CRS-1 Upgrade Procedure:
3.2.x to 3.3.4

Obtain Required PIE files:

The following package files are required to perform the upgrade:

PIE File Description	Sample PIE Filename	Sample Package Name
Composite Mini Package (OS-MBI, Base, Admin, Fwdg, lc Rout)	comp-hfr-mini.pie-3.3.4	disk0:comp-hfr-mini-3.3.4
Multicast Package	hfr-mcast-p.pie-3.3.4	disk0:hfr-mcast-3.3.4
Manageability Package	hfr-mgbl-p.pie-3.3.4	disk0:hfr-mgbl-3.3.4
MPLS Package	hfr-mpls-p.pie-3.3.4	disk0:hfr-mpls-3.3.4
Security Package	hfr-k9sec-p.pie-3.3.4	disk0:hfr-k9sec-3.3.4
Diagnostic package	hfr-diag-p.pie-3.3.4	disk0:hfr-diag-3.3.4

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.

Install Mandatory SMUs:

Install the following SMUs prior to performing the upgrade. These SMUs are available at the following URL (special access privileges are needed to use this link):

http://www.cisco.com/cgi-bin/tablebuild.pl/iosxr-smu?sort=release

For all 3.2.0 version only:

SMU Filename	hfr-base-3.2.0.CSCei45039.pie
DDTS	CSCei45039
SMU Package Name	<boot device>hfr-base-3.2.0.CSCei45039-1.0.0
Problem Summary	Config loss when upgrading from 3.2.0 release
SMU Install Impact	Low. There should be no impact to running system.
SMU Install Procedure	1. Add SMU: router(admin)#**install add <path> /hfr-base-3.2.0.CSCei45039.pie to disk0:** 2. Activate SMU: router(admin)#**install activate disk0:hfr-base-3.2.0.CSCei45039-1.0.0** 3. Trigger the SMU by committing config: router#**config** router(config)#**hostname <same-hostname>** router(config)#**commit** router(config)#**exit** 4. Commit SMU: router(admin)#**install commit**

For all 3.2.x versions (3.2.0, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.50):

SMU Filename	hfr-base-3.2.x.CSCsd24398.pie
DDTS	CSCsd24398
SMU Package	<boot device>hfr-base-3.2.x.CSCsd24398-1.0.0 (where 3.2.x is the release

Name	number)
Problem Summary	3.2.x to 3.3.x upgrade - MSC bootflash cleanup
SMU Install Impact	There will be no impact to router operation. Install error messages will be reported from the Standby RP while activating this SMU. These error message can be safely ignored: [..] RP/0/RP0/CPU0:Mar 22 18:06:07 : instdir[195]: %INSTALL-INSTMGR-2-NODE_FAILED_TO_RESPOND_POST_PONR : Failed to receive a response to install end get reply message from node '0/RP1/CPU0' [..] Install 42: [100%] 'Install Manager' detected the 'warning' condition 'An error was reported on at least one of the nodes participating in the install operation. Either the node(s) failed to respond to the message, or the node(s) responded with an error.' [..]
SMU Install Procedure	1. Add SMU: router(admin)#**install add <path> /hfr-base-3.2.x.CSCsd24398.pie to disk0:** 2. Activate SMU: router(admin)#**install activate disk0:hfr-base-3.2.x.CSCsd24398-1.0.0** 3. Commit SMU: router(admin)#**install commit**

SMU Filename	hfr-base-3.2.x.CSCsd68855.pie
DDTS	CSCsd68855
SMU Package Name	<boot device>hfr-base-3.2.x. CSCsd68855-1.0.0
Problem Summary	Config lost on upgrade caused by broken banner config in alternate config
SMU Install Impact	Low. There should be no impact to running system.
SMU Install Procedure	1. Add SMU: router(admin)#**install add <path> /hfr-base-3.2.x.CSCsd68855.pie to disk0:** 2. Activate SMU: router(admin)#install **activate disk0:hfr-base-3.2.x.CSCsd68855-1.0.0** 3. Commit SMU: router(admin)#**install commit**

Check System Stability:

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

show platform	(verify that all nodes are in "IOS XR RUN" state)
show redundancy	(verify that a Standby RP is available and in "ready" state)
show ipv4 interface brief	
<or>	
show ipv6 interface brief	(verify that all interfaces are "UP")
show install active	(verify that the proper set of packages are active)

cfs check (in user and admin mode; verify and clear configuration inconsistency)

Perform Pre-Upgrade Tasks:

1) Check ROMMON version. Upgrade to the latest ROMMON version supported if necessary. Refer to the Release Notes for the latest version supported and for the ROMMON upgrade procedure.
   router(admin)#**show diag**
2) Save a backup copy of the router configuration:
   router# **cfs check**
   router# **copy running-config <filename>**
3) Check for the boot device. If the boot device is not disk0:, then config loss is expected after upgrading to 3.3. Please refer to the item #2 in the **Caveats** section below for additional details.
   The output of 'show install active' command will display the package in the format of <boot device><package name>. In the following example, the boot device is "disk0:":
   disk0:hfr-mcast-3.2.1

Upgrade:

Special Upgrade Instructions:

Upgrading from **all 3.2.x** releases:

Execute the following steps prior to upgrading to 3.3.4. Failure to follow these steps can result in config loss after the upgrade:

1. Verify that the mandatory SMU (hfr-base-3.2.x. CSCsd68855-1.0.0) is active. If this SMU is not active, then refer to the **Install Mandatory SMUs** section above on how to activate this mandatory SMU.
   router# **show install active**
2. Clear NVGEN cache:
   router# **run nvgen –F 1**
3. Create dummy config commit:
   router# **config**
   router(config)#**hostname <hostname>**
   router(config)#**commit**
   router(config)#**end**
4. 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"**

1) Add the required pies to disk:
   router(admin)#**install add <source>/<path>/<pie> to <target> 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>/comp-hfr-mini.pie-3.3.4 <source>/hfr-mcast-p.pie-3.3.4 <source>/hfr-mgbl-p.pie-3.3.4 <source>/hfr-mpls-p.pie-3.3.4 <source>/hfr-k9sec-p.pie-3.3.4 <source>/hfr-diag-p.pie-3.3.4 to disk0: sync***

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

*Note4: There may be warning messages from wdsysmon indicating excessive CPU usage on SP nodes. Please refer to item #3 in the **Caveats** section for more details.*
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.

2) Test the activation using the 'test' option. Testing the activation will give you a preview of the activation.
   router(admin)#**install activate disk0:comp-hfr-mini-3.3.4 disk0:hfr-mcast-3.3.4 disk0:hfr-mgbl-3.3.4 disk0:hfr-k9sec-3.3.4 disk0:hfr-mpls-3.3.4 disk0:hfr-diag-3.3.4 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.
   Note3: Such removed config can be reapplied using the 'load config removed <config>.cfg' command from config mode.

3) Activate all of the packages added in step 1:
   router(admin)#**install activate disk0:comp-hfr-mini-3.3.4 disk0:hfr-mcast-3.3.4 disk0:hfr-mgbl-3.3.4 disk0:hfr-k9sec-3.3.4 disk0:hfr-mpls-3.3.4 disk0:hfr-diag-3.3.4 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.

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 to the starting point.

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 item #1 in 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**

Downgrade:

Special Downgrade Instructions:

1. Downgrading to **3.2.**x images only:
   All 'banner' configurations must be removed prior to downgrading from 3.3.4. The removed 'banner' config can be reapplied once the downgrade is completed. Failure to do so can result in a large config loss.
   router(config)# **no banner < >**
   router(config)# **commit**
2 Save a backup copy of the router configuration. If there are Logical Routers configured, then login to each dLRSC node of each LR and execute the procedure to save LR specific configuration:
   router# **cfs check**
   router# **copy running-config <filename>**

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: The output will detect if any incompatible config and will be removed. 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.
   Note3: Please refer to item #1 in the ***Caveats*** *section for more details on how to handle incompatible config.*

4) Perform the rollback operation:
   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_file_name> 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 **Perform Pre-Upgrade Tasks** section.

6) Install commit the newly activated software.
   router(admin)# **install commit**

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

Post-Upgrade / Post-Downgrade Procedure:

Once software upgrade or downgrade has been completed, disk space can be recovered (optional) by removing any inactive packages that are no longer needed (if the packages are required at a later time, they can be re-added). Please follow these steps to remove inactive packages:

1) Obtain the list of inactive packages and note the names of packages that are not needed:
   router(admin)# **show install inactive brief**
2) Remove the unnecessary inactive packages:
   router(admin)# **install remove disk0:<package_name1> disk0:<package_name2> .. disk0:<pkg_nameN> sync**

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

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. If the boot device is not disk0:, then config loss is expected upon upgrade to 3.3 or downgrade from 3.3. This is due to fact that in R3.2.x, config is stored in disk0: by default. But in R3.3, config is stored on the boot device. Hence, when the boot device is not disk0: in pre-3.3 release, and when we do an upgrade to R3.3 or downgrade from R3.3 we expect to see config loss. Use the following commands to load any configuration that were backed up prior to upgrade or downgrade:

```
router# configure
router(config)# load <backup config>
router(config)# commit replace
router(config)# end
```

3. During the upgrade from 3.2.x to 3.3.x, wdsysmon cpu hog warning messages could be seen on SP nodes. These indicate that there is a temporary cpu hog on the node. There is no side-effect on the install upgrade operation and it will complete successfully (CSCsd94329, CSCei24761).

```
Install 8: [  1%] Going ahead to install the package...SP/0/FC1/SP:Mar 28
20:58:45.983 : wdsysmon[125]: %HA-HA_WD-6-CPU_HOG_1 : CPU hog: cpu 0's
sched count is 0.
SP/0/FC1/SP:Mar 28 20:58:45.990 : wdsysmon[125]: %HA-HA_WD-6-CPU_HOG_2
: CPU hog: cpu 0's ticker last ran 3.749 seconds ago.
SP/0/13/SP:Mar 28 20:58:45.804 : wdsysmon[125]: %HA-HA_WD-6-CPU_HOG_1 :
CPU hog: cpu 0's sched count is 0.
SP/0/FC0/SP:Mar 28 20:58:46.354 : wdsysmon[125]: %HA-HA_WD-6-CPU_HOG_1
: CPU hog: cpu 0's sched count is 0.
SP/0/1/SP:Mar 28 20:58:45.156 : wdsysmon[125]: %HA-HA_WD-6-CPU_HOG_1 :
CPU hog: cpu 0's sched count is 0.
```