

Cisco NCS5700

IOS-XR7 Release 24.2.11

IOS-XR7 System Upgrade Procedure

Table of Contents

1 Introduction	3
1.1 Purpose, Scope and Audience	3
1.2 Summary of Upgrade Steps	3
1.3 Upgrade/Downgrade Matrix and Bridge SMUs	3
1.4 Packages for Upgrade	5
1.5 Required Package files	5
2 Pre-Upgrade Task	6
2.1 Configuration Backup	6
2.2 System Stability check	6
2.3 Cost out IGP	7
2.4 Enable auto-fpd upgrade	7
2.5 Disk Cleanup	7
2.6 Managing External server/repo reachability	7
3 Software Upgrade.....	9
3.1 Single-Command Upgrade using install replace	9
3.2 Multi-Step Upgrade (install package replace & install apply)	10
3.3 Optional packages installation procedure	11
4 Post Upgrade Tasks	13
5 Other Boot Options (GISO/IPXE/USB)	14
6 Downgrade from 24.2.11 IOS XR Release	15
6.1 Post Downgrade Tasks	15
7 FPD	16
8 Caveats.....	17

1 Introduction

1.1 Purpose, Scope and Audience

The purpose of this document is to describe the upgrade and downgrade procedure for the Cisco NCS 5700 Series Network Convergence System Router, Release IOS-XR 24.2.11

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

Single Step Upgrade is supported for following releases:

Platform	Supported From	To
NCS5700L	IOS-XR 7.5.2/7.6.2/7.7.2/7.7.21/7.8.x/7.9.x/ 7.10.x/7.11.x/24.1.x	IOS-XR 24.2.11

Supported variants under NCS5700L:

- NCS-57B1-6D24-SYS/NCS-57B1-5DSE-SYS
- NCS-57C1-48Q6-SYS
- NCS-57D2-18DD-SYS

1.2 Summary of Upgrade Steps

1. Perform install replace to do single-command upgrade.
(or)
Perform install package replace, install package add <optional rpm> and install apply reload.
2. Perform install commit to save the upgrade.

1.3 Upgrade/Downgrade Matrix and Bridge SMUs

Bridge SMU – Bridge SMUs need to be present on the running software, and

Target SMU – target SMUs need to be present in the target software (via a GISO)

For certain upgrade/downgrade paths, bridge SMU for upgrade and target SMU for downgrade is required when we are moving to/from 24.2.11 image.

NCS5700							
Device	From Release	To Release	Bridge SMU	Device	From Release	To Release	Bridge SMU
NCS5700	2421	24211		NCS5700	24211	2421	
NCS5700	2412	24211		NCS5700	24211	2412	
NCS5700	2411	24211		NCS5700	24211	2411	
NCS5700	7112	24211		NCS5700	24211	7112	
NCS5700	7111	24211		NCS5700	24211	7111	
NCS5700	7102	24211		NCS5700	24211	7102	
NCS5700	7101	24211		NCS5700	24211	7101	
NCS5700	7721	24211		NCS5700	24211	7721	Target SMU CSCwd71524
NCS5700	791	24211		NCS5700	24211	791	
NCS5700	792	24211		NCS5700	24211	792	
NCS5700	782	24211		NCS5700	24211	782	Target SMU CSCwd71524
NCS5700	781	24211		NCS5700	24211	781	Target SMU CSCwd71524
NCS5700	772	24211		NCS5700	24211	772	Target SMU CSCwd71524
NCS5700	762	24211		NCS5700	24211	762	Target SMU CSCwd71524
NCS5700	752	24211	CSCwd71524	NCS5700	24211	752	Target SMU CSCwd71524



IMP Note :- Following limitations are applicable for all downgrade paths other than 7.10.x/7.11.x

1. To ensure config preservation, use the **install replace <ISO>** command to perform upgrades and downgrades between different XR versions.
2. Cannot run “install commit” after downgrade as transaction is automatically committed.
3. Cannot rollback by performing reload after downgrade as operation gets automatically committed.
To revert to the previous XR version replace or reimage to the relevant ISO
4. XR config history is lost after downgrade. Note that, XR config will be preserved.
5. XR config history is lost except for last operation (the downgrade operation) after downgrade.
6. Longer downtime than usual downgrades as the operation is performed via a reimage
7. Cannot downgrade using “install package replace” command, must use “install replace”. This means there is no control over when the reload occurs.
8. Any 3rd party apps will need to be reinstalled after the downgrade is complete.
9. Type 6 encryption config will be lost post downgrade. To restore the config - Type 6 master key will have to be reconfigured with command “key config-key password-encryption” command and configuration needs to be re-applied.
10. Crypto keys and certificates will have to be regenerated after downgrade

1.4 Packages for Upgrade

Following files are available to download for various boot options:

Table 1: IOS-XR Software files available for download

#	File	Contents	Comment
1	ncs5700-x64-24.2.11.iso	NCS 5700 IOS XR Software	Contains Boot image
2	ncs5700-x64-k9sec-rpms.24.2.11.tar	NCS 5700 IOS XR Software 3DES	Contains k9sec rpm
3	ncs5700-x64-usb-24.2.11.zip	NCS 5700 IOS XR Software	Contains USB Boot Package
4	ncs5700-x64-optional-rpms.24.2.11.tar	NCS 5700 IOS XR Software	Optional Packages

1.5 Required Package files

Mini ISO Package is mandatory to perform the System Upgrade and upgrade needs to be done from XR VM.

Description	Package Name
Boot Image	ncs5700-x64-24.2.11.iso

2 Pre-Upgrade Task



Note

Note: Config backup, precheck, Image download, tar file copy to router and install add are hitless operation and can be done outside of MW.

2.1 Configuration Backup

- Copy the running-configuration to a harddisk: on the router.

```
RP/0/RP0/CPU0:57XX# copy running-config harddisk:/running_config
```

- Copy the running-configuration to a remote scp server

```
RP/0/RP0/CPU0:57XX#scp harddisk:/running_config <user_name>@<server ip>:/<path>
```

2.2 System Stability check

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

show platform	Verify that all nodes are in "IOS XR RUN/OPERATIONAL" 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
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 configuration file system To 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 alarms	Shows any outstanding alarms in system
show media	Shows the disk usage
show inventory	Shows chassis inventory information
show logging	Capture show logging to check for any errors

2.3 Cost out IGP:

Cost-out IGP: To minimize traffic loss during the upgrade please follow below steps:

For OSPF use “max-metric” command.

```
RP/0/RP0/CPU0:57XX(config-ospf)# max-metric router-lsa
```

For ISIS use “set-overload-bit” command.

```
RP/0/RP0/CPU0:57XX(config-isis)# set-overload-bit
```

2.4 Enable auto-fpd upgrade:

Enable auto FPD auto upgrade from XR if it is not already enabled on the router.

```
RP/0/RP0/CPU0:57XX(config)#fpd auto-upgrade enable
RP/0/RP0/CPU0:57XX(config)#commit
```

Note: From 781, it will be enabled by default without any explicit configuration from user.

2.5 Disk Cleanup:

Check available space in install repository. At least 2G of free space is required to perform System upgrade. If user is going to copy the packages and SMU's to the harddisk, please ensure enough free space is available on the harddisk.

```
RP/0/RP0/CPU0:57XX# show media location 0/RP0/CPU0
```

2.6 Managing External server/repo reachability:

Install replace using external server (http/ftp) or installing rpm/smu via external/remote repo requires connectivity from router Linux NW stack to external server, since the install infra uses ‘curl’ Linux utility to access it.

1. If the connectivity to external server is via an In-band data port ethernet interface:
 - a. Please verify that external server is able to reach the router's lowest-numbered loopback interface (Ex:Loopback0), since the Linux networking uses loopback as source interface. Ping should work from external server to router's lowest-numbered loopback interface IP address.

Alternatively, from router bash prompt, please verify the ping to external server is working.

```
RP/0/RP0/CPU0:Router#bash
[Router:~]$ping <server-ip>
```

Ping should be working to external server from router's bash prompt.

<or>

- b. If connectivity is instead needed to an external server that cannot route to the lowest-numbered loopback interface of router, then user must manually add a new route to Linux with source ip which will help in connectivity.

Example:

```
RP/0/RP0/CPU0:Router#bash
[Router:~]$ ip route add <server-ip/mask> dev to_xr scope link
src <source-ip>
```

```
[Router:~]$ping <server-ip>
```

Ping should be working to external server from router's bash prompt.

2. If the connectivity to external server is via the Management interface:

User should add a static route on bash routing table to reach external server via Mgmt. interface, since by default Linux networking will be using router's lowest-numbered loopback interface as source and static route from XR will not be imported into bash.

CLI to add static route:

```
RP/0/RP0/CPU0:Router#bash
[Router:~]$ ip route add <server-ip/mask> via <Mgmt. gateway IP>
dev Mg0_RP0_CPU0_0
```

Verify ping after adding static route:

```
RP/0/RP0/CPU0:Router#bash
[Router:~]$ping <server-ip>
```

Ping should be working to external server from router's bash prompt.

3 Software Upgrade

3.1 Single-Command Upgrade using install replace:



Cisco recommends using this single cli – ‘install replace’ method to perform system upgrade.

Step 1. Download the image from CCO and Copy the ISO (or GISO) image to the remote server location.

Verify that the md5 checksum on remote server matches with CCO

Upgrade the system to replace the current software with the .iso image and activate it using http/ftp option

Example for http:

```
Router#install replace http://<httpserver-ip>/<PATH OF IMAGE>/ncs5700-x64-24.2.11.iso noprompt
```

Example for ftp:

```
Router#install replace ftp://<ftpserver-ip>/<PATH OF IMAGE>/ncs5700-x64-24.2.11.iso noprompt
```

<or>

Download the image from CCO and Copy the ISO (or GISO) image to the `hddisk:` location on the router

Verify that the md5 checksum on router `hddisk:` matches with CCO

Upgrade the system to replace the current software with the .iso image and activate it.

Example:

```
Router#install replace /hddisk:/ncs5700-x64-24.2.11.iso noprompt
```

Step 2. Verify that the image is activated successfully.

Example:

```
Router#show install request
Router#show install active summary
```

Step 3. Commit the transaction and execute show version to check the details.

Example:

```
Router#install commit
```

Example:

```
RP/0/RP0/CPU0:ROUTER #show version
Cisco IOS XR Software, Version 24.2.11 LNT
Copyright (c) 2013-2024 by Cisco Systems, Inc.
```

Build Information:

```
Build By   : cisco
Build On   : Tue Jul 02 14:32:37 UTC 2024
Build Host : iox-ucs-067
```

Workspace : /auto/srcarchive11/prod/24.2.11/ncs5700/ws/
Version : 24.2.11
Label : 24.2.11-Renum

cisco NCS5700 (D-1633N @ 2.50GHz)
cisco NCS-57D2-18DD-SYS (D-1633N @ 2.50GHz) processor with 32GB of memory
NC57D2-PE45 uptime is 9 hours, 18 minutes
NCS 57D2 7.2T Fixed Base Chassis 66 QSFP-DD flexible ports

3.2 Multi-Step Upgrade (install package replace & install apply):

This method is used to install iso along with optional rpms. This will require user to perform ‘install package replace’ to upgrade iso followed by ‘install package add’

Step 1. Download the image from CCO and Copy the ISO (or GISO) image to the remote server location.

Verify that the md5 checksum on remote server matches with CCO

Upgrade the system to replace the current software with the .iso image using http/ftp option

Example for http: (Assume 10.1.1.1 is HTTP server IP)

```
Router#install package replace http://10.1.1.1/<PATH OF  
IMAGE>/ncs5700-x64-24.2.11.iso
```

Example for ftp: : (Assume 10.1.1.1 is FTP server IP)

```
Router#install package replace ftp://10.1.1.1/<PATH OF  
IMAGE>/ncs5700-x64-24.2.11.iso
```

<or>

Download the image from CCO and Copy the ISO (or GISO) image to the `harddisk:` location on the router

Verify that the md5 checksum on router `harddisk:` matches with CCO

Upgrade the system to replace the current software with the .iso image

Example:

```
Router#install package replace /harddisk:/ncs5700-x64-24.2.11.iso
```

Step 2. (Optional step) Install optional rpm or smu rpm using method described in section 3.3

Step 3. Activate the new .iso image and rpm added on the router by applying the changes.

Example:

```
Router#install apply reload noprompt
```

Include the keyword `noprompt` in the command to enable the system to bypass your permission to reload the router.

Step 4. Verify that the image is activated successfully.

Example:

```
Router#show install request  
Router#show install active summary
```

Step 5. Commit the transaction and execute show version to check the details.

Example:

```
Router#install commit
```

Example:

```
RP/0/RP0/CPU0:ROUTER #show version
Cisco IOS XR Software, Version 24.2.11 LNT
Copyright (c) 2013-2024 by Cisco Systems, Inc.
```

Build Information:

```
Built By   : cisco
Built On   : Tue Jul 02 14:32:37 UTC 2024
Build Host : iox-ucs-067
Workspace  : /auto/srcarchive11/prod/24.2.11/ncs5700/ws/
Version    : 24.2.11
Label      : 24.2.11-Renum
```

```
cisco NCS5700 (D-1633N @ 2.50GHz)
cisco NCS-57D2-18DD-SYS (D-1633N @ 2.50GHz) processor with 32GB of memory
NC57D2-PE45 uptime is 9 hours, 54 minutes
NCS 57D2 7.2T Fixed Base Chassis 66 QSFP-DD flexible ports
```

3.3 Optional packages installation procedure

- Copy the required RPMs in a repository and make sure the repository and server is reachable from the router.
- Repository can be hosted locally on the router or on a remote server which is reachable over http/https/ftp
- Creating a local repository:
 1. Create a directory under the /harddisk:/, say "new_repo"
 2. Copy the rpm .tgz/.tar file on the router under this "new_repo" directory
 3. Unzip and untar all the .tgz/.tar file: "tar -xzvf <rpm tar ball>"
 4. Convert the dir into repository by running 'createrepo_c </repo-dir-path/>' on router linux prompt
 5. Configure the local repository on XR, as per below example

Sample config of local repository:

```
RP/0/RP0/CPU0:iso#show run install
install
 repository new-repo
  url file:///misc/disk1/new_repo
!
```

- Creating a remote repository:
 1. Identify a remote linux machine which is reachable over http/https/ftp from router
 2. Create a directory, say 'repo' under the http root dir(ideally '/var/www/html/') on the remote server
 3. Copy the rpm .tgz/.tar file to the remote server inside the 'repo' directory
 4. Unzip and untar all the .tgz/.tar file: "tar -xzvf <rpm tar ball>"
 5. Convert the dir into repository by running 'createrepo --database </repo-

dir-path/>' on remote server

- 6. Configure the remote repository on XR, as per below example.

Sample config of remote repository:

```
RP/0/RP0/CPU0:ios#show run install
install
 repository repo
  url http://192.168.1.20/repo
!
```

- Check 'show install available' to make sure the RPMs are available to install.

Sample output:

```
RP/0/RP0/CPU0:ios#show install available
Trying to access repositories...
```

Package Repository	Architecture	Version
xr-cdp local-repo	x86_64	24.2.11v1.0.0-1
xr-eigrp local-repo	x86_64	24.2.11v1.0.0-1
xr-telnet local-repo	x86_64	24.2.11v1.0.0-1
xr-syslog local-repo	x86_64	24.2.11v1.0.1-1

- Install optional rpm packages as shown below:

```
RP/0/RP0/CPU0:ios#install package add xr-cdp xr-telnet
```

NOTE: Do not use 'install package upgrade', it is used when installing packages of different versions/smu fixes.

- Install smu rpm packages as shown below:

```
RP/0/RP0/CPU0:ios#install package upgrade xr-syslog
```

- Once this operation is completed, execute the below command:

```
RP/0/RP0/CPU0:ios#install apply reload
```

- After reload, once the device is up with latest image, perform the install commit:

```
RP/0/RP0/CPU0:ios#install commit.
```

4 Post Upgrade Tasks

- Verify/fix configuration file system (mandatory):

```
RP/0/RP0/CPU0:57XX#cfs check
```

- Verify fpd versions running are current:

```
RP/0/RP0/CPU0:57XX#show hw-module fpd
```

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

OSPF

```
RP/0/RP0/CPU0:57XX# (config-ospf)# no max-metric router-lsa
```

ISIS

```
RP/0/RP0/CPU0:57XX# (config-isis)# no set-overload-bit
```

- Check to see if there were any failed startup configurations.

```
RP/0/RP0/CPU0:57XX#show configuration failed startup
```

- Make sure install commit is done post upgrade. This can be checked via “show install committed”. If committed version is showing as previous version, then 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/CPU0:57XX#install commit
```

5 Other Boot Options (GISO/IPXE/USB)

Please refer below for various boot options:

Router Bring up:

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-setup/77x/b-system-setup-cg-ncs5500-77x/m-ncs5700-system-setup.html>

GISO/IPXE and USB Boot option:

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-setup/77x/b-system-setup-cg-ncs5500-77x/m-additional-install-operations.html>

Please find below the link for more information about installation of optional rpms.

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/system-setup/77x/b-system-setup-cg-ncs5500-77x/m-install-ios-xr-software.html>

6 Downgrade from 24.2.11 IOS XR Release

Downgrade can be performed by following options.

Using install replace method as described in section 3.1 with downgrade version iso file.

Example:

```
Router#install replace /harddisk:/<downgrade iso> noprompt
```

6.1 Post Downgrade Tasks

- Verify/fix configuration file system (mandatory):

```
RP/0/RP0/CPU0:57XX#cfs check
```

- Verify fpd versions running are current:

```
RP/0/RP0/CPU0:57XX#show hw-module fpd
```



If FPD upgrade was done as part of IOS-XR 24.2.11 installation, FPDs do not need to be updated again once the downgrade version is activated.

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

OSPF

```
RP/0/RP0/CPU0:57XX(config-ospf)# no max-metric router-lsa
```

ISIS

```
RP/0/RP0/CPU0:57XX(config-isis)# no set-overload-bit
```

- If downgrade version is 7.10.x then install commit needs to be performed.

7 FPD

From release 781 onwards, fpd auto upgrade is enabled by default (without any configuration applied by user) for NCS5700 based XR7 platforms.

However, the configuration support (fpd auto-upgrade enable/disable) will still be in place and honored by XR incase if the user wants to enable/disable it.

8 Caveats

1. Please refer to section 1.3 table for Upgrade/Downgrade Matrix and Bridge SMUs
2. CSCwh99825: Upon downgrading the NCS5700 router's software from release 24.2.11 to the 78x release, an issue has been identified where the router unexpectedly powers down in about 4 minutes after getting downgraded to 78x. FAN Out of Tolerance critical alarms are observed on the router which triggers a system shutdown.

Include fix of CSCwh99825 in the 78x release to prevent unexpected shutdowns of the NCS5700 router, when router is downgraded from 24211 to 78x.