XR 12000 Upgrade Procedure:

3.3.x/3.4.x/3.5.0/3.5.2 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	Sample Package Name
Composite Mini Package (OS-MBI, Base, Admin, Fwdg, lc Rout)	c12k-mini.pie-3.5.2	disk0:c12k-mini-3.5.2
Multicast Package	c12k-mcast.pie-3.5.2	disk0:c12k-mcast-3.5.2
Manageability Package	c12k-mgbl.pie-3.5.2	disk0:c12k-mgbl-3.5.2
MPLS Package	c12k-mpls.pie-3.5.2	disk0:c12k-mpls-3.5.2
Security Package Diagnostic package	c12k-k9sec.pie-3.5.2 c12k-diags.pie-3.5.2	disk0:c12k-k9sec-3.5.2 disk0:c12k-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 two packages has been removed from the mini.pie. They can be installed the same way as the regular pies if necessary:

c12k-doc.pie-3.5.2 – documentation package including man pages

c12k-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	C12k-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> c12k-base-3.3.x.CSCsg40006-1.0.0
Problem Summary	Config loss when upgrading from 3.3.1 release
SMU Install Impact	Low. There should be no impact to running system.
SMU Install Procedure	Add SMU: router(admin)#**install add <path>/c12k-base-3.3.x.CSCsg40006.pie sync** Activate SMU:

	router(admin)#**install activate disk0:c12k-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 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**

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**

d. 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 from 3.3.x:

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;, 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-3.5.2 <source>/c12k-mcast.pie-3.5.2 <source>/c12k-mgbl.pie-3.5.2 <source>/c12k-mpls.pie-3.5.2 <source>/c12k-k9sec.pie-3.5.2 sync>/c12k-diags.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.

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-3.5.2 disk0:c12k-mcast-
3.5.2 disk0:c12k-mgbl-3.5.2 disk0:c12k-k9sec-3.5.2 disk0:c12k-mpls-3.5.2
disk0:c12k-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:c12k-mini-3.5.2 disk0:c12k-mcast-
3.5.2 disk0:c12k-mgbl-3.5.2 disk0:c12k-k9sec-3.5.2 disk0:c12k-mpls-3.5.2
disk0:c12k-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 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**

6) 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..

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 4.2.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 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	c12k-base-3.5.2.CSCsl64079
DDTS	CSCsl64079
Affected images	This SMU is necessary for 3.5.2 only
SMU Package Name	<boot device> c12k-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.x, the 3.5.x 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.x 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.x 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.x, the default behavior is to restore the router running configuration using the new-format configuration files left behind from the last time 3.5.x 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.x 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. MDR – Minimum

This feature is not supported for upgrades to 3.5.2 release due to:

* boot flash limitation
* Kernel Changes

5. CSCsk86218 - Ensure MBI is compatible before s/w upgrade

Symptom:
1. While upgrading lower releases to 3.5.2.
   Standby PRP gets stuck in MBI state.
2. While downgrading from 3.5.2 to lower releases.
   Standby PRP gets stuck in MBI state.

Condition:
1. During Upgrade/After the Upgrade if standby is not coming up(stuck in MBI state).
   This will happen since there is a version mismatch in the Active and Standby PRPs.i,e one is 3.5.2 and other one is 3.x.x.
   Then standby card may not come up since there is incompatibility in the images.
   Please follow the Workaround 1 or 2 below.

2. During Downgrade/After the Downgrade if standby is not coming up(stuck in MBI state)..
   This can happen since there is a version mismatch in the Active and Standby PRPs. i,e one is 3.x.x and other one is 3.5.2.
   Then standby card may not come up since there is incompatibility in the images.
   Please follow the Workaround 3 below.

3. This issue occurs mainly when there are MBI incompatibility encountered between software versions and install commit is not issued for one of the software. In that situation when RP reloaded it will try to load last committed software that is when the issue occurs.

Workaround:
1. If the issue is encountered after the successful upgrade to 3.5.2 from 3.4.x, but any of the non-dSC RPs reloaded due to an error condition when booting up or an OIR event before "install commit" was issued.

Non-dSC RP is either a standby RP or an RP in non-Owner SDR. Below instructions mention standby RP, the steps are the same for non-Owner RPs.

(a) Verify that this is the issue/situation. Check for
- install operation completed successfully before issuing a reload for all nodes (console logs)
- wait for active RP to come up and verify that it's running 3.5.2 ("show install active")
- verify that standby RP is trying to boot 3.4.2, this can be seen on the standby console in the banner when the image is booting (e.g. :
"Cisco IOS XR Software for the Cisco XR c12000-mbiprp, Version 3.4.2[1]")
- there should be the following error displayed periodically on the standby console:
Insthelper encountered a fatal error condition, and is exiting:
Error value = (1341786888), Error string = ('Subsystem(8180)' detected the 'warning' condition 'Code(5)': Host is down)

(b) Bring standby RP to ROMMON.
This can be done, for example:
- issue "hw-module loc <location> reload" from dSC.
- issue "send break" on the standby RP console line when the following displayed

DRAM DIMM Slot 1: 2048M found, Slot 2: Empty
MPC7457 platform with 2097152 Kbytes of main memory

(c) Reset BOOT variable to a new value
- Check it's current value, it should be pointing to disk0:c12k-os-mbi-3.4.2/mbiprp-rp.vm
- Check if 3.5.2 MBI exists on disk, e.g. :

```
rommon 7 > dir disk0:c12k-os-mbi-3.5.2.14I
  File size   Perms    File name
  0           drw-     etc
  0           drw-     instdb_v
  0           drw-     mbi
  0           drw-     drp
  0           drw-     gsr
  10088776    -rw-     mbiprp-rp.vm
  0           drw-     instdb
```

- Set BOOT variable to new 3.5.2 MBI value, e.g. :

```
rommon 8 > BOOT=disk0:c12k-os-mbi-3.5.2.14I/mbiprp-rp.vm
rommon 9 > sync
```

- do "reset" to reload this node and let it come up with 3.5.2 MBI

Note 1: if you changed config-register value when brining to ROMMON, change it back to the original value.
Note 2: if 3.5.2 MBI is not present on disk, need to go through "diskboot procedure" for standby, please refer to scenario 2 below.

(d) Verify, "install commit"
- verify that the node comes up successfully with 3.5.2, wait until it's in IOX-RUN state.
- when all non-dSC RP nodes are up, issue "install commit"

2. If the router is running 3.5.2 sw and a new standby (or non-Owner) RP is inserted that was diskbooted with 3.4.x previously.

Prepare the new RP in the same way as with original diskboot procedure for standby. For example, by booting mbiprp-rp.vm from tftp or ftp.
E.g. on the standby console:

```
rommon 1 > boot tftp address://directory/mbiprp-rp.vm-3.5.2 192.85.16.23
```

For more documentation on diskboot procedure refer here (only to the steps for standby):

http://www.cisco.com/en/US/products/ps5845/products_installation_guide_chapter09186a008070ab15.html#wp1128296

[Note: this is from documentation for 3.4, needs to be replaced with 3.5 when it's available, or possibly there is a better link]

3. If the issue is encountered when:
- Downdgrading from 3.5.2 to 3.4.x, but a non-dSC RP rebooted/OIR and booting 3.5.2 while the dSC RP is 3.4.x

- The router is booted with 3.4.x sw, and a new RP is inserted that was baked with 3.5.2 previously.