Release Notes for Cisco MGX 8880 Software Release 5.2.10

These release notes are Part Number OL-9186-01 Rev D0, March 2007

Table of Contents

Table of Contents 1
Overview 2
About Release 5.2.10 3
- Type of Release 3
- Locating Software Updates 3

Features and Enhancements in Release 5.2.10 3
Features in Previous Release 5.2.00 4
- MGX-VXSM-T3 Card 4

System Requirements 4
- Software/Firmware Compatibility Matrix 4
- MGX and RPM Software Version Compatibility Matrix 5
- SNMP MIB Release 6
- Hardware Supported 6
  - Hardware in Release 5.2.10 6
  - MGX 8880 Product IDs and Card Types 6

Service Class Template (SCT) File Information 7
- AXSM/B 7
- AXSM-E 8

Limitations, Restrictions, and Notes for 5.2.10 9
- Upgrading the VISM-PR Image 9

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Higher Level Logical Link Limits 9
AXSM-32-T1E1-E 10
AXSM-E OAM 11
CLI Configurable Access 11
Disk Space Maintenance 11
Saving Configurations 12
clrsmcnf Command 12
AXSM Card APS Limitations 13
Path and Connection Trace 13
Priority Routing 13
SPVC Interoperability 14
Manual Clocking 14
Priority Bumping 14
Other Limitations and Restrictions 15
Clearing the Configuration on Redundant PXM45 Card 15
Known MGX 8880 Media Gateway Anomalies 15
Known Route Processor Module Anomalies 15
Documentation 16
Obtaining Documentation 16
Cisco.com 16
Product Documentation DVD 16
Ordering Documentation 16
Documentation Feedback 17
Cisco Product Security Overview 17
Reporting Security Problems in Cisco Products 17
Obtaining Technical Assistance 18
Cisco Technical Support & Documentation Website 18
Submitting a Service Request 19
Definitions of Service Request Severity 19
Obtaining Additional Publications and Information 19
Acronyms 21

Overview

These release notes contain the following sections:

- "About Release 5.2.10" section on page 3
- "Features in Previous Release 5.2.00" section on page 4
- "System Requirements" section on page 4

- "Service Class Template (SCT) File Information" section on page 7
- "Limitations, Restrictions, and Notes for 5.2.10" section on page 9
- "Known MGX 8880 Media Gateway Anomalies" section on page 15
- "Known Route Processor Module Anomalies" section on page 15
- "Documentation" section on page 15
- "Obtaining Documentation" section on page 16
- "Documentation Feedback" section on page 16
- "Cisco Product Security Overview" section on page 17
- "Obtaining Technical Assistance" section on page 18
- "Obtaining Additional Publications and Information" section on page 19
- "Acronyms" section on page 21

About Release 5.2.10

Version .206 of Release 5.2.10 is a patch release that does not introduce new features.

Version .204 of Release 5.2.10 is a patch release that does not introduce new features. For information about resolved anomalies, refer to the *Release Notes for Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Switches, Release 5.2.10*.

Version .201 of Release 5.2.10 contains fixed VXSM anomalies, which are listed in the *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.2.10.201*.

For the list of updated files in this release, see Table 2 in the "MGX and RPM Software Version Compatibility Matrix" section.

Release 5.2.10 is a maintenance release of Release 5.2 and contains no new features. For a list of resolved bugs, see Known MGX 8880 Media Gateway Anomalies, page 15. These release notes describe the system requirements and limitations that apply to Release 5.2.10 of the Cisco MGX 8880 Media Gateway, and provide Cisco support information.

Type of Release

Release 5.2.10 is a software and hardware release for the MGX 8880 Media Gateway.

Locating Software Updates

Release 5.2.10 software is located at:

http://www.cisco.com/kobayashi/sw-center/wan/wan-planner.shtmlnp

RPM IOS images are located at:

http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml

Features and Enhancements in Release 5.2.10

This release does not introduce new features or enhancements.

Features in Previous Release 5.2.00

This release includes the following new hardware:

- MGX-VXSM-T3 front card
- VXSM-BC-3T3 back card

For additional information and details about the new software features in VXSM Release 5.2.10, refer to the *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.2.10.201*.

For additional information and details about the new software features in VISM-PR Release 3.3.20, refer to the *Release Notes for the Cisco Voice Interworking Service Module (VISM), Release 3.3.25*.

MGX-VXSM-T3 Card

Cisco MGX 8880 Release 5.2.00 introduced a third VXSM card for the support of T3 lines. The card consists of a front card with six T3 ports and a half height back card with three T3 ports. The front card can be configured with either a single back card or two back cards.

System Requirements

This section describes software compatible with this release and lists the supported hardware.

Software/Firmware Compatibility Matrix

Table 1 lists Cisco WAN or IOS products that are compatible with Release 5.2.10.

Table 1 Release 5.2.10 Compatibility Matrix

Switch or Component	Compatible Software Version
MGX 8880 (PXM45/C)	MGX 5.2.10
VXSM	VXSM 5.2.10
VISM-PR	VISM 3.3.25
IOS RPM-XF	12.3(11)T9
IOS RPM-PR (supported only with VISM-PR cards)	12.3(11)T9
AXSM	AXSM 5.2.10

MGX and RPM Software Version Compatibility Matrix

Table 2 lists the software that is compatible for use in a switch running Release 5.2.10 software.

Table 2 MGX and RPM Software Version Compatibility Matrix

Board Pair	Boot Software	Runtime Software
PXM45/C	pxm45_005.002.010.204_bt.fw	pxm45_005.002.010.206_mgx.fw
MGX-VXSM-155	vxsm_005.002.010.201_bt.fw	vxsm_005.052.010.201.fw (CALEA image) vxsm_005.002.010.201.fw (non-CALEA image)
MGX-VXSM-T3	vxsm_005.002.010.201_bt.fw	vxsm_005.052.010.201.fw (CALEA image) vxsm_005.002.010.201.fw (non-CALEA image)
MGX-VXSM-T1E1	vxsm_005.002.010.201_bt.fw	vxsm_005.052.010.201.fw (CALEA image) vxsm_005.002.010.201.fw (non-CALEA image)
MGX-VISM-PR-8T1	vism_8t1e1_VI8_BT_3.2.00.fw	vism-8t1e1-003.053.025.201.fw (CALEA image) vism-8t1e1-003.003.025.201.fw (non-CALEA image)
MGX-VISM-PR-8E1	vism_8t1e1_VI8_BT_3.2.00.fw	vism-8t1e1-003.053.025.201.fw (CALEA image) vism-8t1e1-003.003.025.201.fw (non-CALEA image)
MGX-SRME/B	N/A (Obtains from PXM)	N/A (Obtains from PXM)
MGX-RPM-PR-512 (supported only with VISM-PR cards)	rpm-boot-mz.123-11.T9	rpm-js-mz.123-11.T9
MGX-RPM-XF-512	rpmxf-boot-mz.123-11.T9	rpmxf-p12-mz.123-11.T9
AXSM-1-2488/B	axsm_005.002.010.200_bt.fw	axsm_005.002.010.200.fw
AXSM-16-155/B		
AXSM-4-622/B		
AXSM-16-T3/E3/B		
AXSM-32-T1E1-E	axsme_005.002.010.200_bt.fw	axsme_005.002.010.200.fw

SNMP MIB Release

The SNMP MIB release for 5.2.10 is *mgx8XXXrel5210mib.tar.*

Note SNMP manuals are replaced by the online MIB tool at URL http://tools.cisco.com/ITDIT/MIBS/jsp/index.jsp

Hardware Supported

This section lists the MGX 8880 Product IDs, 800 part numbers, and revision levels.

Hardware in Release 5.2.10

Release 5.2.10 does not introduce new hardware.

MGX 8880 Product IDs and Card Types

Table 3 lists Product IDs, minimum 800 part numbers, and the minimum revision levels for the MGX 8880.

Table 3 MGX Chassis, Card, and APS Configurations

Front Card Type	Min. 800 Part Number and Revision	Back Card Types	APS Con	Min. 800 Part Number and Revision
PXM45/C	800-20217-04-A0	PXM-HD	—	800-05052-03-A0
		PXM-UI-S3/B	—	800-21557-01-A0
MGX-VXSM-155	800-15121-06-A0	VXSM-BC-4-155		800-21428-06-A0
MGX-VXSM-T3	800-4074-02-A0	VXSM-BC-3T3		800-3095-03
MGX-VXSM-T1E1	800-24073-02-A0	VXSM-BC-24T1E1		800-23088-03-A0
MGX-VISM-PR-8T1	800-07990-02-A0	AX-RJ48-8T1		800-02286-01-A0
		AX-R-RJ48-8T1		800-02288-01-A0
MGX-VISM-PR-8E1	800-07991-02-A0	AX-SMB-8E1		800-02287-01-A0
		AX-R-SMB-8E1		800-02410-01-A0
		AX-RJ48-8E1		800-02286-01-A0
		AX-R-RJ48-8E1		800-02409-01-A0
MGX-SRME/B	800-21629-03-A0	MGX-BNC-3T3-M	—	800-03148-02-A0
		MGX-STM1-EL-1	—	800-23175-03-A0

Table 3 MGX Chassis, Card, and APS Configurations (continued)

Front Card Type	Min. 800 Part Number and Revision	Back Card Types	APS Con	Min. 800 Part Number and Revision
MGX-RPM-XF-512	800-09307-06-A0	MGX-XF-UI	—	800-09492-01-A0
		MGX-1-GE	—	800-18420-03-A0
		MGX-2-GE	—	800-20831-04-A0
		MGX-1OC12 POS-IR	—	800-08359-05-A0
		MGX-2OC12 POS-IR	—	800-21300-04-A0
		GLC-LH-SM (was MGX-GE-LHLX)	—	30-1301-01-A0
		GLC-SX-MM (was MGX-GE-SX1)	—	30-1299-01-A0
		GLC-ZX-SM (was MGX-GE-ZX1)	—	10-1439-01-A0
MGX-RPM-PR-512 (supported only with VISM-PR cards)	800-07656-02-A0	MGX-RJ45-4E/B	—	800-12134-01-A0
		MGX-RJ45-FE	—	800-02735-02-A0
AXSM-1-2488/B	800-07983-02-A0	SMFSR-1-2488/B	Yes	800-07255-01-A0
		SMFLR-1-2488/B	Yes	800-08847-01-A0
		SMFXLR-1-2488/B	Yes	800-08849-01-A0
AXSM-4-622/B	800-07910-05-A0	SMFIR-2-622/B	Yes	800-07412-02-B0
		SMFLR-2-622/B	Yes	800-07413-02-B0
AXSM-16-155/B	800-07909-05-A0	MMF-8-155-MT/B	Yes	800-01720-02-A0
		SMFIR-8-155-LC/B	Yes	800-07864-02-B0
		SMFLR-8-155-LC/B	Yes	800-07865-02-B0
AXSM-16-T3E3/B	800-07911-05-A0	SMB-8-T3	—	800-05029-02-A0
AXSM-32-T1E1-E	800-22229-01-A0	MCC-16-E1	—	800-19853-02-A0
		RBBN-16-T1E1	—	800-21805-03-A0

Service Class Template (SCT) File Information

This section contains SCT file information for Release 5.2.00.

AXSM/B

The AXSM/B SCTs have the following characteristics:

- SCT 2 - policing enabled, PNNI
- SCT 3 - policing disabled, PNNI

- SCT 4 - policing enabled, MPLS and PNNI
- SCT 5 - policing disabled, MPLS and PNNI

The file names and check sums for the SCT files are as follows

- AXSM_SCT.PORT.0.V1: Check sum is = 0x6aadd6c6= 1789777606
- AXSM_SCT.PORT.2.V1: Check sum is = 0x78ccfb22= 2026699554
- AXSM_SCT.PORT.3.V1: Check sum is = 0x987919a7= 2558073255
- AXSM_SCT.PORT.4.V1: Check sum is = 0x775bfaa2= 2002516642
- AXSM_SCT.PORT.5.V1: Check sum is = 0xe84c696a= 3897321834
- AXSM_SCT.CARD.0.V1: Check sum is = 0x6aadd6c6= 1789777606
- AXSM_SCT.CARD.2.V1: Check sum is = 0x78ccfb22= 2026699554
- AXSM_SCT.CARD.3.V1: Check sum is = 0x987919a7= 2558073255
- AXSM_SCT.CARD.4.V1: Check sum is = 0x775bfaa2= 2002516642
- AXSM_SCT.CARD.5.V1: Check sum is = 0xe84c696a= 3897321834

A user can do **dspsctchksum** <filename> to confirm that the checksum of the Cisco-released SCT file and the file on the node match.

AXSM-E

The AXSM-E SCTs have the following characteristics:

- CARD and PORT SCT 5 - policing enabled for PNNI, disabled for MPLS
- PORT SCT 6 - Policing disabled, used for PNNI ports.
- CARD and PORT SCT 52 - Policing enabled on PNNI, disabled on MPLS
- PORT SCT 53 - Policing disabled on PNNI and MPLS
- PORT SCT 54 - Policing enabled on PNNI, disabled on MPLS
- PORT SCT 55 - Policing disabled on PNNI and MPLS

The following are checksums for the AXSM-E SCT file:

- AXSME_SCT.PORT.5.V1: Checksum is = 0x793c56d0= 2033997520
- AXSME_SCT.PORT.6.V1: Checksum is = 0xe92db9a5= 3912087973
- AXSME_SCT.PORT.52.V1: Checksum is = 0x51241b7a= 1361320826
- AXSME_SCT.PORT.53.V1: Checksum is = 0x34bdf8b9= 884865209
- AXSME_SCT.PORT.54.V1: Checksum is = 0xb5df2c5c= 3051301980
- AXSME_SCT.PORT.55.V1: Checksum is = 0xc5d355c8= 3318961608
- AXSME_SCT.CARD.5.V1: Checksum is = 0x793c56d0= 2033997520
- AXSME_SCT.CARD.52.V1: Checksum is = 0x972810ac= 2535985324

Limitations, Restrictions, and Notes for 5.2.10

This section includes information about limitations, restrictions, and notes pertaining to MGX Release 5.2.00.

- Due to granularity limitations in the AXSM-E hardware, cell traffic does not reach the configured PCR rate when WFQ is enabled. You must configure connections that have WFQ enabled with a PCR of 101% of the actual required rate. ABR has the same Qbin priority as UBR in the SCT tables. In this case ABR and UBR share excess bandwidth if WFQ is enabled.
- The VXSM cards, when installed for the first time or after clearing the slot configuration, create default configuration. This creation of default configuration involves writing large amount of data to the hard disk in the node.

  When multiple VXSM cards are installed simultaneously or the configuration of multiple VXSM slots are cleared simultaneously, one or more VXSM cards could fail to be installed. This potential failure results in following recommendations (refer to CSCed12646):

  – Install VXSM cards, using **setrev** command, one at a time. Install another VXSM after the earlier one is installed completely and is Active.

  – Clear the VXSM slot configuration using **clrsmcnf** command (with no option where the slot primary software version is preserved) one at a time. Wait until the VXSM rebuilds after clearing its slot configuration (without clearing the slot primary software version) before clearing the slot configuration of another VXSM slot.

Upgrading the VISM-PR Image

If you are upgrading the VISM-PR image to Release 3.2.1x or later and the PXM1E or PXM45 image from Release 4.x or earlier to Release 5.x, first upgrade the VISM-PR cards. Then, upgrade the PXM1E or PXM45 cards in the same node.

Do not configure the new VISM features until you have fully upgraded the network. After you upgrade your network to PXM1E or PXM45 Release 5.x or later and VISM-PR to Release 3.2.1x or later, apply the standard upgrade process.

Higher Level Logical Link Limits

The numbers of logical links in the higher levels of the PNNI hierarchy is limited to 30 per level when the complex node configuration is turned on. The limit is essential to reduce the processing time involved in finding the bypasses between the logical links. Whenever a significant change occurs in bandwidth in one of the links within the peer group, the bypass calculation is triggered and the bypasses are usually found from one logical link to another.

If there are *n* logical links, the calculation involves the finding *n***n* bypasses. If the number of logical links *n* is large, a lot of processing time is used for calculating the bypasses. The number of logical links per level must be limited to 30. The number can be controlled by configuring the appropriate number of aggregation tokens for the outside links for that peer group.

AXSM-32-T1E1-E

The following notes apply:

- IMA version fall back is part of IMA group operation. If a group is configured with version 1.1 and it is connected to a far end group which is configured with version 1.0, this group falls back to version 1.0.
- The IMA link Loss of IMA Frame (LIF) and Link Out of Delay Synchronization (LODS) defect integration times are configurable.
- ATM layer configuration for line and IMA ports takes an additional parameter, AIS enable. It is enabled by default.
- In T1 mode, payload scrambling is disabled by default and in E1 mode it is enabled by default on all lines and IMA groups.
- Only 10 SVC calls per second is guaranteed.
- FDL support for Loopback code detection is not supported.
- Far End Line Performance counters are supported only for E1. They are not supported for the T1 interface.
- HMM support is not available for the IMA and the Framer devices. When a switchover occurs, it can take up to 3.5 seconds for the IMA groups to recover. Data is lost until the groups recover.
- IMA Auto-restart (persistent RX IMA ID) feature is supported.
- IMA group cannot have links from upper and lower bays together.
- ITC clocking mode on IMA is not supported.
- One way transmission delay of more than 500 ms on the T1/E1 IMA links is not supported.
- There is 5 ms fluctuation on IMA delay tolerance.
- While the IMA group accumulated delay is being removed with **clrimadelay**, the following applies:
  - Any changes to this IMA group configuration are temporarily blocked.
  - Any changes in the FE IMA links in this group can cause the NE IMA group to restart.
- The VC and COSB thresholds are updated when the links are added/deleted from the IMA groups.
- The thresholds for the connections added when there are N links in the group can differ from connections added when there are (N+1) links in the IMA group.
- BERT is only supported on the T1 interfaces. BERT is not supported on E1 interfaces.
- The port number in the pnport (shelf.slot:subslot.port:subport) could be a random number. Do not interpret this number as line or IMA group number. Refer to CSCdy08500.
- PNNI requires SCR = 453 cells per second and PCR = 969 cells per second for the control connection.
- SSCOP requires of SCR = 126 cells per second and PCR = 2000 cells per second.

AXSM-E OAM

The following notes apply to AXSM-E OAM cells:

- Any connection can receive E2E/OAM loopback cells up to the line rate (as long as the policing policy permits).
- If the connection is not in the loopback mode and is operating in the normal mode, then the AXSM-E card can receive up to 1,500 segment OAM loopback cells per second. Any excessive segment OAM loopback cells are dropped. This limitation applies for all the connections on a card.

  For example, if only one connection exists, that connection can receive 1,500 segment OAM loopback cells per second. If 2,000 connections exist on an AXSM-E card, and one segment OAM loopback cell per second is being pumped through on each connection, then there can only be up to 1,500 connections to receive loopback cells at any given second. The additional 500 connections are not received for that second.
- The limitation is 1,500 segment OAM loopback cells per card and not per connection. The 1,500 cps assumes an even flow rate.

CLI Configurable Access

The following notes pertain to how command access levels can be configured:

- Not all CLI commands are allowed to be changed and a command cannot be changed to CISCO_GP group access level.
- Only the switch software is allowed to generate the binary file. This file has an authentication signature which has to be validated before the file can be used. Any manual changes to the file would make the file void.
- If the binary file becomes corrupted, then the command access levels revert back to the default values during the card bring-up. To recover, repeat the installation process or retain a copy of the binary file and do **cnfcli accesslevel install** on that service module.
- Currently, command names are verified, but an invalid command name might be parsed and be added to the binary file. However, this invalid name is ignored later.
- If replication to standby failed, the installation process failed.
- The **cnfcli accesslevel default** command restores all command access levels to default for the service module that this command is executed on. This command does not remove the binary file, and this change is not persistent. If the command is executed on the active card of a redundancy pair, the standby card is not affected. When the card is reset and the binary file exists, it will configure from the binary file when it is brought up.

Disk Space Maintenance

Because the firmware does not audit the disk space usage and remove unused files, the disk space in C: and E: drives must be manually monitored.

Manually delete any unused saved configuration files, core files and firmware files and the configuration files of the MGX-RPM-PR-512 and MGX-RPM-XF-512 cards to avoid a shortage of disk space required to store event logs: configuration upload files in the C: drive and the configuration of MGX-RPM-PR-512 and MGX-RPM-XF-512 cards in the E: drive.

The following steps are recommended to remove files on the system from the active controller card:

Step 1 Change to the directory that needs grooming.

```
CLI cc <directory_name>
```

Step 2 List the directory to identify old files that can be removed and available disk space.

```
CLI ll
```

Step 3 Remove any old files (you may also use wild cards in the filename).

```
CLI rm <complete_filename>
```

Step 4 List the directory to see if the file has been removed and disk space is available.

```
CLI ll
```

Saving Configurations

The system keeps only the two most recent copies of the saved system configuration under the C:/CNF directory. You can use FTP to transfer all of the saved configurations under C:/CNF to their local server for future reference. All files under C:/CNF are not replicated over to the standby controller card under any circumstances.

clrsmcnf Command

These notes pertain to the **clrsmcnf** command:

- Cisco does not recommend executing **clrsmcnf** on more than one card at a time
- For the clear service module configuration feature, if there is a controller card switchover before the clear service module configuration operation is complete, the **clrsmcnf** command needs to be re-issued to ensure that the configuration is completely cleared to avoid any incomplete cleanup.
- For the clear service module configuration feature, using the **clrsmcnf** command might result in discrepancy in the PNNI configuration. For example, some connections might be in the mis-match state.
- If the **clrsmcnf** command is given with the <*all*> option to clear the software version for the slot as well, then the card goes into the boot/empty state after the operation is complete.
- If the **clrsmcnf** command is given with the <*all*> option, for cell bus service module, the card goes into boot/empty state. For a broadband service module (for example, AXSM or MPSM-155-T3E3), the card goes into fail/active state.
- While using the **clrsmcnf** command, the card in the specified slot is not usable until the operation has successfully completed.

AXSM Card APS Limitations

These notes pertain to the APS feature:

- For AXSM APS, the backcard of the active card must be present for APS to function.
- AXSM cards need the backcard of the active front card for the APS to work. This implies that AXSM cards do not support the cross backcard removal—the upper backcard of one AXSM and lower backcard of another AXSM.
- If you remove the upper backcard of the active front AXSM, it triggers switching active card. At this point the APS is OK. However, if the lower backcard of the current active AXSM is removed at this time, it will not trigger switching active card since the standby card is missing one of the backcard. At this point the lower backcard APS does not work since the backcard of the active front card is missing.
- Port LED lights on AXSM-E front cards indicate the receive status of physical line connected to it only when the card is in active state. For a standby AXSM-E cards, the LEDs always remain green whether the lines are in LOS irrespective of which lines are Active (refer to anomaly CSCdv68576).

Path and Connection Trace

These notes pertain to the path and connection trace features:

- Path trace is not supported on the control port.
- Path trace does not have the accurate information when there is a crankback on the connect path.
- Path and connection trace support point to point connections.
- Path and connection trace support MPG (multi-peer group) and SPG (single-peer group).

Priority Routing

These notes pertain to the priority routing feature:

Prioritized reroute of SPVCs is not guaranteed if the SPVCs originate on a signaling port. SPVCs might get routed out of order. In-order routing of SPVCs is guaranteed on non-signaling ports.

- RPM does not support configuration of routing priority. All RPM mastered SPVCs are assigned a routing priority of 8 by the PXM.
- Changing the routing priority for DAX connections does not change the priority of the associated SVCs. The SPVCs are not derouted and rerouted if just the endpoint parameters are changed, and routing priority is an end-point parameter. Also, since DAX connections are never derouted even when the UNI port goes down and the **rrtcon** command is not supported for DAX connections, the routing priority change never gets reflected. The only way for this to get reflected is to do a **dncon** and **upcon**. Since DAX connections are never derouted, the effect of this limitation is voided.
- Priority routing operates in a best effort manner for the following reasons:
  - Two in-order releases can still arrive out of order at the master node if they take two different paths.
  - Under congestion scenarios releases can be expected to be transmitted out-of-order. This is because releases of other calls must not be held up if you are not able to send releases on one of the interfaces because it is congested. The calls that were not released could be higher priority calls.

  - Lower priority SPVCs can be routed ahead of higher priority SPVCs. This can happen if you have attempted several times to route higher priority SPVCs, but failed. To prevent starvation of lower priority SPVCs, software will start to route lower priority SPVCs and software will get to the higher priority SPVCs at a later point in time.

SPVC Interoperability

These notes pertain to SPVC interoperability:

- NNI SPVC Addendum Version 1.0 is not supported.
- CC (Continuity Check) shall not be available at the slave end of a single-ended SPVC.
- Reporting AIS detection to CWM is not available at the slave end of a single-ended SPVC.
- The slave end of a single-ended SPVC is not visible to CWM.
- If single-ended SPVCs originated from MGX switches, they can only be configured via CLI and not from CWM in the current release.
- Single-end provisioning is not supported for DAX connections as no value addition is seen for interoperability.
- SPVC statistics are not available for the slave endpoint of a single-ended SPVC because this endpoint is non-persistent.
- When the persistent slave endpoint of an existing SPVC connection is deleted and the master endpoint is allowed to remain, the connection might get established as a single-ended SPVC connection. In this case, CWM shows the connection as "Incomplete."
- Override of SVC connections on a VPI due to an incoming SPVP request for that VPI is not supported The following override options alone are supported:
  - spvcoverridesvc
  - spvcoverridesvp
  - spvpoverridesvp

Manual Clocking

When **resetcd** is invoked, the primary and secondary (if configured) clock sources are recommitted. However, the clock to which the node is latched is not requalified. Only the backup clock is qualified if present. Recommitted means that the primary and secondary get requalified, and the node temporarily latches onto the internal oscillator. After the clock is requalified, the node locks onto the primary clock source once again.

Priority Bumping

When you enable priority bumping on the node, you cannot change the booking factor for AXSM signaling ports. You can change the booking factor for non-signaling ports.

Other Limitations and Restrictions

Other limitations and restrictions are as follows:

- When configuring virtual interfaces (for example, VUNI, VNNI, EVUNI, EVNNI), the physical interface must be of all one ATM header type, either UNI or NNI. The signaling that is applied to a virtual port is independent of the actual virtual port ATM header. The only limit will be that the VPI value must be within the UNI ATM header limitations.
- If command **clrchancnt** is executed while a **dspchancnt** command is currently active, the data displayed is incorrect. Restarting the **dspchancnt** after the previous one has completed displays correct data.
- The **clrsmcnf** command does not work for redundant service modules.
- The **clrsmcnf** does not work if an upgrade is in progress.
- If RPM-XF is configured as a Label Switch Controller (LSC), execution of **clrsmcnf** command on those LSC slots is rejected as designed.
- Configuration information is not synchronized between PXMs during upgrades. If any changes are made to the configuration during upgrades, the standby PXM must be rebooted. The standby PXM must be rebooted when it is in a stable state.

Clearing the Configuration on Redundant PXM45 Card

These notes apply to redundant cards.

- Due to checks to prevent an inserted card from affecting the system, an additional step might be required when inserting two non native PXM45 cards in a shelf. Insert the first PXM45, use the **clrallcnf** command, and allow this to become active before inserting the second PXM45.
- After a **clrallcnf**, explicitly clean up stale SCT files (see anomaly CSCdw80282).

Known MGX 8880 Media Gateway Anomalies

For information about anomalies in MGX Release 5.2.10 on other platforms, refer to the *Release Notes for Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Switches, Release 5.2.10*.

For information about anomalies with the VXSM card, refer to *Release Notes for the Cisco Voice Switch Service Module (VXSM), Release 5.2.10.201*.

For information about anomalies with the VISM card, refer to *Release Notes for the Cisco Voice Interworking Service Module (VISM), Release 3.3.25*.

Known Route Processor Module Anomalies

For information about anomalies with the MGX-RPM-XF-512 card, refer to *Release Notes for Cisco MGX Route Processor Module (RPM-XF) IOS Release 12.3(11)T9 for PXM45-based Switches, Release 5.2.10*.

For information about anomalies with the MGX-RPM-PR-512 card, refer to *Release Notes for Cisco MGX Route Processor Module (RPM-PR) IOS Release 12.3(11)T9 for MGX Releases 1.3.12 and 5.2.10*.

Documentation

A *Guide to Cisco Multiservice Switch Documentation* ships with your product. That guide contains general information about how to locate Cisco MGX, BPX, SES, and CWM documentation online.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Acronyms

Table 4 lists acronyms that have been referenced in these release notes.

Table 4 Acronyms Used in These Release Notes

Acronym	Description
AXSM	ATM Switch Service Module. In these release notes, *AXSM-A* refers to the original AXSM card (*A* did not appear on the card), and AXSM/B refers to the newer AXSM/B card (*B* does appear on the card).
ABR	Available bit rate
APS	Automatic Protection Switching
CALEA/LI	Communications Assistance for Law Enforcement Act/ Lawful Intercept
CBSM	Cell bus service module. CBSMs were formerly called narrow band service modules (NBSMs).
CLI	Command Line Interface
CoS	Class of service
CUG	Closed User Group
CWM	Cisco Wide Area Network Manager
GE	Gigabit Ethernet
IAP	Intercept Access Point
IMA	Inverse Multiplexing over ATM
LANE	Local Area Network Emulation
LFI	Link Fragmentation Interleaving
MFR	Multi-Link Frame Relay
MLPPP/LFI	Multi-Link PPP
MPSM	Multi-Protocol Service Module
MTI	Multicast Tunnel Interface
NBSM	Narrow band service module (traditional name for cell bus service modules in Release 4 and higher)
P2MP	Point-to-Multipoint
PE	Provider Edge
PER	Product Enhancement Request
PNNI	Private Network-to-Network Interface
POS	Packet over SONET
POST	Power On Self-Test
PPP	Point-to-Point Protocol
PXM	Processor Switch Module
RPM	Route Processor Module
SFP	Small Form Factor Pluggable Unit
SM	Service Module

Table 4 Acronyms Used in These Release Notes (continued)

Acronym	Description
SONET	Synchronous Optical NETwork
SPVC	Soft permanent virtual connection
SRM	Service Resource Module
SVC	Switched virtual circuit
VISM	Voice Interworking Service Module
VPN	Virtual Private Network
VRF	VPN Routing / Forwarding
VXSM	Voice Switch Service Module
XF	Express Forwarding