Release Notes for Cisco Voice Interworking Service Module Release 3.1(2)

September 2003

The Voice Interworking Service Module (VISM) product is supported by MGX Voice Media Gateways. Refer to these release notes for Media Gateway and version level support guidelines.

About Release 3.1(2)

The VISM 3.1(2) Release is a maintenance release of the VISM 3.1 Release and contains no new features. This release is a general availability (GA) firmware release for VISM/VISM-PR. See the "Resolved Caveats in Release 3.1(2)" section on page 12 for information on the caveat resolutions introduced with this release.

Note The content of VISM Release 3.1(2) supersedes Release 3.1(1) and all previous releases.

The software Release 3.1(2) for VISM/VISM-PR is supported by the *Cisco VISM Installation and Configuration Guide*, which is available on the Web at the following locations:

- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism31
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8250/vism31
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8230/vism31
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8830/vism31
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/release3/vism/relnotes
- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px1e/release3/vism/relnotes

CISCO SYSTEMS

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

Contents

These release notes contain the following sections:

Features Introduced in Previous Releases of VISM Software

You can access lists of features and descriptions of features contained in previous releases of VISM software at the following location:

- http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/index.htm

Elements of Release 3.1(2)

This section describes the following elements of software Release 3.1(2) for VISM/VISM-PR:

VISM Management Information Base

The VISM Management Information Base (MIB) Version 0.0.30 is available by request through your Cisco VISM Product Marketing representative.

VISM Redundancy

Table 1 provides the support level for 1:N Service Module Redundancy (N = 1 through 11).

Table 1 Service Module Redundancy

Front Card Model Number	Redundancy Support
MGX-VISM-8T1	1:N redundancy (bulk mode support for T1 lines only).
MGX-VISM-8E1	1:N redundancy (bulk mode support for E1 lines only).
MGX-VISM-PR-8T1	1:N redundancy (bulk mode support for T1 lines only).
MGX-VISM-PR-8E1	1:N redundancy (bulk mode support for E1 lines only).

Note You can use a VISM-PR card as a redundant card for a VISM card, but a VISM card cannot be used as a redundant card for a VISM-PR card.

There is support for Bulk Distribution using the SRM-3T3 and SRM-E (OC3) cards.

VISM Call Rate

Software Release 3.1(2) for VISM/VISM-PR handles 10 CAS, SS7, or PRI calls per second per VISM card.

Compatibility

VISM software interoperability with Cisco MGX 8830, Cisco MGX 8850 PXM1E-based, Cisco MGX 8850 PXM1-based, Cisco MGX 8850 PXM45-based, Cisco MGX 8250, and Cisco MGX 8230 platform software is listed in Table 2.

Table 2 VISM Software Interoperability

Product	CW2000 Name	Latest Firmware	Min. Firmware
PXM1	MGX 8850	1.2.20	1.2.10
PXM1E	MGX 8850/MGX 8830	3.0.23	3.0.10
PXM45	MGX 8850	3.0.23	3.0.10
SES	SES	3.0.23	3.0.10
BPX	BPX	9.4.00	9.3.42
RPM-PR	RPM-PR	12.2.15-T2	12.2.13-T4
RPM-XF	RPM-XF	12.2.15-T2	12.2.15
SRM-E	SRM-E	—	—
SRM-C	SRM-C	—	—
AUSM	AUSM	10.2.20	10.2.10

Table 2 VISM Software Interoperability (continued)

Product	CW2000 Name	Latest Firmware	Min. Firmware
AXSM	AXSM	3.0.23	3.0.10
CWM	CWM	12.0.00	12.0.00

VISM software interoperability with other Cisco products is described in Table 3.

Table 3 Software Release 3.1(2) for VISM/VISM-PR Interoperability with Other Cisco Products

Cisco 3810	12.2(8)T1
AS5400	122-10.7
PGW Software	9.3.2

Table 4 describes the software images available for Release 3.1(2) for VISM/VISM-PR.

Table 4 Software Images for Release 3.1(2) for VISM/VISM-PR

Product Name	Software Image	Firmware	Description
MGX-VISM-SW3120	003.001.002.000.FW	vism-8t1e1-003.001.002.000.fw	This image does not support the CALEA[1] feature.
MGX-VISM-LISW3120	003.051.002.000.FW	vism-8t1e1-003.051.002.000.fw[2]	Use this image for CALEA[1] feature support.

1. CALEA = Commission on Accreditation for Law Enforcement Agencies.
2. The CALEA implementation supports the CALEA law intercept confirmation interface.S

Table 5 describes the software boot code and run-time firmware requirements for software Release 3.1(2) for VISM/VISM-PR.

Table 5 Software Release 3.1(2) for VISM/VISM-PR Software Boot and Run-time Firmware Requirements

Board Pair	Latest Boot Code Version	Minimum Boot Code Version
MGX-VISM-8T1	vism_8t1e1_VI8_BT_3.1.01.fw	vism_8t1e1_VI8_BT_3.1.00.fw
MGX-VISM-8E1	vism_8t1e1_VI8_BT_3.1.01.fw	vism_8t1e1_VI8_BT_3.1.00.fw
MGX-VISM-PR-8T1	vism_8t1e1_VI8_BT_3.1.01.fw	vism_8t1e1_VI8_BT_3.1.00.fw
MGX-VISM-PR-8E1	vism_8t1e1_VI8_BT_3.1.01.fw	vism_8t1e1_VI8_BT_3.1.00.fw

Note Loading this release of the backup bootcode is required for existing VISM cards not using this new release.

Limitations and Restrictions

The following limitations and restrictions are valid for software Release 3.1(2) for VISM/VISM-PR:

- Software Release 3.1(2) for VISM/VISM-PR requires you to use 64 Mb VISM cards or VISM-PR cards exclusively.
- Cisco recommends that you use the **cnfcodecjtrdelay** command to configure the *jitter-delay* argument to 20 msec when using DSP firmware versions 3.4 and 3.6.
- In a PNNI network, upspeeding SVC fax or modem calls requires an increase in bandwidth between the voice codec and the vbd codec. For fax calls to go through, you must disable policing.

Installation and Upgrade Procedures

This section describes the following installation and upgrade procedures:

VISM Firmware and Boot Code Download Procedure for PXM1

Step 1 Download the selected revision of service module boot code into the service module in the selected.

a. **tftp** <*node_name* or *IP address*>

b. **bin**

c. **put** <*backup boot*> POPEYE@SM_1_0.BT

d. **quit**

Step 2 Proceed to Step 2c. to upgrade all VISM cards or proceed to Step 2d. to upgrade an individual VISM card.

a. **tftp** <*node_name or IP address*>

b. **bin**

c. **put** <*FW file*> POPEYE@SM_1_0.FW

quit

d. **put** <*FW file*> POPEYE@SM_1_<*slot number of card to upgrade*>.FW

quit

Note Do not enter two **put** commands in the same TFTP session.

Step 3 Proceed to the "Installing VISM Software Updates with PXM1 Cards" section on page 8 to install the download.

VISM Firmware and Boot Code Download Procedure for PXM1E and PXM45

Step 1 Access the image on the Cisco Web site in order to download the image.

Step 2 Use the **ftp** *node-ip* command, where *node-ip* is the IP address of the node to which you want to download the image, to download the image.

Step 3 Enter your username and password.

Step 4 Type **cd C:FW** to access the appropriate directory.

Step 5 Type **bin**.

Step 6 Use the **put** *image-version*, where *image-version* is the downloaded image from Step 1, to download the image to your C:FW directory.

Step 7 Type **bye** to exit the download procedure.

VISM/VISM-PR Firmware Upgrade

Software Release 3.1(2) is for VISM and VISM-PR cards. For hardware graceful upgrades from VISM to VISM-PR, complete the following steps. Ensure that the VISM and VISM-PR cards have the minimum boot code version of vism_8t1e1_BT_3.1.00.fw.

The following versions of VISM software Release 3.1(2) are available:

- 003.001.002.000—without CALEA
- 003.051.002.000—with CALEA

Note You do not have to complete these instructions to use software Release 3.1(2) for VISM/VISM-PR. However, if you do not perform this upgrade procedure, refer to the VISM Features section of the *Release Notes for Cisco Voice Interworking Service Module Release 3.1(0)* for features that are not available to you.

VISM and VISM-PR cards use the same back cards. No new back cards are introduced with this release. In the following procedure:

- Perform the firmware upgrade in the following procedure on the VISM cards; do not remove the VISM cards and replace them with VISM-PR cards at this time.
- Two VISM cards are involved in a redundancy group, initially with the primary card in the active state and the secondary card in the standby state.

- Old-rev refers to the firmware before the upgrade (2.2).
- New-rev refers to the firmware after the upgrade (3.1).

Step 1 Log in to the active PXM1 card (slot 7 or 8).

Step 2 Save the existing configuration as a contingency plan by entering:

savesmcnf <*SM slot#*>

This will save the existing configuration in the C:CNF directory. This file can be used during the downgrade procedure, if necessary.

Step 3 Execute the PXM **install** command:

install sm <*SM slot#*> <*new-rev*>

where:

SM slot# is the slot number of the primary VISM card and *new-rev* is the file name of the new firmware (for example, vism_8t1e1_300.001.000.000.fw).

This command causes the secondary VISM card to reset and come up in the standby state, running the new-rev firmware. The primary VISM card is unaffected by this command.

Step 4 Execute the PXM **newrev** command:

newrev sm <*SM slot#*> <*new-rev*>

where:

SM slot# is the slot number of the primary VISM card and *new-rev* is the filename of the new firmware.

This command causes the primary VISM to reset and the secondary VISM card to become the active VISM running the new-rev firmware.

Step 5 Execute the PXM **commit** command:

commit sm <*SM slot#*> <*new-rev*>

where:

SM slot# is the slot number of the primary VISM card and *new-rev* is the filename of the new firmware.

The two VISM cards are now back to their original condition except that both cards are now running the new-rev firmware.

Step 6 Log in to the active VISM card and use the display commands (dspendpts, dspcasvar, etc.) to confirm that the configuration has been preserved through the upgrade process.

Note For more than one primary VISM card in a redundancy group, ensure that the secondary card is in the standby state and repeat Step 4 and Step 5 for each VISM card in the redundancy group.

It is also recommended to perform the following verifications:

- Make minor modifications to the configuration.
- Check that the changes have been executed correctly.
- Change the configuration back again.

Note If the VISM card is not part of a redundancy group, Step 1 to Step 3 are sufficient.

VISM to VISM-PR Hardware Upgrade

Complete the following steps to upgrade your system from VISM cards to VISM-PR cards.

Caution You must install the redundant (standby) VISM-PR card first. Failure to follow this recommendation results in traffic loss. In addition, do not remove an active VISM card from your chassis. Ensure that you configure an active VISM card to the standby state before you remove it and replace it with a VISM-PR card.

Step 1 Remove the redundant (standby) VISM card from your chassis.

Step 2 Install a VISM-PR card in the slot you removed the VISM card from in Step 1.

Step 3 Administratively configure the VISM-PR card you installed in Step 2 as primary (active).

Step 4 Remove the now redundant VISM card from your chassis.

Step 5 Install a VISM-PR card in the slot you removed the VISM card from in Step 4.

Step 6 Log into the redundant (secondary) VISM-PR card and execute the **dspcd** command. Verify that the output from the **dspcd** command lists the card type under FunctionModuleType as a VISM-PR card. If the card type still indicates the VISM card, execute the **resetcd** *slot-num* command from the PXM and repeat the **dspcd** command to insure that the correct card type is shown.

Step 7 Log into the active VISM-PR card and execute the **dspcd** command. Verify that the output from the **dspcd** command lists the card type under FunctionModuleType as a VISM-PR card. If the card type still indicates the VISM card, execute the **resetcd** *slot-num* command from the PXM and repeat the **dspcd** command to insure that the correct card type is shown.

Step 8 If you have no other VISM cards in your chassis, you have completed the hardware upgrade procedure; do not proceed to Step 9. If you have more VISM cards in your chassis, proceed to Step 9.

Step 9 Remove a standby VISM card from your chassis.

Step 10 Install a VISM-PR card in the slot you removed the VISM card from in Step 9.

Step 11 Repeat Step 9 and Step 10 to remove any remaining VISM cards in your chassis and replace them with VISM-PR cards.

Step 12 Repeat Step 6 and Step 7 on the remaining VISM-PR cards to insure the correct card type is shown.

Installing VISM Software Updates with PXM1 Cards

Software Release 3.1(2) for VISM/VISM-PR provides a procedure for the graceful upgrade (one in which the existing VISM configuration is preserved throughout the upgrade procedure) from the earlier VISM 2.0 release.

Caution Installing VISM software updates from VISM Release 2.2 with CALEA to VISM Release 3.0 without CALEA is not graceful.

Caution Temporary traffic loss occurs during Step 4 and Step 5 of the VISM graceful upgrade procedure of the Upgrade Procedure for software Release 3.1(2) for VISM/VISM-PR.

Initial Conditions

The following initial conditions are required before the graceful upgrade procedure can be started:

- The MGX 8000 Series shelf must be configured with at least two VISM cards in a redundant configuration.

  For more information refer to the add redundancy, **addred**, command in the Cisco MGX 8250, Cisco MGX 8230, and Cisco MGX 8850 PXM1-based Command Reference documentation and the Cisco MGX 8830 and MGX 8850 PXM1E/ PXM45-based Command Reference documentation.
- The VISM cards must be running VISM 2.0 and be configured to the desired configuration.
- The software Release 3.1(2) for VISM/VISM-PR must have been already downloaded to the MGX shelf.
- Ensure that you have the version of VISM software that supports CALEA, if you are using the CALEA feature.

Upgrade Procedure

Upgrades are available for the following releases:

- From VISM 1.5 to VISM 3.1(2)
- From VISM 2.1 to VISM 3.1(2)
- From VISM 2.2 to VISM 3.1(2)
- From VISM 3.0 to VISM 3.1(2)
- From VISM 3.1(0) to VISM 3.1(2)
- From VISM 3.1(1) to VISM 3.1(2)

Installing VISM Software Updates with PXM1E or PXM45 Cards

Complete the following steps to update the VISM software when you are using PXM1E or PXM45 cards in your MGX 8000 Series chassis:

Step 1 Log on to the active PXM1E or PXM45 card.

Step 2 Ensure that the card is in the redundant mode, where the active card is the primary card.

Step 3 Use the **saveallcnf** command to save the existing configuration as a contingency plan.

Step 4 Use the **loadrev** *sm-primary-slot-num new-rev* command, where *sm-primary-slot-num* is the slot number of the VISM/VISM-PR card you to which you want to install the new software, and *new-rev* is the new firmware version number for the VISM software.

Step 5 Use the **runrev** *sm-primary-slot-num new-rev* command to execute the download.

Step 6 Use the **commitrev** *sm-primary-slot-num new-rev* command to commit the new download to the VISM/VISM-PR card.

You have completed the steps. Proceed to the VISM Boot Code Upgrade Procedure with PXM1E and PXM45 Cards, page 11.

VISM Boot Code Upgrade Procedure with PXM1 Cards

The boot code has not changed from VISM Release 3.1(1) to Release 3.1(2). Therefore, the procedure in this section is the same as the upgrade procedure for Release 3.1(1).

Complete the following steps to upgrade the new backup boot code when you are using PXM1 cards in your MGX 8230, MGX 8250, and MGX 8850 chassis:

Note This procedure re-programs the VISM boot code for previous VISMs using the VISM runtime image version 1.0 to 2.0.

Step 1 Telnet to MGX shelf and **cc** to the VISM card.

Note VISM must be in the active state in order to update the VISM boot code.

Step 2 Access the server where the VISM boot code resides and TFTP the VISM boot code to the VISM card with the following procedure:

a. Type **tftp** <*IP address of the MGX shelf*>

b. Type **bin** at the tftp prompt.

Caution Ensure that you perform Step 2b. If you to not perform Step 2b. the boot code is corrupted and not recoverable.

c. Type **install** [bt] [sm <*slot*>] <*version*> at the PXM prompt.

Caution Do not touch the VISM card until the status comes back ('Sent xxx bytes in yyy seconds'). Failure to follow this recommendation will corrupt the boot code and it will not be recoverable.

When the boot code is being written to PROM, you will see comments displayed at the VISM prompt. This is normal and expected behavior.

Step 3 Use the **resetcd** command for VISM from the PXM card for the latest boot take effect.

Step 4 Type the **version** command to verify the correct boot code.

Note Step 4 is optional.

You have completed upgrading the new VISM backup boot code.

VISM Boot Code Upgrade Procedure with PXM1E and PXM45 Cards

The boot code has not changed from VISM Release 3.1(1) to Release 3.1(2). Therefore, the procedure in this section is the same as the upgrade procedure for Release 3.1(1).

Complete the following steps to upgrade the new backup boot code when you are using PXM1E or PXM45 cards in your MGX 8000 Series chassis:

Step 1 Complete the steps in the VISM Firmware and Boot Code Download Procedure for PXM1E and PXM45, page 6.

Step 2 Log on to the PXM1E or PXM45 card.

Step 3 Use the **burnboot** *sm-primary-slot-num new-rev* command, where *sm-primary-slot-num* is the slot number of the VISM/VISM-PR card you want to upgrade and *new-rev* is the firmware version number of the new VISM software, to upgrade the VISM/VISM-PR boot code.

The VISM/VISM-PR card automatically resets and becomes active with the latest boot code image. You have completed the boot code upgrade procedure.

VISM Downgrade Procedure

Use this procedure to downgrade VISM software from software Release 3.1(2) for VISM to the earlier VISM Releases 3.1, 3.0, 2.2, 2.1, and 2.0. By following the downgrade procedure described here, the configurations will be retained after downgrade.

Note It is important to note that the configurations that existed with old-rev firmware should have been saved earlier. You cannot downgrade from VISM-PR to VISM.

Complete the following steps to downgrade the VISM software from software Release 3.1(2) for VISM/VISM-PR to Release 3.1, 3.0, 2.2, 2.1, or 2.0:

Step 1 If the VISM card is in a redundancy group, remove the redundancy.

delred <*SM slot#*>

Step 2 Download the old-rev firmware onto the MGX shelf.

Step 3 Execute the PXM **clrsmcnf** command:

clrsmcnf <*SM slot#*>

where:

SM slot# is the slot number of the VISM card to be downgraded.

The VISM card will be reset on executing this command. Wait for the card to come active.

Step 4 Execute the PXM **restoresmcnf** command:

restoresmcnf -f <*filename*> -s <*SM slot#*>

where:

The *filename* is the name of the old configuration file that was saved while the old-rev firmware was running. The file can be found in the C:CNF directory on the MGX shelf.

The *SM slot#* is the slot number of the VISM card to be downgraded.

The VISM card will be reset again. When the card comes active, it will have the old-rev firmware running and will have the old configuration.

Step 5 Reconfigure redundancy group, if required.

Caveats for VISM Release 3.1(2)

This section describes resolved and open software caveats for Release 3.1(2) of VISM. Caveats describe unexpected behavior or defects in VISM software.

Resolved Caveats in Release 3.1(2)

Table 6 describes the caveats that have been resolved in VISM Release 3.1(2).

Table 6 Resolved Caveats for VISM Release 3.1(2)

DDTS Issue	Description
CSCdy67348	AAL2 SVCs: Path confirmation fails on some endpoints with 248 SVCs.
CSCdx68992	AAL1 SVC: DSP failed to detect tones in AAL1 encapsulation.
CSCdy73727	NY: VISM gets a dummy PXM switchover message, unable to make further SVC calls.
CSCdy57985	VISM requires RtpConnMode be mandatory for configuration.
CSCdz32849	Announcement file on VISM-PR is distorted due to different SSRC.
CSCdz37440	VISM crashes running SPVC load with statistics enabled from CWM.
CSCdz43252	VISM switchover causes entire SPVC network into line alarm.
CSCdz49351	Heavy noise distortion VISM VOIP solution Call Manager.
CSCdz58275	VISM: VISM considers M: connection mode parameter to be mandatory in MDCX.
CSCdz89440	PRI sessions are not switching when Call Agents switch over.
CSCea15910	MGCP on VISM cannot parse SIP messages from 827.
CSCdy19561	VISM rejects call with supported codec (G.723.1-H).
CSCdy73454	No MGCP response with mgciSendUdpPacket failure.
CSCdy82378	NY: RTP trunked connections remain in alarm when PVC goes in/out of alarm.
CSCdz30279	VISM needs to support case insensitivity of DNS and MGCs.
CSCdz64830	Broadcast T.38 Fax relay calls on 40+ endpoints on the VISM fails.

Table 6 Resolved Caveats for VISM Release 3.1(2) (continued)

DDTS Issue	Description
CSCdz65510	T.38 calls fail in VoIP trunking.
CSCdz69373	Voice quality issues with fixed jitter mode on G726-32K.
CSCdz74863	VISM does not resolve domain names after a shelf reset.
CSCdz75592	TI POS fix, reduce POS detection time to 100ms.
CSCdz75653	TI fix, use configurable dual tone detector for Marconi phones.
CSCin12468	The addses command accepts session priority > 4.
CSCdx58768	HI: G.723.1 codecs not displayed properly in dspcodecparams output.
CSCdx80992	PCR > 50000 allowed for vbr-rt AAL2 bearer application for VISM-8T1.
CSCdz27893	VISM 3.1 doesnt notify ORBK when flash is detected on 911 trunks.
CSCdz83314	DSP does not suppress the mid-call dtmf tones on the bearer in SVC.
CSCea03861	AUEP with F: s,e,r,n gets strange string in response
CSCea14620	VISM: MGCP parse error for AS53xx SDP string with T.38 parameters
CSCea24517	COT testing with CRCX M:loopback failed for switched AAL2 PVC mode
CSCea24522	make oam loop back timer configurable
CSCea53197	loud noise heard when line alarm is being cleared
CSCea53238	bad announcement file causes VISM to reboot

Open Caveats in Release 3.1(2)

Table 7 describes the open caveats in VISM Release 3.1(2).

Table 7 Open Caveats for Software Release 3.1(2) for VISM/VISM-PR

DDTS Issue	Description
CSCdx94130	Symptom: VISM loses some DTMF digits when ON time is less than 45ms. Conditions: VISM randomly fails to detect some of the digits resulting in call failure. Workaround: The equipment should generate DTMF digits with ON time greater than or equal to 45ms.
CSCdy60917	Symptom: NY: VISM resets when connection on PXM1 is misconfigured. Conditions: None. Workaround: To configure a PXM1 connection, refer to the *Cisco MGX 8850 Multiservice Switch Installation and Configuration Guide.*
CSCdy82951	Symptom: VISM-PR card reboots when all E1 lines with CIDs goes into alarm. Conditions: None. Workaround: None.

Table 7 Open Caveats for Software Release 3.1(2) for VISM/VISM-PR (continued)

DDTS Issue	Description
CSCdz64206	Symptom: Degradation of voice quality occurs when sending announcement RQNTs on 240 endpoints. Voice quality is good up to 185 endpoints, but quality starts to progressively deteriorate up to 240 endpoints. Conditions: When more than 145 concurrent announcements exist on VISM and VISM-PR cards, traffic is lost on multiple endpoints. This symptom occurs on MGX 8850 with VISM cards running Release 3.1.0.35-I. Workaround: Limit concurrent announcements on VISM and VISM-PR cards to 130.
CSCdz65552	Symptom: Running Fax Pass-Thru load over ISDN PRI fails in VoIP Switching mode Description: On a VISM-T1 in Voip Switching mode, running a fax pass thru call load over ISDN PRI for extended periods of time causes call completion rate to go down. Workaround: None.
CSCea13662	Symptom: Latency increases when VAD Off is selected from cnfprofelemvoice. Conditions: None. Workaround: Disable VAD using the MGCP message.
CSCea42208	Symptom: VISM card stuck in boot after switchcc; standby VISM does not take over. Conditions: Shelf is moderately loaded with light traffic. Workaround: 1. Reset the card that is stuck in boot, which makes standby take over. 2. Softswitch to make primary card active.
CSCea45931	Symptom: VISMs do not recover after a power outage on the node. Conditions: None. Workaround: Physically remove and reinsert the VISM cards.
CSCea62890	Symptom: DSP crashes after a failed T.38 fax call timeout. After a failed T.38 fax call, the call timeouts. VISM attempts to recover the call by sending the compression DSP idle mode command and voice mode commands. The voice mode command has 22 (T.38) as the payload type and 0 as the payload size, which makes the compression DSP crash. Conditions: This symptom occurs when the VISM has already switched to T.38 fax mode, and the T.38 fax has failed. Workaround: None.
CSCea64244	Symptom: VISM reset due to CTRL-X. Conditions: User reset by CTRL-X is a generic message that is used when the reset reason is unknown. Workaround: Unknown.
CSCea64302	Symptom: VISM resets while running T.38 VoIP trunking and VoIP switching load. Conditions: This problem is associated with running a load of T.38 fax calls over a VISM T1 card configured for PRI D-channel signaling. Workaround: Use T1 in CAS signaling mode when running more than two spans of T.38 fax calls.

Table 7 Open Caveats for Software Release 3.1(2) for VISM/VISM-PR (continued)

DDTS Issue	Description
CSCea74389	Symptom: 5ms of VAD delay even when VAD is off and not running. Conditions: None. Workaround: None.
CSCea76010	Symptom: VISM-PR card only supports 145 endpoints after card upgrade. After upgrading from a VISM legacy card to a VISM-PR card, you cannot add endpoints beyond 145 if you are using codec template 1. The VISM-PR card must be reset to add the additional endpoints. Conditions: This symptom occurs on the MGX 8850 while upgrading from a VISM legacy card to a VISM-PR card running release 3.1.0.59. Workaround: Reset the VISM-PR card by using the **resetcd** or **softswitch** commands from PXM.
CSCea86291	Symptom: AAL2 switched virtual circuit (SVC) active calls are dropping during PXM45 switchover. Conditions: If voice calls are configured on an MGX utilizing AAL2 SVCs, the voice calls are dropped when a manual or automatic PXM switch-over occurs. Workaround: None.

Anomaly Status Changes in Release 3.1(2)

The following table lists anomalies that have changed status since in Release 3.1(2). Changed status means that the anomaly went from open to a state other than resolved. The status field states whether the anomaly is closed, junked, duplicated, or unreproducible.

Bug ID	Status
CSCdy88166	Voice clipping with buffer overflow; Closed. Workaround: If you use AAL2 trunking, it is recommended that you use the cnfcodecjtrdelay "codecType jitter_mode jitter_initdelay" to set the jitter_mode to fixed and the init_delay to 20 ms.

Caveats Resolved in Release 3.1(1)

Table 8 describes the caveats issued against VISM software that have been resolved in software Release 3.1(1).

Table 8 Resolved Caveats for Software Release 3.1(1) for VISM/VISM-PR

DDTS Issue	Description
CSCuk38197	VISM replies Line Out Of Service to AUEP after cnflnoos/cnflnis.
CSCdw65362	Announcement file play volume is too high, causes distortion.
CSCdy26382	VISM encapsulates UDPTL for T.38 over RTP
CSCdy36418	CSCdy36418 VISM-PR card must be reset after initial installation into MGX shelf
CSCdy39693	Demotion from GW to Line is not happening
CSCdy46975	vismscalarchange trap not generated with ip address change
CSCdy87408	POS problem, modem calls failing with G729 codec
CSCdy89344	endpts stay active even when gw. is forced oos
CSCdy89423	DLCX always sent to Inactive call agent
CSCdy89462	need a command to display VCCI
CSCdy89474	cnfoamparams / dspoamparams should be accessible in all mode
CSCdy89494	dspmgcgrps and dspdnallips show different status for MGC
CSCdz00374	POS problem, modem calls failing with G729 codec
CSCdz01636	VISM Reboots when Domain Name has a lengthy name
CSCdz06991	E1 CCS NFAS bits not configurable
CSCdz12617	T38 Fax call made on VISM to 5400 causes VISM DSP to crash
CSCdz32964	Dynamic Payload broken due to file merge

Related Documentation

The following documents contains information that may be useful to software Release 3.1(2) for VISM/VISM-PR:

- *Cisco VISM Installation and Configuration Guide, Release 3.0*
- *Cisco MGX 8830, MGX 8850 (PXM45 and PXM1E), and MGX 8950 Command Reference, Release 3*
- *Cisco MGX 8850 (PXM45 and PXM1E) Hardware Installation Guide, Release 3*
- *Cisco MGX 8850 (PXM45) and MGX 8950 Software Configuration Guide, Release 3*

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this 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 may have 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.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) 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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit your comments by mail by using the response card 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.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- 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

To obtain customized information and service, you can self-register on Cisco.com at this 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 levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- 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.

Cisco TAC Website

You can use the Cisco TAC website 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 website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require 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 this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this 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). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html