CRS-1/CRS-3 Upgrade Procedure

4.1.x - 4.3.x to 5.1.2

This document describes procedure for upgrading CRS system from IOS-XR 4.X image to IOS-XR 5.1.2.

For Upgrade from 3.X to 5.1.2, please refer Section-9

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	Package Name
Composite Mini Package (OS-MBI, Base, Admin, Fwdg, Rout)	hfr-mini-px.pie-5.1.2	disk0:hfr-mini-px-5.1.2
Multicast Package	hfr-mcast-px.pie-5.1.2	disk0:hfr-mcast-px-5.1.2
Manageability Package	hfr-mgbl-px.pie-5.1.2	disk0:hfr-mgbl-px-5.1.2
MPLS Package	hfr-mpls-px.pie-5.1.2	disk0:hfr-mpls-px-5.1.2
Security Package	hfr-k9sec-px.pie-5.1.2	disk0:hfr-k9sec-px-5.1.2
Diagnostic package	hfr-diags-px.pie-5.1.2	disk0:hfr-diags-px-5.1.2
Documentation package	hfr-doc-px.pie-5.1.2	disk0:hfr-doc-px-5.1.2
Field Programmable Device package	hfr-fpd-px.pie-5.1.2	disk0:hfr-fpd-px-5.1.2
Services Pie	hfr-services-px.pie-5.1.2	disk0:hfr-services-px-5.1.2
Video Pie	hfr-video-px.pie-5.1.2	disk0:hfr-video-px-5.1.2
CRS asr9000v Pie	hfr-asr9000v-nV-px.pie-5.1.2	disk0:hfr-asr9000v-nV-px-5.1.2
Lawful Intercept Pie	hfr-li-px.pie-5.1.2	hfr-li-px.pie-5.1.2

Note 1: 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 Fix-SMUs:

There are no mandatory SMUs required at this point to upgrade from 4.1.x to 5.1.2.

Check System Stability:

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

System:
(admin) show platform
show redundancy
show ipv4 interface brief <or> show ipv6 interface brief <or> show interface summary
show install active
cfs check
clear configuration inconsistency
show process cpu location <all slots>
top location <all slots>
show memory summary location all
dir <install disk>
Fabric Health (admin mode)
show controllers fabric plane all
show controllers fabric connectivity all detail
show controllers fabric plane all statistics
show controllers fabric bundle all detail
show controllers fabric link health
show controllers fabric rack all detail
CE Health (admin mode)
show controllers switch udld location <all RP's>
show controller switch inter-rack udld all loc <all SC's>
show controller switch stp location <all RP's/SC's>
show controller switch inter-rack stp location <all SC's>
show controller switch statistics location <all RP's>
show controllers switch inter-rack statistics all brief location <all SC's>

3. Perform Pre-Upgrade Tasks:

1. Standard 5.1.2 px image + packages pie needs about 1.2 G of disk space. Ensure that the install disks on RP's, Standby RP's and DRP's have memory available for installing the image. It is recommended that at least 30% of the disk should be free during normal operation.

   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 that 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 remove inactive
   ```

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

   ```
   install commit
   ```

   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 and SP's should also be checked. Extraneous files such as crashinfo files can be removed. To check the free, stale and available space of the bootflash, use the following admin mode command:

   ```
   router(admin)#sh filesystem bootflash: all location 0/1/SP

   router(admin)#sh filesystem bootflash: all location 0/SM1/SP
   ```

   Even though stale space is counted towards available space, it cannot be used for any install operation till it is reclaimed. To reclaim stale space, use the following admin mode command. Once issued, wait for the reclaim operation to complete. Wait at least 10 minutes after the command reports finished before proceeding further with the install process. Please refer to CSCud11071 for more details.

   ```
   router(admin)#bootflash reclaim
   ```

2. Check if all the cards in the system are all up using the admin command

   ```
   show platform
   ```

If any of the card is not boot properly it has to replaced or be shut down using the admin-configuration command

hw-module power disable location <loc>

Verify NVRAM. See Section 4: caveats of this document for more.

3. 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**

Note1: Prior to release 3.8 the above commands have to be run before the 'install activate' command is executed, resulting in a long period of time when the router is taken out of forwarding path. To minimize this behavior starting from release 3.8, an enhancement has been provided which allows the user to 'pause' the install activate command just prior router reloading and to execute configuration changes such as IGP commands listed above. Following command enables this install option

install activate disk0:*5.1.2* pause sw-change

The user will be prompted prior to the system reload, at which point the IGP cost-out operation can be executed

4. 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://a.b.c.d/path/directory/running_config.txt

router#admin

router(admin)#copy running-config tftp://a.b.c.d/path/directory/admin-running_config.txt

router(admin)#exit

5. Verify Mgmt access to the router.
6. Since 4.0.x a new feature to upgrade fpd on all slots during image upgrade is supported. Use below command to enable this feature.

   RP/0/RP0/CPU0:router(admin-config)#fpd auto-upgrade

4. Upgrade:

All install operations should be done in 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:, harddisk:, 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>/hfr-mini-px.pie-5.1.2 <source>/hfr-mcast-px.pie-5.1.2 <source>/hfr-mgbl-px.pie-5.1.2 <source>/hfr-mpls-px.pie-5.1.2 <source>/hfr-k9sec-px.pie-5.1.2 <source>/hfr-diags-px.pie-5.1.2 sync***

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

Note4: If all packages are available in the same <source> then the <source> can be specified just once rather than for each package. This simplifies the command:

router(admin)# ***install add <source> hfr-mini-px.pie-5.1.2 hfr-mcast-px.pie-5.1.2 hfr-mgbl-px.pie-5.1.2 hfr-mpls-px.pie-5.1.2 hfr-k9sec-px.pie-5.1.2 hfr-diags-px.pie-5.1.2 sync***

Note5: Under idle conditions, this command may take at least 35 minutes to complete, during which the router will be fully functional. This operation will take longer to complete on a Multi-Chassis system.

Note6: If using optional packages such as the hfr-mgbl package on the system's current release, in order to successfully complete the upgrade to the new release, the optional package must also be added and activated. Alternatively the 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 package.

Note7: 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**

The router needs free memory of at least 2 times the tar file size + 300 MB in order to uncompress the tar file. Use "show memory summary" exec command to find available free memory.

2. Test the activation using the 'test' option. Testing the activation will give you a preview of the activation. This preview will list all the s/w changes on all RP's/SC's/LC's . Verify that the changes are correct. No Actual changes will be made when 'test' option is used.

   router(admin)# **install activate disk0:hfr-mini-px-5.1.2 disk0:hfr-mcast-px-5.1.2 disk0:hfr-mgbl-px-5.1.2 disk0:hfr-k9sec-px-5.1.2 disk0:hfr-mpls-px-5.1.2 disk0:hfr-diags-px-5.1.2 sync test**

3. Activate all of the packages added in step 1:

   router(admin)# **install activate disk0:hfr-mini-px-5.1.2 disk0:hfr-mcast-px-5.1.2 disk0:hfr-mgbl-px-5.1.2 disk0:hfr-k9sec-px-5.1.2 disk0:hfr-mpls-px-5.1.2 disk0:hfr-diags-px-5.1.2 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 onwards, the install commands 'install activate *5.1.2* pause sw-change sync' can be used to enable the user to cost the router out of the IGP path just before the router reloads, rather than at the point where the activation commences.*

4. 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.
5. 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**

6. Commit the newly activated software:

   router(admin)# **install commit**

5. 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 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: Rollback from 'px' image to 'p' image is not supported. Rollback from 'px' to 'px' is supported.

Note2: Rollback from FAT32 to FAT16 file system type is not supported.

Note3: 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.

Note4: Removed configuration 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 configuration 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, run the following command to re-add the relevant packages:

```
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.

Note4: If filesystem has changed

5. Restore the original configuration that was backed up in **Perform Pre-Upgrade Tasks** section.

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

6. Post-Upgrade / Post-Downgrade Procedure

1. Restore IGP metric if changed before the upgrade

   OSPF

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

   ISIS

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

2. 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):

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

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

   b. 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.

3. 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.

4. Upgrade firmware (mandatory)

   Both ROMMON and FPGA firmware needs to be upgraded after the 5.1.2 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

   Please refer software/firmware compatibility matrix for CRS at following location:

   http://www.cisco.com/web/Cisco_IOS_XR_Software/pdf/Software_Firmware_Compatibility_Matrix.pdf

7. 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**

   - Addressing configuration inconsistencies

     In same very rare cases inconsistencies in the content of the internal configuration files can occur. In order to avoid such situations, the following steps are recommended before activating packages:

     a. Clear NVGEN cache:
        router# **run nvgen –F 1** (needs cisco-support privileges)

     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 some cases the following error may be reported:
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.

2. MDR – Minimum Disruption Restart
This feature is not supported for upgrades to 5.1.2 release

3. Limitations with preconfig interface
- Operator 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
- Operator 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. NVRAM problems may cause MSC to not boot in upgrade to 3.7 and later releases.
When a customer is upgrading to 3.7 and later releases from an earlier release, defective NVRAM may cause MSC to fail to boot.
In prior releases, if NVRAM had an uncorrectable problem (i.e. a problem that reformatting NVRAM could not solve, such as a battery problem), the card would still finish initialization and function ... though NVRAM-dependent functions like PCDS storage, environmental data storage fail and syslog messages regarding that NVRAM are occasionally seen.
This notice is to make customers planning such an upgrade (to release 3.7 or later) aware of a change in tolerance for defective NVRAM introduced by CSCso39580 in 3.7.

Workaround :
A customer can prevent being caught by surprise by attempting "dir nvram: location all" prior to the upgrade. Marginal or failed NVRAM will error and not return proper results (all RPs and MSCs should give a directory listing of the NVRAM). These cards can be proactively examined, reformat attempted (if there is a format problem or corruption), and replaced (if necessary). For customers who encounter the problem during an upgrade, a rollback to the earlier release should allow the MSC to recover and function.

5. CSCui34790 – On performing upgrade from 4.x release to 5.1.2, all install related logs will be lost. Any rollback to previous rollback points using "admin install rollback to <>" will not be functional.

In order to retain rollback functionality, please work with Cisco TAC to install workaround fix in 4.x image before starting an upgrade.

8. Upgrading from IOS-XR 3.X Image to IOS-XR 5.1.2

Direct Upgrade from IOS-XR 3.X image to IOS-XR 5.1.2 is not supported.

If any CRS system needs to be upgraded from IOS-XR 3.X image to IOS-XR 5.1.2, following 2 options are available:

Method-I: 2-Step Upgrade

Step-1: Upgrade CRS system to latest 4.1.X / 4.2.X image by following Upgrade procedure available on http://www.cisco.com/web/Cisco_IOS_XR_Software/index.html

Step-2: Once upgraded to 4.X image, upgrade to IOS-XR 5.1.2

Method-II: Turboboot Upgrade

Before attempting turboboot, ROMMON on all nodes has to be upgraded to 2.09 version.

ROMMON can be manually upgraded using the following procedure. Refer to ROMMON upgrade Instructions section and use rommon-2.09.tar file available on CCO.

http://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/migration/guide/ugbook/tbupgapp.html#wp1001606

CRS system can be turbobooted with IOS-XR 5.1.2 image using following procedure:

http://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/migration/guide/prpmigration.html

Refer to Method-2 in the above document.