

XR 12000 Upgrade Procedure:

3.4.x - 3.7.x to 3.8.2

1.	Obtain Required PIE files:	2
2.	Install Mandatory SMUs.....	2
3.	Check System Stability:.....	2
4.	Perform Pre-Upgrade Tasks:.....	3
5.	Upgrade:.....	6
6.	Downgrade:.....	9
7.	Post-Upgrade / Post-Downgrade Procedure:	10
8.	Caveats:.....	11

For the latest upgrade documents please refer to the following page:

http://www.cisco.com/web/Cisco_IOS_XR_Software/index.html

1. Obtain Required PIE files:

Composite Mini Package is mandatory to perform the upgrade. Additional pies listed below are needed depending on the router configuration and required features:

PIE File Description	Sample PIE Filename	Default Package Name
Composite Mini Package (OS-MBI, Base, Admin, Fwdg, Ic Rout)	c12k-mini.pie-3.8.2	disk0:c12k-mini-3.8.2
Multicast Package	c12k-mcast.pie-3.8.2	disk0:c12k-mcast-3.8.2
Manageability Package	c12k-mgbl.pie-3.8.2	disk0:c12k-mgbl-3.8.2
MPLS Package	c12k-mpls.pie-3.8.2	disk0:c12k-mpls-3.8.2
Security Package	c12k-k9sec.pie-3.8.2	disk0:c12k-k9sec-3.8.2
Diagnostic package	c12k-diags.pie-3.8.2	disk0:c12k-diags-3.8.2
Firewall Package	c12k-firewall.pie-3.8.2	disk0:c12k-firewall-3.8.2
Documentation package	c12k-doc.pie-3.8.2	disk0:c12k-doc.pie-3.8.2
Field Programmable Device package	c12k-fpd.pie-3.8.2	disk0:c12k-fpd.pie-3.8.2

Note1: The filenames listed here may not necessarily be the filenames of the actual files since the files can be renamed. The actual filenames used will not affect the operation.

2. Install Mandatory SMUs

N/A

3. Check System Stability:

The following commands should be executed to verify basic system stability before the upgrade:

(admin) `show platform` (verify that all nodes are in "IOS XR RUN" state, PLIM's in "OK" and SPAs in "READY" state)

`show redundancy` (verify that a Standby RP is available and in "ready" state)

`show ipv4 interface brief <or> show ipv6 interface brief <or> show interface summary` (verify that all interfaces are "UP")

`show install active` (verify that the proper set of packages are active)

cfs check/clear configuration inconsistency (verify/fix configuration file system in exec and admin mode)

4. Perform Pre-Upgrade Tasks:

- 1) Due to increasing size of the images sufficient disk space is required to perform the upgrade. 2Gig flash disk option was first introduced in release 3.7.0, optional 4Gig one is available starting 3.8.x release.

When upgrading to release 3.8.2, a PCMCIA flash disk of 2Gig or larger has to be installed in the system BEFORE the software upgrade is performed.

Use "show filesystem" command to check the actual disk0 size:

```
RP/0/RP0/CPU0:Router#sho filesystem
Wed July 30 15:28:57.401 PST PST
File Systems:

      Size (b)      Free (b)      Type  Flags  Prefixes
      -          -          network  rw  qsm/dev/fs/tftp:
      -          -          network  rw  qsm/dev/fs/rcp:
      -          -          network  rw  qsm/dev/fs/ftp:
      1043456      1005568  dumper-lnk  rw  qsm/dumper_nvram:
39929724928 39605428224  dumper-lnk  rw  qsm/dumper_harddisk:
      1004994560      184500224  dumper-lnk  rw  qsm/dumper_disk1:
      1024606208      423608320  dumper-lnk  rw  qsm/dumper_disk0:
      62390272       49101348  dumper-lnk  rw
qsm/dumper_bootflash:
39929724928 39605428224  harddisk  rw  harddisk:
      1024606208      423608320  flash-disk  rw  disk0: ←-----
      1004994560      184500224  flash-disk  rw  disk1:
      1043456       1005568      nvram      rw  nvram:
      62390272       49101348      flash      rw  bootflash:
```

If the disk size is smaller than 2Gig please follow "Cisco XR 12000 and CRS-1 Flash Disk Upgrade Tasks" document which can be found at:

http://www.cisco.com/web/Cisco_IOS_XR_Software/index.html

Note1: if you have already loaded the installation files for the new operating system version onto the router, the 'install remove inactive' will delete these files! Therefore, only load the new packages (via 'install add') after removing the inactive packages.

Note2: In order to provide as much room as possible on the disk, one can remove old files from the disk. This may include files which the operator has placed on the disk device such as .pie files or temporary directory that have been created.

When preparing for the upgrade to the next version of the operating system, the old, non-operational version should be removed.

To remove old SMU files and old versions of the operating system use the admin-commands

install commit

to ensure all active packages are 'committed', then issue the command

install remove inactive

The 'install remove inactive test sync' commands can be used first to show which packages will be removed from the disk.

Note3: In addition to checking the installation disk device, the bootflash device on the MSCs should also be checked. Extraneous files such as crashinfo files can be removed. To check the free space of the bootflash use the following command:

dir bootflash: location 0/1/CPU0

- 2) To minimize traffic loss during the upgrade please follow below steps:
 - a. Make sure that all the traffic flowing through the router which needs to be upgraded has an alternate path. In this scenario one can take one of the redundant routers out of service, upgrade it and then bring it back into service without any significant traffic loss (this should work for the core routers, for the edge devices usually the redundant path may not be available)
 - b. Set IGP metric to the highest possible value so the IGP will try to route the traffic through the alternate path. For OSPF use "max-metric" command.

router(config-ospf)#max-metric router-lsa

For ISIS use "spf-overload-bit" command.

router(config-isis)#set-overload-bit

- c. After all the software is upgraded restore the IGP metric by removing the commands:

OSPF

router(config-ospf)#no max-metric router-lsa

ISIS

```
router(config-isis)#no set-overload-bit
```

3) Copy the running-configuration and admin-configuration to a temporary storage location. This could be on a remote TFTP server or a device such as the harddisk: or disk0: present on the RP.

```
router#copy running-config tftp://...running_config.txt
```

```
router#admin
```

```
router(admin)#copy running-config tftp://...admin-running_config.txt
```

```
router(admin)#exit
```

4) Verify Mgmt access to the router (see caveats section)

5. Upgrade:

All install operations should be done admin mode

- 1) Add the required pies to disk:

```
router(admin)# install add <source>/<path>/<pie> sync
```

Note1: The <source> can be one of disk0:, disk1:, compactflash;, tftp;, ftp: or rcp:.

Note2: The above step must be repeated for each pie file, or all of the pies can be added together in a single 'install add ..' command. To add all pies using a single command, list all of the pies (including their source) within the 'install add ..' command in the following manner:

```
router(admin)# install add <source>/c12k-mini.pie-3.8.2 <source>/c12k-mcast.pie-3.8.2 <source>/c12k-mgbl.pie-3.8.2 <source>/c12k-mpls.pie-3.8.2 <source>/c12k-k9sec.pie-3.8.2 sync>/c12k-diags.pie-3.8.2 sync
```

Note3: The use of 'sync' option will prevent the user from executing any other command during the install operation.

Note4: Since 3.5.0 release <source> can be specified just once rather than for each package. This simplifies the command:

```
router(admin)# install add <source> comp-hfr-mini.pie-3.8.2 hfr-mcast-p.pie-3.8.2 hfr-mgbl-p.pie-3.8.2 hfr-mpls-p.pie-3.8.2 hfr-k9sec-p.pie-3.8.2 hfr-diags-p.pie-3.8.2 sync
```

Note5: Under idle conditions, this command may take at least 35 minutes to complete, during which the router will be fully functional.

Note6: In case there are any other optional packages installed prior to upgrade the current upgrade has to be done with them, so corresponding pie files have to be added and installed as well. Otherwise all optional packages have to be deactivated (following by the commit) before the upgrade. Side effect of this is loss of the configuration supported by the pie.

- 2) Test the activation using the 'test' option. Testing the activation will give you a preview of the activation.

```
router(admin)# install activate disk0:c12k-mini-3.8.2 disk0:c12k-mcast-3.8.2 disk0:c12k-mgbl-3.8.2 disk0:c12k-k9sec-3.8.2 disk0:c12k-mpls-3.8.2 disk0:c12k-diags-3.8.2 sync test
```

Note1: No actual changes will be made when 'test' option is used.

Note2: Any config that is incompatible with the new version being activated will be identified. The 'show configuration removed' command can be used to view what will be removed as result of the software upgrade (see caveats section for details).

Note3: Such removed config can be reapplied using the 'load config removed <config>.cfg' command from config mode AFTER the upgrade has been completed (see caveats section for details).

- 3) Activate all of the packages added in step 1:

```
router(admin)# install activate disk0:c12k-mini-3.8.2 disk0:c12k-mcast-3.8.2 disk0:c12k-mgbl-3.8.2 disk0:c12k-k9sec-3.8.2 disk0:c12k-mpls-3.8.2 disk0:c12k-diags-3.8.2 sync
```

Note1: The output of 'install add' command executed in step 1 provides the list of names of packages to be used in 'install activate ..' command.

Note2: The use of 'sync' option will prevent the user from executing any other command during the install operation.

Note3: The router will reload at the end of activation to start using the new packages.

Note4: Under idle conditions, this operation may take at least 20 minutes to complete.

Note5. From release 3.6.0 a wild card option is available during packages activation:

```
router(admin)# install activate *3.6.0*
```

- 4) Since it takes around 10 min to install add, the following command can be used to check.

```
Router(admin)# sh install request
```

- 5) Verify system stability through commands described under **Check System Stability** section. If system issues are detected or if the upgrade needs to be backed out for any reason, please follow the steps described in **Downgrade** section to rollback the software configuration to the starting point.

- 6) Check to see if there were any failed startup config. If there were any startup config that failed to be applied, then refer to the **Caveats** section to see how it should be handled.

```
router# show config failed startup
```

- 7)Commit the newly activated software:

```
router(admin)# install commit
```

- 8) Verify/fix configuration file system

```
router(admin)# cfs check
```

NOTE 1: From release 3.6.0 an alternate way of adding and installing pies is available. If the pie files are compressed using tar format they can be loaded on the router using the following command:

```
router(admin)# install add tar <source>/<path>/<tar_file> sync
```

From release 3.7.0 pies can subsequently be activated using single command based on the install operation id generated after each install command:

```
router(admin)# install activate id <install_operation_id> sync
```

Install operation id is printed after finishing each install command or can be obtained using "show install log" command.

NOTE2: In some very rare cases inconsistencies in the content of the internal configuration files can appear. In such situations, to avoid configuration loss during upgrade, following steps can be optionally done before activating packages: Its advisable to follow this procedure before upgrade.

a. *Clear NVGEN cache:*

```
router# run nvgen -F 1
```

b. *Create dummy config commit:*

```
router# config  
router(config)# hostname <hostname>  
router(config)# commit  
router(config)# end
```

c. *Force commit update by using the reload command. **Press "n" when the confirmation prompt appears:***

```
router# reload  
Updating Commit Database. Please wait...[OK]  
Proceed with reload? [confirm] <- Press "n"
```

In same cases the following may happen:

```
router#reload  
Preparing system for backup. This may take a few minutes .....System  
configuration backup in progress [Retry later]
```

In such a case please re-try the command after some time.

6. Downgrade:

- 1) List the available rollback points:

```
router(admin)# show install rollback ?
```

- 2) Identify the rollback point by executing the following show command and analyzing the software configuration at the rollback point:

```
router(admin)# show install rollback <rollback point>
```

Note1: A valid rollback point number must be specified. The output will show list of active packages for that rollback point.

- 3) Test the rollback operation using the 'test' option. Testing the rollback operation can give you a preview of the rollback.

```
router(admin)# install rollback to <rollback point> sync test
```

Note1: The output will detect if any incompatible config exist. In such cases, 'show configuration removed' command can be used to view what will be removed as result of the software downgrade.

Note2: Removed command can be reapplied at a later time using the 'load config removed <config>.cfg' command from config mode..

The following is a sample output:

```
Warning: SDR Owner: No incompatible configuration will be removed due to the  
Warning: 'test' option
```

```
Info: SDR Owner: Detected incompatibility between the activated software  
Info: and router running configuration.  
Info: SDR Owner: Removing the incompatible configuration from the running  
Info: configuration.  
Info: SDR Owner: Saving removed configuration in file '20060316131636.cfg'  
Info: on node 'RP/0/0/CPU0:'  
Info: Use the "show configuration removed 20060316131636.cfg" command to  
Info: view the removed config.  
Info: NOTE: You must address the incompatibility issues with the  
Info: removed configuration above and re-apply it to the running  
Info: configuration as required. To address these issues use the  
Info: "load configuration removed 20060316131636.cfg" and "commit"  
Info: commands.
```

Use the command suggested in the above example to display the config that will potentially be removed after the downgrade.

- 4) Perform the rollback operation executing commands:

```
router(admin)# install rollback to <rollback point> sync
```

Note1: Based on the set of packages being activated and deactivated as part of the rollback operation, one or more nodes may be reloaded. Please be patient as this operation could take some time.

Note2: If you previously executed 'install remove' command to permanently remove any packages in the rollback configuration then the rollback operation will not proceed. To resolve this issue, please run the following command to re-add the relevant packages to disk :

```
router(admin)# install add <device or tftp>/<path>/<pie> sync
```

Note3: The use of 'sync' option will prevent the user from executing any other command during the install operation.

- 5) Restore the original configuration that was backed up in **Special Upgrade Instructions** section.

```
router#config
router(config)#load <source/filename>
router(config)#commit replace
router(config)#show configuration failed
Verify any rejected configuration
router(config)#exit
Restore the admin-running-configuration as follows
router#admin
router(admin)#config
router(admin-config)#load <source/filename>
router(admin-config)#commit replace
router(admin-config)#show configuration failed
Verify any rejected configuration
router(admin-config)#exit
router(admin)#exit
```

- 6) Install commit the newly activated software.

```
router(admin)# install commit
```

- 7) Verify system stability through commands described in **Check System Stability** Section.

7. Post-Upgrade / Post-Downgrade Procedure:

- 1) Disk cleanup (optional)

Once software upgrade or downgrade 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):

- Obtain the list of inactive packages and note the names of packages that are not needed:

```
router(admin)# show install inactive brief
```

- Remove the unnecessary inactive packages:

```
router(admin)# install remove disk0:<package_name1>  
disk0:<package_name2> .. disk0:<pkg_nameN> sync
```

or

```
router(admin)# install remove inactive (to remove all inactive packages)
```

Note1: The use of 'sync' option will prevent the user from executing any other command during the install operation.

- 2) Verify/fix configuration file system (mandatory)

```
router(admin)# cfs check
```

If "max-metric" or "set overload bit" is set during pre-upgrade task restore the metric using commands specified in section 4.

- 3) Upgrade firmware (mandatory)

Both ROMMON and FPGA firmware needs to be upgraded after the 3.8.0 image installation on the system. For detailed upgrade procedure please refer "IOS XR Firmware Upgrade Guide" document which can be accessed at:

http://www.cisco.com/web/Cisco_IOS_XR_Software/index.html

8. Caveats:

1. During software upgrade or downgrade, the system could detect incompatible configuration and remove it from the running configuration. The removed config will be saved to a file on the router. Some configuration could also fail due to syntax or semantic error as the router boots the new version of the software.

The operator must browse the removed or failed configuration and then address the changes so that the config can be properly applied on the new version of software:

- Addressing incompatible and removed configuration:

During the test activation of a new software version, incompatible configuration will be identified and removed from the router running configuration. Syslog and console logs will provide the necessary information on the name of the removed configuration file. To address the incompatible configuration, users should browse the removed configuration file, address the syntax and semantics errors and re-apply the config as required and/or applicable after upgrade.

To display the removed configuration, execute the following command from exec mode:

```
router# show configuration removed <removed config filename>
```

- Addressing failed admin and non-admin configuration during reload:

Some configuration may fail to take effect when the router boots with the new software. These configurations will be saved as failed configuration. During activation of the new software version, operator would be notified via syslog and console log where configuration failed to take effect. To address the failed configuration, user should browse both the admin and non-admin failed configuration, address syntax and semantics errors and re-apply it as required.

To display the failed configuration, execute the following command:

```
router# show configuration failed startup
```

```
router(admin)# show configuration failed startup
```

2. MDR – Minimum

This feature is not supported for upgrades to 3.8.2 release

3. Limitations with preconfig interface

- Customer should check whether persistent and running config is same or different. If it is different then it will have problem after reload/upgrade, because reload/upgrade will use persistent config to restore configuration.

show cfgmgr persistent-config – shows the persistent config in CLI form

show running-config – shows running config

- Customer should not use "no interface preconfig <>" if they find the same config exist in both preconfig and activate. "cfs check" command can be used to resolve the inconsistency.

4. QoS WRED configuration incompatibility

After 3.6 release QoS WRED statements are 'collapsed' in that if different random-detect statements using the same match types (EXP, DSCP, Prec etc) are entered with identical min and max threshold values, a single configuration line will be shown in the output of 'show running'. During rollback to the pre 3.6 release QOS policy will be rejected and will need to be manually entered again.

5. CSCsj77582 report nvram file corrupted for files lost during downgrade
 - Downgrade from anything above 3.6 (including 3.6) to anything below 3.6 (excluding 3.6) will hit nvram[67]: %MEDIA-NVRAM-4-BADFILES : NVRAM File Corrupted (sam_db). This is already in the 3.6 manuals.
6. CSCsy47855 show install inactive does not return anything
 - If present image is 3.5.3 this issue could be encountered.