

CRS-1 Upgrade Procedure:

3.3.x/3.4.x/3.5.0/3.5.1/3.5.2 to 3.5.3

1.	Obtain Required PIE files	2
2.	Install Mandatory SMUs.....	2
3.	Check System Stability:.....	3
4.	Perform Pre-Upgrade Tasks:.....	3
5.	Upgrade:.....	6
6.	Downgrade:.....	9
7.	Post-Upgrade / Post-Downgrade Procedure:	11
8.	Caveats:.....	12

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, Ic Rout)	comp-hfr-mini.pie-3.5.3	disk0:comp-hfr-mini-3.5.3
Multicast Package	hfr-mcast-p.pie-3.5.3	disk0:hfr-mcast-3.5.3
Manageability Package	hfr-mgbl-p.pie-3.5.3	disk0:hfr-mgbl-3.5.3
MPLS Package	hfr-mpls-p.pie-3.5.3	disk0:hfr-mpls-3.5.3
Security Package	hfr-k9sec-p.pie-3.5.3	disk0:hfr-k9sec-3.5.3
Diagnostic package	hfr-diags-p.pie-3.5.3	disk0:hfr-diags-3.5.3

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-3.5.3](#) - documentation package including man pages

[hfr-fpd.pie-3.5.3](#) - 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:

[http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=IOS%20XR%20Software%20Maintenance%20Upgrades%20\(SMU\)&mdfid=279017029&treeName=Routers&mdfLevel=null&url=null&modelName=Cisco%20IOS%20XR%20Software&isPlatform=N&treeMdfid=268437899](http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=IOS%20XR%20Software%20Maintenance%20Upgrades%20(SMU)&mdfid=279017029&treeName=Routers&mdfLevel=null&url=null&modelName=Cisco%20IOS%20XR%20Software&isPlatform=N&treeMdfid=268437899)

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	<i>Config loss when upgrading from 3.3.x release</i>
SMU Install Impact	Low. There should be no impact to running system.

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

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`

`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:

Important Note:

You will need to have minimum 428MB disk size free available before the start of upgrade.

Use "`dir disk0:`" command to check available/free disk space on their router. At the end of the command it will display free disk size.

Following is sample output for that command.

RP/0/RP0/CPU0:BB01#dir disk0:

Directory of disk0:

```

2      drwx 16384  Tue Oct 16 11:52:20 2007  LOST.DIR
18917  dr-x 16384   Tue Nov  6 20:47:29 2007  bcm-cur
10     drwx 16384   Tue Nov  6 21:54:35 2007  instdb

```

65760	-rwx	10397	Mon Nov 5 16:47:59 2007	sam_certdb
65824	-rwx	126	Mon Nov 5 16:47:59 2007	sam_crldb
18922	dr-x	16384	Tue Nov 6 20:49:26 2007	aaa
214	drwx	16384	Tue Nov 6 11:04:51 2007	hfr-rout-3.5.2.00
261	drwx	16384	Tue Oct 16 20:49:17 2007	hfr-base-3.3.5.CSCsi59282-1.0.0
303	drwx	16384	Tue Oct 16 20:49:23 2007	hfr-fwdg-3.3.5.CSCsk31321-1.0.0
369	drwx	16384	Tue Oct 16 20:49:30 2007	hfr-mcast-3.3.5.CSCsk21588-1.0.0
454	drwx	16384	Tue Oct 16 20:49:38 2007	hfr-base-3.3.5.CSCsk28858-1.0.0
527	drwx	16384	Tue Oct 16 20:49:43 2007	hfr-fwdg-3.3.5.CSCsk24515-1.0.0
562	drwx	16384	Tue Oct 16 20:49:49 2007	hfr-fwdg-3.3.5.CSCsk21530-1.0.0
628	drwx	16384	Tue Oct 16 20:50:01 2007	hfr-base-3.3.5.CSCsg91089-1.0.0
775	drwx	16384	Tue Oct 16 20:50:16 2007	hfr-rout-3.3.5.CSCsj93281-1.0.0
935	drwx	16384	Tue Oct 16 20:50:21 2007	hfr-lc-3.3.5.CSCsj87811-1.0.0
980	drwx	16384	Tue Oct 16 20:50:30 2007	hfr-mpls-3.3.5.CSCsj91834-1.0.0
1080	drwx	16384	Tue Oct 16 20:50:45 2007	hfr-rout-3.3.5.CSCsj89020-1.0.0
1240	drwx	16384	Tue Oct 16 20:51:52 2007	hfr-diags-3.3.5
2247	drwx	16384	Tue Oct 16 20:52:24 2007	hfr-k9sec-3.3.5
2574	drwx	16384	Tue Oct 16 20:53:40 2007	hfr-mpls-3.3.5
3283	drwx	16384	Tue Oct 16 20:55:31 2007	hfr-mgbl-3.3.5
4540	drwx	16384	Tue Oct 16 20:56:51 2007	hfr-mcast-3.3.5
5310	drwx	16384	Tue Oct 16 20:58:29 2007	hfr-os-mpi-3.3.5
6772	drwx	16384	Tue Oct 16 21:08:35 2007	hfr-base-3.3.5
11661	drwx	16384	Tue Oct 16 21:11:55 2007	hfr-admin-3.3.5
13608	drwx	16384	Tue Oct 16 21:13:33 2007	hfr-fwdg-3.3.5
14391	drwx	16384	Tue Oct 16 21:18:00 2007	hfr-lc-3.3.5
17608	drwx	16384	Tue Oct 16 21:20:13 2007	hfr-rout-3.3
19062	drwx	16384	Fri Nov 2 21:02:33 2007	license
19065	drwx	16384	Fri Nov 2 07:28:14 2007	shutdown
19066	drwx	16384	Tue Nov 6 17:58:13 2007	config
68864	-rwx	782945	Tue Nov 6 21:31:27 2007	shelfmgr_shutdown
19155	drwx	16384	Tue Oct 16 23:07:49 2007	usr
19156	drwx	16384	Tue Oct 16 23:07:49 2007	var
19176	drwx	16384	Tue Oct 16 23:29:06 2007	snmp
19178	drwx	16384	Tue Oct 16 16:29:17 2007	syslog
69216	-rwx	65583	Tue Oct 16 20:05:17 2007	timeout_devc-vty.txt
19000	drwx	16384	Sun Nov 4 20:47:46 2007	sbcr_phat-sun2-aasrao
69408	-rwx	67068	Wed Oct 31 10:55:55 2007	timeout_statsd_manager.txt
11	drwx	16384	Tue Nov 6 11:06:44 2007	hfr-lc-3.5.2.00
21122	drwx	16384	Tue Nov 6 11:08:08 2007	hfr-fwdg-3.5.2.00
22808	drwx	16384	Tue Nov 6 11:10:17 2007	hfr-admin-3.5.2.00
23977	drwx	16384	Tue Nov 6 11:18:44 2007	hfr-base-3.5.2.00
26033	drwx	16384	Tue Nov 6 11:19:30 2007	hfr-os-mpi-3.5.2.00
32422	drwx	16384	Tue Nov 6 11:23:59 2007	hfr-doc-3.5.2.00
34083	drwx	16384	Tue Nov 6 11:25:55 2007	hfr-diags-3.5.2.00
34905	drwx	16384	Tue Nov 6 11:28:19 2007	hfr-fpd-3.5.2.00
36291	drwx	16384	Tue Nov 6 11:30:25 2007	hfr-mcast-3.5.2.00
38690	drwx	16384	Tue Nov 6 11:31:35 2007	hfr-k9sec-3.5.2.00
39637	drwx	16384	Tue Nov 6 11:34:30 2007	hfr-mgbl-3.5.2.00
18931	drwx	16384	Fri Nov 2 14:04:45 2007	sbcr_phat-sun2-assrao
19024	drwx	16384	Sun Nov 4 20:47:53 2007	sbcr_phat-sun2-2-aasr
70816	-rwx	62915	Fri Oct 26 17:42:39 2007	timeout_obflmgr.txt
70944	-rwx	62016	Mon Oct 29 17:15:20 2007	timeout_msdp.txt
71040	-rwx	88794	Tue Nov 6 23:03:32 2007	timeout_bgp.txt
71136	-rwx	64752	Wed Oct 31 10:36:12 2007	timeout_hsrp.txt
44531	drwx	16384	Wed Oct 17 11:24:13 2007	my_fm_scripts
71296	-rwx	79690	Thu Oct 18 14:17:51 2007	timeout_ospf.txt

```

71392  -rwx 17062224  Thu Oct 18 16:23:50 2007  showtechbundle.10182007
71488  -rwx 55309      Fri Nov 9 07:05:57 2007  timeout_exec.txt
40098  drwx 16384     Tue Nov 6 11:36:01 2007  hfr-mpls-3.5.2.00
46916  drwx 16384     Fri Nov 2 13:57:35 2007  v80800
41469  drwx 16384     Tue Nov 6 11:38:36 2007  hfr-sbc-3.5.2.00
72256  -rwx 49049     Fri Oct 26 17:48:12 2007  timeout_sysmgr.txt
72608  -rwx 58748     Fri Nov 2 02:45:53 2007  timeout_vlan_ma.txt
72736  -rwx 67267     Fri Nov 2 02:43:42 2007  timeout_bundlemgr_distrib.txt
72832  -rwx 62585     Wed Oct 31 10:51:47 2007  timeout_ipv4_ma.txt
72928  -rwx 60171     Wed Oct 31 11:11:07 2007  timeout_pfilter_ma.txt
73056  -rwx 56337     Wed Oct 31 13:48:27 2007  timeout_show_config_changes.txt
73152  -rwx 12288     Fri Nov 2 13:57:35 2007  sl_timeout.tcl.swp

```

1004994560 bytes total (254869504 bytes free)
RP/0/RP0/CPU0:BB01#

- 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
```

5. Upgrade:

Special Upgrade Instructions:

Execute the following steps prior to upgrading to 3.5.3. Failure to follow these steps can result in config loss after the upgrade due to:

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

(NOTE - if you're not going to activate the DOC package until AFTER the .pie upgrade, you should deactivate the DOC package from rls 3.4.1 BEFORE performing the 'install activate 3.5.3 package set' to avoid warning messages. In admin mode 'install deactivate disk0:hfr-doc-3.4.1)

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-3.5.3  
<source>/hfr-mcast-p.pie-3.5.3 <source>/hfr-mgbl-p.pie-3.5.3  
<source>/hfr-mpls-p.pie-3.5.3 <source>/hfr-k9sec-p.pie-3.5.3 sync/hfr-  
diags-p.pie-3.5.3 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) (NOTE - if you have the SMU for CSCsi86270 (comp-hfr-3.4.1.CSCsi86270) installed, when performing the 'install activate test' step or 'install activate', include the disk0:hfr-fpd-3.5.3 package. If the package is not included in the 'activate' step, the installation will fail with the following error:

```
Error: Cannot proceed with the activation because of the following  
Error: package incompatibilities:  
Error: hfr-fpd-3.4.1 needs hfr-os-mbi-3.4.1, or equivalent, to be  
Error: active on the same nodes.  
Error: hfr-fpd-3.4.1.CSCsi86270-1.0.0 needs  
Error: hfr-base-3.4.1.CSCsi86270-1.0.0, or equivalent, to be active on  
Error: the same nodes)
```

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-3.5.3 disk0:hfr-mcast-3.5.3 disk0:hfr-mgbl-3.5.3 disk0:hfr-k9sec-3.5.3 disk0:hfr-mpls-3.5.3 disk0:hfr-diags-3.5.3 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-3.5.3 disk0:hfr-mcast-3.5.3 disk0:hfr-mgbl-3.5.3 disk0:hfr-k9sec-3.5.3 disk0:hfr-mpls-3.5.3 disk0:hfr-diags-3.5.3 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 (without installing "Rollback SMU fix"). But now plans to rollback to 3.3.x/3.4.x. **This SMU is for Multi-Chassis customers only, Single-Chassis customers do not need this SMU.**

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 3.3.5/3.4.1/3.4.2 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-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:

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. 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. 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 3.5.3, the 3.5.3 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 3.5.3 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 3.5.3 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 3.5.3, the default behavior is to restore the router running configuration using the new-format configuration files left behind from the last time 3.5.3 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 3.5.3 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.

3. 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.

4. MDR – Minimum Disruption Restart

This feature is not supported for upgrades to 3.5.3 release due to:

- * boot flash limitation
- * Kernel Changes

5. 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