



# Release Notes for Cisco Voice Switch Service Module (VXSM) Release 5.0.70

---

These release notes are part number OL-7088-01 Rev. B0, July 27, 2005.

The Voice Switch Service Module (VXSM) product is supported by the MGX 8880 Media Gateway and the MGX 8850 Multiservice Switch. Refer to these release notes for platform and version level support guidelines.

The VXSM software release notes are supported by the *Cisco Voice Switch Services (VXSM) Configuration Guide and Command Reference, Release 5*, which is available on [cisco.com](http://cisco.com).

## Table of Contents

Table of Contents .....	1
About Release 5.0.70 .....	2
New Features in Release 5.0.70 .....	2
Support for Media Gateway Control Protocol .....	2
NFAS with D-channel Backup .....	3
Multiprotocol Service Module Interoperability .....	3
New Features in Release 5.0.20 .....	3
Additional Media Gateway Control Protocol .....	3
PRI Backhaul .....	4
Differentiated Services (DiffServ) .....	4
Computer Assisted Law Enforcement Act (CALEA) .....	4
Voiceband Data Profiles and Event Mapping .....	4
Firmware Images .....	5
Upgrading from an Earlier VXSM Release .....	5
Feature Clarifications .....	6
Online Diagnostic feature as applied to VXSM .....	6




---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

DSP Resources under Mixed Codec Conditions .....	6
Configuring Switching and Trunking Applications .....	7
VXSM Management Information Base .....	7
Compatibility .....	7
Caveats for VXSM Release 5.0.70 .....	9
Open Caveats in Release 5.0.70 .....	9
Resolved Caveats in Release 5.0.70 .....	14
Related Documentation .....	14
Obtaining Documentation .....	15
Cisco.com .....	15
Documentation DVD .....	15
Ordering Documentation .....	15
Documentation Feedback .....	16
Cisco Product Security Overview .....	16
Reporting Security Problems in Cisco Products .....	16
Obtaining Technical Assistance .....	17
Cisco Technical Support Website .....	17
Submitting a Service Request .....	17
Definitions of Service Request Severity .....	18
Obtaining Additional Publications and Information .....	18

## About Release 5.0.70

The VXSM Release 5.0.70 follows VXSM Release 5.0.20.

## New Features in Release 5.0.70

The following new features are introduced in the 5.0.70 release of VXSM.

### Support for Media Gateway Control Protocol

VXSM Release 5.0.70 now supports the Media Gateway Control Protocol (MGCP 1.0) in addition to the two protocols (TGCP and H.248) that are supported in the previous release. At any time only one gateway control protocol is supported on a VXSM card. The protocol is user selectable when the VXSM image is loaded from the PXM disk. This is accomplished through the PXM **setrev** command using the *-ccp <CallControlProtocol>* parameter.

Support for MGCP 1.0 permits interoperability between VXSM and Cisco PGW media gateway controllers.

## NFAS with D-channel Backup

In VXSM Release 5.0.70, when performing ISDN PRI backhaul, the D-Channel in a Non-Facility Associated Signaling (NFAS) voice stream can be protected with the use of a backup D-channel.

NFAS voice streams employ 479 B channels plus 1 D-channel that controls up to a maximum of 20 DS1s interfaces. If the D channel fails it can bring down all the 479 bearer B channels.

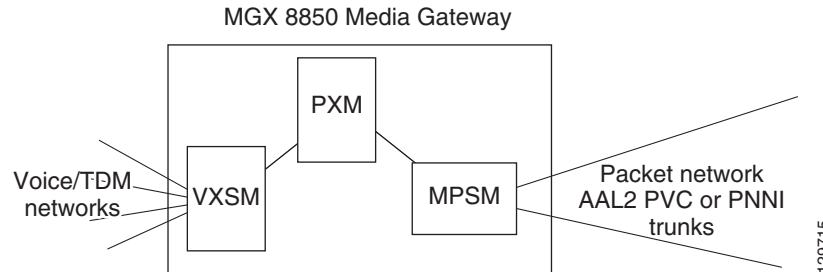
With this feature, the active D channel is protected with a backup D channel. If the active D channel fails, there is a switch over to the backup channel. Failure of the active D-channels causes only the transient calls to be lost during the switch over process. Active calls are maintained, and new calls after the switch over, are handled as usual.

The switch over is handled at the layer 3 (Q.931) level, there are no new VXSM commands associated with this feature.

## Multiprotocol Service Module Interoperability

For AAL2 trunking applications, VXSM can now operate in conjunction with a Multiprotocol Service Module (MPSM) in which the MPSM provides the interface to the ATM network. Interworking with the MPSM enables the MGX Voice Gateway to support IMA, ATM and Frame Relay services with channelized capability on DS1 and DS0 levels.

The MPSM card must be configured for ATM context using the `MPSM cnfclctx atm` command. After the context is set to ATM, provisioning is performed with the `upln`, `addport` and `addcon` command sequence. For more details, please refer to the MPSM user documentation.



## New Features in Release 5.0.20

The following new features were introduced in the 5.0.20 release of VXSM.

### Additional Media Gateway Control Protocol

The Trunking Media Gateway Control Protocol (TGCP) is now supported for communication between the VXSM card and the Media Gateway Controller in switching applications. This is in addition to the H.248 protocol supported in earlier releases. VXSM does not support both protocols simultaneously. The user must select which one of the two protocols is to be used when the VXSM image is loaded initially from the PXM.

## PRI Backhaul

In application where ISDN D channel signaling lines are connected to VXSM, the VXSM card can be configured to extract the layer 3 (Q.931) packets and backhaul them to the media gateway controller

For communication between VXSM and the media gateway controller the protocol stack is based upon the Cisco proprietary Session Manger and RUDP (Reliable UDP).

Communication between the VXSM and the gateway controller is session based. One session set must be established. The session set contain one or two session groups (one for non-fault tolerant or two for fault tolerant configurations). Each session group can support up to four RUDP sessions.

## Differentiated Services (DiffServ)

VXSM provides support for the quality of service (QOS) feature known as DiffServ. The DiffServ feature permits devices at the edge of the network to specify the contents of the Type of Service (TOS) field in the IPv4 header as a differentiated services point code. This point code can then be used by routers in the network to determine per hop behavior (PHB).

## Computer Assisted Law Enforcement Act (CALEA)

VXSM provides support for CALEA intercepted calls. The CALEA feature functions only in switching applications using the TGCP gateway control protocol.

During call setup, the media gateway controller uses the TGCP commands of CRCX and MDCX with CALEA parameters to signify that a call is to be subject to CALEA surveillance. During a CALEA call, the VXSM sends a duplicate of the call contents to a TGCP defined CALEA server.

VXSM supports up to 60 concurrent CALEA calls. Statistics collection for CALEA streams is not supported.

CALEA support is an orderable item. Customers who require this feature must specify the VXSM CALEA firmware image at the time of order.

## Voiceband Data Profiles and Event Mapping

Within a voice circuit call, VXSM now supports the handling of voiceband data such as clear channel, fax, and modem transmissions. VXSM can detect tones associated with voiceband data on both the voice and IP sides of the networks, and act accordingly. Upon detection of a voiceband tone, VXSM will perform the necessary upspeed procedure that may involve the following processing:

- Codec manipulation
- Silence suppression
- Disabling echo cancellation
- Modify packetization period, gain, DC offset, and jitter parameters.

VXSM informs the other (remote) end of the connection when an upspeed procedure is to be performed. There are two different methods by which upspeed at the remote end is triggered.

The first method is Fax/Modem passthrough with a Cisco proprietary protocol in which a Named Signaling Event (NSE) is sent to the remote end.

The second method is Fax/Modem passthrough with IP side tone detection and relies on both ends of the connection being able to detect tones on both the TDM and IP sides. This method is only supported with TGCP or MGCP call setup.

Fax/Modem passthrough features are as follows:

- FAX/Modem Provisioning redundancy.
- Upspeed codec from G711 to G711.
- Upspeed codec from G711 to G726.
- Upspeed codec from G729 to G711 with VXSM to VXSM with low priority.
- Upspeed codec from CCD to G711 with VXSM to VXSM with low priority.
- Upspeed codec from CCD to G726 with VXSM to VXSM with low priority.
- Graceful upgrade for fax/modem provisioning.
- Detection of the following tones, CNG(1100hz), CED/ANS(2100hz), /ANS(2100hz with phase reversal, and V.21 Fax Preamble.

The voiceband event mapping feature permits VXSM to determine how VBD events are to be handled. When this feature is configured, VBD events are mapped to different event handling functions categorized by the attributes defined in different kinds of profiles, such as fax relay profile, or VBD profile.

## Firmware Images

For each VXSM card type (OC-3 or T1/E1), two firmware images are available, namely, Non-CALEA and CALEA. At order time, the user must specify whether a Non-CALEA or CALEA image is required.

The Non-CALEA image is available in three versions. One version supports the H.248 media gateway controller protocol, one supports the MGCP media gateway controller protocol, and the third supports the TGCP media gateway controller protocol. The user must choose between the H.248, MGCP, and TGCP versions when the image is first loaded from the PXM using the **setrev** command.

The CALEA image supports TGCP only. However, this protocol must be explicitly selected when the image is loaded from the PXM using the **setrev** command.

## Upgrading from an Earlier VXSM Release

VXSM can be gracefully upgraded (configuration is preserved) from VXSM Release 5.0.20 so long as the original and the upgraded images are of the same version. Because MGCP is being introduced in this release and does not exist in earlier releases, the only supported upgrades to 5.0.70 are as follows:

- Non-CALEA, TGCP version to Non-CALEA, TGCP version
- Non-CALEA, H.248 version to Non-CALEA, H.248 version.
- CALEA, TGCP version to CALEA, TGCP version.

When loading or upgrading a boot or runtime image to a VXSM card, users must observe the following caution.

**Caution**

Many of the commands involved in loading or upgrading boot and runtime images can take several minutes to execute completely. If the user resets or otherwise disturbs the VXSM card during a loading or upgrading process, the card can easily be damaged to the extent that it must be returned to the factory for repair.

THE REAPPEARANCE OF THE COMMAND PROMPT AFTER A COMMAND IS ENTERED DOES NOT INDICATE THAT THE IMAGE LOAD OR UPGRADE HAS BEEN COMPLETED.

After the execution of the burnboot, clrsmcnf, loadrev, or setrev commands, the user must execute either a **dspcds** or **dsprev** command periodically to verify that the state of the VXSM card being loaded or upgraded is either Active, Standby, or Failed.

ONLY WHEN THE CARD IS DISPLAYED TO BE IN ONE OF THESE STATES IS IT SAFE TO GO TO THE NEXT STEP.

## Feature Clarifications

### Online Diagnostic feature as applied to VXSM.

The online diagnostics feature as implemented on the PXM45 card is supported on VXSM Release 5.0. When enabled, using the PXM45 **cnfdiag** command, this feature performs non-intrusive diagnostic tests that use four of the VXSM's DSP codecs.

If the user executes the VXSM **dspdspcodecpools** command, the resulting display shows the four codecs being used (for diagnostics) and subtracts them from the remaining available codecs (see example below).

```
MGX8850.9.VXSM.a > dspdspcodecpools
=====
                    DSP codec capacity usage
=====

Codec pool          Current utilized  Current available
                    capacity (#calls)  capacity (#calls)
=====
G711 family         4                      8060
G729/G726/T.38 family 0                      4030
```

The online diagnostics feature does not reduce the maximum number of 8064 codecs available for calls on the VXSM card. If the number of call requests on the VXSM is sufficiently high, the online diagnostic feature is disabled automatically and the four codecs are made available for active calls.

### DSP Resources under Mixed Codec Conditions

When the same codec is used to setup calls on the gateway the available DSP resources will be fully utilized. However when different codecs are used to setup calls the amount of utilizable DSP resources may be limited in certain cases due to fragmentation.

Fragmentation is said to have occurred when the available capacities on two different DSP resources have enough available capacity to support a call of a particular codec type but cannot support that codec type individually.

Consider two DSP resources whose available capacity is 1 unit each making the total available capacity 2 units. However a codec that requires 2 units cannot be supported in the system because the available capacities have been fragmented across the individual DSP resources.

The DSP allocation algorithm on VXSM does make an attempt to smooth the effects of fragmentation but towards the end, fragmentation could happen as the future pattern of calls cannot be predicted beforehand.

## Configuring Switching and Trunking Applications

The simultaneous operation of mixed applications (Switched VoIP applications and Non-switched Trunking applications) is not supported on a VXSM card. However, both applications can be supported in the Media Gateway by using multiple VXSM cards.

## VXSM Management Information Base

The VXSM Management Information Base (MIB) Version 5.0.70 is available by request through your Cisco VXSM product marketing representative.

## Compatibility



### Note

VXSM Release 5.0.70 is only supported with PXM-45.

VXSM software interoperability with the Cisco MGX 8850 (PXM45) Multiservice Switch or the MGX 8880 Media Gateway platform software is listed in [Table 1](#).

**Table 1** VXSM Software Interoperability

Product	Latest Firmware	Min. Firmware
PXM45	5.0.20	5.0.20
RPM-XF	12.3(7)T3	12.3(7)T3
CWM	15.0.0P4	15.0.0P4
MGM	5.0.0	5.0.0
VISM-PR*	3.3.10	3.3.10
MGX-AXSM-16-155/B	5.0.20	5.0.20
MGX-AXSM-4-622/B	5.0.20	5.0.20
BTS*	4.4.2	4.4.2
PGW	9.5.2	9.5.2
Cisco 2600 Series Routers*	c2600-ipvoice-mz.123-9.13.T	c2600-ipvoice-mz.123-9.13.T

**Table 1 VXSM Software Interoperability (continued)**

Product	Latest Firmware	Min. Firmware
Cisco 2600 for use as an IP Transfer Point*	c2600-ity-mz.122-21.SW bin	c2600-ity-mz.122-21.SW bin
Cisco 3700 Series Routers*	c3725-ipvoice-mz,123-9.13.T	c3725-ipvoice-mz,123-9.13.T
Cisco ATA 188*	3.2.0 for SIP/MGCP/H323	3.2.0 for SIP/MGCP/H323
Linksys PAP2 Phone Adapter	Version 2.0.6 (LS)	Version 2.0.6 (LS)
Linksys RT31 Router	Version 1.27.01	Version 1.27.01

Table 2 describes the software images available for Release 5.0.70 for VXSM.

**Table 2 Software Images for Release 5.0.70 for VXSM**

Board Pair	Latest Boot Code Version	Minimum Boot Code Version	Firmware
MGX-VXSM-155, CALEA	vxsm_005.000.070.200_bt.fw	vxsm_005.000.070.200_bt.fw	vxsm_005.050.070.200.fw
MGX-VXSM-155, Non-CALEA	vxsm_005.000.070.200_bt.fw	vxsm_005.000.070.200_bt.fw	vxsm_005.000.070.200.fw
MGX-VXSM-T1E1, CALEA	vxsm_005.000.70.200_bt.fw	vxsm_005.000.070.200_bt.fw	vxsm_005.050.070.200.fw
MGX-VXSM-T1E1, Non-CALEA	vxsm_005.000.070.200_bt.fw	vxsm_005.000.070.200_bt.fw	vxsm_005.000.070.200.fw

# Caveats for VXSM Release 5.0.70

This section describes software caveats for Release 5.0.70.

## Open Caveats in Release 5.0.70

Table 3 describes the open caveats in VXSM Release 5.0.70.

**Table 3** Open Software Caveats for VXSM Release 5.0.70

DDTS Issue	Description
CSCeh52082	<p><b>Headline:</b> Card in failed state after vsi callback err</p> <p><b>Symptom:</b> Standby card went failed after doing lot of cnfcon for priority routing change and preferred route change with 900 connections on the card.</p> <p><b>Conditions:</b> VSI Conn. call back failed on standby.</p> <p><b>Workaround:</b> This has happened once, need to reproduce it again to find the root cause. Workaround: is not to execute lot of priority bumping</p>
CSCeh55195	<p><b>Headline:</b> vxsm-oc3 in failed state after burnboot or resetcd</p> <p><b>Symptom:</b> vxsm cards in failed state after reset or burnboot on both active and standby</p> <p><b>Conditions:</b> The problem was reported once, but the condition for the error to occur is unclear. Therefore, the root cause is still under investigation.</p> <p><b>Workaround:</b> Perform clrsmcnf to bring the cards back to service.</p>
CSCeh11539	<p><b>Headline:</b> Card failed with CRML DSPAPI ERR, sustaining 2STM1 g.729a</p> <p><b>Symptom:</b></p> <ul style="list-style-type: none"> <li>a) Call-setups fail with 'Channel EXCEPTION! (non-fatal)' logged onto the PXM log</li> <li>b) In a remote scenario the involved DSP could throw a DSP Exception (fatal). This will result in a VXSM switchover if redundancy is configured. If redundancy is not configured, the card will go into an Active-F state.</li> </ul> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>a) The issue occurs only when codec negotiation is used in the call-setup. In other words, the problem occurs only when the call-agent does not specify a codec list, resulting in the gateway opening a DSP channel with the entire list of codecs. This list is then shrunken when the final choice of codec is made.</li> <li>b) The issue occurs when the VXSM is operating near full-capacity. In other words, when the DSPs have close to no room left to setup new calls.</li> </ul> <p><b>Workaround:</b> Do not use codec negotiation. The call-agent needs to specify the exact codec that needs to be used on the call.</p>

**Table 3** Open Software Caveats for VXSM Release 5.0.70 (continued)

<b>DDTS Issue</b>	<b>Description</b>
CSCeh47956	<p><b>Headline:</b> sysDiag reported online diag failure for VXSM causing reset</p> <p><b>Symptom:</b> Online diag failure</p> <p><b>Conditions:</b> The error happened under intermittent hardware failure condition of the ATMizer parity on the one card.</p> <p><b>Workaround:</b> Online diag may be turned off by issuing cnfdiag slot# disable However, the errors noted was one-time occurrence for one card where the hardware failure occurred, and was un-reproducible on another chassis. The card will not be reset if there is no redundancy (as the diagnostic failures are Major, not fatal). If there is redundancy set up, the card would be reset.</p>
CSCeh48876	<p><b>Headline:</b> dspchanloops shows the opposite of configured chan loop type</p> <p><b>Symptoms:</b> VXSM displays wrong loopback type information with dspchanloops command.</p> <p><b>Conditions:</b> This symptom was observed while displaying dspchanloops command.</p> <p><b>Workaround:</b> Use dspchanloop command to display loopback information.</p>
CSCeh49855	<p><b>Headline:</b> vsi callback err caused card reset</p> <p><b>Symptom:</b> Standby card reset one more time after resetting all the service modules in the shelf back to back</p> <p><b>Conditions:</b> VSI connection call back failed and after one reset, the standby came up ok</p> <p><b>Workaround</b> This has happened once, need to be reproduced to find the root cause.</p>
CSCeh12805	<p><b>Headline:</b> ip availability should not block entering configuration</p> <p><b>Symptom:</b> addmgcgrpmgc,cnfxgcpmgc can not be done if cnfmgc returns error.</p> <p><b>Conditions:</b> cnfmgc can fail if DNS server is not configured for this mgc domain or DNS server is not reachable.</p> <p><b>Workaround:</b> None. (If resolved IP addresses for a mgc name are known, can have a static mgc defined on the VXSM till DNS server is back up)</p>
CSCeh50745	<p><b>Headline:</b> cardMon task exception error caused card reset.</p> <p><b>Symptom:</b> When resetcd is performed on a VXSM card there is a very slight chance that.it will encounter a Vector 7 Exception and then reset itself again. It should.then come up normally.</p> <p><b>Conditions:</b> A large amount of VXSM resetcd calls should lead to this problem.</p> <p><b>Workaround:</b> None is needed since it is self-correcting. Once it hits this Vector 7 exception it will reset itself and come up normally afterwards.</p>
CSCeh56654	<p><b>Headline:</b> AAL2MP:VSIC-2-VSIMAJORERR on VXSM-RED after PXM45 reset</p> <p><b>Symptom:</b> VSI error log on the system</p> <p><b>Conditions:</b> This error is for releasing TCB buffers and it happens when PXM card gets reset in the shelf without having redundancy for PXM card.</p> <p><b>Workaround:</b> The error is harmless but needs to be identified</p>

**Table 3** Open Software Caveats for VXSM Release 5.0.70 (continued)

DDTS Issue	Description
CSCeh39863	<p><b>Headline:</b> AAL2MP:SYS-3-RUNAWAYTASK error logged during Offline Diag</p> <p><b>Symptom:</b> A SYS-3-RUNAWAY warning message is logged during offline diag execution.</p> <p><b>Conditions:</b> There is no condition which will cause the message to be logged.</p> <p><b>WorkAround:</b> There is no affect on the node and card under test, other than the warning message being logged.</p>
CSCeh43530	<p><b>Headline:</b> Ecan still ON during V.34 modem calls with AAL2 M-&gt;M configuration</p> <p><b>Symptom:</b> When make trunking modem call (CED with PR), during upspeed, the ECAN on the original side kept as ON. The modem call passed successfully.</p> <p><b>Conditions:</b> It is happen only if both CAC are set to master.</p> <p><b>Workaround:</b> Set CAC to slave in one side if it is allowed; otherwise none.</p>
CSCeh44232	<p><b>Headline:</b> CPRO provides CRML old traffic params on slave end upon VSIRM update</p> <p><b>Symptom:</b> The master and slave ends have different traffic parameters after cnfcon on the master end.</p> <p><b>Conditions:</b> Always.</p> <p><b>Workaround:</b> Execute cnfcon on slave and as well, with same parameters as on the master.</p>
CSCeh46000	<p><b>Headline:</b> PcmTraceTask hogging mem.buffer (all caller-ctc_msg_evt_deliver)</p> <p><b>Symptom:</b> PcmTraceTask blocks while taking an Empty Binary Semaphore. This could be viewed as a ssi memory leak.</p> <p><b>Conditions:</b> The task will remain blocked until PCM tracing has started.</p> <p><b>Workaround:</b> None</p> <p><b>Further Problem Description:</b> The resource will be held up until PCM tracing is performed in order to debug any issue. With that the Empty Binary Semaphore is released and the Pcmtrace task unblocks. This is a very minor issue and the memory held is very small and it does not vary. There is not impact on the performance of other tasks and there is no resource contention with other tasks.</p>

**Table 3** Open Software Caveats for VXSM Release 5.0.70 (continued)

DDTS Issue	Description
CSCeh46551	<p><b>Headline:</b> tDspApi ssiSemGive errors for the block owned by different task</p> <p><b>Symptom:</b> The PXM error log may occasionally contain messages like "tDspApi ssiSemGive SSI_SEMID 0xyyyyyy is not owned by giving task. It is owned by task 0xffffffff".</p> <p>yyyyyy above can be a six-digit number.</p> <p><b>Conditions:</b> This may be seen only when certain lines, PVC's or CID's go in or out of alarm in an AAL2 Trunking scenario.</p> <p><b>Workaround:</b> None.</p> <p>Further problem description: These messages are harmless and can be ignored.</p>
CSCeh47935	<p><b>Headline:</b> tsyncRamdb failed to unblock the application</p> <p><b>Symptom:</b> Failed to unblock application error</p> <p><b>Conditions:</b> During card reset</p> <p><b>Workaround:</b> None</p>
CSCef92799	<p><b>Headline:</b> In AAL2 trunking, vad and ec while uspeeding gives wrong state</p> <p><b>Symptom:</b> This is only for trunking upspeed (fax call) between VXSM and VISM and the fax call from VXSM to VISM which means the call is detected on VISM side. During upspeed, the ECAN of the VXSM changed to disable, but the ECAN of VISM kept as enable. The reason of ECAN of VXSM changed to disable is VISM sending NSE193 to VXSM.</p> <p><b>Conditions:</b></p> <p>(1) Add cid between VXSM and VISM as: VAD on ECAN on</p> <p>(2) Send fax call from VXSM to VISM (V.21 Fax pre. tone detected on VISM side)</p> <p>(3) During upspeed check ECAN for both VXSM cid and VISM cid: ECAN off in VXSM cid ECAN on in VISM cid</p> <p>(4) the fax call passed successful</p> <p><b>Workaround:</b> None.</p>

**Table 3** Open Software Caveats for VXSM Release 5.0.70 (continued)

<b>DDTS Issue</b>	<b>Description</b>
CSCeh00191	<p><b>Headline:</b> Notify not sent when COT played multiple times</p> <p><b>Symptom:</b> Gateway informs Call agent about Transponder COT success even when TDM equipment does not stop playing back COT tone. Ideally Gateway should respond a timeout in this situation (rfc 3336).</p> <p><b>Condition:</b></p> <ul style="list-style-type: none"> <li>-CA requests GW to do Transponder COT.</li> <li>-GW generates COT tone towards TDM equipment.</li> <li>-TDM equipment sends COT tone back towards GW.</li> <li>-TDM equipment does not remove COT tone after specified duration (rfc3336).</li> </ul> <p><b>Workaround:</b> None.</p>
CSCeh16122	<p><b>Headline:</b> CUTW-5-INVALID_PARM messages are flooding the log</p> <p><b>Symptom:</b> CUTW-5-INVALID_PARM messages flooding the log</p> <p><b>Conditions:</b> Normal</p> <p><b>Workaround:</b> NONE</p>
CSCeh17624	<p><b>Headline:</b> Upspeed Codec should default to G.711a on E1</p> <p><b>Symptom:</b> Upspeed Codec should default to G.711a on E1</p> <p><b>Conditions:</b> Normal</p> <p><b>Workaround:</b> Set Upspeed Codec to G.711a on E1 card</p>
CSCeh36036	<p><b>Headline:</b> AAL2MP: Delcon failed on slave, stuck in Mismatch, after Switched</p> <p><b>Symptoms:</b> VXSM was confogired for redundancy. VXSM displays "Invalid opcode in received passup response msg!" error instead of appropriate error when delcon command was executed while Standby is coming up.</p> <p><b>Conditions:</b> This symptom was observed while deleting slave connection during standby card was in initialization state.</p> <p><b>Workaround:</b> Don't delete the slave connection while standby is coming up.</p>
CSCeh34165	<p><b>Headline:</b> AAL2MP: Addcon w/slave failed, need more clear Error msg.</p> <p><b>Symptoms:</b> With the VXSMs SPVC conns thru PNNI, when the Master end already exists, Addcon on the slave end was rejected with "Passthrough failed!" instead of "Connection already exists!" message.</p> <p><b>Conditions:</b> This symptom was observed while adding slave connection after deleting the connection.</p> <p><b>Workaround:</b> Delete master connection before slave connection.</p>

## Resolved Caveats in Release 5.0.70

Table 4 describes the open caveats that existed in VXSM Release 5.0.20 and are now resolved in Release 5.0.70.

**Table 4 Release 5.0.20 Caveats that are resolved in Release 5.0.70**

DDTS Issue	Description
CSCeg20645	Headline: Enabling VAD causes voice quality score to drop
CSCin85117	Headline: cnfvifterm fails with error code 921 when descriptive name enabled
CSCeg48031	Headline: VXSM sends line level RSIP instead of root level
CSCeg51035	Headline: MGC traversal does not work in the right order for RSIP
CSCeg53337	Headline: End to end bearer path is established when COT is in progress
CSCeg54211	Headline: delvif after switchover does not generate RSIP
CSCeg55517	Headline: Unsolicited Console display during CAC rejection
CSCin84810	Headline: Service Change not sent from 1.4 OC3 line upon introducing alarms
CSCeg29796	Headline: CCD codec upspeed has diff. Ecan state on ori & term. endpoints
CSCeg40468	Headline: delevntmapping needs to delete entry with just one index
CSCeg51713	Headline: With AAL2 trunking - some dtmf missing with vad on (G711 and G726)
CSCeg46095	Headline: DTMF Relay doesn't work when MGC omits optional NTE fntp line
CSCeg57781	Headline: VXSM should reject RQNT if GW is forced OOS using cnfgwoos
CSCeg60497	Headline: cli updated needed for sensor 6 for new version hw
CSCeg64615	Headline: RCON information displayed incorrectly when using VXSM.
CSCeg60879	Headline: Upgrade fails from 5.50(15.23)A to 5.50(16.17)P1

The MGX-VXSM-155 card is also known as the MGX-VXSM-4OC card.

The MGX-VXSM-T1/E1 card is also known as the MGX-VXSM-48T1/E1 card.

## Related Documentation

The following documents contains information that may be useful to software Release 5.0 for VXSM:

- *Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Configuration Guide, Release 5*
- *Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Hardware Installation Guide, Releases 2 Through 5*
- *Cisco ATM Services (AXSM) Configuration Guide and Command Reference for MGX Switches, Release 5*
- *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*
- *Cisco MGX 8880 Media Gateway: A Guide to User Documentation.*
- *Release Notes for Cisco MGX 8850 (PXM1E/PXM45), Cisco MGX 8950, and Cisco MGX 8830 Switches, Release 5.0.00*

# 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/univercd/home/home.htm>

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](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

### Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>

- *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>

- 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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2005, Cisco Systems, Inc.  
All rights reserved.

