WAN Switch Software Node-by-Node Upgrade Script

Contents

Introduction

This document describes the Cisco recommended 34 point process for a successful IPX, IGX 8400 Series Switch, or BPX 8600 Series Switch software upgrade. This upgrade is for networks running a WAN switch software release that supports the Node-by-Node upgrade feature. This document lists the minimum required steps, and then addresses each step in some detail. The plan outlined in this document has been used to successfully upgrade Cisco IPX/IGX/BPX networks.

This document is intended to be used as an aid for conducting successful switch software upgrades, but is not a substitute for proper planning with your Cisco Sales Engineer, Systems Engineer, or Account Manager.

 **Caution:** It is essential that you follow the steps in the WAN Switch Software Upgrade Planner before performing the steps below. Performing the steps listed below without first consulting the Upgrade Planner will result in network problems.

Prerequisites

Requirements

There are no specific requirements for this document.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Background

Upgrades to switch software for the IPX/IGX/BPX products, while usually requiring some planning, often result in little or no perceived network outage.

The technique employed to achieve upgrades that do not affect service has remained the same since very

early versions of the product. Prior to release 8.4, the IPX/IGX/BPX software architecture required that all nodes in a network run the same major release of switch software. In order to meet this requirement, it was necessary to upgrade all nodes at the same time.

As networks increased in size, so did the amount of management traffic generated at the time of the upgrade. As a result this procedure has been devised to ensure a graceful upgrade in any size of network. This upgrade technique is the recommended course of action when you are upgrading from one software release that supports the Node-by-Node upgrade feature to another software release that also supports the Node-by-Node upgrade feature.

The Node-by-Node feature allows many of the steps to be tailored to only those IPX/IGX/BPX switches that are being upgraded. This tailoring allows for greater control during a switch software upgrade.

In this document the network nodes to be upgraded are called target nodes. Target nodes are assumed to be a subset of the total network node population. A reasonable number of target nodes in a 100-node network would be 10. For switch software release 8.4, the Node-by-Node upgrade function may need to be enabled using the **cnffunc** command.

This document has been written to aid users who are involved in IPX/IGX/BPX upgrades in an 8.4.X and later environment. It is not assumed that the reader has an in-depth knowledge of these switches, but it is assumed that the reader does have an understanding of basic switch configurations.

Please note that as of switch software release 9.2 the IPX platform is not supported. IPX switches may need to be replaced prior to an upgrade to 9.2.

High-level Plan

The following summarizes the steps that are necessary for a successful upgrade. All steps should be completed irrespective of network size.

Stage 1: Planning

Task	Description
1	Select new revision of switch software or Cisco WAN Manager (CWM) (formerly known as StrataView Plus (SV+)).
2	Evaluate known software anomalies in the selected releases.

3	Review release notes for upgrade steps specific to this release.
4	Audit card firmware and hardware revisions and ensure these are supported by the new software release.
5	Write scripts, which is an optional task to aid the parameter changes required in certain sections of Stage 3.

Stage 2: Network Preparation

Note: This stage needs to be completed one week before software upgrade

Task	Description
6	Network health check.
7	Exercise standby control cards.
8	Monitor network closely until time of upgrade.
9	Upgrade CWM (SV+) stations.
10	Verify network management connectivity to network nodes.

Stage 3: The Upgrade

Management access to the network during this period should be closely monitored using the CWM (SV +) topology map and the **dspcds** and **dspalms** commands.

Task	Description
11	Provisioning freeze starts.
12	If available, save network configuration to CWM (SV +).
13	Stop statistics collection.

14	Clear card errors, software logs and disable processor self tests.
15	Disable statistic sampling state machines.
16	Load new revision into CWM (SV+) stations.
17	Change **cnfdlparm** parameters.
18	Stop all automatic jobs.
19	Load new revision into target network nodes.
20	Validate processor card burn.
21	Set parameters in preparation for network upgrade.
22	Remove the cause of all MAJOR alarms and if possible all MINOR alarms.
23	Shutdown CWM (SV+) stations - reconfigure if required.
24	If required, implement workarounds identified in tasks 2 and 3.
25	If network has been stable for 30 minutes, upgrade switch software.
26	Let network settle and run customer specific validation tests.
27	Unlock standby processors. Repeat Tasks 25 through 27 for each of the nodes being upgraded.
28	Set operational parameters.
29	Restart CWM (SV+) workstations.
30	Network health check.
31	Restart statistics collection.
32	Restart all automatic jobs.
33	Save network configuration to CWM (SV+).
34	Provisioning freeze ends.

Task Detail

Stage 1: Planning

Task 1	**Select new revision of switch software CWM (SV +).**

The selection of suitable switch software, and hence, CWM (SV+) will depend on a number of variables including current software revision, hardware requirements, and so on. Contact Cisco Technical Support for further information.

To select the appropriate release of CWM (SV+), review the release notes for the appropriate version in the Cisco WAN Manager Releases documentation on CCO.

Note: CWM needs between one and two hours to start collecting and showing statistics after an upgrade or a reinitiation of the application.

Task 2	**Evaluate known software anomalies in the selected releases.**

Some software anomalies may require additional preparation in order to ensure a smooth upgrade. This may mean:

- Additional upgrade steps
- More parameter changes to be added in Task 21
- Workarounds that can be included in Task 24.

Task 3	**Review release notes for upgrade steps specific to this release.**

As in Task 2, this task may result in:

- Additional steps in the upgrade plan

- More parameter changes to be added in Task 21
- Workarounds that can be included in Task 24.

Task 4	**Audit card firmware and hardware revisions and ensure these are supported by the new software release.**

On an IPX/IGX/BPX, the revision of a card can be obtained using the **dspcds** command. This information can then be used in conjunction with the switch software / firmware / hardware compatibility matrix provided in the switch software release notes to assess whether any changes are necessary. You can find these release notes in the Cisco WAN Switching Solutions pages.

For switches with redundant processor cards (NPC, NPM, or BCC), verify that the firmware version, BRAM size, and RAM size for both cards match.

dspcds Command

The **dspcds** command produces this output for each slot:

```
3 FRM DTV FRI-V35 BF Standby
```

The meaning of each of the elements of the output is:

Output:	3	FRM	DTV	FRI-V35	BF	Standby
Meaning:	<slot #>	<card type>	<front card revision>	<back card type>	<back card rev>	<card state>

The <front card revision> section is illustrated with "DTV" in the output above. The way in which this is interpreted is shown below.

Output:	D	T	V
Meaning:	Model of the Card	Hardware Revision of the Card	Firmware Revision

The first letter indicates the model of the card (in this case '**D**'). This describes the feature set for the card and may only be changed by Cisco or its partners.

The second letter indicates the hardware revision of the card (in this case '**T**'). This can only be changed by sending the card back to the factory.

The third letter indicates the firmware revision (in this case '**V**'). This is a variation on the model and is altered following minor feature enhancements and bug fixes. It can be changed by downloading the new code from a CWM (SV+) workstation and then burning it into the card.

The designator for a particular firmware image as it can be found on CCO is of the form A.B.C, where:

- A specifies the card type
- B specifies the model designator, which specifies much of the capabilities a card has. For example, UVM model C (rev. A) has firmware DCA, while UVM model D (rev. A) has firmware DDA. Model C was the first UVM model that supported G.729 compression (amongst other new features). Model D supports everything that is supported by model C and adds Idle Code Compression to the supported features (amongst others).
- C specifies the firmware version level, which typically indicates the bug-fix level. The latest UVM firmware level used for this example is release E or DDE indicating UVM model D version E.

When you want to check the release level of a card that is installed in a BPX or IGX you can check this through the command **dspcds**. As you will find, the nodes provide the release information in a different way than the notation method used in the CCO filenames. In fact, the nodes provide you with an extra piece of information for hardware compatibility. The notation used by switch software is of the form TYPE B.D.C, where:

- TYPE gives the full name of the card type (UVM, for example)
- B specifies the model designator
- D specifies the hardware version level
- C specifies the firmware version level

Task 5	**Write scripts to aid the parameter changes required in certain sections of stage 3 (optional).**

Writing and testing scripts will:

- Make the parameter change process easier to execute
- Highlight any commands that have changed in the new software release.

There are products to set parameters in preparation for a network upgrade. Software packages that have been used successfully for upgrades are:

- Procomm  : Traditionally used by StrataCom Program Managers. Scripts have been written that read in command lists from EXCEL. Execute them and write success / failure information back to the spreadsheet.
- *Crosstalk*: Used by the Network Audit Team.

Stage 2: Network Preparation

Task 6	**Network health check**

See Appendix A

Task 7	**Exercise standby control cards.**

See Appendix B

Task 8	**Monitor network closely until time of upgrade.**

Task 6 should highlight any existing network issues, but it is prudent to monitor the network for new software errors and card errors right up to the time of the upgrade. Report recurring errors to Cisco Technical Support.

See Appendix A for details on checking for software errors and card errors.

Task 9	Upgrade CWM (SV+) stations.

CWM (SV+) releases can manage networks that are running software which is up to two releases behind the CWM (SV+) release.

Task 10	Verify network management connectivity to network nodes.

Ensure that every network switch can be connected-to using either Inband or Out of Band access. Using TELNET, connect to each IPX/IGX/BPX in the network. If the network uses both Inband and Out of Band access, test each method separately.

Stage 3: The Upgrade

Task 11	Provisioning freeze starts.

Halt provisioning of new services until completion of upgrade.

Task 12	Save network configuration.

If the Configuration Save and Restore feature has been purchased, save a snapshot of the network configuration on a CWM (SV+) workstation.

Further details on this procedure can be obtained from the command reference manual that is for the release of software being used.

Task 13	Stop statistics collection and shutdown the Statistics Collection Manager.

See Appendix D.

Task 14	Clear card errors and software logs, and then disable processor self tests.

On all nodes to be upgraded clear card-errors and software-logs using the following commands:

- **clrcderrs ***
- **clrswlog**
- **clrswlog s**

The processor self test is disabled by entering the **cnftstparm** command, and then selecting the processor type that is relevant to the node that is being reconfigured.

Task 15	Disable statistic sampling state machines.

Cisco engineering now recommends the disabling of the statistics sampling state machines during the **loadrev** phase of an upgrade. Previously, statistics were disabled during the **runrev** phase.

These state machines can be disabled on all nodes to be upgraded using the **off1** or **off2** commands.

The following parameters should be disabled.

- Conn Stat Sampling
- Line Stat Sampling
- Port Stat Sampling

Note: The disabling of these functions will effectively disable the **dspchstats**, **dsptrkutl**, **dspportstats** statistics commands. Should these commands be required for troubleshooting purposes, the state machine can be re-enabled on a node-by-node basis after the new software has been loaded (the node is in the *Upgraded* state). All state machines re-enabled must be disabled before the **runrev** section of the upgrade. State machines may be re-enabled using the **on1** or **on2** commands.

Task 16	Load new software revision into CWM (SV+) stations.

Load new software version into CWM (SV+) stations. Verify that the images have loaded successfully. Validate the revision image on each CWM (SV+) station by issuing the **validate_image** <*filename.img*> command. Note that the filename is different for IPX/IGX/BPX switches

- The IPX image number is appended with an N.
- The IGX image number is appended with a G.
- The BPX image number is appended with a B.

Task 17	Change cnfdlparm parameters.

This task can speed up the software distribution phase (Task 19) of an upgrade. Configure the *Session Timeout* and *Request Hop Limit* parameters as follows using the **cnfdlparm** command. If the nodes to be upgraded are clustered in the same topological region of the network, the target (non-CWM) nodes may have the *Request Hop Limit* reduced to 4. To determine the number of hops between nodes, issue the **drtop** command.

We are interested in the session time out and the hop fields of the **cnfdlparm** command. If the nodes to be upgraded are in the same area then we can reduce the request hop limit. To determine the request hop limit use the **drtop** command.

- All network nodes: *Session Timeout* 30000
- CWM (SV+) nodes: *Request Hop Limit* 1
- Target (non-CWM) nodes: *Request Hop Limit* 8

Task 18	Stop all automatic jobs.

Delete or disable all automatic jobs that have been configured on the target IPX/IGX/BPX nodes.

Further details on automatic jobs can be obtained from the command reference manual that is relevant to

the release of software being used.

Task 19	Load new revision into target network nodes.

This is accomplished by executing the **loadrev <new_revision> <node_name>** command on each of the target nodes.

The software download is complete when the **dsprevs** command shows all redundant nodes as having a *Running* primary revision and an *Upgraded* secondary revision. The secondary revision should correspond to the revision used in the **loadrev** command. For additional information about processor card status during a switch software upgrade, refer to Active and Standby Control Card States During a WAN Switch Software Upgrade.

Non-redundant nodes will show the secondary revision as being *Loaded*, and not *Upgraded*.

Failures connected with the programming of the processor card electrically erasable, programmable, read-only memory (EEPROM) results in flash failure alarms in conjunction with software errors. In the event of such an alarm, try the loadrev process again. Use the **loadrev** command to bring the node back to the current software release running in the network. The syntax of the command is:

loadrev <current_running_revision> <node_name>

Enter the command, and then start task 19 again. Any further failures will require the currently *Active* card to be replaced. In this case, as before, issue the **loadrev** command to restore the node to the current running software release. After the **loadrev** command is issued, verify that the node is stable by issuing the **dspcds** and **dsprevs** commands. The **dspcds** command should display *Active* and *Standby* processor cards. The **dsprevs** command should display only the current running software release for the node. After the node is stable, enter the **switchcc** command. The *Standby* (was the *Active* processor) processor card can now be replaced.

See Appendix C.

Task 20	Validate processor card burn.

Note: This step is to be performed after all target node standby processors are upgraded. See task 19.

Validate processor card burn on all target nodes by performing the following task:

1. Execute the **chkflash** command

2. When *Command* prompt returns, check the software error log for any errors logged as a result of the **chkflash** command (check error timestamp).

3. Should the **chkflash** command fail, software errors 872, 873 or 874 will be logged, but other errors may also occur.

4. All errors should be reported to Cisco Technical Support. Do not continue the upgrade process. It is possible that the revision of software on the node or nodes that logged the errors is corrupt.

Task 21	**Set parameters in preparation for network upgrade.**

See Appendix E for parameter changes.

Include required nonstandard changes identified in tasks 2 and 3.

Task 22	**Remove the cause of all major alarms, and if possible, all minor alarms.**

Ideally, the network should be alarm free at the time of the software upgrade (Task 25). If this is not possible, at least the reason for all major alarms should be identified and noted, and then suitable reconfiguration should be made in order to remove the alarm. Verify target node load models by issuing the **chklm** and **dsplm** commands as described in Appendix A.

Note: Suitable reconfiguration should not involve making configuration changes via the CLI or CWM (SV+) to the IGX/BPX/IPX nodes as one processor card is in the *Upgraded* state.

Any minor alarms should be noted so that, after the upgrade, a comparison can be made.

Note: A switch software upgrade should not be attempted while there are unreachable nodes in the network.

Task 23	**Shutdown CWM (SV+) stations - reconfigure if required.**

For a complete network upgrade, all CWM (SV+) workstations should be shutdown. This is achieved by selecting the **Stop Core** option from the CWM (SV+) main menu. For a partial network upgrade, this task may not be required.

Any reconfiguration that is required in order for CWM (SV+) to work with the new software release should be done at this time.

Task 24	**If required, implement workarounds identified in tasks 2 and 3.**

Any workarounds that are required for a graceful upgrade will have been identified in tasks 2 and 3.

Task 25	**Upgrade switch software if network is stable for 30 minutes.**

If no topology changes have occurred within the network for a period of 30 minutes since the successful completion of Task 19 and steps 20 through 24 were successfully completed, execute the

runrev <new_revision> <node_name>

command from one of the target nodes. This will execute the new release on a network node.

To verify target node stability, issue the following commands in the order listed:

Command	Action You Must Take
dspprf	Verify that *IDLE RT* is greater than 40. If it is not, contact Cisco Technical Support.
dsprevs	Verify that correct software revisions are loaded.

dspcds	Verify that the processors cards are in the *Active* and *Locked* state.
dspalms	Verify that there are no MAJOR alarms on the target node.

Note: Since the upgrade process will involve the network temporarily switching clock sources, care must be taken when issuing the **runrev** command on the highest numbered network node. Coordinate the upgrade of the lowest and highest numbered nodes with the Cisco Sales Engineer, Systems Engineer, or Account Manager.

Task 26	**Let network settle and run network validation tests.** **Note: For additional information on runrev interval for advanced users, read Appendix G.**

Let the target node processors complete all management update tasks. The amount of time this will take depends on the number of nodes in the network. Allow at least 10 minutes per node. During this period, logging onto nodes via the command line interface (CLI) should be kept to a minimum.

After 10 minutes, login to the target node and verify health using the following commands.

Issue these commands in the order listed.

Command	Action You Must Take
dspprf	Verify that *IDLE RT* is greater than 40. If it is not, contact Cisco Technical Support.
dsprevs	Verify that correct software revisions are loaded.
dspalms	Verify that there are no MAJOR alarms on the target node.
dspcds	Verify that the standby processor is in the *Locked* state and no cards are in a Failed state.
dspswlog	Check for new software errors.

dspswlog s	Check for new software errors.
dspcderrs	Check for new card errors.
dsptrks	Verify status of all trunks.
dspnds	Check for any unreachable nodes.
dspnode	Verify status of Feeder shelves (if applicable).
dspsloterrs	Check for new slot errors.

Note: Various state machines were disabled in Task 15, so commands such as the **dspportstats** and the **dspchstats** commands will not be functioning.

This period provides an ideal time to run tests to check that the new software is functioning correctly.

Interrogate all external management systems that are used to manage any routers that are connected to the IPX/IGX/BPX network. This interrogation is done to ensure that all devices are reachable.

If possible, end users should be contacted and asked to check that all network connections are in proper working order.

Note: In the unlikely event that a decision is taken to revert back to the previous software revision, Cisco Technical Support should be contacted prior to switching to the old revision. Important information as to why the new software is not functioning correctly will be lost after switching back to the old revision.

Task 27	**Unlock standby processors.**

Repeat Task 25, Task 26, and Task 27 for each of the nodes being upgraded. Allow sufficient time between individual node upgrades to verify node stability, and run operational tests. See Appendix F.

Task 28	**Set operational parameters.**

All parameters changed in Task 12, Task 17, and Task 21 should be reverted to their original settings, as was captured in Task 6.

Note: Actual commands used to change the parameters may have changed. In addition to this, it may be

necessary to adjust other parameters for correct network operation while running the new software release. Consult release notes for engineering recommendations and new default values.

Task 29	Restart CWM (SV+) stations.

Select the **Start Core** option from the CWM (SV+) main menu.

Task 30	Network health check

See Appendix A

Task 31	Restart statistics collection.

Restart the Statistics Collection Manager (SCM) by selecting the relevant option from the CWM (SV+) main menu.

Select all relevant statistics (refer to notes made in Task 13). Do the following:

1. From the **config** pull down menu, select **stats enable**.
2. Check all statistics groups, and then move required statistic types to the **selected** section.
3. Send a **stats enable** to all nodes using the following procedure:
    - From the **config** pull down menu, select **node selection**.
    - Make sure all nodes are selected, depress **Send Stats Enable** radio button followed by *OK*.
    - Monitor the *Outgoing Requests / Incoming Responses* windows within the SCM main window to ensure that an SNMP *put* is sent to all nodes and a matching *OK* response is received in return.
4. Enter the **-config** command.
5. Enter the -node command.

6. Make sure all nodes are selected, depress **Start Statistics Collection** radio button, and then click *OK*.

Task 32	Restart all automatic jobs.

All automatic jobs that have been configured on the target IPX/IGX/BPX nodes should re-enabled. This also applies for any cron jobs on the CWM (SV+) stations.

Further details on jobs can be obtained from the command reference manual that is relevant to the release of software being used.

Task 33	Save network configuration.

See Task 12.

Task 34	Provisioning freeze ends.

Appendix A Task 6: Network Health Check

Follow these instructions.

1. Audit the parameters using the following commands. Settings should be consistent across all nodes of the same type within the network. Document differences and any variations from the default values.
    - **cnfnodeparm**
    - **cnfcmparm**
    - **cnfdlparm**
    - **cnffstparm**
    - **cnfdiagparm**

- **cnftstparm**
- **cnfprfparm**
- **on1**
- **on2**
- **on3**
- **cnfsysparm** (only need to check one node as settings are network wide)
- **cnffunc**
- **dspmnupdt**
- **cnftlparm** (8.4 onwards)
- **cnfsnmp**
- **cnfcmb** (IGX/IPX only, settings are network wide)

Parameter differences between nodes of the same type and variations from the defaults should be assessed to ensure they will not impact the software upgrade. Contact Cisco Technical Support if advice is required.

2. Audit network for recent software errors (active and standby controller cards), CPU idle time, card errors, load model inconsistencies, trunk errors and alarms. Use the following commands to accomplish these tasks:
   - **dspswlog**
   - **dspswlog s**
   - **dspcderrs** or the **dspcderrs <slot#>**
   - **dsptrkerrs**
   - **dspalms**, **dspslotalms**, **dspbuses**, **dspsloterrs** (for BPX only)
   - **dspprf**, or **dspprfhist**

Use these commands to check the amount of free time that a node's CPU has. These commands sample the amount of CPU time each process is using every 20 seconds. In this case, node *igx16* is idle for about 88% of the time. A typical display is shown below:

```
igx16   TN   StrataCom   IGX 16    8.2.56   Oct. 13
1997 17:47 GMT

Active    0   262079990   -20   262059990   -40
262039990 Current

Proc   RT  HSds LSds      RT  HSds LSds        RT  HSds
LSds
IDLE   88   43    0       89   46    0         88
65    0
RSC     0   12    0       0   13    0          0
15    0
CBUS    0   76    0       0   75    0          0
78    0
NETW    0   53    0       0   48    0          0
58    0
TRNS    2  199    0       2  187    0          2
216    0
FAIL    4    8    0       3    4    0          4
2    0
SNMP    0    0    0       0    0    0          0
1    0
PROT    0    0    0       0    2    0          0
1    0
TXIO    0    0    0       0    0    0          0
0    0
ILMI    0    0    0       0    0    0          0
0    0
SUMM    2    4    0       3    1    0          2
2
```

- **chklm** or **dsplm** : These commands compare sections of the current node's database with all other nodes in the network. Run the **chklm** command on every node in the network sequentially. When complete, return to the first node and run the **dsplm** command. Sample output is shown below:

```
igx16   TN   StrataCom   IGX 16   8.2.56   Oct. 13
1997 17:52 GMT
```

```
Nd T L C LC
32 P P P P
```

This example is taken from a network that contains two nodes:

```
NodeName J/Num

igx16     /16
igx32     /32
```

The output from the **dsplm** command executed on *igx16* shows the results of the comparison between certain sections of *igx16*'s databases and that of *igx32*. In this case, the *P* in the output stands for pass, which indicates that everything is in order. Any failures are indicated by an *F* in the **dsplm** command output screen.

Note: For software releases above 8.4, the **dsplm** command will give incorrect results if the network topology has recently changed.

Follow these instructions.

1. Investigate the following:

   - **Recent software errors**: Any nodes that continually log errors or have logged recent errors should be reported to Cisco Technical Support.

   - **Card errors**: Cards that are logging self / background test failures or have a history of hardware errors should be investigated by Cisco Technical Support.

   - **Nodes with less than 40% CPU idle time (20% in the case of PCCs)**: Are not usually found within BPX/IGX/IPX networks. These nodes should be examined closely. If the idle time is consistently low, you should contact the Cisco Technical Support.

   - **Load model failures**: These should be reported to the Cisco Technical Support. Remember that software release 8.4 and above use trunk based loading and may show load model failures shortly after network topology changes.

   - **Any trunks that are logging errors**: Should either be fixed or configured not to pass management traffic for the duration of the upgrade.

   - **All alarms should be accounted for**. The real purpose of this check is to make sure that

there are no alarms, such as bus failures, that will require special intervention before the upgrade.

2. Ensure that any necessary corrections are made before the start of the upgrade.

3. The location of any automatic jobs should be noted as these will have to be removed during the upgrade.

Appendix B Task 7: Standby control card test

This task will take roughly 60 minutes per node, depending on network size.

1. Log on as Service to each IPX/IGX/BPX in the network in turn and check which processor is *Active* and which is in *Standby* by issuing the **dspcds** command.

2. Verify CC redundancy in each IPX/IGX/BPX. Issue the **cnfnodeparm** command and inspect the *CC Redundancy Cnfged* field for *Y*. A *Y* in the *CC Redundancy Cnfged* field indicates that CC redundancy is enabled. If CC redundancy is not enabled, investigate and re-enable if possible.

3. Issue the **resetcd <card_number> h** command to reset the *Standby* processor

   Note: If the *Active* card is reset in error, the node will rebuild.

4. After the NPC/NPM/BCC returns to *Standby* mode, check software logs for recent errors by issuing the **dspswlog** and the **dspswlog s** commands. A flash programming failure will cause both an alarm and a controller card switch. Report such occurrences to Cisco Technical Support.

5. When the reset card has gone back into *Standby*:

   - Issue the **dspqs** command to check if there are any updates pending.

   - If there are no updates pending, issue the **switchcc** command, which will switch to the standby processor.

   - The **switchcc** will disconnect the current session.

6. Log back into the IPX/IGX/BPX and monitor the network's health. The *Standby* card will go through the following states: Downloader, Update, Standby. The *Standby* card update may take as long as 3 hours to complete for each node, so time should be scheduled accordingly.

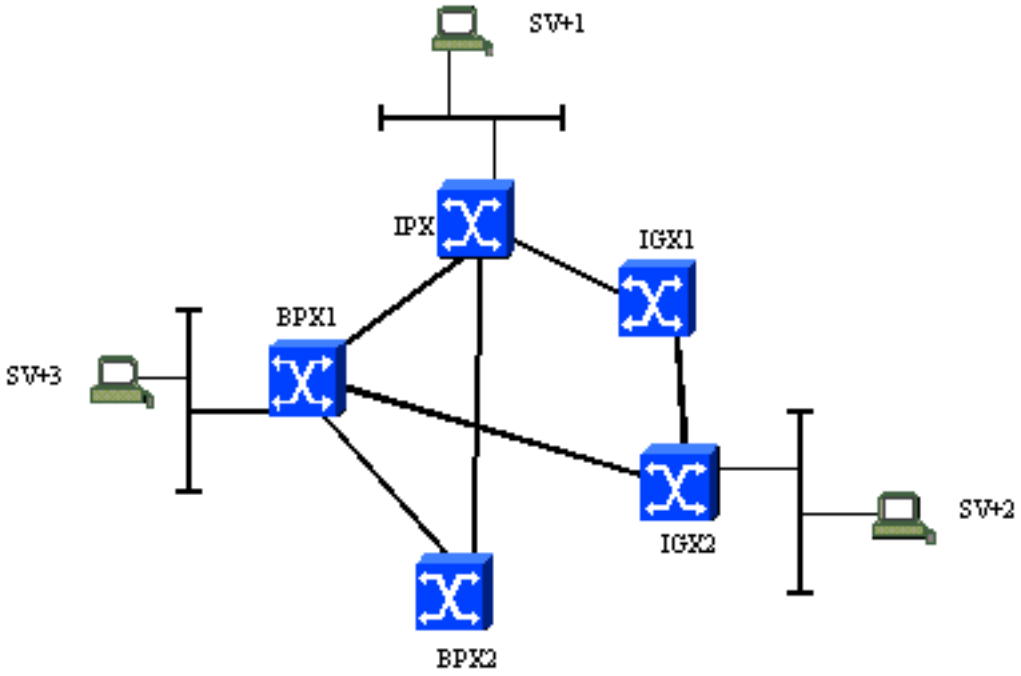
7. After the NPC/NPM/BCC returns to *Standby* mode, check software logs for recent errors by issuing the **dspswlog** and the **dspswlog s** commands. A flash programming failure will cause an alarm and a controller card switch. Report such occurrences to Cisco Technical Support.

8. This procedure should be repeated for each node being upgraded in the network, one node at a time. Ensure that each node's standby card has come out of *Update* mode before proceeding to next node. When the gateway node is switched, communications between CWM (SV+) and the network will be temporarily lost.

   Note: In the case of BPXs, it is recommended that the active card at the start of an upgrade (first **loadrev** command) is in slot 8.

Appendix C Task 19: Procedure to Load New Revision into Network

There are two cases to consider when completing Task 19. Both are listed below, and both refer to the following topology:



Case 1

If there is a CWM (SV+) workstation (indicated by the SV+ prefix in the topology image above) attached to one of each type of node in the network, Task 19 is easily achieved.

To download the new software revision to one of each type of node in the above network, assuming that all switches have default configurations and the CWM (SV+) workstations have the correct software revision loaded, the following commands need to executed from any node:

- **loadrev <new_revision>BPX1**

- **loadrev <new_revision>IGX2**
- **loadrev <new_revision> IPX**

Case 2

Referring to the topology above, if SV+2 and SV+3 do not exist, and new revisions of software for all switch types only reside on SV+1, completion of Task 19 requires a small amount of reconfiguration to some switches.

The download is initiated by the execution of the same commands used in Case 1, but this alone will only result in software being loaded to IPX. In order to load the new software into IGX2 and BPX1, the following reconfiguration must take place:

1. Enter the the **cnffunc** command on both nodes, which will enable the *download from remote strataview* function.
2. Use the **drtop** command to verify the number of hops between target nodes. IGX2 is more than one hop away from IPX, the node to which the CWM (SV+) station is connected. To accommodate this increased distance at IGX2, the *Request Hop Limit* parameter must be set to the actual hop count (in this case 2) using the **cnfdlparm** command.
3. When the software download is complete revert any changes made.

In both Case 1 and Case 2, the software download is complete once:

- The output from the **dsprevs** command shows the node as having a *Running* primary revision.
- An *Upgraded* secondary revision that corresponds to the revision used in the **loadrev** command.

Note: Non-redundant nodes (nodes with one processor) will show the secondary revision as being *Loaded* and **NOT** *Upgraded*. For example, assume that the BPX1 in the topology above has only one processor card. The output from the **dsprevs** command following the completion of the software download would show the following (where 8.4.09 is the new software revision and 8.1.71 is the current revision):

```
BPX1    TN       StrataCom      BPX 15    8.1.71       Oct.
13 1997 17:20 GMT

                  ------ Primary ------       -----
Secondary -----
```

```
NodeName            Status     Revision         Status
Revision

IGX2                Running    8.1.71           Upgraded
8.4.09
BPX1                Running    8.1.71           Loaded
8.4.09
IPX                 Running    8.1.71           Upgraded
8.4.09
BPX2                Running    8.1.71
IGX1                Running    8.1.71
Failures connected with the programming of the card's
electrically erasable programmable
read-only memory (EEPROM) will result in Flash failure
alarms in conjunction with
software errors. In the event of such an alarm, try the
loadrev process again.
Any further failures will require the card to be replaced.
```

When the software download is complete (see above), validate the software burn by performing the following tasks:

1. Execute the **chkflash** command on the nodes with the new software revision.

2. When the *Command* prompt returns, check the software error log entries and timestamps for any errors logged as a result of the **chkflash** command. Enter the **dspswlog** command to accomplish this.

Errors should be reported to Cisco Technical Support. Do not continue the upgrade process, as it is possible that the revision of software on the node / nodes that logged errors is corrupt.

Appendix D Task 13: Procedure to Disable CWM (SV+) TFTP Statistics Collection

This task is only required on the nodes that are to be upgraded. If 10 out of 100 nodes will be upgraded, statistics collection need only be disabled on the 10 target nodes.

1. Determining statistics collection status.

Verify whether statistics collection is disabled or enabled by entering the **dspstatparms** command on each node in the network. Sample output is show below with the *Stats Collection*: status in bold text.

```
igx16      TN       StrataCom        IGX 16
8.1.71        Date/Time Not Set

Statistics Configuration Parameters

TFTP Retry Count:              3     TFTP Read Grant
Delay (sec):      1
TFTP ACK time-out (sec):     10     Enable Date:
00/00/00 00:00:00
Bucket Interval:               0     Enabled from: not
enabled
File Interval:                 0     Rt Interval:
00/00/00 00:00 GMT
Peak Enable Flag:        DISABLED    Nt Second
Offset:                  0
Object Count:                  0          STATS
COLLECTION: DISABLED
Object Subtype Counts:    0 0 0 0         STANDBY
UPDATES: ENABLED
Total File Memory Used:        0
Number of File Allocated:      0
Current File Size:           531
Stat Memory Allocated:         0
Auto Memory Allocated:         0
Auto Mem Rgn Size:        153600

Last Command: dspstatparm
```

As is shown above, on the right side of the display the field *Stats Collection*: indicates the current status. In later releases of software this field is called *Interval stats*: and has additional information on the actual number of statistics enabled.

If statistics collection is found to be enabled, proceed with the remaining steps.

2. Disable statistics collection.

    a. On the statistics master workstation, open the **StrataView Statistics Manager** window. If the SCM is not running on this machine, it will have to be started from the CWM (SV+)

main menu.

b. Within the main SCM window select *config* followed by *Node selection*. All target nodes must appear in the *Selected Nodes* box on the right-hand side of the screen. If they do not appear, click on the right arrow next to each of the target nodes.

c. Under the *Select Action* box, depress the **Stop Statistics Collection** radio button and then close the box by clicking the **OK** button.

d. In the main SCM window, the *Current Status* field should show *Stopped*.

e. Record all *Selected Statistics* so they can be re-enabled after the upgrade.

f. Select *config*, *Stats Enable*, and then select each of the statistic groups in turn.

3. Under each of the statistic groups there is a *Statistics Enable / Disable* window. Within this window there is a **Statistics Type** button that lists all categories for that particular group. For example, the following categories exist under the *Connections* group:

   - Voice
   - Data
   - Frame Relay
   - Fast PAD
   - ASI
   - AXIS Frame Relay
   - ATM connection
   - CE connection

4. Each category must be selected, and any selected statistics must be moved to the *Unselected* window. When all categories have been checked, close the *Enable / Disable* window for that group, and then proceed to the next one and repeat.

5. When all groups have been checked, all statistic types should be deselected. Ensure all *Enable / Disable* windows are closed, and then select *Config* followed by *Node Selection* from within the main SCM window. This selects the nodes that need to have statistics re-enabled.

6. A **Stats Enable** message should now be sent to each of the target nodes. The **Stats Enable** message should be sent to a maximum of 10 nodes at a time. To achieve this, do the following:

    a. Click on the left arrow next to the word *All* to deselect all nodes.

    b. Highlight the target nodes in the list (up to 10 nodes), and move them to the *Selected* box by clicking on the right arrow next to the word **Selected**.

    c. In the *Select Action* box, click the **Send Stats Enable** radio button, and then click the **Apply** button.

    d. Monitor the *Outgoing Requests / Incoming Responses* window within the main SCM window to ensure that an SNMP *put* is sent to all nodes and a matching *OK* response is received in return.

    e. Repeat this for the next ten nodes in the list.

    f. When all nodes have been processed, select the **OK** button to close the window.
7. Verify that statistics collection on all nodes is disabled by entering the **dspstatparms** command on each node in the network. This command should show *Stats Collection: DISABLED*. If this is not the case, resend the **Stats Enable** message to the enabled nodes individually as you did above. If statistics collection is still shown as ENABLED, contact Cisco Technical Support.

Appendix E Task 21: Set Parameters

The changes listed below are those that are recommended to be made in preparation for a switch software upgrade. All other parameters should be at the default settings for the current operating software. An exception to this would be parameters that, having been identified as being different from the defaults during the network health check, have subsequently been judged not to have an impact on a switch software upgrade.

Note: The point at which the following parameters appear within a command may vary from software release to software release.

IPX and IGX

Command: **cnfnodeparm**

Parameter	Value for Upgrade

Update Initial Delay	10000
Update Per-Node Delay	60000
Comm Break Test Delay	60000
Network Timeout Period	10000
Num Normal Timeouts	50
Comm Fail Interval	30000
Comm Fail Multiplier	6
Standby Update Timer	15
Stby Updates Per Pass	20
Gateway ID Timer	90
GLCON Alloc Timer	90
Comm Fail Delay	240

Command: **cnfdlparm**

Parameter	Value for Upgrade
Session Timeout	30000
Request Hop Limit (only applicable for loadrev)	4

Command: **cnffunc**

Parameter	Value for Upgrade
Logging of conn events in local event log	disabled
Logging of conn events in CWM (SV +) event log	disabled

Command: **off1 / on1**

Parameter	Value for Upgrade
Standby Terminal	enabled
Line Diag	disabled
Modem Polling	disabled
Conn Stat Sampling	disabled

Command: **off2 / on2**

Parameter	Value for Upgrade
Statistical Sample (Line Stat Sampling)	disabled
Statistical Alarm	disabled
Job Ready Checker	disabled
Power Supply Monitor	disabled
FRP Port Sampling (Port Stat Sampling)	disabled
Robust Updates	disabled
Robust Alarm Updates	disabled
Realtime Counters	disabled
Update Standby Stats	disabled
Junction ID	disabled

Command: **cnffstparm**

RTD Measurement time	255

Command: **cnftstparm**

Turn off self tests and background tests for all card types

BPX

Command: **cnfnodeparm**

Parameter	Value for Upgrade
Update Initial Delay	10000
Update Per-Node Delay	60000
Comm Break Test Delay	60000
Network Timeout Period	10000
Num Normal Timeouts	50
Comm Fail Interval	30000
Comm Fail Multiplier	6
Standby Update Timer	15
Gateway ID Timer	90
GLCON Alloc Timer	90
Comm Fail Delay	240

Command: **cnfdlparm**

Parameter	Value for Upgrade
Session Timeout	30000
Request Hop Limit (only applicable for loadrev)	4

Command: **cnffunc**

Parameter	Value for Upgrade
Logging of conn events in local event log	disabled

Logging of conn events in CWM (SV +) event log	disabled

Command: **off1 / on1**

Parameter	Value for Upgrade
Standby Terminal	enabled
Line Diag	disabled
Conn Stat Sampling	disabled

Command: **off2 / on2**

Parameter	Value for Upgrade
Statistical Sample (Line Stat Sampling)	disabled
Statistical Alarm	disabled
Job Ready Checker	disabled
Card Statistical Alms	disabled
Card Stat Sampling	disabled
ASI Port Sampling (Port Stat Sampling)	disabled
Robust Updates	disabled
Robust Alarm Updates	disabled
Realtime Counters	disabled
Update Standby Stats	disabled
Junction ID	disabled

Command: **cnftstparm**

Turn off self tests and background tests for all card types

Appendix F Task 27: Unlock Standby Processors

This procedure ensures that a Flash failure in the Active processor only results in a processor card switch, rather than a node rebuild.

1. Log into each of the target nodes and execute the following command:

   loadrev x.x.x <node_name> (**x.x.x** is a dummy revision name)

   The node will declare *revision x.x.x* as unavailable as x.x.x is a nonexistent release. Verify this by entering the **dsprevs** command.

2. Disable processor card redundancy, by setting the *CC Redundancy Cnfged* parameter to *N*. To do this, enter the **cnfnodeparm** command. This will cause the standby NPC/NPM/BCC update process to begin.

   Note: Wait for card to go into *Standby* state.

3. Re-enable processor card redundancy by setting the *CC Redundancy Cnfged* parameter to *Y*. To do this, enter the **cnfnodeparm** command.

4. Activate burn process with the following command:

   loadrev <new_revision><node_name>

5. Issue the **dspdnld** command and verify that Flash starts to erase.

Appendix G: Additional Information on runrev Interval

Note: Failure to properly monitor the network could result in a network outage.

Use the **runrev** interval mentioned in the main document section above on upgrade procedure. In large networks, the **runrev** task could take a long time to complete; therefore, if really needed, decrease the default **runrev** interval. Below are some guidelines to adjust this interval. These guidelines should be used cautiously and the network should be closely monitored.

The safe interval between each **runrev** task depends on whether the large network is national or international and the degree of trunking.

Single thread each **runrev** task beginning with 10-5 minutes per **runrev** on the largest nodes (largest

node is identified by the highest number of connections on the node). If the upgrade progresses without alarming signs, the interval between **runrev** tasks can be reduced gradually to as low as one minute intervals.

Monitor the CPU load, the log, and updates using commands **dspprfhist, dsplog**, and **dspqs**. Monitor for alarming signs such as Unreachable alarms due to excessive network messaging. If **IDLE** time is shown to be too low (less than 10%) with **dspprfhist**, then suspend the upgrade process and investigate the low **IDLE** time. If the **IDLE** time returns to normal values when you suspend the upgrade, then proceed with the upgrade with a larger interval between **runrevs**.

An interval less than one minute between **runrevs** makes it difficult to monitor **dspprfhist**, **dspqs**, and **dsplog**. For instance each **dspprfhist** interval is 20 seconds, and you should monitor at least two intervals to watch for a downward trend. Therefore, do not execute runrevs with an interval less than one minute.

The display of the command **dsptech** provides a concise overview for monitoring the switch.

As stated in the upgrade procedure, shut down the Cisco WAN Manager during the upgrade process. If you do not do this, make sure to monitor the gateway node more stringently.

Related Information

- **WAN Switch Software Upgrade Planner**
- **WAN Switch Software Upgrade Script**
- **Cisco WAN Switching Solutions - Cisco Documentation**
- **Downloads - WAN Switching Software**
- **Technical Support - Cisco Systems**
