XR 12000 Upgrade Procedure:

3.4.x/3.5.x to 3.6.0

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:

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)	c12k-mini.pie-3.6.0	disk0:c12k-mini-3.6.0
Multicast Package	c12k-mcast.pie-3.6.0	disk0:c12k-mcast-3.6.0
Manageability Package	c12k-mgbl.pie-3.6.0	disk0:c12k-mgbl-3.6.0
MPLS Package	c12k-mpls.pie-3.6.0	disk0:c12k-mpls-3.6.0
Security Package Diagnostic package SBC	c12k-k9sec.pie-3.6.0 c12k-diags.pie-3.6.0 c12k-sbc.pie-3.6.0	disk0:c12k-k9sec-3.6.0 disk0:c12k-diags-3.6.0 disk0:c12k-sbc.pie-3.6.0

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: Additional packages. They can be installed the same way as the regular pies if necessary:

c12k-doc.pie-3.6.0 – documentation package including man pages

c12k-fpd.pie-3.6.0 – Field Programmable Device package necessary for field firmware upgrades

2. Install Mandatory SMUs

No mandatory SMUs are needed at this point to perform an upgrade from 3.4.x and 3.5.x release.

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. Use "dir disk0:" command to check the available disk space on the router.

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

Directory of disk0:

2 drwx 16384 Tue Oct 16 11:52:20 2007 LOST.DIR

…….

1004994560 bytes total (254869504 bytes free)

In order to calculate the estimated disk space needed for the new image one can do the following:

- check the actual pie size for each pie which will be installed on the system. This can be done using the following command which gives the size of the file after decompression:

  RP/0/RP0/CPU0:CRS-E(admin)#show install pie-info tftp://.../comp-hfr-mini.pie-3.4.2

  Wed Aug 22 14:35:39.634 PST PDT

  Contents of pie file '/tftp://…/comp-hfr-mini.pie-3.4.2':

  Expiry date : Nov 3, 2011 15:55:24 PDT

  *Uncompressed size : **170502781***

  comp-hfr-mini-3.4.2

  hfr-rout-3.4.2

  hfr-lc-3.4.2

  hfr-fwdg-3.4.2

hfr-admin-3.4.2

hfr-base-3.4.2

hfr-os-mbi-3.4.2

Note1: Above command is an example of the 3.4.2 file size. Images changes size every release.

- Usually the size of the image on the disc needs more space than the uncompressed file size. A rough estimate how much space is really needed can be derived using the formula:

  *Total value from pie-info * 1.23*

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 as 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.

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 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) 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.

Note2: See section 8 for rommon and fpd upgrade details

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**

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://…running_config.txt

   router#admin

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

   router(admin)#exit

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

5. Upgrade:

Special Upgrade Instructions:

Execute the following steps prior to upgrading to 3.6.0. 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.

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 are not going to activate the DOC package until AFTER the .pie upgrade, you should deactivate the DOC package from the current installation BEFORE performing the 'install activate 3.6.0 package set' to avoid warning messages. In admin mode 'install deactivate disk0:c12k-doc-3.x.x

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-3.6.0 <source>/c12k-mcast.pie-3.6.0 <source>/c12k-mgbl.pie-3.6.0 <source>/c12k-mpls.pie-3.6.0 <source>/c12k-k9sec.pie-3.6.0 sync>/c12k-diags.pie-3.6.0 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.

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:c12k-mini-3.6.0 disk0:c12k-mcast-3.6.0 disk0:c12k-mgbl-3.6.0 disk0:c12k-k9sec-3.6.0 disk0:c12k-mpls-3.6.0 disk0:c12k-diags-3.6.0 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-3.6.0 disk0:c12k-mcast-3.6.0 disk0:c12k-mgbl-3.6.0 disk0:c12k-k9sec-3.6.0 disk0:c12k-mpls-3.6.0 disk0:c12k-diags-3.6.0 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 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**

7) Verify/fix configuration file system

    router(admin)#**cfs check**

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:

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:

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:<package1> disk0:<package2> .. disk0:<packageN> sync**

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.

8. Rommon and fpd upgrade

The following links contains information for to perform rommon or fpd upgrade:

- ROMMON

http://www.cisco.com/en/US/customer/products/ps5845/products_configuration_guide_chapter09186a00807e0a2f.html

- FPD

http://www.cisco.com/en/US/products/ps5845/products_configuration_guide_chapter09186a0080848d9d.html

9. 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 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
```

If the router running pre-3.5.0 release is managed inbound and do not have MgmtEth ports configured or do not have Console access during upgrade process, following the upgrade it will not be accessible. Therefore MgmtEth or Console access has to be enabled before the upgrade.

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. MDR – Minimum

This feature is not supported for upgrades to 3.6.0 release

4. 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.

5. DSA key regenaration

Due to nvram changes in 3.6.x release upgrade from pre 3.6.x image preceded by the downgrade from the 3.6.x release results in deletion of the DSA keys without any warning message. Keys need to be regenerated manually after the upgrade by using the following command executed in EXEC mode:

crypto key generate dsa

The presence of generated keys can be confirmed using the command

show crypto key mypubkey <dsa | rsa>

This issue is not happening while upgrading/downgrading between 3.6.x and newer releases