Cisco ASR 9000 Series Aggregation Services Router Release 5.3.4

Upgrade and Downgrade Procedure

Contents

1. Introduction 3
1. Purpose, Audience and Scope 3
2. Summary of Upgrade Steps 3
3. Cisco Software Manager 4
4. Mandatory SMUs 4
5. Selection of Packages for Upgrade 4
2. Upgrade to IOS XR Release 5.3.4 6
3. Turboboot Option for Upgrades 7
4. FPD Upgrade 7
5. Downgrade from IOS XR Release 5.3.4 8
6. ISSU SMU Upgrade in IOS XR Release 5.3.4 8
7. Caveats 9

1. Introduction

1. Purpose, Audience and Scope

The purpose of this document is to describe the upgrade and downgrade procedure for the Cisco ASR 9000 Series

Aggregation Services Router, Release 5.3.4

Audience: This guide is for Cisco Systems Field Engineers and Network

Operators. It's split into four sections.

1) Simple one command install upgrade process & detailed IOS XR install upgrade process
2) Turboboot (Highly NOT recommended)
3) FPD upgrades
4) Caveats and CLI changes

2. Summary of Upgrade Steps

1. IOS-XR upgrade from pre-4.2.1 is not supported and has not been covered in testing, the upgrade from pre 4.2.1 can be attempted through a standard Turbo boot method or install upgrade, and caveats may apply. Please review the install cheat sheet for short cuts. https://supportforums.cisco.com/document/12440491/ios-xr-install-upgrade-cheat-sheet

2. It's highly recommended that CSM is used to come up with a list of optimized set of SMUs or Service Packs which should be installed on the release that is going to be deployed. SMUs/SP + Major release can be installed together in one install operation to save time and avoid multiple reloads. For more information on Service packs, see the following link, when possible it's always preferred to deploy Service Packs http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xr-software/117550-technote-product-00.pdf

4. (Optional) before an upgrade, Bridge SMU's may need to be installed on the current release to ensure that installation of new software succeeds. Check section "Mandatory SMUs" and download the ASR9k-iosxr-px-5.3.4-bridge_smus.tar file if required. Extract only **the** packages that are applicable to your currently running release. Install activate these prior to upgrading the router to the new release. No Bridge SMUs are required to upgrade from any release after 4.3.x.

5. For upgrading from Pre - 5.3.1 images to 5.3.4 you must install a post-expiry SMU along with the new root certificate. You can install additional SMUs or pie files after adding the post-expiry SMU.

   Refer below link for details:

   http://www.cisco.com/c/en/us/td/docs/routers/technotes/MOP-CSS-to-Abraxas.html

   Hitless/Recommended SMU, Post-Expiry-Cert Expiration Mandatory SAM SMU.

3. Cisco Software Manager

Cisco Software Manager (CSM) can be used to manage SMUs, to create your own SMU tarball, or find out which SMUs are applicable to your network. More information on CSM:

Download CSM
http://software.cisco.com/download/release.html?mdfid=282414851&flowid=2137&softwareid=284777134&release=2.0&relind=AVAILABLE&rellifecycle=&reltype=latest

User Documentation: http://www.cisco.com/en/US/docs/routers/asr9000/software/smu/csmuser.html

CSMServer 3.3 has been released, it does Major, Minor Release and SMU upgrade or downgrade automation, conformance reporting, as well as many other productivity and automation tasks.

https://software.cisco.com/download/release.html?mdfid=283876390&flowid=34962&softwareid=284777134&release=3.3&relind=AVAILABLE&rellifecycle=&reltype=latest

4. Mandatory SMUs

The following table outlines the SMUs that must be installed for upgrade and downgrade procedure.

Table 1. Needed Mandatory SMUs

Release	Mandatory SMUs (p)		Mandatory SMUs (px)	
	Upgrade SMUs	**Downgrade SMUs**	**Upgrade SMUs**	**Downgrade SMUs**
R4.2.3	CSCud98419** CSCud37351 CSCud54093		CSCud98419** CSCud37351 CSCud54093	
R5.1.0	Not Applicable	Not Applicable	No	CSCui99165
R5.3.4	Not Applicable	Not Applicable	No	No

** The SMU for CSCud98419 should be used if fpd auto-upgrade option is being used during the upgrade.

Please refer to Section 4 for more information. CSCud37351 and CSCud54093 are the pre-requisite SMUs for CSCud98419.

5. Selection of Packages for Upgrade

As software features grow, so do file sizes. So in order to ease the downloading experience and TFTP size issues, Cisco is changing its package delivery system by providing multiple files of smaller sizes as shown below:

Table 1- New IOS-XR Packaging Format (Beginning R5.1.3)

#	File	Contents	Comment
1	ASR9k-iosxr-px-5.3.4-bridge_smus.tar	Contains all bridge SMUs + other miscellaneous SMUs	Important – If applicable, Bridge SMUs are loaded onto your existing XR version before upgrading to R5.3.4. Refer to Section 9 for a list of mandatory SMUs and install as needed.

2	ASR9K-iosxr-px-5.3.4-turboboot.tar	Only the mini-vm file	Once installed, you will need to load the optional packages in Row 3 or Row 4 to complete the installation
3	ASR9K-iosxr-px-5.3.4-pies.tar	The mini.pie + optional packages (e.g., mcast, mpls, etc.). No mini-vm file.	The mini.pie constitute the base package. Optional packages add features as needed. No Mini.vm and no k9-sec pie.
4	ASR9k-iosxr-px-5.3.4-k9-pies.tar	Same as Row 3 + k9-sec pie	Contains Line item-3 + K9sec pie.

2. Upgrade to IOS XR Release 5.3.4

All install operations must be performed in **"admin"** mode. The optional packages (mpls, mcast, mgbl etc...) that are being installed/upgraded must match the active packages, else the install will fail.

Cisco recommends that you do a backup of the ASCII configuration to the harddisk: or off box location

Two install options are covered; the first is a single command install upgrade. The second is two command install upgrade.

1. *Single command upgrade:* **"admin install add <pkgs+smus or SP> activate"**

IOS XR install upgrades can be performed with a single command, in the format of **"admin install add <pkgs+smus or SP or TAR> activate"** and **"admin install commit"** after the operation is completed. Examples of popular single command install:

Example 1) Standard install
A9K-PE1(**admin**)#install **add** source tftp://10.10.10.1/ asr9k-px-5.3.4.CSCcd54321.pie asr9k-px-5.3.4.CSCab12345.pie asr9k-px-5.3.4.CSCef12345.pie activate

Example 2)This is an example of a create your own TAR install:
A9K-PE1(**admin**)#install **add** source tftp://10.10.10.1/ Rel5_3_1.tar **activate**

Example 3)If the file server is reachable through a vrf, in the example here the vrf name is "**management**":
A9K-PE1(**admin**)#install **add** source ftp://root:root@1.1.1.1;management/ asr9k-px-5.3.4.CSCcd54321.pie asr9k-px-5.3.4.CSCab12345.pie asr9k-px-5.3.4.CSCef12345.pie **activate**

2. *Two command upgrade:*

The above can be broken down into two operations if needed. Perform **"admin install add <pkgs+smu's or SP>"** to copy the software from TFTP/SFTP/SCP/FTP server to the router. *This is a hitless operation and can be formed outside a maintenance window.* Example:

A9K-PE1(**admin**)#install **add** source tftp://10.10.10.1/ asr9k-mini-px.pie-5.3.4 asr9k-mpls-px.pie-5.3.4 asr9k-mcast-px.pie-5.3.4 asr9k-px-5.3.4.CSCab12345-0.0.0.pie synchronous

Or a TAR

A9K-PE1(**admin**)#install **add** source tftp://10.10.10.1/ Rel5_3_4.tar synchronous

1. After the add is successful perform **"admin install activate <pkgs+smus or SP>"** on packages, SMU's or SP to activated, at this point the router will reboot. After the router has reloaded and sufficient checks have been done, then perform the following steps. **"admin install commit" this** will make the software (packages and smu's) persistent across reloads.

A9K-PE1(admin)# install activate disk0:asr9k-mini-px-5.3.4 disk0:asr9k-mpls-px-5.3.4 disk0:asr9k-mcast-px-5.3.4 asr9k-px-5.3.4.CSCab12345-0.0.0 synchronous

Another shortcut is to activate the install add operation id
A9K-PE1(admin)# install activate id <install add operation id>

Another shortcut is to activate with a wildcard:
A9K-PE1(admin)# install activate disk0:*5.3.4*

Note: use **ignore-pkg-presence-check** keyword if an upgrade is attempted without installing all the optional pies. This can be useful when offloading some unused pies. "*admin#install activate* **ignore-pkg-presence- check** <*operation id or package list*> "

2. It's recommended that **"auto fpd"** firmware upgrade is enabled prior to the upgrade. Refer to the FPD section for more details.
3. When the upgrade is completed and **"install commit" is** performed an **"install remove inactive" can** be used to clear old images from the disk. This is a hitless operation.
4. If the install operation fails collect the relevant show tech install output

3. Turboboot Option for Upgrades

Turboboot should not be necessary for an upgrade to XR5.3.4 if the instructions are followed that are documented. Any upgrade that is not part of the matrix may require a turboboot or has other possible requisitions.. Turboboot Instructions are well documented in this location:

https://supportforums.cisco.com/document/123576/asr9000xr-understanding-turboboot-and-initial-system-bring

4. FPD Upgrade

FPD upgrade is not mandatory it's a best practice, Auto-fpd feature is fully supported for upgrade from R4.2.3 onwards. The feature could be enabled from the admin-config mode as follows:

RP/0/RSP0/CPU0:router1(admin-config)# fpd auto-upgrade

Auto-fpd feature is not supported for upgrade from pre-R4.2.3. Please disable the feature from admin config mode if upgrading from a pre-4.2.3 release:
RP/0/RSP0/CPU0:router1(admin-config)# no fpd auto-upgrade.

Manual fpd upgrade can be performed after R5.3.4 upgrade is install committed. Run the "show hw-module fpd location all" command to check which firmware files need to be upgraded, by inspecting the Upg/Dng column. If there is any 'Yes' marked, manual upgrade is required. Issue the following command to upgrade FPD:

RP/0/RSP0/CPU0:router(admin)#**upgrade hw-module fpd all location all**

Note: Except CBC update, router reload is required after running the "upgrade hw-module fpd all location all" command, to make the changes in effect. No reload is required after running the upgrade **hw-module fpd cbc location all** command. The new CBC firmware will be active. The software automatically resets the local CAN Bus. FPD pie is mandatory for the above steps.

AutoFPD requirements:

1. CSCuj69940: Auto-FPD upgrade will not work if the source release does not have FPD Package installed and the user has configured auto-fpd prior to upgrade.
2. CSCul00317: Auto-FPD upgrade will not work if FPD being upgraded is 2 releases old or if no new FPD changes are available. Workaround is to perform a manual FPD upgrade.
3. CSCut97560: FPD upgrade (both auto and manual) fails if there is not enough space on harddisk: Workaround is to clear some unwanted files in the harddisk before doing the fpd upgrade

5. Downgrade from IOS XR Release 5.3.4

To Downgrade from 5.3.4 to 5.3.x/5.2.x/4.3.x (4.3.0, 4.3.1, 4.3.2, 4.3.4), if user has **not** performed "install commit" on Release 5.3.4, the router can be reverted back to its prior committed state by performing "reload location all" from admin mode. If the user has performed "install commit", then "install rollback to <>" procedure needs to be initiated. However, due to the linecard VSM introduction in 5.1.1, this "install rollback" would fail if the system has x86 based RP and a software fix is available in 5.1.2 and 5.2.0. Please do not use "install rollback.." command but as a workaround, use "install activate .." to go back to the previous image needed.

To Downgrade from 5.3.4 to pre-430 images, Turboboot is the only option. Due to CSCud37497, downgrade from R5.3.4 requires the **turboboot with the format option** (e.g., ROMMON Variable set as "TURBOBOOT=on, disk0, format"). This is because R5.3.4 image is a combo image unlike pre-430 images, which has –p and –px versions.

6. ISSU SMU Upgrade in IOS XR Release 5.3.4

ISSU SMU Upgrade is deprecated since XR 5.2.2

7. Caveats

The caveats listed below are summaries only. Please view each release note enclosure (RNE) for complete details (Including known workarounds and/or actions to take).

1. CSCun82453: Firmware upgrade for Delta V2 power module may fails.
2. CSCud63564: On downgrading to 4.2.3 and below with newer cards like VSM and A9K-40GE-SE/TR and to 4.3.0 with SIP-700(8G), shelfmgr process crashes followed by periodic router reloads are encountered.
3. CSCum75609: Image downgrades using "install rollback" will not work due to software changes introduced to accommodate a new line card type in R5.1.x/R5.2.x. Users are advised to use the "admin install activate" command instead.
4. CSCug38404: ROMMON downgrading isn't allowed on certain line cards with a 2.00 ROMMON Version. The downgrade operation will fail.
5. CSCtx28180: Due to the CLI change from "label-allocation-mode" to "label mode" introduced, when performing a software downgrade from R5.3.4 to R4.3.0 (or earlier), "label mode" configuration will be lost if any. It is recommended to remove "label mode" config and re-apply the Configuration as "label- allocation-mode" after the downgrade.
6. After upgrading to R5.3.4, OSPF area format error would be seen if the user has "area 0.0.0.0" configured in pre-4.3.1 releases. Change the OSPF area format from "area 0.0.0.0" to "area 0" before upgrading to R5.3.4
7. Release 5.1.1 introduces a new Services Line Card named 'VSM'[A9K-VSM-500], which requires 'services-infra' package. Refer to VSM install instructions for more details. Please refer to CGv6 Configuration Guide.

Note: 5.3.4 is the last release that will support the "Trident" generation cards.