-May-20 03:16 by pallavik
Starting Initialization of FMAN0
Loading ucode for FMAN0, size: 31424, ver: 106.04.14
Silicon Rev Major:Minor [1:1]
Initializing the pci..
IOFPGA version[2008241e]
Boot ROM1
Last reset cause: PowerOn
UEA platform with 1048576 Kbytes of main memory
```

Step 3 Execute the **show upgrade hw-programmable** command to verify the upgrade.

Example:

```
Router#show upgrade hw-programmable adm 0 firmware-version
Hw-programmable ADM Firmware Versions

version[0]                version[1]                version[2]
------------------------------------------------------------------------------
0                         1                         1
```

Note

- For Cisco NCS4202-SA, the current firmware version is 0.1.0 and the upgraded version is 0.1.1.

Loading the New Image and Preparing for Upgrade

The following sections describe the steps required to load a new image and prepare for an upgrade.

Creating a Service Upgrade Directory

Before creating a new Service Upgrade directory, verify if that directory already exists in the bootflash of the active and standby RSPs.

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx            16384  Jan 12 2016 02:05:30 +00:00  lost+found
310689  drwx             4096  May 10 2016 17:14:20 +00:00  .prst_sync
   12  -rwx           145860  Jul 30 2016 00:12:46 +00:00  smartdebug.tcl
523265  drwx            77824  Jul 31 2016 15:52:38 +00:00  tracelogs
   13  -rwx             7074  Jan 12 2016 02:06:34 +00:00  tracelogs.508
179873  drwx             4096  Jul 21 2016 21:59:18 +00:00  core
98113  drwx             4096  Jan 12 2016 02:19:45 +00:00  .rollback_timer
605025  drwx             4096  Jan 12 2016 02:20:40 +00:00  .installer
752193  drwx             4096  Jul 29 2016 23:48:14 +00:00  su
```

If the SU directory exists, skip to Deleting an Existing packages.conf File.

If the directory does not exist in the bootflash, create the directory by running the following command:

```
Router# mkdir su
Create directory filename [su]?
Created dir bootflash:/su
```

Deleting an Existing packages.conf File

Before loading the new image to bootflash:su/, you must delete the existing packages.conf file. This step is required only if the bootflash:su/ directory already existed in the bootflash and contains an expanded image with a packages.conf file.

Note Remove all other unused images (.bin, or expanded image with .conf and .pkg as file extensions) from the existing SU directory.

To delete packages.conf on the active RSP:

```
Router# delete bootflash:su/packages.conf

Delete filename [su/packages.conf]?
Delete bootflash:su/packages.conf? [confirm]
```

Repeat this procedure on the standby RSP by running the command **delete stby-bootflash:su/packages.conf**.

If you created the SU directory in the previous step, skip to Copying the Image to bootflash:su/.

Copying the Image to Bootflash

Caution Ensure that upgrade image that you have chosen is supported by your current software version.

From the privileged EXEC mode:

```
Router# copy usb0:ncs4200rsp3-universalk9_npe.03.18.08v.S.156-2.S8v-std.bin bootflash:su/

Destination filename [su/ncs4200rsp3-universalk9_npe.03.18.08v.S.156-2.S8v-std.bin]?
```

For more information on copying the image from a remote server, seehttp://www.cisco.com/c/en/us/td/docs/routers/ncs4200/configuration/guide/sysmgmt/sysimgmgmt-ncs4200-book.html.

Preparing System for Upgrade

The system is ready for upgrade only if this meets the following conditions:

- The value of the configuration register is set to either 0x2 or 0x2102. These values ensure that the system boots using a specified image in the NVRAM.

  ```
  Router# show bootvar
  BOOT variable = bootflash:su/packages.conf,12;
  CONFIG_FILE variable =
  BOOTLDR variable does not exist
  Configuration register is 0x2
  ```

  If the value of the configuration register is not 0x2 or 0x2102, set the correct value by running the following command:

  ```
  Router# configure terminal
  Router(config)# config-register 0x2
  ```

- The system boot statement points to the packages.conf. This ensures that the systems boots using the packages.conf file.

  ```
  Router#show running-config | section boot
  boot-start-marker
  boot system bootflash:su/packages.conf
  boot-end-marker
  ```

  If the system boot statement points to a different file, delete that file and point the boot statement to the correct file by running the following commands:

  ```
  Router# configure terminal
  Router(config)# no boot system
  Router(config)# boot system bootflash:su/packages.conf
  Router(config)# do copy running-config startup-config
  Router(config)# exit
  Router# reload
  ```

Note A system reload affects all services on the system.

Upgrading the Cisco NCS4200 Series Chassis

The following sections describe:

- Upgrading a single-RSP chassis with boot in sub-package mode
- Upgrading a redundant-RSP chassis with boot in sub-package mode

Upgrading a Single-RSP Chassis With Boot in Sub-package Mode

This section describes the standard procedure for all upgrades in an NCS4200 chassis with a single RSP.

Note Ensure that you have followed all instructions in the previous sections to ensure an efficient upgrade.

Expanding the Consolidated Image and Reloading to the New Image

```
Router# request platform software package expand file
bootflash:su/ncs4200rsp3-universalk9_npe.03.18.07v.S.156-2.S7v-std.bin
Router# reload
```

Caution A system reload affects all services on the system.

Note Connectivity to the system is lost while the RSP reboots. Wait for 15 minutes and then reconnect to the system.

Verifying the New Image

After reloading the new image on the chassis, you must verify that the correct image was reloaded.

```
Router# show version

Cisco IOS XE Software, Version 03.18.08v.S - Standard Support Release
```

Upgrading the Firmware on the CEM Cards

First, verify the firmware version on the CEM cards.

```
Router# show hw-module all fpd

==== ====================== ====== ============================================
                             H/W  Field Programmable
                                                    Current      Min. Required
Slot Card Type             Ver.  Device: "ID-Name"  Version      Version
== ====================== ====== ================== =========== ==============
 0/0 NCS4200-1T8LR-PS        1.0   32-UEA 8x1G 1x10G   69.22        69.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/2 NCS4200-1T8LR-PS        1.0   32-UEA 8x1G 1x10G   69.22        69.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/3 NCS4200-48T3E3-CE       0.1   44-UEA LOTR DSX FP  1.22         1.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/4 NCS4200-48T1E1-CE       0.1   44-UEA LOTR DSX FP  1.22         1.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/5 NCS4200-1T8S-10CS       0.2   43-UEA EOWYN OCX F  1.12         1.12
```

To upgrade the firmware version, run the following command to reset and reload the new version.

```
Router# upgrade hw-module subslot 0/4 fpd bundled reload
% Are you sure that you want to perform this operation? [no]: yes
```

Caution A module reload affects all services on that module.

Upgrading the Redundant-RSP Chassis With Boot in Sub-package Mode

This section describes the standard procedure for all upgrades in an NCS4200 chassis with a redundant RSP.

Note Ensure that you have followed all instructions in the previous sections to ensure an efficient upgrade.

Confirming Stateful Switch-Over Configuration

If IGP and MPLS are configured on the chassis, it is recommended that NSR or NSF configuration are enabled for IGP and MPLS. These configuration reduce the loss of traffic during RSP switchover during the upgrade process.

Before upgrading a redundant-RSP chassis, verify if the *redundancy* and *mode sso* are set.

```
Router# show running-config | section redundancy
redundancy
mode sso
```

If the above values are missing, run the following commands to configure the chassis for SSO redundancy:

```
Router(config)# redundancy
Router(config-red)# mode sso
Router# exit

Router# show redundancy states | include peer
peer state = 8 -STANDBY HOT
Router#
```

Note The standby RSP should be in 'STANDBY HOT' state.

Upgrading Using a Single Command

The single-command upgrade initiates the installation procedure using the consolidated image.

You can adjust the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM) using the **interface-module-delay** keyword.

Warning It is recommended to set the value of the **interface-module-delay** to 1200 seconds or more to ensure sufficient time for IM software upgrades.

```
Router# request platform software package install node file bootflash:issu/
ncs4200rsp3-universalk9_npe.03.18.06v.S.156-2.S6v-std.bin interface-module-delay 1200
```

Caution In case of firmware upgrade on an IM, the IM is reset and services on the IM are affected.

Note Connectivity to the system is lost while the active RSP switches over to the standby RSP. Wait for a minute and then reconnect to the system.

Verifying the New Image

After reloading the new image on the chassis, you must verify that the correct image was reloaded.

```
Router# show version

Cisco IOS XE Software, Version 03.18.08v.S - Standard Support Release
```

Upgrading the Firmware on the CEM Cards

First, verify the firmware version on the CEM cards.

```
Router# show hw-module all fpd

==== ====================== ====== ===============================================
                              H/W  Field Programmable
                                                    Current      Min. Required
Slot Card Type             Ver.  Device: "ID-Name"  Version      Version
== ==================== ====== ================== =========== ==============
 0/0 NCS4200-1T8LR-PS        1.0   32-UEA 8x1G 1x10G   69.22        69.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/2 NCS4200-1T8LR-PS        1.0   32-UEA 8x1G 1x10G   69.22        69.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/3 NCS4200-48T3E3-CE       0.1   44-UEA LOTR DSX FP  1.22         1.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/4 NCS4200-48T1E1-CE       0.1   44-UEA LOTR DSX FP  1.22         1.22
---- ---------------------- ------ ------------------ ----------- --------------
 0/5 NCS4200-1T8S-10CS       0.2   43-UEA EOWYN OCX F  1.12         1.12
```

To upgrade the firmware version, run the following command to reset and reload the new version.

```
Router# upgrade hw-module subslot 0/4 fpd bundled reload
% Are you sure that you want to perform this operation? [no]: yes
```

Caution A module reload affects all services on that module.

Verifying the Upgrade

Example: Single Command Software Upgrade

```
Router# request platform software package install node file bootflash:XE371_k9_0810.bin
interface-module-delay 150


NOTE: Currently node has booted from a provisioning file
```

```
NOTE: Going to start a dual rp sub-packages node ISSU install
--- Starting initial file path checking ---
Copying bootflash:XE371_k9_0810.bin to stby-bootflash:XE371_k9_0810.bin
Finished initial file path checking
--- Starting config-register verification ---
Finished config-register verfication
--- Starting image file expansion ---
Expanding image file: bootflash:XE371_k9_0810.bin
Image file expanded and copied
Expanding image file: stby-bootflash:XE371_k9_0810.bin
Image file expanded and copied
Finished image file expansion
STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Found asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Found asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished compatibility testing
```

```
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
 Added asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.
STAGE 2: Restarting standby RP
==============================
--- Starting standby reload ---
Finished standby reload
--- Starting wait for Standby RP to reach terminal redundancy state ---
Finished wait for Standby RP to reach terminal redundancy state
STAGE 3: Installing sipspa package on local RP
==============================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
WARNING:
```

```
WARNING: Candidate software combination not found in compatibility database
WARNING:
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Software sets are identified as compatible
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished compatibility testing
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-sipspa.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting IM: 0/0
Skipping IM reload for Ethernet IM
  Restarting IM: 0/1
Skipping IM reload for Ethernet IM
  Restarting IM: 0/2
Skipping IM reload for Ethernet IM
  Restarting IM: 0/3
Skipping IM reload for Ethernet IM
  Restarting IM: 0/4
Skipping IM reload for Ethernet IM
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
STAGE 4: Installing software on active RP
=========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
```

```
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Found asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Found asr903rsp1-sipspa.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Verifying image file locations
Inspecting image file types
    WARNING: In-service installation of IOSD package
    WARNING: requires software redundancy on target RP
    WARNING: or on-reboot parameter
    WARNING: Automatically setting the on-reboot flag
    WARNING: In-service installation of RP Base package
    WARNING: requires software reboot of target RP
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
Determining whether installation is valid
Determining whether installation is valid ... skipped
Verifying image type compatibility
Checking IPC compatibility for candidate software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Checking package specific compatibility
Finished compatibility testing
--- Starting list of software package changes ---
Old files list:
  Removed asr903rsp1-espbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpaccess.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpbase.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpcontrol.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-rpios-universalk9_npe.2012-08-12_15.26_amprajap.pkg
  Removed asr903rsp1-sipbase.2012-08-12_15.26_amprajap.pkg
New files list:
  Added asr903rsp1-espbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpaccess.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpcontrol.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
  Added asr903rsp1-rpios-universalk9_npe.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg

  Added asr903rsp1-sipbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Finished list of software package changes
--- Starting commit of software changes ---
```

```
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.
STAGE 5: Restarting active RP (switchover to stdby)
================================================
--- Starting active reload ---
Finished active reload
SUCCESS: node ISSU finished successfully.
RUDY-1#
RUDY-1#Aug 24 07:54:41.715 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: reload fru
 action requested
System Bootstrap, Version 15.3(1r)S1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Tue 26-Jun-12 12:42 by ccai
Current image running: Boot ROM0UEA platform with 3670016 Kbytes of main memory
Located packages.conf
Image size 7519 inode num 38, bks cnt 2 blk size 8*512
#
Located asr903rsp1-rpbase.BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021.pkg
Image size 34216240 inode num 90631, bks cnt 8354 blk size 8*512
################################################################################
################################################################################
################################################################################
########################################################################
Boot image size = 34216240 (0x20a1930) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
        calculated e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d
        expected   e7674970:dbc1eb86:325219c7:b3da0e0f:077e5e4d
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): load_crash_kernel took: 2 seconds, expected
max time 2 seconds
%IOSXEBOOT-4-DEBUG_CONF: (rp/0): File /bootflash/debug.conf is absent, ignoring
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): Chassis initialization took: 26 seconds,
expected max time 10 seconds
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (rp/0): upgrade hw-programmable took: 2 seconds,
expected max time 2 seconds
             Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M),
Experimental Version 15.2(20120810:081250)
[v152_4_s_xe37_throttle-BLD-BLD_V152_4_S_XE37_THROTTLE_LATEST_20120810_070021-ios 131]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 10-Aug-12 03:50 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
```

```
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco ASR-903 (RSP1) processor with 540359K/6147K bytes of memory.
Processor board ID FOX1518P0GP
32768K bytes of non-volatile configuration memory.
3670016K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
Press RETURN to get started!
```



Note

```
scanning usb for storage devices... 1 Storage Device(s) found
```

In the above output, the USB and storage device denote the following:

- **“scanning usb for storage devices”**---> It is a print that indicates to check as a part of USB scanning.
- **1 Storage Device(s) found**---> This denotes the number of storage devices that are found. The default bootflash is a storage device, hence it shows as above.

The system always counts the internal bootflash as one storage device. So even without a USB, it shows as 1 device found. When a USB is connected and detected, the message updates to:

```
scanning usb for storage devices... 2 Storage Device(s) found
```

This indicates that:

- 1 device = bootflash
- 1 device = USB

Secure eUSB Configuration

Table 12: Feature History

Feature Name	Release Information	Description
Secure eUSB Configuration	Cisco IOS XE Bengaluru 17.6.1	Use the **platform secure-cfg** command to provide enhanced security to the routers.

Effective with Cisco IOS XE Bengaluru Release 17.6.1, use the **platform secure-cfg** command to provide enhanced security to the routers. When you enable the command, the router does not boot if the eUSB is

replaced, swapped, or modified externally. Thus, you cannot format the eUSB externally and this prevents the misuse of the router.

This feature is applicable on the Cisco NCS4216-RSP routers.

To enable the **platform secure-cfg** command:

```
Router#enable
Router#configure terminal
Router(conf)#platform secure-cfg
Router(conf)#end
Router# write memory
```

Use the following command to verify that the **platform secure-cfg** command is enabled.

```
Router#show running-config | i secure-cfg
platform secure-cfg
```

Software Upgrade Process Using Install Commands

Cisco ASR 900 Series Aggregation Services Routers support In-Service Software Upgrades (ISSU) procedure to upgrade the software. The *ISSU-using-install-cmds-for-RSP3* feature introduces a new method of software upgrade process by using the install command for Cisco ASR 903 Series Aggregation Services Routers.



Note Starting with Cisco IOS XE Amsterdam 17.3.1, the Install Workflow based ISSU method is supported on the Cisco RSP3 module .

Prerequisite

- Ensure that the standby RP is in the standby-hot state.
- Enable autoboot when using the install command so that the device is automatically reloaded with the configuration registry using the boot system command.

Guidelines

- Perform software upgrade process only during a maintenance window.
- Do not enable new features during a software upgrade process as it may require configuration changes.

Sub-Package Upgrade

Upgrading Software Using Step-By-Step Workflow

The step-by-step workflow involves, to add, activate, and commit the configuration. After activation, all the cards are upgraded to the new software version but does not commit automatically. You must manually commit using the install commit command. The advantage is that, it allows the system to roll back to a previous software version. The system automatically rolls back if the rollback timer is not stopped using the install abort-timer-stop command. If the rollback timer is stopped, then the new software version could be run on the device for any duration and then roll back to the previous version.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **install add file {bootflash:| tftp:}**

Example:

```
Router# install add tftp bootflash:
```

Downloads the image into the bootflash. The image is copied to the boot directory (boot_dir), the location where Route Processors (RPs) are booted.

Step 3 **install activate issu [linecard-delay seconds]**

Example:

```
Router# install activate issu
```

Provisions the standby RP with the new software and reloads with the new software version.

- linecard-delay *seconds* — Waits for a specified duration before upgrading the next slot.
- The rollback timer will be restarted.

Step 4 **install commit**

Example:

```
Router# install commit
```

Saves the configuration, performs the necessary clean-up, enables the new software as permanent (removing the older version of the software) and stops the rollback timer.

Note
There is no rollback when this command is used.

Upgrading Software Using Single-Step Workflow

The single-step workflow involves, to add, activate, and commit the configuration. Rollback is not supported, as the upgrade is committed automatically.

Rollback

You can rollback the system before a commit. You can rollback a device to the initial stage using the **install abort issu** command or after the expiry of the rollback timer before the install commit command is used. If the install commit command is used, then rollback is not allowed.

Rollback involves the following:

- Provision and reset the standby RP.
- Provision and reset the active RP.

If the rollback timer is not stopped by using the **install abort stop-timer** command, the device rolls back to an earlier software version on expiry of the rollback timer. The default value of the rollback timer is 120 minutes.

The rollback timer value can be set via the **install activate location standby auto-abort-timer seconds** command.

Performing Single-Step Workflow

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **install add file {bootflash: | tftp: } activate issu [linecard-delay seconds] commit**

Example:

```
Router# install add tftp bootflash: activate issu commit
```

Enables the standby RP with new software and triggers the standby RP to become active RP with new software version.

- linecard-delay *seconds* — Waits for a specified duration before upgrading the next slot.
- commit — Saves the configuration, performs the necessary clean-up, enables the new software as permanent (removes the older version of the software) and stops the rollback timer. Any reboot after the commit, boots with the new software. There is no rollback when this keyword is used.

Tracking Software Upgrade

You can track the ISSU progress using the **show issu state detail** command.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS master command list	Cisco IOS Master Command List , All Releases
Cisco IOS High Availability commands	*Cisco IOS High Availability Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html