



1.1.70 Software Release Notes for the SES Controller

Contents

This document contains the following sections:

Contents	1
About Release 1.1.70	2
System Requirements	4
Hardware Compatibility Matrix	4
Software Compatibility	5
Compatible Releases	6
Additional Deliverables	6
New and Changed Information	7
Upgrading the SES Node	9
Upgrading to a New Software Release	9
Special Installation/Upgrade Requirements	9
Upgrading from SES Release 1.0.16 to Release 1.1.70	9
Upgrading the SES PNNI Runtime Image	13
Upgrading the Runtime Image on Non-Redundant Systems	14
SES PNNI Controller Bring Up Procedure	15
Limitations and Restrictions	16
General Limitations and Restrictions	16
Recommendations	17
Caveats	17
Open Anomalies in Release 1.1.70	18
Problems fixed in Release 1.1.70	19

Anomalies Status Changes for Release 1.1.70	20
Know Anomalies for Release 1.1.60	20
Related Documentation	23
Obtaining Documentation	23
World Wide Web	23
Documentation CD-ROM	23
Ordering Documentation	24
Documentation Feedback	24
Obtaining Technical Assistance	24
Cisco.com	24
Technical Assistance Center	25

About Release 1.1.70

These release notes describe the system requirements, new and changed procedures, upgrade procedures, and limitations that apply to Release 1.1.70 of the SES controller. These notes also contain Cisco support information. The 1.1.70 software release supports the Cisco WAN switching products: BPX 8600 series with SES controller.

SES PNNI and SVC Controller

Release 1.1.70 of the Service Expansion Shelf (SES) controller is compatible with the BPX 8600 series software Release 9.3.30 and with the later 9.3 Releases. The SES controller is connected to the BPX 8600 series switch via a BXM-155 (or T3/E3) port configured as a trunk. Redundant SES systems contain two controller cards which offer APS protection on the ports connecting to the BPX.

Feature Overview

The SES controller is a Virtual Switch Interface (VSI) controller which provides a BPX 8600 series wide-area switch the capability to create switched virtual circuits (SVCs) and soft permanent virtual circuits (SPVCs) using the User-to-Network Interface (UNI) and Private Network-to-Network Interface (PNNI) protocols. One SES controller is required for each BPX 8600 series node that will be originating, transporting, or terminating SVC/SPVC connections. The SES controller is offered in redundant or non-redundant configurations.

Detailed Feature Information

As networks grow in size, PNNI becomes a critical element in the ability to scale a network. PNNI provides a standard, interoperable, and scalable method to grow PVC (SPVC) networks to large sizes. In addition, applications such as voice, video, and LAN require WAN switches to provide dynamic connection capabilities in the form of SVCs. The SES controller provides the BPX 8600 series switch with a centralized controller for establishing SPVCs and SVCs in both the BPX 8600 series networks and in mixed vendor environments.

The BPX 8600 series switch in combination with the SES controller (Release 1.1) supports the following features:

- ATM UNI 3.0/3.1, 4.0 (CBR, VBR, UBR)
- PNNI Single Peer Group and Multiple Peer Group (MPG)
- AINI
- 60 K LCN
- Point to Point SVCs, SPVCs, and SPVPs
- IISP with PNNI Inter-networking
- E.164 and AESA/NSAP (DCC, ICD, E.164) addressing
- Address filtering (source and destination)
- ILMI 4.0
- SPVC and SPVP endpoint provisioning (including ABR)
- OC-3/STM-1, T3/E3 interfaces
- OC-12/STM-4 interfaces
- Intelligent CAC
- Call Processor Redundancy (calls stable across switchover)
- APS on controller uplinks to BPX 8600
- Connection and Path Trace facilities
- Integrated management via CWM and SNMP MIBs
- 50 K connections (SVC+SVP+SPVC+SPVP) per node
- 100 K max endpoints per node (if all 50K connections are DACS)
- 99 UNI/PNNI SVC ports per node
- 100 calls per second
- Dynamic partitioning and soft partitioning
- SPVC support on feeder trunks
- Dedicated Q-bin for control signaling
- Graceful upgrade on the SES controller from Release 1.0.15 or 1.1.60 to Release 1.1.70.

System Requirements

This section describes the hardware supported in this release and the software compatibility requirements.

Hardware Compatibility Matrix

Table 1 and Table 2 list the hardware supported in Release 1.1.70, and show which back cards are compatible with each front card.

Table 1 OC3 Hardware Compatibility

OC3 Combinations (Shipping/Customer Configurations)				
No.	Description	Front Card (PXM)	PXM UI Back Card	PXM Uplink Back Card
1	MMF OC3	SES-PXM-CNTL-4-155 (with 4-port OC3) P/N 800-06454-01 or later	PXM-UIA Rev. A0 or later	MMF-4-155 Rev. A0 or later
2	SMF-OC3, Intermediate Range	SES-PXM-CNTL-4-155 (with 4-port OC3) P/N 800-06454-01 or later	PXM-UIA Rev. A0 or later	SMFIR-4-155 Rev. A0 or later SMFIR-4-155/B Rev. A0 or later

Table 2 T3/E3 Hardware Compatibility

T3/E3 Combinations (Shipping/Customer Configurations)				
No.	Description	Front Card (PXM)	PXM UI Back Card	PXM Uplink Back Card
1	T3	SES-PXM-CNTL-2T3E3 (with 2-port T3E3) P/N 800-06699-01	PXM-UIA Rev. A0 or later	BNC-2T3 Rev. A0 or later
2	E3	SES-PXM-CNTL-2T3E3 (with 2-port T3E3) P/N 800-06699-01	PXM-UIA Rev. A0 or later	BNC-2E3 Rev. A0 or later

Table 3 lists the MGX hardware which is compatible with Release 1.1.70 of the SES controller.

Table 3 *MGX Hardware Compatibility*

Feeder	MGX 8850 R1	MGX 8220
Release	1.1.34	5.0.16
HW Cards	PXM-1	FRSM-4T1/4E1/4T1-C/4E1-C
	PXM1-2T3E3	SRM-T1E1
	PXM1-4OC3	SRM-3T3
	PXM1-OC12	CESM-4T1/4E1
	SRM-3T3	CESM-8T1/8E1
	CESM-8E1	AUSM-4T1/4E1
	CESM-8T1	FRSM-8T1/8E1
	AUSMB-8E1	AUSM-8T1/8E1
	AUSMB-8T1	AUSMB-8T1/8E1
	CESM-T3	AUSMB-8T1/8E1
	CESM-E3	FRSM-HS1
	FRSM-8E1	FRSM-HS1/B
	FRSM-8T1	FRSM-HS2
	FRSM-HS2	IMATM-T3T1/E3E1
	FRSM-2CT3	IMATMB-T1/E1
	FRSM-2T3	
	FRSM-2E3	
	FRSM-HS1/B	
	VISM-8T1	
	VISM-8E1	
	RPM	
	RPM-PR	

Software Compatibility

Table 4 lists the software that is compatible for use in a switch running Release 1.1.70 software.

Table 4 *Software Compatibility Matrix*

Board Pair	SES Controller Release	Latest Boot Code Version	Minimum Boot Code Version	BXM Firmware	SWSW	CWM
PXM1	1.0.10	pxm1_001.000.001.000_bt.fw	1.0.01	MFH	9.3.10	10.3
PXM1	1.0.11	pxm1_001.000.011.001_bt.fw	1.0.11	MFJ	9.3.10	10.4
PXM1	1.0.12	pxm1_001.000.011.001_bt.fw	1.0.11	MFL	9.3.11	10.4

Table 4 Software Compatibility Matrix (continued)

Board Pair	SES Controller Release	Latest Boot Code Version	Minimum Boot Code Version	BXM Firmware	SWSW	CWM
PXM1	1.0.13	pxm1_001.000.013.000_bt.fw	1.0.13	MFM	9.3	10.4
PXM1	1.0.14	pxm1_001.000.013.000_bt.fw	1.0.13	MFN	9.3.11 9.3.24	10.4
PXM1	1.0.15	pxm1_001.000.013.000_bt.fw	1.0.13	MFN	9.3.11 9.3.24	10.4
PXM1	1.1.60	pxm1_001.001.060.102_bt.fw	1.1.60	MFN	9.3.30	10.5
PXM1	1.1.70	pxm1_001.001.070.201_bt.fw	1.1.60	MFR	9.3.35	10.5.10

Compatible Releases

Release 1.1.70 of the SES controller is been certified with the following releases:

- Graceful upgrade to Release 1.1.70 from Release 1.0.16 and Release 1.0.15.
- BPX SWSW Version 9.3.30 or later (see Software Compatibility Notes Matrix, first and second bullets)
- BXM Firmware version MFN through MFR(see Software Compatibility Notes Matrix, first and second bullets)
- CiscoView Version 5.0
- Cisco WAN Manager (CWM) Release 10.5
- BCC-3-64
- BPX-BCC-4V or BPX-BCC-4V/B
- MGX 8850 Release 1, Release 1.1.40
- MGX 8220 5.0.16
- SNMP MIB for Release 1.1.70 is sesmibs1170.tar

For further information on the BXM card, refer to the *9.3 Version Release Notes Cisco WAN Switching Software*.

Additional Deliverables

The SES controller MIB is being provided with the delivery of Release 1.1.70 of the SES controller software on CCO. The MIB is in standard ASN.1 format, and is included in the same directory where the SES controller software is located within CCO. The SNMP SES controller MIB file can be compiled with most standards-based MIB compilers.

Refer to the *Cisco SES PNNI Controller Software Configuration Guide, Release 1*, Appendix E, “SNMP Management Information Base,” for a description of the MIBs supported by the SES controller.

New and Changed Information

This section describes new and changed features in Release 1.1.70 of the SES controller.

60K Logical Connection Numbers (LCNs)

Release 1.1.70 of the SES controller supports up to 60 K channels for VSI connections on trunks, ports, or a combination of trunks and ports. The enhanced BXM-E card models DX and EX support up to 60K channels per card slot. Prior to Release 1.1.70, the total number of channels used by AutoRoute and VSI connections could not exceed 32 K, and the maximum AutoRoute channels supported was 32 K.

To upgrade a BXM-E card slot with 32 K channel configuration, enter the **upgvsilen** command. To configure a BXM card slot to use the 60 K channels feature, follow the procedure for “Hitless Upgrade of BXM to BXM-E” documented in Release 9.3, and then enter the **upgdvsilen** command.

UNI 4.0

The SES controller provides UNI signaling compliant with ATM Forum UNI 4.0 (af-cs-0107.000). This feature allows you to utilize the UNI 4.0 protocol when connecting to ATM UNI devices that require signaling support. This feature also supports the ITU signaling specification Q.2931.

The UNI 4.0 signaling capability provides complete and standard interoperability with commonly used UNI devices. Full implementation of UNI 4.0 enables the following applications:

- Voice transport
- Connection to certain Class 5 voice switching equipment
- Enhanced SVC UNI services, including ABR

AINI

The ATM Inter-Network Interface (AINI) is the new internetworking standard for PNNI-to-PNNI, PNNI-to-B-ISUP, and B-ISUP-to-B-ISUP internetworking. AINI provides most of the advantages of PNNI networking, and provides a secure interface that does not allow the exchange of network topology and availability information.

AINI uses many aspects of PNNI to provide a resilient interface between networks. Despite using static routes, the AINI feature provides crankback, alternate routes, and load balancing across multiple parallel links. When a connection setup encounters a failure, the crankback feature partially releases the connection setup while it is in progress. Crankback enables alternate routing on the controller.

AINI support includes the following features:

- UNI 4.0 based signaling
- Supports UNI 4.0 call types including ABR
- Crankback on AINI links used for alternate routing
- Load balancing across multiple AINI links
- Path and Connection Trace across AINI links
- Support for Hop Counter Information Element to detect loops
- Configurable VPI/VCI allocator node (between AINI peer nodes)
- Connection terminates at AINI ports.

**Note**

Path and connection trace on AINI can be enabled or disabled. For standards compliance, it should be disabled.

AINI allows two or more carriers to interconnect their PNNI networks without exchanging topology information. It provides end-to-end provisioning and resiliency of connections. This is a significant manageability improvement over the traditional method of interconnecting such networks using standard NNI links.

The DSL Forum has defined AINI as the preferred protocol for interconnecting ATM switches with DSLAMs. AINI allows the use of the MGX 8850 in applications such as DSL, wireless, and other aggregation applications.

Hierarchical PNNI Multiple Peer Group (MPG)

Hierarchical PNNI (also referred to as Multiple Peer Group PNNI) allows the growth of PNNI networks to very large sizes. For example, a network with two levels of hierarchy and 50 nodes in each peer group will have 2500 nodes. Another example is as follows:

Expanding a group of 50 peer groups (each containing 50 nodes) to 3 levels of hierarchy yields 125,000 nodes.

While network topology constraints will usually limit the size to smaller numbers, the growth potential is clear. The practical size of the PNNI networks is limited by the following factors, all of which use either processor real time or memory on the node:

- Number of nodes in a peer group.
- Number of “visible” nodes.

This is the number of nodes seen by a node connecting to other peer groups. This number includes the number of nodes in the local peer group, as well as all other peer groups that can be seen from a particular node’s view into the hierarchical network.
- Number of PNNI links in a peer group.
- Number of registered ATM addresses in a network.
- Number of connections supported on the local node.
- Average number of 10 links per node and 2000-addresses per node, with an average of 2-summary addresses per node.

For complete details of PNNI networking, refer to the *Cisco MGX and SES PNNI Network Planning Guide*.

The SES controller supports up to 10-hierarchical levels. Testing of Release 1.1.70 is performed for 4-hierarchical levels. To prepare for the future addition of hierarchy to a PNNI network, the addressing scheme should be planned prior to the provisioning of any connections on a PNNI network. If, at any time in the future, hierarchy must be added to a network in which the addressing was not planned properly, connections need to be re-provisioned using the new addressing scheme.

The introduction of hierarchical PNNI enables the building of very large ATM networks. It also enables the growth of flat PNNI networks with the addition of hierarchy. Enabling hierarchy on an existing PNNI network has no impact on existing ATM connections, assuming that the addressing scheme was planned in advance to accommodate hierarchy. Since connections can be managed end-to-end across a hierarchical network, the manageability of networks can be increased in situations that previously required splitting a large network into multiple routing domains.

Upgrading the SES Node

Use the following sequence to upgrade an SES node:

-
- Step 1** At the BPX node, upgrade the BXM firmware to MFR. For detailed information on BXM firmware upgrades, refer to the *9.3 Version Release Notes Cisco WAN Switching Software*.
 - Step 2** At the BPX node, upgrade the BCC switch software to Release 9.3.35. For detailed information on BCC switch software upgrades, refer to the *9.3 Version Release Notes Cisco WAN Switching Software*.
 - Step 3** Upgrade the SES controller to release 1.1.70. The current boot image is pxm1_001.001.070.201_bt.fw. The current runtime software is pxm1_001.001.070.201_ses.fw. The latest upgrade procedures are included in the sections that follow.
 - Step 4** If applicable, upgrade other feeders in your network to a newer release.
-

Upgrading to a New Software Release

This section contains installation and upgrade instructions. For complete details, refer to the *Cisco SES PNNI Controller Software Configuration Guide, Release 1.1* part number 78-13539-01.



Note

You can gracefully upgrade the SES controller software from Release 1.1.60 to Release 1.1.70.

When upgrading your node, upgrade the software in the following order:

- PXM boot software
- PXM runtime software

The following sections describe how to upgrade the PXM cards.

Special Installation/Upgrade Requirements

This section covers the procedures for upgrading the backup boot and runtime images for the following hardware:

1. Redundant controller card
2. Single controller card (the PXM)

Upgrading from SES Release 1.0.16 to Release 1.1.70

The recommended sequence for upgrading the software on PXM cards is as follows:

1. PXM boot software
2. PXM runtime software

The procedures for performing these upgrades are in the sections that follow.



Note

You can only upgrade to Release 1.1.70 from Release 1.1.60. If you are running a release prior to 1.1.15 (such as 1.0.12, 1.0.13, or 1.0.14), you must upgrade to 1.0.15 before you download the 1.1.70 boot and runtime images. For information on upgrading to Release 1.0.15, refer to the *1.0.15 Version Software Release Notes Cisco SES Controller Software*.

Upgrading the Backup Boot Image

This section provides instructions for upgrading the backup boot images from Release 1.1.60 to Release 1.1.70. The boot upgrade can be graceful or non-graceful, depending on the type of card to be upgraded and the configuration of the node.

Upgrading the Backup Boot on Redundant Systems



Note

Use the following procedure to upgrade the boot on both the active and the redundant controller cards. When performing upgrades on redundant cards, run this procedure on the standby card and not on the active card. This keeps the node in service during the upgrades. Before you upgrade the boot image, FTP the new backup boot firmware, `pxm1_001.001.070.201_bt.fw`, to the disk (should be the same as the PXM FW procedure.)

To upgrade the boot image on the active controller cards on redundant systems, follow these steps:

Step 1

Transfer the backup boot image to the card disk, as follows:

- a. At the SES CLI, enter the **dspipif** command on the active controller card to find the node's IP address. The field internet address for *InPci 0* interface is the node IP address.
- b. From the workstation containing the PXM backup boot image, enter **ftp <Node IP address>**.
- c. Enter the username **cisco**.
- d. Enter your password.



Note

Your password is supplied with the image.

- e. Enter the **cd C:/FW** command to get to the switch directory.
- f. Enter the **bin** command (for a binary transfer).
- g. Enter the **put <PXM backup boot image name>** command to transfer the backup boot and runtime files from the server to the switch directory C:/FW. See the following example:

```
put pxm1_001.001.070.201_bt.fw
```

Replace *<PXM backup boot image name>* with the boot image name. For Release 1.1.70 of the SES, the boot image name is `pxm1_001.001.070.201_bt.fw`.

- h. Enter the **bye** command to end your session.

Step 2

At the SES controller CLI, enter the **dspecds** command to determine the standby card slot number.

Step 3

To verify that the boot IP for both the active and standby card is unique, enter the **bootchange** command.

Step 4

Press **Enter** until you see inet on ethernet (e). This is the boot IP address for the active PXM.

To change the boot IP address to make it unique, type a new address at the inet on ethernet (e) prompt.



Note Changing the boot IP address on the active PXM also changes it on the standby PXM.

Step 5 Enter the **cc** *<slot number>* command to change to the standby card.

```
ses1.1.PXM.a> cc 2
```

Replace *<slot number>* with the slot number of the card you want to work on.

Step 6 Type **sh** to go to the shellConn.

```
ses1.2.PXM.s> sh
```

Step 7 Enter the **sysBackupBoot** command.

```
PXM1> sysBackupBoot
```

Step 8 Press **Return** after you see the disk sync message to get back to active PXM.

Step 9 Exit or open a new telnet window. Telnet into the standby IP host inet address from Step 3.



Note An alternate way to get to the standby card is via the console port on the standby.

Step 10 Use the following procedure to reset the card:

- a. Verify that the card is at the `pxm1bkup>` prompt. If it is not, enter the **sysBackupBoot** shellConn command on the standby card.
- b. Enter the **sysPxmRemove** command:

```
pxm1bkup>sysPxmRemove
```

After you issue the **sysBackupBoot** command, it takes about one minute for the active PXM to reset the card. If the active PXM resets the standby PXM, wait until it comes to the standby state (approximately four or five minutes), then telnet into the standby and repeat Step 5 and Step 6. After the **sysPxmRemove** command is issued the active PXM can not reset the standby.

Step 11 Enter the **cd** `"C:/FW"` command from `pxm1bkup>` prompt to get the FW directory.

```
pxm1bkup> cd "C:/FW"
```

Step 12 Enter the **ls** command to verify that the boot firmware file is there.

```
pxm1bkup>ls
```

Step 13 Enter the **sysFlashBootBurn** *<"boot firmware file name">* command to burn the image on the disk:

```
pxm1bkup>sysFlashBootBurn "pxm1_001.001.060.102_bt.fw"
```

The system will ask if you want to proceed. Enter **Y** for Yes.

Step 14 When the `pxm1bkup>` prompt returns, enter the **reboot** command.

```
Flash Download completed...
value = 0 = 0x0
pxm1bkup> reboot
```

Step 15 Log in to the active PXM.

- a. Enter the **dspcds** command to ensure the standby is in standby state.
- b. Enter the **dspcd** *<standby slot #>* command to verify the firmware was loaded successfully.

Step 16 Load the backup boot onto the active PXM.

- a. Enter the **switchcc** command to change cards.

```
ses1.1.PXM.a> switchcc
```

- b. Log in to the SES controller.
- c. Perform Step 5 to Step 13 on the new standby PXM.

Upgrading the Backup Boot on Non-Redundant Systems

The upgrade of the boot on a non-redundant controller card is non-graceful. This means the traffic gets disrupted on the card during this operation. The upgrade can only take place when the card is in the BOOT stage. Because there is only one controller card, there will be a node outage as well.

For non-redundant systems, follow these steps to upgrade the backup boot:

Step 1 Transfer the backup boot image to the card disk using FTP as follows:

- a. At the SES CLI, enter the **dspipif** command at the active controller card to find the Node's IP address. The field internet address for *InPci 0* interface is the node IP address.
- b. From the workstation containing the PXM backup boot image, enter **ftp <Node IP address>**.
- c. Enter the username **cisco**.
- d. Enter your password.



Note Your password is supplied with the image.

- e. Enter the **cd C:/FW** command to get to the switch directory.
- f. Enter the **bin** command (for a binary transfer).
- g. Enter the **put <PXM backup boot image name>** command to transfer the backup boot and runtime files from the server to the switch directory C:/FW. See the following example:

```
put pxm1_001.001.070.201_bt.fw
```

Replace *<PXM backup boot image name>* with the boot image name. For Release 1.1.70 of the SES, the boot image name is *pxm1_001.001.070.201_bt.fw*.

- h. Enter the **bye** command to end your session.

Step 2 Log in to the SES.

Step 3 At the shell, enter the **sysBackupBoot** command to put the controller card into the PXM backup prompt stage.

```
pxm1>sysBackupBoot
```

The PXM card resets.

Step 4 Log in to the PXM.

Step 5 Enter the **cd "C:/FW"** command at the `pxm1bkup>` prompt to get the FW directory.

```
pxm1bkup>cd "C:/FW"
```

Step 6 Enter the **ls** command to verify the boot firmware file is there.

```
pxm1bkup>ls
```

- Step 7** Enter the **sysFlashBootBurn** <“*boot firmware file name*”> command to burn the image on the disk.

```
pxmlbkup>sysFlashBootBurn“pxm1_001.001.070.201_bt_fw”
```

The system will ask if you want to proceed. Enter **Y** for Yes.
- Step 8** At the `pxmlbkup>` prompt, enter the **reboot** command.

```
pxmlbkup> reboot
```

The node resets.
- Step 9** Log in to the node.
- Step 10** Log in to active PXM.
- Step 11** Enter the **dspscd** <*active card*> command to determine if the upgrade was successful.

```
ses1.1.PXM.a> dspscd 1
```


Upgrading the SES PNNI Runtime Image

This section provides instructions for upgrading the runtime images from 1.1.60 to 1.1.70.

The upgrade of the runtime image on the redundant controller card is graceful. This means the traffic will not be disrupted. The new runtime image for 1.1.70 is `pxm1_001.001.070.201_ses.fw`.

Upgrading the Runtime Image on Redundant Systems

Follow these steps to upgrade the runtime image on redundant systems:

- Step 1** Use FTP to transfer the runtime image to the card disk.
- At the SES CLI, enter the **dspipif** command at the active controller card to find the node's IP address. The field internet address for *InPci 0* interface is the node IP address.
 - From the workstation containing the PXM backup boot image, enter **ftp** <*Node IP address*>.
 - Enter the username **cisco**.
 - Enter your password.
-  **Note** Your password is supplied with the image.
- Enter the **cd** `C:/FW` command to get to the switch directory.
 - Enter the **bin** command (for a binary transfer).
 - Enter the **put** <*runtime image name*> command to transfer the runtime files from the server to the switch directory `C:/FW`. See the following example:

```
put pxm1_001.001.070.201_ses.fw
```
 - Enter the **bye** command to end your session.
- Step 2** Enter the **dspscds** command to determine the standby slot.

Step 3 Enter the **loadrev** *<standby slot>* *<image version>* command to load the new version of runtime image on the controller card.

```
ses1.1.PXM.a>loadrev 2 1.1(70.200)
```

The standby card resets and comes up in the new revision.

Step 4 When the standby card is in the STANDBY state, enter the **runrev** *<standby slot>* *<image version>* command to run the new version of runtime image on the controller card.

```
ses1.1.PXM.a>runrev 2 1.1(70.200)
```

The active card resets and the standby card takes over as active. Both cards are running the new revision.

Step 5 When the standby card is in STANDBY again, enter the **abortrev** *<standby slot>* *<image version>* command to abort this upgrade if needed, as in the following example:

```
ses1.1.PXM.a>abortrev 1 1.1(70.200)
```

Step 6 Enter the **commitrev** *<standby slot>* *<image version>* command to commit the new version of the runtime image of the controller card, as in the following example:

```
ses1.1.PXM.a>commitrev 2 1.1(70.200)
```

Step 7 Enter the **dspcd** command to verify a successful upgrade.

```
ses1.1.PXM.a>dspcd 1
ses1.1.PXM.a>dspcd 2
```

Upgrading the Runtime Image on Non-Redundant Systems

The upgrade of the runtime image on the a non-redundant controller card is non-graceful. That means the traffic is disrupted on the card during this operation.

For non-redundant systems, follow these steps.

Step 1 Use FTP to transfer the runtime image to the card disk.

- a. At the SES CLI, enter the **dspipif** command at the active controller card to find the node's IP address. The field internet address for *InPci 0* interface is the node IP address.
- b. From the workstation containing the PXM backup boot image, enter **ftp** *<Node IP address>*.
- c. Enter the username **cisco**.
- d. Enter your password.



Note Your password is supplied with the image.

- e. Enter the **cd C:/FW** command to get to the switch directory.
- f. Enter the **bin** command (for a binary transfer).
- g. Enter the **put** *<runtime image name>* command to transfer the runtime files from the server to the switch directory C:/FW. See the following example:

```
put pxm1_001.001.070.201_ses.fw
```

- h. Enter the **bye** command to end your session.

Step 2 Set the new version of the runtime image on the controller card as in the following procedure:

- a. Enter the **loadrev** *<slot>* *<image version>* command as in the following example:

```
ses1.1.PXM.a>loadrev 1 1.1(70.200)
```



Note No cards will reset.

- b. Reply **Y** (yes) to the proceed question.
 c. Enter the **dspcd** command in the following example:

```
ses1.1.PXM.a>dspcd 1
```

The secondary revision on the PXM is set to new image version.

Step 3 Enter the **runrev** *<slot>* *<image version>* command to run the new version of runtime image on the controller card.

```
ses1.1.PXM.a>runrev 1 1.1(70.200)
```

The card will reset and run the new revision when it returns.

Step 4 Enter the **dspcd** command to verify a successful upgrade.

```
ses1.1.PXM.a>dspcd 1
ses1.1.PXM.a>dspcd 2
```

Step 5 At this point, you can still

Step 6 abort this upgrade if needed. To abort the upgrade, enter the **abortrev** command.

```
ses1.1.PXM.a> abortrev 1 1.1(70.200)
```

Step 7 Enter the **commitrev** *<slot>* *<image version>* command to commit the new version of the runtime image of the controller card.

```
ses1.1.PXM.a> commitrev <slot> <image version>
```

```
ses1.1.PXM.a> commitrev 1 1.1(70.200)
```

Step 8 Enter the **dspcd** command to verify that the runtime image is correct on the card.

```
ses1.1.PXM.a> dspcd 1
```

Upgrade Path

Release 1.1.70 supports upgrades from Release 1.1.60 to Release 1.1.70. If you are running a release prior to 1.0.15, you must upgrade to Release 1.0.15 before you upgrade to Release 1.1.70.

For information on upgrading to Release 1.0.15, refer to the *1.0.15 Version Software Release Notes Cisco SES Controller Software*.

SES PNNI Controller Bring Up Procedure

For detailed procedure changes, refer to the *Cisco SES PNNI Controller Software Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/pnni_ses/re111/sescnf/index.htm

Limitations and Restrictions

The following sections describe issues in this release:

- [General Limitations and Restrictions](#)
- [Recommendations](#)

General Limitations and Restrictions

The following list describes limitations and restrictions that apply to this release:

- A graceful upgrade can only be completed from the SES controller software Release 1.0.15 or higher.
- The number of connections is always less than the max con value used in the **addpart** command. This is due to the fact that each card needs 1 LCN for control VC. If it is a PNNI network, there is another VC for RCC. Therefore, if the max con value is set to 9000 connections, only 8999 or 8998 connections can be added.
- The **dspscons** command does not support ranges for VPI/VCI. If you enter **dspscons -vpi 2**, all SPVCs with a VPI less than and equal to 2 are displayed; not just the SPVCs with a VPI equal to 2.
- The Route Optimization algorithm is node-by-node and is based on connection mastership. It is not distributed across the node. For example, if Node A is connected to Node C via Node B, Node A only knows about the connections from A to B, and not about the connections from B to C. This limitation does not allow Node A to use route optimization for connections from B to C.
- There is no check for preventing multiple masters of SPVC connections from pointing to the same slave. When provisioning a second connection to a slave VPI/VCI that is already used, there will be no CLI warning that the connection has failed.
- In a large network, it can take up to 30 seconds (or more) to accept new calls after a switchover. This is because PNNI relearns the topology on a switchover. For existing connections, the control plane and the data plane are not affected on a switchover.
- Node names are not required for each node. A node name can be entered and distributed, but there is no check for node name uniqueness within the network. Multiple nodes with the same name do not cause inconsistencies in PNNI routing.
- BXM interface (OC and T3) traffic policing only works if the cell rate is higher than 50 cells per second.
- When the master endpoint is deleted on a DAX SPVC connection, the slave endpoint is also deleted.
- The following limitation is in the BXM firmware release MFL and all the releases that follow: due to limited memory space on the BXM card and increased code size, channel statistics level 0 is no longer supported on BXM cards (BXM-155-4, BXM-155-8, BXM-622, BXM-622-2, BXM-T3-8, BXM-T3-12, BXM-E3-8, BXM-E3-12 models). When the BXM card firmware is upgraded to MFL or any post MFL release, regardless how many connections have been provisioned, channel statistics level 0 is no longer supported. If a BXM card has channel statistics level 0 turned on, use one of the following upgrade paths to upgrade BXM firmware to MFL or any post MFL release:
 - Change the BXM card to run channel statistics level 1. Statistics level 1 supports a maximum of 16 K connections on a card. If a card has more than 16 K connections configured, some connections must be relocated to other BXM interfaces to reduce the total number of connections to be less than 16 K. Reset the card after changing to statistics level 1.

- Upgrade the BXM card to the BXM-E card. The BXM-E card can continue running statistics level 0. Statistics level 0 can support a maximum of 32 K connections on a card.

Recommendations

The following recommendations apply to Release 1.1.70 of the SES controller:

- SPVC connections are provisioned according to a two-ended provisioning model, similar to the way connections are provisioned using AR. This provisioning model enables more robust management (including fault conditions) of both connection endpoints, as opposed to a model which only provisions the master endpoint.

In order to establish a DAX or a routed SPVC, provision the slave endpoint before provisioning the master endpoint. The traffic parameters and QoS parameters on both the master and slave endpoints must match in order to establish an SPVC.

Interoperability with other equipment using a single-ended provisioning model is supported, but the provisioning must be done carefully. The operator must ensure that the slave provisioning matches exactly with the parameters signaled from the master endpoint.

- For each SPVC addition, deletion, or modification, the SES controller generates a trap to CWM. This trap enables CWM to sync up its connection management database with the BPX SES node in real time. The trap information exchange between CWM and SES is handled by an inter-system communication protocol. The trap-handling rate is much slower than the script driven SPVC setup or delete rate. When you use a script to do burst SPVC addition or deletion, the trap queue may overflow and cause trap loss due to limited trap queue size. If burst SPVC add/delete size is more than 1 K connections, Cisco recommends that you pace your setup/delete rate to be 1 connection per second to avoid trap loss.
- The minSvccVci value for the partition is defaulted to 35. VCI 33 and 34 are marked for future control plane use.
- In the case of obtaining optimized routes while performing PNNI on demand route lookup, Cisco recommends that you change the routing policy to the *best fit* option

Caveats

This section provides information on the open anomalies in Release 1.1.70.

Open Anomalies in Release 1.1.70

The following table describes known anomalies in this SES controller software delivery. A more in depth discussion of each bug is available in the release note enclosure in Bug Navigator.

Table 5 *Open Anomalies for Release 1.1.70*

Bug ID	Description
S2 BUGS	
CSCdt12655	<p>Symptoms: Too many stat collection FTP errors.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCdw03688	<p>Symptom: Software error on handler when executing runrev while upgrading .</p> <p>Condition: None</p> <p>Workaround: None.</p>
S3 BUGS	
CSCds74052	<p>Symptom: Given a redundant SES node, pull out the trunk back-card from the active PXM's slot. This causes the active PXM to reboot and the standby PXM to take over as the active front-card. The previously-active PXM card should come up as the standby card but instead, it keeps rebooting.</p> <p>Condition: Not known as yet. It is suspected that some task is trying to access the NOVRAM on the (absent) trunk back-card.</p> <p>Workaround: None. The only thing to do is not to pull out the trunk back-card while the front-card is either in the active or standby role.</p>

Table 5 Open Anomalies for Release 1.1.70 (continued)

CSCdv22425	<p>Symptom: Standby card goes into rolling boot.</p> <p>Condition: Enter the resetcd command to reset the standby card.</p> <p>Workaround: None</p>
CSCdw15621	<p>Symptom: Cannot enable diagnostics on SES PNNI.</p> <p>Condition: Enter the cnfdiag command to enable diagnostics (online/offline) .</p> <p>Workaround: None</p>

Problems fixed in Release 1.1.70

The following table describes known anomalies in this SES controller software delivery. A more in depth discussion of each bug is available in the release note enclosure of the problem record in Bug Navigator.

Table 6 Open Anomalies for Release 1.1.70

Bug ID	Description
S1 BUGS	
CSCdv48381	Bulk set on proxy slave not functioning.
CSCdv54458	Upgrade from 1.0 to 1.1.60 does not work due to SHM_REP_RAM_NODE_DB chg.
CSCdv57330	Connection addition fails (disk update failing).
CSCdv59710	PNNI link corrupted after upgrade from 1.0.15 to 1.1(60.101).
CSCdv84753	Call stuck in setup state.
S2 BUGS	
CSCdt08059	DLS—Telnet daemon allows access without authentication.
CSCdt78006	DLS—switchcc resulted in temporary connection mismatch on 2 nodes.
CSCdu22913	Pulling out feeder trunk led to pnrndman reset stdby(window timeout).
CSCdu24540	1.0.13verify:dbsvr failed to upgrade after stdby pxm1 reset.
CSCdv49665	JAN: AIS sent down to VSIS, but not to LSM in slot1 only.
CSCdv58746	60302 not send out when conn created failed,chanID reused in new con.
CSCdv63740	After changing SES nodename to small one, conn shows part of old name.
CSCdv67375	SLT: PXM got rst in SES shelf and IPC buffer leaks after configuration.
CSCdv79733	DEV: ADDR-5-ADDR_ERROR in dsperrs after reroutes.
CSCdv81833	Port stuck in down in progress.

Table 6 *Open Anomalies for Release 1.1.70 (continued)*

CSCdw07942	REG21:cnfcon -frame option does not work on SES shelf.
CSCdw09142	addshelf command not working in the SES image.
CSCdw10812	Few SPVC are in temprary failure.
CSCdw17431	REG21: standby PXM1 failed after clralcnf/restoreallcnf in SES PNNI.
S3 BUGS	
CSCdv12060	Bpx report wrong intf physical ID, dsppnport not work, pnccb runaway.
CSCdv27904	Duplicate error message in spvc2cli_errcd.
CSCdv37284	Evt.Log: <ccc session> continuous error message.
CSCdv46656	MGX/BPX: Incompatible info_length interpretation in sys_cap IG.

Anomalies Status Changes for Release 1.1.70

The following table describes known anomalies in this SES controller software delivery. A more in depth discussion of each bug is available in the release note enclosure of the problem record in the Bug Navigator.

Table 7 *Anomalies Status Changes for Release 1.1.70*

Bug ID	Description
S2 BUGS	
CSCdu19130	1.0.13Verify:node crashes after abortrev on other node in network; duplicated.

Know Anomalies for Release 1.1.60

The following table describes known anomalies in the Release 1.1.60 SES controller software delivery. A more in depth discussion of each bug is available in the release note enclosure of the problem record in the Bug Navigator.

Table 8 *Fixed Anomalies for Release 1.1.60*

Bug ID	Description
S2 BUGS	
CSCdt08059	<p>Symptoms: The telnet daemon allowed user access into the switch without authentication.</p> <p>Conditions: While in boot mode, you can telnet to the node. Access via telnet during boot mode is not restricted.</p> <p>Workaround: None.</p>

Table 8 Fixed Anomalies for Release 1.1.60 (continued)

CSCdt12655	<p>Symptoms: Too many stat collection FTP errors.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCdu19130	<p>Symptoms: After entering the abortrev command on one node in the network, the other node with 50 K routed connections crashed. It did not respond to certain CLI commands, such as dsppnports and dspscons.</p> <p>Conditions: There are 50 K routed connections between node pswpop7/pswbpx2 and orses18/svcbpx23 via node pswpop6/pswbpx6. I entered the loadrev and runrev commands to upgrade the orses18 node from 1.0 to 1.1. Everything was fine after upgrade. I then entered the abortrev command to bring the orses18 node back to the 1.0 image. After entering the abortrev command on the pswpop7 node, it suddenly crashed; many tasks were deleted. The pswpop7 node did not respond to some CLI commands, such as dsppnports, dspscons, and dspsconinfo. However, the dspsdate, dspslogs, and dspserrs commands worked fine.</p> <p>Workaround: None.</p>
CSCdu22913	<p>Symptoms: The SSI_SRAM_WIN_TIMEOUT Redman Error caused the standby PXM reset.</p> <p>Condition: There were about 50 k routed SPVC connections between two Orion/BPX nodes. One Orion node had redundant PXM cards. I pulled out the Y-cable on the feeder trunk. The RedmanError SSI_SRAM_WIN_TIMEOUT caused the standby PXM to reset.</p> <p>Workaround: Unknown.</p>
CSCdu24540	<p>Symptoms: After running the script to dncon/upcon on an SES node, the dbsvr command failed to upgrade after the standby PXM reset.</p> <p>Condition: There were about 50 K routed SPVC connections between node orses18/svcbpx23 and node pswpop7/pswbpx2. I ran script to dncon/ upcon on orses18, at the same time reset standby PXM1 on orses18. dbsvr failed to upgrade.</p> <p>Workaround: Unknown.</p>

Table 8 Fixed Anomalies for Release 1.1.60 (continued)

CSCdt78006	<p>Symptoms: Connections went into mismatch after replacing the PXM's in a node and entering the switchcc command.</p> <p>Conditions: A customer was going through an exercise of replacing PXM's on their nodes. On two nodes, the standby PXM was replaced, and the switchcc command was entered to make the new PXM the active one. Connections went into mismatch state for a short while, and then cleared. We were not able to get into the node to collect information while this condition existed.</p> <p>Workaround: Unknown.</p>
S3 BUGS	
CSCds74052	<p>Symptoms: I pulled out the trunk back-card from the active PXM's slot on a redundant SES node. This caused the active PXM to reboot and the standby PXM to take over as the active front-card. The previously-active PXM card should have come up as the standby card, but it kept rebooting.</p> <p>Condition: Unknown. It is suspected that some task is trying to access the NOVRAM on the (absent) trunk back-card.</p> <p>Workaround: None. Do not pull the trunk back-card out while the front-card is in the active or standby role.</p>

Related Documentation

The following Cisco publications contain additional information related to the operation of this product and associated equipment in a Cisco WAN switching network.

Table 9 *SES PNNI Controller Release 1.1 Documentation*

Title	Description
<i>Cisco SES PNNI Controller Software Configuration Guide, Release 1.1</i> DOC-7813539=	Describes how to configure, operate, and maintain the SES PNNI Controller.
<i>Cisco SES PNNI Controller Software Command Reference, Release 1.1</i> DOC-7813541=	Provides a description of the commands used to configure and operate the SES PNNI Controller.
<i>Cisco MGX and SES PNNI Network Planning Guide</i> DOC-7813543=	Provides guidelines for planning a PNNI network that uses the MGX 8850 switch and the BPX 8600 switches. When connected to a PNNI network, each BPX 8600 series switch requires a SES for PNNI route processing.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products Marketplace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)