CRS-1 Upgrade Procedure:

3.3.x/3.4.x/3.5.0/3.5.1 to 3.5.2

1. Obtain Required PIE files

The following package files are required to perform the upgrade:

PIE File Description	Sample PIE Filename	Package Name
Composite Mini Package (OS-MBI, Base, Admin, Fwdg, lc Rout)	comp-hfr-mini.pie-3.5.2	disk0:comp-hfr-mini-3.5.2
Multicast Package	hfr-mcast-p.pie-3.5.2	disk0:hfr-mcast-3.5.2
Manageability Package	hfr-mgbl-p.pie-3.5.2	disk0:hfr-mgbl-3.5.2
MPLS Package	hfr-mpls-p.pie-3.5.2	disk0:hfr-mpls-3.5.2
Security Package Diagnostic package	hfr-k9sec-p.pie-3.5.2 hfr-diags-p.pie-3.5.2	disk0:hfr-k9sec-3.5.2 disk0:hfr-diags-3.5.2

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.

Note2: The following packages has been removed from the mini.pie. They can be installed the same way as the rest of the pies if necessary.

hfr-doc.pie-3.5.2 - documentation package including man pages

hfr-fpd.pie-3.5.2 - Field Programmable Device package necessary for field firmware upgrades

2. 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

SMU Filename	hfr-base-3.3.x.CSCsg40006.pie
DDTS	CSCsg40006
Affected images	This SMU is necessary for 3.3.0 and 3.3.1 releases only
SMU Package Name	<boot device> hfr-base-3.3.x.CSCsg40006-1.0.0
Problem Summary	*Config loss when upgrading from 3.3.x release*
SMU Install Impact	Low. There should be no impact to running system.
SMU Install Procedure	Add SMU:

	router(admin)#**install add <path>/hfr-base-3.3.x.CSCsg40006.pie sync** Activate SMU: router(admin)#**install activate disk0:hfr-base-3.3.x.CSCsg40006-1.0.0 sync** Commit SMU: router(admin)#**install commit**

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 necessary 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) 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 | i ROMMON**

Note1: If rommon upgrade is needed one can load the new rommon image without reloading the router and proceed with the upgrade procedure. This can save one router reload downtime.

2) To minimize traffic loss during the upgrade please follow the procedure:

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 8.1)

5. Upgrade:

Special Upgrade Instructions:

Execute the following steps prior to upgrading to 3.5.2. Failure to follow these steps can result in config loss after the upgrade due to:

CSCek61038 - config loss during 3.3.x to 3.5.2 upgrade due to file truncation.

CSCek61243 - rip proto config not properly nvgened, resulting config loss on upg

1. Clear NVGEN cache:
   router# **run nvgen –F 1**
2. Create dummy config commit:
   router# **config**
   router(config)#**hostname <hostname>**
   router(config)#**commit**
   router(config)#**end**
3. 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.

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:, 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>/comp-hfr-mini.pie-3.5.2 <source>/hfr-mcast-p.pie-3.5.2 <source>/hfr-mgbl-p.pie-3.5.2***

<source>/hfr-mpls-p.pie-3.5.2 <source>/hfr-k9sec-p.pie-3.5.2 sync/hfr-diags-p.pie-3.5.2 sync

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

Note4: 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.

Note5: 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:comp-hfr-mini-3.5.2 disk0:hfr-mcast-3.5.2 disk0:hfr-mgbl-3.5.2 disk0:hfr-k9sec-3.5.2 disk0:hfr-mpls-3.5.2 disk0:hfr-diags-3.5.2 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 section 8.1 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 section 8.1 for details).

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

router(admin)# **install activate disk0:comp-hfr-mini-3.5.2 disk0:hfr-mcast-3.5.2 disk0:hfr-mgbl-3.5.2 disk0:hfr-k9sec-3.5.2 disk0:hfr-mpls-3.5.2 disk0:hfr-diags-3.5.2 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.

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 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**

6. Downgrade:

Important Note: Assume that someone has already upgraded to 3.5.x / 3.6.x (without installing "Rollback SMU fix"). But now plans to rollback to 3.3.x/3.4.x.

1. Install "Rollback SMU fix" for the older image i.e. 3.3.x / 3.4.x. DO NOT ACTIVATE THE SMU.

(admin)# **install add <Rollback SMU fix for 3.3.x/3.4.x> sync noprompt**
(admin)# **install commit**

2. Specify the actual install activate command to be used instead of the normal rollback command that would pick and activate the the "Rollback SMU fix".

(admin)# **install activate <3.3.x/3.4.x pie's> <3.3.x/3.4.x SMU's> <3.3.x/3.4.x Rollback SMU fix> sync**
(admin)# **install commit**

SMU Filename	hfr-os-mbi-3.3.x.CSCsk54170.pie hfr-os-mbi-3.4.X.CSCsk54170.pie
DDTS	CSCsk54170
Affected images	This SMU is necessary for 3.3.4/3.3.5/3.4.1/3.4.2 releases only
SMU Package Name	<boot device> hfr-base-3.3.x.CSCsk54170-1.0.0 <boot device> hfr-base-3.4.x.CSCsk54170-1.0.0

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 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:

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.

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
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
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:

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**

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

router(admin)#**cfs check**

4) If "max-metric" or "set overload bit" is set during pre-upgrade task restore the metric using commands specified in section 4.2.d.

8. Caveats:

1. Starting 3.5.0 a new feature is introduced which allows mgmt traffic only on the interfaces which are configured for management plane. By default only control ethernet and console ports are enabled to allow management traffic so in order to use other interfaces they have to be explicitly configured after the 3.5 image is loaded. Following example shows how to enable ssh protocol on POS interface:

```
control-plane
 management-plane
  inband
   interface POS0/3/0/0
    allow SSH
```

Management Plane Protection (MPP) protects management server applications (Telnet, SSH etc) from being attacked. By default access by telnet/ssh to the box is enabled only on the Management Ethernet interfaces, and explicit MPP configuration is needed to enable telnet, ssh, snmp access on any other interface. This implies that any customer upgrading from a pre-3.5.2 release without access to console/aux and does not use Management ethernet interfaces would not be able to access the box (via telnet/ssh)

For customers that do not use Management Ethernet interfaces and with no access to console/aux should install the following MPP "bridge SMU" along with the upgrade. This effectively disables MPP. To use the MPP feature, **configure MPP on the interfaces that need to allow access, and then deactivate/un-install this bridge SMU**.

SMU Filename	hfr-base-3.5.2.CSCsl64079
DDTS	CSCsl64079
Affected images	This SMU is necessary for 3.5.2 only
SMU Package Name	<boot device> hfr-base-3.5.2.CSCsl64079-1.0.0

2. 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**

3. Changes have been made to the format of the file system used to store router configuration files. These result in the following behavior when upgrading from software releases 3.3.1 and earlier:

- On the first upgrade from 3.3.1 (or earlier) to 3.5.2, the 3.5.2 software will create new-format configuration files based on the contents of the old-format files left behind by the 3.3.1 (or earlier) software. Included in the files created in this way are those that contain the persistent copy of the router configuration, which will be used to restore the running configuration. The history of changes to the running configuration, however, is not re-created. This means that after the upgrade, it will not be possible to view or rollback any changes previously contained in the configuration history.

- If the router is subsequently downgraded back to 3.3.1 (or earlier), the default behavior is to restore the router running configuration using the old-format configuration files left behind from the last time 3.3.1 (or earlier) was running. This means that any changes to the running configuration made while 3.5.2 was running will be lost. To prevent this from happening, the following command should be run before performing the downgrade operation:

delete disk0:/config/running/commitdb/*

("disk0:" should be substituted with the appropriate device name if an alternate boot device is being used.)

This will force the 3.3.1 (or earlier) software to create old-format configuration files based on the contents of the new-format files left behind by the 3.5.2 software. Included in the files created in this way are those that contain the persistent copy of the router configuration, which will be used to restore the running configuration. The history of changes to the running configuration, however, is not re-created. This means that after the downgrade, it will not be possible to view or rollback any changes previously contained in the configuration history.

- If the router is then re-upgraded back to 3.5.2, the default behavior is to restore the router running configuration using the new-format configuration files left behind from the last time 3.5.2 was running. This means that any changes to the running configuration made while 3.3.1 (or earlier) was running will be lost. To prevent this from happening, the following command should be run before performing the re-upgrade operation:

delete disk0:/config/lr/running/commitdb/*

("disk0:" should be substituted with the appropriate device name if an alternate boot device is being used.)

This will force the 3.5.2 software to create new-format configuration files based on the contents of the old-format files left behind by the 3.3.1 (or earlier) software - just as was done during the first upgrade.

4. CSCsg47962 - Avoid a reload of nodes when the bootup admin config is being applied. During MC (Multi-chassis) upgrade with the non-DSC rack running as named-SDR on the RPs it

will not be upgraded properly to the new release and will fall back to 3.3.x. The workaround is to power off non-DSC rack before issuing “install activate” on the DSC and power it back on after the installation is complete on DSC. Fixed in release 3.4.1 and onwards.

5. MDR – Minimum Disruption Restart

This feature is not supported for upgrades to 3.5.2 release due to:
* boot flash limitation
* Kernel Changes

6. Limitation with preconfig interface

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

2. Customer should not use "no interface preconfig <>" if they find the same config exist in both preconfig and activate