



ASR9K

IOS-XR Release 7.11.2 (64-bit)

System Upgrade Procedure

Table of Contents

1 Introduction	3
1.1 Purpose, Scope and Audience	3
1.2 Version Upgrade Support	3
1.3 Summary of Upgrade Steps	3
1.4 Cisco Software Manager	4
1.5 Mandatory SMUs	4
1.6 Packages for Upgrade	5
1.7 Required & Optional Package files	6
2 Pre-Upgrade Tasks	8
2.1 Configuration Backup	8
2.2 System Stability check	9
2.3 Cost out IGP	10
2.4 Enable auto-fpd upgrade	10
2.5 Disk Cleanup	11
3 Software Upgrade	12
4 Post-Upgrade Tasks	14
5 GISO Install Procedure	15
6 Other Boot Options (IPXE/USB)	16
7 FPD Upgrade	17
8 Downgrade from 7.11.2 IOS XR Release	19
8.1 Pre-Downgrade Tasks	19
8.2 Downgrading IOS XR	19
8.3 Post-Downgrade Tasks	21
9 Caveats	22

1 Introduction

1.1 Purpose, Scope and Audience

The purpose of this document is to describe the upgrade and downgrade procedure for the Cisco ASR 9000 Series Aggregation Services Router, Release 7.11.2.

Audience: This guide is for Cisco Systems Field Engineers and Network Operators. It is split into four sections.

- 1) Simple one command install upgrade procedures & detailed IOS XR install upgrade procedures.
- 2) Other boot options
- 3) FPD upgrade
- 4) Caveats and CLI changes

1.2 Version Upgrade Support

These releases are taken from 7.11.2 Compatibility Matrix.

Single Step Upgrade is validated for following releases.

Platform	Validated From	To
ASR9K Fixed + Modular Chassis	7111,7921,7102,7101,792,791,782,781,772,771,762,761,752,751, 742,741,734,732,731,713,7.1.25,712,7.1.15,711,702,663	7.11.2

For downgrade from 7.11.2 to prior releases, please see Section 7: Downgrade from 7.11.2 IOS XR Release

1.3 Summary of Upgrade Steps

1. Backup existing configuration
 2. Perform system and network maintenance tasks.
 3. Copy the image to the router using tftp, http, sftp, scp
 4. Add the software to the router using install add source.
 5. Activate the image via install activate.
 6. Perform system and network stability check.
 7. Verify all the services are UP and operational.
 8. Commit the software via install commit.
- Following cards will not be supported from release:
 - No hardware is deprecated in 7.11.2.
 - Please refer to the following DDTs for the unsupported cards from release 6xx:
 - CSCuz35344

1.4 Cisco Software Manager

CSM Server is a web-based, server-side automation and orchestration framework. It gives service providers the ability to simultaneously schedule and deploy SMUs & software upgrades across hundreds of routers in a scheduled manner through a simple point and click Web interface. It can be used to manage SMUs, to create your own SMU tar ball, or find out which SMUs are applicable to your network.

More information on CSM: [Download CSM/ CSM Documentation](#)

1.5 Mandatory SMUs

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

Table 1: Mandatory SMUs

Release	Mandatory/Optional SMUs
	Upgrade SMUs
R6.6.3	CSCvw57276
R7.0.x	CSCvw57276
R7.1.15	CSCvw57276
R71x	N/A
R72x	N/A
R73x	N/A
R74x	N/A
R75x	N/A
R76x	N/A
R77x	N/A
R78x	N/A
R79x	N/A
R710x	N/A
R7111	N/A

* Above table applicable only to 64-bit IOS-XR.

1.6 Packages for Upgrade

As software features grow, so do file sizes. 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 2: New IOS-XR Packaging Format

File	Contents	Comment
asr9k-mini-x64-7.11.2.iso	64-bit mini.iso image only	Contains 64-bit mini.iso upgrade image only
ASR9K-x64-iosxr-px-7.11.2.tar	All 64-bit rpms. No mini.iso or k9sec rpm.	Contains all rpms except the mini.iso, and k9sec rpm
ASR9K-x64-iosxr-px-k9-7.11.2.tar	All 64-bit rpms. No mini.iso.	Contains all rpms including k9sec except the mini.iso rpm.
asr9k-cnbnng-x64-1.0.0.0-r7112.x86_64.rpm	cnBNG 64-bit rpm	Contains cloud native BNG user plane packages on Cisco IOS XR platform
ncs5k-mini-x-7.11.2.iso	NCS5000 satellite 64-bit image	The NCS5000 mini.iso
asr9k-mini-x64-migrate_to_eXR.tar-7.11.2	64-bit migration tarfile consists of mini.iso	64-bit migration tar file. Refer "ASR9K-Migration-to-ios-xr-64-bit" documentation on CCO.
asr9k-x64-usb_boot-7.11.2.zip	Cisco ASR9000 64-BIT IOS XR Software	Contains USB Boot Package

1.7 Required & Optional Package files

The mini ISO package is mandatory to perform the System Upgrade from the XR VM. The additional XR packages listed below are needed depending on the router configuration and required features.

Feature Set	Package Name	Description
Boot Image	asr9k-mini-x64-7.11.2.iso [Boot image]	Contains the required core packages, including OS, Admin, Base, Forwarding, Modular Services Card, Routing, FPD, SNMP Agent, and Alarm Correlation. The mini iso file is used for upgrading to the new release.
Mpls	asr9k-mpls-x64-1.0.0.0-r7112.x86_64.rpm	LDP, MPLS Forwarding, MPLS OAM, Link Manager Protocol Optical User Network Interface and Layer-3 VPN.
mpls-rsvp-te	asr9k-mpls-te-rsvp-x64-1.0.0.0-r7112.x86_64.rpm	MPLS Traffic Engineering (MPLS-TE), Resource Reservation Protocol (RSVP).
Bng	asr9k-bgp-x64-1.0.0.0-r7112.x86_64.rpm	Includes binaries to support BNG features.
bng-supp	asr9k-bng-supp-x64-1.0.0.0-r7112.x86_64.rpm	Includes binaries to support BNG features.
Cnbng	asr9k-cnbng-x64-1.0.0.0-r7112.x86_64.rpm	Includes cloud native BNG user plane packages
bng-ipoe	asr9k-bng-ipoe-x64-1.0.0.0-r7112.x86_64.rpm	Includes binaries to support BNG features.
bng-pppoe	asr9k-bng-pppoe-x64-1.0.0.0-r7112.x86_64.rpm	Includes binaries to support BNG features.
multicast	asr9k-mcast-x64-1.0.0.0-r7112.x86_64.rpm	Multicast Routing Protocols, Internet Group Management Protocol, Tools and Infrastructure and Bidirectional Protocol Independent Multicast.
Ospf	asr9k-ospf-x64-1.0.0.0-r7112.x86_64.rpm	Includes OSPF link state protocol support software
Isis	asr9k-isis-x64-1.0.0.0-r7112.x86_64.rpm	Includes IS-IS Link state protocol support software
Li	asr9k-li-x64-1.0.0.0-r7112.x86_64.rpm	Includes LI software images.
services	asr9k-services-x64-1.0.0.0-r7112.x86_64.rpm	Includes rpm to support Cisco IOS XR 64-bit inline MAP-T function
Eigrp	asr9k-eigrp-x64-1.0.0.0-r7112.x86_64.rpm	Includes EIGRP protocol support software

k9sec	asr9k-k9sec-x64-1.0.0.0-r7112.x86_64.rpm	Support for Encryption, Decryption,, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).
Mgbl	asr9k-mgbl-x64-1.0.0.0-r7112.x86_64.rpm	CORBA2 agent, XML3 Parser, and HTTP server packages. This RPM also contains some SNMP MIB infrastructure.
asr9000v	asr9k-9000v-nV-x64-1.0.0.0-r7112.x86_64.rpm	Includes rpm to support Cisco ASR9000v Series Router Software and to support Cisco ASR 9000v Series Router as a satellite for Cisco ASR 9000 Series Router
Optic	asr9k-optic-x64-1.0.0.0-r7112.x86_64.rpm	Firmware for the optics feature for Cisco ASR 9000 Series Aggregation Services Router Chassis. It enables Transport / OTN feature under interfaces.
m2m	asr9k-m2m-x64-1.0.0.0-r7112.x86_64.rpm	Machine to Machine communication software

Note: The physical BNG package (asr9k-bng-x64*.rpm) and the cnBNG package (asr9k-cnbnng-x64*.rpm) are mutually exclusive. You cannot install both the packages on the router. For installing the cnBNG package , please refer to the chapter “Installing Cloud Native BNG User Plane Packages” in “Cloud Native BNG User Plane configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x”

2 Pre-Upgrade Tasks

Note: Config backup, precheck, image download, tar file copy to router and install add are hitless operations and can be done outside of the upgrade maintenance window.

2.1 Configuration Backup

- 1) Copy the running-configuration to a harddisk: on the router:

```
RP/0/RP0/CPU0:ASR9K#copy running-config harddisk:/running_config
```

- 2) Copy the running-configuration to a remote server:

```
RP/0/RP0/CPU0:ASR9K#scp /harddisk:/<file name> <username>@<server-IP>:/<file name>/config
```

2.2 System Stability check

The following commands should be executed at the XR prompt to verify basic system stability before the upgrade.

show platform	verify that all nodes are in "IOS XR RUN/OPERATIONAL" state
show platform vm	verify that all nodes are in "FINAL Band" state
show redundancy	verify that a Standby RP is available and the system is in "NSR-ready" state
show ipv4 interface brief <or> show ipv6 interface brief <or> show interface summary	verify that all necessary interfaces are "UP"
show install active	verify that the proper set of packages are active
admin show install active	verify on sysadmin plane
show install committed	verify that the proper set of committed packages are same as active. If not, execute 'install commit'
cfs check/ clear configuration inconsistency	verify/fix configuration file system
show hw-module fpd	Ensure all the FPD versions status are CURRENT Please refer to "Field Programmable Versions Document" for FPD version information.
show pfm location all	Shows any outstanding alarms in system
show alarms	Shows any outstanding alarms in system
admin show environment all	Shows temperature, Fan, Voltage, Power status
admin show led	Shows LED status
show media (both XR and Admin mode)	Shows the disk usage in XR and admin state
show inventory	Shows chassis inventory information
show logging	Capture show logging to check for any errors

2.3 Cost out IGP

To minimize traffic loss during the upgrade please follow the below steps:

For OSPF use “max-metric” command.

```
RP/0/RP0/CPU0:ASR9K(config-ospf)# max-metric router-lsa
```

For ISIS use the “spf-overload-bit” command.

```
RP/0/RP0/CPU0:ASR9K(config-isis)# set-overload-bit
```

2.4 Enable auto-fpd upgrade

Enable auto FPD auto upgrade from XR and Sysadmin.

```
RP/0/RP0/CPU0:ASR9K(config)#fpd auto-upgrade enable  
RP/0/RP0/CPU0:ASR9K(config)#commit
```

```
sysadmin-vm:0_RP0(config)# fpd auto-upgrade enable  
sysadmin-vm:0_RP0(config)# commit
```

2.5 Disk Cleanup

Check the available space in install repository. At least 2G of free space is required to perform system upgrade. If copying the packages and SMUs to the harddisk, ensure 50% free space on the harddisk. Check both the XR and admin plane.

XR:

```
RP/0/RP0/CPU0:ASR9K# show media location 0/RP0/CPU0
```

```
RP/0/RP0/CPU0:ASR9K# show media location 0/RP1/CPU0
```

Admin:

```
sysadmin-vm:0_RP0# show media location 0/RP0
```

```
sysadmin-vm:0_RP0# show media location 0/RP1
```

Check inactive packages and remove them before upgrading in XR and Admin plane.

```
XR: RP/0/RP0/CPU0:ASR9K#install remove inactive all
```

```
Admin: sysadmin-vm:0_RP0# install remove inactive
```

Check and delete core files and any other files which are not required in harddisk in XR and admin plane.

XR:

```
RP/0/RP0/CPU0:ASR9K#run
```

```
[xr-vm_node0_RP0_CPU0:~]$cd /misc/disk1
```

```
[xr-vm_node0_RP0_CPU0:/misc/disk1]$rm *core*
```

Admin:

```
RP/0/RP0/CPU0:ASR9K#admin
```

```
sysadmin-vm:0_RP0# run
```

```
[sysadmin-vm:0_RP0:~]$ cd /misc/disk1
```

```
[sysadmin-vm:0_RP0:~]$ rm *core*
```

3 Software Upgrade

All System Upgrade related install operations should be done in the XR VM plane. The optional packages (mpls, mcast, mgbl etc.) that are being installed/upgraded must match the active packages, else the install will fail.

- Download the 7.11.2 image (mini.iso and optional RPMs .tar) from CCO. Untar the RPMs and create a single tar that includes the mini.iso and all optional RPMs. Copy tar file to scp server and verify the contents of the tar file:

```
tar -tvf 7.11.2-iso-and-rpms.tar
```

- Copy the 7.11.2 tar file to the router harddisk and verify that file is copied successfully:

```
RP/0/RP0/CPU0:ASR9K#scp <username>@<server-IP>://<file path>/<image file>  
/misc/disk1/.
```

- Verify the md5 checksum of the tar/individual rpms with the original MD5 values on CCO:

```
[xr-vm_node0_RP0_CPU0:/misc/disk1]$md5sum <tar file>
```

- Perform 'install add' of the 7.11.2 tar file:

```
RP/0/RP0/CPU0:ASR9K #install add source harddisk:/ 7.11.2-iso-and-rpms.tar
```

- Take a note of the install operation id generated by the add operation in previous step:

```
Install operation id# finished successfully.
```

- Copy & add recommended SMUs for 7.11.2 if not already in initial tarball (optional):

```
RP/0/RP0/CPU0:ASR9K#install add source harddisk: <SMU tar file>
```

- Take a note of the install operation id generated by the add operation in previous step.

```
Install operation id# finished successfully.
```

- Prepare the packages added in the previous step:

```
RP/0/RP0/CPU0:ASR9K#install prepare id id#
```

Or, if multiple add operations occurred:

```
RP/0/RP0/CPU0:A9K#install prepare id id1 id2
```

- Activate all the packages:

```
RP/0/RP0/CPU0:ASR9K#install activate
```

- Router will reload at the end of activation to start using the new packages.



This operation may take up to 30 minutes to complete.

- Verify that all the packages are installed correctly in XR and SysAdmin:

```
RP/0/RP0/CPU0:ASR9K#show install active
sysadmin-vm:0_RP0# show install active
```

- Verify system stability through commands described under Check System Stability section (2.2) after router comes up with new software.
- Verify show version to check router is upgraded:

```
RP/0/RSP0/CPU0:cnBNG-SRG2#sh version

Sat Mar 30 07:44:14.119 UTC

Cisco IOS XR Software, Version 7.11.2

Copyright (c) 2013-2024 by Cisco Systems, Inc.
```

Build Information:

```
Built By      : swtools
Built On      : Fri Mar 29 15:24:05 PDT 2024
Built Host    : iox-ucs-036
Workspace     : /auto/srcarchive11/prod/7.11.2/asr9k-x64/ws
Version       : 7.11.2
Location      : /opt/cisco/XR/packages/
Label        : 7.11.2
```

```
cisco ASR9K () processor
```

```
System uptime is 1 hour 16 minutes
```

- Check to see if there were startup configurations which failed:

```
RP/0/RP0/CPU0:ASR9K#show configuration failed startup
```

4 Post-Upgrade Tasks

1. Restore IGP metric if changed before the upgrade (this is done from xr vm).

OSPF

```
RP/0/RP0/CPU0:ASR9K# (config-ospf)# no max-metric router-lsa
```

ISIS

```
RP/0/RP0/CPU0:ASR9K# (config-isis)# no set-overload-bit
```



Make sure the system is stable and all the services are restored before performing install commit.

2. Execute 'install commit' to commit the newly active software (install commit is required after any install activate operation else after router reload, nodes will go back to previously committed software):

```
RP/0/RP0/CPU0:ASR9K#install commit
```

3. Disk cleanup: Once software upgrade has been completed, disk space can be recovered by removing any inactive packages that are no longer needed (if the packages are required at a later time, they can be re-added):

```
RP/0/RP0/CPU0:ASR9K#install remove inactive all
```

4. Verify/fix configuration file system (mandatory):

```
RP/0/RP0/CPU0:ASR9K#cfs check
```

5. Verify fpd versions running are current:

```
RP/0/RP0/CPU0:ASR9K#show hw-module fpd
```

5 GISO Install Procedure

For GISO, please refer to the chapter "Customize Installation using Golden ISO" in "System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers", IOS XR Release 24.1.x

<https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/system-setup/configuration/guide/b-system-setup-cg-asr9000-711x.html>

- Copy the 7.11.2 golden tar file to the router harddisk and verify that file is copied successfully:
RP/0/RP0/CPU0:ASR9K#scp <username>@<server-IP>://<file path>/<image file> /misc/disk1/.
- Verify the md5 checksum of the tar rpms with the original MD5 values on server:
[xr-vm_node0_RP0_CPU0:/misc/disk1]\$md5sum <tar file>
- Install the golden iso image

RP/0/RP0/CPU0:ASR9K# install replace harddisk://< asr9k-goldenk9-x64-7.11.2-PROD_BUILD_7_11_2 >
noprompt

- Router will reload at the end of activation to start using the new packages.



Note

This operation may take up to 30 minutes to complete.

- Verify that all the packages are installed correctly in XR and SysAdmin:
RP/0/RP0/CPU0:ASR9K#show install active
sysadmin-vm:0_RP0# show install active

Commit active packages.

RP/0/RP0/CPU0:ASR9K# install commit

6 Other Boot Options (IPXE/USB)

For USB and iPXE, please refer to the chapter "Bring-up the Router" in "System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers", IOS XR Release 7.11.x

For instructions on migration to 64-bit, please refer to the following document:

<https://www.cisco.com/c/en/us/td/docs/routers/asr9000/migration/guide/b-migration-to-ios-xr-64-bit.html>

For instructions on upgrading nvSatellite, please refer to the following documents:

<https://www.cisco.com/c/en/us/support/docs/routers/asr-9000-series-aggregation-services-routers/118807-technote-asr-00.html>

Please refer to the chapter "Configuring the Satellite Network Virtualization (nV) System" in "nV System Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x"

<https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/nv-system/configuration/guide/b-nv-system-cg-asr9000-711x.html>

7 FPD Upgrade

Automatic FPD Upgrade

If you enable the 'fpd auto-upgrade enable' command, FPD images are automatically updated when:

- Software upgrade is carried out.
- Line cards are added to an existing router or reloaded.

The following conditions must be met for an Automatic FPD Upgrade to work on a system upgrade:

- The 'fpd auto-upgrade enable' command must be configured in both XR Configuration and Admin configuration mode.

Note:

1. In all cases where the automatic FPD upgrade is not performed, you must perform a manual FPD upgrade using the 'upgrade hw-module location <> fpd <>' command.
2. Although the FPD upgrade is performed during the install operation, there is no install commit performed. Therefore, once the FPD has been upgraded, if the image is rolled back to the original version, the FPD version is **not** downgraded to the previous version.
3. **Power Module** upgrades are time consuming and cannot be implicitly upgraded as a part of automatic FPD upgrades. These modules must be upgraded independent of the other fpga upgrades.

Manual FPD Upgrade

Manual FPD upgrade on CISCO IOS XR 7.11.2 release can be performed after image upgrade is install committed. Use the “show hw-module fpd location all” command to determine if an FPD upgrade is required.

Check for NEED UPGD in the Status column. If there are any marked ‘NEED UPGD’, manual upgrade is required.

Use the show fpd package command to find out which FPGAs are supported with your current software release and minimum hardware requirements for each module.

Issue the following command to upgrade FPD:

```
RP/0/RP0/CPU0:ASR9K#upgrade hw-module location all fpd all
```

```
RP/0/RP0/CPU0:ASR9K#upgrade hw-module location <node> fpd <specific fpd>
```

Note:

1. The FPD upgrade procedure is performed while the card is online.
2. At the end of the procedure the card must be reloaded before the FPD upgrade is complete. To reload the card, you can use the ‘**hw-module location <location> reload**’ command in Admin mode.
3. During the FPD upgrade, you *must not* do the following:
 - Reload, perform an online insertion and removal (OIR) of a line card (LC), or power down the chassis. Doing so may cause the node to enter an unusable state.
 - Press Ctrl-C if the console appears to hang without any output. Doing so may abort the upgrade.
4. No reload is required after running the ‘upgrade hw-module location <> fpd cbc’ command as the new CBC firmware will be active. The software automatically resets the local CAN Bus. FPD pie is mandatory for the above steps.
5. 711x, we are bringing in Parallel PEM level FPD upgrade. Main goal here is to decrease the power module FPD upgrade time taken without disturbing the system. We will bringdown the power module before FPD upgrade starts. We will check the Total power capacity in the node is greater than the total power required then only, we can bringdown the power module and upgrade the FPD. Total power capacity > Total power required. [CSCwd87559 - Parallel PM FPD upgraded support at PEM level"]

```
RP/0/RP0/CPU0:ASR9K#upgrade hw-module location pm-all fpd all
```

8 Downgrade from 7.11.2 IOS XR Release

Please see Section 8: Caveats, item number 2, for caveats specific to downgrading from 7.11.2 to prior IOS-XR releases.

8.1 Pre-Downgrade Tasks

If, after upgrading to 7.11.2, hardware was inserted that is not supported by the release to which you are about to downgrade, please remove that hardware from the equipment before the downgrade. Please refer to the target release's hardware support documentation, or the module's hardware data sheet, for software and hardware support details.

8.2 Downgrading IOS XR

There are multiple options to choose from to downgrade IOS XR.

If FPD upgrade was done as part of 7.11.2 installation, FPDs do not need to be updated again once the previously published image is activated.

Option 1: If install commit was not done after upgrade to 7.11.2, a router reload will bring it back to previous install committed image.

Option 2: Use install add, prepare and activate to install a CCO image with a lower version.

Example:

```
install add source harddisk: asr9k-mini-x64-7.6.1.iso ASR9K-x64-iosxr-px-k9-7.6.1.tar

install prepare id <id>

install activate id <id> noprompt

install commit
```

Option 3: If downgrade image is present in inactive packages, "install activate <package list>" can be used to activate the image on the router.

Collect the list of inactive packages using "show install inactive summary", e.g.:

```
asr9k-xr-7.6.1

asr9k-common-7.6.1

asr9k-m2m-x64-2.0.0.0-r761
```

```

asr9k-isis-x64-1.1.0.0-r761
asr9k-k9sec-x64-2.1.0.0-r761
asr9k-li-x64-1.1.0.0-r761
asr9k-mpls-x64-2.0.0.0-r761
asr9k-services-x64-1.0.0.0-r761
asr9k-optic-x64-1.0.0.0-r761
asr9k-ospf-x64-1.0.0.0-r761
asr9k-mcast-x64-2.0.0.0-r761
asr9k-mpls-te-rsvp-x64-2.1.0.0-r761
asr9k-mini-x64-7.6.1
asr9k-9000v-nV-x64-1.0.0.0-r761
asr9k-bng-x64-1.0.0.0-r761
asr9k-mgbl-x64-2.0.0.0-r761
asr9k-eigrp-x64-1.0.0.0-r761
asr9k-bng-suppl-x64-1.0.0.0-r761

```

Use “install activate <list of inactive packages, separated by spaces>” to activate the software on the router. Exclude the package starting with asr9k-xr- & asr9k-common-:

```

install activate asr9k-m2m-x64-2.0.0.0-r761 asr9k-isis-x64-1.1.0.0-r761
asr9k-k9sec-x64-2.1.0.0-r761 asr9k-li-x64-1.1.0.0-r761 asr9k-mpls-x64-
2.0.0.0-r761 asr9k-services-x64-1.0.0.0-r761 asr9k-optic-x64-1.0.0.0-r761
asr9k-ospf-x64-1.0.0.0-r761 asr9k-mcast-x64-2.0.0.0-r761 asr9k-mpls-te-rsvp-
x64-2.1.0.0-r761 asr9k-mini-x64-7.6.1 asr9k-9000v-nV-x64-1.0.0.0-r761 asr9k-
bng-x64-1.0.0.0-r761 asr9k-mgbl-x64-2.0.0.0-r761 asr9k-eigrp-x64-1.0.0.0-r761
asr9k-bng-suppl-x64-1.0.0.0-r761

```

Option 4: Install remove the inactive packages and re-add the downgrade iso image+rpm via install add, prepare, activate to downgrade

Note: Please refer to the caveats section prior to downgrading.

8.3 Post-Downgrade Tasks

1. Disk cleanup: Once software upgrade has been completed, disk space can be recovered by removing any inactive packages that are no longer needed. If the packages are required at a later time, they can be re-added:

```
RP/0/RP0/CPU0:ASR9K#install remove inactive all
```

2. Verify/fix configuration file system (mandatory):

```
RP/0/RP0/CPU0:ASR9K#cfs check
```

3. Verify fpd versions running are current:

```
RP/0/RP0/CPU0:ASR9K#show hw-module fpd
```

4. Restore IGP metric if changed before the upgrade (this is done from xr vm)

OSPF

```
RP/0/RP0/CPU0:ASR9K# (config-ospf)# no max-metric router-lsa
```

ISIS

```
RP/0/RP0/CPU0:ASR9K# (config-isis)# no set-overload-bit
```

9 Caveats

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

- CSCvp19524: If downgrading from 7.11.2 to any release lower than 742 This downgrade path is exposed to CSCwb36344 which causes the system to land up in an irrecoverable state. Please refer to CSCwb36344's RNE or the document upgrade-downgrade-guide-ASR9K-eXR-xr 7112 for more details."CSCwi95358, CSCwh61644
- CSCwb36344: Software downgrade can fail from 7.6.1 and later releases (including 7.11.2) to releases lower than 7.6.1. Stub implementation of the DLLs may be loaded on the router instead of full DLLs during downgrade via the XR install process, which can result in continuous multiple process crashes and respawns due to undefined symbols on the RP and LC(s).
 - Recommended workaround:
 - If you are upgrading from an older release to CISCO IOS XR 7.11.2, do not perform install commit after upgrade. If reverting to the prior image is required, a hw-module reload of the system will revert to the previously committed software image
 - CSCwd30936 : Process "ema_server_sdr" crashed if downgrading from 7112 to older release
 - In scenarios where the above are not available options, the following may be alternative workarounds:
 - Software installation via iPXE or USB
 - If 7.6.1, or a later release such as 7.11.2, is the committed software on the system and a downgrade to an older release is required, Engineering SMU for CSCwb36344 for the older release can be provided. The packages used for the initial release downgrade must consist only of the release default .iso and packages, plus the SMU for CSCwb36344. After downgrade, perform install commit, deactivate the packages for CSCwb36344, and proceed to add any other required or recommended SMUs for the release. Please contact your TAC representative for more details.